

Hybrid FM Stereo Encoder using DDS

for carrier and pilot signal generation

Manolis G.Tampouratzis ¹

¹ Department of Electronic Engineering

Faculty of Applied Sciences

Technological Educational Institute of Crete

Romanou 3 Chalepa, 71333 Chania, Crete, Greece

{tampouratzis@chania.teicrete.gr}

George A. Adamidis ² (MSc in Electronic Physics)

² 1 E.K Heraklion – Technical School Laboratories

Division of Electronics

Itanou 40 Kipoupoli, 71307 Heraklion, Crete, Greece

{sv7fid@yahoo.gr}

Abstract - An fm-stereo generator device uses a complex modulation system, according to F.C.C standards, to achieve a compatible mono/stereo system of broadcasting. There are several approaches for building an FM-Stereo generator. In the current implementation, we present an hybrid FM-stereo generator which uses both digital and analog techniques. We use Direct Digital Synthesis (DDS) module for carrier and pilot tone generation which gives unlimited control over phase shift and the ability to produce clean (purely sinusoids) signals with great frequency accuracy and stability. Reference clock frequency (or crystal choice) is not very critical in a high resolution DDS and signal generation becomes simple, robust and completely accurate. Finally using DDS also diminishes the necessity of using complex (high order) filtering.

Keywords – direct digital synthesis (DDS) , fm stereo generator, pilot signal, carrier, balanced modulator, fm stereo spectrum

I. INTRODUCTION

FM stereo broadcasting was introduced during the early 1960s. The fm stereo system which approved for use by the F.C.C in the U.S and later was adopted worldwide uses a complex modulation system to achieve a compatible mono/stereo system of broadcasting. Essentially, the system performs the multiplexing of two audio signals and further combines them into a complex baseband signal that modulates the FM carrier.

The system works by broadcasting a sum of the left (L) and right (R) audio channels, a pilot tone of 19 kHz and a double sideband suppressed carrier (DSBSC) sub-channel that contains the difference of the two audio channels (see fig. 1).

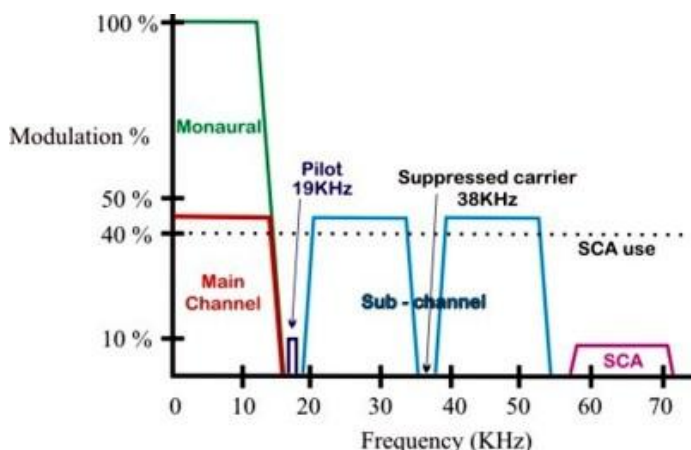


Fig. 1. The Composite FM-Stereo Spectrum

In a simple monaural system, the FM channel is frequency modulated $\pm 75\text{KHz}$ with the audio information and the monaural audio signal occupies the 0-15KHz spectrum of the transmitted frequency spectrum (see figure 1). When stereo is transmitted, the same monaural signal (left plus right channel combined) remains in the 0-15KHz spectrum of the FM stereo signal and an additional sub – channel, centered at 38 KHz, which is a double sideband suppressed carrier signal (DSBSC) is additionally transmitted (see figure 1). This subcarrier is a left-subtracted-from-right (L-R) signal, which, when fed through a matrix with the monaural main channel on the receiver, forms the individual left and right channels. An additional pilot carrier signal at 19 KHz is also transmitted. The pilot signal is phase-cohered (synchronized), to the suppressed 38 KHz carrier.

In an FM-stereo system, the monaural signal is modulated about 45%, the sub channel and the pilot tone are modulated 45% and 10%, respectively, so that the total modulation for a stereo FM- station is 100%. In modern stations where some SCA or RDS/RBDS subcarriers are also used, the modulation of the main and the sub channel are furthermore reduced in order to the total modulation being kept less than 100% ($\pm 75\text{KHz}$ deviation).

In an FM-stereo receiver the 19 KHz pilot signal indicates that the transmission is stereo. The receiver regenerates the 38 KHz carrier and then uses coherent detection for the sub-channel. Coherent detection only works when the carrier is present at the receiver. Of course, the receiver can not obtain the 38 KHz carrier from the baseband signal directly (because the carrier is suppressed during transmission). The carrier is actually obtained in the receiver from the 19 KHz pilot signal.

The composite FM-stereo signal that modulates the FM carrier in any FM-station is generated from a device which is often called as an “FM-Stereo Generator” or as an “FM-Stereo encoder”. The typical theoretical diagram of an FM-stereo generator is shown on fig. 2

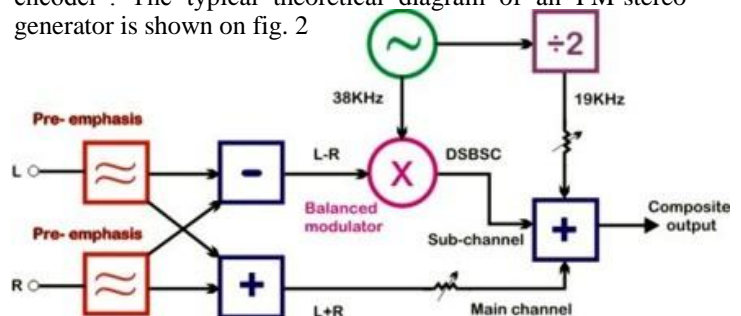


Fig. 2. Typical Theoretical diagram of an FM-Stereo Generator

With respect to figure 2, both the left and the right audio channels are pre-emphasized, just as normal monaural signal would be. Then, the left and the right signals are both added and subtracted on a matrix. The audio signals added (L+R), form the monaural signal which is the main channel. The subtracted signals (L-R) are modulated on a 38 KHz carrier, to form the sub-channel. A balanced modulator is used; because the system requires that the carrier at 38 KHz will be suppressed, leaving only the modulated audio information. The 38 KHz oscillator is divided by 2 to produce the coherent 19 KHz pilot signal. Both the carrier and the pilot signal should be purely harmonics (sinusoidal), otherwise some undesirable (spurious - noise) signals may appear in the composite spectrum.

The three components of the stereo signal, i.e. the main channel, the sub channel and the pilot tone, are combined at the proper ratios (45%, 45%, 10%), forming the composite output.

II. THE HARDWARE – GENERATION OF CARRIER AND PILOT SIGNALS

Before the DDS era, producing “clean” carrier and pilot signals at 38 and 19 KHz respectively, considered to be a difficult task. An oscillator based on a crystal or a ceramic resonator, was often used. Since there are not many 38 KHz resonators available in the market, carrier and pilot signals often produced after some divisions (usually by 12 and 24) from a 455-456 KHz ceramic resonator. The dividers were digital circuits based on flip-flops and modulo-x counters and they produced pulsed signals rather than “clean” sinusoids. Some filters had to be used for suppressing the harmonics and producing the sinusoids. Unfortunately, the filters could not fully suppress harmonics and they also produced some phase shift (pilot tone was phase sifted in respect to the carrier). Harmonics induced undesirable noise (indermodulation products) and significantly degraded the composite stereo signal. The phase shifts also, made carrier regeneration and coherent detection of the sub-channel problematic at the receiver.

After 90s decade, many designers preferred to use an alternative approach for carrier and pilot generation. That approach based on using a microcontroller for producing the carrier rather using an ordinary oscillator. The pilot tone was still derived by using division by 2. That approach gives some flexibility on choosing the reference crystal, but microcontrollers and dividers produce pulsed (digital) signals and strict filtering was yet essential.

Fortunately, now (in 2014) we have DDS, which gives unlimited control over phase shift and the ability to produce clean (purely sinusoids) signals with great frequency accuracy and stability. Reference clock frequency (or crystal choice) is not very critical in a high resolution DDS and signal generation becomes simple, robust and completely accurate. Using a DDS also diminishes the necessity of using complex (high order) filtering.

Here’s a breakdown of the internal circuitry of a DDS device: its main components are a *phase accumulator*, a means of *phase-to-amplitude conversion* (often a sine look-up table), and a DAC. These blocks are represented in Figure 3.

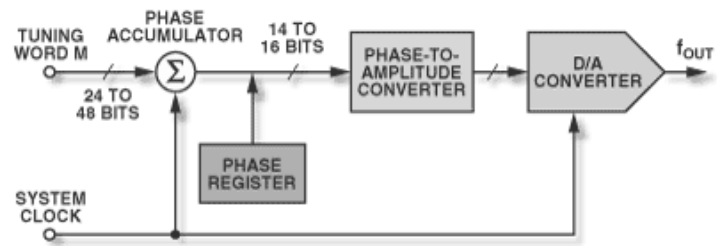


Fig. 3. Components of a direct digital synthesizer.

A DDS produces a sine wave at a given frequency. The frequency depends on two variables, the *reference-clock* frequency and the binary number programmed into the frequency register (*tuning word*).

The binary number in the frequency register provides the main input to the phase accumulator. If a sine look-up table is used, the phase accumulator computes a phase (angle) address for the look-up table, which outputs the digital value of amplitude—corresponding to the sine of that phase angle—to the DAC. The DAC, in turn, converts that number to a corresponding value of analog voltage or current. To generate a fixed-frequency sine wave, a constant value (the phase increment—which is determined by the binary number) is added to the phase accumulator with each clock cycle. If the phase increment is large, the phase accumulator will step quickly through the sine look-up table and thus generate a high frequency sine wave. If the phase increment is small, the phase accumulator will take many more steps, accordingly generating a slower waveform.

A phase-to-amplitude lookup table is used to convert the phase-accumulator’s instantaneous output value with unneeded less-significant bits eliminated by truncation into the sine-wave amplitude information that is presented to the (10-bit) D/A converter. The DDS architecture exploits the symmetrical nature of a sine wave and utilizes mapping logic to synthesize a complete sine wave from one-quarter-cycle of data from the phase accumulator. The phase-to- amplitude lookup table generates the remaining data by reading forward then back through the lookup table. This is shown pictorially in Figure 4.

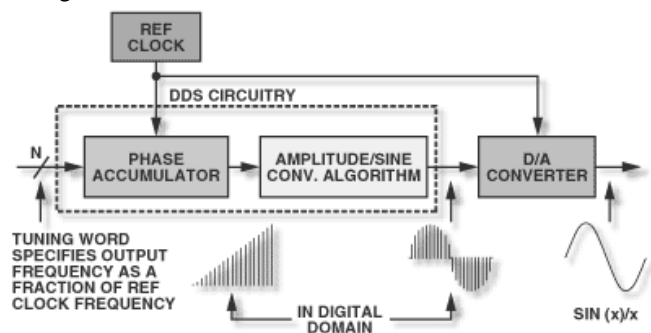


Fig.4 Signal flow through the DDS architecture.

A. The DDS Generator

In this fm-stereo encoder, we use Direct Digital Synthesis (DDS) for carrier and pilot tone generation. Referring to the DDS generator circuit section, the carrier and the pilot signal are generated from two AD9834 DDS ICs. Every AD9834 is used to generate a pure sinusoid signal. Both DDS IC's are kept synchronized by using the same reference clock, and their phase relationship can be digitally controlled. An 18F1220 PIC microcontroller is used to control the DDS generators through I2C signalling interface. The I2C interface is implemented as "bit-banging" on normal I/O.

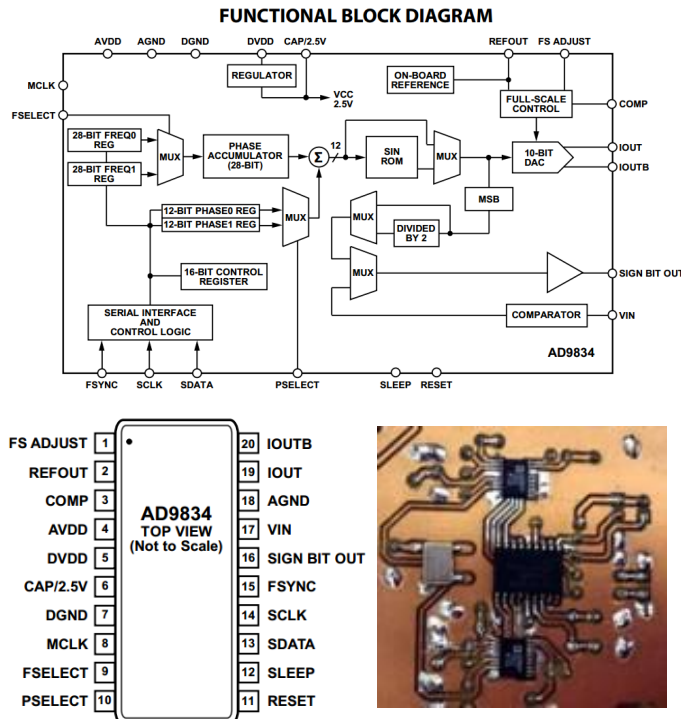


Photo 1. The DDS generator. The carrier and the pilot signal are generated from two AD9834 DDS IC's. An 18F1220 PIC microcontroller (at the center of the photo) is used to control the DDS generators. Both DDS ICs are kept synchronized by the same reference clock (seen at the left side of the photo).

– Fig. 6. Functional Block Diagram AD9834 IC – Fig.7 . Pin Configuration AD9834 IC.

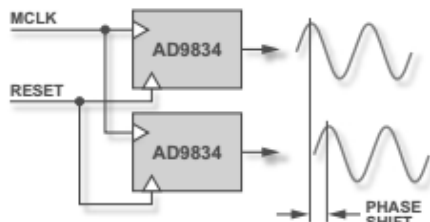


Fig.8 Multiple DDS AD9834s IC's Synchronous Mode Setup of DDS generation with the same reset pin and master reference clock

A reset, after power-up and prior to transferring any data to the DDS, sets the DDS output to a known phase, which serves as the common reference point that allows synchronization of multiple DDS devices. When new data is sent simultaneously to multiple DDS units, a coherent phase relationship can be maintained, and their relative phase offset can be predictably shifted by means of the phase-offset register.

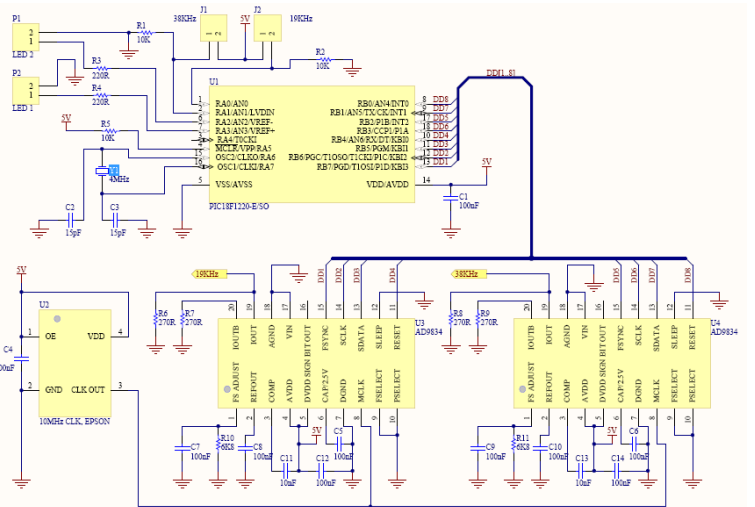


Fig. 5. DDS Section – Carrier and Pilot Tone Generation

The microcontroller is used to initiate the generators with the proper frequency and initial phase during start-up. It is also used to turn off or turn-on any generator at any moment, according to users will. User's commands are triggered from 2 external switches (J1 and J2). The AD9834 offers 28bits resolution over frequency and 12bits over phase control. By using a 10 MHz reference clock, we achieve frequency and phase accuracy of about 0.037 Hz ($10\text{MHz}/2^{28}$) and 0.09 degrees ($360/2^{12}$), respectively. The reference clock frequency is intentionally chosen to be high enough in order to can be easily filtered out from the carrier and the pilot signals, using only some simple R-C filters.

The source code is very simple. The microcontroller is used to initialize the DDS generators and then periodically checks J1 and J2, running on an infinite loop. J1 and J2 are used to turn on or off the carrier and (or) the pilot signal, thus enabling or disabling the stereo broadcasting.

Besides main, there are only very few other routines in the code. These routines are responsible for initializing and turning on or off the carrier and (or) the pilot signal according to user will and also implementing the I2C interface, for the DDS chips, as "bit-banging" on normal I/O. Finally, there is also another essential parameter, regarding the correct phase relationship between the carrier and the pilot signal. The correct phase relationship between those signals is essential for achieving maximum "stereo-separation". The optimum phase relationship has been adjusted once through code, and the stereo encoder was initially calibrated. Initial calibration constants are

kept on some code lines (marked by the “Phase shift value” comment). These code lines are located in the void Pilot_on (void) routine and are used to set the initial phase parameter on the pilot tone DDS generator (please, refer to the AD9834’s datasheet for more details about the phase parameter).

B. The Balanced Modulator

Modern approach on building a low frequency balanced modulator tends to be the use of DSP. However, traditional analogue techniques are still used due to simplicity. After all, the composite fm-stereo signal is a completely analogue signal. We may live in the digital era, but we still using the old and good analogue fm-stereo.

Following the tradition, we use an analogue balanced modulator for the generation of the 38 KHz sub-channel. The modulator is based on the well known MC1496 IC, which is able to suppress the carrier for more than 60db.



Photo 2. The modulator is based on the well known MC1496 IC, which is able to suppress the carrier for more than 60db

Carrier suppression is defined as the ratio of each sideband output to carrier output for the carrier and signal voltage levels specified. The carrier suppression for the MC1496, is very dependent on the carrier input level. A low value of the carrier results in lower signal gain, hence lower carrier suppression. A higher than optimum carrier level results in unnecessary device and circuit carrier feed through, which again degrades the suppression figure. The optimum carrier level for optimum carrier suppression at carrier frequencies in the vicinity of 50 kHz, is about 60mVrms (170 mVp-p). This Optimum value is achieved through R47 adjustment.

Besides the carrier input, there is also another input for the L-R audio channel. The balanced modulator accepts both signals and performs the multiplication $(L-R) \times \text{carrier}$ in the time domain. A multiplication in the time domain is equivalent to frequency shifting in the frequency domain i.e. the L-R audio signal bandwidth is frequency shifted by the carrier frequency. This operation is better known as frequency mixing or shifting and the product of mixing is a DSB (Double Sided Band) signal.

There is a simple R-C filter at the carrier input of the modulator. This filter consists of the R56 and C48 and it is used to suppress the reference clock frequency (10 MHz). The DDS generates the carrier signal by using a 10bit DAC and the reference clock frequency is actually the sampling-frequency of the generated carrier signal. Since the reference clock frequency is much higher than the carrier frequency, it can be easily removed from the carrier signal by using a very simple

low-pass (1st order) filter. The simple low-pass filter produces some phase shift, which is cancelled, through appropriate phase shifting of the DDS generator. (see Fig. 8)

While the R47 is used to adjust carrier level at the input of the modulator, the R51 potentiometer is used to adjust the carrier suppression level. Carrier suppression better than 60db, can be easily achieved through the appropriate adjustment of R51. For best performance, the modulator is powered from two independent voltage sources; +12V and -8V, respectively. These are the recommended supply voltages, as described in the MC1496 datasheet.

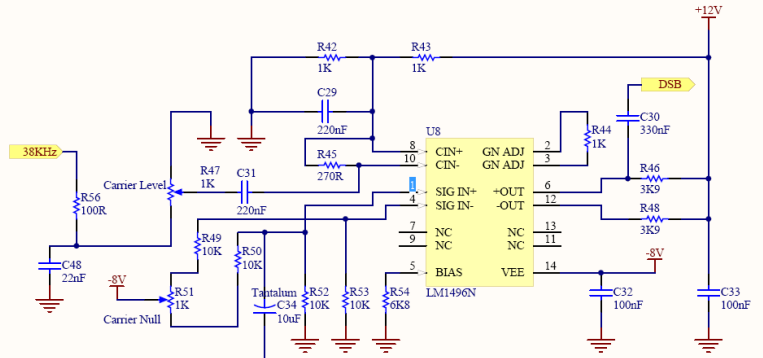


Fig. 9. Balanced Modulator Section

C. The Op-Amp Matrix

The heart of the fm-stereo generator is the matrix circuit. This circuit accepts the left and the right audio signals, the pilot tone and the DSBSC signal from the modulator, and performs the appropriate additions and subtractions, in order to produce the composite FM-stereo signal. The circuit also pre-emphasizes the left and right audio channel, just as normal monaural signal would be. The matrix circuit is based on operational amplifiers.

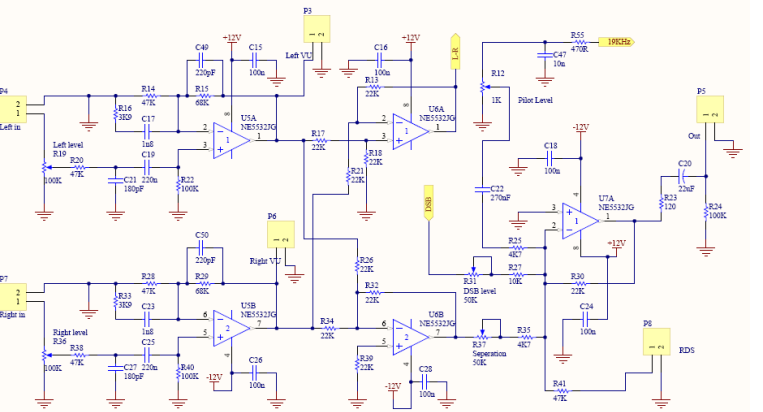


Fig. 10. The matrix circuit is based on operational amplifiers

Referring to the matrix electronic schematic, U5A and U5B are used to pre-emphasize the left and right audio channel. U5A, R14-16, R20, R22, C49, C19, C21 and U5B, R28-29, R33, R38, R40, C23, C27, C50 form pre-emphasis networks for the pre-emphasis of the left and the right audio channel, respectively. A pre-emphasis network is actually a high pass filter and pre-emphasis refers to a process designed to increase the magnitude of some higher frequencies with respect to the magnitude of lower frequencies. The pre-emphasis network characteristics are shown on figure 11.

In Europe, fm broadcasters use $50\mu\text{s}$ pre-emphasis, while it is $75\mu\text{s}$ in the U.S. Our FM-stereo generator prototype uses $50\mu\text{s}$ pre-emphasis, because it was built and tested in Europe (Greece). However, it can be easily changed to $75\mu\text{s}$ by simply changing C17 and C23 to 2.7nF .

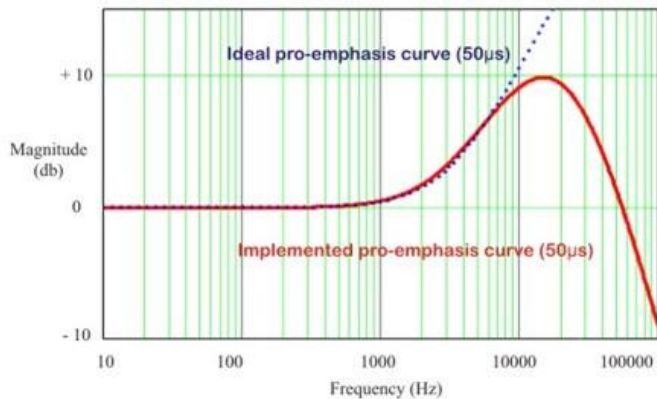


Fig. 11. Pre-emphasis network response curve.

Pre-emphasis on the transmitter and the minor operation (de-emphasis) on the receiver, are used to improve the overall signal-to-noise ratio by minimizing the adverse effects of the noise which is louder at higher frequencies. While the minor operation is called de-emphasis, the system as a whole is called emphasis.

Fm channel is inherently very noisy and this makes emphasis very essential. Emphasis is also used in monaural broadcasting but it is even more important for FM-stereo. This is due to the fact that the fm-stereo signal carries most of its information in high frequencies located between 22 and 54 KHz and noise tends to be louder on those high frequencies. In the receiver side, decoding the stereo channel into left and right means that the noise is shifted down into the audible range.

Referring to the electronic schematic of the matrix again, U6A is used as a subtractor and produces the L-R signal, and U6B is used as an adder which produces the L+R sum. U7 is the final adder which accepts the pilot tone, the main channel and the sub-channel and produces the composite output. At this final stage, an additional input (P8) is providing for adding any SCA or RDS/RBDS subcarriers.

R12, R31 and R37 are used to adjust the proper ratios for combining the three components of the stereo signal, i.e. the pilot tone level, the sub channel level and the main channel level, respectively. Proper adjustment of these potentiometers is essential for the optimum operation of the stereo-encoder.

R55 and C47 are forming a low-pass filter for the pilot tone. This filter is used to eliminate the reference clock frequency (10 MHz), from the pilot signal. Besides the final output, which is P5, there are two other outputs. Those are the P3 and P6 outputs that are used to provide the left and the right audio signal, respectively, to an external VU-meter.

D. The Power Supply Unit

The fm-stereo generator uses a simple linear power supply unit which is based on 78XX and 79XX linear regulators.

Referring to the power supply electronic schematic, U9, U10, U11 and U12 are used to provide +5V, +12V, -12V and -8V respectively. The DDS generator section is powered from +5V only, while the modulator uses both +12V and -8V. The matrix section uses $\pm 12\text{V}$ of symmetrical power supply.

III. ASSEMBLY DETAILS

The prototype uses a double-sided printed circuit board with metal-plated holes. Excluding the AD9834 ICs, the PIC microcontroller and the clock generator, all other components are of through-hole type and they are placed on the top-side of the board. The microcontroller, the DDS ICs and the clock generator are placed on the bottom surface of the PCB. All resistors, except for those used on the matrix, are of $1/4\text{W}$ -5% type. In the matrix, I use low-tolerance 1% resistors and low tolerance (5%) capacitors.

The PIC microcontroller was programmed on board, using a MPLAB ICD 3 programmer from Microchip.

IV. CALIBRATING THE FM-STEREO ENCODER

The FM-generator, needs to be calibrated before use. The calibration process includes 5 steps as described below:

- **Adjust the carrier level at the input of the modulator.** Connect your oscilloscope on R47's tap. You should measure a 38 KHz sinus waveform, which is the carrier. Adjust R47, in order to get about 160mVp-p on its tap, in respect to ground.
- **Achieve carrier null by means of the bias trim potentiometer R51.** Turn R19 and R36 at zero scale (fully anticlockwise). Connect the oscilloscope on any pin of C30. Normally, you will get a 38 KHz sinus waveform on your oscilloscope. Adjust R51 in order to get 0Vp-p (null the carrier). Well, you will never get the absolute zero, but just some mVp-p (around 5mVp-p or less).
- **Combine main-channel and sub-channel at the proper ratio.** Set R36 at full-scale and R19 at zero-scale. Connect an audio signal generator on R audio input and apply a 1 KHz audio tone of about 0.6Vp-p. Short-circuit J2 to turn off the pilot tone. Measure the output of the generator using an oscilloscope. Adjust R37 and R31 in order to get a 3Vp-p signal, like the one shown on figure 12.

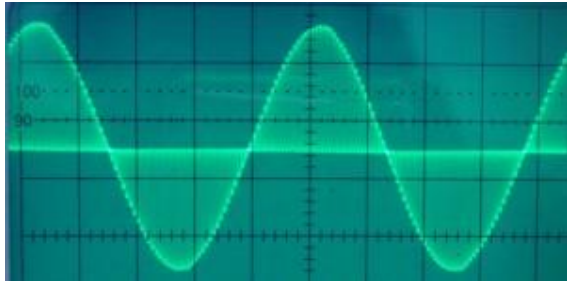


Fig. 12. Right Channel only: Used to Balance Gain and Sub-channel

- **Adjust the pilot level.** Set R19 and R36 at zero scale (full anticlockwise). Open J2 to turn on the pilot tone. Measure the output of the generator using an oscilloscope. You should measure a 19 KHz sine wave. Adjust R12 trimmer, in order to get about a 320mVp-p signal.
- **Adjust the VU-meter.** Set the left and right channel of the VU meter at full scale for 1Vp-p input. Adjust by using the trim potentiometers on VU-meter's board.

V. CONCLUSION

In this hybrid FM-stereo generator we use mixed digital and analog techniques in order to achieve optimum performance. We use Direct Digital Synthesis (DDS) to produce clean (purely sinusoids) signals with great frequency accuracy and stability for carrier and pilot tone generation. Reference clock frequency (or crystal choice) is not very critical in a high resolution DDS and signal generation becomes simple, robust and completely accurate. Using a DDS also diminishes the necessity of using complex (high order) filtering and we use very simple low-pass, 1st order filtering. The simple low-pass filter produces some phase shift, which is cancelled, through appropriate phase shifting of the DDS generators. The correct phase relationship between the carrier (38kHz) and the pilot (19kHz) tone is essential for achieving maximum stereo-separation, and the optimum phase relationship has been adjusted once, through code, according to trial and error method.

ACKNOWLEDGMENT

This project is a part of the production line of a new "Start - Up" small Business, "CircuitLib - Electronics". CircuitLib - Electronics was awarded with the First Prize at the "Secondary Student Contest on Business Plans and Innovative Ideas". The Student Contest on Business Plans and Innovative Ideas was organised from TEI of Crete, started on June of 2013 and ended on March of 2014.

REFERENCES

- [1] Clifford B. Schrock, "FM Broadcast Measurements Using the Spectrum Analyzer" Application Note 26AX-3582-3, Tektronix 1981
- [2] Eva Murphy, Colm Slattery "Direct Digital Synthesis (DDS) Controls Waveforms in Test, Measurement, and Communications" Analog Dialogue 39-08, August (2005)
- [3] PIC18F1220/1320 Data Sheet 18/20/28-Pin High-Performance, Enhanced Flash Microcontrollers with 10-Bit A/D and nanoWatt Technology 2007 Microchip Technology Inc.
- [4] MC1496, MC1496B Balanced Modulators/Demodulators Datasheet On Semiconductor Components Industries, LLC, October 2006, - Rev. 10
- [5] Eva Murphy, Colm Slattery "All About Direct Digital Synthesis" Analog Dialogue 38-08, August (2004) <http://www.analog.com/library/analogDialogue/>
- [6] Data Sheet AD9834 - 20 mW Power, 2.3 V to 5.5 V, 75 MHz Complete DDS, Analog Devices www.analog.com
- [7] CircuitLib - The Electronics Circuit Library www.circuitlib.com

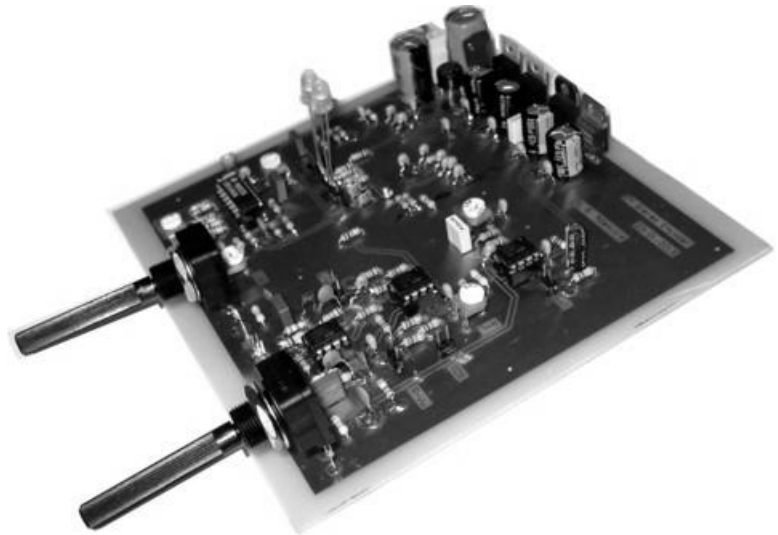


Photo3. The electronic board of the hybrid Fm Stereo Encoder

Manolis G. Tambouratzis was born in 1986 at Heraklion, Crete, Greece. In 2011 he graduated from the Department of Electronic Engineering, Faculty of Applied Sciences, TEI of Crete with grade "Very Good" 7.32 / 10 drawing up his internship at the Technical Department of the Hellenic Telecommunications Organisation (OTE). He holds a professional License "Radioelectronics Cat B" and a degree in Electronic Communications - Radio-Amateurs 'Cat 1' with the distinctive code "SV9RGJ" from 2012. His interests are focused on Electronic Circuits Technology for Telecommunication Applications (RF Systems Design), Wireless Telecommunications Systems Technology and Electromagnetic Fields Measurements from Base Stations Transmitters. He is a member of scientific societies IEEE (Student Branch - TELoC), FITCE and EETEM and has attended numerous training seminars in the fields of Communications & Information Technology in recent years.

George A. Adamidis - Physicist and Electronic Engineer.

Studies: Physics (2000), MSc in Electronic Physics (2002), from Aristotle University of Thessaloniki, Greece.

Current occupation: High - School teacher in Physics & Electronics, Assistant Researcher in the Centre of Technological Research of Crete.

Research interests: Embedded Systems, RF technology, Smart Antennas, Antenna design and Electromagnetic Compatibility.

Modular Analog Audio Mixer

Design in Practice

George A. Adamidis¹

MSc in Electronic Physics

¹ I.E.K Heraklion – Technical School Laboratories

Division of Electronics

Itanou 40 Kipoupoli, 71307 Heraklion, Crete, Greece

{sv7fid@yahoo.gr}

Manolis G. Tampouratzis²

² Department of Electronic Engineering

Faculty of Applied Sciences

Technological Educational Institute of Crete

Romanou 3 Chalepa, 73133 Chania, Crete, Greece

{tampouratzis@chania.teicrete.gr}

Abstract - Our goal is to introduce a design procedure for building a high-quality modular audio mixing console. Modular refers to a design that can be split into smaller portions (modules) so when complete, they can be joined together to form one system. A modular audio mixer is formed by assembling some main modules that can be varied in number and/or disposition to suit individual needs. Being determined to motivate electronic engineering students to be involved on analog circuits design from not just a theoretical and mathematical perspective, we have implemented an educational platform in order to encourage learning in practice.

Keywords - Operational Amplifiers Topologies, Audio Frequency response, Analog Electronics, Tone Control Circuit, Audio EQ Circuit

I. INTRODUCTION

An audio mixer, also called a mixing console, is an electronic device for combining, and modifying audio signals. The modified audio signals are summed to produce some combined output signals. Audio mixers can be analog or digital. Digital mixing consoles use Digital Signal Processing concepts and analog mixers are usually based on op-amps (operational amplifiers) electronic circuits. Although digital signal processing is the current trend, analog circuits are still in use due to their simplicity, and low cost.

To illustrate the approach, we will describe our recent efforts to develop a modular design. Modular design is a form of splitting an object into smaller portions such that when they are done, they are joined together to form one complete system. A modular audio mixer is formed assembling some main modules that can be varied in number and/or disposition to suit everyone needs. In a modular mixing console, the constructor can decide how many inputs should be provided. The input audio signals could be anything from microphones, CD players, PC sound cards or any other type of analog audio sources.

Our basic mixer will be able to combine these signals from different signal sources, change the volume of each input channel as well as the overall volume of the output. Later, we will proceed to a more complex structure by adding some circuits for audio equalization. We will discuss about adding circuits for attenuating or boosting a range of frequencies e.g., bass, midrange, and treble on each audio channel and also about a general graphic equalizer to perform general equalization control at the output, a VU meter device and a headphone monitor.

II. AUDIO MIXER BASICS

A. Summing Amplifier

The heart of the mixing console is the summing circuit shown in figure 1. This circuit is also known as the summing amplifier. It consists of an operational amplifier, n input resistors ($R_1, R_2 \dots R_n$) and a feedback resistor (R_f). A summing amplifier sums several (weighted) voltages. Its output voltage V_o is given by the formula: $V_o = -(A_1 \cdot V_1 + A_2 \cdot V_2 + A_3 \cdot V_3 + \dots + A_n \cdot V_n)$. A_x is the voltage gain for the x th input and it is equal to R_f/R_x .

When all input resistors (R_1, R_2, \dots, R_n), and also the feedback resistor R_f , have the same value then the voltage gain for each input channel becomes equal to the unity and the formula becomes: $V_o = -(V_1 + V_2 + V_3 + \dots + V_n)$. The minus sign indicates that the summing output is inverted or otherwise phase shifted by 180 degrees. However, phase shift has no audible effect.

If the value of the feedback resistor, R_f , becomes greater than the value of any input resistor, R_x , then the gain for channel x , will be greater than unity (and equal to R_f/R_x).

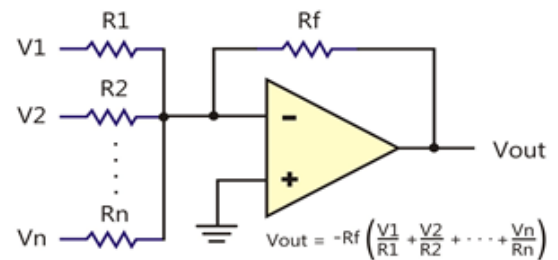


Figure 1. The summing amplifier is itself a mixer.

The summing circuit is actually an adder, and a basic mixer is really nothing more than an adder too, so the summing circuit is itself a mixer. This holds true but we must also notice that the summing circuit has not any adjusting elements for adjusting sound volume (voltage levels). An audio mixer usually has, and adding them should be the next challenge.

In our design, we will add some more circuits according to the block diagram of figure 2. We will add a matching circuit at every input to ensure that any signal source is not unduly

overloaded. Every matching circuit will serve as a preamplifier and a volume level adjuster for each input channel, and from now on we will call it as the “input module”. The outputs of all input modules will all be combined in a summing amplifier. We will also provide a potentiometer to our summing amplifier which will be the “master” volume adjuster (for adjusting the volume of the output).

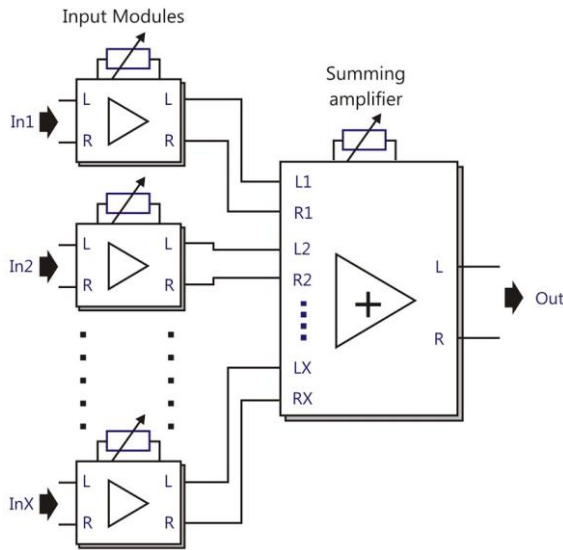


Figure 2. A simple stereo-mixer.

B. Line Input Modules

Most audio signals used to transmit analog sound between audio components such as CD and DVD players, TVs, audio amplifiers, and mixing consoles are Line-level signals. As opposed to line level, there are weaker audio signals, such as those from microphones and instrument pickups, and stronger signals, such as those used to drive headphones and loudspeakers. Below, we will present a line-level input module. Later, we will design additional input modules for weaker audio signals.

For designing a line-type input module, we must consider two facts:

- Cables between line output and line input are generally extremely short compared to the audio signal wavelength in the cable. So, there are no transmission lines effects and no impedance matching required. However, line level circuits use the impedance bridging principle, in which a low impedance output drives a high impedance input. A typical line out connection has an output impedance from 100 to 600 Ω . Line inputs present a much higher impedance, typically 10 k Ω or more. The two impedances form a voltage divider (see figure 3) with a shunt element (R_{in}) having a large resistor value relative to the resistor value of the series element (R_{out}), which ensures that little of the signal is shunted to ground and that current requirements are minimized. Most of the

voltage asserted by the output appears across the input impedance (R_{in}) and almost none of the voltage is dropped across the output impedance (R_{out}).

- The approximate nominal voltage level of a line-type signal is about 320 mV root mean square (V_{rms}) or 1.2 V_{rms} , for consumer and professional audio equipment, respectively.

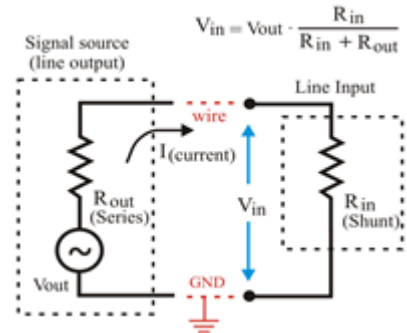


Figure 3. Line-output and line-input impedances form a voltage divider.

An appropriate input module circuit which conforms with the above criteria is shown in figure 4.

The circuit of figure 4 is actually an Inverting Amplifier. An inverting amplifier is a very common circuit, based on an op-amp. Its basic function is to scale (or amplify) and invert the input signal. The inversion is equivalent to a phase shift and has no audible effect.

Referring to the left-hand channel (the right-hand channel is, of course, identical) and as long as the op-amp gain is very large, the amplifier gain is determined by the external resistors (the feedback resistors R_{2A} and R_3 and the input resistor R_1). The voltage gain is equal to the ratio of $(R_{2A}+R_3)/R_1$. Moreover, the input impedance (R_{in}) of the circuit is approximately equal to R_1 because the operational amplifier's inverting (i.e., $-$) input is a virtual ground.

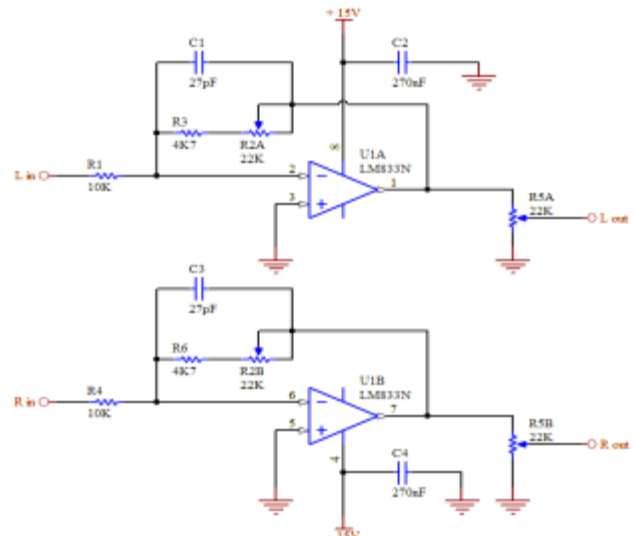


Figure 4. A line-type input module. Left and right channels are identical. R_2 and R_5 are logarithmic-type stereo sliding-potentiometers.

We have chose R1 to be equal to 10K in order to comply with the criterion of the minimum input impedance required on a line-type input. Intentionally, we use a minimum value for R4 in order to avoid thermal noise (we will discuss about this later). R3 is equal to 4.7K, and R2A can be varied from 0 to 22K, so that the voltage amplification $(R2A+R3)/R1$ can be varied from about 0.5 to 2.6 (from -6.5 to +8.5db). This way, R2 acts as a gain adjuster, and the nominal output level can be adjusted from 160 to 830mV rms or from 0.6 to 3.12 V rms, for consumer and professional audio equipment, respectively. C1 is used for high-frequency noise filtering and for preventing oscillations. Together with R2 and R3, it forms a low pass filter. Filter's cut-off frequency is above the upper limit of the audible range (20Hz-20KHz), and varies inversely proportional to the change in value of R2 (see figure 5). The R5 potentiometer implements an adjustable voltage divider and acts as the volume level adjuster.

The circuit off figure 4 is a good example of what can be used as a line-input module in a mixer. Of course, many other circuits can also used for the same purpose. Any voltage preamplifier which has adequate input impedance (equal or higher than 10K) and has also a volume level adjuster can be used at the input stages of a mixer. Actually, there are some additional requirements for the right candidate. The input stages must not produce any noise or distortion, they must have flat frequency response from 20Hz to 20KHz (audible range) and must also be stable. Almost everything depends on the right choice of the operational amplifier, the use of appropriate filtering and also the use of as small as possible resistor values.

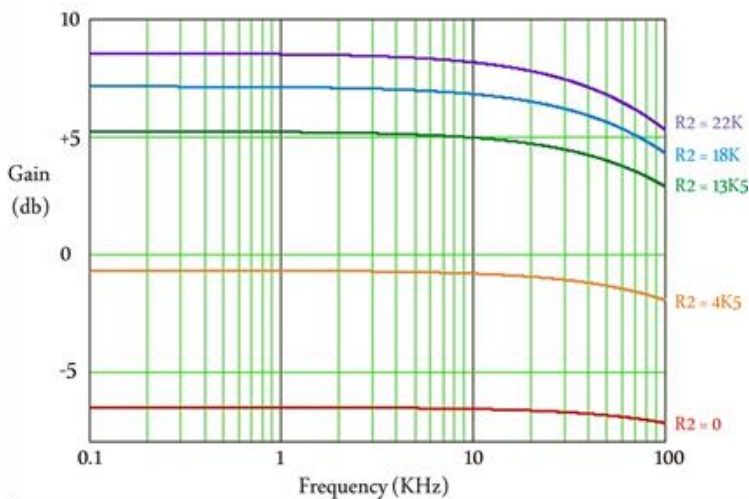


Figure 5. Line-input module frequency response for different wiper positions of R2

In the prototype (see photo 3), we use the classic LM833 dual operational amplifier which has been designed with particular emphasis on performance in audio systems. We also use as small as possible resistor values in order to avoid thermal noise. It is well known that any resistor produces some thermal noise voltage which is proportional to the resistor's value.

So, minimizing resistor values is essential for minimizing thermal noise level. Unfortunately, for a single stage circuit as this of figure 4, choosing the input impedance to be at least 10K, somehow limits our choices.

Thermal noise power is also proportional to the total bandwidth. Keeping the total bandwidth as low as possible is essential for reducing noise level. For this purpose, low pass-filtering is used in every audio mixer for rejecting spectral content above 20KHz (the upper limit of the audible range). Although filtering improves the overall SNR (signal to noise ratio), it also affects the frequency response of the preamplifier, and it is somehow difficult to ensure both good filtering and flat frequency response (at the entire audio range 20Hz-20KHz) at the same time. In our circuit we use rather simple filtering and we mostly focus on achieving flat response (see figure 5).

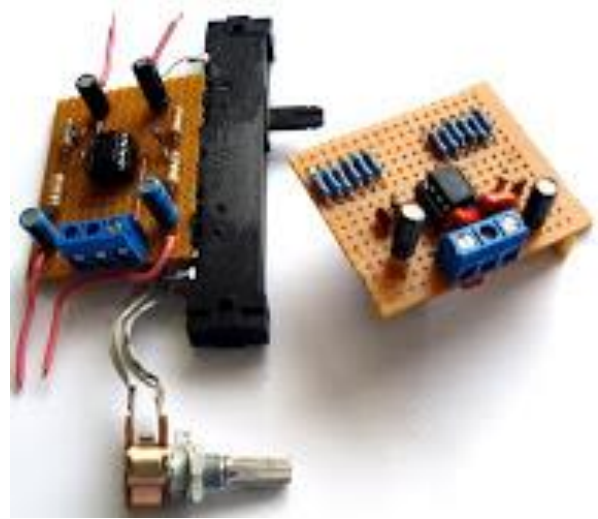


Photo 3. The Line-input module (at the left) and the summing amplifier module (at the right), built on prototyping matrix-boards.

There is also another important notice regarding the circuit of figure 4. We use DC-coupling for flat response even at very low frequencies. This is an advantage as far as the input source does not have any DC-leakage (offset). If there is any DC at the input, it will be amplified and will pass at the output, and may saturate the next stages. Adding a DC-blocking capacitor at the input (in series with R1) will solve the problem. The capacitor will limit somehow the flatness at very low frequencies and some low frequency content may be attenuated, unless a large enough value is used (the recommended value is about 10uF or more).

C. The Summing Amplifier Circuit

The summing amplifier circuit of our mixing console is shown in figure 6. Referring to the left-hand channel (the right-hand channel is identical), R7A is the feedback resistor and R1L, R2L,...RXL, are the input resistors. The feedback resistor is a 4.7K stereo potentiometer (R7) which is used to enable the output level to be matched to the sensitivity of the unit to which the mixer is connected. In other words, R7 acts as the master-level adjuster.

The input resistors (R1L-RXL or R1R-RXR) have the same value and they are all equal to 4.7K, so that the gain, which is equal to $R7/R1$, can be varied between 0 and 1 (negative infinity to 0db). C8 performs basic filtering, and is used to attenuate high-frequency signals in order to reduce noise level. There is also a series RC network at the output. The purpose of this network is to prevent any DC-offset appearing at the output of the mixer and also obviate any tendency to oscillation caused by a capacitive load (such as long screened cables). Using the modular-design concept (see photo 4), the summing amplifier module can be easily assembled on a prototyping matrix-board (see photo 3).

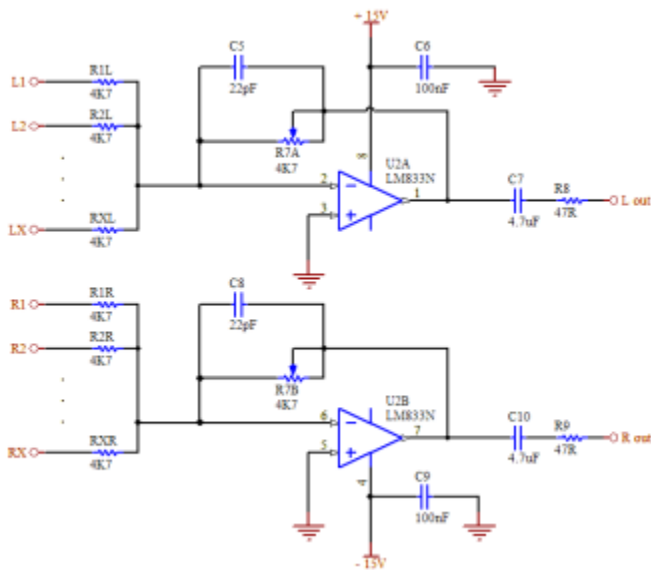


Figure 6. The summing amplifier circuit. Left and right channels are identical. R7 is a logarithmic-type stereo sliding-potentiometer.



Photo 4. The mixer uses the modular-design concept. However, building some modules on the same board minimizes the number of cable connections required.

D. Additional Outputs

Besides the main output, most mixers usually have additional outputs. The main output is usually connected on a final amplifier and other outputs are usually intended to be used as signal sources for monitoring or recording equipment.

Adding outputs is rather a simple task and it is based on the concept of using one or more voltage followers. A voltage follower is a basic op-amp circuit. It is called a "follower" due to its ability to "follow" its input without any loss. It is actually a unity-gain voltage amplifier which has very high input impedance, and very low output impedance at the same time, thus providing maximum isolation between its input and output. The voltage follower circuit is shown on figure 7.

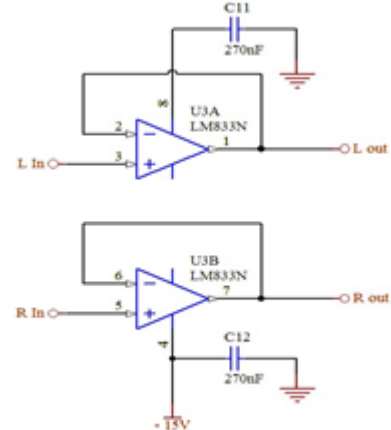


Figure 7. The voltage-follower circuit. It is actually a unity-gain voltage amplifier which provides maximum isolation between its input and output.

By adding one or more voltage followers, having their inputs connected on the summing amplifier's output, we will be able to build a mixer (see photo 5) with as many outputs as we wish. Due to the high input impedance of the voltage-follower circuit, we can connect as many followers as we wish on the summing amplifier's output, without overloading it. (see figure 8). All outputs from the followers will provide the same audio signal but they will be totally isolated one from another



Photo 5. Testing the mixer at the lab.

If we wish to be able to independently adjust the signal level in each output, we may use a potentiometer at the input of every voltage follower. The wiper of each potentiometer should then be connected to the input of each voltage follower (and the other two pins of each potentiometer should be connected to the summing amplifier's output and the ground, respectively). The specific arrangement is shown on figure 9. These potentiometers will then act as volume-adjusters for each output, and one of them may serve as the “master” volume adjuster. In this specific arrangement, R7 (see figure 6) is no more needed to be used as a volume adjuster, and it may be replaced with a fixed value resistor (or a trimmer resistor).

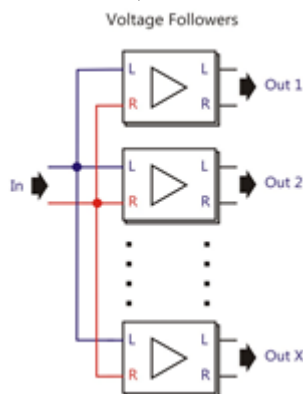


Figure 8. Adding outputs using one or more voltage followers.

Using potentiometers at the inputs of the voltage followers, reduces their input impedances. The total impedance “seen” by the summing amplifier will be reduced also, and will be about R_{pot}/N (where R_{pot} is the resistor value of each potentiometer, and N is the total number of potentiometers). This will limit somehow the maximum number of voltage followers can be connected at the main output. However, by using potentiometers of about 47K each, adding up to 4 or 5 outputs will not be a problem.

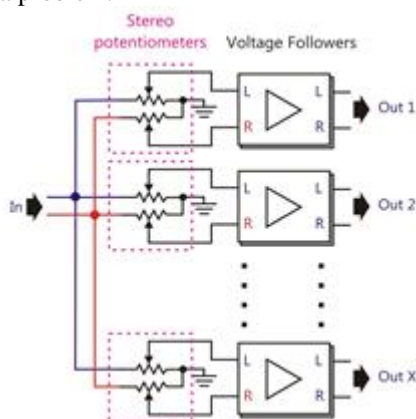


Figure 9. Using potentiometers at the inputs of the voltage followers enables independent volume adjustment for each output.

D. Adding Tone Control

Tone control allows listeners to adjust sound to their liking. It also enables them to compensate for recording deficiencies, hearing impairments, room acoustics or shortcomings with playback equipment.

Our mixing console is of modular design. Not only we can build as many input channels as we wish but we can also upgrade the design to use some additional modules for equalization (tone control). Such an upgraded design (see photo 6) which uses an additional module for tone control at each input is presented in figure 10. Obviously, this is not the only possible arrangement. Different arrangements may use tone control modules only at specific inputs, instead of all. You may also use one tone control module at the output (at the output of the summing amplifier).

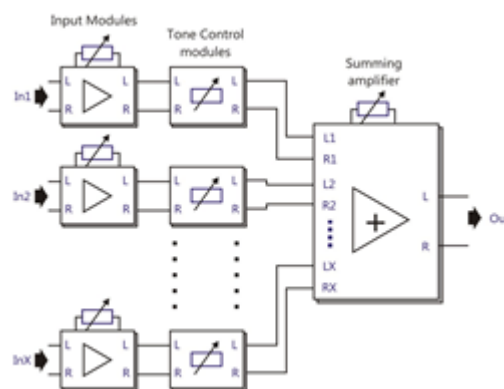


Figure 10. An audio mixer which uses tone-control modules.

Usually, the additional module required for tone control is a 2-bands or a 3-bands tone control circuit. Example designs for tone controls circuits, are presented in figures 11 and 13.



Photo 6. This prototype has 12 inputs and uses 3-bands tone control modules at all of them.

The circuit of figure 11 is a 2-bands tone control, and it is able to attenuate or boost bass and treble (2-frequency bands). The circuit is based on design formulas, found on page 14 of LM833-N's datasheet. R1 and R2 potentiometers provide independent control of bass and treble frequencies, respectively; both bass and treble can be boosted (when wipers

is on left) or cut (wipers on right) and with both controls at their mid positions, the circuit provides a relatively flat frequency response.

The 2-bands tone control circuit (see photo 7) uses one low pass and one high pass filter at each audio channel. Both filters are almost flat-top at their pass-band, and the flat-top gain of any filter can be varied between -20 and +20db, independently from the other one. The cut-off frequencies (-3db points) for the low and the high pass filters are preset at 34Hz and at 11 KHz, respectively (see figure 12). If you wish to alter them, refer to the design formulas.

The electronic schematic is quite simple and the circuit can be easily built on a universal board (prototyping matrix-board). However, we must take care to use low tolerance components to ensure the same response for both (R and L) audio channels. The circuit operates normally when connected to a low-impedance voltage source (like the line-input module of our mixer). Due to DC-coupling, any DC present at the input may cause some problems. So, use DC-blocking capacitors, if necessary.

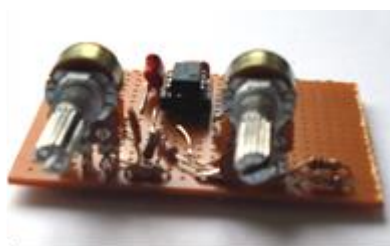


Photo 7. A 2-bands control module, built on a prototyping matrix-board.

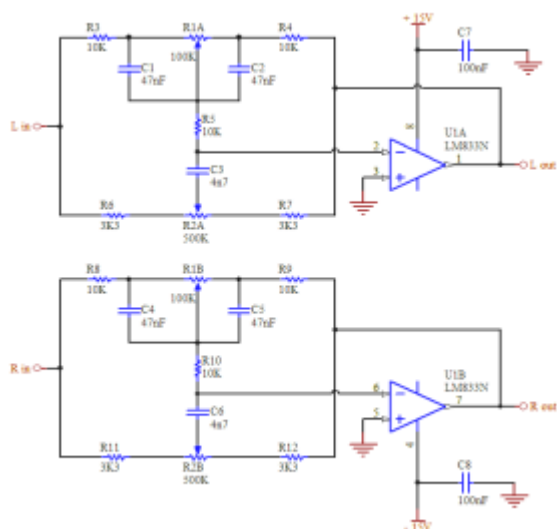


Figure 11. A 2-bands tone control circuit

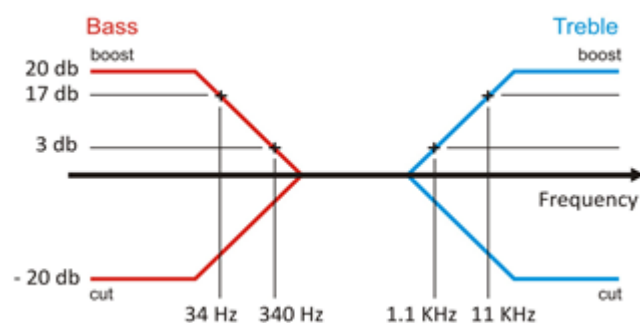


Figure 12. 2-bands tone control circuit frequency response (Bode plot)

The circuit of figure 13 is based on the popular low-noise NE5532 operational amplifier and has three separate adjustable filters. The first one is an adjustable-gain low pass filter; the second one is a band-pass adjustable filter and the third one is an adjustable high-pass filter. Each filter enables the adjustment for bass, mid and high frequencies, respectively (see figure 14). The cut-off frequencies (-3db points) for the bass and high frequency filters are about 20 Hz and 8 KHz, respectively. The central frequency of the band-pass filter is about 1 KHz. The normal gain, G , (when pots are at midrange) is given by $G=20 \cdot \text{LOG}(R2/R1)$. By using equal resistor values for $R2$ and $R1$, the normal gain becomes equal to 0db.

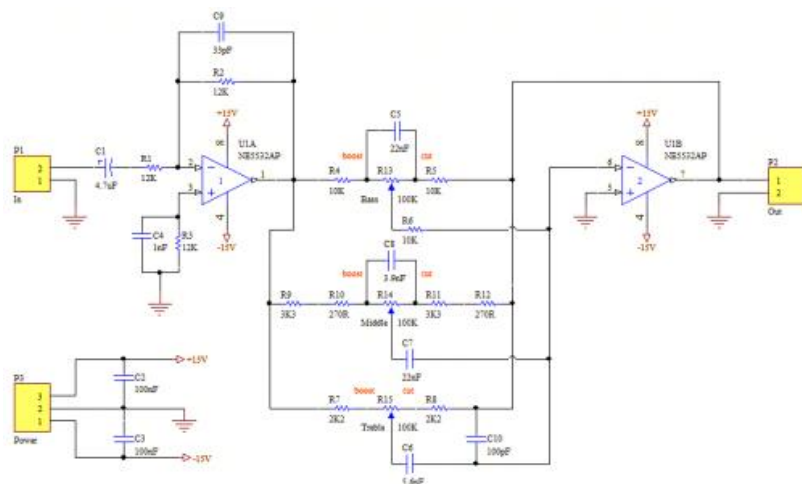


Figure 13. A 3-bands tone control circuit

In figure 13, and due to limited space available, only the right-hand audio channel circuit block is presented. The same circuit block, should be also used for the left-hand audio channel

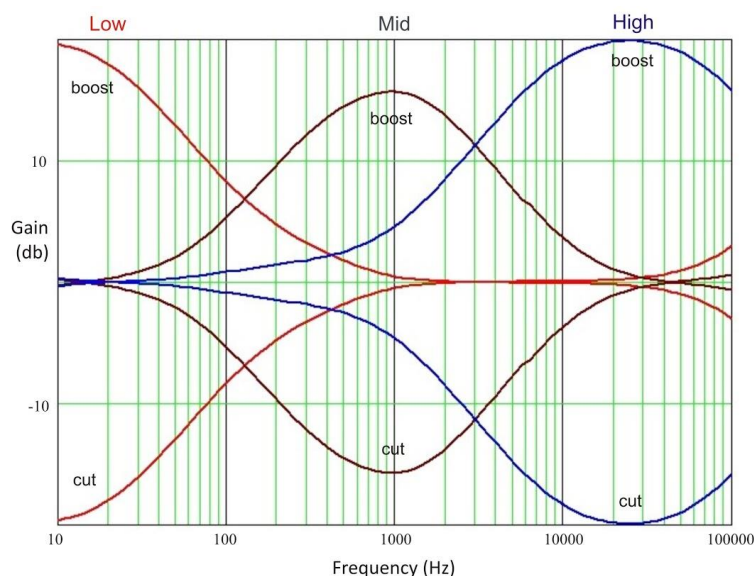


Figure 14. 3-bands tone control circuit frequency response (simulation on Electronics Workbench software)

D. Adding an Equalizer

At this point, our mixer uses relatively simple filters for limited adjustments. Graphic and parametric equalizers have much more flexibility in tailoring the frequency content of an audio signal than a simple tone-control module. An audio equalizer is actually a bank of many adjustable filters. Using the modular concept, we can use one equalizer at every input of our mixer. However, since an equalizer is a quite complex and expensive circuit, it is more practical to use it only once, at our mixer's output as shown in figure 15.

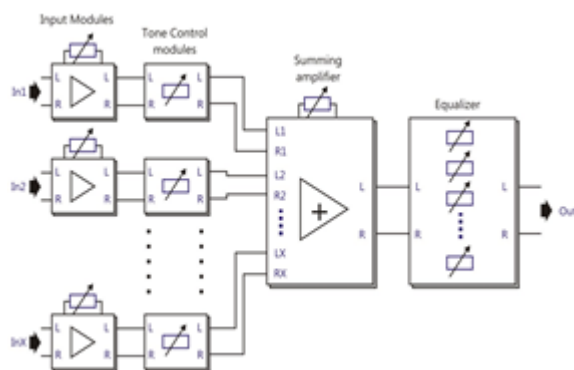


Figure 15. Adding an equalizer at mixer's output

A reference design for a graphic audio equalizer is presented in figure 16. The specific circuit is based on Philips Semiconductors Application Note 142 (first published on October 1984). The circuit itself has great performance and uses a top performance operational amplifier; the NE5532. The graphic-equalizer consists of an input buffer (IC1 -a), several variable-boost/ cut active filters (IC2-a), and an output

summing amplifier (IC1-b). The IC1-a circuit is designed for unity gain and is used mainly for impedance-matching between the input source and the equalizer filters. Each filter is a variable-bandpass or notching device, depending on the setting of the control potentiometer R2 (see frequency response on figure 17).

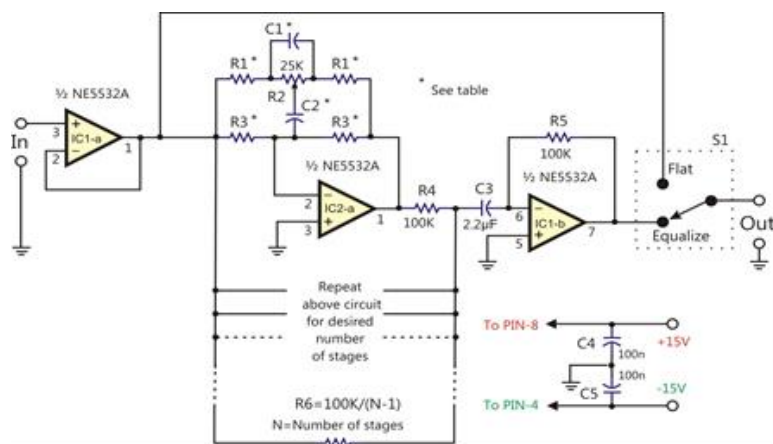


Figure 16. A reference design for a graphic audio equalizer

Any number of equalizer filter-stages can be used within the range of about 20 Hz to 20 KHz. The more stages you have, the easier is to boost or cut a particular frequency without affecting the response at adjacent frequencies. All the filter stages use the same R-C feedback-network configuration, to provide a maximum of about 13-dB of boost or cut at F_o , their center frequency. Different values for C1 and C2 are used in each stage, for setting the value of F_o .

A list for the values of R1, R3, C1 and C2 for a 7-bands graphic equalizer is presented on table 1. Values for different arrangements can be found on page 3 of the Philips Semiconductors Application Note 142 (which now is available for download from NXP's web site). C1 is about ten times as large as C2 and the values for R1 and R3 are both related to the value of R2, approximately by a factor of 10. The center frequencies of the list have been selected so that C1 and C2 are standard, off-the-shelf, values. The equalizer uses linear slide potentiometers for R2.

The value of R6 depends on the number of filter stages used. It insures that the gain across the equalizer is unity when all controls (R2's) are in the FLAT or 0 dB position. The nominal value of R6 is 100K (the value of R4-R5) divided by N-1, where N is the number of stages used. For a 7-bands equalizer, the nominal value of R6 is 100K/6, which equals about 16.7K. Note that only one audio channel is shown in the circuit schematic. In order to build a stereo version of the Audio Graphic Equalizer you'll need two of those circuits.

R1=2.4K, R3=240K, R2=25K, R6=16.7K		
Fo	C1	C2
60 Hz	0.47uF	0.047uf

158 Hz	0.15uF	0.015uF
425 Hz	0.056uF	0.0056uF
1082 Hz	0.022uF	0.0022uF
2382 Hz	0.01uF	0.001uF
6000 Hz	0.0039uF	390pF
15880 Hz	0.0015uF	150pF

Table 1. 7-bands Audio Equalizer component values

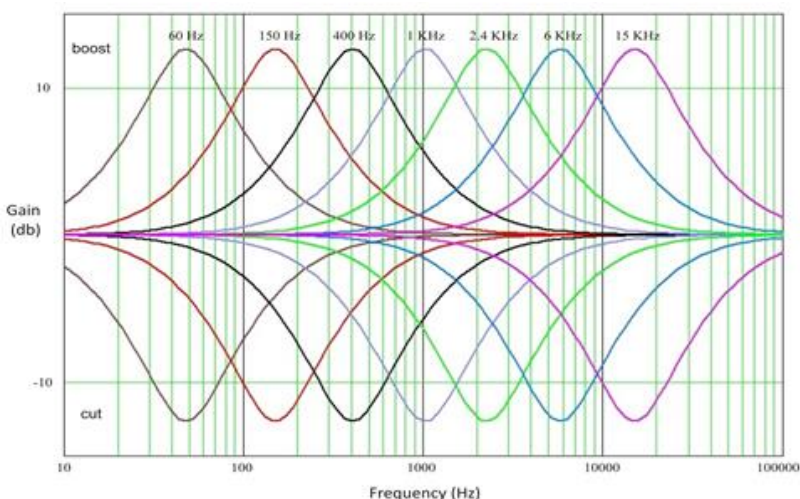


Figure 17. 7-bands audio equalizer frequency response (simulation on Electronics Workbench software)

The circuit described above is based on the concept of adding signals from several filters outputs. There are also other interesting reference designs for audio equalizers, based on different concepts. One of them is the one described on Texas Instruments AN-435 (*Designing with the LMC835 Digital-Controlled Graphic Equalizer*). The topology described on AN-435 is based on the gyrator concept rather than summing filters outputs.

E. Adding a VU meter

A Vu meter (Volume Unit Meter) is a device which is used to display a representation of the signal level. Think the Vu meter as a special kind of voltmeter which can be connected directly to any audio signal line of interest similarly to a high impedance voltmeter or oscilloscope input, measuring the voltage at the specific line of interest while drawing minimal current (and hence minimal power) from the source. As long as the vu-meter has enough input impedance it will not affect the performance of the mixer circuits.

Most mixers have only one vu meter at their output lines, but some quite expensive mixing consoles offer independent signal level indication for every input channel. Since we have a modular design we can use as many vu-meters as we like by simply connecting them directly to the signal lines

of interest (for example, at mixer's output or at any input-module's output).

An accurate LED-type stereo VU meter (see photo 8), based on the well-known Texas Instruments LM3915 IC is presented on Figure 18. The specific VU meter operates from a single supply voltage in the range of 3V to 6V. The maximum supply current at full scale is about 400mA and it is not dependent on the power supply voltage.



Photo 8. A bar-graph LED volume unit (VU) meter module, based on LM3915 IC

The LM3915 senses analog voltage levels and drives ten LEDs on a bar-graph, providing a logarithmic 3 dB/step analog display. We use 2 x LM3915 ICs; one for the Right (R) and another one for the Left (L) audio channel. We also use the MCP6022– dual operational amplifier IC as a Precision Half-Wave Rectifier and Preamplifier.

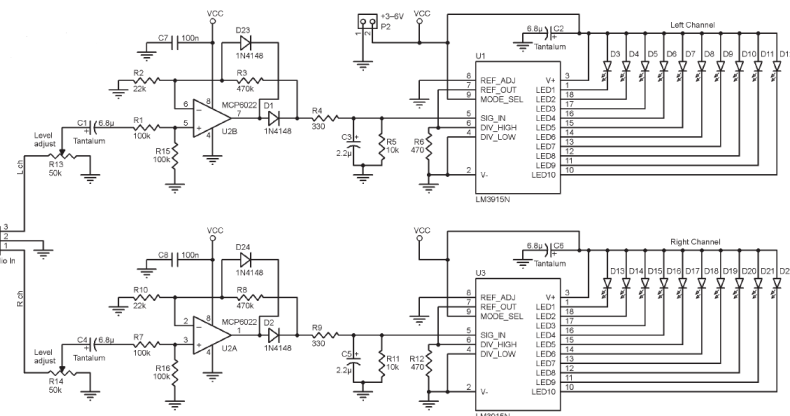


Figure 18. The stereo volume unit (VU) meter circuit

The input impedance in each channel (R and L) is more than 33K. R13 and R14 are used for full-scale voltage level adjustment. The minimum full-scale voltage level can be as low as 150mV. Vu-meters used at mixers outputs, are usually adjusted for full-scale reading at about 1.4V. C3, R4, R5 and C5, R9, R11 networks are simple integrators and they adjust the vu-meter's rise and fall times for the L and R audio channel, respectively. The VU-meter intentionally "slows" measurement, averaging out peaks and troughs of short duration. The "speed" of measurement is preset according to author's preferences but can be easily set to another value.

By replacing C3, R4, R5 and C5, R9 and R11 and after some trial and error you will be able to find the ideal values according to your preferences. Once a time, there were some standards for VU meters response but I think they mostly concern the case of old passive electromechanical devices.

F. Adding Microphone Inputs

Since now, the input stages are unable to provide significant gain for a microphone source. Our mixer has only “line-type” audio inputs. We can overcome this limitation by adding a microphone preamplifier at any channel we wish to convert it from a “line-type” audio input to a “microphone-type” one. The specific method is illustrated in figure 19.

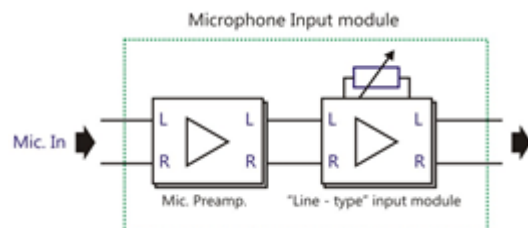


Figure 19. Converting a line-type audio input to a microphone-type one.

Two reference designs for microphone preamplifiers are presented in Figures 20 and 21. The circuit of figure 20 is based on the MAX4468 IC from Maxim, and it is optimized to be used with an electret microphone-capsule. The second circuit (figure 21) is a balanced microphone preamplifier based on the NE5534 operational amplifier, and it is an excellent choice for low impedance dynamic microphones.

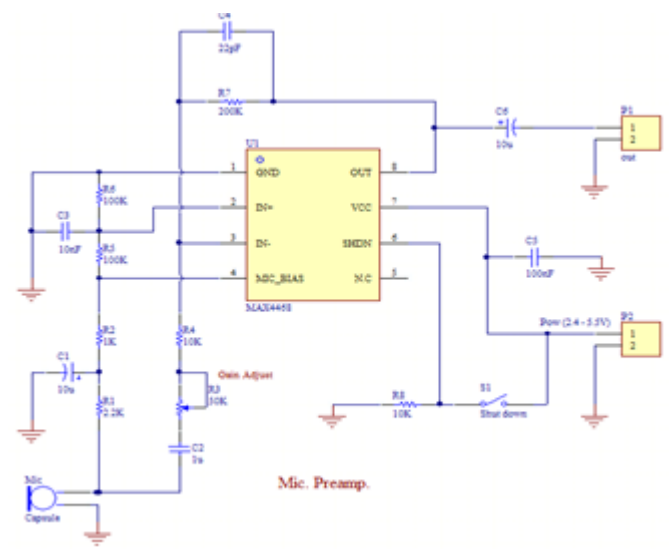


Figure 20. A microphone preamplifier, optimized optimized to be used with an electret microphone-capsule

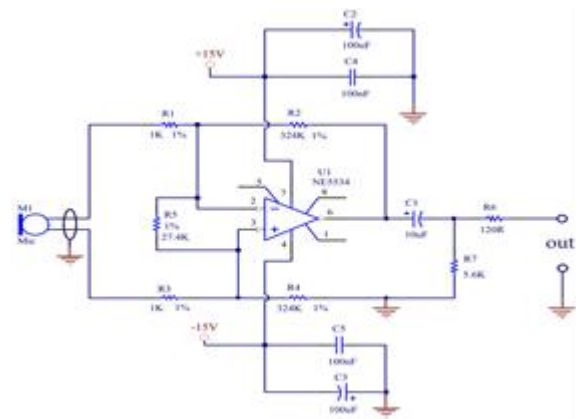


Figure 21. A balanced microphone preamplifier for low impedance dynamic microphones.

G. Adding “Phono” Inputs

A “phono” input refers to a Phonograph input. It is a special type input which can accept signals from an analog turntable or a magnetic guitar-pickup (or some specific other types of equipment). A phono input always uses a special circuit to boost the incoming signal and also provides the RIAA equalization necessary to restore the original sound. If you are still enjoying vinyl sound or you have a guitar which uses a RIAA magnetic pickup, you definitely need a phono input in order to be able to connect your classic turntable or your beloved music instrument to the mixer. Again, all you need is to convert one “line-type” audio input to a “phono-type” input by simply adding a phono preamplifier as illustrated in figure 22.

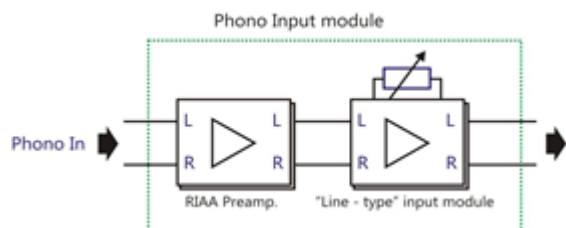


Figure 22. Converting a line-type audio input to a phono-type one.

Reference designs for RIAA preamplifiers can be found on page 14 of LM833-N's datasheet, on Texas Instrument's AN-346 application report on High-Performance Audio Applications of the LM833, and on Philips Semiconductors Application Note 142 (which is available for download from NXP's web site).

H. Adding Headphones Monitor

If you wish to add headphone monitoring capability in your audio mixing console, you need to use a headphone amplifier. With it you will be able to monitor the output of the mixer or any input. A headphone amplifier is just a small stereo power amplifier which provides a sufficient output to operate a pair of standard headphones.

A stereo headphone monitor circuit which is especially designed to be embedded in a homemade audio mixer is shown in figure 23. The circuit is equipped with a stereo volume-control potentiometer (R2) which allows the sound to be adjusted to a

comfortable listening level. Due to its small size (see photo 9) it may be mounted inside an audio mixer by using the volume-potentiometer bush fixing alone.

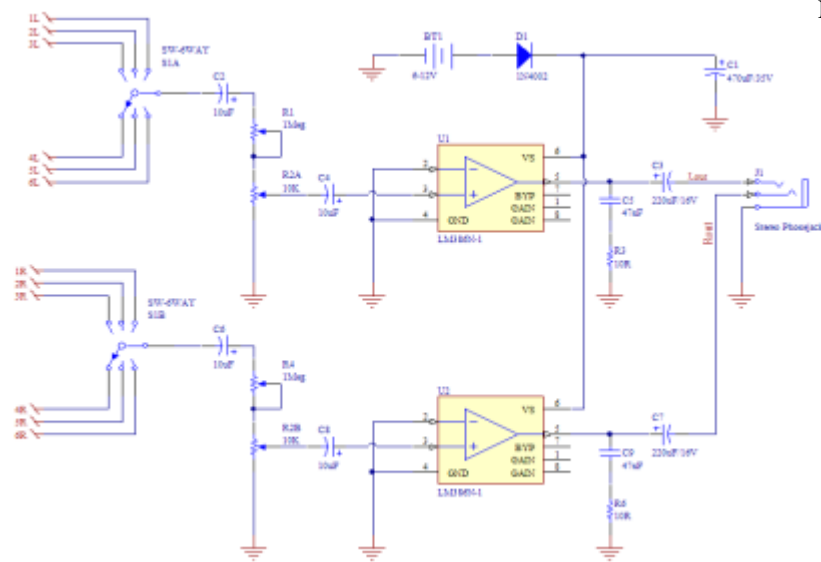


Figure 23. A stereo headphone monitor circuit especially designed to be embedded in a homemade audio mixer

The circuit comprises two sections and a small number of components common to both sections. The first section is based on U1 and it is associated with the Left audio channel. The second section is based on U2 which is responsible for the Right audio channel. Integrated circuits U1 and U2 are LM386 amplifiers. LM386 can provide up to 325mW into an 8Ω load. Standard headphones usually have greater impedance than this, so the available output will be reduced. However, this does not matter because only a very small output is sufficient to fully load the headphones. Since the components used on both audio sections are identical, only a description of a single channel is needed:

For any input signal level, the preset potentiometer R1 must be adjusted so that, when volume control (R2) is at maximum, there is minimal distortion combined with sufficient volume. R4, which is the preset potentiometer for the Right audio channel, must also be adjusted so that there is a correct balance (equality) in the volume between the left and the right channels.

The amplified signal of the Left channel appears at the output pin (pin 5) of U1 and AC-coupled to the left-hand headphone throw C3. Capacitor C5, which is connected in series with R3, is used to stabilize the amplifier and prevent any oscillation that might otherwise occur. The circuit can be powered from a 6-15V power source through D1. D1 is used to provide reserved-polarity protection.

S1 is a stereo, 6-way rotary pickup selector switch, which is used to select a specific input source (from 6 in total). In order to use the headphone monitor in your homemade audio mixer, you should connect inputs 1L, 2L,...6L and 1R, 2R,...6R, to the L and R outputs, respectively, of the modules you wish to monitor. Think the headphone monitor as a special kind of a

signal probe which can be connected directly to any audio signal line of interest similarly to a high impedance voltmeter or oscilloscope input. Using a 6-way selector switch, you will be able to monitor up to 6 modules. For N inputs, you will need a N-way selector switch.



Photo 9. The headphone monitor module (without the rotary pickup selector switch)

I. Power Supply Unit

For powering the audio section, we use a simple linear power supply unit which is based on 7815 and 7915 linear regulators. Referring to the power supply electronic schematic (figure 24), U10 and U11 are used to provide +15V and -15V respectively. A current of less than 1A is enough to power up to 50 modules.

We use a separate 5V power supply unit (see photo 10) for the VU-meter. The PSU used to power the VU-meter is based on Texas Instruments LM7525N-5 switch-type regulator (see figure 25).

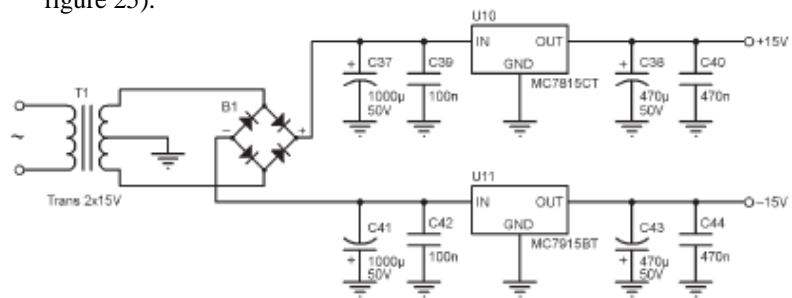


Figure 24. Simple linear power supply unit which is based on 7815 and 7915 linear regulators

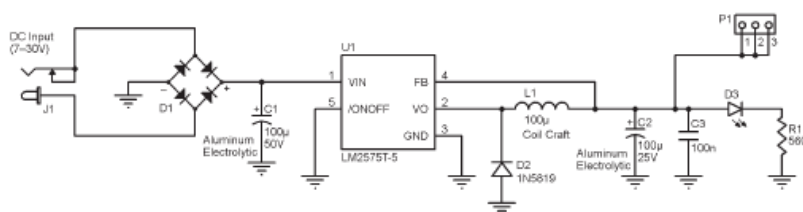


Figure 25. The PSU used to power the VU-meter is based on Texas Instruments LM7525N-5 regulator



Photo 10. The small PSU, used to power the VU-meter

CONCLUSION

The target of this article was to introduce a design procedure for building a high quality, modular, audio mixing console. The modular design procedure refers to a design which can be split into smaller portions (modules) such that when they are done, they can be joined together to form one complete system. A modular audio mixer is formed assembling some main modules that can be varied in number and/or disposition to suit everyone needs. The examples presented here are only for reference. The constructor is free to use the examples as they are or to use different configurations than those described here. The circuits described here are also for reference. They have been built and tested and exhibit good performance. However, we can not guarantee that they are the best of their kind. There is always room for improvements and you may always refer to bibliography, if you are looking for them. You may notice that building an audio mixing console from modules, requires many wires. However, after taking decisions about the number of modules you wish to use and their specific arrangement, you may design a printed circuit board which will minimize the number of cable connections required.

ACKNOWLEDGMENT

This project is a part of the production line of a new “Start – Up” small Business, “CircuitLib – Electronics”. CircuitLib – Electronics was awarded with the First Prize at the “Secondary Student Contest on Business Plans and Innovative Ideas”. The Student Contest on Business Plans and Innovative Ideas was organised from TEI of Crete, started on June of 2013 and ended on March of 2014.

REFERENCES

- [1] Texas Instruments, Inc. | www.ti.com LM833-N and NE5532 Op-amps, LM3915 IC, LM386 amplifier, and LM7525N-5 regulator
- [2] Electronics Workbench Group National Instruments Corp. | www.interactiv.com
- [3] Microchip Technology, Inc. | www.microchip.com MCP6022 Dual op-amp IC
- [4] Maxim Integrated | www.maximintegrated.com MAX4468 IC
- [5] Texas Instruments, Inc “AN-346 High-Performance Audio Applications of the LM833,” Application Report, www.ti.com/lit/an/snoa586d/snoa586d.pdf
- [6] Texas Instruments, Inc., LM833-N Dual Audio Operational Amplifier datasheet, www.ti.com/lit/ds/symlink/lm833-n.pdf.
- [7] Phillips Semiconductors, “Audio circuits using the NE5532/3/4,” Application Note: AN142, October 1984, www.nxp.com/documents/application_note/AN142.pdf
- [8] George A. Adamidis “Build your Own Audio Mixer – Part I&II” Audio Xpress Magazine, November - December 2014 www.audioxpress.com
- [9] CircuitLib – The Electronics Circuit Library www.circuitlib.com



Photo: The complete Modular Analog Stereo-Mixer Console with one microphone input, four line-inputs, a voltage unit (VU) meter, bass and treble tone controls, and a headphone monitor.

EvoRDF: A Framework for Exploring Ontology Evolution

Haridimos Kondylakis¹✉, Melidoni Despoina², Georgios Glykokokalos²,
Eleftherios Kalykakis², Manos Karapiperakis², Michail-Angelos Lasithiotakis²,
John Makridis², Panagiotis Moraitis², Aspasia Panteri², Maria Plevraki²,
Antonios Providakis², Maria Skalidaki², Athanasiadis Stefanos²,
Manolis Tampouratzis², Eleftherios Trivizakis², Fanis Zervakis²,
Ekaterini Zervouraki², and Nikos Papadakis²

¹ Institute of Computer Science, FORTH, Heraklion, Crete, Greece
kondylak@ics.forth.gr

² Department of Informatics Engineering, Technological Educational Institute of Crete,
Heraklion, Greece

Abstract. The evolution of ontologies is a reality in current research community. The problem of understanding and exploring this evolution is a fundamental problem as maintainers of depending artifacts need to take a decision about possible changes and ontology engineers need to understand the reasons for this evolution. Recent research focuses on identifying and statically visualizing deltas between ontology versions using various low- or high-level language of changes. In this paper, we argue that this is not enough and we provide a complete solution enabling the active, dynamic exploration of the evolution of RDF/S ontologies using provenance queries. To this direction, we construct an ontology of changes for modeling the language of changes and we store all changes as instances of this ontology in a triple store. On top of this triple store two visualization modules, one individual app and one protégé plugin allow the exploration of the evolution using provenance queries. To the best of our knowledge our approach is unique in allowing the dynamic exploration of the evolution using provenance queries.

1 Introduction

Dynamicity is an indispensable part of the web. Ontologies are constantly evolving [8] for several reasons such as the inclusion of new experimental evidence or observations, or the correction of erroneous conceptualization. Understanding this evolution using the differences (deltas) between ontology versions has been proved to play a crucial role in various curation tasks, like the synchronization of autonomous developed dataset versions, the integration of interconnected linked datasets etc. To this direction, various approaches have been used for formally describing those deltas, ranging from low-level deltas (describing simple additions and deletions), to high-level ones (describing complex updates, such as for instance, different change patterns in the subsumption hierarchy) [5].

However, only listing those changes is insufficient for the purpose of understanding what actually happened. First attempts in the area, provide static statistical information

of the type of changes [4, 5]. In addition, in our past work [1] we provided algorithms for exploring ontology evolution using provenance queries without offering however a visualization/exploration interface.

In this demonstration, we present for the first time a framework enabling the dynamic exploration of RDF/S ontology evolution using provenance queries. The framework gets as input the change log and transforms it using a change ontology in order to be saved in a Virtuoso triple store. Then two visualization modules, one application and one Protégé plugin, enable the exploration of the evolution using provenance queries. Those queries can answer *when* a resource was introduced (which ontology version), and *how* (by which change operation) whereas the list of change operations that led to the creation of that specific resource can also be computed and presented.

The remaining of this paper is structured as follows: In Sect. 2 we present the architecture of the EvoRDF framework and we describe the corresponding components. Then in Sect. 3 we highlight the demonstration items that will be presented in the conference. Finally Sect. 4 concludes this paper and presents directions for future work.

2 Architecture

The workflow for exploring ontology evolution and the high-level architecture of the EvoRDF is shown in Fig. 1. The whole process starts by getting the change log constructed between two ontology versions output from a change detection algorithm similar to [3, 5]. The change log contains multiple change operations.

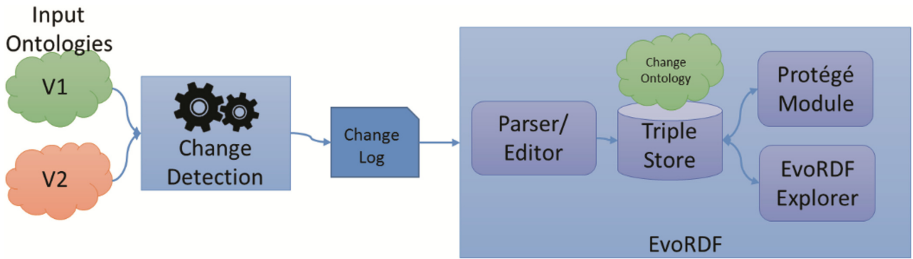


Fig. 1. Workflow for exploring ontology evolution

Definition (change operation): A change operation u over an RDF ontology O , is any tuple (δ_a, δ_d) where $\delta_a \cap O = \emptyset$ and $\delta_d \subseteq O$. A change operation u from O_1 to O_2 is a change operation over O_1 such that $\delta_a \subseteq O_2 \setminus O_1$ and $\delta_d \subseteq O_1 \setminus O_2$.

Obviously, δ_a and δ_d are sets of triples $\delta_a(u) \cap \delta_d(u) = \emptyset$ and $\delta_a(u) \cup \delta_d(u) \neq \emptyset$ if $O_1 \neq O_2$. The interested reader is forwarded to [3] for more information on the aforementioned language of changes. Two change operations for example are *Generalize_Domain*(*has_cont_point*, *Actor*, *Person*) and *Merge_Properties*(*{street, city}, address*). The first one denotes that the domain of the *has_cont_point* property has been generalized from the *Actor* class to the *Person* class and the second one that the *street* and the *city* properties has been merged to formulate the *address* property.

The file containing these change operations is then provided as input to the EvoRDF framework, which is composed of the following components:

- **The Change Ontology:** In order to model all changes identified by the change detection mechanism a change ontology has been constructed (Fig. 2c). The ontology consists of 24 classes and 39 properties and depicts all different types of change operations available and their corresponding arguments. Additional meta-data are saved such as the authors, the ontology versions etc.

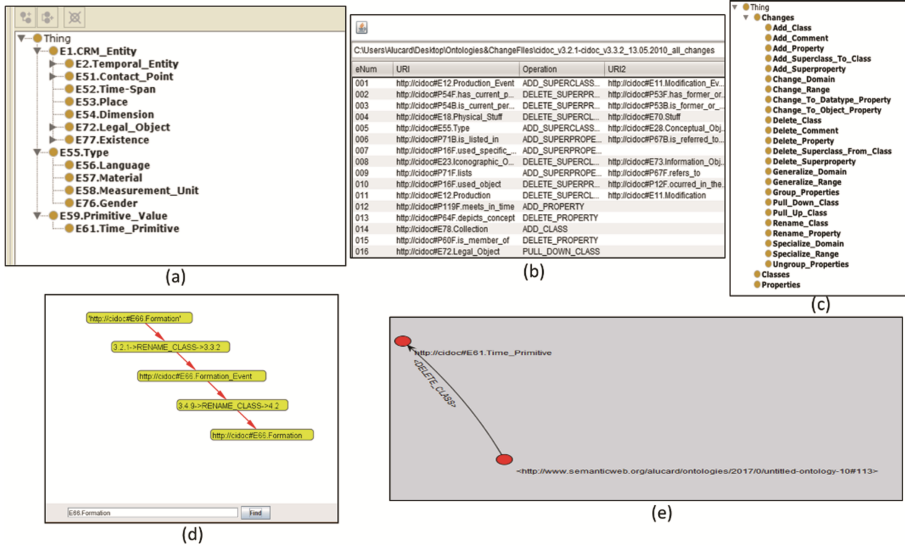


Fig. 2. Screenshots of the various parts presented in the demonstration: (a) CIDOC-CRM v3.2.1 in conjunction with (b) changes as they are identified by the change detection algorithm; (d) the Protégé plugin and (e) the individual application.

- **EvoRDF Explorer & Protégé plugin:** Having all change operations as instances of the Change Ontology the EvoRDF Explorer and the Protégé plugin issue SPARQL queries to the Virtuoso triple store in order to collect information about the change operations. These modules implement various algorithms, an initial version of which was presented in [1] for enabling ontology exploration using provenance queries. Three types of queries are available using these modules:

- When queries: An end-user can search for the specific version that a resource was introduced. In order to return the corresponding answer the proper SPARQL query is formulated requesting the version of the change operation that introduced this resource.
- How queries: In addition, an end-user can search for the change operation that introduced a specific resource (how). Again the proper SPARQL query is formulated and the answer is returned to the user.
- Extended-how queries: Finally, the change path (i.e. the consecutive list of change operations) that led to the creation of a specific resource can be computed and

presented to the user allowing further exploration and understanding of the evolution of the ontology. Extended-how queries are possible not only for specific resources but for specific change operations as well.

Those queries can be formulated and answered either using the individual application EvoRDF Explorer shown in Fig. 2e or using the Protégé plugin shown in Fig. 2d.

3 Demonstration

To demonstrate the functionalities of the aforementioned platform, we will use three versions of the CIDOC-CRM¹ ontology (v3.2.1, v3.3.2 and v4.2) and the corresponding evolution log. CIDOC-CRM is an ISO standard modeling information about cultural heritage, which consists of nearly 80 classes and 250 properties. The demonstration will proceed in five phases shown in Fig. 2 whereas a video is available demonstrating some basic functionality².

- (i) *Visualizing ontology & Evolution log*: The demonstration will start by visualizing one version (v3.2.1) of the CIDOC-CRM ontology using Protégé. Then we will present the corresponding change log between CIDOC-CRM versions v3.2.1 and v4.2 using the developed parser explaining the identified changes. The detected change log contains 726 total changes among those versions making it impossible to explore evolution looking only this evolution log.
- (ii) *Ontology for modeling evolution*: Next we will present the ontology for modeling evolution and we will show how the developed parser enables the transformation and storage, of all information available in the evolution log, in a triple store (Virtuoso).
- (iii) *Exploring ontology evolution using EvoRDF plugin*: Then, we will demonstrate how the EvoRDF Protégé plugin works by loading CIDOC-CRM 3.2.1 and providing a Virtuoso connection endpoint. The visualization options will be explained and the idea behind the corresponding evolution exploration algorithms will be provided. In this phase some interesting observations will be commented. For example, we will show that in the evolution of the CIDOC-CRM ontology from version v3.2.1 to version v3.3.2, one ontology engineer renamed the class “*E11 Modification*” to “*E11 Modification Event*”. A few years later another ontology engineer was employed to evolve the ontology. So in v4.2 we can see that the class “*E11 Modification Event*” was again renamed to “*E11 Modification*”. If the second ontology engineer had an indication of the previous renaming he would avoid cycles and he would be able to identify possibly the reasons behind each renaming - we are also able to show comments from the ontology evolution. So, using provenance queries to explore ontology evolution can be a valuable tool reducing greatly the time spent on understanding evolution.
- (iv) “*Hands-on*” phase: In this phase conference participants will be invited to directly interact with the plugin and explore ontology evolution

¹ <http://www.cidoc-crm.org/>.

² <http://www.ics.forth.gr/~kondylak/ESWC2017/>.

4 Conclusion

In this demonstration, we present a whole framework enabling the exploration of ontology evolution. Our framework gets as input the change log of the corresponding change detection algorithms and generates the corresponding instances of the ontology change. Those instances are saved to a triple store, on top of which two visualization modules allow the formulation of how, when and extended-how provenance queries for exploring ontology evolution. As future work several challenging issues need to be further investigated, for example extending our approach to OWL ontologies and presenting summaries [2, 6] of the overall evolution [7].

References

1. Kondylakis, H., Plexousakis, D.: Exploring RDF/S evolution using provenance queries. In: EDBT/ICDT Workshops (2014)
2. Pappas, A., Troullinou, G., Roussakis, G., Kondylakis, H., Plexousakis, D.: Exploring importance measures for summarizing RDF/S KBs. In: Blomqvist, E., Maynard, D., Gangemi, A., Hoekstra, R., Hitzler, P., Hartig, O. (eds.) ESWC 2017. LNCS, vol. 10249, pp. 387–403. Springer, Cham (2017). doi:[10.1007/978-3-319-58068-5_24](https://doi.org/10.1007/978-3-319-58068-5_24)
3. Papavasileiou, V., Flouris, G., Fundulaki, I., Kotzinos, D., Christophides, V.: High-level change detection in RDF(S) KBs. *ACM Trans. Database Syst.* **38**(1), 1:1–1:42 (2013)
4. Roussakis, Y., Chrysakis, I., Stefanidis, K., Flouris, G.: D2 V: a tool for defining, detecting and visualizing changes on the data web. In: ISWC (Posters & Demos) (2015)
5. Roussakis, Y., Chrysakis, I., Stefanidis, K., Flouris, G., Stavrakas, Y.: A Flexible framework for understanding the dynamics of evolving RDF datasets. In: ISWC (2015)
6. Troullinou, G., Kondylakis, H., Daskalaki, E., Plexousakis, D.: Ontology understanding without tears: the summarization approach. In: SWL (2017)
7. Troullinou, G., Roussakis, G., Kondylakis, H., Stefanidis, K., Flouris, G.: Understanding ontology evolution beyond deltas. In: EDBT/ICDT Workshops (2016)
8. Zablit, F., Antoniou, G., D'Aquin, M., Flouris, G., Kondylakis, H., Motta, E., Plexousakis, D., Sabou, M.: Ontology evolution: a process-centric survey. *Knowl. Eng. Rev.* **30**, 45–75 (2015)

Discone Rectenna Implementation for Broadband RF Energy Harvesting

Manolis G. Tampouratzis¹, Demosthenes Vouyioukas¹, Dimitrios I. Stratakis²

¹Department of Information and Communication Systems Engineering, University of the Aegean, Karlovasi, GR 83200 Greece, {tampouratzis, dvouyiou}@aegean.gr

²Department of Informatics Engineering, Technological Educational Institute of Crete, Heraklion, GR 71500 Greece, dstrat@staff.teicrete.gr

Abstract—In this study, a broadband RF energy harvester implementation is presented. The system uses a broadband discone antenna, which can operate efficiently in a broad frequency spectrum, including LTE, DCS 1800 and UMTS 2100 cellular frequency bands. The system is able to acquire energy from many electromagnetic field sources increasing the total amount of energy harvested, in order to charge a storage energy element efficiently in a short time. The prototype broadband RF energy harvester was tested on the laboratory and also in a typical urban environment.

Index Terms—Broadband Antennas, Discone Antenna, Rectennas, Radio Frequency (RF) Energy Harvesting, Schottky Diode, Voltage Doubler Rectifier (VDR).

I. INTRODUCTION

Energy harvesting from radio waves is possible through devices that called Radio Frequency Harvesters. A basic radio frequency energy harvester consists of an antenna, a matching network, a high frequency rectifier and an energy storage element. A rectenna is a rectifying antenna, a special type of receiving antenna that is used for converting electromagnetic energy into direct current (DC), and usually found in the bibliography to describe both the antenna and the rectifier sections of a harvesting system. The total power harvested from a radio frequency harvester, depends on: a) the available power spectral density ($W/m^2/Hz$), b) the effective area of the antenna and c) the operating bandwidth of the system.

The available power spectral density depends only on the electromagnetic environment. Limitations on the physical size of a RF energy harvester impose limitations on the physical size of the antenna and hence on its effective area. Thus, the most efficient way to increase the total power is by increasing the bandwidth of the system, in order to collect energy from more sources in a wider frequency range. The performance of a RF Energy Harvester is defined as the ratio of the power delivered to its output to the total available power in the harvester antenna [1,2].

II. THE BROADBAND DISCONE ANTENNA

The discone antenna is a version of biconical antenna, where one of two cones have been replaced by a disc. It is usually placed vertically, with the disc at the top and the cone at the bottom. A coaxial cable is usually attached at the point of intersection of the disc with the cone, to feed the antenna. The discone antenna is omni-directional, linear polarized and has a gain similar to that of a half wavelength dipole. It has excellent broadband characteristics at a frequency range up to 10:1. This type of antenna can be ideal for RF energy harvesting, beside of large size and its 3D geometry.

That makes its sensitivity higher in the direction of the horizon and noticeably smaller for signals coming from vertical directions. The standing wave ratio (SWR), is typically 1.5:1 or less in several octave frequencies. The behavior of this antenna as a function of frequency, is like a high-pass filter. Below the active cut-off frequency, significant standing waves appear in the feed line [3,4].

A. Structure Description

A discone antenna can be made from solid metal foil for use at higher frequencies of the radio spectrum. At lower frequencies, a sufficient number of metal wires or rods are often used, thereby simplifying construction and reducing wind resistance at the same time. The rays may be made from rigid wire or welding rods. The optimal number of rods found in the bibliography, including the disc and the cone, is from 8 to 16 [5,6]. The discone antenna consists of three main components: a) the disc, b) the circular cone and c) the insulator (Fig. 1):

- The disc has a diameter equal to 70% of the cone diameter. The antenna's feed point is located in the center of the disc. It is usually powered by a 50Ω coaxial cable, with the main conductor connected to the tray and the outer conductor to the cone.
- The height of the cone must be 30% of the wavelength of the lowest operating frequency of the antenna. The inner cone angle is generally from 30 up to 100 degrees.
- The disc and the cone are separated by an insulator. The thickness of the insulator, determines some of the antenna's properties, especially on near its high frequency limits [3].

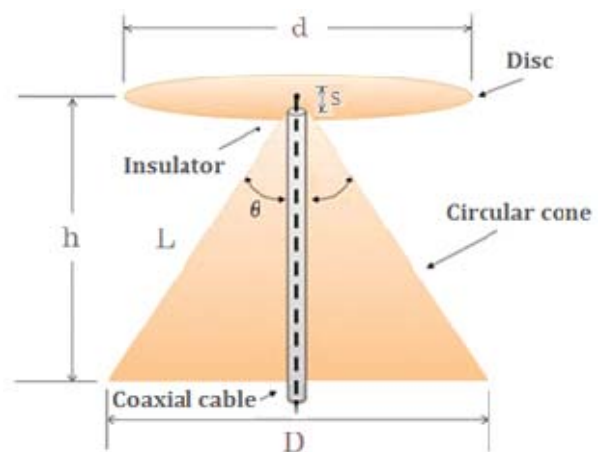


Fig 1. The main parts of the discone antenna: a) the disc, b) the circular cone and c) the insulator

B. Radio Amateurs' Construction Combinations

Different dimensional combinations of the discone antenna previously tested by radio amateurs, have demonstrated the following [7]:

- The construction is not extremely dimensional, if $0.58D < d < 0.75D$ and $s \ll \lambda$ (where s is the gap between the disc and the cone). Angles from 60° to 100° represent the angle θ values range that there is a satisfactory matching for coaxial lines of 75Ω and 50Ω . Smaller angles, reflect better matching with an 75Ω line, while larger angles are best adapted to 50Ω line. However, the gain stability and the mean gain of the antenna in the useful bandwidth seems to be inversely proportional to the inner cone angle θ .
- The useful bandwidth is defined by a peak SWR ratio of 3:1, at a frequency range of 10:1. For higher frequencies the s/λ ratio increases, while the useful bandwidth is constantly decreasing.
- The lower operating frequency is determined by the height h . At the lower operating frequency (VSWR 3:1) $h \sim 0.21\lambda$. At this point, the gain of the antenna seems to increase as the length L (up to $\sim 5\text{dBi}$) is increased, as opposed to the useful bandwidth, which decreases.
- The discone antenna can be operated with a SWR ratio 2:1 at a frequency range of 4.5:1 in HF and 3:1 at the upper UHF band.
- The horizontal radiation pattern (H-plane) is omnidirectional and the polarization is vertical. The gain of the antenna varies between 1.5 and 5dBi (1.5dBi at the frequency where $L \sim 0.28\lambda$ and 5dBi at the frequency where $L \sim 0.7\lambda$, where L is the side length of the cone). Also, by approaching the upper frequency limit of the useful operating range, maximum radiation occurs at small angles ($3-10^\circ$) below the plane of the disc. At these frequencies, the discone antenna behaves as a conical monopole.

C. Discone Antenna Construction – Design Expressions

With the aid of the design equations connecting the disc dimension to the antenna cone, the prototype that is described in this study was made from 0.3 mm thick copper foil, with cone angle 90° . The height h for the antenna is 12 cm, which determines the lower cut-off frequency (in the present design corresponds to the frequency of $F_{\min}=750\text{MHz}$), such as the response of a high-pass filter [5].

The mathematical expression that connects the height h (in m) of the cone with the wavelength λ (in m), and consequently the cut-off frequency F_{\min} (MHz) of the discone antenna is $h/\lambda = 0.3$. Considering the wave equation $c = \lambda \cdot f$, the height becomes:

$$h = 0.3 \frac{300}{F_{\min}(\text{MHz})} \quad (1)$$

The disc diameter d is correlated to the diameter of the cone D , by:

$$d = 0.7D \quad (2)$$

A cylindrical SMA (female) type connector is attached on the top of the cone. The barrel of the connector is solder

directly on the cone. This way the cone acts as a ground plane. The center sleeve is solder directly on the disc. The joint is made at the center of the disc.

The design that is described in this work has been based on conclusions from measurements on several structures [7], with common features: $h > 0.21\lambda$ at the lowest operating frequency, $30^\circ < \theta < 100^\circ$ and $0.58D < d < 0.75D$. Measurements have shown that the gain of the antenna is somehow inversely proportional to its bandwidth, thus the design that is optimized for maximum bandwidth has minimum gain. In this study maximizing the bandwidth while keeping the impedance of the antenna as possible near to 50Ω was the main design criterion.



Fig. 2. Discone antenna prototype from copper foil, with inner cone angle 90° , height 12 cm and low-cut frequency 750 MHz

D. Antenna Simulation

The simulation of this antenna type was carried out with Antenna Magus software, to extract the electrical characteristics, the radiation patterns in polar and cartesian form, and the 3D radiation charts in cooperation with CST Microwave Studio Suite 2016 software. The SWR is about 1.5:1, and the reflection coefficient (S_{11}) ranges from -10dB to -20dB in a wide band of frequencies, as shown in Fig.3.

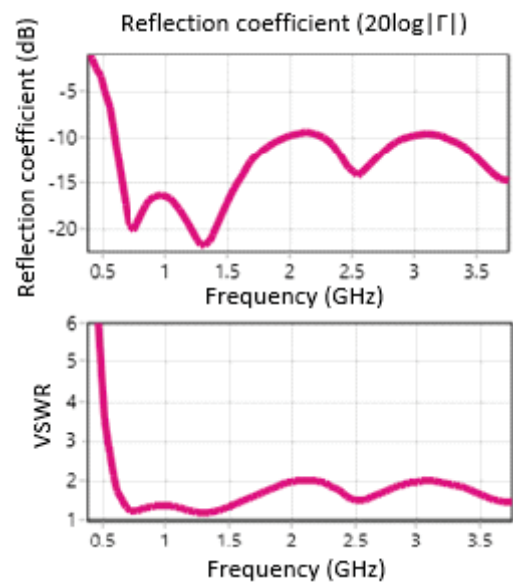


Fig. 3. The Reflection Factor in dB (upper) and the SWR ratio versus frequency (lower) discone antenna's simulation results from Antenna Magus Software

III. THE DICKSON N-STAGE RECTIFIER BASIC THEORY

A famous RF signal rectifier topology is the Dickson rectifier with 2 or N -stages, as depicted in Fig 4. The output of the circuit as a Voltage Doubler Rectifier (VDR) is given by:

$$V_{out} = 2V_{RF_{in}} - V_{th1} - V_{th2} \quad (3)$$

where V_{th1} , V_{th2} are threshold voltages of the diodes D_1 , D_2 respectively and $V_{RF_{in}}$ is the RF input voltage. It consists of two sections in cascade: a clamp consisting of elements C_1 and D_1 and a peak rectifier, consisting of C_2 and D_2 . When the circuit is excited by a sine wave signal with amplitude V_p , the clamping section produces a waveform that positive peaks are bounded to 0, while the negative ones reach $-2V_p$. Taking this waveform, the peak detector segment provides, along C_2 , a negative DC voltage of magnitude $2V_p$ [8].

The individual stages of the VDR circuit can be in sequence (N steps), so as to increase the rectifier output voltage at a resistive terminal load, which is defined as:

$$V_{out,Load} = 2NV_{RF_{in}} - 2NV_{th} - \frac{(N-1)I_{Load}}{f_o C} \quad (4)$$

where I_{Load} is the load current, C is the capacity of the blocking capacitors and f_o is the operating frequency of the system. Considering the losses of the substrate, the average input power is given by the following equation:

$$P_{in} = 2N I_{D,sat} B_1 \left(\frac{V_{out}}{V_T} \right) \exp \left(-\frac{V_{RF_{in}}}{2NV_T} \right) + \frac{N}{2} V_{out}^2 R_{Sub} (\omega_o C_{Sub})^2 \quad (5)$$

where V_T is the thermal voltage, B_1 is the modified first order Bessel function, R_{Sub} and C_{Sub} are the resistance and the substrate capacity respectively. By solving (5), it is noteworthy that for a constant output voltage and power consumption, the larger the number of the N -stages, the smaller the input voltage required to obtain a given DC output voltage and thus power consumption. However, the optimal number of stages is the trade-off between high DC output voltage and low power losses due to diode consumption and substrate losses. Experimental tests have shown that the optimum number of N stages is between 1 and 2. High saturation current ($I_{D,sat}$), low crossover capacitance (C_J) for low threshold voltage V_{th} , small resistor in series (R_s), and finally low cross-resistance (R_J), are some characteristics of a diode for loss reduction. The HSMS series of Avago diodes are a good solution, commercially available for these applications [9].

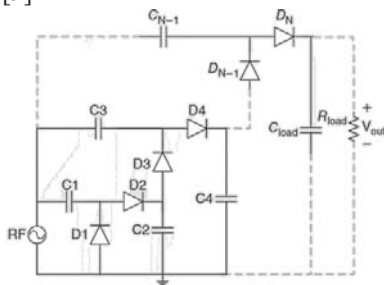


Fig. 4. Dickson N-Stage RF Rectifier basic topology

IV. THE RF RECTIFIER DIODE - HSMS 2862

The basic rectifying element of the device was the AVAGO Schottky HSMS-2862 diode [10], ideal for radio frequency applications due to its features, such as low switching time, low voltage drop, short recovery time and low contact capacity. According to the manufacturer's datasheet, this component is capable of rectifying broadband signals with operating frequencies ranging from 915MHz to 5.8GHz used by modern wireless communications systems, such as DCS-1800, LTE, UMTS and Wi-Fi. Indicatively, according to the datasheet, the sensitivity of the component reaches 35mV/ μ W at 2.45 GHz.

V. THE RF-DC RECTIFIER CIRCUIT DESIGN

The rectifier design described in this study was based on a Dickson 2-Stage Rectifier; this topology is actually a voltage doubler. The specific design was studied and simulated on Agilent ADS software and was finally manufactured on a FR4 substrate. For the simulation of HSMS-2862 Schottky diode, the corresponded models from ADS library were used. For the passive components, general purpose models were used. The rectifier's capacitors values were selected at 100pF to satisfy the condition for the time constant τ , to be much greater than 10 RF cycle for the operating frequency of the circuit, which corresponds to 0.58nsec at 1700MHz. The storage element has been connected at the rectifier's output. The storage element is an AVX (TAJ Series) 330 μ F surface mount device (SMD) tantalum capacitor, with very low equivalent series resistance (ESR) value. In series with the tantalum capacitor, a half-turn coil with low thickness (~ 0.6 mm) was placed, to act as a "RF choke" having an induction, approximately of 100nH (Fig.5).

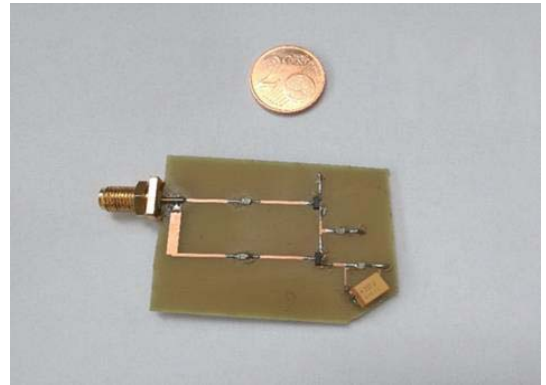


Fig. 5. The RF-DC rectifier circuit implementation from FR4 PCB board with dielectric constant $\epsilon_r = 4.35$

VI. BROADBAND RF ENERGY HARVESTING IN THE ELECTROMAGNETIC FIELD

The proposed RF harvester was placed for testing at the laboratory and nearby a base station in urban environment, with transmissions from wireless communications systems, such as DCS-1800, LTE, UMTS in the town of Heraklion, Crete, Greece. At the place of harvester installation, the equivalent power density average value (about 0,023 W/m²) measured from a Narda AMS-8061/G frequency selective EMF area monitor of the EMF project [11]. At the laboratory, harvester was irradiated from a 3115 ETS LINDGREN Horn

antenna driven by Agilent E4438C generator, in several frequencies. The experiment setup is showed in Fig.6 and the measurement results are presented hereinafter (Figs.7,8). From the obtained measurements it can be concluded, that the storage capacitor harvested energy derived from the electromagnetic field [12], is sufficient to power a terminal load of 10k Ω for 15 seconds, if we consider that:

$$\tau = R \cdot C \quad (6)$$

Thus, for a 10k Ω load and a 330 μ F storage capacitor, the constant time is $\tau=3.3$ sec. Knowing that a capacitor is completely discharged at a time of 5τ , with these component's setup, it can be assumed that for 15sec the voltage capacitor will exponentially reduce to zero. For constant time ($\tau=3.3$ sec), the voltage will exponentially reduce due to $0.368V_{max}$ value as described by:

$$V_c = V_{max} \exp\left(-\frac{t}{RC}\right) \quad (7)$$

where V_c is the capacitor's voltage at time t and V_{max} is the initial maximum voltage value from charging, at time $t=0$.

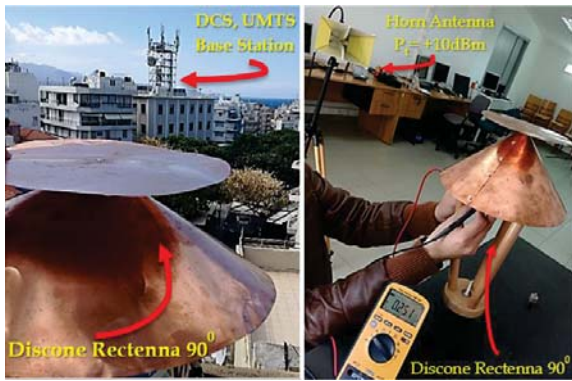


Fig.6. The broadband discone rectenna experiment setup nearby a base station in urban environment (left), and at the laboratory (right)

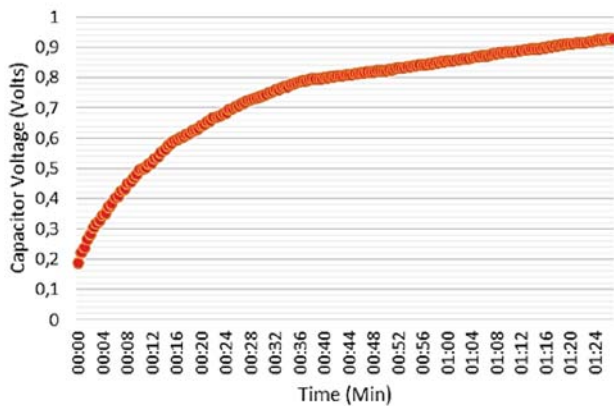


Fig.7. The storage capacitor charging response from RF Energy Harvesting with equivalent power density average value 0,023 W/m², 200m away from base station, in urban environment

The power of the storage capacitor, is a function of the charging time. When the voltage of the element reaches to its maximum value, the capacitor ceases to save more energy, and the average power is minimized. In this case, where the power is not constant, it is meant to refer to the energy at a given time.

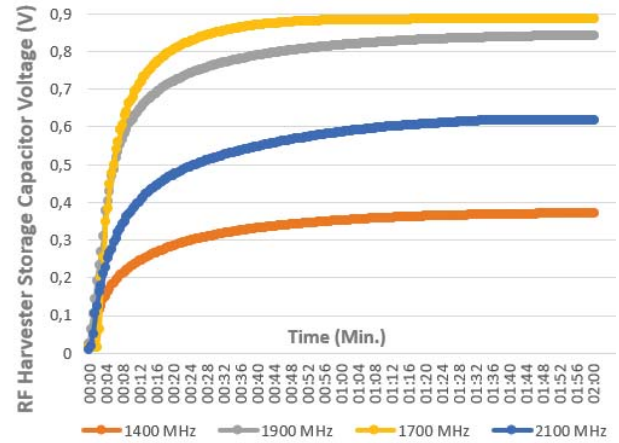


Fig.8. The storage capacitor charging response in several frequencies, testing at laboratory with received signal power at discone antenna -25dBm

VII. CONCLUSIONS

This study demonstrates a broadband energy harvesting system implementation to utilize base station signals from LTE, DCS-1800 and UMTS-2100 mobile systems in the downlink frequency band, in order to charge a storage energy element (330 μ F) efficiently at the urban environment, in a short time (about 1min) at 1Volt. Measurements proved that a 10k Ω load can be powered for 15 seconds from RF harvested energy with broadband E-field average strength value of 3V/m. The available total harvested power can be increased by increasing the bandwidth of the system, in order to collect energy from more sources in a wider frequency range, using an ultra-wideband antenna, such as the proposed discone antenna.

REFERENCES

- [1] C. R. Valenta and G. D. Durgin, "Harvesting Wireless Power: Survey of Energy-Harvester Conversion Efficiency in Far-Field, Wireless Power Transfer Systems," in *IEEE Microwave Magazine*, vol. 15, no. 4, pp. 108-120, June 2014.
- [2] C. Mikeka, H. Arai, "Design Issues in Radio Frequency Energy Harvesting System" *Sustainable Energy Harvesting Technologies - Past, Present and Future*, Intech, pp.236-256, 2011.
- [3] A. Kandoian, "Three New Antenna Types and Their Applications", *Proceedings IRE*, Vol. 34, pp. 70-75, Feb. 1946.
- [4] C. Balanis, "Antenna Theory, Analysis & Design" (3rd Edition), John Wiley & Sons, 2005, p.521.
- [5] W. Stutzman, G. Thiele, "Antenna Theory and Design," John Wiley & Sons, 1981, p.243.
- [6] G. Kennedy, B. Davis, "Electronic Communication Systems" (4th ed.), McGraw-Hill, 1992, pp. 298-300.
- [7] G. Adamidis, "Discone Antenna Implementation", Postgraduate Project, Physics Department, Aristotle University of Thessaloniki, 2001.
- [8] A. Sedra, K. Smith: "Microelectronic Circuits", (5th Edition), Oxford, 2004, pp.189-190.
- [9] D. Pavone, A. Buonanno, M. D'Urso, and F. D. Corte, "Design Considerations for Radio Frequency Energy Harvesting Devices", *Progress in Electromagnetics Research B*, vol. 45, pp. 19-35, 2012.
- [10] Avago Technologies - HSMS-2862 Series Surface Mount Microwave Schottky Detector Diode, August 2006
- [11] "National Observatory of Electromagnetic Fields", Greek Atomic Energy Commission, <https://paratiritirioemf.eeae.gr>
- [12] P. Aminov, J.P. Agrawal "RF Energy Harvesting", 64th Electronic Components & Technology Conference (ECTC), Florida, USA, pp. 1838-1841, 2014.

Design of Planar CPW-Fed UWB Trapezoidal Monopole Antennas with Band Rejection Characteristics

Manolis G. Tampouratzis¹, Evangelos Katsos², Demosthenes Vouyioukas¹, Dimitrios Stratakis³, Traianos Yioultsis⁴

¹Department of Information and Communication Systems Engineering, University of the Aegean, Karlovasi, GR 82300 Greece, {tampouratzis, dvouyiou}@aegean.gr

²Faculty of Pure and Applied Sciences, Open University of Cyprus (OUC), Nicosia, CY 2252 Cyprus, evangelos.katsos1@st.ouc.ac.cy

³Department of Electrical and Computer Engineering (ECE), Hellenic Mediterranean University (HMU), Heraklion GR 71004 Greece, dstrat@hmu.gr

⁴Department of Electrical and Computer Engineering (ECE), Aristotle University of Thessaloniki (AUTH), Thessaloniki GR 54124 Greece, traianos@auth.gr

Abstract—Planar CPW-Fed trapezoidal monopole antennas with single and dual band rejection characteristics are presented in this study. These antennas can be used to remove interfering frequencies from wireless communication systems such as military services and WiMAX networks at 3 GHz and 3.5 GHz respectively. The antenna prototypes were assembled on single layer FR4 substrate with $\epsilon_r=4.35$ occupying small surfaces of 50 mm x 58 mm and U-shaped slots were utilized, and VSWR of 2:1 in the frequency band of 1.6 - 3.8 GHz and notch mismatches up to 10:1 while maintaining omnidirectional patterns in the H -plane were satisfied. Moreover, measurement results using the Keysight Fieldfox N9915A Vector Network Analyzer (VNA) are compared with theoretical study of the antennas.

Keywords—Trapezoidal Monopole Antennas, Coplanar Waveguide (CPW), Single Frequency Notch, Dual Frequency Notch, Band Rejection, UWB Planar Antennas, U-Shaped Slot.

I. INTRODUCTION

Several Ultra-Wideband (UWB) antennas with band-notch characteristics using slot structures have been proposed by antenna designers [1] aiming to avoid interference between them and narrow bandwidth communication systems. Federal Communications Commission (FCC) has proposed variations on trapezoidal monopole antenna for use in UWB region from 2 GHz to 10 GHz [2,3]. A special kind of slot (U-slot) was introduced in [4] and the initial investigations were based on air and foam substrate. In [2,3] showed that when material substrate was used instead of air and foam substrate the respective antennas maintained their wideband characteristics. U-slot can be applied on the antenna design to achieve the desired impedance and can be experimentally adjusted for the desired frequency response i.e., changing the position of the slot, lower or higher notched bands can be generated avoiding possible interferences in undesired frequencies [5].

II. THE PLANAR CPW-FED TRAPEZOIDAL MONOPOLE UWB ANTENNA

Planar antennas of this kind are fed by a microstrip line or Coplanar Waveguide (CPW) at their base. Their width is increasing towards the top of the monopole in a continuous or stepped fashion. They are very popular in mobile communications due to their reduced size and wide

impedance bandwidth and can also be used in broadband RF energy harvesting such as a UWB discone antenna [6] in combination with planar implementation. The trapezoidal monopole's increased impedance bandwidth with respect to that of a rectangular monopole is due to the step and/or tapered bottom edges which ensure a broadband impedance transition. Aiming in this study to achieve a reflection coefficient (S_{11}) of below -10 dB (which corresponds to $SWR < 2:1$) across a 4:1 bandwidth, the proposed antenna designed to have a triangular base and a rectangular top section with its ground plane in the same plane with the antenna. This type of antenna can be integrated on the same printed circuit board with the transmitter electronics, requiring only one metallized dielectric substrate [7]. Furthermore, coplanar waveguides are particularly useful for fabricating active circuitry due to the presence of the center conductor and the proximity of the ground planes [8].

Structure Description

The antenna consists of a planar rectangular monopole element with tapered bottom and is fed by a Coplanar Waveguide (CPW) similar with the slotline. Thus, it can be viewed as a slotline with a third conductor centered in the slot region. Due to the presence of the additional conductor, even or odd quasi-TEM modes can be supported by this type of line, depending on whether the electric fields in the two slots are in the opposite or in the same direction.

The prototype implementation of the antenna was made on standard single layer FR4 substrate with relative permittivity (ϵ_r) 4.35, substrate height (h_s) 1.65 mm, loss tangent ($\tan\delta$) 0.025 and metal thickness (h_{mt}) 0.035 mm occupying a small planar surface of 50mm x 58mm (Fig.1), where the equations used for the antenna construction are the following:

$$W = \frac{c}{2f} \sqrt{\frac{2}{\epsilon_r + 1}} \quad (1) \quad L_{eff} = \frac{c}{2f \sqrt{\epsilon_{eff}}} \quad (2)$$

$$\Delta L = 0.5 \cdot h \quad (3) \quad L = L_{eff} - (2 \cdot \Delta L) \quad (4)$$

where c is the speed of light in free space, L , L_{eff} , W and h are the length, the effective length, the width, and the substrate's height of the resonant patch respectively. Although these design equations strictly refer to a grounded patch antenna, we will apply them for an estimation of initial dimensions of the CPW-fed monopole, by considering a modified choice of

the effective dielectric constant, as it will be shown in the next paragraph.

The patch has the form of a rectangle with a step at its upper end. Tapered section is used for the connection of rectangular patch with the feed line, and a cylindrical SMA connector is located at the end. This tapered variation improves the matching of the antenna over the operating bandwidth, and the resonant length is a function of the substrate parameters and the operating frequency. However, in this case the patch does not contain a ground plane on the other side of the substrate, hence the effective relative permittivity of the dielectric substrate ϵ_{eff} given by [3]:

$$\epsilon_{\text{eff}} = \frac{\epsilon_r + 1}{2} + \frac{\epsilon_r - 1}{2} \left[1 + A \frac{h}{W} \right]^{-1/2} \quad (5)$$

has to be modified for the constant A , where A is the multiplication coefficient for the term h/W , h is the substrate's height and W is the substrate's width respectively. By simulating different patches with different substrate parameters, it is possible to obtain the appropriate value of the multiplication coefficient A . In [3] the well-suited value of A was found to be 11.25.

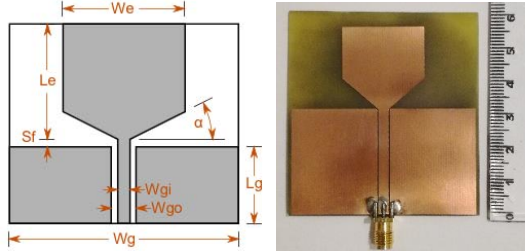


Fig 1. Design Parameters and prototype of proposed CPW-fed UWB (1.6 - 3.8 GHz) Trapezoidal monopole antenna fabricated on FR4 substrate.

Since the capacitance of the gap increases while the distance is decreasing, the width of the gap between the patch and the ground in the longitudinal direction has an important effect for impedance matching. The parameters of the trapezoidal patch i.e.: the gap (S_f), the height of the patch (L_e), the width of the patch (W_e) and the angle (α) are crucial for determining the performance of the antenna. According to [9]

- **Patch Height (L_e):** The first resonant point in the operation band decreases when increasing the height L_e of the antenna, and an appropriate height should be chosen to obtain the optimized performance of the antenna.

- **Gap Width (S_f):** The width of the gap determines the capacitance between the radiating element and the ground in the longitudinal direction influencing the impedance matching of the antenna, and smaller gap width results in higher capacitance.

- **Patch Width (W_e):** The width W_e has no noticeable effect on the performance of the antenna.

III. THE U-SHAPED CPW-FED TRAPEZOIDAL MONOPOLE ANTENNA WITH SINGLE FREQUENCY NOTCH

A side effect of the UWB radio band is possible interference at 3 GHz frequency which used by military applications [10]. One way of reducing this problem, is to incorporate a *U-shaped* slot near the base of the monopole. At the resonant frequency of the slot, the reflection coefficient is much larger than in the rest of the band, rejecting the interfering signal. Prototype implementation and design

parameters of the proposed single band rejection monopole antenna are shown at Table I and Fig.2, respectively.

Parameter	Description	Value
L_e	Monopole element length	20.5 mm
W_e	Monopole element width	25 mm
α	Taper angle at monopole base	40°
S_f	Feed gap	88.76 μm
W_g	Ground-plane width	50 mm
L_g	Ground-plane length	37.5 mm
W_{gi}	CPW inner width	3 mm
W_{go}	CPW outer width	3.9 mm
W_s	Slot width	1 mm
L_{sb}	Slot bottom length	18.5 mm
L_{ss}	Side slot length	8.5 mm
S_s	Slot offset	12.5 mm

Table I. Physical Parameters of proposed Single Band Rejection CPW-fed UWB Trapezoidal Monopole Antenna fabricated on FR4 substrate.

The U-Shaped Slot

The antenna's slot in this study, is *U-shaped* aiming to reject undesired notch frequencies and having reflection coefficient (S_{11}) below -10 dB across a 4:1 bandwidth with a notch mismatch of above -3 dB. The *U-shaped* slot is cut into the monopole element. The total slot length (L_{slot}) was experimentally calculated to be approximately $0.57\lambda_{\text{eff_slot}}$:

$$L_{\text{slot}} = L_{sb} + 2L_{ss} - w_s = 0.57\lambda_{\text{eff_slot}} \quad (6)$$

where $\lambda_{\text{eff_slot}}$ is the effective slot wavelength at the center frequency of the rejected band. The effective wavelength of the slot is given by:

$$\lambda_{\text{eff_slot}} = \frac{\lambda_0}{\sqrt{\epsilon_{\text{eff_slot}}}} \quad (7) \quad \text{where} \quad \epsilon_{\text{eff_slot}} = \frac{\epsilon_r + 1}{2} \quad (8)$$

and λ_0 is the resonant wavelength. This slight difference from half wavelength can be observed due to the fringing effect of the field at the ends of the slot. This slot corresponds to a nearly half-wavelength resonator at the center frequency of the required stop-band and introduces high reflection at its resonance frequency which corresponds to the operation of a band-rejection filtering effect. Thus, at first approximation, in order to obtain the notch frequency (f_{notch}), the required slot length (L_{slot}) is given by the following modified equation:

$$L_{\text{slot}} = \frac{0.57 \cdot c}{f_{\text{notch}} \cdot \sqrt{\epsilon_{\text{eff_slot}}}} \quad (9)$$

This value is used to optimize the slot length and obtain exactly the required band-rejection. It has to be noticed that the slot length has higher effect on the band-rejection than the slot width as the simulations of the antenna showed (the same result was found in [3]).

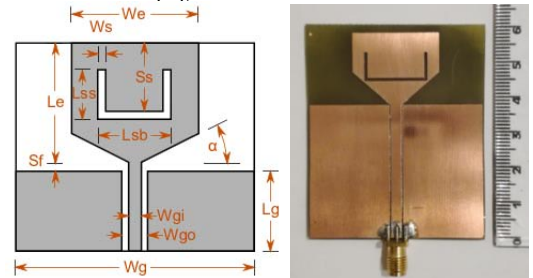


Fig 2. Design Parameters and prototype of proposed single band rejection CPW-fed UWB Trapezoidal monopole antenna fabricated on FR4 substrate.

IV. THE U-SHAPED CPW-FED TRAPEZOIDAL SINGLE NOTCHED MONOPOLE ANTENNA SIMULATION RESULTS

A. Impedance Characteristics

The trapezoidal monopole's increased impedance bandwidth with respect to that of a square or rectangular monopole is depended on the tapered bottom edges which ensures a broadband impedance transition. The length of the element determines the minimum operating frequency, and the reflection coefficient at higher frequencies is affected by several factors. These include the shape of the base taper and the ground-plane dimensions. There are numerous small changes which can be made to the basic topology to reduce the reflection coefficient across the whole band. Examples of this include cutting notches or steps in the base or top of the monopole element [2,3]. The impedance mismatch at slot resonance is generally high but tends to diminish at higher resonant frequencies. The ratio of notch frequency to minimum frequency is limited by the available space on the monopole, the slot shape, and the type of the substrate [7]. Fig.3 presents the simulated and measured VSWR of the proposed single band notched antenna for military service interference rejection at 3GHz. The simulation was carried out with Antenna Magus software in cooperation with CST Microwave Studio Suite software.

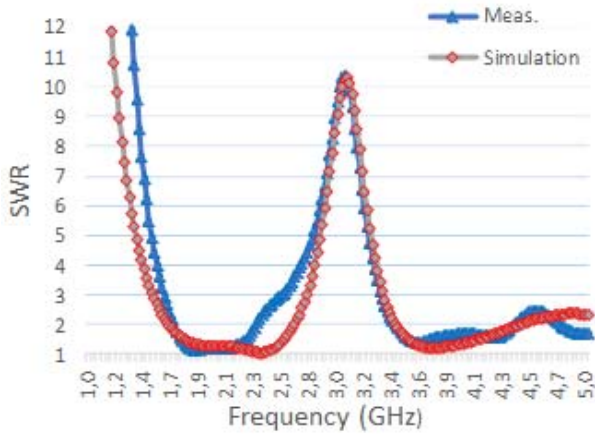


Fig 3. Simulated and Measured VSWR of proposed single band notched CPW-fed UWB Trapezoidal monopole antenna for rejection at 3GHz.

B. Radiation Characteristics

The radiation of the single slot proposed trapezoidal monopole antenna is similar to a planar monopole extending beyond a ground plane, but the asymmetrical geometry distorts the pattern especially at the higher frequencies. This antenna can typically be used in a multi-path environment where radiation pattern is not a limiting factor [7], since the beamwidth calculated from the simulations (Fig.4) is wide enough.

C. Design Guidelines

Low permittivity substrates tend to require very narrow gaps in the co-planar waveguide when designed for 50 Ω line impedance. This makes their construction difficult. In addition, the metal thickness may be of the same order as the gap width, leading to lower line impedance. For the appropriate design of the antenna the below results shall be considered [2,3,7]:

- S_{11} value can be minimized over the operating band by adjusting the taper angle and the feed gap,
- further S_{11} reduction may be obtained by cutting optimized notches or steps in the base or top of the monopole element,
- the notch frequency can be decreased by increasing the total slot length, and
- the notch band rejection may be increased by moving the bottom corners of the slot closer to the bottom of the monopole element.

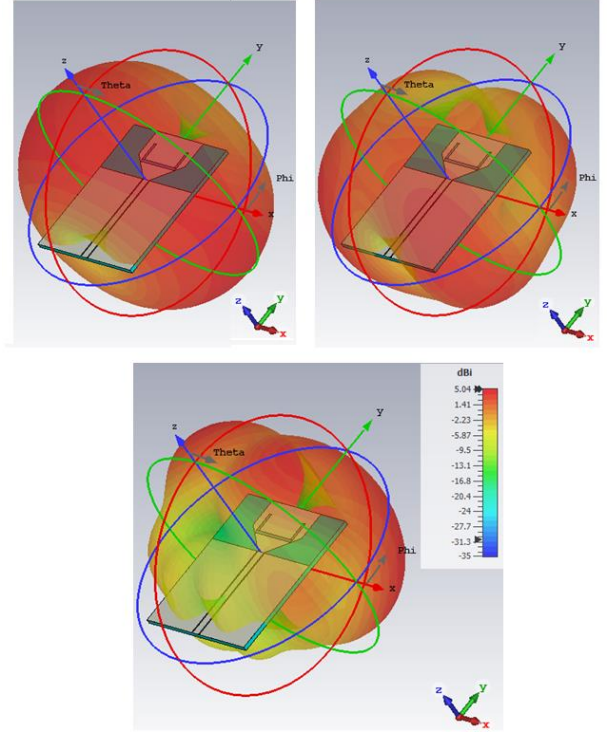


Fig 4. 3D radiation patterns of proposed single band notched CPW-fed UWB Trapezoidal monopole antenna.

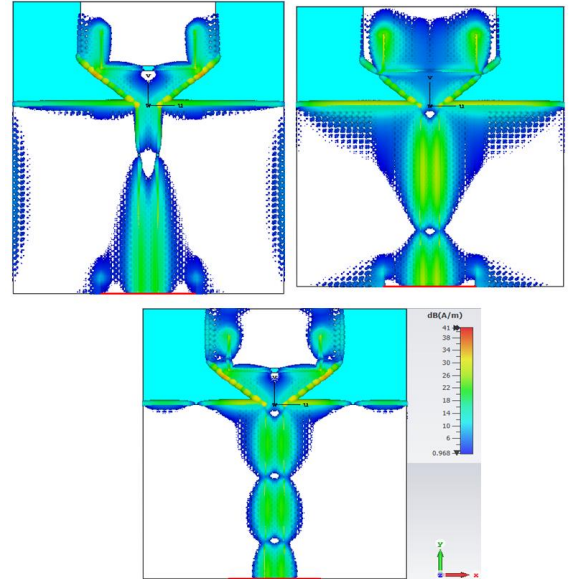


Fig 5. Current distributions of proposed single notched CPW-fed UWB Trapezoidal monopole antenna at rejected frequency 3 GHz.

V. THE U-SHAPED CPW-FED TRAPEZOIDAL DUAL NOTCHED MONOPOLE ANTENNA

In this section, a dual band-notched *UWB CPW-fed* trapezoidal monopole antenna is presented. Two notch elements are formed in the proposed trapezoidal monopole antenna to remove interfering frequencies both from military services and WiMAX networks at 3GHz and 3.5 GHz respectively [10]. The frequency-notch function was achieved by inserting two *U*-shaped slots into the antenna. By properly adjusting the dimensions of the inserted slot, the proposed antenna revealed good *UWB* performance, accompanied by a dual band-rejection function. The notch frequency can be adjusted by changing the slot length [4]. The length of the slot should be approximately half the effective guided wavelength as described by equation (6).

The lengths L_{ss} and L_{ss-2} of the antenna's slots both become critical for determining the center frequency of the notched bands, because the slots act as quarter-wavelength resonators at the desired frequencies. Optimizing the lengths L_{ss} and L_{ss-2} numerically and experimentally, the undesired frequency bands can be notched [4].

The band-rejection frequencies can be changed by changing lengths of the *U*-shaped slots with the other parameters fixed. Thus, the center frequency of every band notch is shifted towards lower frequencies by increasing L_{slot} [11]. The resonant frequency of each *U*-shaped slot can be approximately calculated by:

$$f_{ni} = \frac{170}{l_{ni} \sqrt{\epsilon_{eff_slot}}} \text{GHz} \quad (10)$$

where f_{ni} denotes the resonant frequency of the i_{th} band-notch structure and l_{ni} denotes the length, expressed in millimeters, of the i_{th} band-notch structure with i being the number of slots. As it can be shown from (10) increasing l_{ni} , f_{ni} is decreased [1]. Prototype implementation and design parameters are shown at Fig. 6.

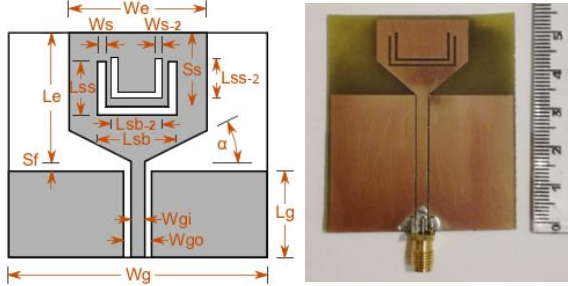


Fig 6. Design Parameters and prototype of proposed dual band rejection CPW-fed UWB Trapezoidal monopole antenna fabricated on FR4 substrate

A. Impedance Matching – VSWR

In Fig.7 the simulated and the measured VSWR performance for distinct values of *U*-slot lengths are presented (the respective parameters are shown in Table II). The antenna appears dual band-notched characteristics (up to 10:1 value of VSWR) at the rejected frequencies of 3 GHz and 3.5 GHz. According to the literature, as the slot length value varies from a lower value, the notch frequency is shifted to lower frequencies. The radiation patterns of proposed dual notched antenna are presented at Fig.9. Fig.16 illustrates the VSWR measurement setup at the laboratory where the Keysight FieldFox N9915A VNA was used.

B. Current Distribution

In Fig.5 and Fig.8 the surface current distributions for single and dual notched antennas are presented at notch frequencies of 3 GHz and 3.5 GHz respectively. It has to be noticed that the current is mainly concentrated around the *U*-shaped slots, and flows in the opposite direction at notch frequency. Strong attenuation and cancellation of the radiating field is observed when the current is out of phase and flows in the opposite direction [12].

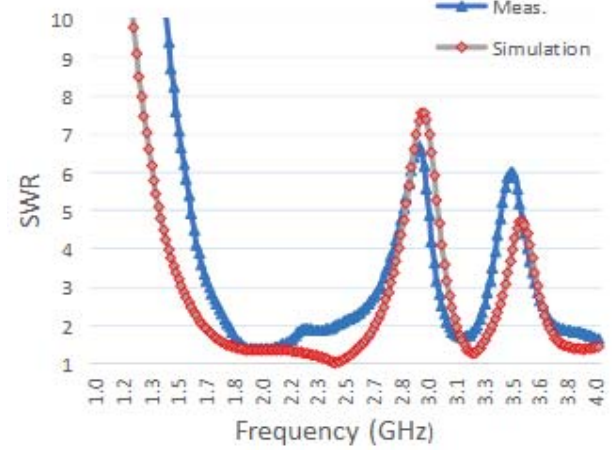


Fig 7. Simulated and Measured VSWR of proposed dual band notched CPW-fed UWB Trapezoidal monopole for rejection at 3 and 3.5GHz.

On the other side, increasing the frequency, the electrical length of the antenna is getting more than the half wavelength. In this scenario, the surface current distributed on the radiating patch will be destructive, and reduction of the radiation pattern at this frequency will be detected [1]. The placement of *U*-slot disturbs the surface current creating another notched band except the band created by the outer dimensions of the patch. The shift of resonance occurs due to the new electrical path that surface current follows when the width of *U*-slot is changed [13].

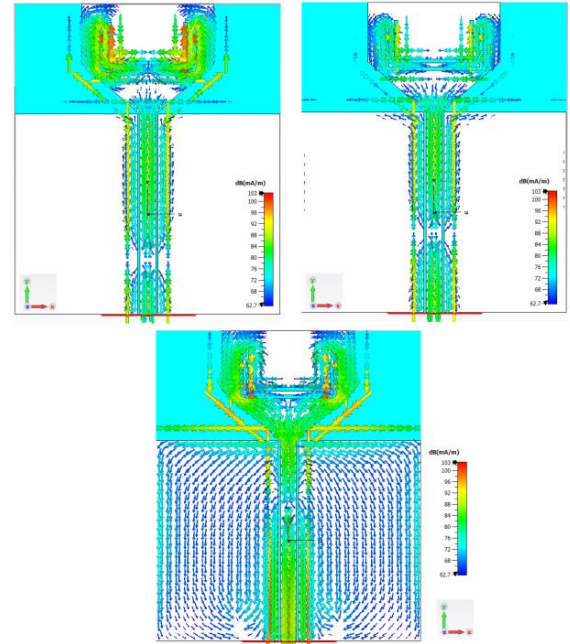


Fig 8. Current distributions of proposed dual notched CPW-fed UWB Trapezoidal monopole antenna at rejected frequencies: 3 GHz and 3.5 GHz.

Parameter	Description	Value
L_e	Monopole element length	20.5 mm
W_e	Monopole element width	25 mm
α	Taper angle at monopole base	40.5°
S_f	Feed gap	88.76 μ m
W_g	Ground-plane width	50 mm
L_g	Ground-plane length	37.5 mm
W_{gi}	CPW inner width	3 mm
W_{go}	CPW outer width	3.9 mm
W_s	Slot width	0.7 mm
L_{sb}	Slot bottom length	18.5 mm
L_{ss}	Side Slot length	8.5 mm
S_s	Slot offset	12 mm
L_{sb-2}	2 nd Slot bottom length	15 mm
L_{ss-2}	2 nd Side Slot length	8 mm
S_{s-2}	2 nd Slot offset	-6 mm
W_{s-2}	2 nd Slot width	0.7 mm

Table II. Physical Parameters of proposed UWB Trapezoidal dual band rejection CPW-fed monopole antenna fabricated on FR4 substrate.

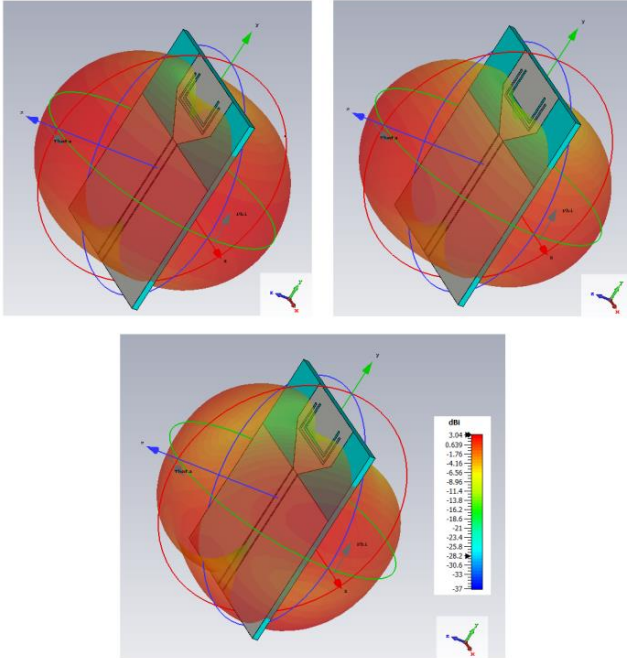


Fig 9. 3D radiation patterns of proposed dual band notched CPW-fed UWB Trapezoidal monopole antenna.

VI. PARAMETRIC STUDY ANALYSIS RESULTS

D. Single U-shaped Slot Parametric Study Analysis

The parametric study analysis was carried out with Antenna Magus software. Three basic parameters were examined (Slot bottom length - L_{sb} , Side slot length - L_{ss} , and Slot width - W_s) to accurately determine the dimensions of the U-slot, and consequently apply the desired cut-off frequency of the proposed trapezoidal monopole antenna at 3 GHz.

- **Slot bottom length (L_{sb}):** As the bottom length of the slot L_{sb} decreases or increases the cut-off frequency becomes higher or lower respectively as shown in Fig.10 [2,14].

- **Side slot length (L_{ss}):** As the length of the slot L_{ss} decreases or increases, the cut-off frequency moves to higher or lower values respectively, as shown in Fig.11 [4,11].

- **Slot width (W_s):** Parametric Study Analysis showed that the thickness W_s of the slot does not have such a significant effect on the cut-off frequency. Nevertheless, a slight shift in the cut-off frequency to higher or lower values is observed with a corresponding increase or decrease in the W_s of the notch, as shown in Fig.12.

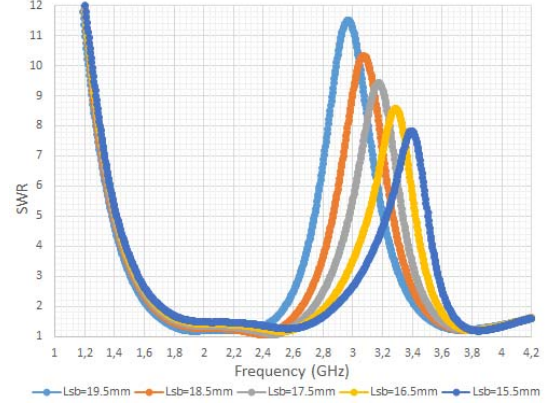


Fig 10. Slot bottom length (L_{sb}) Parametric Study Analysis.

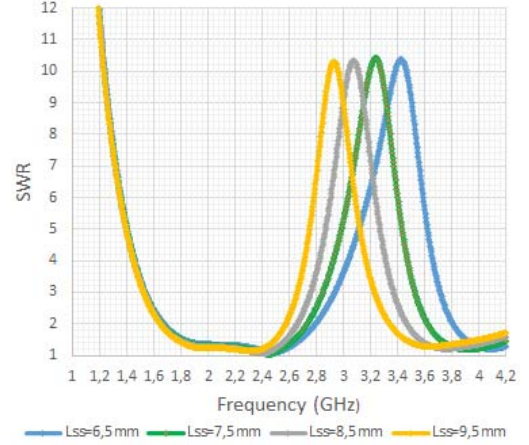


Fig 11. Side slot length (L_{ss}) Parametric Study Analysis.

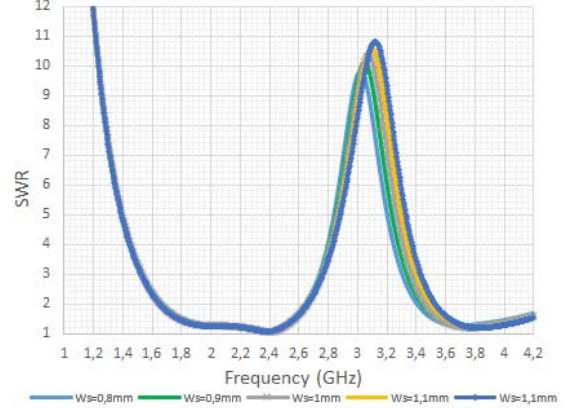


Fig 12. Slot width (W_s) Parametric Study Analysis.

E. Dual U-shaped Slot Parametric Study Analysis

Maintaining the initial dimensions of the first slot, the parametric analysis of the second slot was also performed for the same parameters (L_{sb-2} , L_{ss-2} , W_{s-2}). The simultaneous appearance of the second cut-off frequency at 3.5 GHz of the proposed trapezoidal monopole antennas was a crucial factor for the prototype implementation. Similarly, to the study for the 1st slot, the results from the study for the 2nd slot are presented at Figs 13 to 15.

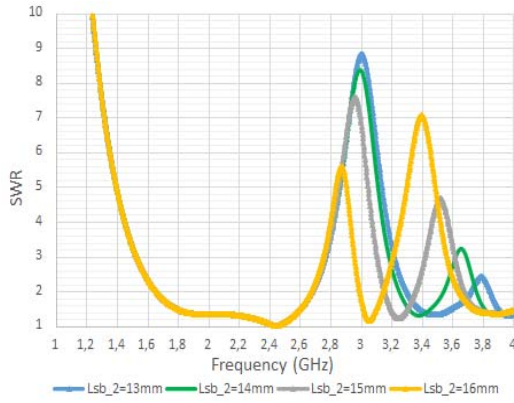


Fig 13. 2nd Slot bottom length (L_{sb-2}) Parametric Study Analysis.

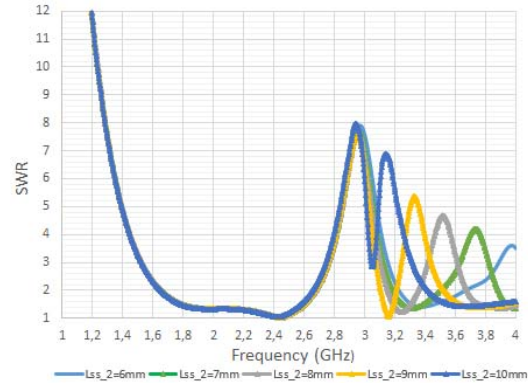


Fig 14. 2nd Side slot length (L_{ss-2}) Parametric Study Analysis.

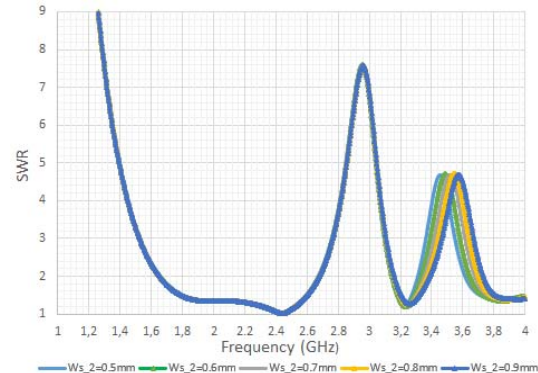


Fig 15. 2nd Slot width (W_{s-2}) Parametric Study Analysis.

VII. CONCLUSIONS

This study demonstrates the design methodology of planar CPW-Fed UWB trapezoidal monopole antennas with single and dual band rejection characteristics by U-shaped slot utilization. These antennas can be used to avoid possible interferences in undesired frequency bands. In this study antenna prototypes fabricated on single FR4 layer substrates with $\epsilon_r = 4.35$ occupying small surface of 50mm x 58mm, and were designed to reject services at 3 GHz and 3.5 GHz. The VSWR measurements taken with a Keysight FieldFox N9915A VNA are compliant with parametric study analysis of the antennas. As a result, band-notched characteristics up to 10:1 VSWR appeared on undesired frequencies while maintaining omnidirectional patterns in the H -plane. Summarizing, the proposed antennas seem to be a good solution for UWB communications requiring band-notched applications additionally with planar implementation and small size.

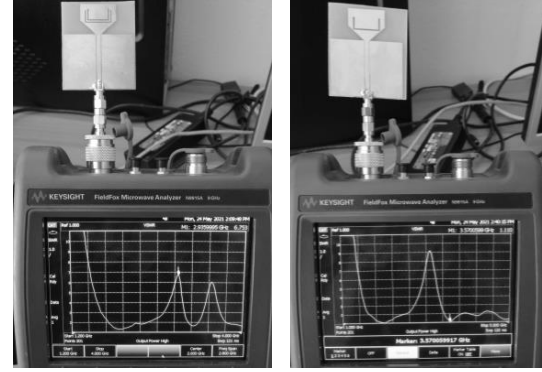


Fig 16. SWR measurement results of proposed Single-Dual band-rejected CPW-fed Trapezoidal Monopole Antenna prototypes on Keysight N9915.

VII. ACKNOWLEDGMENTS

«The implementation of the doctoral thesis was co-financed by Greece and the European Union (European Social Fund-ESF) through the Operational Programme «Human Resources Development, Education and Lifelong Learning» in the context of the Act «Enhancing Human Resources Research Potential by undertaking a Doctoral Research» Sub-action 2: IKY Scholarship Programme for PhD candidates in the Greek Universities» (MIS-5113934).



Operational Programme
Human Resources Development,
Education and Lifelong Learning
Co-financed by Greece and the European Union



REFERENCES

- [1] Junjun Wang, Xudong He, "Analysis and Design of a Novel Compact Multiband Printed Monopole Antenna", International Journal of Antennas and Propagation, vol. 2013, Art. ID 694819, 8 pages, 2013.
- [2] Lee, J.N. and Park, J.K. (2005), Impedance characteristics of trapezoidal ultra-wideband antennas with a notch function. Microw. Opt. Technol. Lett., 46: 503-506.
- [3] H. M. Zamel, A. M. Attiya and E. A. Hashish, "Design of a Compact UWB Planar Antenna with Band-Notch Characterization," 2007 National Radio Science Conference, 2007, pp. 1-8.
- [4] Xi, J.-M. and Liang, C.-H. (2010), CPW-fed trapezoidal antenna with dual band-notched characteristic for UWB application. Microw. Opt. Technol. Lett., 52: 898-900.
- [5] N. Z. A. Naharuddin and N. H. Noordin, "UWB trapezoidal antenna with a band-notch characteristic," 2015 International Workshop on Electromagnetics: Applications and Student Innovation Competition (iWEM), 2015, pp. 1-2.
- [6] Tampouratzis, M.G.; Vouyioukas, D.; Stratakis, D.; Yioultsis, T. Use Ultra-Wideband Discone Rectenna for Broadband RF Energy Harvesting Applications. Technologies 2020, 8, 21.
- [7] Antenna Magus - The Leading Antenna Design Tool.
- [8] Pozar, David M. Microwave Engineering. Hoboken, NJ :Wiley, 2012.
- [9] Lvxia, S. & Huiping, G. & Xueguan, L. & Ying, W. (2012) Ultra-wideband planar monopole antenna with parametric study. Microwaves, Antennas & Propagation, IET. 6, pp 172-177.
- [10] Federal Communications Commission (FCC) <https://www.fcc.gov>
- [11] Seo, Yeon Seok & Jung, J.W. & Lee, Hae June & Lim, Y.S.. (2012). Design of trapezoid monopole antenna with band-notched performance for UWB. Electronics Letters. 48: 673-674.
- [12] Kumar S, Lee GH, Kim DH, Haunan NS, Choi HC, Kim KW. Compact Planar Super-Wideband Monopole Antenna with Four Notched Bands. Electronics. 2020.
- [13] Hasan, Md Nazmul & Shah, S.W. & Babar, M.I. & Sabir, Zeeshan. (2012). Design and simulation based studies of a dual band u-slot patch antenna for WLAN application. 997-1001.
- [14] Jin, Yunnan & Tak, Jinpil & Choi, Jaehoon. (2016). Quadruple Band-Notched Trapezoid UWB Antenna with Reduced Gains in Notch Bands. Journal of Electromagnetic Engineering & Science 16. 35-43.

IoT-based ELF Magnetic Flux Density Meter

Manolis G. Tampouratzis¹, George A. Adamidis², Demosthenes Vouyioukas¹, Traianos Yioultsis³, Dimitrios Stratakis⁴

¹Department of Information and Communication Systems Engineering, University of the Aegean, Karlovasi, GR 82300 Greece, {tampouratzis, dvouyiou}@aegean.gr

²Department of Electronics Engineering, Hellenic Mediterranean University (HMU), Chania, GR 73133 Greece, sv7fid@yahoo.gr

³Department of Electrical and Computer Engineering (ECE), Aristotle University of Thessaloniki (AUTH), Thessaloniki GR 54124 Greece, traianos@auth.gr

⁴Department of Electrical and Computer Engineering (ECE), Hellenic Mediterranean University (HMU), Heraklion GR 71004 Greece, dstrat@hmu.gr

Abstract—This study presents an IoT-based ELF magnetic field meter that can measure magnetic flux density from 100nT. The proposed device has a flat response across the frequency range from 40Hz to 10 KHz, detecting and measuring most magnetic field sources. The proposed meter can measure fields from the power supply network (usually 50 or 60Hz) and harmonic frequencies extending several times above the base frequency in the operating frequency band. The proposed circuit of the magnetic flux density (magnetic field) meter is quite simple for implementation and the measured field can be displayed on any mobile device with Wi-Fi connectivity. A WeMos D1 Arduino board with an embedded ESP-8266 module is responsible for data transferring from the sensor to the cloud as a complete IoT solution, supported by the Blynk application via Android and iOS operating systems or web interface.

Keywords—IoT, Magnetic Field Measurements, Magnetic Flux Density, Coil, RMS Detector, Reasonable - Gain Integrator.

I. INTRODUCTION

Several studies have shown that long-time exposure to strong extremely low-frequency (ELF) magnetic fields (1Hz - 100KHz) can cause serious health problems [1]. A considerable rise in blood triglycerides, a putative stress indicator in humans, the disorientation of chicks, and a reduced response time in monkeys are some unsettling effects of exposure to ELF fields [1],[2]. Although some other research shows no link, epidemiological studies show a positive association between residential and occupational exposure to ELF fields and several forms of cancer.

Magnetic fields (MFs) depend on the radiation's type, field, frequency, and wavelength. Depending on the current feed, either static magnetic fields (SMF) with direct current (DC) or alternating magnetic fields (AMF) with alternative current (AC) are created. In contrast to SMFs, the polarity of an AMF remains constant despite periodic changes in the direction of the current flow. Many devices create powerful low-frequency magnetic fields such as transformers, electric motors, electric heaters, electric toothbrushes, hair dryers, speakers, cathode ray tubes (CRTs), as well as the production, distribution, and consumption of 50 and 60Hz electric energy. In medicine, magnetic resonance imaging (MRI) uses strong SMF, and the patients are often subjected to between 1.5 and 3T. The public has expressed the most worry about these appliances' use as high magnetic field sources.

Depending on the exposure source and the distance from that source, magnetic field strengths might vary significantly. Depending on how well the opposing magnetic flux lines cancel each other out or how well the current-carrying lines

are balanced, the rate at which the field intensity decreases with distance might differ from one source to another. At an increasing distance, fields from coils, magnets, or transformers degrade quickly by a factor of $1/r^3$. In power lines, partial field cancelling causes the drop-off to be $1/r^2$ when currents flow in opposite directions. When there is an imbalanced current, the field intensity decreases more slowly than $1/r$, as shown in Figure 1 [2].

Strong magnetic field sources can be detected with an ELF magnetic field meter, taking the necessary precautions [3], [11].

II. MAGNETIC FLUX DENSITY METER OPERATING PRINCIPLE

According to the Law of Electromagnetic Induction (*Faraday's law*), the induced electromotive force in any closed circuit is equal to the negative time rate of the change of the magnetic flux enclosed by the circuit. Thus, when some magnetic flux passes through a coil it produces some voltage across it which depends on the field intensity rate and the total surface enclosed by the boundary of the coil. In mathematical terms:

$$E = -\frac{d\Phi}{dt} = -A N \frac{dB}{dt} \quad (1)$$

where Φ is the magnetic flux passing through the coil, A is the area enclosed by each turn of the coil, N is the total number of turns of the coil, B is the magnetic flux density of the field (magnetic field) and t is the time. The rate of change of the magnetic flux density is essentially the time derivative of the magnetic flux density (a derivative of the magnetic flux concerning time).

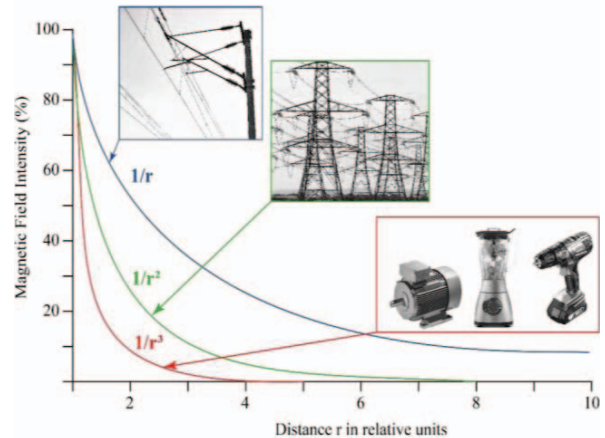


Fig. 1. The magnetic field intensity decreases with the growing distance from the field with fast ($1/r^2$, $1/r^3$) or slow ($1/r$) drop-off [1].

Considering that in the space there is a harmonic (sinusoidal) magnetic field of the form:

$$B(t) = B_o \cos(2\pi ft) \quad (2)$$

where $B(t)$ is the instantaneous value of the magnetic flux density (function of time), B_o is the maximum value of the oscillating field and f is the frequency of oscillation. From (1) and (2) we conclude that if a coil is placed into the harmonic field, then a harmonic voltage $E(t)$ will be induced at its terminals which will be equal to:

$$E(t) = 2\pi f A N B_o \sin(2\pi ft) \quad (3)$$

We observe that the induced voltage is proportional to the geometric characteristics of the coil (A , N), the frequency f , and the field strength B_o . The harmonic term $\sin(2\pi ft)$ shows that voltage is a harmonic function of time and has a phase difference of 90° concerning the field. From (3), we observe that if the induced voltage E can be measured, then the B field can be calculated, as long as the exact frequency f is known. In practice, when the magnetic field of an arbitrary (unknown) source is measured, we are not aware of its frequency. To solve the problem of the unknown frequency, both sides of equation (3) are multiplied with the absolute value of $G/2\pi f$ term, where G is a constant for any specific frequency f , corresponding to amplifier voltage gain. Then we will have:

$$\left| \frac{G}{2\pi f} \right| E(t) = G A N B_o \sin(2\pi ft) \quad (4)$$

by setting:

$$V(t) = \left| G / 2\pi f \right| E(t), \text{ hence:}$$

$$V(t) = G A N B_o \sin(2\pi ft) = G A N B(t) \quad (5)$$

Referring to *RMS* terms (*Root Mean Squared values*) the *RMS* voltage (V_{rms}) is proportional to the *RMS* magnetic field density (B_{rms}) and independent of the frequency [4]:

$$V_{rms} = G A N B_{rms} \quad (6)$$

Therefore, is easy to calculate the magnetic flux density (B_{rms}) by measuring the voltage value (V_{rms}) with an analog electronic device i.e., a magnetic flux density meter. Figure 2 illustrates the block diagram of the proposed IoT magnetic flux density meter, providing cloud-based services. The electronic circuit (analog section) of the proposed magnetic flux density meter is simple for implementation, and the components have a low tolerance for measurement error minimization. A detector coil with well-defined geometric characteristics as a field sensor, an amplifier with voltage gain equal to $G/2\pi f$, an *RMS* detector, and a voltage display are required for a real circuit that makes use of equation (6).

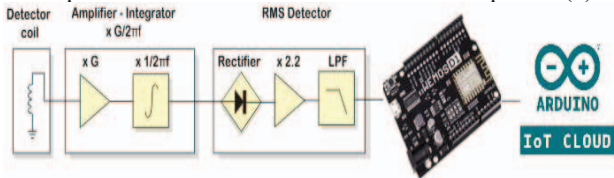


Fig. 2. The block diagram of the proposed IoT-based magnetic flux density meter. A WeMos D1 Arduino board is used to provide Wi-Fi connectivity.

In the proposed implementation, a WeMos D1 Arduino board is used instead of a common voltmeter at the analog output of the device, providing network connectivity for data transferring to the IoT cloud [5],[8]. The measured voltage values at the analog output correspond to magnetic field strength values and can be displayed on any mobile device.

A. The Amplifier with $G/2\pi f$ gain

A circuit having a $1/f$ response is an integrator [6] (a low pass filter with a linear amplitude response and an ideal cut-off frequency of 0 Hz). An almost perfect integrator can be implemented by using an operational amplifier and some passive components. One high-gain integrator or several amplifying stages in series with a reasonable-gain integrator are required to achieve high gain value. In the proposed circuit it is preferred the second solution where the amplifier unit is used before the integrator. High amplification is necessary for the detector to be sensitive without having to use any large coil (since the output voltage for a reasonably sized coil is relatively small, especially at low frequencies).

B. The *RMS* detector

For the implementation of a magnetic field meter that will be able to measure *RMS* field values rather than average or peak values, a section of the *RMS* detector is needed. The output of the integrator is an *AC* signal. To measure the *RMS* value of this signal, a rectifier is used to extract the *DC* component of the rectified signal. Indeed, the *DC* component of a rectified signal is shown to be directly proportional to the *RMS* value of the harmonic input signal.

Considering a half-wave rectified voltage V_s , during a full cycle ($0 - 2\pi$ rad):

$$V_s = V_m \sin(\omega t) \quad \text{for } 0 \leq \omega t < \pi \quad \text{and} \quad (7)$$

$$V_s = 0 \quad \text{for } \pi \leq \omega t < 2\pi$$

where V_m is the maximum value of the half-wave rectified voltage. The Fourier series of the above function is [7]:

$$V_s = \frac{V_m}{\pi} + \frac{V_m}{2} \sin(\omega t) - \frac{2V_m}{3\pi} \cos(2\omega t) - \frac{2V_m}{15\pi} \cos(4\omega t) + \dots \quad (8)$$

and hence,

$$V_s = \frac{V_m}{\pi} + \frac{V_m}{2} \sin(\omega t) + \sum_{N=2}^{\infty} \frac{V_m [1 + (-1)^N]}{\pi (1 - N^2)} \cos(N\omega t) \quad (9)$$

Moreover, we are aware that in half-wave rectified signal:

$$V_{DC} = \frac{1}{T} \int_0^T V_{out}(t) dt = \frac{1}{T} \int_0^{T/2} V_m \sin\left(\frac{2\pi t}{T}\right) dt = \frac{V_m}{\pi} \quad (10)$$

and,

$$V_{rms} = \sqrt{\frac{1}{T} \int_0^T V_{out}^2(t) dt} = \sqrt{\frac{1}{T} \int_0^{T/2} V_m^2 \sin^2\left(\frac{2\pi t}{T}\right) dt} = \frac{V_m}{2} \quad (11)$$

The first term in (9) represents the *DC* component of the semi-rectified signal, the second term is the 1st harmonic (base frequency) and the remaining terms are higher-order harmonics. Assuming that in a harmonic (sinusoidal) signal:

$$V_{rms} = \frac{V_m}{\sqrt{2}}, \quad V_{DC} = \frac{\sqrt{2} V_{rms}}{\pi} \quad \text{so} \quad V_{rms} = \frac{\pi V_{DC}}{\sqrt{2}} \quad (12)$$

The *RMS* value of the input harmonic signal is equal to the $\pi/\sqrt{2}$ of the *DC* component of the semi-rectified signal. At the rectifier's output (V_{out}), apart from the *DC* component, a large number of harmonics should be rejected. The rejection - filtering of the harmonics can be done with a low pass filter. The cut-off frequency of the low pass filter should be as low as possible to obtain perfect harmonics rejection.

Therefore, the *RMS* detector can be implemented with a half-wave rectifier and a low-pass filter.

III. THE ELECTRONIC CIRCUIT OF THE PROPOSED EMF MAGNETIC FLUX DENSITY METER (ANALOG SECTION)

Figure 3 presents the proposed magnetic field meter's electronic circuit (analog section).

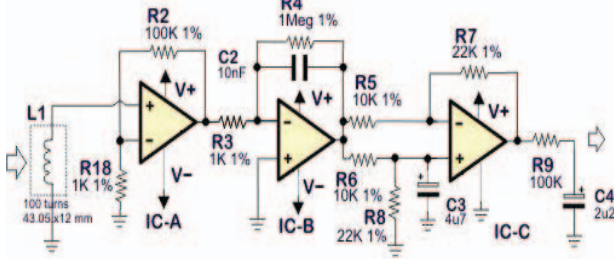


Fig. 3. The electronic circuit of the proposed magnetic flux density meter.

The Op-Amp A is used as a typical non-inverting amplifier with G_a gain:

$$G_a = 1 + \frac{R_2}{R_{18}} \quad (13)$$

The gain G_a is defined by R_2 and R_{18} as described in equation 13, it is equal to 101 and does not depend on frequency. In practice, the gain of the amplifier would be less than 101 for frequencies lower than 40Hz. At higher frequencies, the response of the amplifier is limited by the characteristics of the op-amp (the gain-bandwidth product). However, from 40Hz to 10KHz, the amplifier response is almost flat and the gain is approximately equal to the theoretical value with a potential error of less than 1dB if 1% accuracy resistors are used for R_2 and R_{18} .

The integrator follows up the amplifier. The integrator is made from Op-Amp B, R_4 , R_3 , and C_2 . The response of the integrator is inversely proportional to the frequency due to C_2 . Indeed, if we analyze the integrator as a typical inverse amplifier, we will find that its gain G_b is equal to:

$$G_b = - \frac{R_F}{R_3} \quad (14)$$

The R_F value is the impedance resulting from the parallel combination of resistor R_4 and the X_c impedance (reactance) of C_2 . That is:

$$R_F = X_c // R_4 = R_4 X_c / (R_4 + X_c) \quad (15)$$

Knowing that X_c reactance is equal to:

$$X_c = \frac{1}{2\pi f C_2} \quad (16)$$

By combining equations (14), (15), and (16) we find that:

$$G_b = \left(- \frac{R_4}{R_3} \right) / \left(1 + 2\pi f R_4 C_2 \right) \quad (17)$$

It is noticed that the above relationship is not exactly in the form of $1/f$, because we do not have a perfect integrator due to R_4 . However, with the components we use, the product $2\pi f R_4 C_2$ is much larger than 1 for frequencies above 40Hz and the “1” in the denominator can be omitted. Therefore, for frequencies above 40Hz, the gain of the integrator becomes equal to the:

$$G_b = \left(- \frac{1}{R_3 C_2} \right) \left(\frac{1}{2\pi f} \right) \quad (18)$$

The total gain of the amplifier and integrator chain would be the product of the G_a and G_b , namely:

$$G_t = G_a G_b \quad (19)$$

From equations (13), (18), and (19), we conclude that:

$$G_t = \left(1 + \frac{R_2}{R_{18}} \right) \left(- \frac{1}{R_3 C_2} \right) \frac{1}{2\pi f} \quad (20)$$

where,

$$G = \left(1 + \frac{R_2}{R_{18}} \right) \left(- \frac{1}{R_3 C_2} \right) \quad (21)$$

Taking into account equations (21) and (6), we notice that at the output of the integrator, an *AC* voltage (V_{rms}) is produced which is equal to:

$$V_{rms} = \left(1 + \frac{R_2}{R_{18}} \right) \left(- \frac{1}{R_3 C_2} \right) A N B_{rms} \quad (22)$$

From equation (22) we observe that the produced voltage is directly proportional to the field and does not depend on the frequency, as shown in Figure 4.

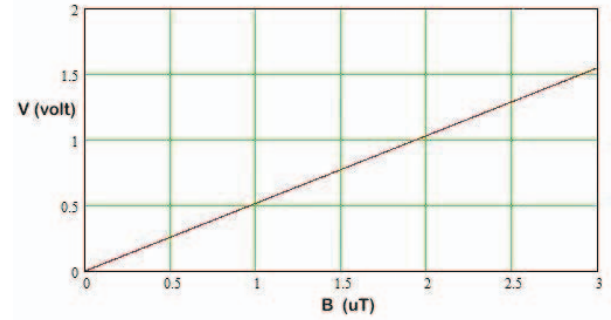


Fig. 4. The output voltage of the proposed RMS detector as a function of the magnetic flux density (using a coil of 100 turns of 43.05x12mm rectangular cross-section).

By the actual value calculation of the G constant, we observe that:

$$G = \left(1 + \frac{R_2}{R_{18}} \right) \left(- \frac{1}{R_3 C_2} \right) = 101 \times 10^5 \quad (23)$$

Winding a coil with a certain number of turns and specific dimensions may constitute the magnetic field probe of the ELF meter. Suppose that the V_{rms} voltage is needed to be 1.2V when the coil is placed inside a 2.3μT (*RMS*) magnetic field. According to equation (22), we should make:

$$A N = 0.05166 \text{ m}^2 \quad (24)$$

By choosing a coil with 100 turns, each turn should include an area of $516.6 \times 10^{-6} \text{ m}^2$. For a rectangular cross-section coil, the desired area can be achieved if each turn is 43.05mm x 12mm. The meter coil should be 100 turns of a 43.05mm x 12mm rectangular cross-section.

After the integrator follows up the rectifier circuit. The rectifier circuit is implemented from The Op-Amp C. It is an uncommon circuit of rectification since there is no diode anywhere. The rectification takes place because the negative half-period of the signal is simply cut off. The Op-Amp C along with the resistors R_5 , R_6 , R_7 , and R_8 is a classical circuit of subtraction (differential amplifier). The voltage applied to the left end of R_5 is subtracted from the voltage applied to the left end of R_6 . However, the left edges of R_5

and R6 are short-circuited, and therefore a voltage equal to zero will always exist at the output of the subtractor. However, this is the case only for *DC*. For the *AC* signal, the capacitor C3 acts as a short circuit and grounds the non-inverting input of Op-Amp C. With this technique, the subtractor is converted to an inverting AC amplifier, with an amplification equal to $R7 / R5 = 2.2$.

The above analysis shows that Op-Amp C eliminates the *DC* component of the signal and amplifies the residual *AC* signal by 2.2 times. In addition to the above, Op-Amp C also performs half-rectification of the signal. Half-rectification occurs because the Op-Amp operates at a 0V reference level and there is no negative supply voltage. Therefore, it can only amplify the positive half-period of the signal and during the negative half-period its output becomes zero (that is, the half-phase rectification occurs). At the output of Op-Amp C, we have a semi-rectified signal. The semi-rectified signal contains a *DC* component and some harmonics (see the Fourier series mentioned above). The harmonics are filtered out from a simple low pass filter formed by R9 and C4. The cut-off frequency of this specific filter is equal to $1/2\pi R_9 C_4 = 4.5\text{Hz}$, which is a very low one and approximately the filter passes only the *DC* component. Normally, the *DC* component of a half-rectified signal is equal to $\sqrt{2}/\pi$ of the *RMS* value of the input signal of the rectifier. The term $\sqrt{2}/\pi$ is equal to about 1/2.2. However, since we use amplification equal to 2.2 in the rectifier, we make the half-rectified signal have a *DC* component equal to the exact *RMS* value of the input signal (by cancelling out the 1/2.2 factor). The circuit has an analog output providing voltage equal to 0.1mV/nT at the Analog to Digital (*ADC*) port of the Arduino WeMos D1 board. For instance, for a $2\mu\text{T}$ field, there will be a voltage of 200mV at the analog output of the ELF meter. This output is provided on C4 terminals. C4, along with R9, forms a low-pass filter that extracts the *DC* component from the output of the rectifier as described above.

IV. IoT APPLICATION WITH ESP-8266 WEMOS D1 BOARD FOR REAL-TIME ELF FIELD MONITORING

The value of the measured magnetic field can be displayed in real-time on any mobile device with Wi-Fi connectivity via the Blynk application [10] supported by Android and iOS platforms. An Arduino WeMos D1 board with an ESP-8266 [9] module was used via the *ADC* port for data transferring from the meter to the cloud, as a complete IoT solution [8] as shown in Figure 5. The Blynk user interface can display on mobile terminal both the magnetic field strength H (*A/m*) and the flux density B (*Tesla*) values at the same time using the following transformation formula:

$$B(\text{Tesla}) = \mu_r \mu_0 H(\text{A/m}) \quad (25)$$

where μ_r is the relative and μ_0 is the free space magnetic permeability respectively. Magnetic field levels up to 300nT are considered within safe limits in most countries of the world. The field is regarded as potentially harmful from 400nT to $1\mu\text{T}$, and dangerous from $1\mu\text{T}$ and above.

IV. CONCLUSIONS

This study presents the basic principles of an IoT-based ELF magnetic flux density meter. The prototype circuit can measure magnetic flux density from 100nT with a flat response across the operating frequency range from 40Hz to 10KHz . The device can measure with accuracy, all magnetic fields coming from sources such as transformers, electric motors, electric heaters, hair dryers, and power supply

network and their harmonic frequencies. A WeMos D1 Arduino board with an integrated Wi-Fi module is responsible for the data transferring from the sensor to the cloud, as a complete IoT solution. The measured field is displayed on any mobile device with Wi-Fi connectivity, supported by the Blynk application via Android and iOS operating systems or web interface. An improvement or addition that can be taken place in the proposed basic meter version should be the implementation of identical sensor probes for isotropic field measurements in the X, Y, and Z planes, as a future aspect.



Fig. 5. Measuring the magnetic flux density of various devices by the proposed IoT-based meter. The ELF field strength values (*in A/m and Tesla*) are displayed on the Blynk application supported by the Android platform in a mobile phone with Wi-Fi network connectivity as a complete IoT solution.

IV. ACKNOWLEDGMENTS

«The implementation of the doctoral thesis was co-financed by Greece and the European Union (European Social Fund-ESF) through the Operational Programme «Human Resources Development, Education and Lifelong Learning» in the context of the Act «Enhancing Human Resources Research Potential by undertaking a Doctoral Research» Sub-action 2: IKY Scholarship Programme for PhD candidates in the Greek Universities» (MIS-5113934).



Operational Programme
Human Resources Development,
Education and Lifelong Learning
Co-financed by Greece and the European Union



REFERENCES

- [1] Maffei, Massimo E. 2022. "Magnetic Fields and Cancer: Epidemiology, Cellular Biology, and Theranostics" International Journal of Molecular Sciences 23, No. 3: 1339.
- [2] Reinhard Metz, "Build this Magnetic Field Meter", Radio Electronics-Electronic Experimenter's Handbook, 1993.
- [3] H. Bonekamp, "Magnetic - field meter", Elektor Magazine, p.26, Issue 1, 1997.
- [4] Daniel I. Gordon, Robert E. Brown, John Haben, "Methods for Measuring the Magnetic Field" IEEE Transactions on Magnetics, Vol.8, No.1, March 1972.
- [5] Khaengkarn S., Nonkeaw K., Wonglomklang T., Srisertpol J., "Real-Time Tracking and Environmental Monitoring System for Ice Trucks using IoT Techniques," WSEAS Transactions on Information Science and Applications, Vol. 19, pp. 297-302, 2022.
- [6] Chaniotakis and Cory, "6.071 Introduction to Electronics, Signals and Measurement", Spring 2006, Massachusetts Institute of Technology.
- [7] Jambunatha Sethuraman, "A Note on Fourier Series of Half Wave Rectifier, Full Wave Rectifier, and Unrectified Sine Wave", Vinayaka Mission's Kirupananda Variyar Engineering College, Salem Tamil Nadu India.
- [8] Getting Started With the Arduino IoT Cloud <https://docs.arduino.cc/>
- [9] ESP8266 Module Technical Reference <https://www.espressif.com/>
- [10] Blynk IoT Platform: For Businesses and Developers <https://blynk.io/>
- [11] G.Adamidis M.Tampouratzis "CircuitLib" <https://www.circuitlib.com/>

Storage Efficiency Optimization in Capacitor-based Energy Harvesting Systems

Manolis G. Tampouratzis¹, Nikolaos Plevritakis², Demosthenes Vouyioukas¹, Traianos Yioultsis³, Dimitrios Stratakis⁴

¹Department of Information and Communication Systems Engineering, University of the Aegean, Karlovassi, GR 82300 Greece, {tampouratzis, dvouyiou}@aegean.gr

²Department of Electronic Engineering, Hellenic Mediterranean University (HMU), Chania, GR 73133 Greece, nplevr@gmail.com

³Department of Electrical and Computer Engineering (ECE), Aristotle University of Thessaloniki (AUTH), Thessaloniki, GR 54124 Greece, traianos@auth.gr

⁴Department of Electrical and Computer Engineering (ECE), Hellenic Mediterranean University (HMU), Heraklion, GR 71004 Greece, dstrat@hmu.gr

Abstract—A design methodology for storage efficiency optimization in capacitor-based energy harvesting systems is presented in this study. The proposed approach demonstrates a storage system to utilize efficiency maximization by tank capacitors switching, taking full advantage of inactive charging time. For the implementation, an ultra-low power AVR128DA48 microcontroller was used at 32KHz internal clock reference with a power consumption of 1mW at 1.8V minimum operating voltage.

Keywords—Storage Capacitors, Tank Capacitors, Storage Efficiency, Transient State, Steady State, Capacitor-based Energy Harvesting Systems, Low-Power Micromachines.

I. INTRODUCTION

For a capacitor-based energy harvesting system (EH), the critical parameter for determining its performance is the elapse of the charging time [1]. In such systems the efficiency varies with time [2], hence the energy they can store. During the charging of a capacitor, the rate of energy storage, which also means its instantaneous power, is high at the beginning of charging (*Transient State*), while it almost ceases to store energy after a constant time τ and then up to times 2τ , 3τ , 4τ , 5τ (*Steady State*) [3]. As can be easily demonstrated, the maximization of energy storage, and hence the instantaneous power $P_c(t)$, occurs at the instant just before a time constant (τ), while half of the maximum charging voltage is reached in the storage element. The instantaneous power during the charging in a capacitor (and therefore the rate of energy storage) is a function of the charging time, and is given by the mathematical equation:

$$P_c(t) = V_c(t) \cdot I_c(t) \quad (1)$$

By substituting the following equations for the voltage $V_c(t)$ and the current $I_c(t)$ at a capacitor during charging:

$$V_c(t) = V_{max}(1 - e^{-\frac{t}{\tau}}) \quad (2) \quad \text{and} \quad I_c(t) = \frac{V_{max}}{R} e^{-\frac{t}{\tau}} \quad (3)$$

the instantaneous power $P_c(t)$ is given by:

$$P_c(t) = V_{eqv}(1 - e^{-\frac{t}{\tau}}) \cdot \frac{V_{eqv}}{R_{eqv}} e^{-\frac{t}{\tau}} = \frac{V_{eqv}^2}{R_{eqv}} (1 - e^{-\frac{t}{\tau}}) \cdot e^{-\frac{t}{\tau}} \quad (4)$$

It is noticed that V_{max} , refers to *Thevenin* voltage (V_{eqv}), and R refers to the *Thevenin* resistance (R_{eqv}) of the circuit preceding the storage element respectively. Therefore, (4) can be expressed as:

$$P_c(t) = P_{cMAX} \cdot (1 - e^{-\frac{t}{R_{eqv}C}}) \cdot e^{-\frac{t}{R_{eqv}C}} \quad (5)$$

The above mathematical equation determines the instantaneous power which corresponds to the energy rate that a capacitor stores over time. By calculating the 1st derivative of this equation, is easy to calculate the time t_{Pmax} when the instantaneous power $P_c(t)$ of the storage element is maximized (P_{cMAX}), resulting as given by (6):

$$t_{Pmax} = \frac{dP_c(t)}{dt} = \tau \cdot \ln 2 = R_{eqv}C \cdot \ln 2 \quad (6)$$

Therefore, over the beginning of charging time and up to time t_{Pmax} according to (5,6), the storage element stores energy (*Transient State*). Beyond this time (t_{Pmax}), the instantaneous power $P_c(t)$ of the storage element decreases and tends to zero, while the charging voltage $V_c(t)$ tends to reach its maximum value (*Steady State*) as described in Fig. 1.

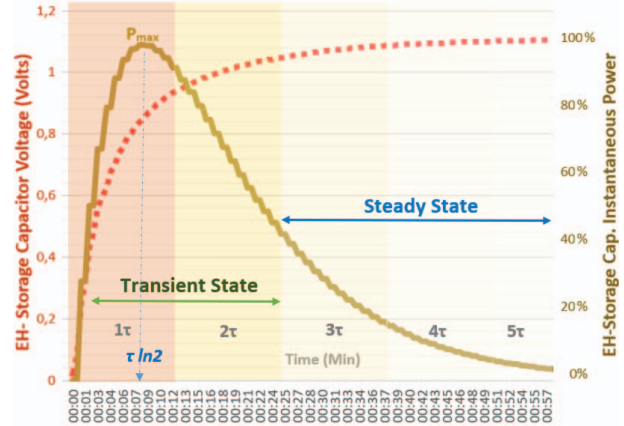


Fig 1. EH's storage capacitor charging response versus the storage efficiency. When the voltage V_c reaches its maximum value, the storage element ceases to save more energy, and the average power is minimized.

As it is known that during a time constant (τ) the charging voltage of a capacitor is done at about 63%, while during 2τ the value has already reached 86%, it is obvious that for the following time constants 3τ , 4τ and 5τ (full charge), the charging time essentially remains unexploited (see Table I). These time intervals correspond to instantaneous power minimization time determined by the following inequality:

$$\tau \cdot \ln 2 < t_{P_{cinst. Minimization}} \leq 5\tau \quad (7)$$

II. APPROACH IMPLEMENTATION

In our approach, an attempt is made to utilize the unused charging time (t_{unused}) by alternating the activation of the harvesting system's storage elements. The above process is

illustrated in Fig.2. It is necessary to have a second identical storage element (*tank capacitor*) which will always operate in a different state from the first one. For example, while the 1st tank capacitor will be in charging mode, the 2nd tank capacitor will be in discharging mode, and vice versa. Consequently, the active storage element will always be in a transient state as long as possible. This would result in operating the device at a lower voltage than the maximum, knowing that the charging voltage where it has been reached up the time t_{Pmax} when the instantaneous power $P_c(t)$ is maximized, corresponds to half of the maximum voltage.

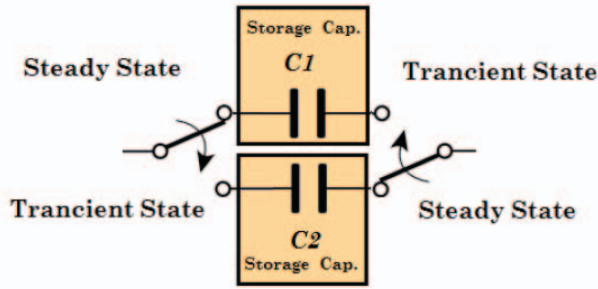


Fig 2. Tank capacitors' switching for storage efficiency optimization at the transient state, taking full advantage of inactive charging time.

EH-System's Indicative Average Power Calculation

As a result of the proposed implementation, the average power (P_{ave}) calculation in a single capacitor-based energy harvesting (EH) system will be compared with a dual one with equal fragmentation of charging time in storage elements. Assuming that, a 100 μ F capacitor is used for charging time at about 1 minute (that corresponds to 5τ time) for max charging voltage equal to 1 Volt. The average power (P_{ave}) of the capacitor of the system is calculated by the following mathematical equation (8), where E_{0cap} is the harvesting energy at time t_0 (at the beginning of charging) and E_{1cap} is the harvesting energy at time t_1 (full charging) that corresponds to 5τ and reaches to 100% of charging voltage:

$$P_{ave} = \frac{\Delta E}{\Delta t} = \frac{E_{(t_1)cap} - E_{(t_0)cap}}{t_1 - t_0} = \frac{\frac{1}{2} C_{cap} \cdot (V_c^2(t_1) - V_c^2(t_0))}{t_1 - t_0} = 0,83 \mu W \quad (8)$$

On the other side, the average power (P_{ave}) of the proposed dual capacitor-based system is being considered by the alternating activation of the circuit's storage elements into equal fragmentation of charging time [4]. Each time charging fragmentation segment corresponds to time τ , where the charging voltage reaches 63,2 % of the maximum value, and at the same time, the instantaneous power $P_c(t)$ of the storage element is maximized (93,1% of P_{cMax}). For the available charging time of 5τ (*full charge*), the average power (P_{ave}) of the proposed system is given by the equation (9) respectively, assuming that the energy of each charged tank capacitor is completely consumed (*full discharge*) feeding a load or a dc/dc converter by energy bursts, as shown in Fig. 3.

$$P_{ave} = \sum_{i=1}^3 \frac{\Delta E_{(i)cap1}}{\Delta t} + \sum_{i=1}^2 \frac{\Delta E_{(i)cap2}}{\Delta t} = \sum_{i=1}^5 \frac{\Delta E_{(i)cap}}{\tau} = 8,32 \mu W \quad (9)$$

According to this methodology, it follows that the average power (P_{ave}) of the energy harvesting system with the same available charging time (60 sec.) is almost tenfold in case where two storage elements are used in mutation instead of one, and at the same time, the charging time is fragmented

into 5 equal time segments of τ for each tank capacitor, taking advantage of instantaneous power $P_c(t)$ maximization.

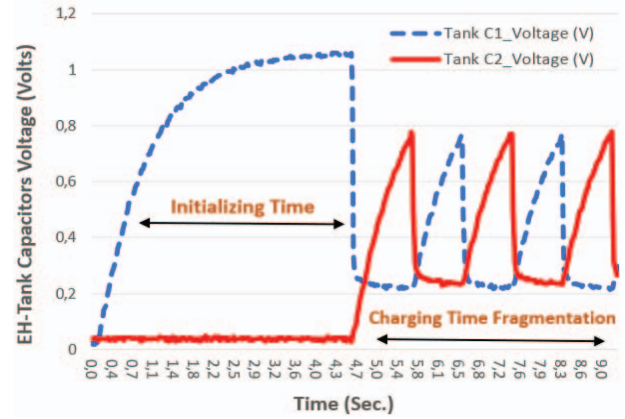


Fig 3. Tank capacitors' charging voltage versus the available charging time taken by OWON XDS2102A oscilloscope. The initialization time (5τ) and its corresponding fragmentation into 5 equal segments of one constant time (τ) reaching 93,1% of P_{cMax} and 0,63 of V_{max} , are distinguished respectively.

Proposed Circuit Operation

To achieve the intended purpose, it is necessary to use active electronic components for the switching of each storage element (*tank capacitor*). One solution could be the usage of MOSFET transistors as electronic switches with low channel activation voltage, and tank capacitors with leakage voltage as low as possible, driven by a microcontroller unit. The schematic of the proposed electronic circuit is presented in Fig.4, and the MOSFET's switching states for the tank capacitors' discrete modes are given in Table II. In practice, from the proposed implementation there will be energy losses for the opening/closing of the MOSFET transistors as well as from the leakage voltage of the capacitors [5].

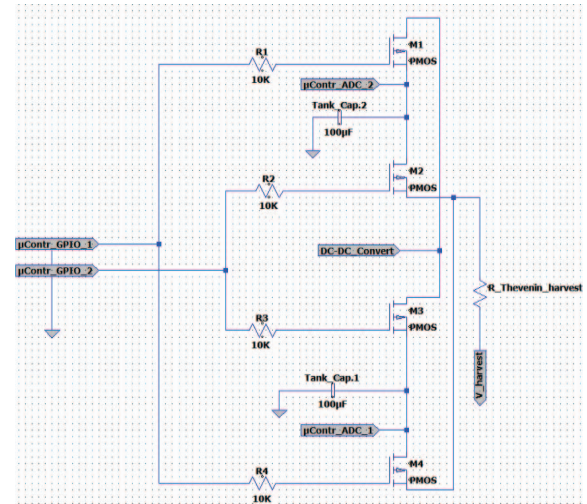


Fig 4. The schematic of the proposed electronic circuit based on *p*-channel MOSFET transistors and tank capacitors for storage efficiency optimization

For the prototype implementation, 4 *p*-channel BS-250 MOSFET transistors [6] and 2 equal 100 μ F tank capacitors as storage elements, were used. A common Arduino UNO board was initially used as a controller unit, which was later replaced by ultra-low power AVR128DA48 Curiosity Nano board [7] to minimize the power consumption of the active circuit. Fig.5 presents the instantaneous power of EH's tank capacitors and the available charging time fragmentation.

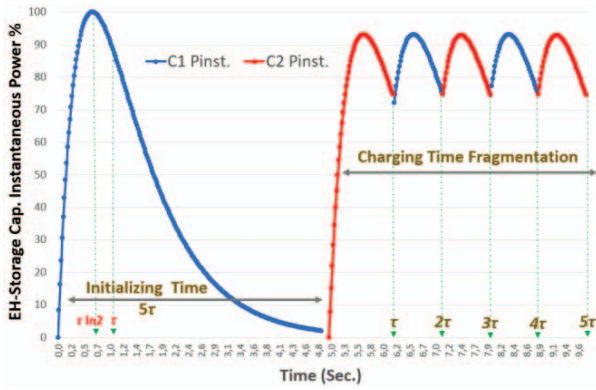


Fig 5. EH-Tank Capacitors' Instantaneous Power and the available charging time fragmentation corresponding to 5 equal slots of one constant time (τ).

Software Operation and Power Consumption

These microcontroller series start using the internal clock reference of 32 KHz to reduce the transient current during the boot stage, making it ideal for ultra-low power applications. Subsequently, the microcontroller initializes the GPIO outputs, the analog to digital converter (ADC) at 12 bits and 8 kS/s, with the V_{ref} voltage to V_{cc} value. Then at the main loop the algorithm measures and checks the voltages of the tank capacitors by alternating the MOSFET transistors as switches, for charging and discharging the capacitors accordingly via GPIO ports. The GPIO pins and ADC peripheral with interrupts are initialized by the microcontroller after power-up. At the initialization state, the microcontroller is measuring the charging voltage on the first capacitor to find the maximum value; this is accomplished by comparing the previous ADC value with the current one in a loop until both are equal and storing it to a variable V_{max} . Then the microcontroller runs in an infinite loop to measure the voltages of the capacitors to switch the charging of C_1 to C_2 and vice versa; when the voltages reach 0.63 value of the V_{max} accordingly. The software is implemented in C using Microchip's Studio and GCC compiler. The current consumption of the microcontroller unit reached about 550 μ A at a minimum operating voltage of 1.8V, which corresponds to power consumption of 1mW for the tank capacitors circuit derived from energy harvesting. Power is measured using the Microchip's power debugger tool, as shown in the experimental setup in Fig. 6.

Time Constant (τ)						
$0,5 \tau$	$\ln 2 \tau$	1τ	2τ	3τ	4τ	5τ
Tank Capacitor's Instantaneous Voltage Value - $V_C(t)$						
39,3%	50,3%	63,2%	86,5%	95%	98,2%	99,3%
Tank Capacitor's Instantaneous Current Value - $I_C(t)$						
60,7%	49,7%	36,8%	13,5%	5%	1,8%	0,7%
Tank Capacitor's Instantaneous Power Value - $P_C(t)$						
95,5%	100%	93,1%	46,5%	18,4%	6,8%	2%
$P_{C \text{ Max}}$	$P_{C \text{ Max}}$	$P_{C \text{ Max}}$	$P_{C \text{ Max}}$	$P_{C \text{ Max}}$	$P_{C \text{ Max}}$	$P_{C \text{ Max}}$

Table I. Instantaneous values of tank capacitor's voltage (V_C), current (I_C), and power (P_C) up to full charging (5τ).

Tank Capacitor	Capacitor State	
C_1	Charging	Discharging
	Mosfet $S1_{ON}, S2_{OFF}$	Mosfet $S1_{OFF}, S2_{ON}$
C_2	Discharging	Charging
	Mosfet $S3_{OFF}, S4_{ON}$	Mosfet $S3_{ON}, S4_{OFF}$

Table II. Mosfet switching states for tank capacitors' storage efficiency utilization at transient state, taking full advantage of inactive charging time.

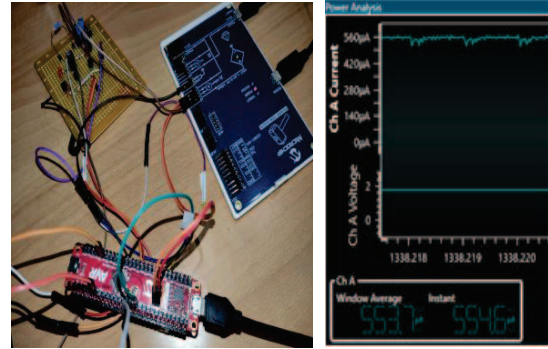


Fig 6. Prototype's implementation measurements with Microchip Power debugger and low-power AVR128DA48 Curiosity Nano as a control unit.

III. ACKNOWLEDGMENTS

«The implementation of the doctoral thesis was co-financed by Greece and the European Union (European Social Fund-ESF) through the Operational Programme «Human Resources Development, Education and Lifelong Learning» in the context of the Act «Enhancing Human Resources Research Potential by undertaking a Doctoral Research» Sub-action 2: IKY Scholarship Programme for PhD candidates in the Greek Universities» (MIS-5113934).



Operational Programme
Human Resources Development,
Education and Lifelong Learning
Co-financed by Greece and the European Union



IV. CONCLUSIONS

In this study, a design methodology for storage efficiency optimization in capacitor-based energy harvesting systems is presented. The proposed approach demonstrates the implementation of a pulse harvester system by switching tank capacitors to utilize the efficiency maximization at the transient state, taking full advantage of inactive charging time by using an ultra-low power AVR128DA48 microcontroller with consumption of 1mW at 1.8V minimum operating voltage. Power consumption can be further reduced by using an external analog to digital converter as a future aspect. Additionally, the sleep mode function of the processor could be used in a future version of the implementation algorithm to reduce power consumption even further, making it functional for RF-EH applications.

REFERENCES

- [1] Kushnerov, A. Transient and steady-state analysis of a single switched capacitor DC-DC converter. International Journal of Electronics Letters 2019, pp. 367-375.
- [2] Tampouratzis, M.G.; Vouyioukas, D.; Stratakis, D.; Yioultsis, T. Use Ultra-Wideband Discone Rectenna for Broadband RF Energy Harvesting Applications. Technologies 2020, 8, 21.
- [3] T. A. Boghdady, S. N. Alajmi, W. M. K. Darwish, M. A. Mostafa Hassan, A. Monem Seif, "A Proposed Strategy to Solve the Intermittency Problem in Renewable Energy Systems using a Hybrid Energy Storage System," WSEAS Transactions on Power Systems, vol. 16, pp. 41-51, 2021
- [4] Hagerty, Joseph & Zhao, Tian & Zane, Regan & Popovic, Zoya. "Efficient broadband rf energy harvesting for wireless sensors", 2003.
- [5] Cultura, A.B. & Salameh, Z., Modeling, "Evaluation and Simulation of a Supercapacitor Module for Energy Storage Application" International Conference on Computer Information Syst. & Industrial Applications (CISIA 2015), Bangkok, Thailand, June 28-29, 2015.
- [6] BS-250 P-Channel Enhancement Mode Vertical D-MOS Transistor.
- [7] Microchip Ultra-Low power AVR128DA48.

A Comparative Study of Copy-Move Forgery Detection Techniques

Brecht Lauwers
Department of Electronics-ICT
Thomas More, Campus De Nayer
Sint-Katelijne-Waver, Belgium
brechtlauwers02@gmail.com

Konstantinos Karampidis
Department of Electrical & Computer
Engineering
Hellenic Mediterranean University
Heraklion, Greece
karampidis@hmu.gr

Manolis Tampouratzis
Department of Electrical & Computer
Engineering
Hellenic Mediterranean University
Heraklion, Greece
tampouratzis@hmu.gr

Manos Vasilakis
Department of Electrical & Computer
Engineering
Hellenic Mediterranean University
Heraklion, Greece
mvasilakis@hmu.gr

Giorgos Papadourakis
Department of Electrical & Computer
Engineering
Hellenic Mediterranean University
Heraklion, Greece
papadour@hmu.gr

Nikos Mastorakis
Technical University of Sofia, Sofia,
Bulgaria and Hellenic Naval Academy,
Piraeus, Greece
mastor@hna.gr

Abstract—In the modern world, the popularity of image editing software has risen sharply, making it easy for non-experts to manipulate images. This poses significant challenges regarding image authenticity and integrity. Consequently, a lot of attention has been aroused by researchers working on this topic and many methods have been developed to discover image forgeries. Copy-move is a manipulation technique that involves copying a region in an image and pasting it in a different location on the same image, leading to misinterpretation. In this paper, a comparative study between conventional and deep learning-based methods is presented. More specifically a statistical-based method is compared against a transfer learning method. Various experiments have been conducted on six different publicly available datasets for different copy-move scenarios. The experiments revealed the superior performance of the deep learning approach, surpassing the statistical method in most cases. This study highlights the effectiveness of deep learning techniques in the field of copy-move forgery detection. Furthermore, the comparative analysis presented in this paper serves as a valuable reference for researchers to accomplish further advancements in image forensics.

Keywords—copy-move, digital forensics, image forensics, deep learning

I. INTRODUCTION

In modern world, utilization of digital data is becoming more and more popular. Although, the use of digital data make our lives easier, it also brings some disadvantages. One of the biggest drawbacks is the difficulty to verify the authenticity and the integrity of these files [1]. Images can be easily manipulated with the use of widely available photo editing software. Typically, this specialized software is used for professional or personal purposes e.g., a photographer who filters his images or a person who applies visual filtering before posting a photo on social media. However, manipulated images may cause serious problems if used for malicious intent, i.e., fake news, misleading the authorities, etc.

Therefore, it is crucial to find efficient methods that can detect forged images. The contemporary forgery techniques can be divided into active and passive approaches. Fig. 1 shows the categories belonging to these types.

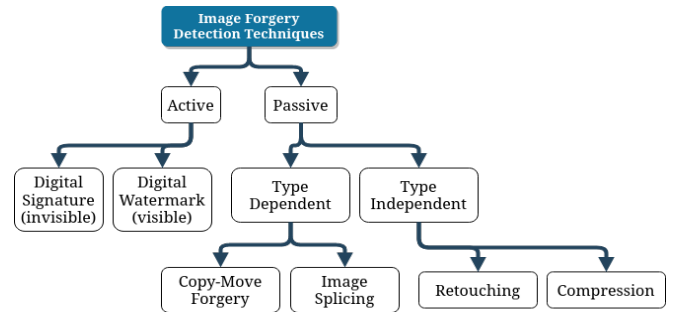


Fig. 1. Image Forgery Detection Techniques.

Active techniques are mostly based on digital signatures [2] or watermarking [1] and rely on the information provided by the genuine image. However, the latter is in most cases unavailable. Passive methods do not need any form of original photo data and therefore are easier to deploy and more widely used. However, passive techniques may not perform well when the image is very compressed (problems with robustness).

In this paper, we will examine the copy-move forgery (CMF) problem and its detection (CMFD). Copy-move forgery is a technique where a region of an image is copied and pasted to a different location within the same image to cause misleading or misinterpretation. An example can be seen in Fig. 2, where it is visible that CMF was used to copy a pigeon. The copied part was pasted on the image without additional transformations or adjustments, but this is not always the case. If rotation, translation, compression, etc. are applied, detection can become much more difficult, and the model must be robust enough for this.

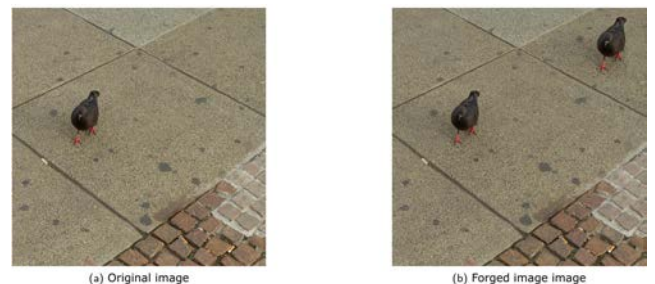


Fig. 2. A copy-move forgery example – Source [3]

The existing traditional CMFD techniques can be divided into two categories, namely a) block-based and b) keypoint-based. The difference between these two categories relies on the way they extract the feature vector which will be then fed into a classifier. Block-based methods are the most popular and widespread. These methods divide an image into several blocks (Fig. 3) or circles that can be overlapping or non-overlapping. Let I an image sized $M \times N$, which is divided into overlapping blodblocks of the image can be calculated using (1) [4].

$$\text{Total blocks} = (M - B + 1) \times (N - B + 1) \quad (1)$$

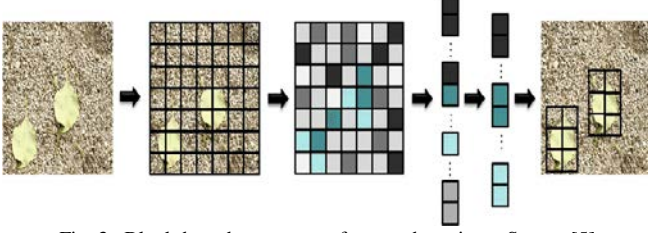


Fig. 3. Block-based copy-move forgery detection – Source [5]

Keypoint-based extract high entropy points from the image i.e., distinctive points in the image like corners and edges. A descriptor is then made of these points and their surroundings and afterwards, these points and the descriptors are compared with each other to find matches (Fig. 4).

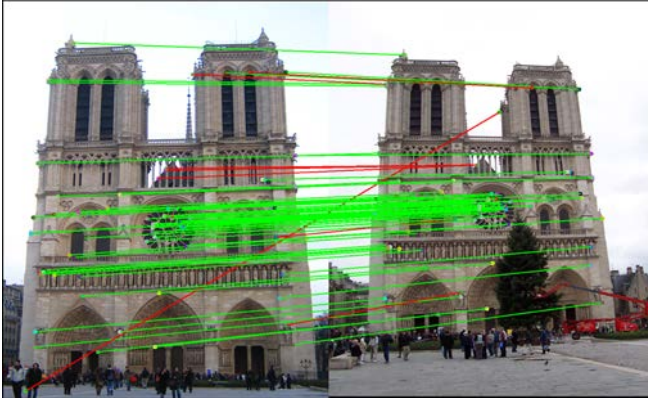


Fig. 4. Keypoint-based CMFD example – Source [6]

Keypoint-based methods are less computationally complex, fewer features are extracted and are in general more robust and reliable against transformations and noise. A problem that arises is that if parts without much texture are copied, such as the sky or a whiteboard, very few key points will be extracted from them, and the copy-move forgery detection will fail.

Recent research combines key-point methods and block-based methods, capable of detecting these smooth regions. These hybrid models can achieve very high accuracy but have the disadvantage that the complexity increases. According to Fridrich et al. [7] there are three requirements that every detection algorithm must meet:

- The detection algorithm must allow for an approximate match of small image segments.
- It must work in a reasonable time while introducing a few false positives (i.e., detecting incorrect matching areas).
- Another natural assumption that should be accepted is that the forged segment will likely be a connected

component rather than a collection of very small patches or individual pixels.

In the aforementioned conventional approaches, the most critical part is the extraction and selection of relevant features. This requires human input and intervention and mostly expertise in the field. This human-centric model can be avoided by using deep learning. Deep learning typically concerns deep neural networks that can learn directly from input data and extract complex features. The process, therefore, does not change much compared to the statistical approach, except that the feature extraction step is automated. Nevertheless, although deep learning algorithms require a huge amount of data and a long time to train a deep learning model, the running time is fast. On the contrary, statistical methods require limited data for training but they are much slower in running time. Deep learning methods were deployed for CMFD in the last decade, and therefore less research has been conducted compared to traditional methods. There are still many challenges to overcome when deploying deep learning models to CMFD [8]:

- Most deep learning models have been trained and validated with only one dataset, limiting their use to another kind of tampered images, i.e., they lack generalization.
- Most methods do not report image prediction times, and therefore it is not possible to know if they are suitable for deployment to real-time applications or massive data analysis.

Similar works have also investigated the CMFD problem. However, some are outdated and do not include state-of-the-art techniques [9], [10], or do not evaluate the presented methods by performing experiments [11], [12].

The rest of this paper is organized as follows. In Section II, various block-based methods for CMFD are described. In Section III key point-based methods are presented, while Section IV describes the most utilized deep learning algorithms for CMFD. Section V presents the experimental setup and Section VI the experimental results. Finally, in Section VII a conclusion is given.

II. BLOCK-BASED METHODS

Block-based methods can be further discriminated into various categories as shown in Fig. 5.

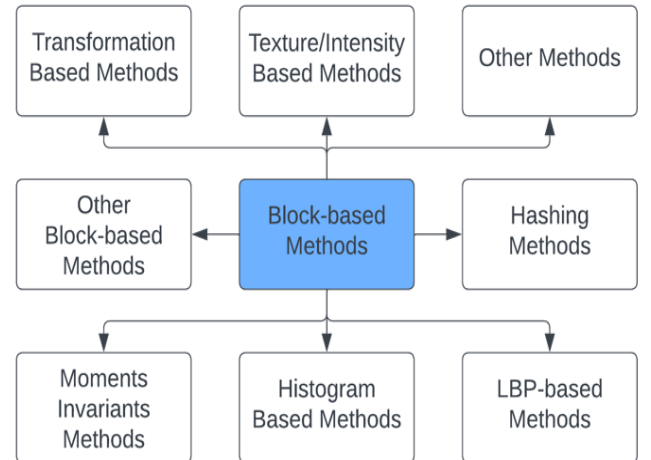


Fig. 5. Taxonomy of Block-based CMFD methods

A. Transformation-based Methods

In transformation-based techniques, a transformation is applied to convert the original image data from the spatial

domain into a different domain. Common examples of this, are the discrete cosine transform (DCT) used for compression, the Discrete Fourier Transform (DFT) used in filtering and noise removal, and the Discrete Wavelet Transform (DWT) used for data compression, denoising, and fusing images. These transformations extract useful information from the images avoiding noise and distortion.

B. Texture Intensity-based Methods

These methods extract texture and intensity values. Similar pixels can be taken together in blocks and put into a histogram. This way features can show similarities in the image, based on textures, patterns, colour information or intensity values. Due to their simplicity, these methods are considered the most straightforward methods for image feature extraction.

C. Hashing Methods

Hashing or sometimes referred to as a 'digital fingerprint' from an image is a method in which an algorithm converts the original image data to a different data type with a predetermined size, called the image hash. This image hash can be used to find duplicates very quickly and therefore it is also useful in the field of CMFD. A perceptual hashing algorithm that is robust against attacks aimed at altering the contrast ratio, luminance and hue of an image, was introduced in [13]. However, other types of attacks like rotation and scaling, on the other hand, are not handled well.

D. LBP-based Methods

Local binary pattern (LBP) is a simple statistical method for texture analysis which labels pixels by looking at the surrounding pixels. Each pixel gets a result as a binary number, and this is done for the full image. It is used in CMFD because it is robust to grey-scale changes, e.g., illumination variations, and due to its computational simplicity.

E. Histogram-based Methods

Histograms are widely used when working with digital images. Information such as gradient or colour is extracted from the image blocks and placed in a histogram for comparison with each other. A histogram of gradients (HOG) is typically utilized as a robust feature descriptor for the image blocks. These descriptors capture information about gradient and edge structure, and local contour information, making them suitable for CMFD.

Another method used -similar to HOG- is the histogram of orientated Gabor magnitude (HOGM). There are similarities to both techniques, but there are also differences in the types of features they capture and the underlying method. They both capture gradient-based information, but HOGM extends HOG by using a Gabor filter to capture texture patterns. This means that orientation information is extracted instead of only edge structure and local contour information. HOGM is applied for CMFD on different blocks in an image to extract feature vectors. These vectors are combined in a histogram and can be sorted to detect possible forgeries. Other works [14] utilize colour histograms as features. Colours are extracted from the different blocks and placed in histograms to be comparable with each other.

F. Moments Invariants Methods

Moment invariant is a technique to extract global features that are invariant to translation, scaling and rotation. These features can be used for shape classification and object recognition. The Hu moments along with DWT were utilized in [15] to detect CMF. Several copy-move areas can be discovered with this technique, even when they undergo different post-processing attacks. The initial moments like Zernike moments [16], Exponent moments [17], Krawtchouk's moments [18], and Blur invariant moments [19], have been adopted in recent proposed methods.

G. Other block-based Methods

There are many other methods found in the literature that do not belong to a specific category or are utilized rarely. An example can be found in [20]. The authors used the grey-level co-occurrence matrix (GLCM) to extract features. GLCM calculates the spatial relationship between pixels, and how often it occurs in an image, and these data are processed in a matrix. Afterwards, statistical measures were extracted from the GLCM and compared to find matches. An advantage of this method is that it is not computationally complex, making it ideal for real-time predictions.

Halftoning-based block truncation coding (HBTC) is another method used for CMFD [21]. This is a typical grayscale image compression method, but progress has been made to extend usability to CMFD.

III. KEYPOINT-BASED METHODS

The use of keypoint-based techniques is limited because not every existing technique can be applied to CMFD. There are three main factors of concern [22] which must be taken into account if a keypoint-based method is used: speed, uniqueness and robustness. SIFT [23], SURF [24] and Harris corner detection [25] are the most utilized algorithms for CMFD. SIFT is an algorithm that detects and matches local features in images. It is applicable in object recognition, 3D modelling, gesture recognition, etc. SIFT is widely used because it is highly robust against post-processing like rotation and scaling. However, the algorithm is computationally expensive, is incapable of distinguishing between regions that look naturally the same or manually modified ones, and in low-texture areas only few key points are extracted.

SURF is similar to SIFT but is faster and it reduces feature vector dimensions. SURF is unable to detect small, copied regions in an image. It improves the processing speed but can achieve less accuracy than SIFT. One of the first works that utilized SURF for CMFD was proposed by Reshma and Niya [26]. SURF keypoint descriptors were extracted and matched against each other to detect possible forgeries.

Harris corner detector is another digital image feature extractor that extracts corners and edges from images based on a local auto-correlation function (ACF). An ACF extracts and describes the spatial patterns from an image. The Harris corner detector was utilized for CMFD and proved to be more robust against scaling and rotation. The logic behind this approach lies in the observation that at a corner, the image intensity undergoes significant changes in multiple directions, whereas, at an edge, the image intensity experiences changes in a specific direction [27].

IV. DEEP LEARNING METHODS

A. Convolutional Neural Networks

More recent works use convolutional neural networks (CNN) to extract features and provide a classification for image forgery detection. CNNs have been around for a long time and are widely used in image classification [28], [29] and computer security [30]–[32].

B. Siamese Networks

A Siamese network is a neural network type that utilizes two or more identical subnetworks, that share the same architecture and weights. It can be used to learn similarities between inputs and can therefore be used in the field of CMFD. The output vectors of the networks can be compared with each other to obtain a similarity metric. Siamese networks can be applied to CMFD by measuring the similarity between image patches or regions to detect whether an image is forged or not.

C. Autoencoders

An autoencoder is a neural network mostly used for unsupervised learning. It learns to represent the input data efficiently and reconstruct it afterwards to the original input data. This type of data compression can be used to extract features from images; hence, it has been used in the field of CMFD.

D. Recurrent Neural Networks

A recurrent neural network (RNN) is a type of neural network that processes sequential data. Nodes in the network create a cycle that allows information to be looped back. It enables the network to maintain memory with captured information from previous inputs. This influences the processing of the next cycle and future inputs. Typically, they are used in conjunction with CNNs, i.e., a ConvLSTM (Convolutional – Long Short-Term Memory) for feature extraction and a CNN for CMFD. A ConvLSTM replaces the fully connected layers in an LSTM, with convolutional layers to make it more suitable for processing images. The proposed algorithm extracts image patches that are used as input for a ConvLSTM network. This network can analyze the image patch sequences and effectively detect copy-move forgeries.

E. Transfer Learning

Deep learning has shown remarkable results in almost every field and lately to CMFD. However, designing from scratch a new deep learning model and training it, requires expertise, time, computational power and a huge amount of data. Pre-trained models are lately widely used and show very good results when available data are limited. Moreover, much less time computational power is needed to train them. VGG16 [33] and Mobile Net [34] are the most used models for CMFD.

V. EXPERIMENTAL SETUP

A. Datasets

Six different publicly available datasets have been used to the experiments. These contain MICC-F2000 [35], MICC-F220 [35], CoMoFoD [3], CASIAv1 [36], CASIAv2 [36] and GRIP [37]. The class distribution for each one of these datasets can be found in Table 1. The UNIFIED dataset is a combination of the six datasets.

Table 1. Dataset distribution

Dataset	Total Images	Genuine Images	Forged Images
MICC-F2000	2000	1300	700
MICC-F220	220	110	110
CoMoFoD	399	200	199
CASIAv1	1250	800	450
CASIAv2	10786	7491	3295
GRIP	80	0	80
UNIFIED	14735	9901	4834

Typically, in literature, only one dataset or several datasets of the same family are used (e.g., MICC-F2000 and MICC-F220). As a result, the proposed model cannot generalize and will not perform well on other unseen data.

B. Methodology

To evaluate the effectiveness of the aforementioned methods, various experiments were conducted. More specifically, a pre-trained CNN namely, the VGG16 was utilized along with the statistical method SIFT for comparison. Initially, the SIFT method and the transfer learning method were applied to each one of the datasets mentioned in section A (Datasets). Afterwards, a new experiment has been made utilizing a new unified dataset which comprised the six datasets utilized in the first experiment. Class distribution (Table 1) shows that there are more genuine images than forged ones. This class imbalance could lead to a biased model and performance issues for the minority class. This problem was solved by setting different weights for each class to penalize misclassification in the minority class. Equations (2), and (3) explain how the weights are calculated per class. They return 0.0001 for the original class weight and 0.0002 for the forged class weight respectively.

$$\text{Original class weight} = \frac{1}{\text{Original class count}} \quad (2)$$

$$\text{Forged class weight} = \frac{1}{\text{Forged class count}} \quad (3)$$

C. Evaluation Metrics

In order to calculate the effectiveness of the examined methods, commonly used metrics in CMFD such as True Positive Ratio (TPR), False Positive Ratio (FPR), Precision, Recall and F1-score were utilized. The calculation for these metrics is presented in Equations 4-8.

$$\text{TPR} = \frac{\# \text{ of images correctly classified as forged}}{\# \text{ of forged images}} \quad (4)$$

$$\text{FPR} = \frac{\# \text{ of images incorrectly classified as forged}}{\# \text{ of original images}} \quad (5)$$

$$\text{Precision} = \frac{\text{Forged region} \cap \text{Detected region}}{\text{Detected region}} \quad (6)$$

$$\text{Precision} = \frac{\text{Forged region} \cap \text{Detected region}}{\text{Forged region}} \quad (7)$$

$$\text{F1 - score} = 2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}} \quad (8)$$

D. Pre-trained Model

The VGG-16 model was chosen for the experiments. VGG16 can classify images into 1000 different object classes. It consists of 16 layers in total, comprising of 13 convolutional layers followed by 3 fully connected layers. Small 3x3 convolutional filters are used in each convolutional layer

followed by ReLU activation function, and 2x2 max-pooling layers interspersed throughout the network. Those max-pooling layers in the network are used to downsample the feature maps from the previous layers. The classification is performed in the three fully connected layers, and finally a softmax layer produces a probability distribution over the different classes. To adapt this model to binary classification (forged or original) the last layer was adjusted to have only 1 or 2 output neurons. The original fully connected layers from VGG-16 were removed and a new classification layer was added. This layer consists of 2 fully connected layers with a dropout layer in between -with a dropout rate of 0.5- to prevent overfitting. The last layer comprises of two output units which represent the probability to which class an image belongs.

A batch size of 40 was used for the training set and 20 for the test set. The learning rate was set to 0.0001 and the total number of epochs was set to 200. Early stopping was used to prevent overfitting, by stopping the training process when there was no further improvement after 6 epochs. The stochastic gradient descent (SGD) optimizer was used, with a momentum of 0.9. The momentum speeds up the training process by pushing the gradient vectors in the right direction. As a result, the model converges more quickly. Finally, the training time for each VGG-16 model was tracked and the data were split into a training (80%) and validation set (20%).

E. Software - Hardware

The copy-move forgery detection algorithms were implemented using Python and the PyTorch deep learning framework. The training was performed on an Intel Xeon E5-2680 v4, with 32GB system RAM and two GeForce GTX 1080 Ti working in parallel.

VI. EXPERIMENTAL RESULTS

A. First Experiment

During the first experiment, both the transfer learning method and the SIFT algorithm were trained on each one of the six datasets. The obtained results are shown in Tables 2-6.

Table 2. MICC-F2000

Model	F1-score	Precision	Recall	Accuracy	Training Time
SIFT	0.580	0.424	0.919	0.534	-
VGG-16	0.981	1.000	0.962	0.980	8.9h

Table 3. MICC-F220

Model	F1-score	Precision	Recall	Accuracy	Training Time
SIFT	0.612	0.646	0.581	0.632	-
VGG-16	1.000	1.000	1.000	1.000	0.15h

Table 4. CoMoFoD

Model	F1-score	Precision	Recall	Accuracy	Training Time
SIFT	0.716	0.699	0.734	0.709	-
VGG-16	0.833	0.761	0.921	0.830	0.3h

Table 5. CASIAv1

Model	F1-score	Precision	Recall	Accuracy	Training Time
SIFT	0.777	0.898	0.684	0.858	-
VGG-16	0.722	0.784	0.669	0.664	0.08h

Table 6. CASIAv2

Model	F1-score	Precision	Recall	Accuracy	Training Time
SIFT	0.555	0.762	0.436	0.786	-
VGG-16	0.758	0.787	0.731	0.672	0.53h

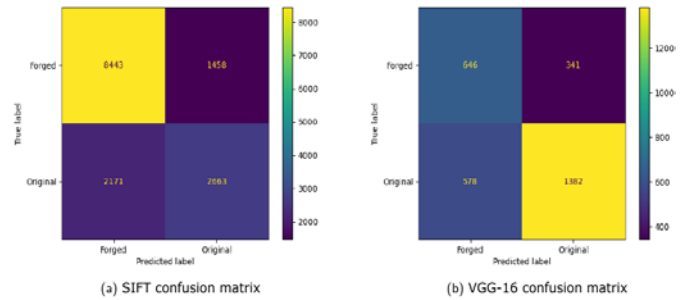
The experimental results reveal that the VGG-16 transfer learning method achieves the best performance in most cases. Only with CASIAv1 and CASIAv2, there was a problem where the validation loss did not decrease. By experimenting on these two datasets alone, and lowering the learning rate to 0.00001, the validation loss decreased and achieved an F1-score of 0.744.

B. Second Experiment

In this experiment, all datasets were combined in order to make the model more robust and generalize better to unseen data. Thus, 14735 images were used in total, from which 9901 were genuine and 4834 forged. The hyperparameters used for training have remained the same as in the first experiment, except for the learning rate that was set to 0.00001 and the train/test batch sizes that were changed to 64/32 respectively. SIFT was again used as the conventional method for comparison. The obtained results can be found in Table 7 and Fig. 6. It can be seen that again the VGG-16 model has achieved a higher F1-score, precision and recall.

Table 7. Unified dataset

Model	F1-score	Precision	Recall	Accuracy	Training Time
SIFT	0.595	0.646	0.551	0.754	-
VGG-16	0.750	0.802	0.705	0.688	0.53h



(a) SIFT confusion matrix

(b) VGG-16 confusion matrix



(c) VGG-16 loss graph

Fig. 6. Results on the unified dataset.

C. Discussion

The obtained results confirmed our expectations. Deep learning has overperformed classical approaches like the SIFT method. However, in some cases when the VGG16 was trained with CASIAv1 & CASIAv2, the validation loss did not decrease. Moreover, although the results were better than the ones obtained from the SIFT method, they cannot not be considered as excellent and there is room for improvement. These improvements may consider a) the utilization of more data. This highlights the gap that exists to available public datasets. As reported in Table 1, the number of available images per dataset is small –especially for deep learning methods- and there is also a class imbalance. b) the use of another pre-trained model c) experimentation of fine-tuning the model.

VII. CONCLUSION

Copy-move forgery is a popular tampering technique that involves copying and pasting a certain area of an image, within the same image. In this paper we presented the most utilized conventional and deep learning methods, to gain a better insight into different possible CMFD techniques. Moreover, various experiments were conducted to examine and compare the efficiency of the presented methods. A transfer learning method, namely the VGG-16 model was compared against the statistical method SIFT. To make the model more robust and generalize better, six different publicly available datasets were utilized. The obtained results showed that although the SIFT methods performed well, the deep learning approach behaved better. The expectations for the performance of deep learning were slightly higher than the achieved results but further research and experimentation like fine-tuning the pre-trained model, can provide better results. In the future we plan to examine more pre-trained deep learning models and compare their accuracy. However, the examined deep learning model can certainly be utilized as a basis for further research and as a valuable tool in image forensics.

REFERENCES

- [1] K. Karampidis, E. Kavallieratou, and G. Papadourakis, "A review of image steganalysis techniques for digital forensics," *Journal of Information Security and Applications*, vol. 40, pp. 217–235, Jun. 2018, doi: 10.1016/J.JISA.2018.04.005.
- [2] K. Karampidis, G. Papadourakis, and I. Deligiannis, "File Type Identification -A Literature Review," in *9th International Conference on New Horizons in Industry Business and Education, NHIBE 2015*, Skiathos, Greece: 9th International Conference on New Horizons in Industry Business and Education, 2015, p. 141. [Online]. Available: [http://nhibe2015.vsn-net.eu/proceedings/papers/3_15_\[P\]0076.pdf](http://nhibe2015.vsn-net.eu/proceedings/papers/3_15_[P]0076.pdf)
- [3] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, "CoMoFoD — New database for copy-move forgery detection," in *Proceedings ELMAR*, 2013, pp. 49–54. Accessed: Aug. 19, 2023. [Online]. Available: <https://ieeexplore.ieee.org/document/6658316>
- [4] T. Mahmood, T. Nawaz, A. Irtaza, R. Ashraf, M. Shah, and M. T. Mahmood, "Copy-Move Forgery Detection Technique for Forensic Analysis in Digital Images," *Math Probl Eng*, vol. 2016, p. 8713202, 2016, doi: 10.1155/2016/8713202.
- [5] D. Tralic, P. L. Rosin, X. Sun, and S. Grgic, "Copy-Move Forgery Detection Using Cellular Automata," pp. 105–125, 2014, doi: 10.1007/978-3-319-06431-4_6.
- [6] "GitHub - deepanshut041/feature-detection: Oriented FAST and Rotated BRIEF using opencv." <https://github.com/deepanshut041/feature-detection> (accessed Aug. 19, 2023).
- [7] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy-move forgery in digital images," in *Proceedings of digital forensic research workshop*, 2003, pp. 652–663.
- [8] Y. Rodriguez-Ortega, D. M. Ballesteros, and D. Renza, "Copy-Move Forgery Detection (CMFD) Using Deep Learning for Image and Video Forensics," *Journal of Imaging* 2021, Vol. 7, Page 59, vol. 7, no. 3, p. 59, Mar. 2021, doi: 10.3390/JIMAGING7030059.
- [9] N. B. A. Warif *et al.*, "Copy-move forgery detection: Survey, challenges and future directions," *Journal of Network and Computer Applications*, vol. 75, pp. 259–278, Nov. 2016, doi: 10.1016/J.JNCA.2016.09.008.
- [10] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1841–1854, 2012, doi: 10.1109/TIFS.2012.2218597.
- [11] J. Malathi *et al.*, "A Review on Copy-Move Image Forgery Detection Techniques," *J Phys Conf Ser*, vol. 1892, no. 1, p. 012010, Apr. 2021, doi: 10.1088/1742-6596/1892/1/012010.
- [12] S. Teerakanok and T. Uehara, "Copy-Move Forgery Detection: A State-of-the-Art Technical Review and Analysis," *IEEE Access*, vol. 7, pp. 40550–40568, 2019, doi: 10.1109/ACCESS.2019.2907316.
- [13] H. Wang and H. Wang, "Perceptual Hashing-Based Image Copy-Move Forgery Detection," *Security and Communication Networks*, vol. 2018, p. 6853696, 2018, doi: 10.1155/2018/6853696.
- [14] H. Zhou, Y. Shen, X. Zhu, B. Liu, Z. Fu, and N. Fan, "Digital image modification detection using color information and its histograms," *Forensic Sci Int*, vol. 266, pp. 379–388, Sep. 2016, doi: 10.1016/J.FORSCIINT.2016.06.005.
- [15] T. Mahmood, T. Nawaz, M. Shah, Z. Khan, R. Ashraf, and H. A. Habib, "Copy-move forgery detection technique based on DWT and Hu Moments," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 14, no. 5, pp. 156–161, 2016.
- [16] A. Khotanzad and Y. H. Hong, "Invariant Image Recognition by Zernike Moments," *IEEE Trans Pattern Anal Mach Intell*, vol. 12, no. 5, pp. 489–497, 1990, doi: 10.1109/34.55109.
- [17] X. yang Wang, Y. nan Liu, H. Xu, P. Wang, and H. ying Yang, "Robust copy-move forgery detection using quaternion exponent moments," *Pattern Analysis and Applications*, vol. 21, no. 2, pp. 451–467, May 2018, doi: 10.1007/S10044-016-0588-1/FIGURES/8.
- [18] P. T. Yap, R. Paramesran, and S. H. Ong, "Image analysis by Krawtchouk moments," *IEEE Transactions on Image Processing*, vol. 12, no. 11, pp. 1367–1377, Nov. 2003, doi: 10.1109/TIP.2003.818019.
- [19] B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants," *Forensic Sci Int*, vol. 171, no. 2–3, pp. 180–189, Sep. 2007, doi: 10.1016/J.FORSCIINT.2006.11.002.
- [20] P. Mohanaiah, P. Sathyanarayana, and L. Guru Kumar, "Image texture feature extraction using GLCM approach," *International journal of scientific and research publications*, vol. 3, no. 5, pp. 1–5, 2013.
- [21] J. M. Guo and H. Prasetyo, "Content-based image retrieval using features extracted from halftoning-based block truncation coding," *IEEE Transactions on Image Processing*, vol. 24, no. 3, pp. 1010–1024, Mar. 2015, doi: 10.1109/TIP.2014.2372619.
- [22] S. Teerakanok and T. Uehara, "Copy-Move Forgery Detection: A State-of-the-Art Technical Review and Analysis," *IEEE Access*, vol. 7, pp. 40550–40568, 2019, doi: 10.1109/ACCESS.2019.2907316.
- [23] D. G. Lowe, "Object recognition from local scale-invariant features," *Proceedings of the IEEE International Conference on Computer Vision*, vol. 2, pp. 1150–1157, 1999, doi: 10.1109/ICCV.1999.790410.
- [24] H. Bay, T. Tuytelaars, and L. Van Gool, "SURF: Speeded up robust features," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Springer, Berlin, Heidelberg, 2006, pp. 404–417. doi: 10.1007/11744023_32.
- [25] C. Harris and M. Stephens, "A combined corner and edge detector," in *Alvey vision conference*, Aug. 1988.
- [26] R. Raj and N. Joseph, "Keypoint Extraction Using SURF Algorithm for CMFD," *Procedia Comput Sci*, vol. 93, pp. 375–381, Jan. 2016, doi: 10.1016/J.PROCS.2016.07.223.

- [27] L. Chen, W. Lu, J. Ni, W. Sun, and J. Huang, "Region duplication detection based on Harris corner points and step sector statistics," *J Vis Commun Image Represent*, vol. 24, no. 3, pp. 244–254, Apr. 2013, doi: 10.1016/J.JVCIR.2013.01.008.
- [28] K. Karampidis and G. Papadourakis, "File type identification for digital forensics," in *Advanced Information Systems Engineering Workshops. CAiSE 2016. Lecture Notes in Business Information Processing*, S. J. Krogstie J., Mouratidis H., Ed., Springer, Cham, 2016, pp. 266–274. doi: 10.1007/978-3-319-39564-7_25.
- [29] K. Karampidis, E. Linardos, and E. Kavallieratou, "StegoPass – Utilization of Steganography to Produce a Novel Unbreakable Biometric Based Password Authentication Scheme," in *14th International Conference on Computational Intelligence in Security for Information Systems and 12th International Conference on European Transnational Educational (CISIS 2021 and ICEUTE 2021)*, Springer, Cham, Sep. 2022, pp. 146–155. doi: 10.1007/978-3-030-87872-6_15.
- [30] K. Karampidis, M. Rousoulitis, and E. Kavallieratou, "A comprehensive survey on fingerprint presentation attack detection," *Journal of Surveillance, Security and Safety*, no. under review, 2021.
- [31] K. Karampidis, E. Kavallieratou, and G. Papadourakis, "A Dilated Convolutional Neural Network as Feature Selector for Spatial Image Steganalysis – A Hybrid Classification Scheme," *Pattern Recognition and Image Analysis*, vol. 30, no. 3, pp. 342–358, Jul. 2020, doi: 10.1134/S1054661820030098.
- [32] K. Karampidis, N. Vasillopoulos, C. Cuevas, C. Roberto Del-Blanco, E. Kavallieratou, and N. Garcia, "Overview of the ImageCLEFsecurity 2019: File Forgery Detection Tasks *," in *CLEF Working Notes*, 2019.
- [33] K. Simonyan and A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Image Recognition," in *3rd International Conference on Learning Representations, ICLR 2015 - Conference Track Proceedings*, International Conference on Learning Representations, ICLR, Sep. 2014. Accessed: Aug. 19, 2023. [Online]. Available: <https://arxiv.org/abs/1409.1556v6>
- [34] A. G. Howard *et al.*, "MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications," Apr. 2017, Accessed: Aug. 19, 2023. [Online]. Available: <https://arxiv.org/abs/1704.04861v1>
- [35] "Copy-Move Forgery Detection and Localization | Image and Communication Laboratory." <http://ici.micc.unifi.it/labd/2015/01/copy-move-forgery-detection-and-localization/> (accessed Aug. 19, 2023).
- [36] J. Dong, W. Wang, and T. Tan, "CASIA image tampering detection evaluation database," in *2013 IEEE China Summit and International Conference on Signal and Information Processing, ChinaSIP 2013 - Proceedings*, 2013, pp. 422–426. doi: 10.1109/CHINASIP.2013.6625374.
- [37] D. Cozzolino, G. Poggi, and L. Verdoliva, "Efficient Dense-Field Copy-Move Forgery Detection," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2284–2297, Nov. 2015, doi: 10.1109/TIFS.2015.2455334.

Anonymization, Hashing and Data Encryption Techniques: A Comparative Case Study

Marios Vardalachakis¹, Manolis Tampouratzis¹, Haridimos Kondylakis¹, Nikolaos Papadakis¹, Nikos Mastorakis²

¹*Department of Electrical and Computer Engineering (ECE), Hellenic Mediterranean University (HMU)
Heraklion, GR 71004 Greece, (mtp237@edu.hmu.gr, tampouratzis@hmu.gr, kondylak@hmu.gr, npapadak@hmu.gr)*

²*Technical University of Sofia, Sofia, Bulgaria and Hellenic Naval Academy
Piraeus, GR 18539 Greece, (mastor@hna.gr)*

Abstract—The Confidentiality of Personal Data has proven to be an important concern for both individuals and organizations around the world in the present day. As a result of rising numbers of security incidents, computer hacking and illicit utilization of personal data effective techniques for preserving the confidentiality of personal data are becoming increasingly important. Three frequently implemented techniques in maintaining data privacy: Anonymization, Hashing and Data Encryption have gained in popularity as time passed. But in general, the right choice of technique relies on the particular application and the necessary degree of integrity and confidentiality of data. In this study, a detailed examination of several anonymization, hashing, and encryption techniques are described. Each technique's strengths and weaknesses will be addressed, as well as recommendations and best practices when using each technique in a variety of situations, based on experimental healthcare data.

Keywords—Personal Data, Data Privacy, Data Anonymization, Hashing, Encryption.

I. INTRODUCTION

In today's technological world, data privacy remains a big issue for individuals and organizations worldwide. Since we keep depending to rely on technology for the preservation and analysis of enormous amounts of data [1], there will be a growing desire for protecting important data in opposition to illicit use and fraud. Several data privacy practices including encryption, hashing and anonymization have been established to try and solve this problem. Since these practices are often utilized when protecting valuable data and it is vital to be conscious of both the benefits and drawbacks they offer. Also, in the age of digital technology data privacy is vital to support a variety of causes. First of all, there are plenty of possibilities personal information might be exploited notably for individual marketing, evaluation of credit and as well as career testing [2]. People may face significant consequences caused by this when actions concerning daily life are sometimes carried out with their data despite their permission or understanding. Furthermore, hacking activities are an increasing concern [3]. These kinds of activities may correspond to the manipulation of personal information, especially banking information, social security numbers and as well as additional information. This could end up in negative publicity, fraud and various other forms of illicit activity. Lastly, the maintenance of free speech alongside other basic privileges relies on data privacy [4].

The idea of this work is to offer an in-depth evaluation of all three data privacy practices and their practical implications behind them. We will look at the benefits and drawbacks of each technique along with a number of its real-life uses, and present tips on selecting the most suitable approach according to specific usage scenarios. It also

shows that several kinds of data privacy techniques comprising anonymization, encryption and hashing techniques have been implemented and this work will be fully investigated in the above study.

Regardless of the similarities between them, they range seriously in how they work and the degree of protection. We will take a look at the distinct characteristics of each of these approaches in this comparative review. The accurate scenario and the degree of security define what type of strategy needs to be utilized. In several instances when a small quantity of data must be exchanged, Anonymization may be suitable. In other instances, encryption might need to be utilized to secure highly confidential information. On the other hand, how encryption handles protecting information about credit cards or medical documents, and hashing might help secure passwords. Although the similarities they seem to share, they are vastly distinct in their functionality and degree of security. While they may seem similar, they have distinct differences in how they work and the level of security they provide. In this comparative review, we will examine the differences between these techniques based on experimental healthcare data. The distinctions among the above approaches will be addressed in this comparative examination.

A. Anonymization

Anonymization is a widely used technique that involves removing Personally Identifiable Information (PII) from a dataset while maintaining its analytical value [5]. The objective of anonymization is to protect individual privacy while still allowing data to be used for research purposes [6]. However, achieving perfect anonymity is challenging due to the risk of re-identification attacks [7]. Therefore, various anonymization techniques have been developed, such as masking, generalization, and perturbation, which we will explore in detail in this study.

B Hashing

Another method for transforming data into a fixed-length string of letters is known as a hash. Since the hash function only works in one direction, it is not possible to reconstruct the original data from the hash. Data storage and transfer frequently employ hashing to ensure data integrity and find any unwanted changes [8]. However, selecting the right hash algorithm is essential to ensuring data security.

C. Encryption

Data may be put into an anonymous form via encryption, which is accessible only with a key or password. The two primary sorts of encryption are symmetric and asymmetric, each having certain benefits and drawbacks [9]. We'll walk through the issues of controlling keys as well as safe key

storage as we thoroughly look at different encryption methods. This study highlights the significance of data privacy and the value of preserving confidential data towards eavesdropping and online risks. The knowledge gained collected from the current research is intended to assist people and businesses and figure out options concerning how to protect their data and minimize the risks of threats to society and data violations

II. BACKGROUND OF ANONYMIZATION TECHNIQUES

By deleting or obscuring Personally Identifying Information (PII), Anonymization techniques are employed for protecting people's privacy and confidentiality in datasets. The idea is to modify the data while maintaining its analysis and research value in an approach which makes it hard or impossible to determine certain individuals. Four main privacy-preserving techniques have been established for Anonymization: Suppression, which replaces a quality value with the special symbol "*", Removing Information, in which a quality value is replaced with a sequence of numbers that range for example from 1 to 469 (total number of observations), Generalization this technique replaces quality values with semantically unvarying less special values hiding the details of the attribute and Bottom Coding, which is an exposure constraint technique that includes limiting the minimum worth of a variable allowed on the file to prevent exposure of individuals or other units with extreme values in a delivery [10].

A. Suppression

It wipes out a record totally from a dataset by applying that approach [11]. When a characteristic is not valuable or critical to analysis, or when there are no additional options to anonymize it, this ought to occur. The dataset for this approach was implemented to analyze Electronic Health Records (EHRs) and has three attributes: the "PatientID", the "PatientGender", and the "PatientRace". Figure 1 shows an example of the original dataset.

PatientID	PatientGender	PatientRace
FB2ABB23-C9D0-4D09-8464-49BF0B982F0F	MALE	UNKOWN
64182B95-EB72-4E2B-BE77-8050B71498CE	MALE	AFRICAN AMERICAN
DB22A4D9-7E4D-485C-916A-9CD1386507FB	FEMALE	ASIAN
6E70-D84D-C75F-477C-BC37-9177C3698C66	MALE	WHITE

Fig.1.Suppression - Original Dataset.

To Anonymize the data, the characteristic "PatientRace" has replaced the whole values with the special symbol "*". After suppressing the "PatientRace" Characteristic:

PatientID	PatientGender	PatientRace
FB2ABB23-C9D0-4D09-8464-49BF0B982F0F	MALE	*
64182B95-EB72-4E2B-BE77-8050B71498CE	MALE	*
DB22A4D9-7E4D-485C-916A-9CD1386507FB	FEMALE	*
6E70-D84D-C75F-477C-BC37-9177C3698C66	MALE	*

Fig. 2. Suppression - Anonymized Dataset.

B. Removing Information

In this approach when determined content is taken away it always additionally departs behind related information that can be beneficial for the examiner [12]. The dataset below has four attributes: the "PatientID", the "PatientGender", the "PatientRace" and the "PatientMaritalStatus". In our approach, Figure 3 shows an example of the original dataset.

PatientID	PatientGender	PatientRace	PatientMaritalStatus
FB2ABB23-C9D0-4D09-8464-49BF0B982F0F	MALE	UNKNOWN	Married
64182B95-EB72-4E2B-BE77-8050B71498CE	MALE	AFRICAN AMERICAN	Separated
DB22A4D9-7E4D-485C-916A-9CD1386507FB	FEMALE	ASIAN	Married
6E70-D84D-C75F-477C-BC37-9177C3698C66	MALE	WHITE	Married

Fig.3. Removing Information - Original Dataset.

To Anonymize the data, the characteristic "PatientGender" has replaced the whole values with Random numbers. After removing Information from the "PatientGender" Characteristic:

PatientID	PatientGender	PatientRace	PatientMaritalStatus
FB2ABB23-C9D0-4D09-8464-49BF0B982F0F	127	UNKNOWN	Married
64182B95-EB72-4E2B-BE77-8050B71498CE	225	AFRICAN AMERICAN	Separated
DB22A4D9-7E4D-485C-916A-9CD1386507FB	315	ASIAN	Married
6E70-D84D-C75F-477C-BC37-9177C3698C66	1/0	WHITE	Married

Fig. 4. Removing Information - Anonymized Dataset.

C. Generalization

A generalization is a different approach that is utilized to swap unique values with more broad or generalized representations of values to avoid exposing important information and trying to guarantee which individuals are unable to instantly recognize right away from the transformed data [13]. The dataset below has four attributes: the "PatientID", the "PatientGender", the "PatientRace" and the "PatientMaritalStatus". Our approach in Figure 5 shows an example of the original dataset:

PatientID	PatientGender	PatientRace	PatientMaritalStatus
FB2ABB23-C9D0-4D09-8464-49BF0B982F0F	MALE	UNKNOWN	Married
64182B95-EB72-4E2B-BE77-8050B71498CE	MALE	AFRICAN AMERICAN	Separated
DB22A4D9-7E4D-485C-916A-9CD1386507FB	FEMALE	ASIAN	Married
6E70-D84D-C75F-477C-BC37-9177C3698C66	MALE	WHITE	Married

Fig. 5. Generalization - Original Dataset.

After applying the generalization algorithm from the "PatientMaritalStatus" Characteristic:

PatientID	PatientGender	PatientRace	PatientMaritalStatus
FB2ABB23-C9D0-4D09-8464-49BF0B982F0F	MALE	UNKNOWN	2
64182B95-EB72-4E2B-BE77-8050B71498CE	MALE	AFRICAN AMERICAN	2
DB22A4D9-7E4D-485C-916A-9CD1386507FB	FEMALE	ASIAN	2
6E70-D84D-C75F-477C-BC37-9177C3698C66	MALE	WHITE	2

Fig. 6. Generalizations - Anonymized Dataset.

D. Bottom Coding

By grouping or classifying specific characteristics or attributes Bottom Coding in data Anonymization describes an approach to reducing the amount of information or specificity in a dataset [14]. It is an approach that is frequently implemented to guarantying respect for the confidentiality and privacy of certain individuals or important information in a dataset while still allowing evaluation and examination The dataset below has five attributes: "PatientID", "PatientGender", "PatientRace", "PatientMaritalStatus" and "PatientLanguage". In our approach, Figure 7 shows an example of the original dataset.

PatientID	PatientGender	PatientRace	PatientMaritalStatus	PatientLanguage
FB2ABB23-C9D0-4D09-8464-49BF0B982F0F	MALE	UNKNOWN	2	ISLANDIC
64182B95-EB72-4E2B-BE77-8050B71498CE	MALE	AFRICAN AMERICAN	2	ENGLISH
DB22A4D9-7E4D-485C-916A-9CD1386507FB	FEMALE	ASIAN	2	ENGLISH
6E70-D84D-C75F-477C-BC37-9177C3698C66	MALE	WHITE	2	ENGLISH

Fig. 7. Bottom Coding - Original Dataset.

After applying the Bottom Coding Technique in the "PatientLanguage" Characteristic:

PatientID	PatientGender	PatientRace	PatientMarital Status	PatientLanguage
FB2ABB23-C9D0-4D09-8464-49BF0B982F0F	MALE	UNKNOWN	2	45000
64182B95-E872-4E2B-BE77-8050B71498CE	MALE	AFRICAN AMERICAN	2	45000
DB22A4D9-7E4D-485C-916A-9CD1386507FB	FEMALE	ASIAN	2	45000
6E70-D84D-C75F-477C-BC37-9177C3698C66	MALE	WHITE	2	45000

Fig. 8. Bottom Coding - Anonymized Dataset.

III. BACKGROUND OF HASHING TECHNIQUES

Although Anonymization and Hashing perform distinct processes, they can be integrated into particular circumstances to enhance privacy and security. In several circumstances instead of utilizing Anonymization, Hashing may occasionally be utilized for extra defense. It's extremely important to keep in mind that hashing cannot provide a similar degree of privacy protection as anonymization on a separate basis. Although knowing that hashing makes it unable to retrieve the initial data from the hash value, it continues to be practicable to seek comparable input data via brute-force or dictionary attacks. Hashing is mainly utilized for multiple protection measures, reliability of data examinations, and storing passwords. By changing important details with immutable hash values, hashing can potentially be used to mask data in the context of data privacy. Four main Hashing Techniques have been established for this research: MD5, which is a famous cryptographic hash approach known as MD5 (Message-Digest Algorithm). A fixed-size (128-bit) hash value comes with the given input (message), which is often a 32-character hexadecimal integer, SHA512 which is a cryptographic hash function that is an integral part of the SHA-2 family of mathematical algorithms and it produces a fixed-size (512 bit) hash value utilizing an input (message) and considered as a secure hash algorithm, CRC32 which it is a hash function that recognizes a message as its input and returns a fixed- size (32-bit) hash result, XXhash64 which a 64-bit hash value has been generated by the hash function and it is famous for being fast and memory - efficient.

A. MD5

The MD5 hashing algorithm is a standard cryptographic approach which it processes a given input (generally a message or a collection of data) and generates a fixed-size 128-bit hash value as well which is frequently displayed as a 32-a character hexadecimal integer [15]. The table in Figure 9 is an example of the MD5 Algorithm. The dataset in this table has three attributes: the "PatientID", the "PatientGender" and the "PatientRace".

PatientID	PatientGender	PatientRace
FB2ABB23-C9D0-4D09-8464-49BF0B982F0F	MALE	UNKNOWN
64182B95-E872-4E2B-BE77-8050B71498CE	MALE	AFRICAN AMERICAN
DB22A4D9-7E4D-485C-916A-9CD1386507FB	FEMALE	ASIAN
6E70-D84D-C75F-477C-BC37-9177C3698C66	MALE	WHITE

Fig. 9. MD5 Algorithm - Original Dataset.

After applying the MD5 Algorithm in the "PatientGender" Characteristic:

PatientID	PatientGender	PatientRace
FB2ABB23-C9D0-4D09-8464-49BF0B982F0F	NK7Zv1jpUjVhQ	UNKNOWN
64182B95-E872-4E2B-BE77-8050B71498CE	fTb.R0bQ7rQ5I	AFRICAN AMERICAN
DB22A4D9-7E4D-485C-916A-9CD1386507FB	IZIE7Yv4Unikk	ASIAN
6E70-D84D-C75F-477C-BC37-9177C3698C66	Cdoqj2nFDB7qg	WHITE

Fig.10. MD5 Algorithm - Anonymized Dataset.

B. SHA512

The SHA512 algorithm is a secure hash function that is a part of the SHA-2 category. For every element of input data, it is meant to generate a fixed-size hash value of 512 bits in length (64 bits). Although provided a transmitted message or data of random measurement, hash algorithms like SHA-512 establish a fixed-size hash result from this. As the hash algorithm is dependent on the given data, any slight modification will result in a significantly varied hash value. SHA-512 makes use of a sort of compression process which repeatedly compresses the original data in groups of 1024 bits and acts on 64-bit bits. The initial data is split up into blocks of information, and the ultimate hash algorithm produces itself by parsing and aggregating each block repeatedly [16]. The table in Figure 11 is an example of the SHA512 Algorithm.

PatientID	PatientGender	PatientRace	PatientMaritalStatus	PatientLanguage
FB2ABB23-C9D0-4D09-8464-49BF0B982F0F	MALE	UNKNOWN	2	45000
64182B95-E872-4E2B-BE77-8050B71498CE	MALE	African American	2	45000
DB22A4D9-7E4D-485C-916A-9CD1386507FB	FEMALE	ASIAN	2	45000
6E70-D84D-C75F-477C-BC37-9177C3698C66	MALE	White	2	45000

Fig. 11. SHA512 Algorithm - Original Dataset.

After applying the SHA512 Algorithm in the PatientRace Characteristic

PatientID	PatientGender	PatientRace	PatientMarital Status	PatientLanguage
FB2ABB23-C9D0-4D09-8464-49BF0B982F0F	MALE	b90e54bb3e16afad4D67b7777163 87559083b84a3a794788f824cd4d8 08fa376Df9d6f7d39673b1779868e bd4f76f628f8e76101256a71476fe5 a5587bb3c22	Married	Icelandic
64182B95-E872-4E2B-BE77-8050B71498CE	MALE	C10988cf79f1174893cf32c9c5266 fb9a4984b05bb24170d50293262cf db62be73b2994a87dc705548a723 67bb04b2937e382a5ec743a9037 5da30a0eef56de	Separated	English
DB22A4D9-7E4D-485C-916A-9CD1386507FB	FEMALE	C33ea9d0ba47653638e278a8d3ca b5856c064a148112d3776b55be58 95b5cb17f6bfcd709e989f32b245 eca33640f2ecf857253d09b4ece80 7884f8ae35c051	Married	English
6E70-D84D-C75F-477C-BC37-9177C3698C66	MALE	7181b5993a52c854f72a475aad503 62a3076e028b9739d5104cf8180d7 cc5df6431a1ef6fdb8abee1f2e6b4ce f4be45b8301abf7106af8f01e6eb86 7143038076	Married	English

Fig. 12. SHA512 Algorithm - Anonymized Dataset.

C. CRC32

A famous hash algorithm strategy called CRC32 (Cyclic Redundancy Check 32-bit) is utilized primarily for identifying errors within electronic data transfers and storage facilities. Considering an identified number of inputs, it generates a 32-bit hash value, and that can often be expressed as a hexadecimal or decimal integer. During

operation, CRC32 separates the data that arrives into equations after analyzing the information as a sequence of bits. The checksum is created utilizing an identified polynomial (generally an IEEE 802.3 polynomial, that has a binary code of 0x04C11DB7). The data that is received is analyzed bit by bit, and the polynomial is utilized to split every single bit. After each of the bits in the information that was provided have been analyzed the above process will continue. The CRC32 hashed value is an outcome of the division of polynomials [17]. The table in Figure 13 is an example of the CRC32 Algorithm.

PatientID	PatientGender	PatientRace	PatientMaritalStatus	PatientLanguage
FB2AB823-C9D0-4D09-8464-49BF0B982F0F	MALE	UNKNOWN	Married	Icelandic
64182895-E872-4E2B-BE77-8050B71498CE	MALE	African American	Separated	English
DB22A4D9-7E4D-485C-916A-9CD1386507FB	FEMALE	ASIAN	Married	English
6E70-D84D-C75F-477C-BC37-9177C3698C66	MALE	White	Married	English

Fig. 13. CRC32 Algorithm - Original Dataset.

After Applying the CRC32 Algorithm in the "PatientMaritalStatus" Characteristic:

PatientID	PatientGender	PatientRace	PatientMaritalStatus	PatientLanguage
FB2AB823-C9D0-4D09-8464-49BF0B982F0F	MALE	UNKNOWN	03cd7b91	Icelandic
64182895-E872-4E2B-BE77-8050B71498CE	MALE	African American	D4296c/c	English
DB22A4D9-7E4D-485C-916A-9CD1386507FB	FEMALE	ASIAN	03cd7b91	English
6E70-D84D-C75F-477C-BC37-9177C3698C66	MALE	White	03cd7b91	English

Fig. 14. CRC32 Algorithm - Anonymized Dataset.

D. XXHASH64

The XXHash collection of algorithms features the non-cryptographic hashing algorithm XXHash64. It's intended to rapidly compute a 64-bit hashing value using provided information. Yann Collet designed XXHash64, which has become famous for its outstanding acceleration as well as its low collision level [18]. By repeatedly iterating across units of data, the XXHash64 algorithm generates a unique hash value. Since it manages data in a continuous design, it can handle enormous quantities of knowledge while utilizing a great deal of storage. This method is computationally efficient due to the way it integrates bit-wise computations including shifts, rotations, and XOR computations. A broad variety of hash values could be produced with XXHash64 as it provides a 64-bit hash integer. As it is a low possibility of collisions and a balanced distribution of the hashing numbers, diverse input data will probably give multiple hash outputs. The table in Figure 15 is an example of the XXHASH64 Algorithm.

PatientID	PatientGender	PatientRace	PatientMaritalStatus	PatientLanguage
FB2AB823-C9D0-4D09-8464-49BF0B982F0F	MALE	UNKNOWN	Married	Icelandic
64182895-E872-4E2B-BE77-8050B71498CE	MALE	African American	Separated	English
DB22A4D9-7E4D-485C-916A-9CD1386507FB	FEMALE	ASIAN	Married	English
6E70-D84D-C75F-477C-BC37-9177C3698C66	MALE	White	Married	English

Fig. 15. XXHASH64 Algorithm - Original Dataset.

After Applying the XXHASH64 Algorithm in the "PatientLanguage Characteristic":

PatientID	PatientGender	PatientRace	PatientMaritalStatus	PatientLanguage
FB2AB823-C9D0-4D09-8464-49BF0B982F0F	MALE	UNKNOWN	Married	Cw023865w6969833
64182895-E872-4E2B-BE77-8050B71498CE	MALE	African American	Separated	f7eefde29f3e16f2
DB22A4D9-7E4D-485C-916A-9CD1386507FB	FEMALE	ASIAN	Married	f7eefde29f3e16f2
6E70-D84D-C75F-477C-BC37-9177C3698C66	MALE	White	Married	f7eefde29f3e16f2

Fig. 16. XXHASH64 Algorithm - Anonymized Dataset.

IV. BACKGROUND OF ENCRYPTION TECHNIQUES

Hashing and also Encryption are two good options for protecting data but each differs in specific aspects. Encryption tends to be utilized to encrypt data while it is in transmission. Data that has to be transmitted needs to be delivered in a manner that avoids unauthorized access because it can only be seen by its intended recipient. Data is encrypted to ensure it is unreadable by everyone outside the holder of the decryption key when it is still in transmission. A few situations where encryption could be desirable over hashing involve databases for storage and retrieval, methods of authentication, and other situations where data needs to be masked at rest while remaining retrievable. Four main Encryption techniques have been established for this research: the "DES" is an algorithm for a symmetric encryption approach for securing data and communications, the "XDES" is an improvement on the symmetric key algorithm "DES" and is utilized to both encrypt and decipher digital information, the "Blowfish" is a symmetric block-cypher which employs a digital key which may range around 32 and 448 bits in depth, and the "AES-512" references to the 512-bit key length used by the Advanced Encryption Standard.

A. DES

The most prevalent symmetric encryption initiative for protecting computer data is DES (Data Encryption Standard). With a 56-bit key, DES converts into and out of blocks of data that are generally 64 bits in length. With a 56-bit key, DES converts into and out of blocks of data that are generally 64 bits in length. Using the given key, this technique executes several kinds of complicated math operations, including substitutions and permutations, on the input data. To encrypt data, the DES algorithm splits the initial information into 64-bit blocks. A maximum of sixteen iterations of encryption operations which include bit modification and replacement lists called S-boxes are now used. A distinct subkey retrieved from the main key is utilized in every phase [19]. The table in Figure 17 is an example of the DES Algorithm. The dataset has 5 attributes: the "PatientID", the "PatientGender", the "PatientRace", the "PatientMaritalStatus" and the "PatientLanguage".

PatientID	PatientGender	PatientRace	PatientMaritalStatus	PatientLanguage
FB2AB823-C9D0-4D09-8464-49BF0B982F0F	MALE	UNKNOWN	Married	Icelandic
64182895-E872-4E2B-BE77-8050B71498CE	MALE	African American	Separated	English
DB22A4D9-7E4D-485C-916A-9CD1386507FB	FEMALE	ASIAN	Married	English
6E70-D84D-C75F-477C-BC37-9177C3698C66	MALE	White	Married	English

Fig. 17. DES Algorithm – Original Dataset.

After Applying the DES Algorithm to the “PatientGender Characteristic”:

PatientID	PatientGender	PatientRace	PatientMaritalStatus	PatientLanguage
FB2AB823-C9D0-4D09-8464-49BF08982F0F	NK7Zv1pUJVhQ	UNKNOWN	Married	Icelandic
64182895-E872-4E2B-BE77-8050871498CE	FTb.R0bQ7rQ5I	African American	Separated	English
DB22A4D9-7E4D-485C-916A-9CD1386507FB	IZIE7Yv4Unlxk	ASIAN	Married	English
6E70-D84D-C75F-477C-BC37-9177C3698C66	CdocJ2NFDB7og	White	Married	English

Fig.18. Applying DES Algorithm - Encrypted Dataset.

B. X-DES

A variation of the Data Encryption Standard (DES) algorithm is “X-DES” often referred to by the acronym “DES”. Because of its relatively small length of the key of just 56 bits, the symmetric key procedure referred to as DES, and that was formerly widely used for encryption. Key whitening, additionally referred to as key masking, is a fundamental tweak that “DES-X” utilizes to improve the security of “DES”. If you want to employ the key whitening process, you need to XOR the initial DES key with a random number referred to as the “whitening key”. The whitening key can be generated pseudorandomly or as a predetermined value that remains constant for every single encryption process. It also improves the encryption process’s difficulty and variability. With this enhancement, greater adaptability for particular cryptographic operations is planned [20]. The table in Figure 19 is an example of the “X-DES” Algorithm. The dataset has 5 attributes: the “PatientID”, the “PatientGender”, the “PatientRace”, the “PatientMaritalStatus” and the “PatientLanguage”.

PatientID	PatientGender	PatientRace	PatientMaritalStatus	PatientLanguage
FB2AB823-C9D0-4D09-8464-49BF08982F0F	MALE	UNKNOWN	Married	Icelandic
64182895-E872-4E2B-BE77-8050871498CE	MALE	African American	Separated	English
DB22A4D9-7E4D-485C-916A-9CD1386507FB	FEMALE	ASIAN	Married	English
6E70-D84D-C75F-477C-BC37-9177C3698C66	MALE	White	Married	English

Fig.19. X-DES Algorithm - Original Dataset.

After Applying the X-DES Algorithm to the “PatientGender” Characteristic:

PatientID	PatientGender	PatientRace	PatientMaritalStatus	PatientLanguage
FB2AB823-C9D0-4D09-8464-49BF08982F0F	_J9__u9ccObnSulTzWoc	UNKNOWN	Married	Icelandic
64182895-E872-4E2B-BE77-8050871498CE	_J9__iw4yS70mjUdRG8Q	African American	Separated	English
DB22A4D9-7E4D-485C-916A-9CD1386507FB	_J9__7ZRYT/rqYQ0g/Dm	ASIAN	Married	English
6E70-D84D-C75F-477C-BC37-9177C3698C66	_J9__wA9jBMpO6xdq1Y2	White	Married	English

Fig.20. X-DES Algorithm - Encrypted Dataset.

C. BLOWFISH

The Blowfish algorithm is a symmetric key block cypher and it has become known to be trustworthy and simple to use. Blowfish may be modified according to various encryption criteria because it operates on 64-bit blocks of data and gives keys with lengths that vary from 32 bits to 448 bits [21]. It has been separated into two distinct

sections:

- Key Generation: A key expansion process utilized by Blowfish for generating a variable-length key. To be able to generate a suitable key product, an initialization vector (IV) and key can only be modified by constantly executing the Blowfish algorithm on the key.

- Block Encryption: The initial text is broken down into 64-bit blocks thanks to Blowfish, and every single one afterwards is tested using several iterations. A starting point of 16 rounds and an aggregate of 56 rounds are permitted based on the key length. A replacement, combination, and key combining procedure composes each round. The table in Figure 21 is an example of the BLOWFISH Algorithm. The dataset has 5 attributes: “PatientID”, “PatientGender”, “PatientRace”, “PatientMaritalStatus” and PatientLanguage.

PatientID	PatientGender	PatientRace	PatientMaritalStatus	PatientLanguage
FB2AB823-C9D0-4D09-8464-49BF08982F0F	MALE	UNKNOWN	Married	Icelandic
64182895-E872-4E2B-BE77-8050871498CE	MALE	African American	Separated	English
DB22A4D9-7E4D-485C-916A-9CD1386507FB	FEMALE	ASIAN	Married	English
6E70-D84D-C75F-477C-BC37-9177C3698C66	MALE	White	Married	English

Fig. 21. Blowfish Algorithm – Original Dataset.

After Applying the BLOWFISH Algorithm in the PatientMaritalStatus Characteristic:

PatientID	PatientGender	PatientRace	PatientMaritalStatus	PatientLanguage
FB2AB823-C9D0-4D09-8464-49BF08982F0F	MALE	UNKNOWN	S2a50650ci/gGd8PrWY E8h0uRzY0uuzY0nPX3 1A0.cciF25ynMberfUTO2 s2vfwaa	Icelandic
64182895-E872-4E2B-BE77-8050871498CE	MALE	African American	S2a5065g7Z3nhqA4CAj k4VapEIVegZE2Om7qw7 yTiafWVvU4033reyN2ZA M	English
DB22A4D9-7E4D-485C-916A-9CD1386507FB	FEMALE	ASIAN	S2a5065fBMMRAoHeOD IL66H20Rw1eH20Rw1e Hw0KYaF0n70bhdDCE Rysu1Y1T0J1	English
6E70-D84D-C75F-477C-BC37-9177C3698C66	MALE	White	S2a5065AOp2679IUZX 48PDlweTuhMDRctYm wS3gY9CgKcbXwCFRQ./ /5	English

Fig.22: Blowfish Algorithm – Encrypted Dataset.

D.AES-512

The whole AES-512 algorithm architecture is impacted when using outputs of 512 bits as opposed to 128 bits. There are four primary byte-based modifications utilized by AES-512. The first alteration is referred to as "Byte Substitution," which swaps the 512-bit numbers utilizing parallel S-boxes. During the second stage of the conversion, Shifting Rows, the results from the prior step's rows are relocated by a distance equivalent to the line position. The final stage of the conversion has the title "Mixing Columns," and it involves dividing every single row of the output from the previous step by an additional number. Combining the Round Key with the last decision made in the current round is the round's supreme transformation [22]. The table in Figure 23 is an example of the AES-512 Algorithm. The dataset has 5 attributes: “PatientID”, “PatientGender”, “PatientRace”, “PatientMaritalStatus” and PatientLanguage.

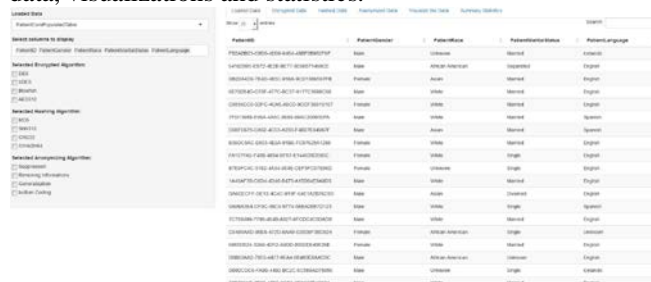
PatientID	PatientGender	PatientRace	PatientMaritalStatus	PatientLanguage
FB2AB823-C9D0-4D09-8464-49BF08982F0F	MALE	UNKNOWN	Married	Icelandic
64182895-E872-4E2B-BE77-8050871498CE	MALE	African American	Separated	English
DB22A4D9-7E4D-485C-916A-9CD1386507FB	FEMALE	ASIAN	Married	English
6E70-D84D-C75F-477C-BC37-9177C3698C66	MALE	White	Married	English

Fig. 23. AES -512 Algorithm - Original Dataset.

PatientID	PatientGender	PatientRace	PatientMaritalStatus	PatientLanguage
F82AB823-C9D0-4D09-8464-49BF0B98270F	MALE	UNKNOWN	Married	{\303\015\004\007\003\0012\3649Kw\342\317\322\001\3067
41618295-E873-4E28-BE77-8050B71495CE	MALE	African American	Separated	{\303\015\004\007\003\0012\2124\275\2344\5302\006g\3228\001\007\324\2458&t∓
DB22A4D9-7E4D-485C-916A-9CD1386507FB	FEMALE	ASIAN	Married	{\303\015\004\007\003\0012\0003\206d\2240\300\203\024\3228\001mm\262\035\}
6E70-D84D-C75F-477C-BC37-9177C3698C66	MALE	White	Married	{\303\015\004\007\003\0012\0003\206d\2240\300\203\024\3228\001mm\262\035\}

V. THE PROPOSED DATA ANONYMIZATION TOOL

As we've already stated before, there is an Anonymization tool that allows the suggested approaches to be utilized continuously. Making use of the previous work [23] as a starting point and guidelines for the utilization of the previous techniques. The software called ShinyAnonymizer is a tool enabling non-expert users to use and combine state-of-the-art privacy models. It permits the software to employ several of the techniques discussed like Suppression and Generalization, establishing a collection of strategies for data anonymizing. As seen in Figure 25, the aforementioned tool provides a graphical tool with a simple interface that allows the import of data, different ways for anonymizing data, visualizations and statistics.



A stand-alone software component is also available with ShinyAnonymizer, making it simple to integrate into different systems. It is additionally adaptable to several better algorithms, thoroughly verified, and carefully documented.

The Table I presents an in-depth analysis of the Anonymization, Hashing, and Data Encryption techniques, illustrating the algorithm's objectives, key requirements, and reversibility. Data security, privacy preservation, and safe information management all require learning how these approaches vary from one another.

<i>Algorithm</i>	<i>Purpose</i>	<i>Characteristic</i>	<i>Key Required</i>	<i>Example Algorithms</i>
<i>Anonymization</i>	To delete or obscure personal identifiers	In the majority of cases irreversible	No	Suppression Generalization Removing Information Bottom Coding
<i>Hashing</i>	To create a fixed-size distinct (hash) value	In the majority of cases irreversible	No	MD5, SHA-512 CRC-32 XXHASH64
<i>Encrypted</i>	To protect data through transforming it to an unreadable format	With a correct key, reversible	Yes	DES, 3DES Blowfish AES-512

Table Comparison

- **Purpose:** Defines every algorithms category's primary objective in its intended use. Hashing produces distinctive identities and anonymization removes identifiable details, and encryption maintains the secrecy of data.

- **Key Required:** Specifies when a key must be present for the algorithm to work properly. Though encryption techniques depend on keys for both encryption and decryption processes, anonymization and hashing do not.

- **Example Algorithm:** In each field, it contains commonly utilized techniques like Suppression and Generalization for Anonymization, MD5 and SHA-512 for Hashing and AES-512 and DES for Data Encryption.

Anonymization is an algorithm used to delete or obscure identifiable information from data while maintaining its analytical and research value. In general, this process is irreversible, which makes it hard to retrieve the initial data from the anonymized version. Suppression and Generalization are two anonymization approaches which are able effectively to protect sensitive data while keeping their practical use. A key is not needed for anonymization.

Using input data, hashing algorithms generate fixed-size distinctive numbers. Hashing is mostly utilized for maintaining data integrity and producing a special identifier for comparing data and validation. Since hash algorithms can frequently be non-reversible it is extremely hard to get back the initial data from a hash. The Hashing Methods MD5 and SHA-512 are frequently deployed. A key is not needed for hashing.

In an attempt to keep secrecy and safeguard valuable information, encryption algorithms transform data towards a form that is impossible to read. As encryption can be reverted given a valid decryption key, it is different from anonymization and hashing because the original data could be accessed. A key is a requirement for data encryption techniques as it is required for both encryption and decoding of the data. The “DES” and “AES-512” are some examples of data encryption algorithms.

In summary, as encryption is reversible and maintains the quality of the initial data while securing it, anonymization and hashing are irreversible procedures that put first data privacy and integrity identification, correspondingly, during the cost of having lost accessibility to the initial data in its entirety.

The specific purposes and needs for data protection define which of the three options: anonymization, hashing, and encryption should be applied. Since the primary goal was to

maintain privacy by obfuscating or deleting personally identifiable data, anonymization is effective. Being able to gain access to the initial information has been compromised because it is irreversible and highlights data privacy. Data integrity and the development of unique identities for comparing data and verification are made available by hashing. It can be used to guarantee data integrity as opposed to preserving secrecy and is practically irreversible. Since both secrecy and reversibility are essential, encryption is the most effective choice. Data has been altered into a completely unreadable form, currently the original data might still be available with a correct decryption key. The best technique should be chosen based on the particular requirements of a given data use case, striking a balance between privacy, integrity, and accessibility concerns. Both organizations and people may determine what approach to employ based on their specific security needs for data by carefully considering the objectives and features of every option.

REFERENCES

- [1] Shrivastva, K.M., Rizvi, M.A., & Singh, S. (2014). Big Data Privacy Based on Differential Privacy a Hope for Big Data. 2014 IEEE International Conference on Computational Intelligence and Communication Networks, pp 776-781.
- [2] Olga Yu. Guseva, Inna O. Kazarova, Ilona Y. Dumanska, Mykhaylo A. Gorodetsky, Lina V. Melnichuk, Volodymyr H. Saienko, "Personal Data Protection Policy Impact on the Company Development," WSEAS Transactions on Environment and Development, vol. 18, pp. 232-246, 2022.
- [3] Smith, L., Chowdhury, M. M., & Latif, S. (2022). Ethical Hacking: Skills to Fight Cybersecurity Threats. EPiC Series in Computing, 82, pp. 102-111.
- [4] Barendt, E. (2005). Freedom of speech. OUP Oxford.
- [5] Olatunji, Iyiola E., et al. "A review of anonymization for healthcare data." Big data (2022).
- [6] LeFevre, Kristen, David J. DeWitt, and Raghu Ramakrishnan. "Workload-aware anonymization." Proceedings of the 12th ACM SIGKDD International Conference on Knowledge discovery and data mining (2006).
- [7] Yazed Alsaawy, Ahmad Alkhodre, Adnan Abi Sen, "NiPA: Nicknames Pool Approach for Protecting Privacy of User Data in Intelligent Transportation Systems," WSEAS Transactions on Computers, vol. 21, pp. 211-220, 2022.
- [8] Chi, Lianhua, and Xingquan Zhu. "Hashing techniques: A survey and taxonomy." ACM Computing Surveys (CSUR) 50.1 (2017): pp.1-36.
- [9] Pub, F.I.P.S. (1999). Data Encryption Standard (DES). FIPS PUB, pp. 46-3.
- [10] Ohm, P. (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA L. Rev., 57, 1701.
- [11] Majeed, A., & Lee, S. (2020). Anonymization techniques for privacy-preserving data publishing: A comprehensive survey. IEEE Access, 9, 8512-8545.
- [12] Lison, Pierre, et al. "Anonymisation models for text data: State of the art, challenges and future directions." Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing (Volume 1: Long Papers), (2021).
- [13] Parmar, Kinjal, and Vinita Shah. "A review on data anonymization in privacy preserving data mining." International Journal of Advanced Research in Computer and Communication Engineering 5.2 (2016): 75-79.
- [14] Prasser, Fabian, et al. "Flexible data anonymization using ARX—Current status and challenges ahead." Software: Practice and Experience 50.7 (2020): 1277-1304
- [15] Rivest, Ronald "RFC1321: The MD5 message-digest algorithm." (1992).
- [16] Sumagita, M., Riadi, I., Sh, J. P. D. S., & Warungboto, U. (2018). Analysis of secure hash algorithm (SHA) 512 for encryption process on a web-based application. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 7(4), 373-381.
- [17] Boland, T., & Fisher, G. "Selection of hashing algorithms". NIST Technical Papers (June 2000).
- [18] Şuiü, Alice Florența, et al. "File Spooler and Copy System for Fast Data Transfer." 7th Conference on the Engineering of Computer-Based Systems, (2021).
- [19] Pub, F. I. P. S. "Data Encryption Standard (DES)." FIPS PUB (1999): 46-3.
- [20] Aleisa, N. (2015). A Comparison of the 3DES and AES Encryption Standards. International Journal of Security and Its Applications, 9 (7), pp. 241-246.
- [21] Khatri-Valmik, M.N., & Kshirsagar, V.K. (2014). Blowfish Algorithm. IOSR Journal of Computer Engineering (IOSR-JCE), 16(2), pp. 80-83.
- [22] Moh'd, A., Jararweh, Y., & Tawalbeh, L. A. (2011, December). AES-512: 512-bit Advanced Encryption Standard algorithm design and evaluation, 7th IEEE International Conference on Information Assurance and Security (IAS), pp. 292-297
- [23] Vardalachakis, Marios, et al. "ShinyAnonymizer: A Tool for Anonymizing Health Data", 5th International Conference on Information and Communication Technologies for Ageing Well and e-Health (ICT4AWE), pp. 325-332 (2019).

Copyright Protection on Electronic Books: Study and Design of a New Approach

Manos Vasilakis¹, Konstantinos Karampidis¹, Manolis Tampouratzis¹, Athanasios Malamos¹, Spyros Panagiotakis¹, Nikos Mastorakis²

¹*Department of Electrical and Computer Engineering (ECE), Hellenic Mediterranean University (HMU)*

Heraklion GR 71004 Greece, (mvasilakis@hmu.gr, karampidis@hmu.gr, tampouratzis@hmu.gr, amalamos@hmu.gr, spanag@hmu.gr)

²*Technical University of Sofia, Sofia, Bulgaria and Hellenic Naval Academy*

Piraeus, GR 18539 Greece, (mastor@hna.gr)

Abstract—In the age of big data, almost everything is digital. Every aspect of our daily lives has gone from analogue to digital and almost everything has adapted to the digital age. Cameras, pictures, texts, newspapers, books, etc. have adopted their digital equivalents. Although these changes make our lives easier, they also harbour many dangers and security risks. E-books have taken over because of their numerous advantages, low cost, easy reproducibility, portability, etc. The main drawback to their utilization concerns copyright issues. E-books, especially those in PDF format, are easy to reproduce without the owner's permission. Thus, it is essential to deploy a security mechanism to protect copyrights and ensure that an ebook is legitimate. In this study, a web application protection system for PDF e-books has been developed. Smart algorithms in cryptography, utilizing advanced encryption techniques based on AES encryption to ensure the integrity of copyright protections and for the steganography covering, based on the Least Significant Bit (LSB) were implemented for this work. This enables us to verify who is the original buyer of a book having all the form fields in our possession to identify the original buyer. Furthermore, a variety of e-book formats, encryption methodologies, cover data approaches and the algorithms supporting the described system copyright protection system are discussed.

Keywords—Copyright Data Protection, Electronic Books, Cryptography Algorithms, Steganography Algorithms.

I. INTRODUCTION

In a digital age, where every given data is almost digital. Like text, audio, video, image and constantly evolving with new technologies and techniques. All this digital information/data can be found in security systems, digital networks and online services in various forms of digital products. Then, a problem that arises in all of this is piracy [1], especially for the companies. This study, focused on copyright protection on electronic books [2], PDF's format.

The most widely used formats for electronic books are PDF (Portable Document Format) [3], the EPUB [3], the MOBI [4], the AZW (Kindle) [4] and the ODF (Open Document Format) [5]. The purpose was to implement a web application in Java in the most popular format pdf, where if someone purchases an E-book has the copyright of it and no one else can claim it [4]. To implement all this, it is necessary to research the methodology. In summary, the implementation model includes an application in which the user will fill in some fields of data according to the purchases E-book and it will be processed on the server [7] to protect [5] the copyright of this book through some algorithms. The first algorithm used is AES [13]. It is a Symmetric key algorithm [12] which means that the sender and receiver have the same key [17], which makes the encryption process faster. When implementing the algorithm with code there are several points to pay attention to such as the mode of operation [10] to use to provide proper security.

Then, getting the cryptography string from all the fields on the first created cover page half implementation is done. On the other part, the steganography algorithm LSB [15], [20] is responsible for hiding each encrypted text in the last 3 bits in all images in the document with procedures pdf manipulation functions for the final result. Decryption is done in the reverse process.

A. The Portable Document Format (PDF)

Portable Document Format, or simply PDF, was created by Adobe in 1993. Is among the most widely used and profitable file types in the digital era. It is a file format that describes documents, as its name suggests. Articles, books and entire series can easily, quickly and securely be created shared and read. After all, this format is the most widespread for correcting and viewing content that is to be published or printed, since it maintains the formatting given by its creator through any application, which simply prints and because there are applications that one can comment on this file.

B. The EPUB

The International Digital Publishing Forum supported the EPUB format as the official Open e-book standard in August 2009. The final version, EPUB 3.0, was published in June 2014. EPUB specifications consist of three files: OPS (Open Publication Structure), OPF (Open Packaging Format), and OCF (Open Container Format). These files are based on XHTML and XML, with HTML files with CSS for manifest, metadata, table of contents, and image files, all placed in a ZIP file.

C. The MOBI

Mobi is a standard used by MobiPocket electronics readers, mobi or. PRC formats. It can be DRM-protected or not. Mobi files can be opened with a Mobipocket reader, Amazon Kindle reader, and compatible devices. MobiPocket template uses XHTML, containing JavaScript and frames, and can use SQL queries with built-in databases.

D. The AZW (Kindle)

The AZW format, a standard used exclusively by Amazon Kindle electronic readers and iPhones, is compatible with smartphones, computers, iPad readers, and tablets. It is based on MOBI standards and offers a service for converting documents to another standard. azw format, for easy reading by Amazon's readers. The DRM on AZW is locked in the serial code of the Kindle device, allowing only the purchased electronic reader to be opened and read. Multiple online readers can be added to an Amazon account, allowing a family to share a purchased book.

E. The Open Document Format (ODF)

This format is based on XML and its Open-Source file format. Used for presentations, exchanging charts, text etc.

These files have common extensions such as ".docx, .xlsx". The list of the common extensions are: .odt for Word, .ods for spreadsheets, .odp for presentations, .odg for graphics and .odf for formulas.

II. DEFINITIONS OF CRYPTOGRAPHY

- **Cryptography:** Initially an art for concealing message content from unauthorized entities, has evolved into a science with numerous applications. It involves transforming messages into incomprehensible formats using cryptographic algorithms, making them unreadable by third parties. Basic definitions are provided to help understand deposit objectives [7].
- **Cryptanalysis:** This is the process of effort disclosure of the original text or key from unauthorized entities potentially attacking. The strategy used by the cryptanalyst depends on the nature of encryption and the information available to him/her [8].
- **Cryptology:** This is a science that includes the two previous branches [7].

Cryptography provides four basic functions [9]:

- **Confidentiality:** Information to be transmitted is only accessible to authorized members. The information is incomprehensible to someone third.
- **Integrity:** Information may only be altered by authorized members and can't be altered without the detection of corruption.
- **Non-Repudiation:** The sender or recipient of the information cannot deny the authenticity of its transmission or creation.
- **Authentication:** The sender and recipient can verify their identities as well as the source and the destination of the information with assurance that their identities are not fake.

Some important expressions on Cryptography, include [7]:

- The **Plain Text** which is called the initial message with information to encrypt it to send the information to the next step.
- The **Cipher Text** which is called the transformed message produced as output by the algorithm encryption. The cipher text is dependent on both the original message and the secret key, different keys produce different ciphers.
- The **Encryption Algorithm** which makes the necessary transformations of the original text to achieve encrypting a message.
- The **Encryption** process, is called the conversion process of the original text into cipher.
- The **Decryption** or *Deciphering*, is called the reverse process of encryption, namely the converting of the cipher into original text.
- The **Key Encryption**, is called the analytical description of the encryption method. The key, for example, can be the correspondence between the original plain text and cipher text.
- The **Padding** is the process of covering a message by the additional text that should be added to the text so that the original text has real original length requires a cryptographic algorithm. Usually, the text is added to the length of the original text followed by zero the cover is removed during decryption.

III. MODES OF OPERATION

One type of algorithm block cipher has several modes of operation. Each mode can have properties beyond those inherited from the basic cipher. The basic modes are the Electronic Code Book (ECB), the Cipher Block Chaining (CBC), the Cipher Feedback Blog (CFB) and the Output Feedback Blog (OFB) [10]. This work uses the CBC mode.

In **CBC (Cipher Block Chaining)** mode, each unencrypted block is combined through the logic operation X-OR with the previously encrypted block, resulting in an encrypted block. It requires an initial value for the first X-OR operation, the so-called Initialization Vector. Identical plaintext blocks are covered by the use of logic operation and the security of the algorithm is increased, as shown in Fig 1. The speed of encryption is the same as the block cipher, but the process cannot be done although decryption can [11].

IV. CATEGORIES OF CRYPTOGRAPHY ALGORITHMS

The encryption algorithms [16], depending on the type of key are divided into two main categories: Secret Key Algorithms (Symmetric) and Public Key Algorithms (Asymmetric) [12].

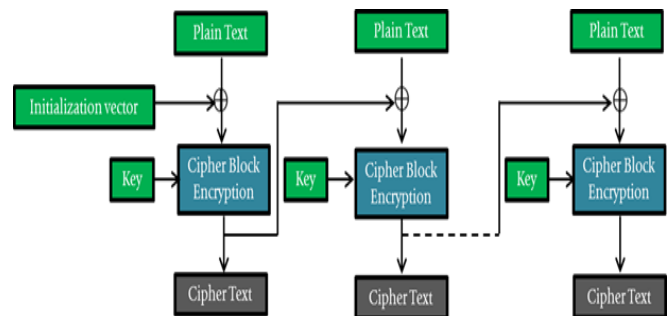


Fig.1 CBC mode encryption [source].

- **Symmetric Encryption Algorithm:** Symmetric cryptography use only one key for encryption and decryption. The sender and receiver of a message know and use the same secret key. The sender and the recipient must use the (Secret Key) for the message encryption and decryption. This technique is called symmetric cryptography or secret key cryptography. The main characteristics of these algorithms are the encryption speed, the decryption speed, the small key length and the easy implementation. It is a secure method of transferring and exchanging keys without anyone else knowing about it. However, it is vulnerable to unauthorized access, as anyone with the right means can record and obtain the key.
- **Asymmetric Encryption Algorithm:** Asymmetric encryption uses two keys for encrypting and decrypting messages. The public key is published, while the private key is kept secret. The secret key is never transmitted over the network, and all communications are based on an asymmetric key. Asymmetric cryptography requires confidentiality and confirmed correlating of public keys with their owners. It has various uses, including encryption and generation of digital signatures. The private key is mathematically related to the asymmetric key, making it difficult to recover from the public. Encryption using asymmetric cryptography involves sending a secret message to a receiver, who then decrypts it using their private key. Only the sender or the receiver with the public key can

decrypt the message. A disadvantage of asymmetric cryptography is its speed, as symmetric keys are faster than asymmetric keys. Moreover, asymmetric cryptography requires certification and verification of public keys from organizations to ensure the identity of legitimate users. Fraudsters can link the public key of a legitimate user to the identity of the authorized user. In some cases, asymmetric cryptography is not necessary, as symmetric cryptography is sufficient in closed environments without internet connections. A computer may hold secret keys, posing a risk of seizure by external factors.

The AES (Rijndael) Algorithm Operation Process

The main processing unit of AES [13] is the byte. Thus, the bits of a block or a key are divided into groups of eight to form the bytes. Each byte of AES corresponds to a polynomial (finite field arithmetic). Assume that the bits of a byte are:

$$P(x) = (\text{byte}7) x^7 + (\text{byte}5) x^5 + (\text{byte}2) x^2 + (\text{byte}1) x^1$$

The bytes [10100110] correspond to the polynomial $x^7 + x^5 + x^2 + x^1$. All the operations performed by the algorithm are on a two-dimensional table called (State). The state is described by a table whose data is bytes. This table has always four rows and columns depending on the key size (128/4 columns, 192/6 columns, 256/8 columns). The plaintext is divided into block sizes of 128 bits (16 bytes). The encryption and decryption process of AES is shown in Fig. 2.

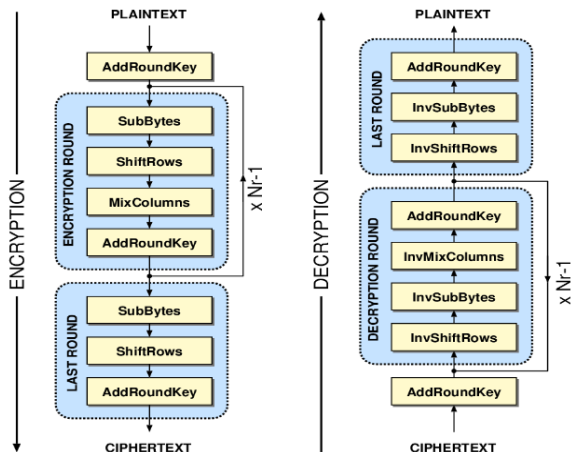


Fig.2 Encryption and Decryption Process [\[source\]](#)

C. Algorithms Characteristic Synopsis

This algorithm is characterized by simplicity, flexibility, resistance to all known cryptanalysis attacks, and high operating speed. It is used for private and non-government information and is considered practically safe from attacks. Although it may crack with brute force attacks, the algorithm can never be broken [13].

V. EXPLORATION OF STEGANOGRAPHY TECHNIQUES

Steganography is a technique that conceals the existence of hidden messages [15]. It originates from ancient Greece and it was widely used by Germany during World War II. Steganography and cryptography differ, while cryptography transforms and hides the message's content but not the message itself, and steganography tries to hide the message's existence. To break a steganography system, an attacker must a) detect the existence of the secret message and b)

reveal the secret message. Depending on the type of cover medium, there are different ways to hide the secret message in steganography:

- **Image:** Due to the inability of human vision to perceive subtle digital changes in image data, image files are an effective file type for steganography. Encoding can be performed using replacement algorithms such as LSB, image algorithms such as DCT, or undeveloped techniques.
- **Audio:** The hidden message is converted into digitized sound by altering the binary sequence of the file's bits. Techniques include LSB, phase encoding, and Spread Spectrum. LSB replaces the resulting binary sequence of bits, phase encoding replaces the original phase frequency of a segment, and Spread Spectrum multiplies the signal with a pseudo-random noise sequence, ensuring the power of the information signal remains lower than the noise power, making it unnoticeable.
- **Video:** The video files are nothing else than a sequence of static images and sound. Therefore, the previous methods can be applied to it as well case.
- **Network Protocol:** This method inserts hidden information into OSI protocol communication packets, such as adding TCP/IP headers or changing IP header values. It ensures maximum security and allows for maximum data storage using intelligent techniques to maximize capacity coverage. This method is crucial for ensuring confidentiality and efficiency.

The LSB and LBP Steganography Algorithms

- **The Least Significant Bit (LSB) Algorithm:** A technique for image encoding can be done with the LSB (Least Significant Bit) algorithm. In this technique, the less significant bit of some image's byte is replaced by the hidden message's bits [20]. An example is RGB values and how the human eyes cannot detect the difference between bits/RGB values, as shown in Figure. 3.



Fig.3 Orange RGB values [\[source\]](#)

The left half of the image is (255, 127, 39) and the right half of the image is (255,126,39). The only difference in the two values is just one bit. Can the human eye detect it? No. Because the human eyes cannot detect such a small difference between two values. Each pixel can store 3 bits from the hidden message.

- **The Local Binary Pattern (LBP)** was developed to extract attributes' texture by studying the grayscale of the image. One of the characteristics of the algorithm used by steganography is to hide the entire message. The fact that grayscale in most images contains some type of noise makes them useful for hiding information without being detected. In recent years, there has been an interest in their implementation of face recognition. Although originally it was proposed to recognize textures [19]. It has an impact on many applications, such as image/video recovery, aerial image analysis and visual surveillance. Mainly used for face recognition, face expression detection and fingerprints. Figure 4 depicts the initial operator of LBP and sets the

values in the pixels of an image through the threshold of one 3x3 neighbourhood pixel [18] of each pixel with the centre pixel value (6) and considers the result as a binary number from which the corresponding decimal number (241) used for the label is derived.

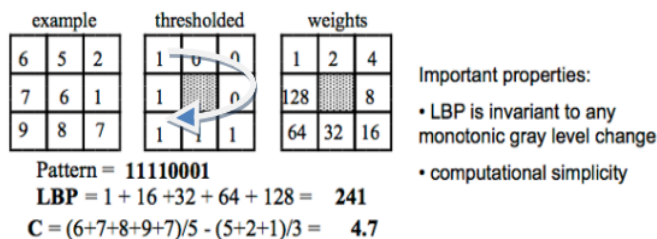


Fig.4 LBP algorithm (source)

VI. METHODOLOGY

In this study, a web application for the protection of copyright on e-books (pdf) has been developed based on the AES encryption algorithm. The proposed method [14] could identify the original customer if a PDF book is bought to own it permanently and be verified as the buyer by another user.

A. Software used for this Study

The software that was used was NetBeans. A complete version of Netbeans contains all of the required files for this project. A Tomcat server runs automatically with Netbeans so long as Netbeans is configured accordingly. Tomcat is required to execute Java servlets and display them all on our website (JSP files). Additionally, the required Java libraries to implement this work are:

- "itext 5.5.10 library", which is a library for pdfs with a large-scale API.
- "javax. crypto" which supports many algorithms, encryption/decryption/hashing for low-level crypto. Moreover, the Java security library is needed for SecureRandom, key management.

B. The Java Server Pages file format (JSP)

The JSP file extension is the file format for Java Server Pages. A JSP is an HTML page that references Java servlets or server-side applets. JSP files facilitate the delivery of server-side, customized web content via servlets. JSP files conceal Java code because they execute server-side (link). Imagine that, it is comparable to the .html file extension. The HTML file is used to display in the browser the content that has been written. On the other hand, there is a server, such as a.php file that communicates with the server (back-end). The view of the content, which in this instance is HTML, but not the content for the server, which is the.php file. SecureRandom, key administration.

C. Project Details

When the Tomcat server is initiated in NetBeans, one must give heed to the following additional information: Figure 5 depicts the messages displayed when the Tomcat server boots up.

```
Using CATALINA_BASE: "C:\Users\xaak\AppData\Roaming\NetBeans\8.2\apache-tomcat-8.0.27.0_base"
Using CATALINA_HOME: "C:\Program Files\Apache Software Foundation\Apache Tomcat 8.0.27"
Using CATALINA_TMPDIR: "C:\Users\xaak\AppData\Roaming\NetBeans\8.2\apache-tomcat-8.0.27.0_base\temp"
Using JRE_HOME: "C:\Program Files\Java\jdk1.8.0_151"
```

Fig.5 Booting up Tomcat Server.

The Catalina base [28] is the root of the directories that exist on the Tomcat Server. Figure 6 demonstrates the Catalina base structure.

conf	3/11/2017 12:05 πμ	Φάκελος αρχείων
logs	1/12/2017 12:14 μμ	Φάκελος αρχείων
nblib	3/11/2017 12:05 πμ	Φάκελος αρχείων
temp	1/12/2017 12:17 μμ	Φάκελος αρχείων
webapps	3/11/2017 12:23 πμ	Φάκελος αρχείων
work	3/11/2017 12:05 πμ	Φάκελος αρχείων

Fig.6 The Catalina base structure.

Thus, the folder "webapps" is needed for web applications. Inside this folder must be created two new folders. The folder "books" and "tmp", as shown in Figure 7.

Όνομα	Ημερομηνία τροπ...	Τύπος	Μέγεθος
books	1/12/2017 1:53 μμ	Φάκελος αρχείων	
tmp	1/12/2017 1:53 μμ	Φάκελος αρχείων	

Fig.7 The Catalina base structure.

The category "books" must contain the uploaded PDF, as well as all other PDFs and the final PDF. When the book is uploaded, all fragmented packets are stored within the "tmp" folder. Navigate to our project using the URL, which also appears in the NetBeans launch window. We are in the index. jsp, which is a page with content that the user can view and submit information on. On the user's display will appear a form similar to Figure 8. The following initial values have been established for our project:

Fig.8 The Index. jsp

The user must enter all of the information required to encrypt the e-book. Then, he should select the book he wishes to encrypt, and selecting the "Encryption" icon will store the book in the TomCat folder we have designated, as depicted in Figure 9.

Fig.9 The PDF Encryption option.

The entire uploading procedure occurs on the TomCat server, where our book is also published (in the appropriate location). As depicted in Figure 10, when the file is submitted, another file with a "snap" link of the uploaded PDF file is summoned.

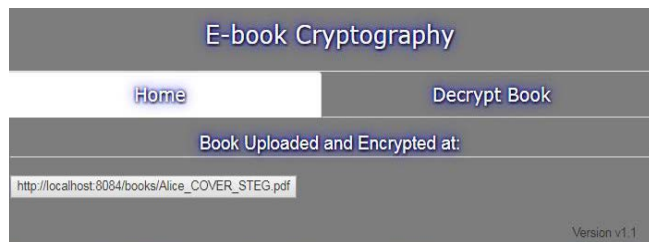


Fig.10 The Snap link.

By clicking on the above URL, the pdf file is downloaded to the user's browser and stored in the download file. The pdf has now been encrypted. The URL is no longer displayed. A new e-book must be uploaded for the URL to reappear.

The encryption process is implemented by certain Java classes on Java servers. The steps to get the final file are:

- **Step 1:** Figure 11 suggests that the first file is Alice.pdf, followed by Alice_COVER. At this point, a new cover page must be created by inserting a new cover page into the PDF and adding the first two form parameters and a crypto string which includes all the form's data encrypted at the end, as shown in Figure 12.

	Alice	Initial pdf	1/12/2017 2:13 μμ	Adobe Acrobat D...	196 KB
	Alice_COVER	Cover pdf	1/12/2017 2:13 μμ	Adobe Acrobat D...	209 KB
	Alice_COVER_STEG	Final pdf	1/12/2017 2:13 μμ	Adobe Acrobat D...	285 KB
	decr_info		1/12/2017 2:13 μμ	Έγγραφο κειμένου	1 KB

Fig.11 The webapps/books folder.

Buyer's Info

Name: John

Surname: Doe

3l88hsoElzRtyel7aQ1BlnbRpWaXykAVDyBrt6aBis5/Izlw7lwqOwdmiGP7vkB2

Fig.12 The first cover page.

- **Step 2:** The algorithm used to encrypt all fields from the form is a symmetric AES 128 with CBC mode. AES encryption uses two pieces of data to encrypt the information. The first is called the IV (Initialization Vector) and the second is called the Key [17]. IV gives more security as if the same plain text is encrypted multiple times, a different IV will give a different ciphertext each time.

- **Step 3:** Searches the file for all existing images and with the steganography technique LSB (*Least Significant Bit*) hides in each image the encrypted text containing all the fields of the form. After all this, the final pdf file is created as shown in Figure 11. Figure 13, represents the structure of the entire methodology described previously.

D. Decryption Process

Selecting the decrypt book label (decryptBook.jsp) initiated the decryption procedure. While in possession of the encrypted PDF, we navigate to the decrypt icon and upload the file previously downloaded from the URL in our download files, or we can upload the file from the TomCat server, as depicted in Figure 13.

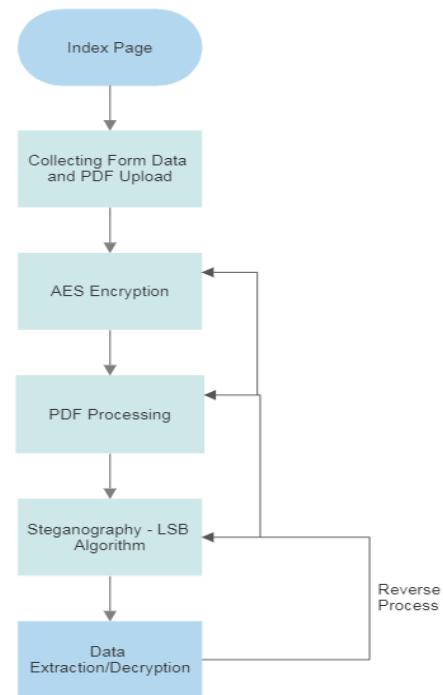


Fig.13 Briefly overview of methodology.

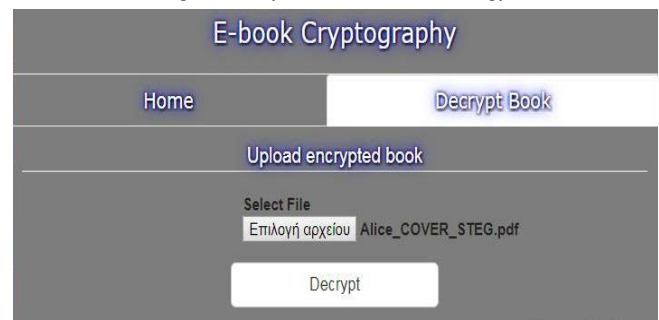


Fig.14 The Ebook selection button.

By selecting the decrypt icon, the data entered into the form or any other PDF could be displayed as shown in Figure 14. The entire decryption procedure is performed on the server, and it is the same process in reverse order as the encryption process.

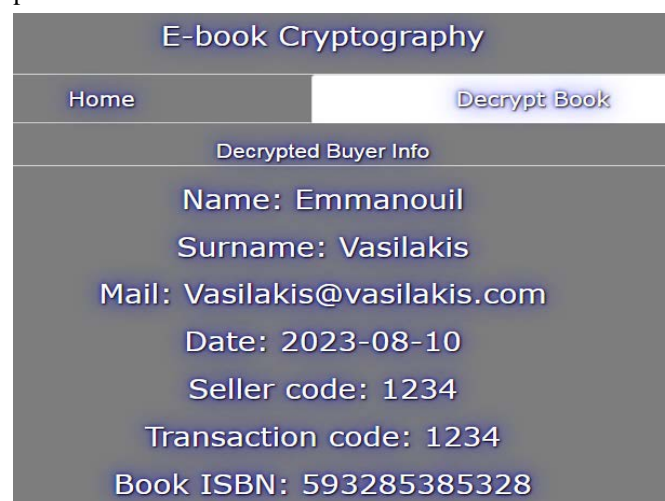


Fig.15 The webapps/books folder.

As depicted in Figure 15, the information entered into the initial form has been deciphered exactly as written. As shown in Figure 16, a specific message when providing an unencrypted book will appear.



Fig.16 The message "Encryption info not found".

VII. DISCUSSION

This work is about an implementation for copyright protection in e-books (PDF) and uses two strong algorithms in combination with them for more security. Figure 17 describes an AES algorithm that uses some keys for encryption, decryption and correspondingly the final crypto string.

```
book:book2_COVER.pdf
encIV:Etb00/0AboOLcjUZNA83eg==
encKey:1GutGtziOTQFvQh0OMo6jw==
line:j1tBqQkn2s5wE+azR641iM33bafkf0Qtz3qa+t6Tps2KRR0oKMmRaCfc
line:aDtGMavHqJ0bNacmLLLeNtUzU8OF70Y=
encr:j1tBqQkn2s5wE+azR641iM33bafkf0Qtz3qa+t6Tps2KRR0oKMmRaCfc
Decrypted Information String:Emmanouil Vasilakis Vasilakis@v
```

Fig.17 Encryption process and Decryption.

On the other hand, an intelligent steganography method introduced a technique in which the encrypted text is passed to each image and each page, and thus a strong combination of security is achieved, as shown in Figures 18 and 19.

```
page 2 -> encoding pdf image [/Im0]...
DONE
page 2 -> encoding pdf image [/Im1]...
DONE
page 2 -> encoding pdf image [/Im2]...
DONE
page 2 -> encoding pdf image [/Im3]...
DONE
page 4 -> encoding pdf image [/Im0]...
DONE
page 5 -> encoding pdf image [/Im0]...
DONE
```

Fig.18 Encoding PDF images.

```
Message in page 2: Emmanouil Vasilakis Vasilakis@vasilakis.com 2023-08-
Message in page 2: Emmanouil Vasilakis Vasilakis@vasilakis.com 2023-08-
Message in page 2: Emmanouil Vasilakis Vasilakis@vasilakis.com 2023-08-
Message in page 2: Emmanouil Vasilakis Vasilakis@vasilakis.com 2023-08-
```

Fig.19 Hiding text in images

One issue that had to be faced was the secure protection of the file that keeps the algorithm key and the encryption key. In such a case, the server that keeps the file must be secured with intrusion detection systems and the file must be encrypted in case someone else tries to open the file and cannot be able to read it. Future extended of the application to be implemented in other formats, such as EPUB.

VIII. CONCLUSIONS

Digital data protection is a critical research field, with cryptography and steganography techniques being developed to safeguard digital objects from illegal attacks. Numerous attacks are being made these days on security systems. Those techniques are suitable for copyright protection systems, and their features depend on the specific application requirements. Cryptography and steganography are effective methods for copyright protection. The combination of the two with proper implementation can hardly be broken. The AES algorithm is still unbreakable in our

days. This study developed a web application for protecting copyright on e-books (PDF) using the AES encryption algorithm and LSB steganography algorithm. The methodology's multi-layer approach strengthens protection against attack vectors and provides robust data security. The application can identify the original customer if a PDF book is bought to own it permanently and verified as the buyer by the system. Those algorithms continuously improve in terms of security and speed, making them integral parts of research for better user requirements.

REFERENCES

- [1] Sadiku, M. N. O., Ashaolu, T. J., Majebi, A. A., Musa, S. M. (2021). Augmented Intelligence. International Journal of Scientific Advances (IJSCIA), Volume 2| Issue 5: Sep-Oct 2021, pp. 772-776.
- [2] Vassiliou, M. and Rowley, J. (2008), Progressing the definition of "e-book", Library Hi Tech, Vol. 26 No. 3, pp. 355-368.
- [3] Faloye, S. T., Ajayi, N. A., Raghavjee, R., & Faniran, V. (2020). Managing the Challenges Facing the Adoption of E-books: A Case of UKZN. (2020) International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD).
- [4] Kogos E., Kogos A. (2017) Digital Rights Management Systems: Challenges and Opportunities of Electronic Book Publishing in Kenya
- [5] Battle S., Vitali F., Di Iorio A., Bernius M., Henderson T., Choudhury M. (2010). DIY eBooks: Collaborative Publishing Made Easy.
- [6] K. Karampidis, S. Panagiotakis, M. Vasilakis, E. K. Markakis and G. Papadourakis, "Industrial CyberSecurity 4.0: Preparing the Operational Technicians for Industry 4.0," 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Limassol, Cyprus, 2019, pp. 1-6.
- [7] Ronald L. RIVEST. (2014) Algorithms and Complexity: Handbook of Theoretical Computer Science, MIT Laboratory for Computer Science, Cambridge, MA 02139, USA.
- [8] Easttom, W. (2021) *Cryptanalysis In Modern Cryptography*, Springer.
- [9] Abbasi F., Singh, P., Cryptography: Security and Integrity of DataManagement, Journal of Management and Service Science, 2021, Vol.1, Issue. 2, pp. 1-9.
- [10] Alimzhanova, Z., Nazarbayev, D., Ayashova, A., Kaliyeva, A. (2022). Analysis of Ciphertext Behaviour Using the Example of the AES Block Cipher in ECB, CBC, OFB and CFB Modes of Operation, Using Multiple Encryption. In: Nguyen, N.T., Tran, T.K., Tukayev, U., Hong, TP., Trawiński, B., Szczerbicki, E. (eds) Intelligent Information and Database Systems. ACIIDS 2022. Lecture Notes in Computer Science, Vol 13758. Springer, Cham.
- [11] Shrivastva, K.M.P., Rizvi, M. A., & Singh, S. Big data privacy based on differential privacy is a hope for big data. IEEE International Conference on Computational Intelligence and Communication Networks, pp. 776-781 (2014).
- [12] Zhang Q., An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption, (2021) 2nd International Conference on Computing and Data Science.
- [13] Zhengyi Lu, Analysis on AES encryption standard and safety, (2022) Proceedings Volume 12462, 3rd International Symposium on Computer Engineering and Intelligent Communications (ISCEIC).
- [14] Vasilakis M, BSc Thesis, Hellenic Mediterranean University (2017).
- [15] Karampidis K., Kavallieratou, E., Papadourakis G. (2018). "A Review of Image Steganalysis Techniques for Digital Forensics" Journal of Information Security and Applications.
- [16] Madjit Malikovich Karimov, Nizomiddin Najmiddin Ugli Ochilov, Abdiqahhar Egamovich Tangirov, "Encryption Methods and Algorithms Based on Domestic Standards in Open-Source Operating Systems," WSEAS Transactions on Information Science and Applications, Vol. 20, pp. 42-49, 2023.
- [17] T. Sivakumar, S. Veeramani, T. Anusha, "Generation of Random Key Stream using Word Grid Puzzle for the Applications of Cryptography," WSEAS Transactions on Computers, vol. 20, pp. 1-9, 2021.
- [18] Kaur, N., Nazir, N., Manik. A Review of Local Binary Pattern Based texture feature extraction, 2021 9th International Conference on Reliability, Infocom Technologies and (ICRITO).
- [19] Zhao H., Sun S., Jing Z., Yang J, (2006) "Local structure based supervised feature extraction", Pattern Recognition, Vol. 38, No. 8, pp. 1546-1550.
- [20] Stoilov P., Hristov G., Zahariev P., (2021) Analysis of the least significant bit substitution algorithm for image steganography, vol.60.

RF Energy Harvesting from Ambient AM Radio Broadcasting Signals for Low-Power Applications

Manolis G. Tampouratzis¹, Demosthenes Vouyioukas¹, Traianos Yioultsis², Dimitrios Stratakis³

¹Department of Information and Communication Systems Engineering, University of the Aegean, Karlovassi, GR 82300 Greece, {tampouratzis, dvouyiou}@aegean.gr

²Department of Electrical and Computer Engineering (ECE), Aristotle University of Thessaloniki (AUTH), Thessaloniki, GR 54124 Greece, traianos@auth.gr

³Department of Electrical and Computer Engineering (ECE), Hellenic Mediterranean University (HMU), Heraklion, GR 71004 Greece, dstrat@hmu.gr

Abstract—The implementation of an RF-EH system by ambient AM radio broadcasting signals utilization for IoT self-powered applications is presented in this study. The system operation took place in the area of Heraklion, Crete, Greece taking advantage of receiving AM radio transmissions from countries in the Middle East, South Africa, and the Balkans. The proposed AM harvester consists of a long copper wire antenna, an LC tuning circuit, a germanium diode (1N34A) diode-based doubler rectifier, and a storage capacitor driven by the commercial DC-DC boost converter BQ22504 enable for powering low-consumption devices such as a medical thermometer, a portal calculator or IoT-based sensors.

Keywords—RF Energy Harvesting (RF-EH), Coil Ferrite Rod Antenna, Medium Wave (MW) Radio Detection, AM Radio Broadcasting, Internet of Things (IoT), Boost Converter.

I. INTRODUCTION

Radio frequency energy harvesting (RF-EH) is an emerging technology that tends to render the batteries unnecessary due to the difficulty of replacement especially in distributed wireless sensor networks (WSNs), while at the same time trying to reduce the maintenance cost of low-power sensor IoT-based applications. Various ambient RF energy sources with their benefits and drawbacks have occasionally been examined, e.g., TV, FM, GSM, UMTS, mmWave, and WiFi. The commercial frequency band of MW radio is 530kHz to 1620kHz, which corresponds to wavelengths ranging from 565m to 187m. In addition, the frequency band of LW radio is 153kHz to 279kHz, corresponding to wavelengths ranging from 1.96Km to 1.07Km respectively, and therefore the excessively long electrical length of the transmitting antennas. With the usage of the amplitude modulation (AM) technique in the aforementioned radio bands, its abbreviation is often associated commercially with the medium wave (MW) band. The propagation of MW and LW band radiowaves is through sky-wave reflection across the *E* and *F* layers of the ionosphere, where it lends itself to achieving long-distance radio communications. The radio propagation in these bands is more favourable during the night as opposed to during the day, a phenomenon that accounts for transatlantic radio transmissions over a distance of hundreds of kilometres. There is a significant incentive to collect energy from that specific region of the radio spectrum since radio transmissions carried out in the medium wave (MW) and long wave (LW) radio bands are often characterized by high RF transmission power on the order of a few KW, including these telecommunication techniques as the most energy-intensive.

Several studies have also dealt with energy harvesting from the medium (MW) and long wave (LW) radio bands [7,9]. In

[1] a wireless sensor system powered by MW broadcast energy harvesting is presented as obtaining high output voltage (up to 14V) and power of 82 μ W, in a typical urban environment by using a single-stage doubler rectifier. Authors in [2] demonstrate a scavenger working at AM frequency band that could work 10 kilometres from a 50kW radio station since the energy processing circuit could function with a minimum input signal level of -39 dBm. Medium wave radio transmissions may be exploited as an emerging “free energy” source to power the next generation of wireless networks, as shown by an optimized RF energy harvester tuned at AM broadcast for powering low-consumption devices, such as a portable calculator [5]. The work in [8] introduced a high-sensitivity AM energy harvester with a dc output voltage of 2.5 V and an efficiency of more than 60% that might be used to power wireless sensors for monitoring the degradation of civilian infrastructures.

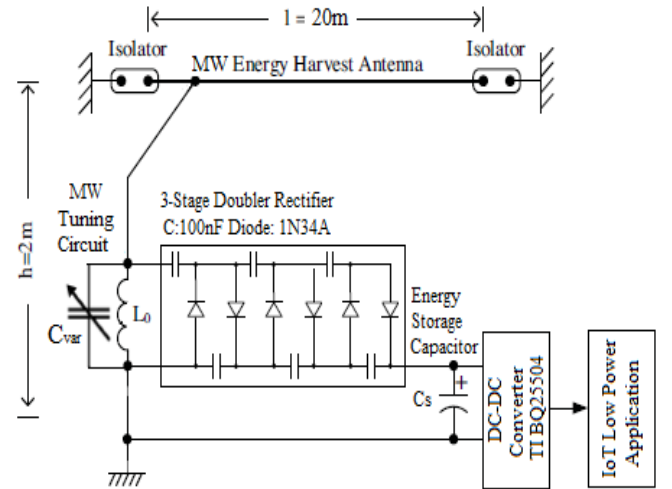


Fig 1. The proposed MW radio harvester schematic for powering low-consumption applications. The system consists of a long copper wire antenna, an LC tuning circuit, a germanium diode-based doubler rectifier, and a storage capacitor feeding by the DC-DC boost converter TI BQ22504

II. OPERATION PRINCIPLES AND SYSTEM IMPLEMENTATION

The proposed AM harvester (Figure 1) is comprised of a long copper wire antenna, an LC tuning circuit, a 3-stage germanium diode (1N34A) doubler rectifier, and a storage capacitor powered by a commercial DC-DC boost converter. The wavelength in the medium wave (MW) radio band is over 100 meters, which makes it difficult to implement receiving antennas in a residential area. For practical implementation, the antenna used for the proposed energy harvesting system was a long horizontal copper wire (about 20 meters) supported by two wooden insulators as shown in Figure 1, degenerating to a short electrical dipole model.

Ferrite Rod Antenna and Medium Wave LC Tuning Circuit

The cathode of the antenna wire feeds a high-quality factor (Q) tuned LC circuit (Figure 2) in the medium wave radio band (530kHz to 1620kHz), as a common radio receiver. Due to its inductive coupling to the antenna, the coil is crucial to the functioning of the system. The coil consists of a ferrite rod, offering the resonant circuit a high-quality factor ($Q > 100$) [3,4]. The tuning of the LC circuit is done through the variable capacitor C_{var} as the inductance of the coil (L_{coil}) is kept constant. The correlation between the resonance frequency (f_{SRF}) and the capacitance value of the capacitor (C_{var}) is given by the Thomson mathematical equation (1), which defines the upper (C_{max}) and lower (C_{min}) capacitance values concerning the upper (f_{max}) and lower (f_{min}) resonant operating frequencies respectively (2,3)

$$f_{SRF} = \frac{1}{2\pi\sqrt{L_{coil}C_{var}}} \quad (1)$$

$$\text{thus, } C_{max} = \frac{1}{4\pi^2 f_{min}^2 L_{coil}} \quad (2) \text{ and } C_{min} = \frac{1}{4\pi^2 f_{max}^2 L_{coil}} \quad (3)$$

To achieve this goal, a variable air gap capacitor (C_{var}) with capacitance values from 18pF to 180pF was chosen for resonance within the MW radio band, while the coil inductance value (L_{coil}) has the constant value of 470μH.

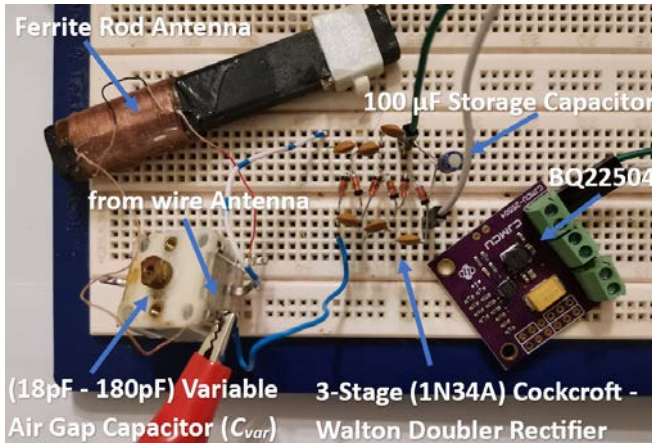


Fig 2. The LC-tuned circuit in the medium wave radio band (530kHz to 1620kHz). The ferrite rod of the coil offers a high-quality factor ($Q > 100$) to the resonant circuit. The tuning is done through the variable capacitor.

To increase the efficiency of a ferrite antenna, parasitic losses due to the ferrite core, DC wiring, and loop radiation resistance must be minimized. Therefore, the quality factor (Q) of the tuned circuit, the antenna loss resistance (R_{ls}), and the radiation resistance (R_r) are the most important parameters for the clarification of a ferrite-based antenna. Consequently, the ferrite core antenna's total loss resistance (R_{ls}) is described given by the following summing in series:

$$R_{ls} = R_{dc} + R_r + R_f \quad (4)$$

As previously noted, R_{dc} , R_r , and R_f are the resistances resulting from DC wiring, the radiation resistance of the loop, and the additional "ferrite loss" for ferrite rods, respectively. The following equation expresses how these resistances relate to the loss tangents:

$$R_{ls} = (tan\delta_{dc} + tan\delta_{ac} + tan\delta_f) \omega L \quad (5)$$

The related loss tangents ($tan\delta$) are provided respectively by

$$tan\delta_{dc} = \frac{4\rho_c l_w 10^9}{\omega A_L N n \pi d^2} \quad (6)$$

$$tan\delta_{ac} = \frac{K_E f N n d^4}{A_L} \quad (7)$$

$$tan\delta_f = K \quad (8)$$

The geometry coefficient (A_L), is determined by the inductance of the coil and its number of turns squared. It is affected by winding perimeter, electrical resistivity, strand number and diameter, proximity effect coefficient of geometry, and ferrite core properties. The parameters K_E and K depend on the characteristics of the ferrite core. MW antennas with ferrite cores have a substantially increased radiation resistance. The resonator radiation resistance (R_r) is denoted by:

$$R_r = 31200 \mu^2 \left(\frac{NA}{\lambda} \right)^2 \quad (9)$$

where N , is the number of coil's turns, μ is the permeability of the ferrite core, A is the core's cross-section, and λ is the wavelength of the detected signal, respectively. Ferrite rods absorb signal power due to the alternating magnetic field flipping the magnetic alignment of domains within the granular structure. Ferrite loss has an equivalent resistance (R_f) for a ferrite rod, as expressed by:

$$R_f = \omega \mu_0 \mu \frac{\mu''}{\mu'} N^2 \frac{A}{l} \quad (10)$$

The quantity μ'/μ'' determines the quality factor (Q) of the ferrite, where μ' and μ'' represent the imaginary and real components of the ferrite's permeability and represents rod length, respectively. The quality factor (Q) and the operating bandwidth (BW) of the circuit are given by the following equations (11) and (12) respectively:

$$Q = \frac{\omega_{SRF} L_{coil}}{R_{ls}} \quad (11) \quad \text{and} \quad BW = \frac{f_{SRF}}{Q} \quad (12)$$

where ω_{SRF} and f_{SRF} are the angular and the self-resonant frequency of the detected signal, L_{coil} is the inductance and R_{ls} corresponds to the loss resistance of the coil respectively, which has the value of 10.5Ω. The quality factor (Q) value varies from 150 to 450 in the proposed tuning circuit.

RF-DC Doubler Rectifier and Boost Converter

The output of the tuned LC circuit indicates the rectifier of the system. A multistage germanium diode-based (1N34A) Cockcroft-Walton rectifier with 100nF blocking capacitors was used for RF to DC conversion. In the prototype implementation, the ability to monitor the output voltage of each rectifier stage is also provided, to obtain additional experimental measurements to select the most efficient number of stages. Subsequently, the harvesting voltage feeds the commercial use DC-DC low power boost converter Texas Instruments BQ22504 [10] for the necessary voltage raising to regulated levels where it can be further used. The BQ22504 is a high-efficiency ultra-low-power boost converter, designed for energy harvesting applications. This device was created with efficiency in acquiring and managing microwatts (μW) to milliwatts

(mW) of power, produced by several DC harvesting sources. It is feasible to start with a V_{IN} as low as 600 mV and continue energy harvesting until the V_{IN} is higher or equal to 130 mV. A storage capacitor (C_s) is placed as the last stage of the system, to store the harvested energy from MW broadcasting signals, capable of driving low-power sensors such as a medical thermometer or a portable calculator.

III. EXPERIMENTAL MEASUREMENTS AND RESULTS

Despite the energy-intensive commercial-use amplitude modulation transmission techniques (*Full-AM*), there are still many transmissions around the world in the medium (*MW*) and long-wave (*LW*) radio bands [6]. In the area of Heraklion, Crete, Greece where this study took place, it is possible to receive about 30 radio programs from a common radio receiver during the night, mainly from emissions originating from countries in the Middle East, South Africa and the Balkans, hundred of kilometres away. To estimate the available power spectral density at the MW radio band (530kHz-1620kHz) in our area, a Keysight VNA N9916A was used, feeding by the horizontal copper wire antenna of the system. The available radio programs with the strongest received signal strength, are shown in Figure 3 and more details such as power transmission, country region etc., are presented in Table I. Figure 4 demonstrates the harvesting (*open-circuit*) voltages induced by these signals, feeding the low-power dc-dc boost converter. Furthermore, continuous experimental measurements were also conducted for 24 hours to assess the stability of the proposed RF-EH system.

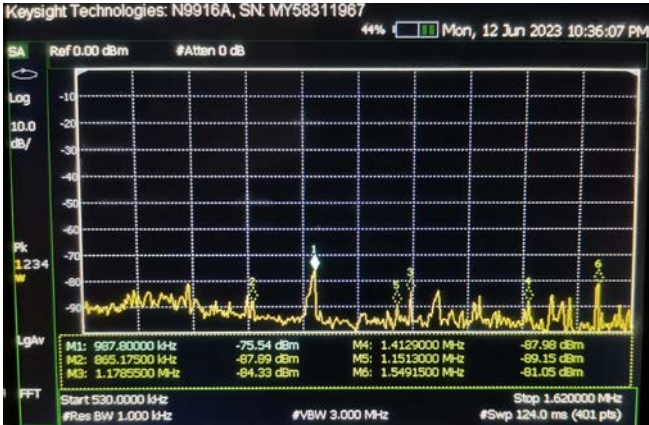


Fig 3. Experimental measurements for the available power spectral estimation in the MW radio band (530KHz to 1620KHz) via the Keysight VNA N9916A in the area of Heraklion, Crete, Greece.

As it was observed, the available power spectral density varies rapidly from daytime to nighttime due to MW radio signals' sky-wave reflection by the layers of the ionosphere, and therefore the harvested voltage ($V_{harvest}$) of the system.

Frequency	Name Station	Country	Transmission Power (kW)
558 KHz	Radio România Actualități	Roumania	400
630 KHz	Radio Timisoara	Roumania	400
711 KHz	Irib Radio Ahwaz	Iran	400
774 KHz	Irib Radio Markazi	Iran	100
855 KHz	Radio Romania International	Roumania	400
864 KHz	NMA Al Quran Al Karim	Egypt	500
999 KHz	Radio Russi	Russia	1000
1179 KHz	SRR România Actualități	Roumania	40
1413 KHz	Radio Vesti	Russia	500
1503 KHz	NMA Al Quran Al Karim	Egypt	25
1512 KHz	SBA Radio Riyadh	Saudi Arabia	1000

Table I. The details of the available MW radio programs with the strongest signal strength received in the area of Heraklion, Crete, Greece.

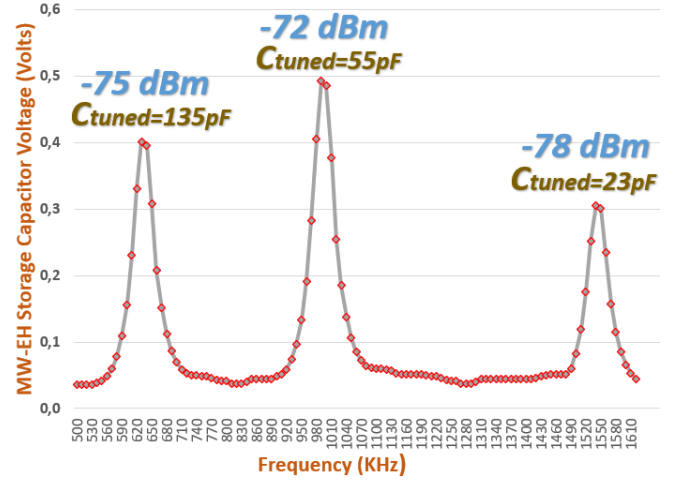


Fig 4. LC tuning at 630KHz, 987KHz and 1549KHz by the capacitance value variation (18pF to 180pF) of the air gap capacitor for MW radio band

RF-EH System Efficiency Determination

For the efficiency determination of the proposed capacitor-based system implementation, it should be noted as a critical parameter that its performance depends on the elapsed charging time. Thus, for the proposed AM harvester, the required time and the achievement harvested voltage of the storage capacitor's full charge were noticed. According to [11], the total efficiency determination is given by (12), as a capacitor-based EH system:

$$n_{RFEH}(t) = \frac{E_{Cstor}(t)}{E_{RF}(t)} = \frac{\frac{1}{2} C_{stor} V_{stor}(t)^2}{t \int_{530 KHz}^{1620 KHz} S(f_{SRF}) A_{eff}(f_{SRF}) df_{SRF}} \quad (12)$$

where $E_{Cstor}(t)$, is the harvested energy at the storage capacitor at time (t) and $E_{RF}(t)$ is the energy of the available RF field (*MW Band*) at time (t). The C_{stor} corresponds to the capacitance value and $V_{stor}(t)$ corresponds to the storage capacitor's voltage at a time (t) respectively. For the RF field energy (E_{RF}) determination at a time (t), the values of the power density S (W/m^2) and the antenna's active surface (A_{eff}) at the target self-resonant frequency (f_{SRF}) of the system should be additionally specified.

MW Radio Transmissions Emulation at the Laboratory

For the complete evaluation of the experimental procedure, radio broadcasts in the medium wave band were also emulated at the laboratory since there are no local radio transmissions nearby. As required by the experimental evaluation, two TTI TG230 laboratory signal generators were used, capable of amplitude modulation (*AM*) from external or internal signal sources. As illustrated in the experimental setup (Figure 6), the transmissions from the laboratory frequency generators gave much stronger signals (up to -45dBm) as shown in Figure 5, essentially simulating corresponding potential local radio broadcastings at a distance of a few kilometers.

Experimental measurements took place at $f_{SRF1}=630KHz$ and $f_{SRF2}=1030KHz$ with variable signal strengths. The (*DC*) harvesting voltage ($V_{harvest}$) can reach up to 2.2 Volts from the receiving signal of -45dBm, caused by the experimental transmission of the laboratory generator and can fully charge the 100μF storage capacitor (C_s) of the proposed EH

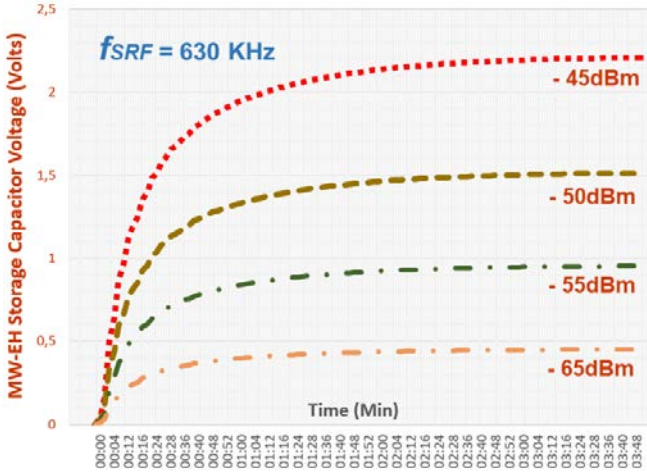


Fig 5. MW-radio transmissions at $f_{SRF}=630\text{KHz}$ in the laboratory by utilization of TTI TG230 signal generator for local broadcasting emulation.

system in about 4 minutes, as shown in Figure 5. The charging curves of the storage capacitor (C_s) show that the maximum charging voltage is directly proportional to the received signal strength in the tuned circuit. The behaviour of rectifier diodes is highly dependent on signal levels, affecting the equivalent resistance ($R_{thevenin}$) of the rectifier circuit and resulting in a variable time constant (τ). It should be noted that in this scenario, the DC-DC boost converter was not necessary for use, due to the high value of receiving signal strength. A medical thermometer was powered by the $100\mu\text{F}$ storage capacitor (C_s), which can normally operate at 1.5V with $29\mu\text{A}$ current consumption. As a result of the obtained measurements, the resistance of this device has a value of $51.7\text{K}\Omega$. If we consider that:

$$\tau_{\text{discharge}} = R_{\text{load}} C_{\text{storage}} \quad (13)$$

for these components' setup the discharge constant time ($\tau_{\text{discharge}}$) is 5.1 sec. Thus, is sufficient to power this low-consumption device until the safety threshold voltage of 1.3V for about 2.7 sec, with the initial capacitor's charged voltage of 2.2Volts, caused by the receiving signal of -45dBm. The storage capacitor of the system could be replaced with a larger one ($220\mu\text{F}$) requiring twice the charging time (about 8 minutes), thereby extending the power-up time of the low-power device to 6 seconds up to the safety threshold voltage (1.3V) with the same experimental requirements.



Fig 6. The experimental setup by the utilization of TTI TG230 laboratory signal generators with Amplitude Modulation (*Full-AM*) features.

IV. ACKNOWLEDGMENTS

«The implementation of the doctoral thesis was co-financed by Greece and the European Union (European Social Fund-ESF) through the Operational Programme «Human Resources Development, Education and Lifelong Learning» in the context of the Act «Enhancing Human Resources Research Potential by undertaking a Doctoral Research» Sub-action 2: IKY Scholarship Programme for PhD candidates in the Greek Universities» (MIS-5113934).



Operational Programme
Human Resources Development,
Education and Lifelong Learning
Co-financed by Greece and the European Union



V. CONCLUSIONS

The proposed approach demonstrates the implementation of an RF-EH system by the ambient AM radio broadcasting utilization, enabling powering low-consumption applications. The proposed AM harvester consists of a long copper wire antenna, an LC tuning circuit, a germanium diode-based (1N34A) Cockcroft-Walton rectifier and a storage capacitor of $100\mu\text{F}$, driven by a commercial DC-DC boost converter. Experimental measurements were shown that the harvesting voltage can reach up to 2.2 Volts and can fully charge a $100\mu\text{F}$ storage capacitor in about 4 minutes. As a result, from this voltage a medical thermometer can be powered for 2.7 sec until its safety threshold of 1.3 Volts.

REFERENCES

- [1] K. Xie, Y.-M. Liu, H.-L. Zhang & L.-Z. Fu (2011) Harvest the Ambient AM Broadcast Radio Energy for Wireless Sensors, Journal of Electromagnetic Waves and Applications, 25:14-15, 2054-2065.
- [2] X. Wang and A. Mortazawi, "Medium Wave Energy Scavenging for Wireless Structural Health Monitoring Sensors," in IEEE Transactions on Microwave Theory and Techniques, vol. 62, no. 4, pp. 1067-1073, April 2014.
- [3] S. Cao and J. Li, "A High-Efficiency Twin Coil Ferrite Rod Antenna for RF Energy Harvesting in AM Band," 2017 5th International Conference on Enterprise Systems (ES), Beijing, China, 2017, pp. 276-280.
- [4] Dyo, V., Ajmal, T., Allen, B., Jazani, D. and Ivanov, I. (2013), Design of a ferrite rod antenna for harvesting energy from medium wave broadcast signals. The Journal of Engineering, 2013: 89-96.
- [5] Leon-Gil, J.A.; Cortes-Loredo, A.; Fabian-Mijangos, A.; Martinez-Flores, J.J.; Tovar-Padilla, M.; Cardona-Castro, M.A.; Morales-Sánchez, A.; Alvarez-Quintana, J. Medium and Short Wave RF Energy Harvester for Powering Wireless Sensor Networks. Sensors 2018, 18, 768.
- [6] S.Otsuka, N. Nakashima "Experimental Results on Energy Harvesting by Using AM Radio Broadcasting," 2014 9th International Conference on Broadband and Wireless Computing, Communication and Applications, Guangdong, China, 2014, pp. 347-35.
- [7] Bezboruah, Tulshi & Thakuria, Tapashi & Singh, Hidam. (2021). Design and simulation of medium wave-based RF energy harvesting system with feedforward controlled DC to DC boost converter. International Journal of Power Electronics. 14. 1.
- [8] X. Wang and A. Mortazawi, "High sensitivity RF energy harvesting from AM broadcasting stations for civilian infrastructure degradation monitoring," 2013 IEEE International Wireless Symposium (IWS), Beijing, China, 2013, pp. 1-3.
- [9] X. Wang and A. Mortazawi, "A self-sensing AM frequency electromagnetic energy scavenger," 2013 IEEE MTT-S International Microwave Symposium Digest (MTT), Seattle, USA, 2013, pp. 1-3.
- [10] Texas Instruments BQ25504 "Ultra-Low-Power Boost Converter with Battery Management for Energy Harvester Applications".
- [11] Tampouratzis, M.G.; Vouyioukas, D.; Stratakis, D.; Yioultsis, T. Use Ultra-Wideband Discone Rectenna for Broadband RF Energy Harvesting Applications. Technologies 2020, 8, 21.

The Future of Privacy: A Review on AI's Role in Shaping Data Security

Marios Vardalachakis¹, Manolis Tampouratzis¹, Konstantinos Karampidis¹,

Giorgos Papadourakis¹, Nikolaos Papadakis¹

¹Department of Electrical and Computer Engineering (ECE), Hellenic Mediterranean University (HMU)

Heraklion GR 71004 Greece

mariosvardalachakis@gmail.com, tampouratzis@hmu.gr, karampidis@hmu.gr, papadour@hmu.gr, npapadak@hmu.gr

Abstract—The rapid adoption of Artificial Intelligence (AI) technological advances marked an era of exceptional growth, significantly converting how we interact with the world of technology. But this adoption has arrived at an enormous cost: the gradual loss of private life. The article starts with an in-depth investigation into the complicated and modifying relationship between AI and privacy, acquiring information via case studies in the real environment. The deployment of powered by AI technology for recognizing faces in public spaces is one prominent case study. Issues around illicit tracking and intrusions of privacy have grown as governments and business entities employ such technologies regularly for recognition and protection reasons. Assessing both the challenges and findings associated with such deployments offers the conceptual debate a practical setting. It explores the various challenges that arise from AI-driven innovations and offers fresh strategies for maintaining and safeguarding individual privacy concerns in emerging data-centric circumstances. It emphasizes AI's dual role as a catalyst of outstanding outcomes and also as a potential risk for personal privacy. Finally, this article is interested in contributing to the current discussion on AI and Privacy, by providing an in-depth examination of the difficulties that might be utilized by lawmakers, stakeholders in the industry, as well as individuals alike. As humanity moves into a scenario where AI encompasses every aspect of daily life, the study acts as a guide for managing the evolving terrain concerning confidentiality in the era of AI, assisting appropriate AI advancement and preserving human privacy rights.

Keywords—Artificial Intelligence (AI), Privacy, Challenge Strategies, Ethics, Confidentiality, Data Collection, Data Breaches, Artificial Bias.

I. INTRODUCTION

The birth of the technological age brought an era of exclusive relationships and innovation based on data. Artificial intelligence (AI) is a revolutionary power in the digital age of today, changing organizations, economies worldwide, and societies. The capability of AI to assess huge amounts of data, expect results, and automate procedures has contributed to its quick formation into various areas of daily life, from modified personalized recommendations to self-driving automobiles. Yet this revolution in technology has led to an enormous issue that affects each phase of our daily lives [1]. While artificial intelligence (AI) features grow and reach various sectors, the huge quantities of data essential for its development and execution have caused an abundance of issues related to the maintenance of individual privacy. Combining AI's tremendous potential with the need to protect personal information represents one of the most significant issues of today's world. The disagreement involving the huge advantages of AI and its invasion of human privacy is the fundamental narrative of this era, and its conclusion is going

to affect the direction of our common fate [2]. The rest of this study is organized as follows: Section II will cover the difficult combination of AI and Privacy. Section III will cover all aspects of the challenges to Data Privacy in the age of AI. Section IV will address the strategies for Data Privacy in the Age of AI looking at how stakeholders ranging from governments to technologists and individuals can work together to overcome these problems and guarantee that the AI-driven future respects human privacy. Section V analyze the topic of Privacy by Design and also talk about Open AI Security Measures. Lastly, section VI makes predictions regarding the way AI and privacy will evolve in the not-too-distant future by predicting advances in AI that prioritize and protect privacy.

II. THE COMBINATION OF AI AND PRIVACY

Humanity has reached an important point in the age of digitization, as technological progress, prompted by artificial intelligence (AI), conflicts with the fundamental right to privacy [3]. The rapid development of AI technology has marked an era of simplicity, productivity, and possibilities that were previously unimaginable [4]. But to welcome these successes, we must also tackle the complicated frequently weak relationship between AI and privacy with the design of AI systems that do not compromise users' privacy and security [5]. This complex shift lies at the core of present-day debates concerning the ethics, compliance, and cultural implications of artificial intelligence, which require us to find an agreement that promotes innovation and freedom of speech [6]. It is crucial to examine the complex and frequently unstable connection between artificial intelligence (AI) and privacy as we find ourselves at the intersection of innovation and individual rights. But among all of these technical considerations, there are complex moral quandaries which require to be answered right now. The combined effect of AI and privacy shows an assortment of difficulties and worries that blur conventional boundaries. Artificial intelligence (AI) offers an important effect on many aspects of daily life, from the efficient operation of autonomous vehicles to the predicting capabilities of robotic advisors. The huge quantities of personally identifiable information obtained in the process—often known as the "new oil" of the current era—ultimately motivate AI's progress as well as its ability to judge. But among all of these technical wonders, there are complex ethical issues that need to be addressed right now [7]. In addition, when such information gets used or victimized, it may end up in a number several breaches, including annoying observing to information stealing [8]. In an era where machines carefully make conclusions regarding how we live, privacy, an essential component of contemporary democratic nations, is threatened. Imagine a

case study of AI-powered recognition of face systems utilized in open spaces. While these advances offer unequalled powers for personal safety and identity identification, they additionally provide reason for issues over illegal tracking and violations of privacy [9]. Exploitation circumstances, which include aggressive reconnaissance to data loss, demonstrate the complex challenges involving the intersection of artificial intelligence and privacy. The objective of the article is not to automatically reject AI or hinder its progress, but instead, to attempt to press for a deeper awareness of the delicate balance that needs to be achieved to ensure that the beneficial effects of AI can be realized while preserving the integrity of individual privacy. We are going to start on a journey across the following sections to build the delicate harmony between AI and privacy. While trying to explore the remaining parts in place, we run upon crucial concerns. In what way will we protect our ethical standards and laws while employing AI to its greatest prospective? Most of all, exactly how can we discuss this constantly shifting landscape to establish an era where data and AI cohabit harmoniously? Knowing the fact that there doesn't seem one solution that's right for anyone, the next stage in this procedure is to find out the beginnings of this intricate and massive system of life. The purpose is to make certain that the unlimited benefits provided by artificial intelligence can be employed while sustaining the fundamental principles of individual security and privacy. The variations, challenges and prospective solutions that exist at the intersection of privacy and AI are going to be addressed in depth in the sections that follow. The necessity for careful negotiation can be demonstrated by particular situations, moral dilemmas are going to be addressed in greater depth, and an improved understanding of the challenges at face will serve as foundations for a thorough inquiry. Our aim once we embark on this path is to preserve the beliefs that the world considers important despite not merely handling complexities but also establishing the foundation for the development of the following era of AI.

III. CHALLENGES TO DATA PRIVACY IN THE AGE OF AI

The latest artificial intelligence (AI) advances have resulted in an era of innovation and productivity in a wide range of fields. AI systems powered by huge amounts of data can modify how we live in an assortment of manners, starting with personalized medical care to autonomous automobiles [10]—these enhancements, still present major challenges to data privacy. As artificial intelligence (AI) grows increasingly and is integrated throughout everyday activities, it generates concerns as to the way individual data is collected, employed, and secured. The integration of AI along with data privacy leads to complexities in the fast-growing field of AI, demanding an extensive understanding of everyday life scenarios, trade-offs, and broader ethical factors [11]. To provide an enhanced awareness, this article explores the main challenges to data privacy in the age of AI and indicates potential solutions.

A. Permissions and Data Collection

The enormous amount of data brought together represents one of the primary challenges to data privacy in the age of AI. To acquire knowledge effectively AI systems, demand huge datasets, which frequently include individual data. The

problem is two-fold: Firstly, individuals could be unclear of the depth that their data has been collected secondly acquiring explicit authorization for data collection can be challenging. To tackle this problem, organizations need to be open concerning their data-collecting laws while offering simple, straightforward approval operations. Laws that include the General Data Protection Regulation (GDPR) of the European Union have set guidelines for obtaining explicit authorization while giving individuals access to their data. Compliance with such requirements, along with the development of easy-to-use agreement connections, constitutes vital stages in solving this problem [12].

a. Real-World Scenarios: A Summary of Concerns About Privacy

We refer to real-life scenarios that demonstrate the complicated nature and consequences resulting from these connections as a way to better understand the challenges that lie at the boundary of AI and privacy. The widespread adoption of face recognition software in public spaces is part of one recognized case study. This sort of technology is utilized by organizations and governments throughout the globe for a wide range of related tasks, which include customer support, personalized advertising, and criminal justice and defence [13]. However, as a result of its expansive consumption, there are reports of illegal monitoring, intrusions of privacy, and greater concerns about the misuse of data. It becomes clearer that this is a trade-off involving enhanced productivity and safety and a reduction in privacy for individuals [14].

b. Trade-Offs in AI Approaches for Maintaining Privacy

AI approaches that guarantee privacy, such as homomorphic encryption differential privacy and federated learning, offer robust protection towards concerns about confidentiality. On a greater level, however, trade-offs are clear. Imagine homomorphic encryption, an approach that enables computing on encrypted data eliminating any requirement for data recovery [15]. Though data security is ensured, issues arise about the computation cost. The trade-off is in improving these approaches for application in real life while achieving a careful balance between computing speed and privacy protection [16].

c. Regional and Ethical Data Privacy Issues

The issues that arise aren't restricted to individual instances they are worldwide in scale. As AI has been created and utilized all over the world, it is essential to carefully look at worldwide moral dilemmas. It remains a challenging endeavour to create consistent guidelines and rules, demanding awareness from various ethical, moral, and cultural settings [17]. Despite fundamental beliefs, moral considerations additionally consider the advantage of cultural differences which have to be understood in the interest of protecting fundamental freedoms for all people.

B. Data Breaches and Security

The increasing reliance on AI systems has boosted the worth of personal data, which makes it a desirable target for hackers. Data breaches could have catastrophic impacts involving theft of identities, financial damage, and negative publicity. When AI systems process more and more important data, the possibility of incidents involving data rises [18]. To deal with this problem, organizations have to

invest in comprehensive data security measures that include encryption, accessibility restrictions, and regular security inspections. Personal data-processing AI algorithms ought to be developed without privacy in thoughts, such as methods that include federated learning, that enable models to be trained to solve a problem. Due to the complex nature underlying the AI-privacy nexus, an extensive and cross-disciplinary approach such as scientists, ethicists, politicians, and the broader community is needed [19]. We aim to shine an insight into the challenging material of AI and privacy with our inquiry, eventually assisting in the building of an increasingly equal, transparent, and privacy-conscious AI on distributed information while exposing private information. Also, legislators ought to set strong fees for data breaches to persuade them to give priority to data security.

a. Real World Scenarios: HealthCare Data Breach

AI is employed in the healthcare industry to assess patient data and offer customized treatment ideas. On the other hand, when confidential medical information becomes compromised, it may end up in data theft, financial damage, and loss of the healthcare vendor's image [20].

b. Trade-offs: Security Policies versus Effectiveness

Companies are frequently unable to find an appropriate balance between enforcing rigorous safety regulations and retaining their operational effectiveness in the constantly evolving field of cybersecurity. The trade-offs engaged in this contrast provide an intricate issue that requires an in-depth analysis of every possible solution and an in-depth knowledge of how the risk scenario is shifting. Strong security laws, which are crucial for maintaining sensitive data and systems, are situated on one side of the trade-off range. Implementing guidelines requiring encryption rules, restricting access, and ongoing checks for safety assists organizations in boosting their barriers against cyberattacks. The laws, particularly are built on standard procedures and compliance requirements, which serve as vital to decreasing the probability of data breaches and ensuring compliance with the law. On the other hand, tight attention to safety measures can sometimes be seen as difficult, which could limit regular activities' adaptability and productivity [21]. Understanding the complicated world of user interfaces and process design can often be needed to achieve the correct balance between security measures and operational efficiency. Multifactor authorization and complex password demand, for instance, enhance security but can result in complexity in interactions with users and suffer from the general user experience. Strong limits on access that prevent the availability of data might additionally hinder quick choices and collaboration, especially in situations where rapid sharing of data is needed [22].

c. Global and Ethical dimensions

Data breaches in the healthcare sector are an international concern with significant ethical and global implications which impact medical systems throughout the globe. They aren't restricted to regional problems. One of the biggest challenges affecting the world nowadays is finding out the complex structure of data ownership. Sensitive patient data related to medical procedures is frequently transferred beyond international borders, creating concerns about

complying with multiple data protection guidelines. Organizations have to confront the complicated world of processing and storing information rules, ensuring confidence that how medical data is managed adheres to worldwide regulations. Since data breaches can undermine trust among communities in transferring important health information, this raises the importance of collaboration across borders, particularly for biomedical research and international health projects. Furthermore, there is a worldwide scope for cybersecurity attacks against healthcare institutions. Since malicious actors may exploit weaknesses from anywhere in the world, international cooperation in cybersecurity initiatives is essential. Information exchange, collaborative efforts, and a dedication to strengthening the resilience of healthcare infrastructures worldwide are all necessary components of a united front against cyber threats. Because healthcare systems are interconnected, everyone must safeguard patient data from cyberattacks, underscoring the necessity of international cooperation in the development of effective cybersecurity measures [23].

C. Discrimination and Artificial Bias

When acquainted with biased data, AI systems may extend and even cause continuing preconceptions. This may lead to discriminating implications such as unfair job decisions unfair approvals for loans, or ethnically discriminatory actions by law enforcement [24]. Eliminating bias caused by algorithms is an essential barrier to the privacy of data and fairness in artificial intelligence. To tackle this problem, organizations need to invest in broad and fair datasets to help train AI models and additional algorithms that constantly detect and mitigate prejudicial opinions [25]. Regular reviews and willingness in AI processes to make decisions may assist in identifying and correcting signs of bias. In addition, regulators ought to create standards for responsible utilization of AI and conduct reviews to guarantee agreement.

a. Real World Scenarios: Technology for facial recognition

Technology for facial recognition is employed by private companies and authorities for authentication and surveillance. This has already been proven that these mechanisms have both gender and racial biases, that may end up in misidentifications and possibly unfair results, especially for women and persons of race [26].

b. Trade-offs: Accuracy vs Fairness

Stronger algorithmic restrictions and actions intended for minimizing bias could undermine the AI system's accuracy, causing the potential for inaccurate results and the removal of applicants who are eligible [27].

c. Global and Ethical dimensions

The international effects of these advances are made apparent by the worldwide consequences of artificial bias and prejudice in AI. Considering the increasing worldwide implementation of AI systems, the adaptability of biased algorithms has a chance to strengthen and potentially amplify disparities in society. When executed in different cultural settings, the biases incorporated into AI models produced in a single setting may inadvertently cause discrimination. Therefore, confronting the global elements of bias demands collaboration to set up social systems and

regulations that exceed national borders. Creating a worldwide AI environment that upholds equality and different cultures demands an equal dedication to bias prevention as a way to find an agreement between invention and accountable adoption. Equal treatment, responsibility, and freedom are essential ethical considerations in the area of bias and produced discrimination. In AI development, respecting people completely no matter their past is a fundamental ethical principle. To be able to offer clients an understanding of how systems conduct themselves, openness becomes important and programmers must explain how they make decisions about their algorithms. When trying to solve circumstances when bias causes unfair effects and establish an environment of ethical innovation in AI, responsibility approaches are important. Furthermore, ethical AI needs ongoing assessment and creation, realizing that minimizing bias is an ongoing task involving reacting to new standards of ethics and merging numerous perspectives to create technology that is by common human principles.

D. Privacy - Preserving AI

This may lead to Combining the positive aspects of AI via data privacy is a challenging task. Differential privacy and homomorphic encryption constitute two privacy-preserving artificial intelligence methods that aim to enable AI systems to work while preserving sensitive data. However, effectively integrating these techniques can be challenging as they usually involve computing costs. Corporations ought to make investments in the study and creation of privacy-preserving AI solutions to address this problem. The grants, tax credits, and rules and regulations are all options available by authorities to foster the utilization of these tactics. AI could consequently continue making improvements while preserving data privacy [28,29].

a. Real World Scenarios: Cooperation in health research

While examining patient data for health research, experts from various medical institutions cooperate to search for patterns as well as potential treatments. Differential privacy [30] ensures the confidentiality of patients throughout cooperation investigation efforts by enabling the exchange of private health information while revealing sensitive data.

b. Trade-offs: Privacy vs Utility

More restrictive encryption or differential settings for privacy are a pair of higher privacy measures that often come with the unintended effects of rendering AI systems less helpful or effective [31]. It became important for establishing tradeoffs amongst the demands for reliable significant findings along with robust privacy protection.

c. Global and Ethical dimensions

The search for an integrated system recognizing the rights of individuals throughout varying cultures and legal environments is an intersection of the worldwide and ethical aspects of privacy-preserving AI. Around the world, the challenge is in harmonizing different standards and norms about data privacy to allow efficient collaboration across borders. International privacy rights must be maintained while managing the complicated landscape of cross-border transfer of data, requiring the development of universal guidelines. Equal treatment, accessibility, and diversity are given the highest priority by moral standards in the

development and utilization of privacy-preserving AI. This involves ongoing examination to protect against biases, open communication on systems functioning properly, and assuring that the positive benefits of AI are accessible and shared properly [32].

E. Ethical Considerations

A further significant issue is the legal adoption of AI in terms of data privacy. Organizations must ensure that artificial intelligence systems honor people's freedoms as well as not compromise privacy in the interest of creativity or revenue. This demands compliance with legal AI requirements and also moving forward with legal examinations of AI applications. A further significant issue is the legal adoption of AI in terms of data privacy. Organizations must ensure that artificial intelligence systems honor people's freedoms as well as not compromise privacy in the interest of creativity or revenue [33]. This demands compliance with legal AI requirements and also moving forward with legal examinations of AI applications. To solve this problem, companies ought to establish moral AI frameworks that control AI creation and utilization [34]. They should also encourage transparency and responsibility in AI systems, permitting individuals to learn about and match computational decisions that harm their privacy. Data privacy is a fundamental issue in the modern era of AI, and dealing with the related challenges is essential to achieving the full potential of AI while preserving people's rights and data security. Companies, authorities, and people need to collaborate cooperatively to come up with and complete strategies that facilitate sustainable AI creation and utilization. We can start preparing the path for a time in which AI and data privacy cohabit by jointly managing fears such as collecting data, security, bias, privacy-preserving methods and principles [35].

a. Real World Scenarios: AI and Data Privacy

Consider a scenario when a social networking site utilizes advanced AI algorithms to choose stuff that is unique for each user, when an application tries to present customized material that enhances its user interface while maintaining users' fundamental right to privacy while preventing algorithmic bias, moral problems become increasingly significant.

b. Trade-offs: Integrity in opposition to exclusive algorithms

The site has to choose either offering clients an understanding of how they make choices while remaining transparent regarding the way its algorithm picks and organizes information and preserving the confidential character of its algorithms—which might be considered to be proprietary information.

c. Global and Ethical dimensions

The difficulty in the global and ethical environment of AI and data privacy is to establish an international framework that protects individual freedoms in a wide range of regulatory and cultural environments [36]. Around the world, it's essential to strike a balance between various standards and requirements regarding data privacy to facilitate efficient cooperation across borders. To develop globally accessible principles and a worldwide knowledge of privacy that takes into consideration an array of cultural

perspectives and regulations, collaborations are needed. Equal treatment, accessibility, and integration are given the highest priority by moral obligations in the development and application of AI. This requires constant examination to protect against biases, open communication on the system working, and assuring that the benefits of AI are accessible and distributed equally. A further barrier of moral dilemmas arises when individuals obtain meaningful choices, which underlines the need for an ethical and global approach to AI that fits with different legal frameworks and cultural standards. By achieving this right balance, we can be certain that AI expands worldwide while conforming to ethical principles, which will be beneficial to a diverse and integrated global community [37].

In conclusion, the period of adverse AI brings exceptional progress while also facing difficulties in the privacy of data. Leveraging the potential benefits of AI without safeguarding people's rights needs transparent data-acquiring techniques, adherence to regulations which includes GDPR, and accurate safety procedures. Moral challenges, which include dealing with bias and discrimination, require expenditures for inaccessible datasets and trustworthy artificial intelligence frameworks. Real-life scenarios including facial detection biases and breaches of health data emphasize the significance of the circumstances at hand. Also, the world's legal and moral aspects demand to work together to bring together guidelines, appreciate various points of view, and guarantee equal consideration, highlighting the need for trustworthy artificial intelligence operations to be compatible with respect for privacy in our increasingly connected humanity.

IV. STRATEGIES FOR DATA PRIVACY IN THE AGE OF AI

Apart from the challenges that exist and are described in the previous section appropriate data privacy laws and strategies must be implemented to strike an appropriate equilibrium between applying the potential of AI and preserving the privacy of individuals. Below are a few strategies that individuals and businesses can employ to enhance the confidentiality of information in the modern day of computational intelligence.

a. Data Minimization

Firstly, the aspect of Data minimization is important because this prevents the dangers that a company keeps a large quantity of personal information. This approach acquires and stores only the amount of data needed for a particular reason. Audit and get rid of data which is no longer necessary [38].

b. Privacy by Design

Privacy By Design becomes an initial preference, promoting the implementation of data privacy principles from the very beginning of the development and creation of AI systems. From beginning to end, we must incorporate a privacy-enhancing technological advance that includes encryption and accessibility constraints [39].

c. Openness

Openness is paramount, which means being truthful and forthcoming regarding your data gathering, utilization, and handling procedures. Educate individuals about how their personal information will be disclosed and utilized ask for

their written permission and provide straightforward user interfaces for obtaining and handling permissions [40].

d. Federated Learning

Federated Learning employs collaborative learning techniques, which permit AI models to be trained on distributed data without having to exchange every record. This approach permits companies to utilize data for training models without risking the security of users [41].

e. Anonymization vs Pseudonymization

Data Anonymization and Pseudonymization play significant roles in reducing the possibility of re-identification we must choose between Anonymization or pseudo-anonymization of data. Anonymization prevents personal information, but pseudonymization alternatives personally identifiable data with false identities, rendering data connection a bit harder [42].

f. Data Encryption

Businesses also must utilize strong encryption technologies that protect data whilst it's in transmission as well as idle status. If a breach takes place, encrypt sensitive information to avoid unintentional disclosure. Implement robust handling of key processes [43].

g. Ethical Principles

Businesses should also Establish and adhere to legal artificial intelligence creation and utilization requirements and guarantee that artificial intelligence technologies are applied in manners which preserve human rights while preventing adverse effects. Analyze the cultural and social effects of applications of AI [44].

h. Data Availability and Monitoring

Individuals need to be allowed greater influence over their personal information and give them ways to see, precisely, or eliminate their data and later adopt information transfer guidelines that enable users to migrate their data from one provider to elsewhere [45].

i. Agreement with Regulations

Lastly, individuals must remain updated on privacy laws like GDPR and CCPA along with other laws that apply [46].

V. PRIVACY BY DESIGN: OPEN AI SECURITY MEASURES

Securing one's privacy has grown increasingly crucial as artificial intelligence (AI) starts to impact the technology world. A key plan of action for addressing the problem is the concept of "Privacy by Design." As a way to make sure that privacy is not a secondary consideration but a vital part of the design procedure, this aggressive technique involves integrating concerns about confidentiality into the basic structure of AI systems throughout their creation [47].

a. Integrating Privacy Rules Immediately

AI system designers require an important change in mindset for them to accomplish Privacy by Design. It focuses extreme value on incorporating privacy notions throughout projects from the very start, observing them as an essential element as opposed to a workaround. From the very start of system architecture, developers must consider the moral consequences of data utilization, analysis, and preservation into consideration [48].

b. Limits over Accessibility and Cryptography

A key component of Privacy by Design involves placing strong encryption and access limits in effect. AI systems can secure sensitive data by encrypting it during transport as well as when it is at rest. To minimize the risk of illegal accessibility, control mechanisms ensure that only authorized individuals or procedures have proper permissions to interact with specific datasets [49].

c. Technologies that Increase Your Privacy

Technology that boosts privacy must be researched and combined, as recommended by Privacy by Design. Technologies like homomorphic encryption and differential privacy are crucial for enabling AI systems to complete operations while securing private information. Deployment of these technologies will be essential for finding an appropriate balance between data privacy and AI innovations, even if these could result in higher calculating expenditures [50].

d. Algorithm Formulation with Ethical Concerns

Privacy by Design depends primarily on the design of algorithms that consider principles into consideration. To prevent skewed outcomes, developers must make an effort to identify and minimize biases in AI systems. To increase trust and ensure fairness, AI decision-making systems must be accessible and exposed to ongoing examinations.

e. Openness Based on Individuals

The primary objective of Privacy by Design is to focus on users' openness. AI systems have to be developed with graphical user interfaces which make it clear how personal data will be collected, managed, and exploited. To continue to establish trust across users and AI applications, it's now important that they obtain accurate authorization via easy authorization procedures.

f. Continuous Analysis and Advancement

Ongoing evaluation and enhancement form a component of the extending procedure for adopting Privacy by Design. Developers have to maintain a close eye on and analyze how AI systems impact privacy, modifying whenever necessary to address novel challenges and adhere to evolving standards and laws [51].

In conclusion, Privacy by Design is a responsible and vital strategy for addressing any potential risks to privacy related to AI. We may encourage creativity while respecting freedoms for individuals if privacy concerns are incorporated into the underlying structure of AI system creation. So additionally mitigating potential issues with privacy caused by AI, privacy by design offers an environment that fosters innovation while protecting individual rights. The approach looks at the moral dilemmas of AI technology along with the value of safeguarding sensitive data. This section highlights the value of a conscious cognitive change, acceptance of technology that enhances privacy, and ongoing efforts to promote ethical and transparent AI operations.

PRACTICAL IMPLEMENTATIONS IN BUSINESSES

The practical application of these strategies demands a fundamental change in everyday operations and choice-making procedures for companies. Implementing data

minimization requires the adoption of specific data oversight regulations, which include common data significance assessments and frequent changes to storage rules. Privacy by design should be built into the framework of AI system development, requiring cooperation across data scientists, engineers, and legal teams to incorporate privacy-enhancing technology into its basic design. Openness can be seen in graphical user interfaces as an organizational benefit, providing everyone have an open view and authority over their data. Federated learning requires a collaborative approach when organizations establish collaborations or teams to learn AI models collaboratively without risking individual data privacy. Training for staff members could be utilized to establish ethical AI frameworks and determine an environment of ethical AI deployment. Also, privacy laws and advanced encryption technology need to be included in regular IT processes, ensuring data protection is an automatic part of business operations.

PRACTICAL IMPLEMENTATIONS IN INDIVIDUALS

Individually, running these approaches starts with aggressive permissions and data access control. Individuals should review and revise their security settings on online services on a regular schedule, having power over the level with which their data is exposed. Data anonymization and pseudonymization involve being aware of the information considered via the internet and decreasing identifiable information. Individuals can support platforms that highlight privacy-preserving AI models, relating what they do with moral concerns. Individuals must engage with privacy rules and test data collection practices to be trained about privacy laws and fight for their rights. When communicating online, utilizing data encryption approaches offers a greater level of privacy to sensitive data. Ethical issues have been an overarching principle for online conversations, allowing people to choose products and services that comply with ethical AI criteria. Individuals' daily use involves establishing a careful and informed approach regarding online connections, permitting them to thrive in the AI world and protecting their privacy.

The strategies mentioned offer a roadmap for businesses and individuals to establish a path beyond the age of AI by dealing with the complex integration of Artificial Intelligence (AI) and data protection. The need for businesses is to drive modifications around data minimization, privacy by design, and openness as fundamental values. Practical implementation of such strategies requires strong oversight of data, shared development actions, and a cultural dedication to trustworthy artificial intelligence frameworks. Businesses can boost data privacy while promoting responsible AI innovation through using federated learning and tackling compliance with regulations. Individuals need to take an active role in managing credentials, anonymizing data, and advocating against individual rights to continue to create a privacy-conscious online environment. Employing encryption techniques along with making recommendations that consider moral issues enhances an individual's data protection place. In basic terms, the combination of such strategies leads to an integrated approach to AI and data privacy that lets individuals and companies collaborate to

secure personal information. While the AI environment changes, this interactive dedication to the appropriate use of data guarantees a future in which development exists with the maintenance of the essential right to privacy. The barriers are crucial, but through employing these strategies, both organizations and people can together guide into a future in which the potential benefits of AI become a reality without risking the underlying thread of privacy.

In conclusion, maintaining data privacy in the modern age of AI demands a holistic strategy that includes scientific, company resources and constitutional precautions. Individuals and businesses can manage the challenges that are presented by AI while preserving critical individual information by employing these techniques and creating a privacy environment. This holistic strategy is for addressing the intricate nature of AI while complying with fundamental confidentiality rules in the constantly evolving field of technology as well as data governance.

VI. PREDICTIONS FOR THE NEXT GENERATION: ADVANCEMENT IN AI THAT RETAINS PRIVACY

Researchers as well as professionals are constantly researching innovative methods and technologies to enhance security for privacy as the discipline of artificial intelligence (AI) and data privacy keeps evolving. The following part analyzes new developments that could contribute to addressing privacy issues in the not-so-distant future.

a. Federated Learning

Federated Learning is currently an innovative approach to AI privacy protection. Utilizing this technique, machine learning models may be collaboratively trained without needing initial information sharing for distributed devices or platforms. Instead, individual data privacy is preserved through shared-only modifications to the model. Federated Learning is an option for circumstances in which privacy and data residence regulations are restrictive as it enables AI systems to collect insights from a range of datasets without risking the privacy of the individual users [52].

b. Homomorphic Encryption

A major development in the protection of sensitive data throughout computations by AI is homomorphic encryption. With the help of this cryptographic approach, data that is encrypted can be instantly relied on with no need for decryption. Encrypted data is analyzed by AI models however its initial data stays private. This maintains user privacy while allowing safe participation in circumstances where sharing information is essential [53].

c. Differential Privacy

In privacy-preserving research on artificial intelligence, differential privacy remains essential. The aforementioned approach adds noise to each of the data points, making it hard to figure out how each statistic relates to the larger model. Differential privacy assists in safeguarding against potential retrieval or unwanted disclosure of private information through the inclusion of regulated randomness throughout the processing of data. Differential privacy remains an essential approach for safeguarding personal privacy [54] as AI systems utilize increasingly bigger datasets.

d. Methodologies for Machine Learning maintaining Privacy

There is currently an increasing amount of research being carried out on machine learning models that emphasize privacy preservation. Academics are looking at patterns that foster confidentiality of information by standard, despite affecting system performance. Models like these seek to achieve an acceptable balance across privacy and accuracy, allowing the ability to gain the positive effects of AI without violating individuals right to privacy [55].

e. Ethical AI Governance Frameworks

Considering the arrival of those innovative technologies and strategies, privacy in the era of artificial intelligence has a promising future. Federated Learning, Homomorphic Encryption, Differential Privacy, and Privacy-Preserving Machine Learning Models offer methods to balance the requirement for protecting individual confidentiality with the potential for change of AI. In addition, an ethical AI governance framework's development and execution demonstrate a commitment to ethical AI principles. These advances open the way to a future where robust privacy protections and AI-driven innovation exist [56].

CONCLUSIONS

While Artificial Intelligence keeps occurring to alter our environment, preserving individual privacy remains ever more crucial. Due to the complicated nature of the connection between AI and privacy, an integrated approach involving technical, managerial, and legal protections must be found. Societies may accept the possibilities of AI without preserving essential rights for all by confronting the challenges raised by AI-driven developments through privacy-protection choices. This article offers an outline for traversing the evolving environment of privacy in the modern age of AI, facilitating ethical AI expansion while safeguarding privacy rights. This constant knowledge, as AI and privacy interact, has become our common responsibility to create a line that lets AI's enormous possibilities become realized while protecting citizens' essential freedoms or worth. Everyone can handle the difficult journey involved with trust by dealing with the issues that have been created by AI-driven creativity through extensive privacy-protection choices, making sure ensuring this present age of AI is associated with ethical progress and safeguarding privacy for anyone.

REFERENCES

- [1] Haenlein, M., & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. *California Management Review*, 61(4), 5-14.
- [2] Shabbir, J., & Anwer, T. (2018). Artificial intelligence and its role shortly. *arXiv preprint arXiv:1804.01396*.
- [3] Donahoe, E., & Metzger, M. M. (2019). Artificial intelligence and human rights. *J. Democracy*, 30, 115.
- [4] Lewis-Kraus, G. (2016). The great AI awakening. *The New York Times Magazine*, 14(12), 2016.
- [5] Stoica, I., Song, D., Popa, R. A., Patterson, D., Mahoney, M. W., Katz, R., & Abbeel, P. (2017). A Berkeley view of systems challenges for AI. *arXiv preprint arXiv:1712.05855*.
- [6] BHATT, Hitesh, et al. Artificial Intelligence and Robotics Led Technological Tremors: A Seismic Shift towards Digitizing the Legal Ecosystem. *Applied Sciences*, 2022, 12.22: 11687.
- [7] Kaplan, A., & Haenlein, M. (2020). Rulers of the world, unite! The challenges and opportunities of artificial intelligence. *Business Horizons*, 63(1), 37-50.

- [8] Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management*, 30(2), 256-286.
- [9] Tao, Mengjun, Richard Jiang, and Carolyn Downs. "Ethics of Face Recognition in Smart Cities Toward Trustworthy AI." *Big Data Privacy and Security in Smart Cities*. Cham: Springer International Publishing, 2022. 23-52.
- [10] Stoica, Ion, et al. "A Berkeley view of systems challenges for ai." *arXiv preprint arXiv:1712.05855* (2017).
- [11] Li, Z., Kong, D., Niu, Y., Peng, H., Li, X., & Li, W. (2023). An Overview of AI and Blockchain Integration for Privacy-Preserving. *arXiv preprint arXiv:2305.03928*.
- [12] Regulation, P. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. Regulation (EU), 679, 2016.
- [13] Mehta, M., Kumar, A., Maurya, S., & Pandey, S. (2021). Facial Recognition in Public Areas. *Journal of Informatics Electrical and Electronics Engineering (JIEEE)*, 2(2), 1-7.
- [14] Zhang, S., Feng, Y., & Sadeh, N. (2021). Facial recognition: Understanding privacy concerns and attitudes across increasingly diverse deployment scenarios. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)* (pp. 243-262).
- [15] Iezzi, M. (2020, December). Practical privacy-preserving data science with homomorphic encryption: an overview. In *2020 IEEE International Conference on Big Data (Big Data)* (pp. 3979-3988).
- [16] Chen, H., Zhu, T., Zhang, T., Zhou, W., & Yu, P. S. (2023). Privacy and Fairness in Federated Learning: on the Perspective of Trade-off. *ACM Computing Surveys*.
- [17] Sommaggio, P., & Marchiori, S. (2020). Moral dilemmas in the AI era: A new approach. *Journal of Ethics and Legal Technologies*, 2 (JELT-Volume 2 Issue 1), 89-102.
- [18] Seh, Adil Hussain, et al. "Healthcare data breaches: insights and implications." *Healthcare*. Vol. 8. No. 2. MDPI, 2020.
- [19] Wei, M., & Zhou, Z. (2022). AI ethics issues in the real world: Evidence from AI incident database.
- [20] Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). Healthcare data breaches: insights and implications. In *Healthcare* (Vol.8, No. 2, p. 133). MDPI.
- [21] Anderljung, M., Barnhart, J., Leung, J., Korinek, A., O'Keefe, C., Whittlestone, J., & Wolf, K. (2023). Frontier AI regulation: Managing emerging risks to public safety. *arXiv preprint arXiv:2307.03718*.
- [22] Parker, S. K., & Grote, G. (2022). Automation, algorithms, and beyond Why work design matters more than ever in a digital world. *Applied Psychology*, 71(4), 1171-1204.
- [23] Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, 21(15), 5119.
- [24] Ntoutsis, Eirini, et al. "Bias in data-driven artificial intelligence systems-An introductory survey." *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* 10.3 (2020): e1356.
- [25] Shestakova, V. (2021). Best Practices to Mitigate Bias and Discrimination in AI. *Performance Improvement*, 60(6), 6-11.
- [26] Hamann, K., & Smith, R. (2019). Facial recognition technology: Where will it take us? *Crim. Just.*, 34, 9.
- [27] Johnson, K. N. (2019). Automating the risk of bias. *Geo. Wash. L. Rev.*, 87, 1214.
- [28] Ashok, M., Madan, R., Joha, A., & Sivarajah, U. (2022). Ethical framework for Artificial Intelligence and Digital technologies. *International Journal of Information Management*, 62, 102433.
- [29] Sébert, A.G. (2023). Combining differential privacy and homomorphic encryption for privacy-preserving collaborative machine learning (Doctoral dissertation, Université Paris-Saclay).
- [30] Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Differential privacy techniques for cyber-physical systems: a survey. *IEEE Communications Surveys & Tutorials*, 22(1), 746-789.
- [31] Zhao, B. Z. H., Kaafar, M. A., & Kourtellis, N. (2020). Not one but many tradeoffs: Privacy vs. utility in differentially private machine learning. In *Proceedings of the 2020 ACM SIGSAC Conference on Cloud Computing Security Workshop* (pp. 15-26).
- [32] Van de Hoven, J., Comandé, G., Ruggieri, S., Domingo-Ferrer, J., Musiani, F., Giannotti, F., & Stauch, M. (2021). Towards a digital ecosystem of trust: Ethical, legal and societal implications. *Opinio Juris In Comparatione*, (1/2021), 131-156.
- [33] Ruane, Elayne, Abeba Birhane, and Anthony Ventresque. "Conversational AI: Social and Ethical Considerations." *AICS*. 2019.
- [34] O'Sullivan, Shane, et al. "Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery." *The International Journal of Medical Robotics and Computer-Assisted Surgery* 15.1 (2019): e1968.
- [35] Bahrevar, R., & Khorasani, K. (2021). Accountability and Transparency in AI Systems: A Public Policy Perspective.
- [36] McGregor, L., Murray, D., & Ng, V. (2019). International human rights law as a framework for algorithmic accountability. *International & Comparative Law Quarterly*, 68(2), 309-343.
- [37] Sullivan, C. (2019). EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross-border data transfers and protection of personal data in the IoT era. *computer law & security review*, 35(4), 380-397.
- [38] Biega, A. J., Potash, P., Daumé, H., Diaz, F., & Finck, M. (2020). Operationalizing the legal principle of data minimization for personalization. *43rd International ACM SIGIR conference on research and development in information retrieval* (pp. 399-408).
- [39] Semantha, F. H., Azam, S., Yeo, K. C., & Shanmugam, B. (2020). A systematic literature review on privacy by design in the healthcare sector. *Electronics*, 9(3), 452.
- [40] Vogel, B., Kajtazi, M., Bugeja, J., & Varshney, R. (2020). Openness and security thinking characteristics for IOT ecosystems. *Information*, 11(12), 564.
- [41] Tan, A. Z., Yu, H., Cui, L., & Yang, Q. (2022). Towards personalized federated learning. *IEEE Transactions on Neural Networks and Learning Systems*.
- [42] Vardalachakis Marios, et al. "ShinyAnonymizer: A Tool for Anonymizing Health Data" *ICT4AWE 2019 Conference* pp. 325-332.
- [43] Vardalachakis Marios, et al. "Anonymization, Hashing and Data Encryption Techniques: A comparative Case Study" *3rd International Conference on Mathematics and Computers in Science and Engineering (MACISE 2023)*, Ierapetra, Crete, Greece, 25-27 August 2023.
- [44] Gordon, J. S., & Nyholm, S. (2021). Ethics of artificial intelligence. *Internet Encyclopedia of Philosophy*, 2161-0002.
- [45] Kondylakis, Haridimos, et al. "EvoRDF: A framework for exploring ontology evolution." *The Semantic Web: ESWC 2017 Satellite Events: ESWC 2017 Satellite Events, Portorož, Slovenia, May 28–June 1, 2017, Revised Selected Papers 14*. Springer International Publishing, 2017.
- [46] Bharti, S. S., & Aryal, S. K. (2023). The right to privacy and an implication of the EU General Data Protection Regulation (GDPR) in Europe: Challenges to the companies. *Journal of Contemporary European Studies*, 31(4), 1391-1402.
- [47] Wong, R. Y., & Mulligan, D. K. (2019, May). Bringing design to the privacy table: Broadening "design" in "privacy by design" through the lens of HCI. In *Proceedings of the 2019 CHI conference on human factors in computing systems* (pp. 1-17).
- [48] Iwaya, L. H., Babar, M. A., & Rashid, A. (2023). Privacy Engineering in the Wild: Understanding the Practitioners' Mindset, Organizational Aspects, and Current Practices. *IEEE Transactions on Software Engineering*.
- [49] Iezzi, M. (2020). Practical privacy-preserving data science with homomorphic encryption: an overview. In *2020 IEEE International Conference on Big Data (Big Data)* (pp. 3979-3988).
- [50] Aziz, R., Banerjee, S., Bouzeffrane, S., & Le Vinh, T. (2023). Exploring Homomorphic Encryption and Differential Privacy Techniques towards Secure Federated Learning Paradigm. *Future Internet* 2023, 15, 310.
- [51] Manheim, K., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy. *Yale JL & Tech.*, 21, 106.
- [52] Alazab, M., RM, S. P., Parimala, M., Maddikunta, P. K. R., Gadekallu, T. R., & Pham, Q. V. (2021). Federated learning for cybersecurity: Concepts, challenges, and future directions. *IEEE Transactions on Industrial Informatics*, 18(5), 3501-3509.
- [53] Marcolla, C., Sucasas, V., Manzano, M., Bassoli, R., Fitzek, F. H., & Aaraj, N. (2022). Survey on fully homomorphic encryption, theory, and applications. *Proceedings of the IEEE*, 110(10), 1572-1609.
- [54] Wei, K., Li, J., Ding, M., Ma, C., Yang, H. H., Farokhi, F., & Poor, H. V. (2020). Federated learning with differential privacy: Algorithms and performance analysis. *IEEE Transactions on Information Forensics and Security*, 15, 3454-3469.
- [55] Liu, B., Ding, M., Shaham, S., Rahayu, W., Farokhi, F., & Lin, Z. (2021). When machine learning meets privacy: A survey and outlook. *ACM Computing Surveys (CSUR)*, 54(2), 1-36.
- [56] Floridi, L., Cows, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V. & Vayena, E. (2021). An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Ethics, governance, and policies in artificial intelligence*, 19-39.



Article

Use Ultra-Wideband Discone Rectenna for Broadband RF Energy Harvesting Applications [†]

Manolis G. Tampouratzis ^{1,*} , Demosthenes Vouyioukas ¹ , Dimitrios Stratakis ² and Traianos Yioultsis ³

¹ Department of Information and Communication Systems Engineering, University of the Aegean, GR 83200 Karlovassi, Greece; dvouyiou@aegean.gr

² Department of Electrical and Computer Engineering (ECE), Hellenic Mediterranean University (HMU), GR 71004 Heraklion, Greece; dstrat@hmu.gr

³ Department of Electrical and Computer Engineering (ECE), Aristotle University of Thessaloniki (AUTH), GR 54124 Thessaloniki, Greece; traianos@auth.gr

* Correspondence: tampouratzis@aegean.gr

[†] This paper is an extended version of our paper published in 8th International Conference on Modern Circuits and Systems Technologies (MOCAST), Thessaloniki, Greece, 13–15 May 2019.

Received: 19 February 2020; Accepted: 20 April 2020; Published: 23 April 2020



Abstract: In this study, a broadband Radio Frequency (RF) energy harvester implementation is presented. The system uses a broadband discone antenna, which can operate efficiently in a broad frequency spectrum, including LTE, DCS 1800 and UMTS 2100 cellular frequency bands. The system is able to harvest energy from various electromagnetic field sources, thus has the potential to efficiently charge a storage energy element in a short time. The prototype broadband RF energy harvester was tested in the laboratory and also in a typical urban environment.

Keywords: broadband antennas; discone antenna; rectennas; radio frequency (RF) energy harvesting; schottky diode; voltage doubler rectifier (VDR)

1. Introduction

Energy harvesting from radio waves is possible through devices that are called Radio Frequency Harvesters. A basic radio frequency energy harvester consists of an antenna, a matching network, a high frequency rectifier and an energy storage element. A rectenna is a rectifying antenna, a special type of receiving antenna that is used for converting electromagnetic energy into direct current (DC), and is usually found in the bibliography to describe both the antenna and the rectifier sections of a harvesting system [1]. The total power harvested from a radio frequency harvester, depends on: (a) the available power spectral density ($\text{W/m}^2/\text{Hz}$), (b) the effective area of the antenna and (c) the operating bandwidth of the system [2,3].

The available power spectral density depends only on the electromagnetic environment. Limitations on the physical size of a RF energy harvester imposes limitations on the physical size of the antenna and hence on its effective area. The proposed antenna in [4] could be a solution for this problem. The study introduced a novel multiport rectenna system, allowing the available area for the rectenna to be fully utilized at all operating frequencies by using different numbers of antenna ports for RF energy harvesting. Measurements proved that this rectenna type could achieve output DC voltages of up to 2.2 V and DC power up to -13.6 dBm.

Thus, the most efficient way to increase the total power is by increasing the bandwidth of the system, in order to collect energy from more sources in a wider frequency range. Multiband and broadband rectennas could be a solution for increasing the bandwidth of the system, in order to collect

energy from more ambient wireless sources that are distributed in a wide frequency range. Multiband rectennas normally have high conversion efficiency contrary to a narrow operating bandwidth, and can be ideal for energy harvesting from wireless communications systems, such as DCS-1800, LTE, UMTS [5].

The authors in [6] proposed a complimentary split ring resonator (CSRR) metamaterial multiband antenna with a hybrid junction ring rectifier as a multiband rectenna that was able to utilize wireless transmissions from four communication bands such as GSM, UMTS, LTE, WiFi, using separately rectifier branches. Subrectifiers have been matched by the hybrid ring junction at each operating band. With this setup, the rectenna has a peak conversion efficiency up to 67% at 1.8 GHz. Additionally, the proposed multiband rectenna was tested in an urban environment.

Broadband rectennas usually have lower conversion efficiency in contrary to a wide operating bandwidth. The design of this type of rectenna is a difficult process due to the complex matching network and the nonlinearity of the rectifiers' diodes [5]. Tapered line matching networks could be a solution for this problem as proposed by the authors of [7] with impedance transformation from the source ($50\ \Omega$) to the load ($140\ \Omega$). The proposed broadband rectenna exhibits an improved conversion efficiency above 30% across the entire frequency range from 1.2 to 5 GHz, using an Archimedean Spiral Antenna and a wideband-tapered microstrip balance-unbalanced transmission line (BALUN).

The authors in [8] proposed a broadband rectenna using a double-sided printed monopole antenna consists of circular patch with a truncated ground plane. This type of rectenna, has an operating bandwidth range from 0.9 to 5.5 GHz and offers maximum efficiency (62.5%) with a resistive terminal load of $5\ \text{k}\Omega$ at 1.8 GHz, as shown from measurements results.

The work in [9] introduced a compact broadband rectenna using a coplanar waveguide (CPW) rectangular monopole antenna with an inverted-L open circuit stub as the matching network and a rectifying circuit based on a voltage doubler with a minimum footprint size ($58 \times 55\ \text{mm}^2$). The proposed rectenna operates from 1.8 to 3.5 GHz and 5.4 to 6 GHz, and is able to utilize transmissions from wireless applications such as GSM 1800, UMTS 2100, WLAN 802.11 a, b and g systems and also WiMAX signals efficiently up to 28% for power conversion.

Although the above systems can effectively operate in several microwave frequency bands (1 to 6 GHz), none of them is a capacitor-based RF harvester. To the best of the authors' knowledge, the only proposed capacitor-based RF harvester is the work in [10], which can efficiently operate in the medium wave frequency band (531–1.611 KHz) using a tunable loop antenna. The system was able to harvest enough energy to charge a super capacitor to 2.8V, and sustain the voltage while no load connected to the circuit. This charge is sufficient to power a $1\ \text{k}\Omega$ load for approximately 1 h. However, in the latest system the efficiency estimation as a function of time is not mentioned.

In this work, a broadband capacitor-based RF energy harvester was fabricated consisting of a 3D discone antenna, a Dickson rectifier and a storage capacitor element for terminal load. For the total efficiency estimation of the harvesting system, we followed a methodology by enhancing the work in [11]. Our approach has taken into consideration the average power of a capacitor, which is a function of charging time and corresponds to the variation rate of its energy. The values of power density, antenna's active surface and storage capacitor's voltage were measured at the place of installation to determine the efficiency of the system. The prototype was tested on the laboratory and also in the urban environment. In summary, the main contributions of this study were:

- A broadband discone antenna was designed and fabricated, with efficient operation in a wide frequency spectrum to acquire ambient RF energy from many electromagnetic field sources, with excellent broadband characteristics (1.5:1 or less standing wave ratio (SWR) at a frequency range up to 10:1).
- In our work, we have introduced a novel approach of capacitor-based energy harvester's total efficiency estimation, and its maximization at the transient state, as proven from laboratory measurements.

The rest of this article is organized as follows: the discone antenna design is presented and analyzed in Section 2. Section 3 gives a description of the Dickson rectifier basic theory and its implementation is described in Section 4. Section 5 gives a short report of the rectifier element. Section 6 is devoted to the experimental performance and measurement set-up. In Section 7, we present and analyze the efficiency estimation approach of the proposed rf harvester and finally, Section 8 gives the conclusion and a discussion on future work.

2. The Broadband Discone Antenna

The discone antenna is a version of the biconical antenna, in which one of the two cones have been replaced by a disc. A coaxial cable is usually attached at the point of intersection of the disc with the cone, to feed the antenna. The discone antenna is omni-directional, linear polarized and has a gain similar to that of a half wavelength dipole. It has excellent broadband characteristics at a frequency range up to 10:1. This type of antenna can be ideal for RF energy harvesting, besides its large size and its 3D geometry. The sensitivity of this antenna is highest in the direction of the horizon because of the narrow radiation pattern in the vertical plane. The standing wave ratio (SWR), is typically 1.5:1 or less in several octave frequencies. The behavior of this antenna as a function of frequency, is like a high-pass filter. Below the active cut-off frequency, significant standing waves appear in the feed line [12,13].

2.1. Structure Description

A discone antenna can be made from solid metal foil. At lower frequencies, a sufficient number of metal wires or rods are often used, thereby simplifying construction and reducing wind resistance at the same time. The rays may be made from rigid wire or welding rods. The optimal number of rods found in the bibliography, including the disc and the cone, is from 8 to 16 [14,15]. The discone antenna consists of three main components: (a) the disc, (b) the circular cone and (c) the insulator (Figure 1):

- The disc has a diameter equal to 70% of the cone diameter. The antenna's feed point is located in the center of the disc. It is usually powered by a 50 Ω coaxial cable, with the main conductor connected to the tray and the outer conductor to the cone;
- The height of the cone must be 30% of the wavelength of the lowest operating frequency of the antenna. The inner cone angle is generally from 30 up to 100 degrees;
- The disc and the cone are separated by an insulator. The thickness of the insulator, determines some of the antenna's properties, especially near its high frequency limits [12].

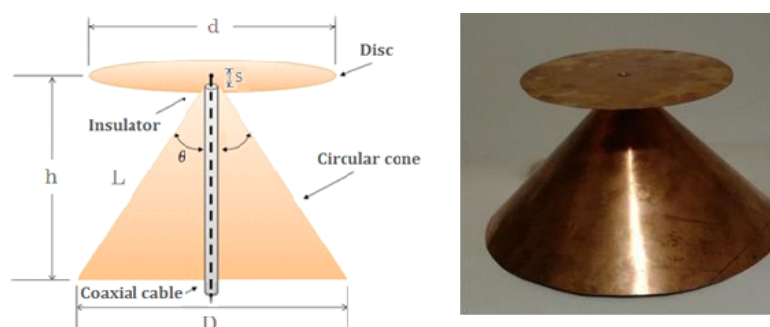


Figure 1. The main parts of the discone antenna: (i) the disc, (ii) the circular cone (iii) the insulator (left) and the antenna prototype from copper foil, with an inner cone angle 90°, height 12 cm and low-cut frequency 750 MHz (right).

2.2. Radio Amateurs' Construction Combinations

Different dimensional combinations of the discone antenna previously tested by radio amateurs, have demonstrated the following [16,17]:

The construction is not extremely dimensional, if $0.58D < d < 0.75D$ and $s \ll \lambda$ (where s is the gap between the disc and the cone). Angles from 60° to 100° represent the angle θ values range that there is a satisfactory matching for coaxial lines of 75Ω and 50Ω . Smaller angles, reflect better matching with an 75Ω line, while larger angles are best adapted to the 50Ω line. However, the gain stability and the mean gain of the antenna in the useful bandwidth seems to be inversely proportional to the inner cone angle θ .

The useful bandwidth is defined by a peak SWR ratio of 3:1, at a frequency range of 10:1. For higher frequencies the s/λ ratio increases, while the useful bandwidth is constantly decreasing. The lower operating frequency is determined by the height h . At the lower operating frequency (VSWR 3:1) $h \sim 0.21\lambda$. At this point, the gain of the antenna seems to increase as the length L (up to ~ 5 dBi) is increased, as opposed to the useful bandwidth, which decreases. The discone antenna can be operated with a SWR ratio 2:1 at a frequency range of 4.5:1 in HF and 3:1 at the upper UHF band.

The horizontal radiation pattern (H-plane) is omnidirectional and the polarization is vertical. The gain of the antenna varies between 1.5 and 5 dBi (1.5 dBi at the frequency where $L \sim 0.28\lambda$ and 5 dBi at the frequency where $L \sim 0.7\lambda$, where L is the side length of the cone). Additionally, by approaching the upper frequency limit of the useful operating range, maximum radiation occurs at small angles ($3\text{--}10^\circ$) below the plane of the disc. At these frequencies, the discone antenna behaves as a conical monopole.

2.3. Discone Antenna Construction–Design Expressions

With the aid of the design equations connecting the disc dimension to the antenna cone, the prototype that is described in this study was made from 0.3-mm thick copper foil, with a cone angle of 90° (Figure 1). The height h for the antenna is 12 cm, which determines the lower cut-off frequency (in the present design corresponds to the frequency of $F_{\min} = 750$ MHz), such as the response of a high-pass filter [14]. The mathematical expression that connects the height h (in m) of the cone with the wavelength λ (in m), and consequently the cut-off frequency F_{\min} (MHz) of the discone antenna is $h/\lambda = 0.3$. Considering that the height h of the antenna is given by:

$$h = 0.3 \frac{300}{F_{\min}(\text{MHz})} \quad (1)$$

The disc diameter d is correlated to the diameter of the cone D , by:

$$d = 0.7D \quad (2)$$

A cylindrical SMA (female) type connector is attached to the top of the cone. The design that is described in this work has been based on conclusions from measurements on several structures [16], with common features: $h > 0.21\lambda$ at the lowest operating frequency, $30^\circ < \theta < 100^\circ$ and $0.58D < d < 0.75D$ as shown in Table 1. Measurements have shown that the gain of the antenna is somehow inversely proportional to its bandwidth, thus the design that is optimized for maximum bandwidth has minimum gain. In this study, maximizing the bandwidth while keeping the impedance of the antenna as possible near to 50Ω was the main design criterion.

Table 1. The Proposed Discone Antenna’s Dimensions.

F_{\min} (GHz)	h (cm)	d (cm)	D (cm)	L (cm)	Θ (deg.)	S (cm)
0.75	12	16	23	17	90	0.5

2.4. Antenna Simulation

The simulation of this antenna type was carried out with Antenna Magus software, to extract the electrical characteristics and the radiation patterns in polar and cartesian form. The SWR is about 1.5:1, and the reflection coefficient (S11) ranges from -10 dB to -20 dB in a wide band of frequencies, as shown in Figure 2. Simulation results fully confirmed the theoretical lower cut-off frequency of the proposed prototype antenna as given by Equation (1). The 3D radiation charts were carried out in cooperation with CST Microwave Studio Suite software, as shown in Figure 3. Radiation patterns simulations were done at minimum ($F_{\min} = 0.75$ GHz), center ($F_{\text{cent}} = 1.5$ GHz) and maximum ($F_{\max} = 3$ GHz) operation frequencies, respectively.

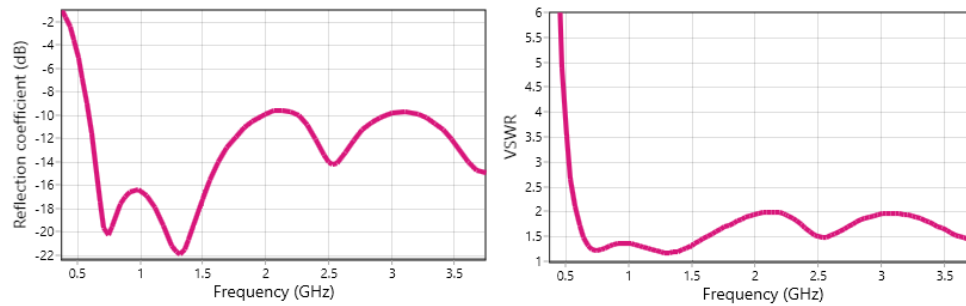


Figure 2. Reflection Factor in dB (left) and standing wave ratio (SWR) versus frequency (right) of the discone antenna's simulation results.

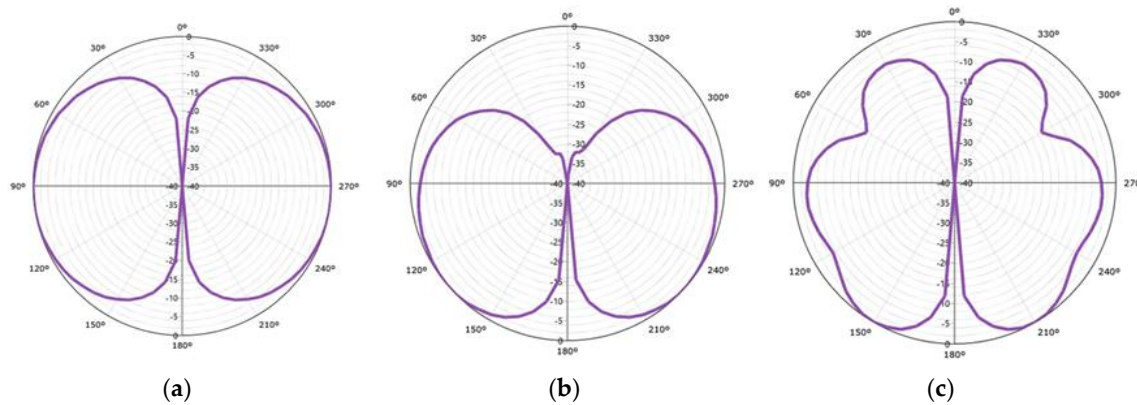


Figure 3. Radiation patterns (vertical plane) of the discone antenna at (a) minimum operation frequency (left), (b) center operation frequency (center), (c) maximum operation frequency (right).

3. Basic Theory of the Dickson N-Stage Rectifier

A famous RF signal rectifier topology is the Dickson rectifier with two or N -stages, as depicted in Figure 4a. The output of the circuit as a Voltage Doubler Rectifier (VDR) is given by:

$$V_{\text{out}} = 2V_{RF_{in}} - V_{th1} - V_{th2} \quad (3)$$

where V_{th1} , V_{th2} are threshold voltages of the diodes D_1 , D_2 respectively and $V_{RF_{in}}$ is the RF input voltage. It consists of two sections in cascade: a clamp consisting of elements C_1 and D_1 and a peak rectifier, consisting of C_2 and D_2 . When the circuit is excited by a sine wave signal with amplitude V_p , the clamping section produces a waveform that positive peaks are bounded to 0, while the negative ones reach $-2V_p$. Taking this waveform, the peak detector segment provides, along C_2 , a negative DC voltage of magnitude $2V_p$ [18].

The individual stages of the VDR circuit can be in sequence (N steps), so as to increase the rectifier output voltage at a resistive load, which is defined as [19]:

$$V_{out,Load} = 2NV_{RF_{in}} - 2NV_{th} - \frac{(N-1)I_{Load}}{f_o C} \quad (4)$$

where I_{Load} is the load current, C is the capacity of the blocking capacitors and f_o is the operating frequency of the system. Considering the losses of the substrate, the average input power is given by the following equation:

$$P_{in} = 2N I_{D,sat} B_1 \left(\frac{V_{out}}{V_T} \right) \exp \left(-\frac{V_{RF_{in}}}{2NV_T} \right) + \frac{N}{2} V_{out}^2 R_{Sub} (\omega_o C_{Sub})^2 \quad (5)$$

where V_T is the thermal voltage, B_1 is the modified first order Bessel function, R_{Sub} and C_{Sub} are the resistance and the substrate capacity, respectively [20]. By solving (5), it is noteworthy that for a constant output voltage and power consumption, the larger the number of stages, the smaller the input voltage required to obtain a given DC output voltage and thus power consumption. However, the optimal number of stages is the trade-off between high DC output voltage and low power losses due to diode consumption and substrate losses. Experimental tests have shown that the optimum number of stages is between 1 and 2. High saturation current ($I_{D,Sat}$), low crossover capacitance (C_j) for low threshold voltage V_{th} , small resistor in series (R_s), and finally low cross-resistance (R_j), are some characteristics of a diode for loss reduction. The HSMS series of Avago diodes are a good solution, commercially available for these applications [21,22].

4. The Rectifier Circuit Design

The rectifier design described in this study was based on a Dickson 2-Stage Rectifier; this topology is actually a voltage doubler. The specific design was studied and simulated on Agilent ADS software and was finally manufactured on a FR4 substrate with dielectric constant $\epsilon_r = 4.35$. For the simulation of HSMS-2862 Schottky diode [23], the corresponding models from the ADS software library were used. For the passive components, general purpose models were used. The rectifier's capacitors values were selected at 100 pF to satisfy the condition for the time constant τ , to be much greater than 10 RF cycle for the operating frequency of the circuit, which corresponds to 0.58 nsec at 1700 MHz. The storage element was connected at the rectifier's output. The storage element is an AVX (TAJ Series) 330 μ F surface mount device (SMD) tantalum capacitor, with very low equivalent series resistance (ESR) value. In series with the tantalum capacitor, a half-turn coil with low thickness (~ 0.6 mm) was placed, to act as a "RF choke" having an induction, approximately of 100 nH (Figure 4b).

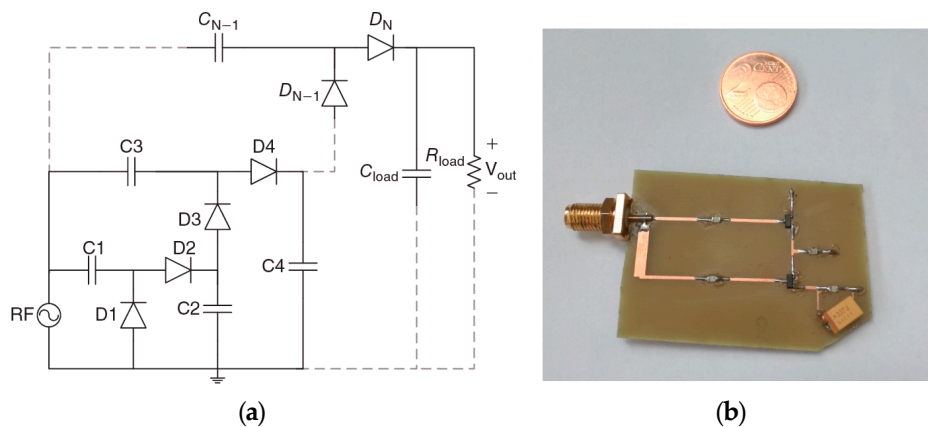


Figure 4. (a) Basic topology of the Dickson N-Stage Rectifier [2], (b) The proposed rectifier circuit implementation from FR4 PCB board with dielectric constant $\epsilon_r = 4.35$.

5. The RF Rectifier Diode HSMS—2862

The basic rectifying element of the device was the AVAGO Schottky HSMS-2862 diode [23], ideal for radio frequency applications due to its features, such as low switching time, low voltage drop, short recovery time and low contact capacity. According to the manufacturer's datasheet, this component is capable of rectifying broadband signals with operating frequencies ranging from 915 MHz to 5.8 GHz used by modern wireless communications systems, such as DCS-1800, LTE, UMTS and Wi-Fi. Indicatively, according to the datasheet, the sensitivity of the component reaches 35 mV/ μ W at 2.45 GHz.

6. Broadband RF Energy Harvesting at the Electromagnetic Field

The proposed RF harvester was placed for testing at the laboratory and nearby a base station in the urban environment, with transmissions from wireless communications systems, such as DCS-1800, LTE, UMTS in the town of Heraklion, Crete, Greece. At the place of harvester installation, the broadband electric field average value (about 3 V/m) and the equivalent power density average value (about 0.023 W/m²) measured from a Narda AMS-8061/G frequency selective EMF area monitor of the EMF project [24]. The storage capacitor's voltage at a given time t , was measured with an Axiomet AX-176 True RMS Multimeter / Datalogger. At the laboratory, the harvester was irradiated from a 3115 ETS LINDGREN Horn antenna driven by Agilent E4438C generator, for the performance evaluation of the system in several frequencies. The electric field value E and the equivalent power density average value S , were measured from a Rohde & Schwarz—FSH8 Spectrum Analyzer, at the place of harvester installation. Finally, the discone antenna's active surface (A_{eff}) value was simulated and also measured approximately according to ANSI C63.5 2006 EMC standard [25,26] at the laboratory in several operating frequencies. The experiment setup is showed in Figure 5 and the measurement results (storage capacitor charging response) are presented in Figure 6, respectively.

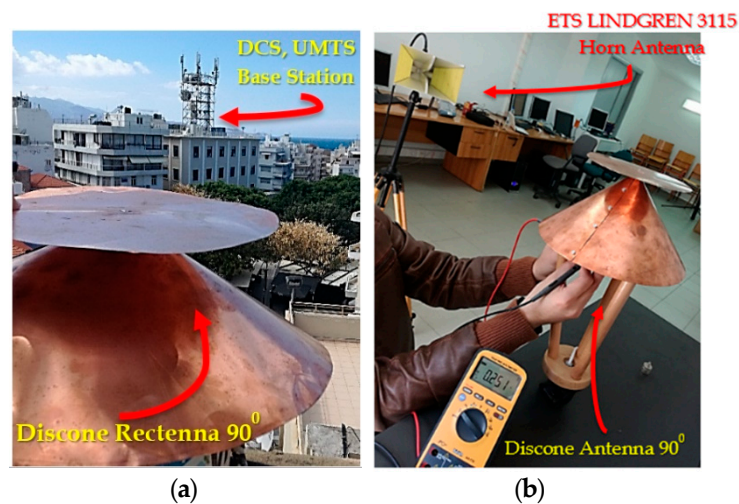


Figure 5. (a) The broadband Discone rectenna experiment setup nearby a base station in the urban environment, at Heraklion, Crete, Greece and (b) testing at the N.I.R.L laboratory of the Hellenic Mediterranean University (HMU).

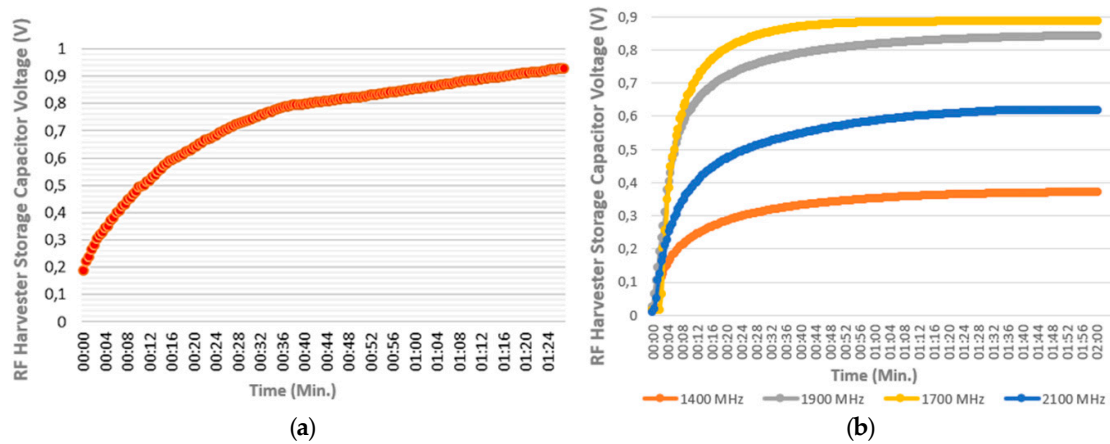


Figure 6. The RF-EH's storage capacitor (330 μ F) charging response (a) from ambient broadband RF energy harvesting with equivalent power density average value 0.023 W/m², 200 m away from base station in the urban environment, (b) testing in several frequencies at the N.I.R.L laboratory.

7. Evaluation of Measurements and Applicability

From the obtained measurements, the storage capacitor's (330 μ F) maximum voltage value (V_{max}) was approximately 1 V. Thus, the stored energy can be calculated according to Equation (10), and corresponds to 165 μ J. The storage element could have higher capacitance for higher energy storage in contrast to a slower charging time. To sum up, the storage capacitor's harvested energy derived from the electromagnetic field, which was sufficient to power a load of 10 k Ω for 15 s, if we consider that:

$$\tau = RC \quad (6)$$

Thus, for a 10 k Ω load and a 330 μ F storage capacitor, the constant time is $\tau = 3.3$ s. Knowing that a capacitor is completely discharged at a time of 5τ , with these component's setup, it can be assumed that for 15 s the capacitor's voltage will exponentially reduce to zero. For a constant time ($\tau = 3.3$ s), the voltage will exponentially reduce due to $0.368V_{max}$ value as described by the solution of the 1st order differential equation:

$$V_c(t) = V_{max} \exp\left(-\frac{t}{RC}\right) \quad (7)$$

where $V_c(t)$ is the capacitor's voltage at time t , V_{max} is the initial maximum voltage value from charging at time $t = 0$, C is the capacitance value and R , the terminal resistive load value, respectively.

In general, small electronic devices with minimum power consumption requirements (e.g., WSN's node), can be powered from ambient RF Energy. The applicability of the proposed improved version of storage-based RF energy harvesting system could be the power supply of a WSN's node for Internet of Things (IoT) applications [27]. A WSN's node can be self-powered from ambient RF energy by the storage-based harvester when the "wake-up" mode is active (e.g., for wireless data transmission). On the contrary, at "sleep" mode of WSN's node, the harvester's storage capacitor will be charged from the beginning etc.

8. RF Energy Harvesting Total Efficiency Estimation Approach

The performance of a RF Energy Harvester is defined as the ratio of the power delivered to its output to the total available power in the harvester antenna. The average power of a capacitor, is a function of charging time and corresponds to the variation rate of its energy as described by (8). In this case, where the power is not constant, it is meant to refer to the energy at a given time.

$$P_{aver.} = \frac{dE_{cap.}}{dt} \quad (8)$$

8.1. Total Efficiency of Narrow Band RF Energy Harvesting Systems

Assuming that, the total efficiency of a harvesting system (α), at a given time (t), can be described by the following equation:

$$\alpha(t) = \frac{E_{cap}(t)}{E_{RF}(t)} \quad (9)$$

where $E_{cap}(t)$, the harvesting energy at the storage capacitor at time (t), and $E_{RF}(t)$, the energy of the RF field at time (t). Knowing that, the harvesting energy at the storage capacitor at the same time (t), is given by:

$$E_{cap}(t) = \frac{1}{2}CV_c(t)^2 \quad (10)$$

where C , the capacitance value and $V(t)$, the voltage at the storage capacitor at time (t). The RF field power is given by the following Equation:

$$P_{RF}(f) = S(f)A_{eff}(f) \quad (11)$$

where S is the power density (W/m^2) and A_{eff} , is the antenna's active surface [3]. We can claim that the energy of RF field at time (t), is given by:

$$E_{RF}(t) = \int_0^t S(f)A_{eff}(f) dt \quad (12)$$

The time (t) can be considered a stable quantity and extracted out of the integral. Therefore, (12), takes the form:

$$E_{RF}(t) = S(f)A_{eff}(f) t \quad (13)$$

Thus from (9), (10) and (13) we can assume that the total efficiency (α) of a single carrier (narrow band) harvesting system, at a given time (t), can be described by:

$$\alpha_{Narrowband}(t) = \frac{\frac{1}{2}CV_c(t)^2}{S(f)A_{eff}(f) t} \quad (14)$$

It is worth mentioning that all quantities in the above equations are measurable, and important to determine for the efficiency of the harvesting systems.

8.2. Total Efficiency of Broadband RF Energy Harvesting Systems

We can assume that the RF energy of the operating bandwidth at time t is given by:

$$E_{RF}(t) = \int_0^t \int_{f_1}^{f_2} S(f)A_{eff}(f) df dt \quad (15)$$

where f_1, f_2 the lower and the upper RF frequency of the operating bandwidth respectively, S the power density (W/m^2), A_{eff} the antenna's active surface, and (t), a given time can be considered a stable quantity and extracted out of the integral. Therefore (15), takes the form:

$$E_{RF}(t) = t \int_{f_1}^{f_2} S(f)A_{eff}(f) df \quad (16)$$

From (9), (10) and (16) we can claim that the total efficiency (α) of a broadband RF-EH system at a given time t , can be described by:

$$\alpha_{\text{Broadband}}(t) = \frac{\frac{1}{2}CV_c(t)^2}{t \int_{f_1}^{f_2} S(f)A_{eff}(f) df} \quad (17)$$

The narrowband total efficiency estimation of the system was computed according to (14) as shown in Figure 7, and the broadband total efficiency estimation of the system was computed according to (17) as shown in Figure 8, respectively.

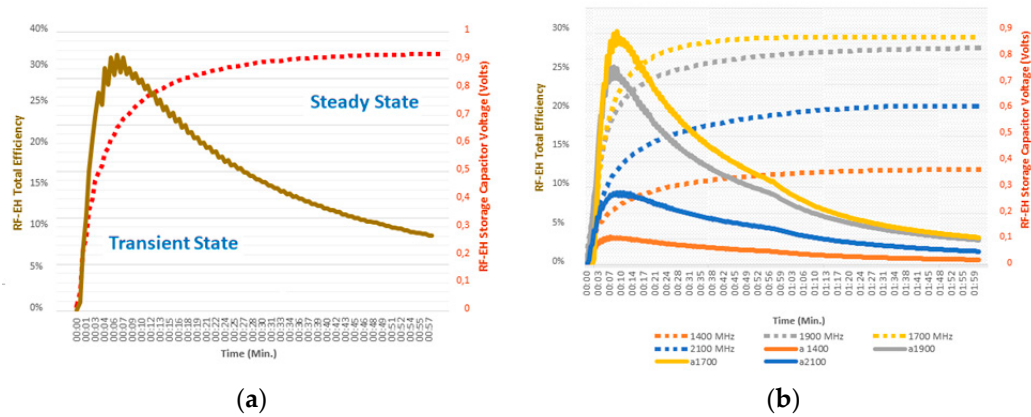


Figure 7. (a) The RF-EH's total efficiency response (a) at 1700 MHz and (b) the RF-EH's total efficiency in several operating frequencies, tested at the laboratory. The RF-EH's storage capacitor charging response is shown by the dashed lines, respectively.

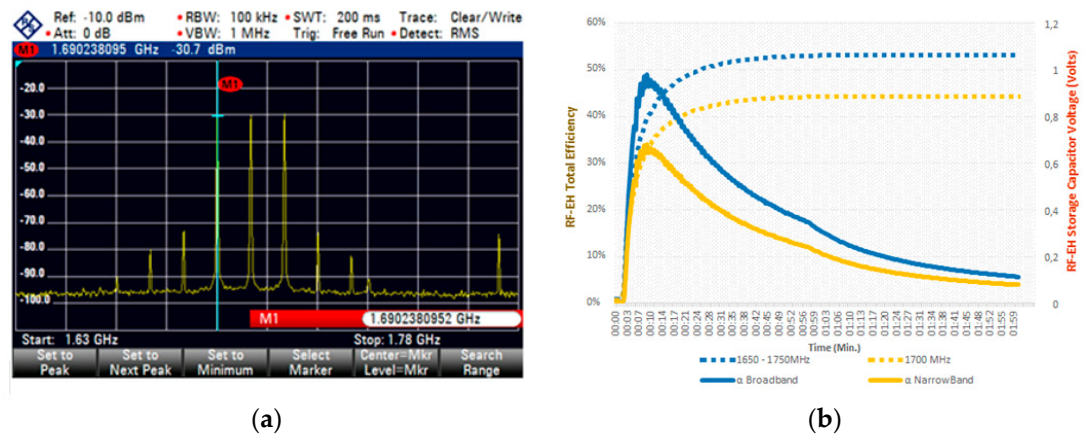


Figure 8. (a) The broadband received RF signal (1650 MHz–1750 MHz) at Rohde & Schwarz—FSH8 Spectrum Analyzer and (b) the RF-EH's broadband total efficiency response (a).

The capacitor's charging is a transitional process. Knowing that, from the obtained measurements it can be concluded that the storage element save energy only at the Transient state and ceases to save at Steady state.

8.3. RF-EH Storage Efficiency Maximization

Knowing that the capacitor's voltage is a function of the charging time, that exponentially reduces to V_{\max} , as described by the solution of the 1st order differential equation:

$$V_c(t) = V_{\max} \left[1 - \exp\left(-\frac{t}{R_{eqv}C}\right) \right] \quad (18)$$

where $V_c(t)$, is the capacitor's voltage at time t , V_{\max} is the maximum voltage value, C is the storage capacitor value and R_{eqv} , is the Thevenin equivalent resistance of the Dickson rectifier in the proposed topology.

Considering (10), the storage capacitor saves maximum value of RF energy, when the variation rate of its voltage is maximized, and thus the total efficiency (α) of the system is maximized. The variation rate of storage capacitor's voltage $dV_c(t)/dt$, corresponds to the 1st derivative of the charging curve. Thus, the 1st derivative of $V_c(t)$ from (18) is given by:

$$\frac{dV_c(t)}{dt} = \frac{V_{\max}}{R_{eqv}C} \left[\exp\left(-\frac{t}{R_{eqv}C}\right) \right] \quad (19)$$

From (19), we can claim that the variation rate of storage capacitor's voltage $dV_c(t)/dt$ is maximized, at the beginning of the charging (Transient state), and thus the total efficiency (α) of the system, as shown in Figure 8. When the storage capacitor's voltage reaches its maximum value, the element ceases to save more energy (Steady state), and the average power P_{aver} is minimized [28].

9. Conclusions and Future Aspects

This study demonstrates a broadband energy harvesting system implementation to utilize base station signals from LTE, DCS-1800 and UMTS-2100 mobile systems in the downlink frequency band, in order to charge a storage energy element (330 μ F) efficiently at the urban environment in a short time (about 1 min) at 1 V. Measurements proved that a 10 k Ω load can be powered for 15 s from ambient RF harvested energy with broadband E-field average strength value of 3 V/m (0.023 W/m² power density average value). The total efficiency α of the proposed harvester system is maximized at the beginning of the storage capacitor's charge, as proven from measurements. Thus, a future aspect can be the construction of a pulse harvester system by switching of storage elements to utilize the efficiency maximization at the transient state, taking full advantage of inactive charging time. A prototype rectifier implementation with higher harvesting sensitivity characteristics, will be a new challenge as another future aspect. The available total harvested power can be increased by increasing the bandwidth of the system, in order to collect energy from more sources in a wider frequency range, using an ultra-wideband (UWB) antenna, such as the proposed discone antenna.

Author Contributions: Writing—original draft, M.G.T.; Writing—review & editing, D.V., D.S. and T.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

References

- Divakaran, S.K.; Krishna, D.D. RF energy harvesting systems: An overview and design issues. *Int. J. RF Microw. Comput. Aided Eng.* **2019**, *29*, 1–15. [CrossRef]
- Valenta, C.R.; Durgin, G.D. Harvesting Wireless Power: Survey of Energy-Harvester Conversion Efficiency in Far-Field, Wireless Power Transfer Systems. *IEEE Microw. Mag.* **2014**, *15*, 108–120.

3. Mikeka, C.; Arai, H. Design Issues in Radio Frequency Energy Harvesting System. In *Sustainable Energy Harvesting Technologies—Past, Present and Future*; Intech: London, UK, 2011; pp. 236–256.
4. Shen, S.; Zhang, Y.; Chiu, C.Y.; Murch, R. An Ambient RF Energy Harvesting System Where the Number of Antenna Ports Is Dependent on Frequency. *IEEE Int. J. Microw. Theory Tech.* **2019**, *67*, 9. [CrossRef]
5. Song, C.; Huang, Y.; Zhou, J.; Paul Carter, P. Recent Advances in Broadband Rectennas for Wireless Power Transfer and Ambient Energy Harvesting. In Proceedings of the 11th European Conference on Antennas and Propagation (EUCAP), Paris, France, 19–24 March 2017.
6. Benayad, A.; Tellache, M. A Compact Energy Harvesting Multiband Rectenna Based on Metamaterial Complementary Split Ring Resonator Antenna and Modified Hybrid Junction Ring Rectifier. *Wiley Int. J. RF Microw. Comput. Aided Eng.* **2019**, *30*, e22031. [CrossRef]
7. Mansour, M.; LePolozec, X.L.; Kanaya, H. Enhanced Broadband RF Differential Rectifier Integrated with Archimedean Spiral Antenna for Wireless Energy Harvesting Applications. *Sensors* **2019**, *19*, 655. [CrossRef] [PubMed]
8. Dardeer, O.; Elsadek, H.; Abdallah, E. Compact Broadband Rectenna for Harvesting RF Energy in WLAN and WiMAX Applications. In Proceedings of the IEEE International Conference on Innovative Trends in Computer Engineering (ITCE'2019), Aswan, Egypt, 2–4 February 2019.
9. Agrawal, S.; Parihar, M.S.; Kondekar, P.N. Broadband Rectenna for Radio Frequency Energy Harvesting Application. *IETE Int. J. Res.* **2017**, *64*, 347–353. [CrossRef]
10. Aminov, P.; Agrawal, J.P. RF Energy Harvesting. In Proceedings of the IEEE 64th Electronic Components & Technology Conference (ECTC), Orlando, FL, USA, 27–30 May 2014; pp. 1838–1841.
11. Tampouratzis, M.G.; Vouyioukas, D.; Stratakis, D. Discone Rectenna Implementation for Broadband RF Energy Harvesting. In Proceedings of the 2019 8th International Conference on Modern Circuits and Systems Technologies (MOCAST), Thessaloniki, Greece, 13–15 May 2019; pp. 1–4.
12. Kandoian, A. Three New Antenna Types and Their Applications. *Proc. IRE* **1946**, *34*, 70–75.
13. Balanis, C. *Antenna Theory, Analysis & Design*, 3rd ed.; John Wiley & Sons: Chichester, UK, 2005; p. 521.
14. Stutzman, W.; Thiele, G. *Antenna Theory and Design*; John Wiley & Sons: Chichester, UK, 1981; p. 243.
15. Kennedy, G.; Davis, B. *Electronic Communication Systems*, 4th ed.; McGraw-Hill: New York, NY, USA, 1992; pp. 298–300.
16. Adamidis, G. Discone Antenna Implementation. Master's Thesis, Physics Department, Aristotle University of Thessaloniki, Thessaloniki, Greece, 2001.
17. Goncalves, R.; Pinho, P.; Carvalho, N.B. Design and Implementation of a 3D Printed Discone Antenna for TV Broadcasting System. In Proceeding of the IEEE International Symposium on Antennas and Propagation & USNC/URSI National Radio Science Meeting, Vancouver, BC, Canada, 19–24 July 2015.
18. Sedra, A.; Smith, K. *Microelectronic Circuits*, 5th ed.; Oxford University Press: Oxford, UK, 2004; pp. 189–190.
19. Karthaus, U.; Fischer, M. Fully Integrated Passive UHF RFID Transponder IC with 16.7- μ m Minimum RF Input Power. *IEEE Int. J. Solid State Circuits* **2003**, *38*, 1602–1608. [CrossRef]
20. De Vita, A.; Lannaccone, G. Design Criteria for the RF Section of Long-Range Passive RFID Systems. In Proceedings of the Norchip Conference Proceedings, Oslo, Norway, 8–9 November 2004; pp. 107–110.
21. Pavone, D.; Buonanno, A.; D'Urso, M.; Corte, F.D. Design Considerations for Radio Frequency Energy Harvesting Devices. *Prog. Electromagn. Res. B* **2012**, *45*, 19–35. [CrossRef]
22. Buted, R.R. Zero Bias Detector Diodes for the RF/ID Market. *Hewlett Pack. J.* **1995**, *46*, 94.
23. Avago Technologies HSMS-2862 Series Surface Mount Microwave Schottky Detector Diode. August 2009. Available online: <https://docs.broadcom.com/doc/AV02-1388EN> (accessed on 19 April 2020).
24. National Observatory of Electromagnetic Fields. Greek Atomic Energy Commission. Available online: <https://paratiritirioemf.eeae.gr> (accessed on 19 April 2020).
25. Tampouratzis, M.G. RF Energy Harvesting Circuits—Design & Implementation. Master's Thesis, Open University of Cyprus (OUC), Nicosia, Cyprus, 2017.
26. Ansi C63.5-2017 (Revision of Ansi C63.5-2005): American National Standard for Electromagnetic Compatibility—Radiated Emission Measurements in Electromagnetic Interference (emi) Control—Calibration and Qualification of Antennas (9 Khz to 40 GHz). IEEE: Piscataway, NJ, USA, 2017. Available online: <https://ieeexplore.ieee.org/document/7920447> (accessed on 19 April 2020).

27. Eltresy, N.; Dardeer, O.; Al-Habal, A.; Elhariri, E.; Hassan, A.; Khattab, A.; Elsheakh, D.; Taie, S.; Mostafa, H.; Elsadek, H.A.; et al. RF Energy Harvesting IoT System for Museum Ambience Control with Deep Learning. *Sensors* **2019**, *19*, 4465. [[CrossRef](#)] [[PubMed](#)]
28. Kushnerov, A. Transient and Steady-State Analysis of a Single Switched Capacitor Converter. *Int. J. Power Electron. Drive Syst.* **2019**, *10*, 342–350.



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

Article

U-Slot Utilization in CPW-Fed UWB Trapezoidal Monopole Antennas for Band Notched Applications[†]

Manolis G. Tampouratzis ^{1,*} , Evangelos Katsos ², Demosthenes Vouyioukas ¹ ,
Traianos Yioultsis ³  and Dimitrios Stratakis ⁴ 

¹ Department of Information and Communication Systems Engineering,
University of the Aegean, Karlovasi, GR 83200 Greece; {tampouratzis, dvouyiou}@aegean.gr

² Faculty of Pure and Applied Sciences,
Open University of Cyprus (OUC), Nicosia, CY 2252 Cyprus; evangelos.katsos1@st.ouc.ac.cy

³ Department of Electrical and Computer Engineering (ECE),
Aristotle University of Thessaloniki (AUTH), Thessaloniki, GR 54124 Greece; traianos@auth.gr

⁴ Department of Electrical and Computer Engineering (ECE),
Hellenic Mediterranean University (HMU), Heraklion, GR 71004 Greece; dstrat@hmu.gr

* Correspondence: tampouratzis@aegean.gr

[†] This paper is an extended version of our paper published in 26th International Conference on Circuits, Systems, Communications and Computers (CSCC), Platanias, Chania, Crete Island, Greece, 19-22 July 2022.

Received: date; Accepted: date; Published: date

Abstract: Planar CPW-Fed trapezoidal monopole antennas with single and dual/triple band rejection characteristics are presented in this study which can be used to remove interfering frequencies from wireless communication systems such as Wi-Fi, military services and WiMAX networks at 2.4 GHz, 3 GHz and 3.5 GHz respectively. The proposed antennas prototypes were assembled on single layer FR4 substrate with $\epsilon_r=4.35$ occupying small surfaces of 49 mm x 57 mm and U-shaped slots were utilized. VSWR of 2:1 in the frequency band of 1.6 - 3.8 GHz and notch mismatches up to 10:1 while maintaining omnidirectional patterns in the H-plane are satisfied by the proposed antennas. Moreover, measurement results using the Keysight Fieldfox N9915A Vector Network Analyzer (VNA) are compared with theoretical study of the antennas.

Keywords: Trapezoidal Monopole Antennas; Coplanar Waveguide (CPW); Single Frequency Notch; Dual/Triple Frequency Notch; Band Rejection; UWB Planar Antennas; U-Shaped Slot.

1. Introduction

Several Ultra-Wideband (UWB) antennas with band-notch characteristics using slot structures have been proposed by antenna designers [1] aiming to avoid interference between them and narrow bandwidth communication systems. Federal Communications Commission (FCC) has proposed variations on trapezoidal monopole antenna for use in UWB region from 2 GHz to 10 GHz [2,3]. A special kind of slot (U-shaped slot) was introduced in [4] and the initial investigations were based on air and foam substrate. In [2,3] showed that when material substrate was used instead of air and foam substrate the respective antennas maintained their wideband characteristics. U-shaped slot constitutes a relatively simple and widespread structure for band rejection characteristics in a UWB antenna. The structure can be applied on the antenna design to achieve the desired impedance and can be experimentally adjusted for the desired frequency response; i.e., changing the position of the slot, lower or higher notched bands can be generated avoiding possible interferences in undesired frequencies [5]. It is observed that the slot width should be small compared to the slot length, and the higher resonant mode is sensitive to the horizontal slot length variation, while the lower resonant mode is highly dependent on the perimeter of the slot structure [6].

Techniques used for obtaining notch characteristics may vary, including the insertion of other slot structures such as C-shaped, E-shaped, I/J-shaped, H-shaped, L-shaped, W-shaped except from U-shaped at the radiation patch of the antenna. In addition, the most common feeding methods are distinguished into microstrip and coplanar waveguide transmission line (CPW), which are used on different radiating element configurations; e.g., trapezoidal, rectangular, circular/elliptical or other patches [7].

The work in [8] introduced a pentagonal compact CPW-Fed monopole antenna implementation on FR4 substrate with triple-band operation, ideal for WiMAX and WLAN applications consisting of a simple planar structure (25 mm x 25 mm) and two inverted U-shaped slots for dual stopband generation. Another single-band notched UWB CPW-fed trapezoidal monopole antennas with omnidirectional radiation patterns are proposed in [9], to avoid undesired interferences from military and satellite telecommunication band. In [1] a microstrip feed, compact multiband printed monopole antenna utilizes three inverted U-shaped slots on the radiant patch to avoid interferences from 3 GHz, 4.25 GHz and 6.25 GHz. The antenna's measurement results show that the proposed monopole efficiently operates at the bands of Bluetooth, WiMAX, WLAN, and X-band satellite communication systems. The elimination of radio bands 5.7 - 5.8 GHz and 7.25 - 7.30 GHz is carried out by the monopole's open slots and the parasitic loop utilization respectively. In [10], another compact UWB antenna with band-notched characteristics for 5.15 - 5.825 GHz by U-shaped slot utilization and microstrip feeding method is presented. The work in [4] introduced a novel CPW-fed UWB monopole antenna in compact implementation (35 mm x 30 mm) with dual band notched characteristics by inserting two nested inverted U-shaped slots to the trapezoidal patch. The proposed antenna successfully covers the entire operating bandwidth (3.1 GHz - 10.6 GHz), having two frequency notches from 3.55–4.57 GHz and 5.55–6.87 GHz. Dual notched characteristics centered at 3.5 and 5.5 GHz appears to UWB microstrip-fed rectangular antennas in [11,12] by etching opposite U-shaped slots to avoid interferences from WiMAX and WLAN or HYPERLAN/2 networks respectively.

The C-shaped slot as a variant of U-shaped slot structure, constitutes another good solution for band notched characteristics in a UWB antenna. The authors in [13] propose a CPW-fed rectangular metal patch antenna to avoid interference from 5 GHz WLAN by C-shaped slot utilization, while simultaneously maintains broadband matched impedance, stable gain and radiation patterns at the bandwidth of 3.1 - 10.6 GHz. The work in [14] introduced a compact and simple design CPW-fed planar antenna for UWB applications with dual band-notch characteristics at 3.3 – 3.9 GHz and 5 – 6 GHz by two nested C-shaped slots utilization. The authors in [15] propose a planar, single-band notched CPW-Fed UWB antenna consists of a rectangular metal radiation patch and a tapered arc-shaped ground plane with band-notch characteristic at 5.5 GHz by C-shaped slot utilization. The proposed antenna appears wide operation bandwidth, satisfactorily band-notch characteristic, stable radiation patterns, good gain flatness and compact size in combination with easy design.

With the combination of slot structures and split ring resonators (SRR) or complimentary split ring resonators (CSRR), UWB antennas appears multiband-notch characteristics with high VSWR values at undesired frequencies. In [16] a UWB CPW-fed monopole antenna is presented with triple band stop functions. The proposed antenna consists of SRR and inverted U-slots on the metallic patch to avoid interferences from WiMAX, WLAN and C bands, maintaining the wide operation bandwidth (3 to 11 GHz) and the compact size of 26 mm x 30 mm.

In this work, the design methodology of planar CPW-Fed UWB trapezoidal monopole antennas with single and dual/triple band rejection characteristics by U-shaped slot utilization is presented. The proposed antennas can be used to remove interfering frequencies from wireless communication systems such as Wi-Fi, military services and WiMAX networks at 2.4 GHz, 3 GHz and 3.5 GHz respectively, as enhancing the work in [17]. In our approach has been taken into consideration the small and single layer implementation surface in combination with CPW-feeding. The antenna prototypes were tested on the laboratory and also in urban environment.

The rest of this article is organized as follows: the structure description of UWB Planar CPW-Fed Trapezoidal Monopole as reference antenna is presented and analyzed in Section 2. Section 3 gives

the U-shape slot utilization for Single Frequency Notch in Trapezoidal Monopole antenna to avoid possible military service interference at 3 GHz. Also, this section is devoted to present the electric circuit equivalent of the structure. The Simulation Results of the impedance and radiation characteristics, current distributions and gain of the proposed Single Notched Monopole Antenna are described in Section 4. Section 5 gives the description of the proposed U-shaped CPW-Fed Trapezoidal Dual and Triple Notched Monopole Antennas for interfering frequencies rejection both from WiFi, military services and WiMAX networks at 2.4 GHz, 3 GHz and 3.5 GHz, respectively. The Simulation Results of the proposed dual notched antenna are also presented in this section. Section 6 is devoted to Parametric Study Analysis Simulation Results and finally in Section 7, the comparison with other State-of-the-Art designs is presented.

2. The Planar CPW-Fed Trapezoidal Monopole UWB Antenna

Planar antennas of this kind are fed by a microstrip line or Coplanar Waveguide (CPW) at their base. Their width is increasing towards the top of the monopole in a continuous or stepped fashion. They are very popular in mobile communications due to their reduced size and wide impedance bandwidth and can also be used in broadband RF energy harvesting such as a UWB discone antenna [18] in combination with planar implementation. The trapezoidal monopole's increased impedance bandwidth with respect to that of a rectangular monopole is due to the step and/or tapered bottom edges which ensure a broadband impedance transition. Aiming in this study to achieve a reflection coefficient (S_{11}) of below -10 dB (which corresponds to $VSWR < 2:1$) across a 4:1 bandwidth, the proposed antenna designed to have a triangular base and a rectangular top section with its ground plane in the same plane with the antenna. This type of antenna can be integrated on the same printed circuit board with the transmitter electronics, requiring only one metallized dielectric substrate [19]. Furthermore, coplanar waveguides are particularly useful for fabricating active circuitry due to the presence of the center conductor and the proximity of the ground planes [20].

2.1. Structure Description

The antenna consists of a planar rectangular monopole element with tapered bottom and is fed by a Coplanar Waveguide (CPW) similar with the slotline. Thus, it can be viewed as a slotline with a third conductor centered in the slot region. Due to the presence of the additional conductor, even or odd quasi-TEM modes can be supported by this type of line, depending on whether the electric fields in the two slots are in the opposite or in the same direction.

The prototype implementation of the antenna was made on standard single layer FR4 substrate with relative permittivity (ϵ_r) 4.35, substrate height (h_s) 1.65 mm, loss tangent ($\tan\delta$) 0.025 and metal thickness (h_{mt}) 0.035 mm occupying a small planar surface of 50mm x 58mm (Figure 1), where the equations used for the antenna construction are the following:

$$W = \frac{c}{2f} \sqrt{\frac{2}{\epsilon_r + 1}} \quad (1) \quad L_{eff} = \frac{c}{2f \sqrt{\epsilon_{reff}}} \quad (2)$$

$$\Delta L = 0.5 \cdot h \quad (3) \quad L = L_{eff} - (2 \cdot \Delta L) \quad (4)$$

where c is the speed of light in free space, L , L_{eff} , W and h are the length, the effective length, the width, and the substrate's height of the resonant patch respectively. Although these design equations strictly refer to a grounded patch antenna, we will apply them for an estimation of initial dimensions of the CPW-fed monopole, by considering a modified choice of the effective dielectric constant, as it will be shown in the next paragraph.

The patch has the form of a rectangle with a step at its upper end. Tapered section is used for the connection of rectangular patch with the feed line, and a cylindrical SMA connector is located at the end. This tapered variation improves the matching of the antenna over the operating bandwidth, and the resonant length is a function of the substrate parameters and the operating frequency. However, in this case the patch does not contain a ground plane on the other side of the substrate, hence the effective relative permittivity of the dielectric substrate ϵ_{reff} given by [3]:

$$\epsilon_{\text{reff}} = \frac{\epsilon_r + 1}{2} + \frac{\epsilon_r - 1}{2} \left[1 + A \frac{h}{W} \right]^{-1/2} \quad (5)$$

has to be modified for the constant A , where A is the multiplication coefficient for the term h/W , h is the substrate's height and W is the substrate's width respectively. By simulating different patches with different substrate parameters, it is possible to obtain the appropriate value of the multiplication coefficient A . In [3] the well-suited value of A was found to be 11.25.

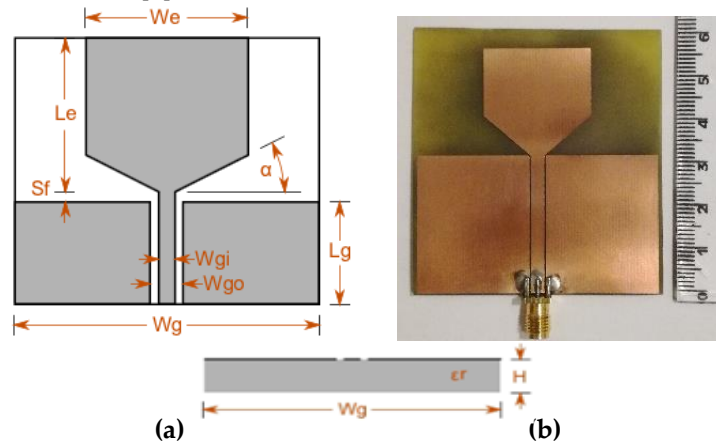


Figure 1. (a) Design Parameters of proposed CPW-fed UWB (1.6 - 3.8 GHz) Trapezoidal monopole as reference antenna and (b) the fabricated prototype on FR4 substrate.

Since the capacitance of the gap increases while the distance is decreasing, the width of the gap between the patch and the ground in the longitudinal direction has an important effect for impedance matching. The parameters of the trapezoidal patch i.e.: the gap (S_f), the height of the patch (L_e), the width of the patch (W_e) and the angle (α) are crucial for determining the performance of the antenna. According to [21]:

- **Patch Height (L_e):** The first resonant point in the operation band decreases when increasing the height L_e of the antenna, and an appropriate height should be chosen to obtain the optimized performance of the antenna.
- **Gap Width (S_f):** The width of the gap determines the capacitance between the radiating element and the ground in the longitudinal direction influencing the impedance matching of the antenna, and smaller gap width results in higher capacitance.
- **Patch Width (W_e):** The width W_e has no noticeable effect on the performance of the antenna.

3. The U-shaped CPW-Fed Trapezoidal Monopole Antenna With Single Frequency Notch

A side effect of the UWB radio band is possible interference at 3 GHz frequency which used by military applications [22]. One way of reducing this problem, is to incorporate a U-shaped slot near the base of the monopole. At the resonant frequency of the slot, the reflection coefficient is much larger than in the rest of the band, rejecting the interfering signal. Prototype implementation and physical parameters of the proposed single band rejection monopole antenna are shown at Figure 2b and Table 1, respectively.

3.1 The U-Shaped Slot for Band Notched Rejection

The antenna's slot in this study, is U-shaped aiming to reject undesired notch frequencies and having reflection coefficient (S_{11}) below -10 dB across a 4:1 bandwidth with a notch mismatch of above -3 dB. The U-shaped slot is cut into the monopole element. The total slot length (L_{slot}) was experimentally calculated to be approximately $0.57\lambda_{\text{eff_slot}}$:

$$L_{\text{slot}} = L_{sb} + 2L_{ss} - w_s = 0.57\lambda_{\text{eff_slot}} \quad (6)$$

where λ_{eff_slot} is the effective slot wavelength at the center frequency of the rejected band. The effective wavelength of the slot is given by:

$$\lambda_{eff_slot} = \frac{\lambda_0}{\sqrt{\epsilon_{eff_slot}}} \quad (7)$$

$$\epsilon_{eff_slot} = \frac{\epsilon_r + 1}{2} \quad (8)$$

and λ_0 is the resonant wavelength. This slight difference from half wavelength can be observed due to the fringing effect of the field at the ends of the slot. This slot corresponds to a nearly half-wavelength resonator at the center frequency of the required stop-band and introduces high reflection at its resonance frequency which corresponds to the operation of a band-rejection filtering effect. Thus, at first approximation, in order to obtain the notch frequency (f_{notch}), the required slot length (L_{slot}) is given by the following modified equation:

$$L_{slot} = \frac{0.57 \cdot c}{f_{notch} \cdot \sqrt{\epsilon_{eff_slot}}} \quad (9)$$

This value is used to optimize the slot length and obtain exactly the required band-rejection. It has to be noticed that the slot length has higher effect on the band-rejection than the slot width as the simulations of the antenna showed (the same result was found in [3]).

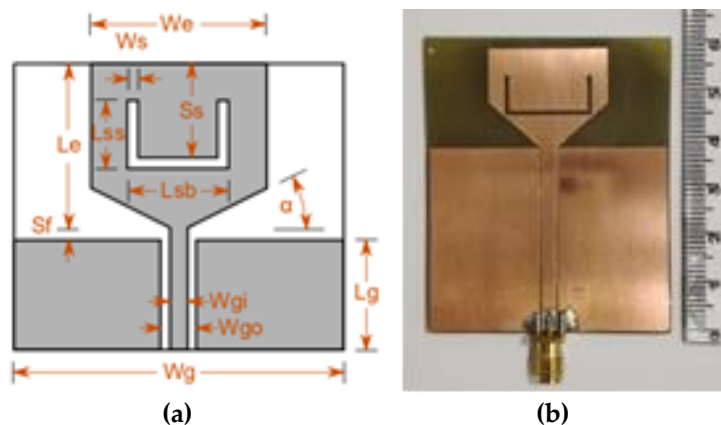


Figure 2. (a) Design Parameters of proposed single band rejection CPW-fed UWB Trapezoidal monopole antenna and (b) the fabricated prototype on FR4 substrate.

Table 1. Physical Parameters of proposed Single Band Rejection CPW-fed UWB Trapezoidal Monopole Antenna fabricated on FR4 substrate.

Parameter	Description	Value	Parameter	Description	Value
L_e	Monopole element length	20.5 mm	W_e	Monopole element width	25 mm
α	Taper angle at monopole base	40°	S_f	Feed gap	88.76 μ m
W_g	Ground-plane width	50 mm	L_g	Ground-plane length	37.5 mm
W_{gi}	CPW inner width	3 mm	W_{go}	CPW outer width	3.9 mm
W_s	Slot width	1 mm	L_{sb}	Slot bottom length	18.5 mm
L_{ss}	Side slot length	8.5 mm	S_s	Slot offset	12.5 mm

3.2. The U-Shaped Slot Equivalent Circuit

The U-shaped slot can be considered as combination of three slot as shown in Figure 2a. Among these, two vertical slots are the arms of the U-slot having dimension ($L_{uv} \times W_{uv}$) and the third one is base of the U-slot and it is horizontal ($L_{ub} \times W_{ub}$), according to [27]. The equivalent circuit of a narrow

slot comprises a series combination of radiation resistance (R_s) and the reactive component (X_s) as shown in Figure 3.



Figure 3. Equivalent circuit of slot.

Therefore, the impedance of the vertical slot can be given as:

$$Z_{UV} = R_{UV} + jX_{UV} \quad (10)$$

where

$$R_{UV} = 60 \left\{ \begin{aligned} & C + \ln(kL_{UV}) - Ci(kL_{UV}) + \frac{1}{2} \sin(kL_{UV}) [Si(2kL_{UV})2Si(kL_{UV})] + \frac{1}{2} \cos(kL_{UV}) \\ & \left[C + \ln\left(\frac{kL_{UV}}{2}\right) + Ci(2kL_{UV}) - 2Ci(kL_{UV}) \right] \end{aligned} \right\} \quad (11)$$

and

$$X_{UV} = 30 \cos^2 a \left\{ \begin{aligned} & 2Si(kL_{UV}) + \cos(kL_{UV}) [2Si(kL_{UV}) - Si(2kL_{UV}) - \sin(kL_{UV})] \\ & \left[2Ci(kL_{UV}) - Ci(2kL_{UV}) - Ci\left(\frac{2kW_{UV}^2}{L_{UV}}\right) \right] \end{aligned} \right\} \quad (12)$$

in which $C=0.5772$ is Euler's constant, k is the propagation constant in free space and functions Si and Ci are the sine and cosine integrals defined as:

$$S_i(x) = \int_0^x \frac{\sin(x)}{x} dx \quad (13) \quad \text{and} \quad C_i(x) = -\int_x^\infty \frac{\sin(x)}{x} dx \quad (14)$$

Similarly, the impedance of the base slot can be given as:

$$Z_{UB} = R_{UB} + jX_{UB} \quad (15)$$

where

$$R_{UB} = 60 \left\{ \begin{aligned} & C + \ln(kL_{UB}) - Ci(kL_{UB}) + \frac{1}{2} \sin(kL_{UB}) [Si(2kL_{UB})2Si(kL_{UB})] + \frac{1}{2} \cos(kL_{UB}) \\ & \left[C + \ln\left(\frac{kL_{UB}}{2}\right) + Ci(2kL_{UB}) - 2Ci(kL_{UB}) \right] \end{aligned} \right\} \quad (16)$$

and

$$X_{UB} = 30 \cos^2 a \left\{ \begin{aligned} & 2Si(kL_{UB}) + \cos(kL_{UB}) [2Si(kL_{UB}) - Si(2kL_{UB}) - \sin(kL_{UB})] \\ & \left[2Ci(kL_{UB}) - Ci(2kL_{UB}) - Ci\left(\frac{2kW_{UB}^2}{L_{UB}}\right) \right] \end{aligned} \right\} \quad (17)$$

where L_{UV} is the length of vertical slot, L_{UB} is the length of base slot, W_{UV} is the width of vertical slot and W_{UB} is the width of the base slot respectively. Hence the input impedance Z_U for *U-shaped* slot can be calculated by:

$$Z_U = \frac{Z_{UV} + 2Z_{UB}}{Z_{UV}Z_{UB}} \quad (18)$$

in which Z_{UV} is the input impedance of vertical slot and Z_{UB} is the input impedance of base slot.

The equivalent circuit of a U-shaped slot presents at Figure 4, where R_{UV} the radiation resistance of vertical slot, R_{UB} the radiation resistance of base slot, X_{UV} the reactive component of vertical slot and X_{UB} the reactive component of base slot respectively.

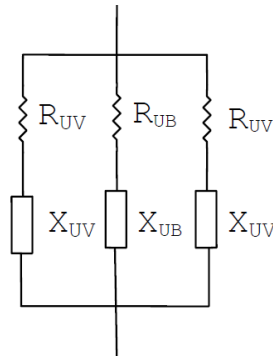


Figure 4. Equivalent circuit of U-shaped slot.

4. The Single Notched Monopole Antenna Simulation Results

4.1 Impedance Characteristics

The trapezoidal monopole's increased impedance bandwidth with respect to that of a square or rectangular monopole is depended on the tapered bottom edges which ensures a broadband impedance transition. The length of the element determines the minimum operating frequency, and the reflection coefficient at higher frequencies is affected by several factors. These include the shape of the base taper and the ground-plane dimensions. There are numerous small changes which can be made to the basic topology to reduce the reflection coefficient across the whole band. Examples of this include cutting notches or steps in the base or top of the monopole element [2,3]. The impedance mismatch at slot resonance is generally high but tends to diminish at higher resonant frequencies. The ratio of notch frequency to minimum frequency is limited by the available space on the monopole, the slot shape, and the type of the substrate [19]. Figure 5a presents the input impedance of the proposed single band notched, 5b the simulated gain and Figure 6 presents the simulated and measured VSWR for military service interference rejection at 3 GHz. The simulation was carried out with Antenna Magus software in cooperation with CST Microwave Studio Suite software.

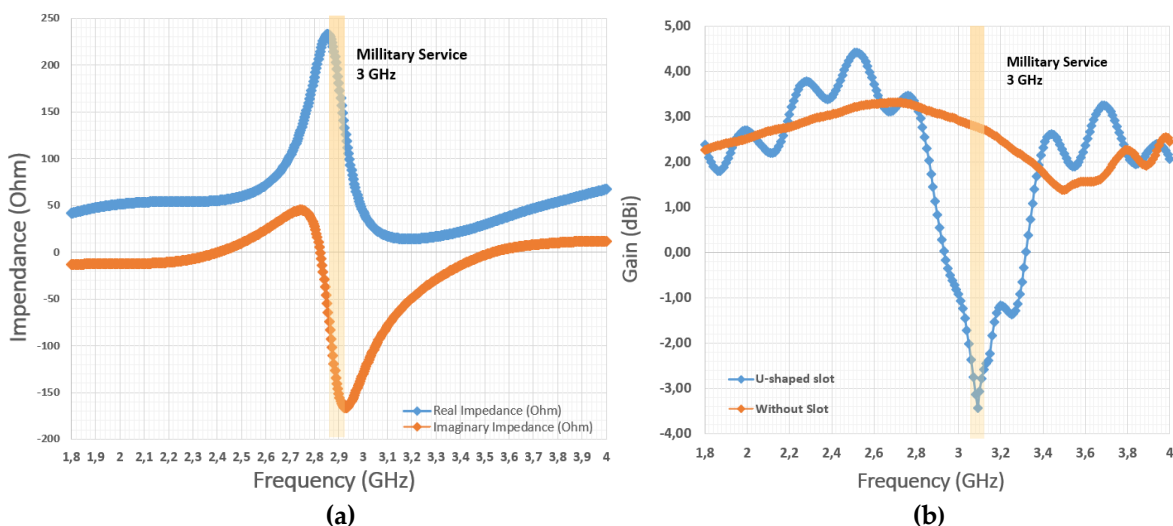


Figure 5. (a) Input impedance and (b) simulated gain of the proposed single band notch antenna for military service rejection at 3 GHz.

4.2 Radiation Characteristics

The radiation of the single slot proposed trapezoidal monopole antenna is similar to a planar monopole extending beyond a ground plane, but the asymmetrical geometry distorts the pattern especially at the higher frequencies. This antenna can typically be used in a multi-path environment

where radiation pattern is not a limiting factor [19], since the beamwidth calculated from the simulations (Figure 7) is wide enough.

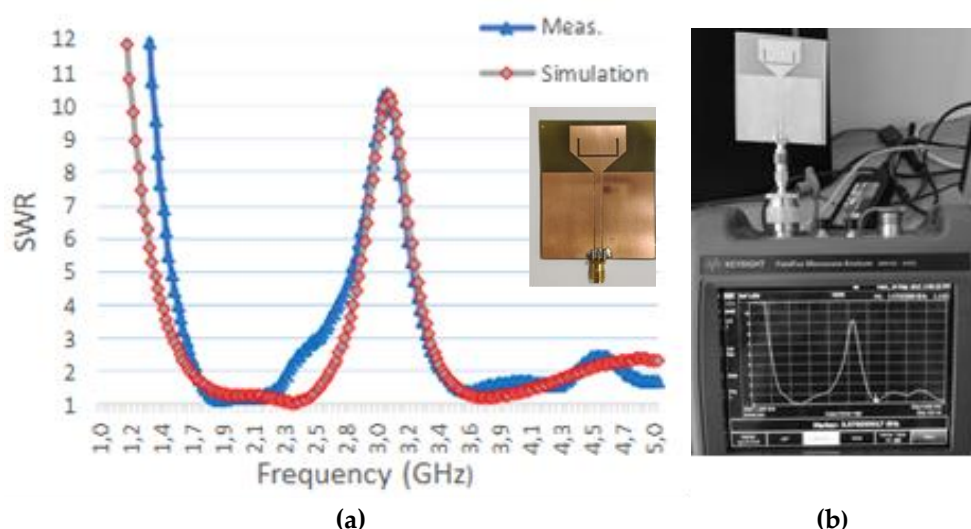


Figure 6. (a) Simulated and Measured VSWR of proposed single band notched CPW-fed UWB Trapezoidal monopole antenna for rejection at 3GHz and (b) Laboratory measurements of proposed prototype on Keysight N9915 VNA.

4.3 Design Guidelines

Low permittivity substrates tend to require very narrow gaps in the co-planar waveguide when designed for 50 Ω line impedance. This makes their construction difficult. In addition, the metal thickness may be of the same order as the gap width, leading to lower line impedance. For the appropriate design of the antenna the below results shall be considered [2,3,19]:

- S_{11} value can be minimized over the operating band by adjusting the taper angle and the feed gap,
- further S_{11} reduction may be obtained by cutting optimized notches or steps in the base or top of the monopole element,
- the notch frequency can be decreased by increasing the total slot length, and
- the notch band rejection may be increased by moving the bottom corners of the slot closer to the bottom of the monopole element.

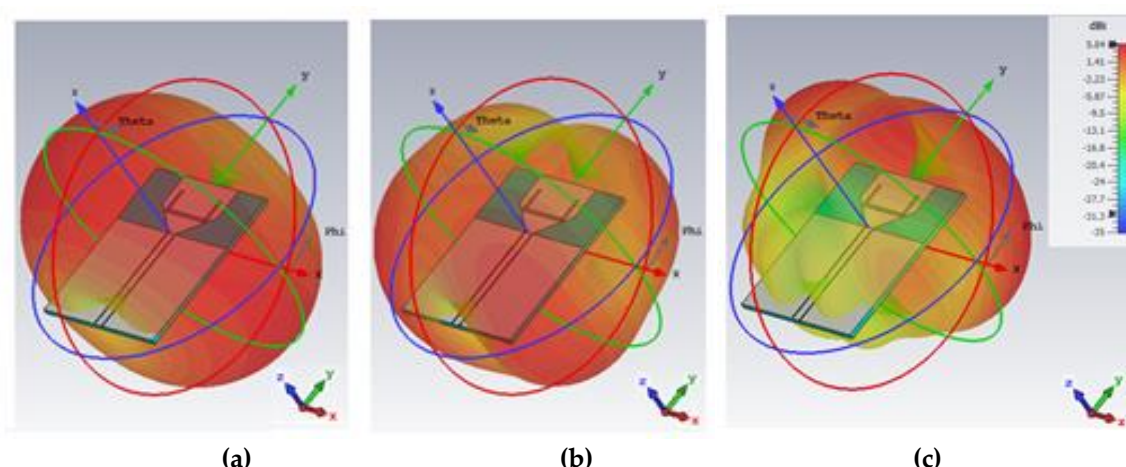


Figure 7. 3D radiation patterns of proposed single band notched CPW-fed UWB Trapezoidal monopole antenna at (a) 1GHz, (b) 2 GHz and at rejected frequency: (c) 3.5 GHz.

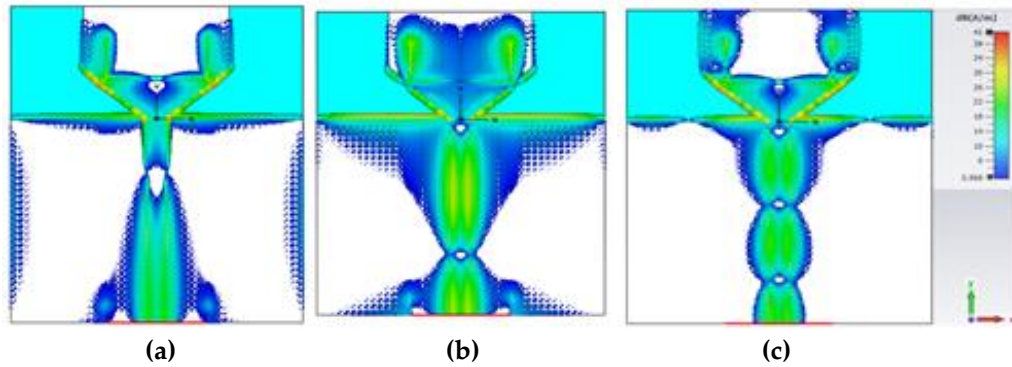


Figure 8. Current distributions of proposed single notched CPW-fed UWB Trapezoidal monopole antenna at (a) 1GHz, (b) 2 GHz and at rejected frequency: (c) 3.5 GHz.

5. The U-shaped CPW-Fed Trapezoidal Dual / Triple Notched Monopole Antenna

In this section, a dual and a triple band-notched UWB CPW-fed trapezoidal monopole antennas are presented. Two nested notch elements are formed in the proposed trapezoidal monopole antenna to remove interfering frequencies both from military services and WiMAX networks at 3 GHz and 3.5 GHz respectively [22] and additionally one for 2.4 GHz Wi-Fi band rejection. The frequency-notch function was achieved by inserting two or three nested U-shaped slots into the antenna. By properly adjusting the dimensions of the inserted slot, the proposed antenna revealed good UWB performance, accompanied by a dual or triple band-rejection function. The notch frequency can be adjusted by changing the slot length [4]. The length of the slot should be approximately half the effective guided wavelength as described by equation (6).

The lengths L_{ss} , L_{ss-2} and L_{ss-3} of the antenna's slots both become critical for determining the center frequency of the notched bands, because the slots act as quarter-wavelength resonators at the desired frequencies. Optimizing the lengths L_{ss} , L_{ss-2} and L_{ss-3} numerically and experimentally, the undesired frequency bands can be notched [4].

The band-rejection frequencies can be changed by changing lengths of the U-shaped slots with the other parameters fixed. Thus, the center frequency of every band notch is shifted towards lower frequencies by increasing L_{slot} [23]. The resonant frequency of each U-shaped slot can be approximately calculated by:

$$f_{ni} = \frac{170}{l_{ni}\sqrt{\epsilon_{eff_slot}}} \text{GHz} \quad (19)$$

where f_{ni} denotes the resonant frequency of the i th band-notch structure and l_{ni} denotes the length, expressed in millimeters, of the i th band-notch structure with i being the number of slots. As it can be shown from (19) increasing l_{ni} , f_{ni} is decreased [1]. Prototypes implementation and design parameters are shown at Figure 9.

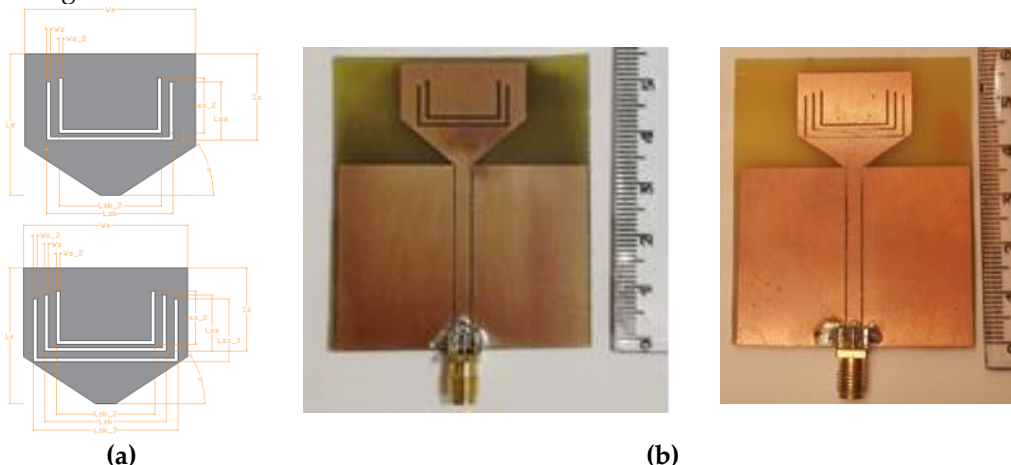


Figure 9. (a) Radiation elements design parameters of proposed dual and triple band rejection CPW-fed UWB Trapezoidal monopole antennas. (b) Fabricated prototypes on FR4 substrate.

5.1 Impedance Matching – VSWR

In Figure 10a the simulated and the measured VSWR performance for distinct values of U -slot lengths are presented (the respective parameters are shown in Table 2). The antenna appears dual band-notched characteristics (up to 8:1 value of VSWR) at the rejected frequencies of 3 GHz and 3.5 GHz. Figure 11a illustrates the simulated and the measured VSWR performance of proposed triple band notched antenna for additionally band rejection at 2.4 GHz (up to 9:1 value of VSWR). According to the literature, as the slot length value varies from a lower value, the notch frequency is shifted to lower frequencies. Figures 19a, 20a presents the input impedance and Figures 19b, 20b presents the simulated gain of the proposed dual and triple band notched antennas, respectively. In Figures 10b and 11b, the VSWR measurement setup at the laboratory is presented, where the Keysight FieldFox N9915A VNA was used.

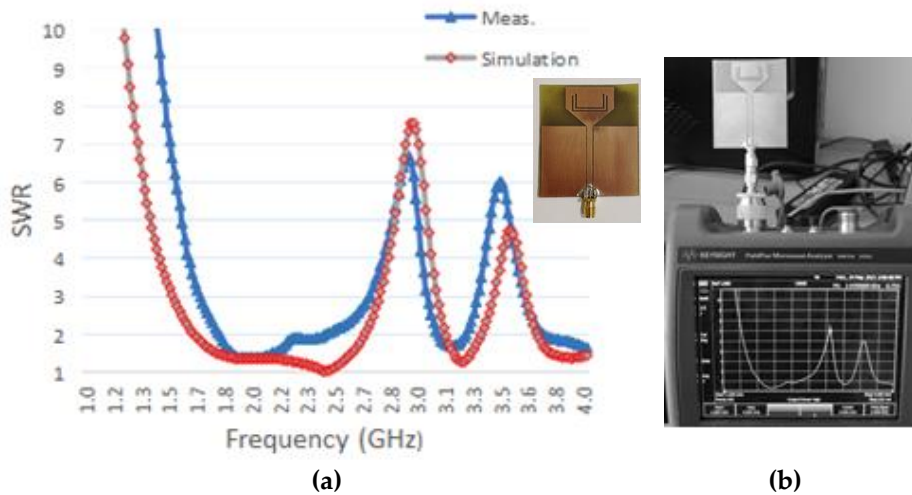


Figure 10. (a) Simulated and Measured VSWR of proposed dual band notched CPW-fed UWB Trapezoidal monopole antenna for rejection at 3 GHz and 3.5 GHz. (b) Laboratory measurements of proposed prototype on Keysight N9915 VNA.

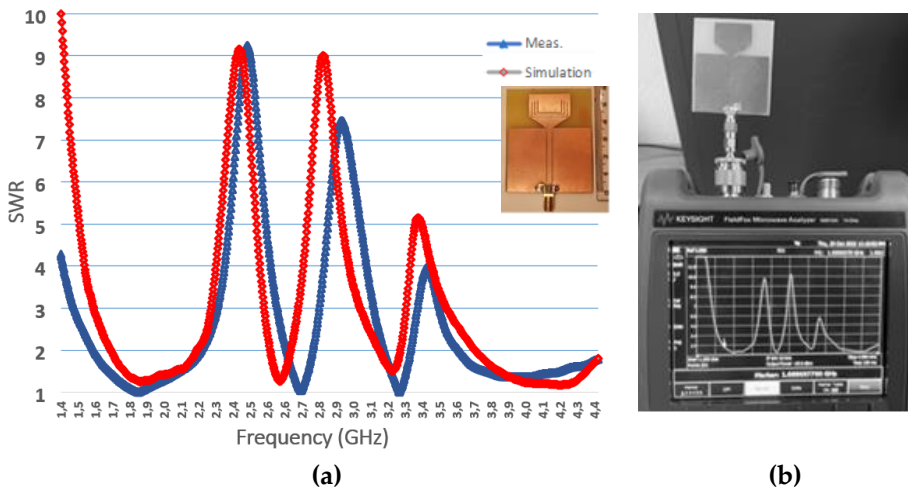


Figure 11. (a) Simulated and Measured VSWR of proposed triple band notched CPW-fed UWB Trapezoidal monopole antenna for rejection at 2.4 GHz, 3GHz and 3.5 GHz. (b) Laboratory measurements of proposed prototype on Keysight N9915 VNA.

5.2 Current Distribution

In Figure 8, Figure 12 and Figure 13 the surface current distributions for single, dual and triple notched antennas are presented at notch frequencies of 2.4 GHz, 3 GHz and 3.5 GHz. It has to be noticed that the current is mainly concentrated around the U -shaped slots, and flows in the opposite direction at notch frequency. Strong attenuation and cancellation of the radiating field is observed when the current is out of phase and flows in the opposite direction [24].

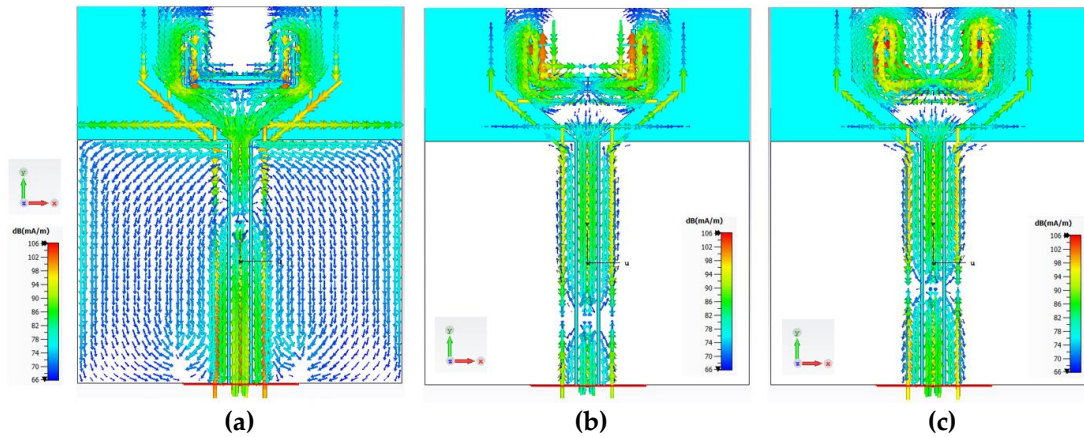


Figure 12. Current distributions of proposed dual notched CPW-fed UWB Trapezoidal monopole antenna at (a) 2GHz and at rejected frequencies: (b) 3 GHz and (c) 3.5 GHz.

On the other side, increasing the frequency, the electrical length of the antenna is getting more than the half wavelength. In this scenario, the surface current distributed on the radiating patch will be destructive, and reduction of the radiation pattern at this frequency will be detected [1]. The placement of *U*-slot disturbs the surface current creating another notched band except the band created by the outer dimensions of the patch. The shift of resonance occurs due to the new electrical path that surface current follows when the width of *U*-slot is changed [25].

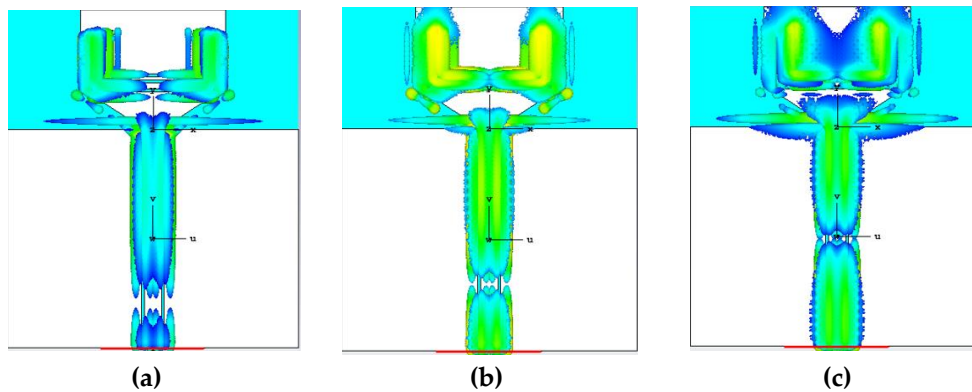


Figure 13. Current distributions of proposed triple notched CPW-fed UWB Trapezoidal monopole antenna at rejected frequencies: (a) 2.4 GHz, (b) 3 GHz and (c) 3.5 GHz.

5.3 Radiation Characteristics

The radiation of the proposed double or triple notch antennas is also similar to a planar monopole, as that of the single notch antenna. The omnidirectional patterns are maintained throughout the operating bandwidth, but the asymmetrical geometry distorts them, especially at the higher frequencies. The radiation patterns of proposed dual and triple notched antennas are presented at Figure 14 and Figure 15, respectively.

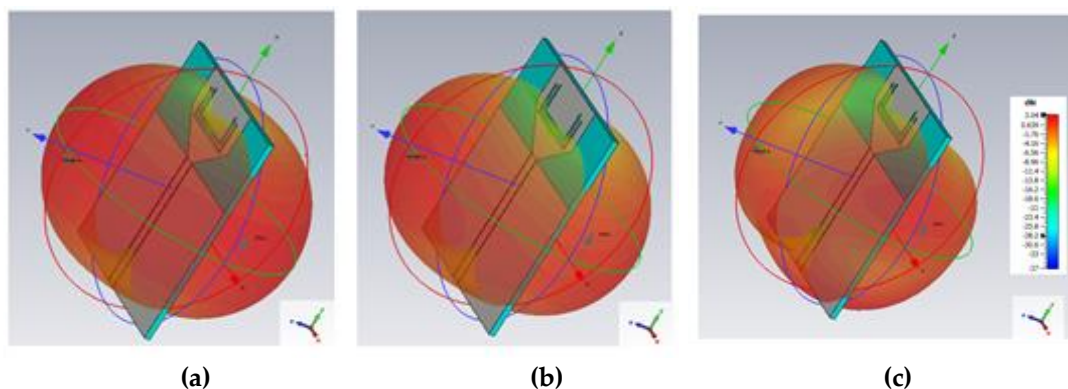


Figure 14. 3D radiation patterns of proposed dual band notched CPW-fed UWB Trapezoidal monopole antenna at (a) 2GHz and at rejected frequencies: (b) 3 GHz and (c) 3.5 GHz.

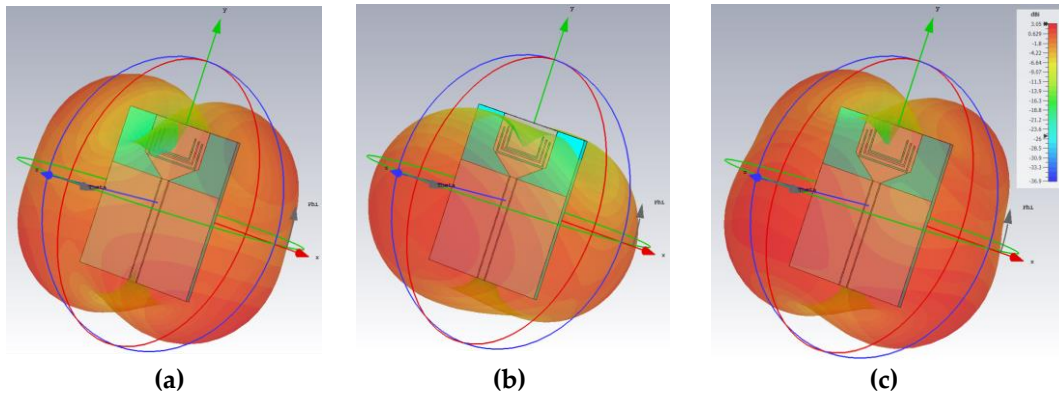


Figure 15. 3D radiation patterns of proposed triple band notched CPW-fed UWB Trapezoidal monopole antenna at rejected frequencies: (a) 2.4 GHz, (b) 3 GHz and (c) 3.5 GHz.

6. Parametric Study Analysis Simulation Results

6.1. Single U-shaped Slot Parametric Study Analysis

The parametric study analysis was carried out with Antenna Magus software. Three basic parameters were examined (Slot bottom length - L_{sb} , Side slot length - L_{ss} , and Slot width - W_s) to accurately determine the dimensions of the U-slot, and consequently apply the desired cut-off frequency of the proposed trapezoidal monopole antenna at 3 GHz.

- Slot bottom length (L_{sb}): As the bottom length of the slot L_{sb} decreases or increases the cut-off frequency becomes higher or lower respectively as shown in Figure 16a [2,26].
- Side slot length (L_{ss}): As the length of the slot L_{ss} decreases or increases, the cut-off frequency moves to higher or lower values respectively, as shown in Figure 16b [4,23].
- Slot width (W_s): Parametric Study Analysis showed that the thickness W_s of the slot does not have such a significant effect on the cut-off frequency. Nevertheless, a slight shift in the cut-off frequency to higher or lower values is observed with a corresponding increase or decrease in the W_s of the notch, as shown in Figure 16c.

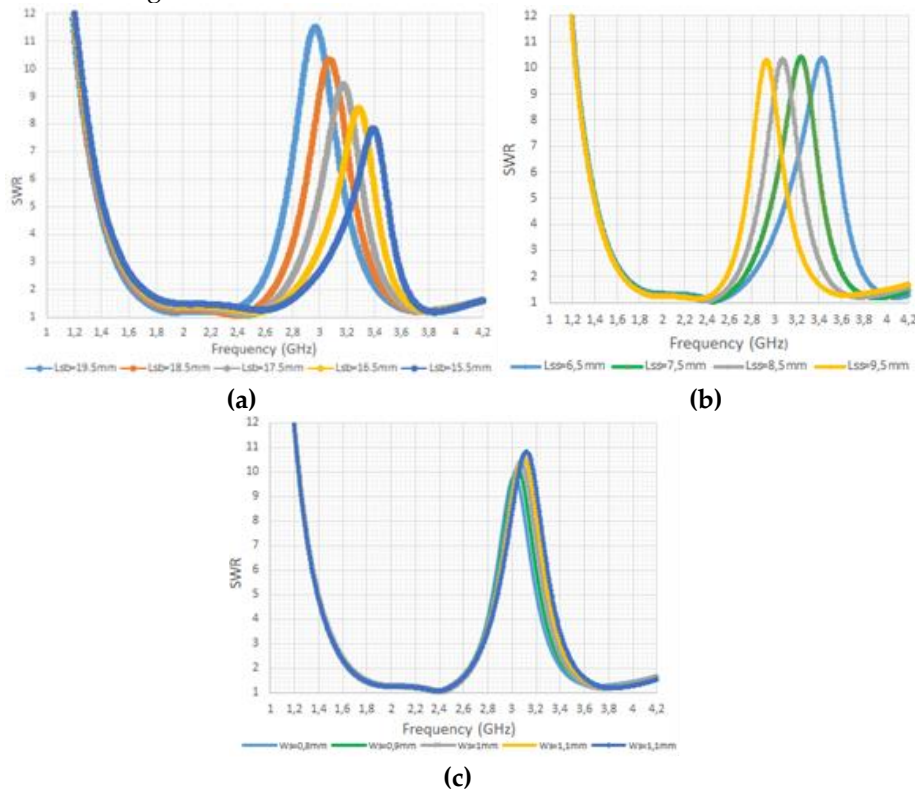


Figure 16. The effect of: (a) Slot bottom length (L_{sb}), (b) Side slot length (L_{ss}) and (c) Slot width (W_s).

6.2. Dual and Triple U-shaped Slot Parametric Study Analysis

Maintaining the initial dimensions of the 1st slot, the parametric analysis of the 2nd and the 3rd one, was also performed for the same parameters (L_{sb-2} , L_{ss-2} , W_{s-2} , L_{sb-3} , L_{ss-3} , W_{s-3}). The simultaneous appearance of the 2nd and 3rd cut-off frequencies at 3.5 GHz and 2.4 GHz of the proposed trapezoidal monopole antennas was a crucial factor for the prototype implementation. Similarly, to the study for the 1st slot, the results from the study for the 2nd and the 3rd slot are presented at Figures 17a to 17c and Figures 18a to 18c, respectively.

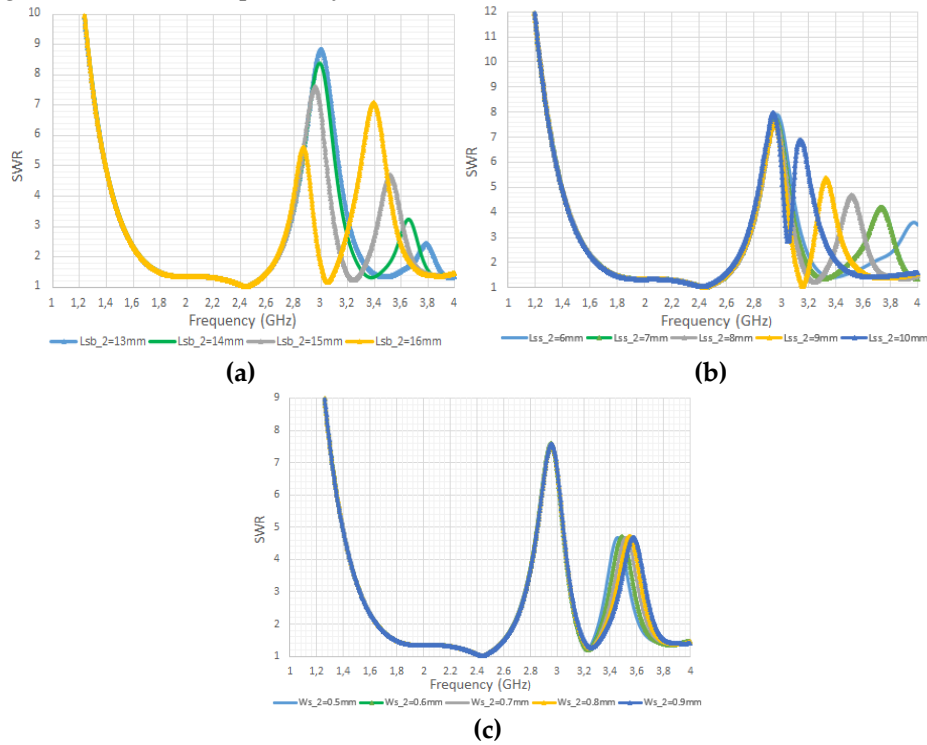


Figure 17. The effect of: (a) 2nd Slot bottom length (L_{sb-2}), (b) 2nd Side slot length (L_{ss-2}) and 2nd Slot width (W_{s-2}).

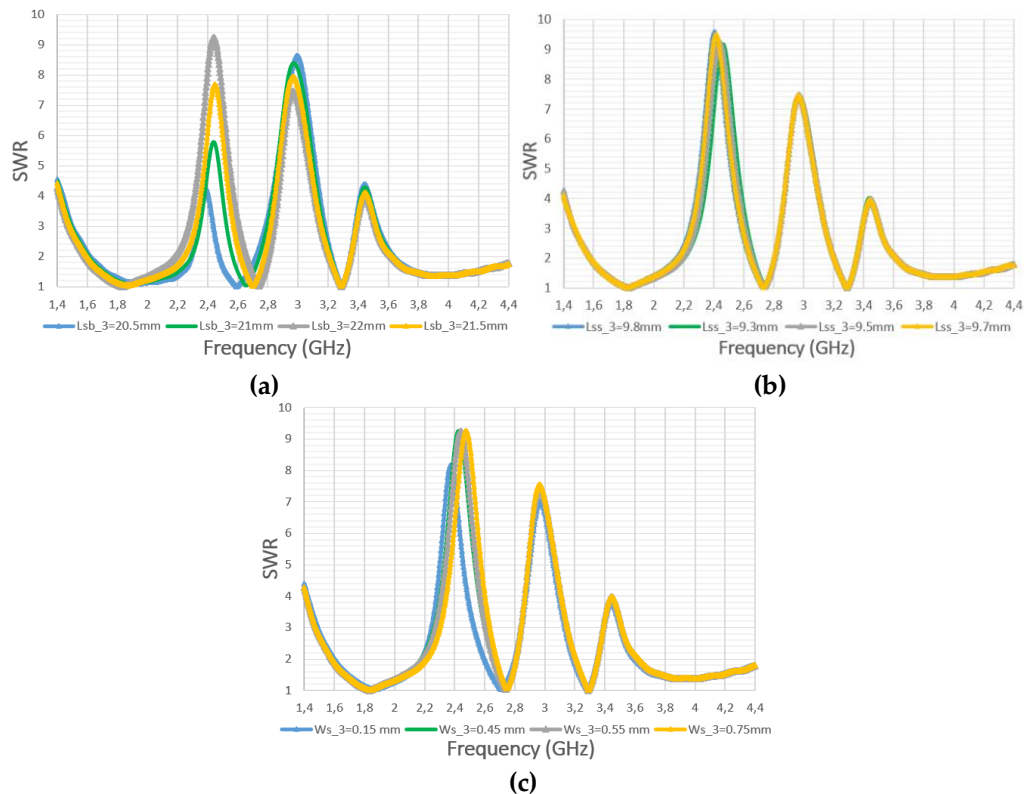


Figure 18. The effect of (a) 3rd Slot bottom length (L_{sb-3}), (b) 3rd Side slot length (L_{ss-3}) and 3rd Slot width (W_{s-3}).

Table 2. Physical Parameters of proposed Dual/Triple Band Rejection CPW-fed UWB Trapezoidal Monopole Antennas fabricated on FR4 substrate.

Parameter	Description	Value	Parameter	Description	Value
L_e	Monopole element length	20.5 mm	W_e	Monopole element width	25 mm
$\alpha_{2/3}$	Taper angle at monopole base	40° / 33°	S_f	Feed gap	88.76 μm
W_g	Ground-plane width	50 mm	L_g	Ground-plane length	37.5 mm
W_{gi}	CPW inner width	3 mm	W_{go}	CPW outer width	3.9 mm
W_s	Slot width	0.7 mm	L_{sb}	Slot bottom length	18.5 mm
L_{ss}	Side slot length	8.5 mm	S_s	Slot offset	12 mm
L_{sb-2}	2 nd Slot bottom length	15 mm	L_{ss-2}	2 nd Side Slot length	8 mm
S_{s-2}	2 nd Slot offset	-6 mm	W_{s-2}	2 nd Slot width	0.7 mm
L_{sb-3}	3 rd Slot bottom length	22 mm	L_{ss-3}	3 rd Side Slot length	9.5 mm
S_{s-3}	3 rd Slot offset	-27.8 mm	W_{s-3}	3 rd Slot width	0.55 mm

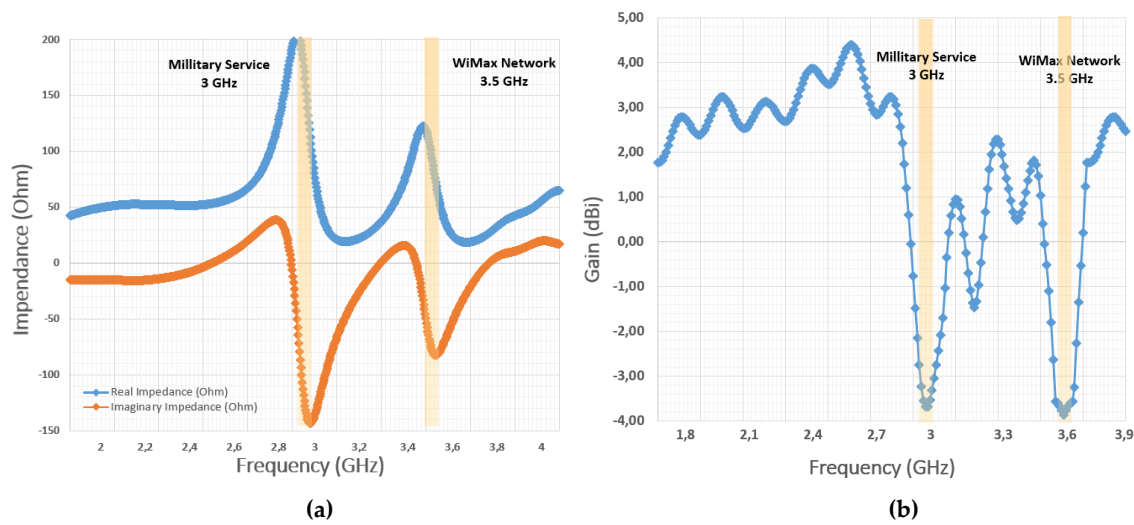


Figure 19. (a) Input impedance and (b) simulated gain of the proposed dual band notched trapezoidal monopole antenna for military service and WiMax rejection at 3 GHz and 3.5 GHz.

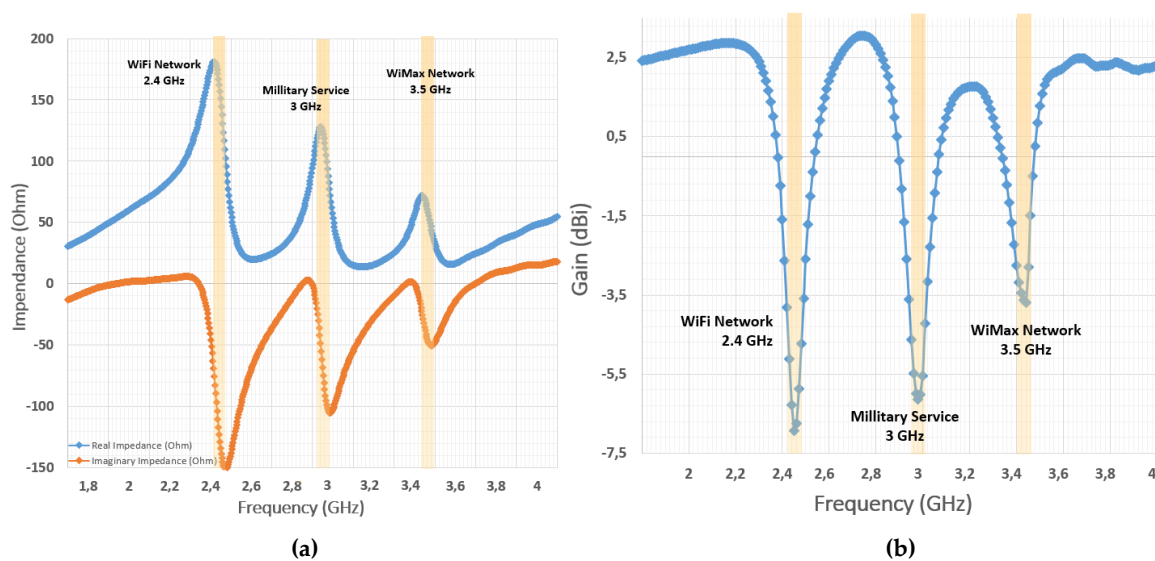


Figure 20. (a) Input impedance and (b) simulated gain of the proposed triple band notched trapezoidal monopole antenna for WiFi, military service and WiMax rejection at 2.4 GHz, 3 GHz and 3.5 GHz.

7. Comparison with Other State-of-the-Art Designs

The design methodology of the proposed planar CPW-Fed UWB trapezoidal monopole antenna with triple band rejection characteristics was also compared with the related literature in terms of implementation techniques, antenna size (mm²), number of notch bands, feeding methods and dielectric constant. This comparison is shown in Table 3, which also reveals that the present antenna has an advantage over the other designs based on of the selected parameters with very simple design complexity to avoid undesired interference from Wi-Fi (2.4 GHz), military services (3 GHz) and WiMax (3.5 GHz) networks, simultaneously. At the same time, the proposed implementation appears an average gain about 2,5 dBi, throughout the operating bandwidth except the rejected frequency bands.

Table 3. Performance comparison with other designs in the literature.

Ref.	Implement. Tech.	Size (mm ²)	Dielectric Const.	No. of Notch	Feeding
[8]	Inverted U-shaped slots	40 mm × 40 mm	FR4	2 (3 / 4.5 GHz)	CPW
[9]	Open slots / Parasitic loop	26 mm × 38 mm	FR4	1 (5.8 / 7.3 GHz)	CPW
[10]	U-shaped slot	28 mm × 24 mm	FR4	1 (5.15-5.825 GHz)	Microstr.
[11]	Opposite U-shaped slots	30 mm × 30 mm	FR4	2 (3.5 / 5.5 GHz)	Microstr.
[13]	C-shaped slot	26 mm × 30 mm	FR4	1 (5.5 GHz)	CPW
[14]	Nested C-shaped slots	26 mm × 30 mm	FR4	2 (3.5 / 5.5 GHz)	CPW
[15]	C-shaped slot	28 mm × 30 mm	FR4	1 (5.5 GHz)	CPW
This work	Nested U-shaped slots	49 mm × 57 mm	FR4	3 (2.4 / 3 / 3.5 GHz)	CPW

8. Conclusions

This study demonstrates the design methodology of planar CPW-Fed UWB trapezoidal monopole antennas with single and dual/triple band rejection characteristics by U-shaped slot utilization. These antennas can be used to avoid possible interferences in undesired frequency bands. In this study antenna prototypes fabricated on single FR4 layer substrates with $\epsilon_r = 4.35$ occupying small surface of 49 mm × 57 mm, and were designed to reject services at 2.4 GHz, 3 GHz and 3.5 GHz. The VSWR measurements taken with a Keysight FieldFox N9915A VNA are compliant with parametric study analysis of the antennas. As a result, band-notched characteristics up to 10:1 VSWR appeared on undesired frequencies while maintaining omnidirectional patterns in the *H*-plane. Summarizing, the proposed antennas seem to be a good solution for UWB communications requiring band-notched applications additionally with planar implementation and small size.

Acknowledgments: «The implementation of the doctoral thesis was co-financed by Greece and the European Union (European Social Fund-ESF) through the Operational Programme «Human Resources Development, Education and Lifelong Learning» in the context of the Act “Enhancing Human Resources Research Potential by undertaking a Doctoral Research” Sub-action 2: IKY Scholarship Programme for PhD candidates in the Greek Universities» (MIS-5113934).

Data Availability Statement: The data used in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare that there is no conflict of interest.

References



1. Junjun Wang, Xudong He, (2013) "Analysis and Design of a Novel Compact Multiband Printed Monopole Antenna", *International Journal of Antennas and Propagation*. [[CrossRef](#)]
2. Lee, J.N. and Park, J.K. (2005), Impedance characteristics of trapezoidal ultra-wideband antennas with a notch function. *Microwave & Optical Technology Letters*, 46: pp 503-506. [[CrossRef](#)]
3. H. M. Zamel, A. M. Attiya and E. A. Hashish, "Design of a Compact UWB Planar Antenna with Band-Notch Characterization," 2007 National Radio Science Conference, pp. 1-8. [[CrossRef](#)]

4. Xi, J.-M. and Liang, C.-H. (2010), CPW-fed trapezoidal antenna with dual band-notched characteristic for UWB application. *Microwave & Optical Technology Letters*, 52: 898-900. [\[CrossRef\]](#)
5. N. Z. A. Naharuddin and N. H. Noordin, "UWB trapezoidal antenna with a band-notch characteristic," 2015 International Workshop on Electromagnetics: Applications and Student Innovation Competition (iWEM), 2015, pp. 1-2. [\[CrossRef\]](#)
6. Siakavara K (2011), "Methods to Design Microstrip Antennas for Modern Applications", *Intech Open Journal Microstrip Antennas*, pp 173-236. [\[CrossRef\]](#)
7. Shome, Partha & Khan, Taimoor & Laskar, Rabul. (2019), A state-of-art review on band-notch characteristics in UWB antennas. *International Journal of RF and Microwave Computer-Aided Engineering*. [\[CrossRef\]](#)
8. Liu, Hsien-Wen & Ku, Chia-Hao & Yang, Chang-Fa. (2010). Novel CPW-fed planar monopole antenna for WLAN/WiMAX applications. *IEEE Antennas and Wireless Propagation Letters*, Vol 9. pp 240 - 243. [\[CrossRef\]](#)
9. Ben Trad, Imen & Rmili, Hatem & Floch, Jean & ZANGAR, Habib. (2011). Design of Planar Mono-Band rejected UWB CPW-Fed Antennas for Wireless Communications. [\[CrossRef\]](#)
10. Hussain, Sajjad & Zafar, Mariam & Saleem, Shahzada & Tariq, Muhammad Usman. (2015). Microstrip antenna for UWB with WLAN band rejection. pp 95-98. [\[CrossRef\]](#)
11. Naghar, Azzeddin & Alejos, Ana & Aghzout, Otman & Essaaidi, Mohamed. (2015). Compact microstrip omnidirectional ultrawideband antenna with dual broad band nested U-shaped slots and flat frequency response. *Microwave and Optical Technology Letters*. Vol 57, pp 2854-2856. [\[CrossRef\]](#)
12. Singh, C., Kumawat, G. (2020) A Compact Rectangular Ultra-Wideband Microstrip Patch Antenna with Double Band Notch Feature at Wi-Max and WLAN. *Wireless Pers Commun* 114, 2063–2077 [\[CrossRef\]](#)
13. Q. -X. Chu and Y. -Y. Yang, "A Compact CPW-fed Planar Ultra-wideband Antenna with a Frequency Notch Characteristic," *Asia-Pacific Microwave Conference*, (2007) pp. 1-4. [\[CrossRef\]](#)
14. Ye, L.-H & Chu, Q.-X. (2010). 3.5/5.5 GHz dual band-notch ultra-wideband slot antenna with compact size. *Electronics Letters*. Vol 46. pp 325 - 327. [\[CrossRef\]](#)
15. Yu Fei, Wang Chunhua (2009). A CPW-Fed Novel Planar Ultra-Wideband Antenna with a Band-Notch Characteristic. *Radioengineering Magazine*. Vol. 18, No. 4, pp 551-555. [\[CrossRef\]](#)
16. Yadav, Ajay & sharma, mamta & Yadav, Rajendra. (2019). A CPW-fed CSRR and inverted U slot loaded triple band notched UWB antenna. *Progress In Electromagnetics Research C*. 89, pp 221-231. [\[CrossRef\]](#)
17. Tampouratzis, M.G.; Katsos, E.; Vouyioukas, D.; Stratakis, D.; Yioultsis, T. "Design of Planar CPW-Fed UWB Trapezoidal Monopole Antennas with Band Rejection Characteristics" *IEEE 26th International Conference on Circuits, Systems, Communications and Computers (CSCC 2022)*, Platania, Chania, Crete Island, Greece, July 19-22, 2022. [\[CrossRef\]](#)
18. Tampouratzis M.G., Vouyioukas, D., Stratakis D., Yioultsis, T. (2020) Use Ultra-Wideband Discone Rectenna for Broadband RF Energy Harvesting Applications. *Mdpi Technologies* 8, 21. [\[CrossRef\]](#)
19. Antenna Magus - The Leading Antenna Design Tool.
20. Pozar, David M. *Microwave Engineering*. Hoboken, NJ Wiley, 2012.
21. Lvxia, S. & Huiping, G. & Xueguan, L. & Ying, W. (2012) Ultra-wideband planar monopole antenna with parametric study. *Microwaves, Antennas & Propagation*, IET. 6, pp 172-177. [\[CrossRef\]](#)
22. Federal Communications Commission (FCC) <https://www.fcc.gov>
23. Seo, Yeon Seok & Jung, J.W. & Lee, Hae June & Lim, Y.S. (2012). Design of trapezoid monopole antenna with band-notched performance for UWB. *Electronics Letters*. 48: 673-674. [\[CrossRef\]](#)
24. Kumar S, Lee GH, Kim DH, Haunan NS, Choi HC, Kim KW. (2020) Compact Planar Super-Wideband Monopole Antenna with Four Notched Bands. *Electronics*. [\[CrossRef\]](#)
25. Hasan, Md Nazmul & Shah, S.W. & Babar, M.I. & Sabir, Zeeshan. (2012). Design and simulation-based studies of a dual band u-slot patch antenna for WLAN application. 997-1001. [\[CrossRef\]](#)
26. Jin, Yunnan & Tak, Jinpil & Choi, Jaehoon. (2016). Quadruple Band-Notched Trapezoid UWB Antenna with Reduced Gains in Notch Bands. *Journal of Electromagnetic Engineering & Science* 16. 35-43. [\[CrossRef\]](#)
27. Ansari J. A., Mishra Anurag, Yadav N. P., Singh P., Vishvakarma B. R. (2011). Compact Triple U-Shaped Slot Loaded Circular Disk Patch Antenna for Bluetooth and WLAN Application. *Int. Journal of Microwave & Optical Technology (IJMOT)*, Vol 6, No. 2, pp. 91-99. [\[CrossRef\]](#)



Article

Isotropic IoT-Based Magnetic Flux Density Meter Implementation for ELF Field Measurements [†]

Manolis G. Tampouratzis ^{1,*} , George A. Adamidis ², Demosthenes Vouyioukas ¹ , Traianos Yioultsis ³ and Dimitrios Stratakis ⁴

¹ Department of Information and Communication Systems Engineering, University of the Aegean, 83200 Karlovassi, Greece; dvouyiou@aegean.gr

² Department of Electronics Engineering, Hellenic Mediterranean University (HMU), 73133 Chania, Greece; sv7fid@yahoo.gr

³ Department of Electrical and Computer Engineering (ECE), Aristotle University of Thessaloniki (AUTH), 54124 Thessaloniki, Greece; traianos@auth.gr

⁴ Department of Electrical and Computer Engineering (ECE), Hellenic Mediterranean University (HMU), 71004 Heraklion, Greece; dstrat@hmu.gr

* Correspondence: tampouratzis@aegean.gr

[†] This article is an extended version of our paper published in the 3rd International Conference on Control, Artificial Intelligence, Robotics and Optimization (ICCAIRO), Ierapetra, Crete Island, Greece, 11–13 April 2023.

Abstract: This article presents the basic principles for an Extremely Low Frequency (ELF) IoT-based isotropic meter implementation, which can measure magnetic flux density from 100 nT up to 10 μ T. The identical sensor probes are used for isotropic field measurements in the X, Y, and Z planes. The prototype has a flat response across the frequency range from 40 Hz to 10 kHz, detecting and measuring several magnetic field sources. The proposed low-cost meter can measure fields from the power supply network and its harmonic frequencies in the operating frequency band. The proposed magnetic flux density meter circuit is simple to implement and the measured field can be displayed on any mobile device with Wi-Fi connectivity. An Arduino board with the embedded Wi-Fi Nina module is responsible for data transferring from the sensor to the cloud as a complete IoT solution, supported by the Blynk application via Android and iOS operating systems or web interface. In addition, an ELF energy harvesting (EH) circuit was also proposed in our study for the utilization of the alternating magnetic fields (50 Hz) derived from the operation of several consumer devices such as transformers, power supplies, hair dryers, etc. using low-consumption applications. Experimental measurements showed that the (DC) harvesting voltage can reach up to 4.2 volts from the magnetic field of 33 μ T, caused by the operation of an electric hair dryer and can fully charge the 100 μ F storage capacitor (C_s) of the proposed EH system in about 3 min.

Keywords: Internet of Things (IoT); Extreme Low Frequencies (ELF); magnetic field measurements; magnetic flux density; magnetic field energy harvesting; detection coil; RMS detector; reasonable-gain integrator



Citation: Tampouratzis, M.G.; Adamidis, G.A.; Vouyioukas, D.; Yioultsis, T.; Stratakis, D. Isotropic IoT-Based Magnetic Flux Density Meter Implementation for ELF Field Measurements. *Appl. Sci.* **2023**, *13*, 12730. <https://doi.org/10.3390/app132312730>

Academic Editor: Alessandro Lo Schiavo

Received: 25 September 2023

Revised: 8 November 2023

Accepted: 10 November 2023

Published: 27 November 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Multiple studies have demonstrated that long-term exposure to significant extremely low-frequency (ELF) magnetic fields (1 Hz–100 kHz) can result in severe health issues. A considerable rise in blood triglycerides, a putative stress indicator in humans, the disorientation of chicks, and a reduced response time in monkeys are some unsettling effects of exposure to ELF fields [1]. Although some other research shows no link, epidemiological studies show a positive association between residential/domestic and occupational exposure to ELF fields and several forms of cancer, such as childhood leukaemia [2].

Magnetic fields (MFs) depend on the radiation's type, field, frequency, and wavelength. Depending on the current feed, either static magnetic fields (SMF) with direct current (DC) or alternating magnetic fields (AMF) with alternative current (AC) are created. In contrast to SMFs, the polarity of an AMF remains constant despite periodic changes in the direction of the current flow. Several devices create powerful low-frequency magnetic fields such as transformers, electric motors, electric heaters, hair dryers, power supplies, and cathode ray tubes (CRTs), as well as the production, distribution, and consumption of 50 or 60 Hz electric energy. In medicine, magnetic resonance imaging (MRI) uses strong SMF, and the patients are often subjected to between 1.5 and 3 T. The public has occasionally expressed great concern about the use of some of these devices as sources of high magnetic fields.

Depending on the exposure source and the distance from that source, magnetic field strengths might vary significantly. Depending on how well the opposing magnetic flux lines cancel each other out or how well the current-carrying lines are balanced, the rate at which the field intensity decreases with distance might differ from one source to another. At an increasing distance, fields from coils, magnets, or transformers degrade quickly by a factor of $1/r^3$. In power lines, partial field-cancelling causes the drop-off to be $1/r^2$ when currents flow in opposite directions. When there is an imbalanced current, the field intensity decreases more slowly than $1/r$, as shown in Figure 1 [3].

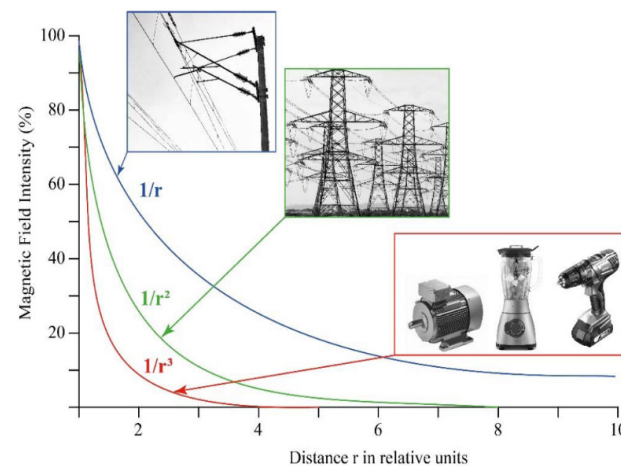


Figure 1. The magnetic field intensity decreases with the growing distance from the field with fast ($1/r^3$, $1/r^2$) or slow ($1/r$) drop-off [1].

The methodology of Extremely Low Frequency (ELF) measurements as defined by the International Telecommunication Union (ITU) is quite complex. Contrary to the measurement of high-frequency fields, extremely low-frequency fields present difficulties in their measurement, since at these frequencies the corresponding wavelengths exceed 100 m, thereby making it difficult to accurately measure in the near field [4]. It should be noted that the quantities of electric field strength, magnetic field strength, and equivalent power density are used to determine public exposure using suitable measuring devices. Regarding exposure to magnetic fields for public safety, the measured values should satisfy the mathematical Equation (1):

$$\sum_{1\text{Hz}}^{150\text{KHz}} \frac{H_i}{H_{Li}} \leq 1 \quad (1)$$

where H_i is the measurement of the magnetic field strength and H_{Li} is the reference level for exposure at frequency i , as reported in Table 1, noting that the electromagnetic radiation limits according to Greek legislation correspond to 70% of the values that are described. The Weighted Peak Method (WPM) [5] was established by the ICNIRP 2010 guidelines for non-sinusoidal multiple-frequency fields. This method, incorporated into Directive 2013/35/EU [6], is required for the assessment of electrostimulation effects (non-thermal) at LF/ELF frequencies and is mandatory in all industrial applications for the safety of workers.

The complex waveforms are weighted using a filter function that takes into account the waveforms' phase, as described by the following equation [7]:

$$\left| \sum_i \frac{A_i}{E_{Li}} \cos(2\pi f_i t + \theta_i + \varphi_i) \right| \leq 1 \quad (2)$$

where t is the exposure time and A_i and E_{Li} are the harmonic component amplitude and the exposure limit at i th harmonic frequency f_i , respectively. The phase and filter angles of the field at the harmonic frequencies are also described by θ_i , φ_i . In addition, knowing that isotropic measurements should be along the X , Y , and Z axes, the total measured magnetic field H_i is described by Equation (3):

$$H_i = \sqrt{H_{x,i}^2 + H_{y,i}^2 + H_{z,i}^2} \quad (3)$$

Table 1. The Electric and Magnetic field reference levels in the European Union for general public exposure focused on Extreme Low Frequencies (ELF) [1,4].

Freq. Band	Electric Field Strength (V/m)	Magnetic Field Strength (A/m)	Magnetic Field Induction (μ T)
0–1 Hz	-	3.2×10^4	4×10^4
1–8 Hz	10,000	$3.2 \times 10^4/f^2$	$4 \times 10^4/f^2$
8–25 Hz	10,000	$4000/f$	$5000/f$
0.025–0.8 kHz	$250/f$	$4/f$	$5/f$
0.8–3 kHz	$250/f$	5	6.25
3–150 kHz	87	5	6.25

Where f , is the frequency in Hz or kHz, depending on how it is defined in the table cell that is in the same row and column of the frequency band. No E -field value is defined for frequencies less than 1 Hz, which are essentially static electric fields.

The continuing interest in making reliable measurements concerning public exposure to extremely low frequency (ELF) magnetic fields has led researchers to implement measurement devices for several years. Strong magnetic field sources can be detected using an ELF magnetic field meter by taking the necessary precautions [3,8]. The authors in [9] introduced a broadband magnetic field meter at the National Bureau of Standards (NBS), in 1985. The proposed meter has an isotropic probe unit consisting of three mutually orthogonal loops, each 10 cm in diameter, for magnetic field measurements up to 30 A/m. The novelty of this implementation was based on several improvements over available instruments for that time, such as the dynamic range of 44 dB, the flat frequency response (about ± 1.0 dB), the isotropic response (about ± 0.3 dB), and the overload capability, using only one probe head. The work in [10] introduced a sensor for isotropic magnetic and electric field measurements at frequencies less than 100 kHz, determining the electromagnetic interferences specialized in the audio frequency band. Three orthogonally oriented coils are used as an EMF sensor by the authors in [11], introducing a measurement method that enables a precise analysis of the field distribution. The study suggests a research technique that involves evaluating the strength of the electromagnetic field produced by the emitting coil in a Wireless Power Transfer (WPT) system in terms of both magnitude and direction.

Nowadays, the technology of Electric and Magnetic Fields (EMF) meters has advanced considerably, offering engineers measurements with less uncertainty and the feature of remote equipment real-time monitoring. A professional solution for continuous monitoring of the electric and magnetic fields is provided by the Narda PMM EHP-50C probe analyzer [12,13] which can begin its acquisition by storing the data over 24 h in the operating frequency range of 5 Hz to 100 kHz. The analyzer features a variety of operating modes, including stand-alone mode without an external apparatus connection and cooperation with a Pocket-PC or Narda PMM 8053A portable display unit via fiber optic communication. In [14], another analyzer for measuring magnetic and electric fields in the workplace

and public places is presented. The Narda EFA-300 provides field analysis using an FFT computation in combination with built-in, isotropic, magnetic field probes, as shown in Figure 2. The measurement process is intended to be substantially simplified by this new generation of equipment. The Narda EFA-300 incorporates the novel STD (Shaped Time Domain) mode in addition to detecting the RMS and peak values using the conventional filter technique, providing simple but reliable measurement even in complex environments. Regarding the magnetic field measurements, the Narda EFA-300 analyzer can detect fields from 1 nT to 31.6 mT over the operating frequency range of 5 Hz to 32 kHz.

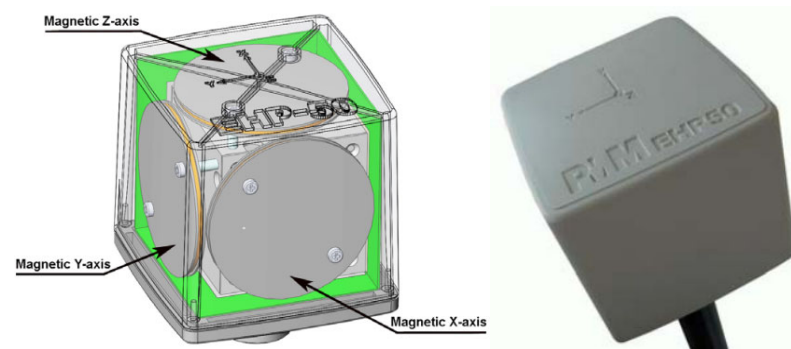


Figure 2. The internal structure of Narda PMM EHP-50C probe-analyzer for measurements of magnetic and electric fields over the frequency range 5 Hz to 100 kHz. The identical circular sensor probes are devoted to isotropic field measurements in the X, Y, and Z planes [13,14].

The authors in [15] introduced a broadband monitoring system for electromagnetic radiation exposure assessment, focused on RF frequencies (from radio and TV broadcastings, mobile telephony systems, Wi-Fi, and TETRA communications) in 2006. The proposed system called “SMS-K”, has been implemented for recording the *E*-field on a 24 h basis and sending the data to a central database via a GSM connection, as an early-stage EMF IoT platform. The real-time measurements are available via a web interface for citizens’ information within the framework of the “FASMA” project [16], supported by Wind Hellas Telecommunications SA. Thereinafter, other EMF monitoring projects called “HERMES” (2002) [17], “Pedion 24” (2006) [18], and “National Observatory of Electromagnetic Fields” (2015) [19] were developed for the continuous remote monitoring of electromagnetic radiation via a distributed network of fixed meters in Greece. In these projects, the Narda area monitors AMS-8061/G [20], AMB-8059 [21], and AMB-8057-03/G [22] were used only for *E*-field measurements at a wide operating frequency band (100 kHz–7 GHz). The measurement data from each stand-alone station are sent to the central database via the 3G/GPRS network for citizens’ information through the web portal of the project.

Undeniably, the existence of magnetic fields in urban and semi-urban environments could be used as another emergency energy source (under certain conditions) to power low-consumption devices, such as IoT sensors. Numerous locations could be beneficial for sensors where the magnetic flux density may be high enough to power a low-consumption WSN’s node, such as in high voltage substations, near railways, etc. Several published studies have covered the research on the magnetic flux density levels (*B*) under overhead power lines [23]. Researchers have verified that the flux density close to the ground is within legal limits. It stands to reason that different types of pylons will have varying overhead power line physical structures and typical line currents, leading to variable magnetic flux densities.

The authors in [24] propose a novel and efficient harvesting bow-tie coil to scavenge the magnetic field energy under overhead power lines, enabling the self-powering of a large number of sensors. In contrast to the typical way of placing the energy harvester on the power lines, the proposed coil does not need to be fastened to the line and may be put just above the ground, allowing for the powering of sensors with a larger volume.

The work in [25] presents a study of a generator that can continually charge batteries for pulsed communications, using the magnetic field created by high-voltage DC lines. In its implementation, no expensive magnetic material is required; however, several insulating issues, including the Corona phenomenon in transmission lines, should be taken into account for the proposed mounted harvester to be used in practice.

In [26], a free-standing inductive harvester for use in locations with ambient magnetic fields caused by far-off and/or difficult-to-reach conductors is presented. Researchers introduced a self-powered wireless sensor by utilizing ambient 50 Hz magnetic fields in High Voltage (HV) substations. The laboratory experimental results have shown that the proposed magnetic field harvester of the sensor can deliver a useful average power of 300 μ W when placed in a magnetic flux density of 18 μ T (RMS).

Based on numerous experiments using different inductors and combinations of current-carrying conductors, the authors in [27] offer a feasibility analysis of energy harvested from stray electromagnetic energy of household AC power lines. The results are encouraging since it is possible to harvest up to 2 mW of power using simple components for the harvester implementation.

The study in [28] presents two distinct configurations evaluated in situ along a Norwegian railway and in a controlled laboratory setting to support the viability of magnetic field energy harvesting (MF-EH) in electrical railways. The power output of the proposed system can reach up to 40.5 mW at 50 Hz when positioned near an emulated section of a railway carrying 200 A, based on the experimental measurements carried out at the laboratory. In a region with moderate traffic, the prototype system harvests 109 mJ from a single electric train, yielding an estimated daily energy output of 1.14 J.

Another magnetic field energy harvester (MF-EH) application for railways is presented in [29] to power wireless sensors for condition monitoring. In that study, an MFEH system was designed, enhanced, and tested for energy harvesting from the rail tracks' traction return currents. The magnetic core was created using two flux collectors to partially enclose the rail track based on the dispersion of the magnetic field around the rail track. Measurements show that the MFEH's power output was decreased by reducing eddy current loss by positioning it farther from the rail track. The experiment's power output decreased from 5.05 to 1.6 W when the MFEH was relocated from a distance of 48 mm to 190 mm, where the eddy current loss was insignificant.

In this work, the implementation of an isotropic Extremely Low Frequency (ELF) IoT-based meter is presented. The proposed low-cost meter can measure the magnetic flux density from 100 nT with three identical sensor probes for isotropic field measurements in the X, Y, and Z planes, enhancing the work in [30]. The proposed device has an almost flat response across the frequency range from 40 to 10 kHz, detecting and measuring several magnetic field sources, including the public power supply network and its harmonic frequencies. In our approach, an Arduino UNO Wi-Fi Rev.2 board is used for data transferring from the sensor to the cloud as a complete IoT solution, supported by the Blynk application via Android and iOS operating systems or web interface. Furthermore, an ELF energy harvesting (EH) circuit was also proposed in our study for the utilization of the alternating magnetic fields (50 Hz) derived from the operation of several consumer devices such as transformers, power supplies, hair dryers, etc. using low-consumption applications.

The rest of this article is organized as follows: the proposed magnetic flux density meter operating principles are presented and analyzed in Section 2. Section 3 gives the full description of the electronic circuit (analogue section) of the proposed EMF meter. Section 4 is devoted to the description of the isotropic ELF sensor implementation. A demonstration of real-time ELF field monitoring as a proposed IoT solution via the Blynk application is presented in Section 5. Section 6 is devoted to the description of the magnetic field utilization derived from the operation of common-use electrical devices, such as a hair dryer at the laboratory using a proposed MFEH harvester, and finally, Section 7 includes the conclusions and a discussion on future work.

2. Magnetic Flux Density Meter Operating Principles

The induced electromotive force in any closed circuit is equal to the negative time rate of change in the magnetic flux contained in the circuit, according to Faraday's Law of Electromagnetic Induction. Consequently, when magnetic flux flows through a coil, a voltage is generated across it, the magnitude of which is dependent on the field's intensity rate and the enclosed surface area. In mathematical terms,

$$E = -\frac{d\Phi}{dt} = -A N \frac{dB}{dt} \quad (4)$$

where Φ is the magnetic flux passing through the coil, A is the area enclosed by each turn of the coil, N is the total number of turns of the coil, B is the magnetic flux density of the field (magnetic field), and t is the time. Essentially, the time derivative of the magnetic flux density determines the rate of change in the magnetic flux density (a derivative of the magnetic flux concerning time).

It is considered that in space there is a harmonic (sinusoidal) magnetic field of the following form:

$$B(t) = B_0 \cos(2\pi ft) \quad (5)$$

where $B(t)$ is the instantaneous value of the magnetic flux density (function of time), B_0 is the maximum value of the oscillating field, and f is the frequency of oscillation. From (4) and (5), we conclude that if a coil is placed into the harmonic field, a harmonic voltage $E(t)$ will be induced at its terminals, which will be equal to the following:

$$E(t) = 2\pi f A N B_0 \sin(2\pi ft) \quad (6)$$

We observe that the induced voltage is proportional to the geometric characteristics of the coil (A , N), the frequency f , and the field strength B_0 . The harmonic term $\sin(2\pi ft)$ indicates that voltage is a harmonic function of time and has a phase difference of 90° concerning the field. From (6), we observe that if the induced voltage E can be measured, the B field can be calculated, as long as the exact frequency f is known. In practice, when measuring the magnetic field of an arbitrary (unknown) source, its frequency is undetermined. The unknown frequency problem is resolved by multiplying both sides of Equation (7) by the absolute value of the $G/2\pi f$ term, where G is a constant for any specific frequency f , corresponding to amplifier voltage gain. Then, we will have:

$$\left| \frac{G}{2\pi f} \right| E(t) = G A N B_0 \sin(2\pi ft) \quad (7)$$

By setting:

$$V(t) = |G/2\pi f| E(t)$$

hence,

$$V(t) = G A N B_0 \sin(2\pi ft) = G A N B(t) \quad (8)$$

where $V(t)$ is the instantaneous value of the harmonic voltage induced in the coil as a product by the absolute value of the $G/2\pi f$ term. Referring to RMS terms (Root Mean Squared values) the RMS voltage (V_{rms}) is proportional to the RMS magnetic field density (B_{rms}) and independent of the frequency [31,32]:

$$V_{rms} = G A N B_{rms} \quad (9)$$

Therefore, it is easy to calculate the magnetic flux density (B_{rms}) by measuring the voltage value (V_{rms}) with an analogue electronic device, i.e., a magnetic flux density meter. Figure 3 illustrates the block diagram of the proposed low-cost IoT magnetic flux density meter providing cloud-based services, as a comparative advantage among similar high-cost measurement equipment [13,14]. The proposed magnetic flux density meter's electronic circuit is straightforward to implement, and the components have a low tolerance for mea-

surement error minimization. A detector coil with well-defined geometric characteristics as a field sensor, an amplifier with voltage gain equal to $G/2\pi f$, an RMS detector, and a voltage display are required for a real circuit that makes use of Equation (9).

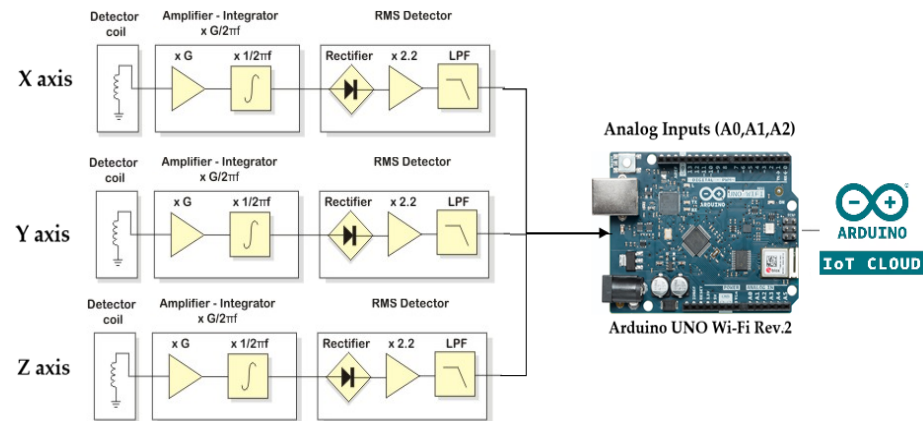


Figure 3. The block diagram of the proposed isotropic IoT-based magnetic flux density meter. An Arduino UNO Wi-Fi Rev.2 board is used to provide 3 analog inputs for measurements in the X, Y, and Z axes and Wi-Fi connectivity, enhancing the previous version of the sensor [30].

In the proposed implementation, the Arduino UNO Wi-Fi Rev.2 board [33] is used instead of common voltmeters at analog outputs of the device, providing network connectivity for data transferring to the Blynk cloud [34], as a complete IoT EMF solution. The measured voltage values at three analogue inputs correspond to the magnetic field strength values in the X, Y, and Z axes, respectively, and can be displayed on any mobile device with Wi-Fi connectivity.

2.1. The Amplifier with $G/2\pi f$ Gain

A circuit with a $1/f$ response is an integrator [35] (a low pass filter with a linear amplitude response and an ideal cut-off frequency of 0 Hz). An operational amplifier and several passive components can be used to create an almost ideal integrator. To achieve high gain value, one high-gain integrator or multiple amplifying stages in series with a reasonable-gain integrator are required. The second approach, in which the amplifier unit is employed before the integrator, is recommended for the proposed circuit. The detector requires high amplification to be sensitive without using any massive coil (since the output voltage for a reasonably sized coil is relatively small, in particular at low frequencies).

2.2. The RMS Detector

A section of the RMS detector is required for the implementation of a magnetic field meter that can measure RMS field values instead of average or peak values. A rectifier is used to extract the DC component and measure the RMS value of the integrators' AC signal output.

The DC component of a rectified signal is shown to be directly proportional to the RMS value of the harmonic input signal. A half-wave rectified voltage V_s is considered during a full cycle ($0-2\pi$ rad):

$$\begin{aligned} V_s(t) &= V_m \sin(\omega t) & \text{for } 0 \leq \omega t < \pi \\ V_s(t) &= 0 & \text{for } \pi \leq \omega t < 2\pi \end{aligned} \quad (10)$$

where V_m is the maximum value of the half-wave rectified voltage. The Fourier series of the previous function is as follows [36]:

$$V_s(t) = \frac{V_m}{\pi} + \frac{V_m}{2} \sin(\omega t) - \frac{2V_m}{3\pi} \cos(2\omega t) - \frac{2V_m}{15\pi} \cos(4\omega t) + \dots \quad (11)$$

and hence,

$$V_s(t) = \frac{V_m}{\pi} + \frac{V_m}{2} \sin(\omega t) + \sum_{N=2}^{\infty} \frac{V_m [1 + (-1)^N]}{\pi(1 - N^2)} \cos(N\omega t) \quad (12)$$

Moreover, we are aware that in half-wave rectified signal:

$$V_{DC} = \frac{1}{T} \int_0^T V_{out}(t) dt = \frac{1}{T} \int_0^{T/2} V_m \sin\left(\frac{2\pi t}{T}\right) dt = \frac{V_m}{\pi} \quad (13)$$

and,

$$V_{rms} = \sqrt{\frac{1}{T} \int_0^T V_{out}^2(t) dt} = \sqrt{\frac{1}{T} \int_0^{T/2} V_m^2 \sin^2\left(\frac{2\pi t}{T}\right) dt} = \frac{V_m}{2} \quad (14)$$

The first term in (11) represents the DC component of the semi-rectified signal, the second term is the 1st harmonic (base frequency), and the remaining terms are higher-order harmonics, respectively. The following is assumed in a harmonic (sinusoidal) signal:

$$V_{rms} = \frac{V_m}{\sqrt{2}}, \quad V_{DC} = \frac{\sqrt{2} V_{rms}}{\pi}, \quad V_{rms} = \frac{\pi V_{DC}}{\sqrt{2}} \quad (15)$$

The RMS value of the input harmonic signal is equal to the $\pi/\sqrt{2}$ of the DC component of the semi-rectified signal. At the rectifier's output (V_{out}), except the DC component, a large number of harmonics should be rejected. A low pass filter can be utilized to reject the harmonic frequencies. To achieve perfect harmonics rejection, the low pass filter's cut-off frequency is required to be as low as possible. Consequently, the RMS detector can be realized consisting of a half-wave rectifier and a low-pass filter.

3. The Electronic Circuit of the Proposed EMF Magnetic Flux Density Meter (Analog Section)

Figure 4 presents the proposed magnetic field meter's basic electronic circuit (analog section).

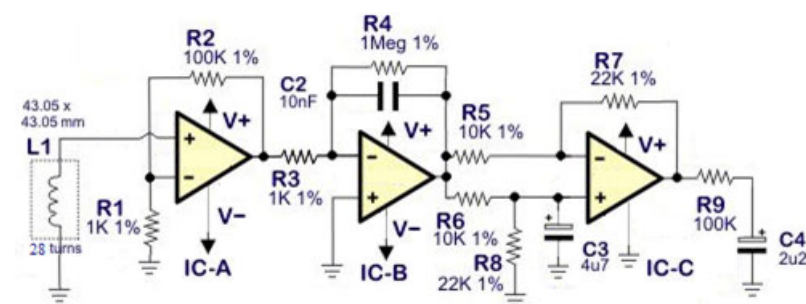


Figure 4. The basic electronic circuit of the proposed magnetic flux density meter. For the implementation of an isotropic meter, 3 identical circuits are also needed for ELF measurements in the X, Y, and Z planes.

The Op-Amp A is used as a typical non-inverting amplifier with G_a gain:

$$G_a = 1 + \frac{R_2}{R_1} \quad (16)$$

The gain G_a is defined by R_1 and R_2 as described in Equation (16); it is equal to 101 and does not depend on frequency. Practically, the gain of the amplifier would be less than 101 for frequencies lower than 40 Hz. The design characteristics of the Op-Amp A

limit the amplifier's responsiveness at higher frequencies (the gain–bandwidth product). Nevertheless, from 40 Hz to 10 kHz, the amplifier response is almost flat, and the gain is approximately equal to the theoretical value with a potential error of less than 1 dB if 1% accuracy resistors are used for R_1 and R_2 . The integrator follows the amplifier, implemented from Op-Amp B, R_4 , R_3 , and C_2 . The response of the integrator is inversely proportional to the frequency due to C_2 . If the integrator is analyzed as a typical inverse amplifier, it is observed that its gain G_b is equal to

$$G_b = -\frac{R_F}{R_3} \quad (17)$$

The R_F value is the impedance resulting from the parallel combination of resistor R_4 and the X_c impedance (reactance) of C_2 . That is,

$$R_F = X_c // R_4 = R_4 X_c / (R_4 + X_c) \quad (18)$$

Knowing that X_c reactance is equal to:

$$X_c = \frac{1}{2\pi f \cdot C_2} \quad (19)$$

By combining Equations (17)–(19), we find that:

$$G_b = \left(-\frac{R_4}{R_3}\right) / (1 + 2\pi f R_4 C_2) \quad (20)$$

It is noticed that the above equation is not exactly in the form of $1/f$, mainly because our integrator is not ideal due to R_4 . Nevertheless, the product $2\pi f R_4 C_2$ is much larger than 1 for frequencies above 40 Hz and the “1” in the denominator can be omitted. Consequently, for frequencies above 40 Hz, the integrator's gain becomes equal to:

$$G_b = \left(-\frac{1}{R_3 C_2}\right) \left(\frac{1}{2\pi f}\right) \quad (21)$$

The total gain of the amplifier and integrator chain would be the product of the G_a and G_b , namely:

$$G_t = G_a \cdot G_b \quad (22)$$

From Equations (16), (21), and (22), we conclude that:

$$G_t = \left(1 + \frac{R_2}{R_1}\right) \left(-\frac{1}{R_3 C_2}\right) \frac{1}{2\pi f} \quad (23)$$

where:

$$G = \left(1 + \frac{R_2}{R_1}\right) \left(-\frac{1}{R_3 C_2}\right) \quad (24)$$

Taking into consideration Equations (24) and (9), we observe that an AC voltage (V_{rms}) is produced at the output of the integrator, which is equal to

$$V_{rms} = \left(1 + \frac{R_2}{R_1}\right) \left(-\frac{1}{R_3 C_2}\right) A N B_{rms} \quad (25)$$

From Equation (25) we notice that the produced voltage is directly proportional to the field and independent of frequency, as shown in Figure 5. Based on the actual value calculation of the G constant, we observe that

$$G = \left(1 + \frac{R_2}{R_1}\right) \left(-\frac{1}{R_3 C_2}\right) = 101 \times 10^5 \quad (26)$$

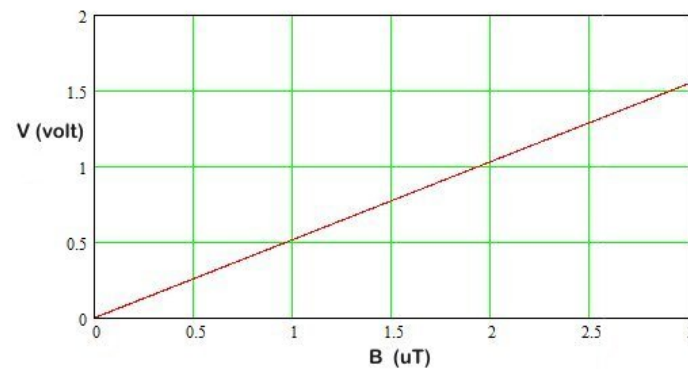


Figure 5. The output voltage of the proposed RMS detector is a function of the magnetic flux density.

The rectifier circuit is subsequent to the integrator, implemented from the Op-Amp C. Since there is no diode anywhere, the rectification circuit is uncommon. The rectification is carried out because the negative half-period of the signal is simply cut off. The Op-Amp C along with the resistors R_5 , R_6 , R_7 , and R_8 is a typical differential amplifier circuit (subtraction). The voltage applied to the left end of R_5 is subtracted from the voltage applied to the left end of R_6 . The output of the subtractor will always have a voltage equal to zero since the left edges of R_5 and R_6 are short-circuited, only in the case of DC. Contrariwise, for the AC signal, the capacitor C_3 acts as a short circuit and grounds the non-inverting input of Op-Amp C. This method converts the subtractor into an inverting AC amplifier with an amplification of $R_7/R_5 = 2.2$.

The previous analysis demonstrates that Op-Amp C eliminates the DC component of the signal and amplifies the remaining AC signal by a factor of 2.2. Furthermore, Op-Amp C performs a half-rectification of the signal at 0 V reference level without negative supply voltage.

Consequently, it can only amplify the positive half-period of the signal, and during the negative half-period, its output is zero (i.e., half-phase rectification occurs). Op-Amp C output produces a semi-rectified signal containing a DC component and some harmonics (according to the Fourier series analysis mentioned above). The harmonics are filtered out from a simple low pass filter formed by R_9 and C_4 . The cut-off frequency of this specific filter is equal to $1/2\pi R_9 C_4 = 4.5$ Hz, which is a very low one and the filter passes only the DC component. Normally, the DC component of a half-rectified signal is equal to $\sqrt{2}/\pi$ of the RMS value of the input signal of the rectifier. The term $\sqrt{2}/\pi$ is equal to about 1/2.2.

However, since we use amplification equal to 2.2 in the rectifier, we make the half-rectified signal have a DC component equal to the exact RMS value of the input signal (by cancelling out the 1/2.2 factor). The circuit has an analog output providing voltage equal to 0.1 mV/nT at the Analog to Digital (ADC) port of the Arduino WeMos D1 board. For instance, for a 2 μ T field, there will be a voltage of 200 mV at the analogue output of the ELF meter. This output is provided on C_4 terminals. C_4 , along with R_9 , forms a low-pass filter that extracts the DC component from the output of the rectifier as described above.

4. The Proposed ELF Isotropic Sensor Implementation

Winding a coil with a certain number of turns and specific dimensions may constitute the magnetic field probe of the ELF meter. Suppose that the V_{rms} voltage needs to be 1.2 V when the coil is placed inside a 2.3 μ T (RMS) magnetic field. According to (25), the following equation should be satisfied:

$$A N = 0.05166 \text{ m}^2 \quad (27)$$

In our initial prototype implementation [30], by choosing a coil with 100 turns, each turn should include an area of $516.6 \times 10^{-6} \text{ m}^2$. The desired area for a rectangular

cross-section coil can be achieved if each turn is $43.05 \text{ mm} \times 12 \text{ mm}$. Thus, the meter coil in the initial design consisted of 100 turns of $43.05 \text{ mm} \times 12 \text{ mm}$ rectangular cross-sections.

In this study, the sensor of the proposed meter consists of three identical square probes in vertical alignment, providing isotropic H -field measurements from the X, Y, and Z planes, respectively, as shown in Figure 6. Each probe should also satisfy Equations (25) and (27) considering that the initial dimensions should be appropriately changed to achieve the cubic structure of the proposed isotropic sensor. The coil of each axis probe consists of 28 turns of $43.05 \text{ mm} \times 43.05 \text{ mm}$ square cross-sections to feed the identical electronic circuits of the meter (Figure 6b), to enhance the work in [30].

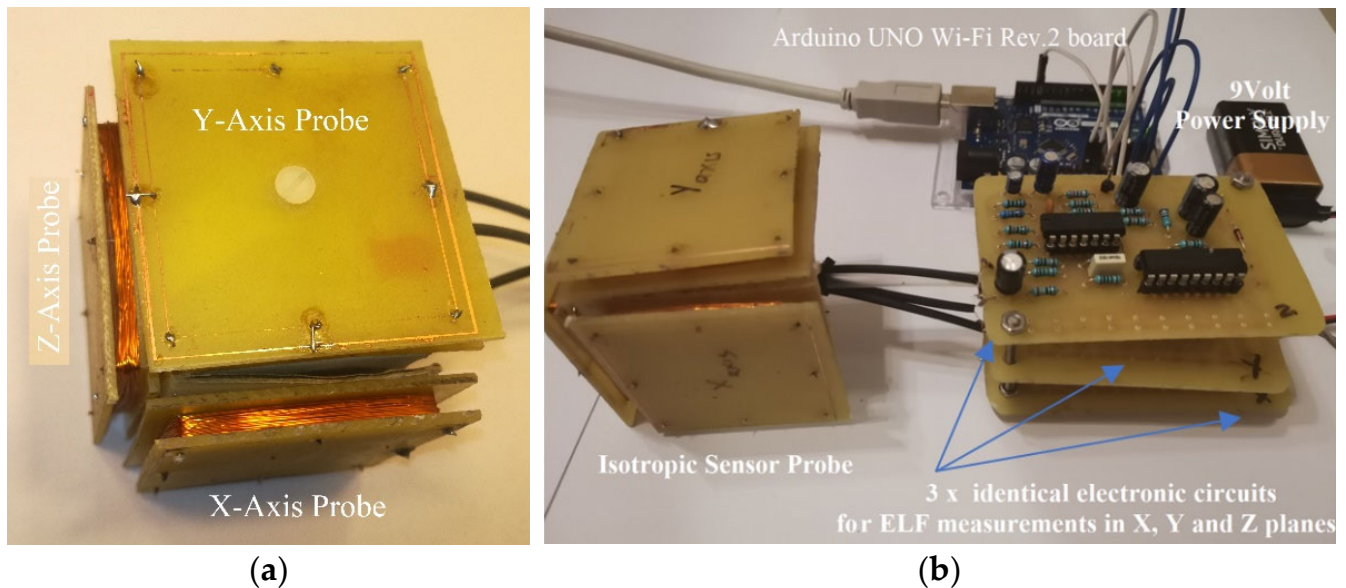


Figure 6. (a) The sensor implementation of the proposed ELF meter consists of three identical square probes in vertical alignment, providing isotropic H -field measurements from the X, Y, and Z planes. (b) The main parts of the proposed magnetic field meter are the isotropic probes, the Arduino board, and the identical electronic circuits.

The measured incident magnetic field of the proposed sensor with three identical square coils is given by the following equation [14]:

$$|H_{inc}| = \sqrt{k_x V_x^2 + k_y V_y^2 + k_z V_z^2} \quad (28)$$

where V_x , V_y , and V_z are the voltages at the outputs of the probe coils of the meter, and k_x , k_y , and k_z are the respective coefficients that are derived from calibrating the device against other available laboratory-calibrated equipment, as the Narda PMM EHP-50C.

For the system's frequency response validation, a TTI TG230 function generator was used to feed a pair of Helmholtz coils to provide a homogeneous magnetic field at the laboratory. Keeping constant the generator's signal amplitude (and at the same time the intensity of the emitted magnetic field at about $2 \mu\text{T}$), the operating frequency of the generator was changing in the ELF band (1 Hz–100 kHz) to achieve the frequency response curve of the proposed meter, as shown in Figure 7a. Experimental measurements show an almost flat response over the frequency range from 40 Hz to 10 kHz, as shown in Figure 7b, respectively. Table 2 shows the comparison of the proposed meter with similar high-precision and ultra-high-cost ELF measurement equipment solutions.

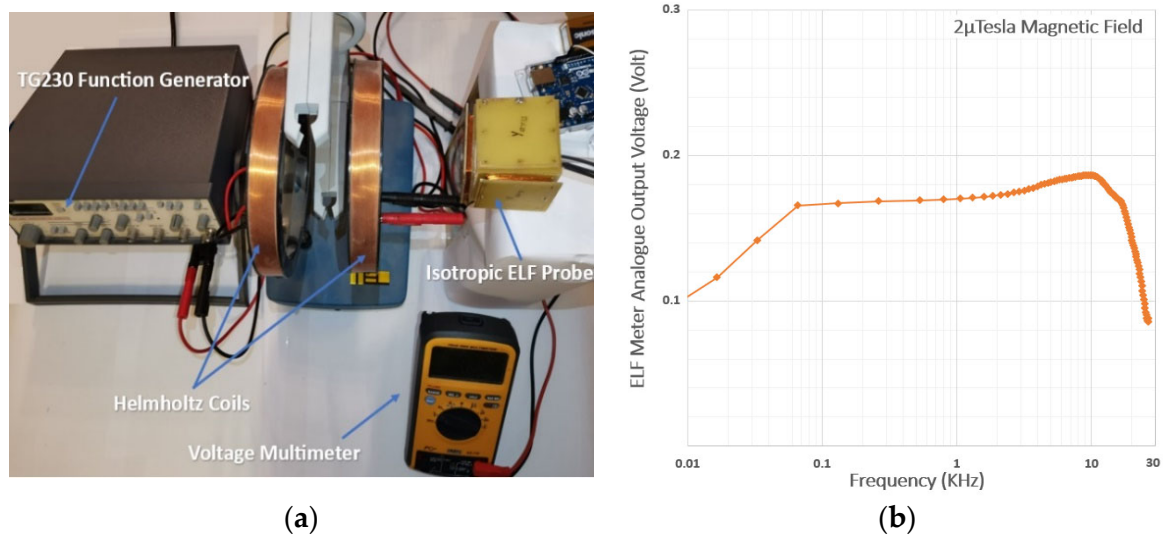


Figure 7. (a) The frequency response validation via Helmholtz coils utilization feeding by a signal generator to provide a homogeneous magnetic field in the ELF band. (b) The frequency response curve of the meter.

5. IoT Application with Arduino UNO Wi-Fi Rev.2 board for Real-Time ELF Field Monitoring

The value of the measured magnetic field can be displayed in real-time on any mobile device with Wi-Fi connectivity via the Blynk application [34] supported by Android and iOS platforms. An Arduino UNO Wi-Fi Rev.2 board with the embedded Wi-Fi Nina [33] module is used to provide three analogue inputs (ADC's) for measurements in the X, Y, and Z axis, respectively to transfer data from the meter to the cloud as a complete EMF IoT solution [37], as shown in Figure 8. The Arduino Uno WiFi uses an 8-bit microprocessor and an onboard inertial measurement unit (IMU). Its Analog to Digital converter (ADC) has a 10-bit resolution, mapping input voltages between 0 and 5 V into integer values between 0 and 1023. This results in readings of 4.9 mV per unit (5 Volts/1024) on the Arduino UNO board.

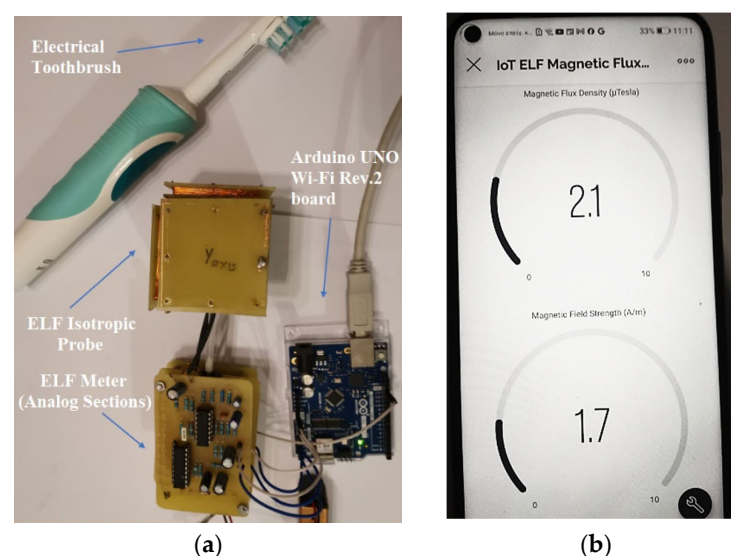


Figure 8. (a) Measuring the magnetic field exposure of an electrical toothbrush by the proposed IoT-based meter. (b) The isotropic ELF field strength values (in A/m and μ Tesla) are displayed on the Blynk application supported by the Android platform in a mobile phone with Wi-Fi connectivity, as a complete IoT solution.

The Blynk user interface can be displayed on the mobile terminal or the web portal and both the magnetic field strength H (A/m) and the corresponding flux density B (μ Tesla) values at the same time, using the following transformation formula:

$$B(\text{Tesla}) = \mu_r \mu_0 H(\text{A/m}) \quad (29)$$

where μ_r is the relative and μ_0 is the free space magnetic permeability. Magnetic field levels up to 300 nT are considered within safe limits in most countries of the world. Several studies have shown that the field is regarded as potentially harmful from 400 nT to 1 μ T, and dangerous from 1 μ T and above [2,23]. Furthermore, the percentage magnetic field contribution (%) of each probe is available to the user to identify the plane direction (X, Y, or Z) of the incident magnetic field.

Table 2. The comparison of the proposed meter with similar ELF measurement solutions.

Ref.	Freq. Response	Meas. Level	Connectivity	Type of Meas.
PMM EHP-50C [13]	5 Hz–100 kHz	1 nT–10 mT	Opt./USB	Magnetic/Electric Field
Narda EHP-50F [38]	1 Hz–400 kHz	0.3 nT–10 mT	Opt./USB	Magnetic/Electric Field
Narda EFA-300 [14]	5 Hz–32 kHz	1 nT–31.6 mT	Opt./Serial	Magnetic/Electric Field
Study in [9]	300 kHz–100 MHz	125 nT–20 mT	Not Mentioned	Magnetic Field
Study in [10]	<100 kHz	Not Mentioned	Not Mentioned	Magnetic/Electric Field
TM192D [39]	30 Hz–20 kHz	up to 200 μ T	USB	Magnetic Field
This work	40 Hz–10 kHz	100 n–10 μ T	WiFi, IoT (Blynk)	Magnetic Field

6. Magnetic Field Energy Harvesting (MF-EH) from the Operation of Commercial-Use Electrical Devices

Several electric devices such as transformers, power supplies electric motors, hair dryers, etc., create powerful low-frequency magnetic fields capable of powering low-consumption applications (such as WSN sensors). In this section of our study, a Magnetic Field Energy Harvesting (MF-EH) circuit is also proposed for 50 Hz magnetic field utilization derived from these common-use electric devices in short distances. The proposed ELF energy harvester is based on an LC tuning circuit, with the same self-resonance frequency (f_{SRF}) as the operation of the public electricity distribution network (50 Hz). The correlation between the resonance frequency (f_{SRF}) of the circuit and the values of the tuning capacitor (C_{tun}) and the inductor coil (L_{tun}), respectively, is given by the Thomson Equations (30) and (31):

$$C_{tun} = \frac{1}{4\pi^2 f_{SRF}^2 L_{tun}} \quad (30)$$

and therefore

$$L_{tun} = \frac{1}{4\pi^2 f_{SRF}^2 C_{tun}} \quad (31)$$

The quality factor (Q) of the circuit is about 6.7, as calculated by Equation (32), as a series tuning circuit, where the resistance value of the coil (R_{coil}) is about 160 Ohms. To achieve resonance at extremely low frequencies (ELF), a relatively high value of either the capacitance or the coil inductance is required. The higher value of the inductance makes the proposed circuit more sensitive for energy harvesting from alternating magnetic fields of 50 Hz.

$$Q = \frac{2\pi f_{SRF} L_{tun}}{R_{coil}} = \frac{1}{2\pi f_{SRF} R_{coil} C_{tun}} = \frac{1}{R_{coil}} \sqrt{\frac{L_{tun}}{C_{tun}}} \quad (32)$$

For our implementation, a value of 3.4H has been chosen for the inductance achieved by hundreds of turns of 0.3 mm insulated copper wire, combined with the addition of an iron core in the resonant coil, as shown in Figure 9a. Thus, the capacitor value (C_{tun}) of the tuning circuit is required to be about 2.9 μ F to achieve oscillation at the resonance frequency of 50 Hz. The parametric study of the components was carried out at the laboratory,

recording the genesis of the descending oscillation using a digital oscilloscope until the desired resonance frequency of 50 Hz (f_{SR}) was reached, as shown in Figure 9c.

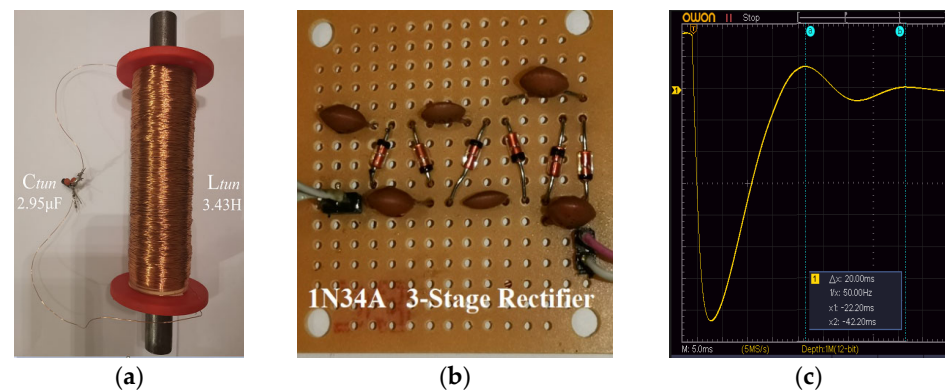


Figure 9. (a) The coil of the LC tuning circuit of the proposed ELF harvester is made by hundreds of turns of 0.3 mm insulated copper wire to achieve 50 Hz resonance frequency. (b) 3-Stage Cockcroft-Walton rectifier. (c) The genesis of the descending oscillation using a digital oscilloscope at the laboratory for the resonance frequency fine-tuning at 50 Hz.

The proposed circuit was tested for alternating magnetic field energy harvesting from electric devices such as transformers, power supplies, etc. in the laboratory. The output of the tuned LC circuit indicates the rectifier of the proposed system. A 3-stage germanium diode-based (1N34A) Cockcroft-Walton rectifier [40] with 100 nF blocking capacitors was used for DC conversion, as shown in Figure 9b. In the prototype, the ability to monitor the output voltage of each rectifier stage is also provided to obtain additional experimental measurements and select the most efficient number of stages at test points 1 to 3, respectively. As already mentioned, the magnetic field intensity decreases with the growing distance from the fields caused by coils, magnets, or transformers by a factor of $1/r^3$, resulting in harvesting voltage drop, respectively. For this limitation compensation, the Texas Instruments BQ22504 DC-DC boost converter [41] could be used as an optional stage of the system for the necessary voltage raising providing power to low-consumption devices, as shown in the block diagram in Figure 10. The BQ22504 is a high-efficiency ultra-low-power boost converter, designed for energy harvesting applications. This device was created with efficiency in acquiring and managing microwatts (μ W) to milliwatts (mW) of power, produced by several DC harvesting sources. It is feasible to start with a V_{IN} as low as 600 mV and continue energy harvesting until the V_{IN} is higher or equal to 130 mV. A storage capacitor (C_s) of 100 μ F is placed to store the harvested energy from magnetic field sources as a capacitor-based EH system [42,43], feeding the BQ22504 boost converter for powering low-consumption applications.

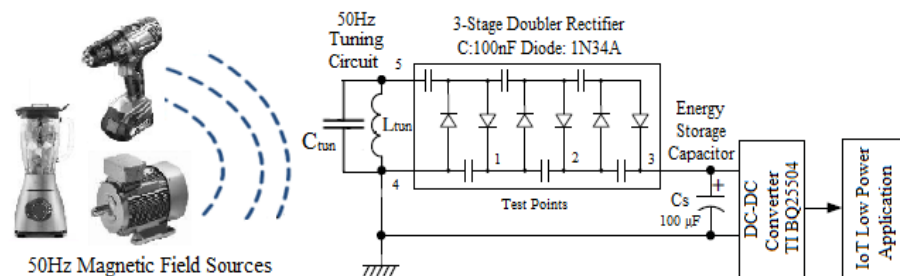


Figure 10. The electronic diagram of the proposed ELF energy harvesting system and some of the magnetic field sources. The test points 1, 2 and 3 corresponds to the individual stages of the rectifier.

7. MF-EH Experimental Results

The experimental measurements showed that at a relatively close distance from the tested magnetic source (hair dryer), the (DC) harvesting voltage can reach up to 4.2 volts, as shown in Figure 11b. The storage capacitor (C_s) of the system can be fully charged in 3 min with a $33 \mu\text{T}$ magnetic field caused by the operation of an electric hair dryer, as depicted in Figures 12 and 11a, respectively. The storage capacitor's (C_s) charging curves demonstrate that the maximum charging voltage (V_{max}) is proportional to the ambient magnetic field strength, as shown in Figure 12. The dynamic behaviour of the rectifier diodes depends to a large extent on the levels of the received signal, consequently affecting the equivalent resistance of the rectifier circuit ($R_{thevenin}$), with the change in the time constant charging (t_{charge}) as a final result. The experimental measurements were also extended to the utilization of the alternating magnetic field near medium voltage substations of the electrical public distribution network. Firstly, magnetic field strength measurements were performed around the perimeter of the metal cabin where the transmission lines of the distribution network are driven, with the Narda EHP-50C PMM field meter, detecting magnetic field values of up to $60 \mu\text{T}$ (at peak time within an urban environment). The experimental setup developed an (open circuit) voltage that reached 8 Volts at points where the magnetic field density was maximum, as shown in Figure 13a,b, respectively. It should be noted that the harvesting voltage is a function of the spatial placement of the tuning circuit of the device, as it is not possible to harvest energy isotopically using the original design of the prototype (axes X, Y, Z).

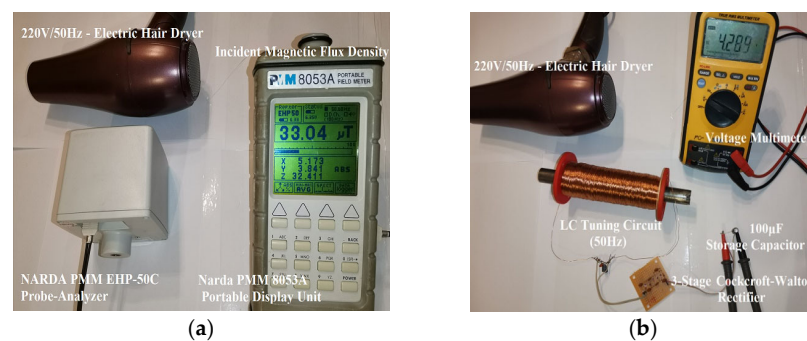


Figure 11. (a) The irradiated magnetic flux density value can reach up to $33 \mu\text{T}$, near a common-use hair dryer, as shown by the Narda PMM EHP-50C analyzer. (b) Experimental measurements showed that the (DC) harvesting voltage can reach up to 4.2 volts from this magnetic field value using the proposed MFEH system.

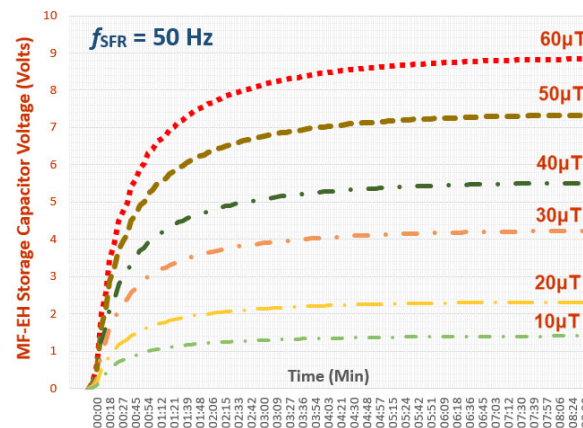


Figure 12. Charging curves of the storage capacitor ($100 \mu\text{F}$) as a function of the intensity of the changing magnetic field (50 Hz) environment. The maximum voltage (V_{max}) of the storage capacitor depends on the intensity of the magnetic field, having also an effect on the charging time constant.

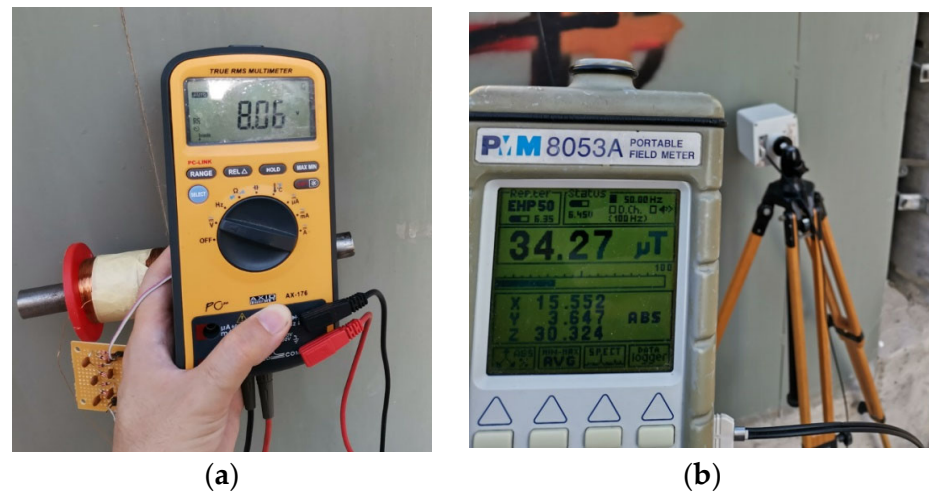


Figure 13. (a) The harvesting voltage is up to 8 Volt near the metal cabin in a medium voltage substation of the public electricity distribution network using the proposed MF-EH. (b) The average value of the magnetic flux density is about $34 \mu\text{T}$, as shown from experimental measurements in a metal cabin of a medium voltage substation within an urban fabric during peak hours.

8. Conclusions and Future Aspects

This study presents the implementation of an isotropic Extremely Low Frequency (ELF) IoT-based meter, as enhanced in our previous work [30]. The prototype circuit can measure the magnetic flux density from 100 nT up to $10 \mu\text{T}$ with 3 square identical sensor probes in vertical alignment, providing isotropic field measurements in the X, Y, and Z planes. The meter has a flat response across the operating frequency range from 40 Hz to 10 kHz . The proposed low-cost device can measure all magnetic fields from sources such as transformers, electric motors, heaters, hair dryers, and power supply network and their harmonic frequencies. An Arduino UNO Wi-Fi Rev.2 board with the integrated Wi-Fi NINA module is responsible for data transferring from the sensor to the cloud, as a complete IoT solution. The measured field can be displayed on any mobile device with Wi-Fi connectivity, supported by the Blynk application via Android and iOS operating systems or web interface. As a future aspect, an improved version of the proposed isotropic meter could be used to implement a distributed EMF IoT sensors network to remotely monitor ELF magnetic field exposure in an interestingly high-risk area. Furthermore, the Arduino FFT feature could also depict the measured magnetic field strength within its harmonic frequencies in future improved implementation. The presence of magnetic fields in urban and semi-urban areas may be exploited as an emergency backup energy source to power low-consumption electronic devices, like Internet of Things (IoT) sensors. In our study, an ELF energy harvesting (EH) circuit implementation was also presented for the utilization of the alternating magnetic field (50 Hz) derived from the operation of transformers, power supplies, and other consumer devices both at the laboratory and at near-distance of medium voltage substations of the electrical public distribution network. Experimental measurements showed that the (DC) harvesting voltage can reach up to 4.2 volts with a magnetic field of $33 \mu\text{T}$, which is caused by the operation of an electric hair dryer, and can fully charge the $100 \mu\text{F}$ storage capacitor (C_s) of the proposed EH system in about 3 min . The usage of a higher value of coil inductance (with a simultaneous change in the capacitance of the capacitor) causes a more sensitive circuit for efficient energy harvested from the magnetic fields of the devices, operating in power frequency (50 Hz).

Author Contributions: Conceptualization, M.G.T.; methodology, M.G.T. and G.A.A.; software M.G.T.; validation, M.G.T.; formal analysis, M.G.T., G.A.A., D.V., T.Y. and D.S.; investigation, M.G.T., G.A.A., D.V., T.Y. and D.S.; resources, M.G.T., G.A.A., D.V., T.Y. and D.S.; data curation, M.G.T.; writing—original draft preparation, M.G.T.; writing—review and editing, M.G.T., D.V., T.Y. and D.S.; visualization, M.G.T.; supervision, D.V., T.Y. and D.S.; project administration, D.V.; funding acquisition, D.V. All authors have read and agreed to the published version of the manuscript.

Funding: The present article is part of the PhD thesis of M.G.T. The implementation of the doctoral thesis was co-financed by Greece and the European Union (European Social Fund-ESF) through the Operational Programme “Human Resources Development, Education and Lifelong Learning” in the context of the Act “Enhancing Human Resources Research Potential by undertaking a Doctoral Research” Sub-action 2: IKY Scholarship Programme for PhD candidates in the Greek Universities (MIS-5113934).



Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used in this study are available upon request from the corresponding author. The data will be publicly available after the completion of the PhD thesis.

Conflicts of Interest: The authors declare that there is no conflict of interest.

References

1. Maffei, M.E. Magnetic Fields and Cancer: Epidemiology, Cellular Biology, and Theranostics. *Int. J. Mol. Sci.* **2022**, *23*, 1339. [CrossRef] [PubMed]
2. Park, J.K.; Jeong, E.H.; Seomun, G.A. Extremely Low-Frequency Magnetic Fields Exposure Measurement during Lessons in Elementary Schools. *Int. J. Environ. Res. Public Health* **2020**, *17*, 5284. [CrossRef] [PubMed]
3. Metz, R. Build this Magnetic Field Meter. In *Radio Electronics-Electronic Experimenter's Handbook*; 1993; Available online: https://www.industrial-electronics.com/re_elec-exp-hndbk_magnetic.html (accessed on 9 November 2023).
4. Stratakis, D.; Miaoudakis, A.; Katsidis, C.; Zacharopoulos, V.; Xenos, T. On the uncertainty estimation of electromagnetic field measurements using field sensors: A general approach. *Radiat. Prot. Dosim.* **2009**, *133*, 240–247. [CrossRef] [PubMed]
5. ICNIRP. Guidelines for limiting exposure to time-varying electric and magnetic fields (1 Hz to 100 kHz). *Health Phys.* **2010**, *99*, 818–836. [CrossRef]
6. EU. Directive 2013/35/EU of the European Parliament and of the Council of 26 June 2013 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields). *Off. J. Eur. Union* **2013**, *2013*, 1–21.
7. Trentadue, G.; Zanni, M.; Martini, G. Assessment of low-frequency magnetic fields in electrified vehicles. In *EUR 30198 EN*; Publications Office of the European Union: Luxembourg, 2020.
8. Bonekamp, H. Magnetic—Field Meter. In *Elektor Magazine*; 1997; p. 26. Available online: <https://www.elektormagazine.com/magazine/elektor-199701/33758> (accessed on 9 November 2023).
9. Cruz, J.; Driver, L.; Kanda, M. Design of the National Bureau of Standards Isotropic Magnetic Field Meter (MFM-10) 300 kHz to 100 MHz. In *Technical Note (NIST TN)*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 1985.
10. David, V.; Antoniou, M.; Cretu, M.; Salceanu, A. An isotropic sensor for the measurement of low frequency electric and magnetic fields. In *Proceedings of the Conference Digest Conference on Precision Electromagnetic Measurements*, Ottawa, ON, Canada, 16–21 June 2002; pp. 20–21.
11. Petrascu, C.; Tulbure, A.; Topa, V. Implementation of an Accurate Measurement Method for the Spatial Distribution of the Electromagnetic Field in a WPT System. *Appl. Sci.* **2023**, *13*, 5773. [CrossRef]
12. Narda PMM 8053A; The Solutions for Every Electromagnetic Problem from 5 Hz up to 40 GHz, User Manual. 2004. Available online: <http://www.gruppompb.com/public/upload/8053BEN-40918-3.16.pdf> (accessed on 9 November 2023).
13. Narda EHP-50C; Electric and Magnetic Field Probe-Analyzer from 5 Hz up to 100 kHz, User Manual. 2009. Available online: https://www.gruppompb.com/public/upload/manuale-v-1_32-ehp-50-c.pdf (accessed on 9 November 2023).
14. Narda EFA-300; For Isotropic Measurement of Magnetic and Electric Fields, User Manual. 2013. Available online: <https://www.narda-sts.com/cn/%E6%9C%8D%E5%8A%A1%E4%B8%8E%E6%94%AF%E6%8C%81/%E4%BA%A7%E5%93%81%E8%B5%84%E6%96%99/efa-cn/pd/pdfs/24104/eID/> (accessed on 9 November 2023).

15. Mavromatis, F.; Boursianis, A.; Samaras, T.; Koukourlis, C.; Sahalos, J.N. A Broadband Monitoring System for Electromagnetic Radiation Assessment. *IEEE Antennas Propag. Mag.* **2009**, *51*, 71–79. [CrossRef]
16. “FASMA” EMF Project—Wind Telecommunications SA. Available online: <https://www.wind.gr/> (accessed on 25 September 2023).
17. “HERMES” EMF Project—Vodafone Telecommunications. Available online: <http://www.hermes.ntua.gr/> (accessed on 25 September 2023).
18. “Pedion 24” EMF Project—Cosmote Telecommunications. Available online: <http://www.pedion24.gr/> (accessed on 25 September 2023).
19. “National Observatory of Electromagnetic Fields-NOEF” EMF Project-Greek Atomic Energy Commission. Available online: <https://paratiritirioemf.eeae.gr> (accessed on 25 September 2023).
20. Narda AMS-8061; Selective Area Monitor—User Manual. Available online: <https://www.narda-sts.com/en/selective-emf/ams-8061/pd/pdfs/23219/eID/> (accessed on 25 September 2023).
21. Narda AMB-8059; Multi-Band Area Monitor—User Manual. Available online: <https://www.narda-sts.com/> (accessed on 25 September 2023).
22. Narda AMB 8057-03/G; Broadband Area Monitor—User Manual. Available online: <https://www.narda-sts.com/en/selective-emf/> (accessed on 25 September 2023).
23. Miroslav, Š.; Lipovský, P.; Draganová, K.; Ňák, J.; Milan, O.; Marek, Š.; Rudolf, A.; Rozenberg, R. Low Frequency Magnetic Fields and Safety. In Proceedings of the 17th Czech and Slovak Conference on Magnetism, Košice, Slovakia, 3–7 June 2019; Acta Physica Polonica Proceedings, A. Volume 137, pp. 693–696.
24. Yuan, S.; Huang, Y.; Zhou, J.; Xu, Q.; Song, C.; Thompson, P. Magnetic Field Energy Harvesting Under Overhead Power Lines. *IEEE Trans. Power Electron.* **2015**, *30*, 6191–6202. [CrossRef]
25. Guo, F.; Hayat, H.; Wang, J. Energy harvesting devices for high voltage transmission line monitoring. In Proceedings of the 2011 IEEE Power and Energy Society General Meeting, Detroit, MI, USA, 24–29 July 2011; pp. 1–8.
26. Roscoe, N.M.; Judd, M.D. Harvesting Energy from Magnetic Fields to Power Condition Monitoring Sensors. *IEEE Sens. J.* **2013**, *13*, 2263–2270. [CrossRef]
27. Gupta, V.; Kandhalu, A.; Ragunathan (Raj), R. Energy harvesting from electromagnetic energy radiating from AC power lines. In Proceedings of the 6th Workshop on Hot Topics in Embedded Networked Sensors (HotEmNets ’10), Killarney, Ireland, 28–29 June 2010; pp. 1–6.
28. Espe, A.E.; Haugan, T.S.; Mathisen, G. Magnetic Field Energy Harvesting in Railway. *IEEE Trans. Power Electron.* **2022**, *37*, 8659–8668. [CrossRef]
29. Yang, K.; Zheng, C.; Tingwen, R.; Tim, L.; Ben, A.; Bimal, N.; Meiling, Z. Magnetic field energy harvesting from the traction return current in rail tracks. *Elsevier J. Appl. Energy* **2021**, *292*, 116911.
30. Tampouratzis, M.G.; Adamidis, G.; Vouyioukas, D.; Yioultsis, T.; Stratakis, D. IoT-based ELF Magnetic Flux Density Meter. In Proceedings of the 3rd International Conference on Control, Artificial Intelligence, Robotics and Optimization (ICCAIRO), Ierapetra, Greece, 11–13 April 2023.
31. Gordon, D.; Brown, R.; Haben, J. Methods for measuring the magnetic field. *IEEE Trans. Magn.* **1972**, *8*, 48–51. [CrossRef]
32. Sebo, S.A.; Caldecott, R.; Kasten, D.G.; Wang, S.; Leach, J.A.; Vinh, T. Magnetic flux density measurement techniques to analyze 345 kV circuit breaker maintenance operations. In Proceedings of the IEEE Porto Power Tech Conference, Porto, Portugal, 10–13 September 2001; Volume 4, p. 5.
33. Wi-FiNINA Arduino Module. Available online: <https://docs.arduino.cc/> (accessed on 25 September 2023).
34. Blynk IoT Platform: For Businesses and Developers. Available online: <https://blynk.io/> (accessed on 25 September 2023).
35. Chaniotakis, M.; Cory, D. *6.071 Introduction to Electronics, Signals and Measurement*; Massachusetts Institute of Technology: Cambridge, MA, USA, 2006.
36. Sethuraman, J. A Note on Fourier Series of Half Wave Rectifier, Full Wave Rectifier, and Unrectified Sine Wave; Vinayaka Mission’s Kirupananda Variyar Engineering College: Salem Tamil Nadu, India. Available online: https://www.academia.edu/7007379/A_NOTE_ON_FOURIER_SERIES_OF_HALF_WAVE_RECTIFIER_FULL_WAVE_RECTIFIER_AND_UNRECTIFIED_SINE_WAVE (accessed on 9 November 2023).
37. Getting Started with the Arduino IoT Cloud. Available online: <https://docs.arduino.cc/arduino-cloud/guides/overview/> (accessed on 25 September 2023).
38. Narda EHP-50F; Electric and Magnetic Field Probe-Analyzer from 1 Hz Up to 400 kHz—User Manual. 2021. Available online: https://www.narda-sts.com/fileadmin/Produktliteratur_BAs_Software/EHP-50F/Bedienungsanleitung_Commands/Manual_EHP50F_EN.pdf (accessed on 9 November 2023).
39. LF Tenmars TM-192/TM-192D, 3-Axis EMF Magnetic Field Meter—User Manual. 2020. Available online: https://www.radonshop.com/mediafiles/Anleitungen/Elektrosmog/Tenmars_TM-192/Tenmars_TM-192_ManualEN.pdf (accessed on 9 November 2023).
40. Jaiwanglok, A.; Eguchi, K.; Julsereewong, A.; Pannil, P. Alternative of high voltage multipliers utilizing Cockcroft–Walton multiplier blocks for 220 V and 50 Hz input. *J. Energy Rep.* **2020**, *6*, 909–913. [CrossRef]
41. Texas Instruments BQ25504 “Ultra-Low-Power Boost Converter with Battery Management for Energy Harvester Applications”—User Manual. 2023. Available online: <https://www.ti.com/lit/ds/symlink/bq25504.pdf> (accessed on 9 November 2023).

42. Tampouratzis, M.G.; Vouyioukas, D.; Stratakis, D. Discone Rectenna Implementation for Broadband RF Energy Harvesting. In Proceedings of the 8th International Conference on Modern Circuits and Systems Technologies (MOCAST), Thessaloniki, Greece, 13–15 May 2019.
43. Tampouratzis, M.G.; Vouyioukas, D.; Stratakis, D.; Yioultsis, T. Use Ultra-Wideband Discone Rectenna for Broadband RF Energy Harvesting Applications. *Int. J. Technol.* **2020**, *8*, 21. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.