

Chameleon Chaotic System-Based Audio Encryption Algorithm and FPGA Implementation

Alaa Shumran*, Abdul-Basset A. Al-Hussein

Electrical Engineering Department, College of Engineering, University of Basrah, Basrah, Iraq

Correspondance

*Alaa Shumran

Electrical Engineering Department,
College of Engineering, University of Basrah,
Basrah, Iraq
Email: pgs.alaash@uobasrah.edu.iq

Abstract

Audio encryption has gained popularity in a variety of fields including education, banking over the phone, military, and private audio conferences. Data encryption algorithms are necessary for processing and sending sensitive information in the context of secure speech conversations. In recent years, the importance of security in any communications system has increased. To transfer data securely, a variety of methods have been used. Chaotic system-based encryption is one of the most significant encryption methods used in the field of security. Chaos-based communication is a promising application of chaos theory and nonlinear dynamics. In this research, a chaotic algorithm for the new chaotic chameleon system was proposed, studied, and implemented. The chameleon chaotic system has been preferred to be employed because it has the property of changing from self-excited (SA) to hidden-attractor (HA) which increases the complexity of the system dynamics and gives strength to the encryption algorithm. A chaotic chameleon system is one in which, depending on the parameter values, the chaotic attractor alternates between being a hidden attractor and a self-excited attractor. This is an important feature, so it is preferable to use it in cryptography compared to other types of chaotic systems. This model was first implemented using a Field Programmable Gate Array (FPGA), which is the first time it has been implemented in practical applications. The chameleon system model was implemented using MATLAB Simulink and the Xilinx System Generator model. Self-excited, hidden, and coexisting attractors are shown in the proposed system. Vivado software was used to validate the designs, and Xilinx ZedBoard Zynq-7000 FPGA was used to implement them. The dynamic behavior of the proposed chaotic system was also studied and analysis methods, including phase portrait, bifurcation diagrams, and Lyapunov exponents. Assessing the quality of the suggested method by doing analyses of many quality measures, including correlation, differential signal-to-noise ratio (SNR), entropy, histogram analysis, and spectral density plot. The numerical analyses and simulation results demonstrate how well the suggested method performs in terms of security against different types of cryptographic assaults.

Keywords

Audio Encryption Algorithm, FPGA, Chameleon Chaotic System, Self-Excited Attractor, Hidden Attractor.

I. INTRODUCTION

The protection of digital data, including audio and video, has become a significant concern in light of the recent and rapid advancements in digital communications. Security is the main objective of the communications system that needs to be met to protect data from assaults (eavesdropping). Before being

transferred, the transmitted data has to be encrypted and protected using several methods [1]. It is critical to use quick and safe encryption techniques to safeguard spoken conversations. Secure speech communications play an important role in military protocols, commerce, politics, e-learning, telephone banking, news broadcast [2], corporate [3], civilian application requirements [4], interactive voice response sys-



This is an open-access article under the terms of the Creative Commons Attribution License, which permits use, distribution, and reproduction in any medium, provided the original work is properly cited.
©2025 The Authors.

Published by Iraqi Journal for Electrical and Electronic Engineering | College of Engineering, University of Basrah.

tems [5], and the Internet of Things (IoT) and Voice over IP (VoIP) [6, 7]. This requires developing a reliable, fast, and strong security system to provide data confidentiality and integrity. To keep up with the advancement of wireless communications technology, researchers have created several encryption methods in this area. Investigating voice encryption methods that may offer a high degree of security, quick processing, and good sound quality in the decoded speech stream is essential. The art of encryption is the creation and use of algorithms that encrypt communication in any format, including audio, video, and images, such that its contents, whether in storage or transmission, cannot be altered or disclosed by uninvited or unauthorized parties. By employing secret keys that are permitted by the sender and recipient's agreement, intended legitimate users who receive the encrypted communication can decode it and view its contents. Numerous scholars have recognized the potential for utilizing the turbulent and dynamic characteristics of a chaotic system in the field of cryptography. The great qualities of these systems include excellent security, non-uniform behavior, and high sensitivity to beginning circumstances and system settings. Because of these subtle nonlinearities, it offers a novel and efficient method of low-complexity secure speech transmission. One of the most significant subjects in nonlinear science is chaos. Over the past 40 years, the scientific, mathematical, and engineering communities have deeply investigated the fascinating and intricate nonlinear phenomena of chaos. Researchers are exploring applications ranging from modeling complex biological processes [8], different engineering applications [9,10], and multiple encryption algorithms employing the strong nonlinear nature of the chaotic system [11]. The integration of chaos theory holds the potential to revolutionize these fields by providing novel methodologies for analysis, prediction, and control, ultimately paving the way for groundbreaking advancements in biomedical research, engineering design, and many other disciplines. Chaos generation has thus grown in importance as a field of study. The well-known Lorenz system served as an inspiration for the development of other chaotic systems [12–15]. In a deterministic system, chaos is defined as long-term aperiodic behavior that demonstrates a sensitive dependency on the initial state [16]. Chaos also has the quality of irregularity. The pathways of the system are not stable at periodic orbits and fixed locations [16]. Additionally, the initial state has a significant impact on the chaotic system. The chaotic model causes the output response to vary very quickly in response to even the smallest alteration in the beginning state. This indicates that there is no connection between the response of the newly formed outputs and the outputs that were produced before altering the original state. Because of their non-periodic character, chaotic systems have traits that make long-term path prediction difficult. Even though these

systems are deterministic, their behavior seems unpredictable, somewhat like that of a system that is heavily impacted by random noise. Because of their broadband nature, sensitivity to beginning circumstances, and non-periodic, noise-like characteristics, chaotic signals are preferred for secure transmission. Chaotic signals have been used in a number of ways to create a secure communication system. Among these is the Pecora-Carroll technique [17, 18], which describes how a state variable from a system that is evolving chaotically is sent as input to a replicating subsystem (receiver) occasionally it synchronizes with the original system (transmitter) when it is sent as input to a replica of a portion of the original system. This finding establishes a connection between chaos theories and communications and creates a new area of study for chaotic communications. A disorganized carrier wave must conceal or scramble the transmitted signal to provide a safe connection. The chaotic carrier signal is often produced by high-frequency chaotic oscillators. Many of the discoveries made in the pursuit of creating chaotic systems with novel properties are based on equilibrium points that display a variety of characteristics, such as chaotic behavior in the absence of any stable equilibria [19–26], and even entire equilibrium curves [27–31]. When creating secure communication networks, these systems are helpful. Chaotic systems with inherent and hidden attractors have been the subject of extensive recent research. In this study, we introduced a chaotic system that we named the chaotic chameleon because, depending on the value of the parameters, the attractor can switch between the hidden attractor and the self-excited attractor.

II. LITERATURE REVIEW

This section focuses on research that uses an FPGA board to study the implementation of a chaotic system and its use in secure chaotic communications. The research may be listed and sorted based on when it was published:

In 2009, C. Eroğlu [32], presented a master's thesis that was filed with the topic of using FPGA to build synchronized chaotic dynamical systems. After discussing the issue of synchronization, the bit stream code is generated and downloaded into the FPGA board, completing the synchronization procedure. The DSP builder tool was utilized in this study to generate the bit streams of the downloading stage, and the theoretical work was confirmed in real-time through practical implementation.

In 2009, S. Sadoudi et al [33], published a paper outlining the Xilinx FPGA board-based Rossler Dynamical system as the foundation for a secure chaotic communication application. In contrast to previous research that produced the desired code by using the Xilinx system generator, the simulation, and practical findings presented here are acquired directly from the VHDL code, and the obtained system results can be applied to secure communication applications.

In 2013, L. Merah et al [34], this study has been regarded as a foundation for information transmission with a security level, based on research into the implementation of the Lorenz chaotic dynamical system by the FPGA board. The Xilinx system generator tool was utilized to apply the study. The simulation results align precisely with the empirical data obtained from laboratory experiments.

In 2015, L. Ding et al [35], suggested a design and testing of hardware circuits to generate chaotic sequences using the Lorenz chaotic system for encryption applications in Field-Programmable Gate Arrays (FPGAs). The study involves modeling and quantizing the Lorenz equations into chaotic sequences and testing them statistically and with logic analyzers to ensure their effectiveness and chaotic properties.

In 2018, Mohammed F. Tolba et al [36], provides an FPGA-based chaotic voice encryption and decryption solution that is based on bit permutations. Techniques for reducing area and delay are used. The addition of a carry look-ahead adder, multi-operand adder, and booth multiplier improves the efficiency of the encryption scheme design. A comparison of the several encryption architectures and an introduction to the state of the art are included. The results demonstrate that the recommended solutions have acceptable security, making them suitable for use in speech transmission. After being simulated using Xilinx ISE 14.7, the designs were implemented on an FPGA Xilinx Virtex-5 xc5lx50T. A throughput of 7.9 Gbit/sec for bit permutation design, 2.6 Gbit/sec for bit permutation, and chaotic modified logistic map is achieved, compared with 1.1 Gbit/sec and 1.49 Gbit/sec for previous work.

In 2018, Munawar A. Riyadi et al [37], suggested A technique for chaotic cryptography has been used to construct a secure voice channel prototype with cipher feedback mode using Spartan-3 FPGA devices. Finally, because the Spartan-3 FPGA can perform chaotic cryptographic algorithms for data at audio frequencies, it offers alternatives for extra speech channel security.

In 2019, Heba M. Yassin et al [38], proposed an innovative approach that relied on the ideas of a chaotic system and DNA modules to create a dynamic S-box that increased security. To deal with chaos, the suggested solution uses a Lorenz chaotic generator. This approach is tested in real-time offline voice encryption and decryption using the Field Programmable Gate Array (FPGA). The experimental results are displayed using an oscilloscope. The security of the system is additionally verified via MATLAB tests.

In 2021, Fethi Dridi et al. [39], using VHDL, researchers evaluated the hardware implementation performance of an FPGA board intended as a secure chaos-based stream cipher (SCbSC) in terms of computational complexity and security. The central part of the system is the proposed secure pseudo-chaotic number generator (SPCNG). Three first-order recursive filters with an internal pseudo-random number (PRN) mixing method and a discrete chaotic map comprise the architecture of the proposed SPCNG. Xilinx XC7Z020 PYNQ-Z2 FPGA platform was utilized to implement the proposed system. Logic resources, throughput, and cryptanalytic and statistical testing showed a favorable trade-off between security and efficiency.

In 2023, GA. Beyene et al [11], proposed a three dimensional fractional-order chaotic system (FOCS) with nonlinear functions included, displaying various forms of equilibria. Different circumstances and parameter values are considered in an analytical and numerical analysis of the system dynamics. The results show that the system is appropriate for reliable encryption applications and has a broad range of dynamic behavior.

In 2023, Mohamad Afendee Mohamed et al [40], suggested a unique three-dimensional chaotic dynamic system with a capsule-shaped equilibrium curve. It is highlighted that the proposed chaotic system has a hidden attractor since it contains an unlimited number of equilibrium locations. An FPGA platform is used to implement the proposed voice cryptosystem. Experimental results show that the proposed encryption technique, with a maximum clock frequency of 178.28 MHz, utilizes 33% of the FPGA.

In this paper, a chaotic chameleon system was used, and its dynamic behavior was studied, and this system was implemented for the first time using a (FPGA). A chaotic chameleon system is one in which, depending on the parameter values, the chaotic attractor alternates between being a hidden attractor and a self-excited attractor. This is an important feature, so it is preferable to use it in cryptography compared to other types of chaotic systems. The dynamic behavior of the pro-

posed chaotic system and analysis methods, including phase portrait, bifurcation diagrams, and Lyapunov exponents, are also studied. The remaining portions of the paper are arranged as follows: Section II presents the dynamics of the chaotic system, such as phase portrait, bifurcation diagrams, and Lyapunov exponents. As well as an introduction to (FPGA), and a brief overview of the ZedBoard Zynq-7000. Section III in this section, we will discuss the audio encryption system based on the chaotic chameleon system using the (XOR). Section IV of the encryption system's performance will be discussed in this section. The system is tested using a number of techniques, including statistical analysis correlation, histogram, spectrogram, and entropy analysis are examples of statistical analyses. The conclusion is presented in the last section V.

III. THE CHAMELEON CHAOTIC SYSTEM DYNAMIC AND FPGA IMPLEMENTATION

A. Chaotic Chameleon System

A chameleon system is a chaotic system where, depending on the values of the parameters, the chaotic attractor alternates between being a hidden attractor and a self-excited attractor. Systems with self-excited attractors and systems with hidden attractors are two categories into which dynamic systems can be divided [41–43]. The hidden attractor has a basin of attraction that does not overlap with any small neighborhoods of equilibrium points, in contrast to the self-excited attractor, which has a basin of attraction linked to an unstable equilibrium. In many engineering issues, hidden attractors are crucial because they permit unexpected responses [44, 45]. The employed system can be described by the equations described by the system (1) [46]:

$$\begin{aligned} \frac{dx}{dt} &= y \\ \frac{dy}{dt} &= a(x + yz) \\ \frac{dz}{dt} &= x^2 + y^2 + bz(z - cx) - d \end{aligned} \quad (1)$$

where a , b , c , and d are the system's parameters. The system (1) behaves as a self-excited attractor when $b \neq 0$ having un-stable equilibrium points, defined as $[0, 0, \sqrt{\frac{d}{b}}]$, and when $b = 0$ the system doesn't have defined equilibrium points and hence shows hidden chaotic oscillations.

The proposed chaotic system is designed under MATLAB-Simulink environment as shown in Fig. 1. The rich behavior of the chaotic system must obfuscate the communication data for higher security requirements. The phase portrait of the presented chaotic system was acquired using the system parameters ($a = -6, b = 0.8, c = 0.1, d = 0.605$) and initial conditions ($x_0 = 0.5, y_0 = 0.5, z_0 = 0.5$) as shown in Fig. 2. It is a self-excited attractor of the chameleon chaotic system (1) at $b \neq 0$ is shown in Fig. 2. Where the system parameter is selected as $a = -6, c = 0.1$ and $d = 0.605$.

When $b = 0$ the system doesn't have defined equilibrium points and hence shows hidden chaotic oscillations, as shown in Fig. 3. To study the parameter dependence of the implemented chaotic chameleon, we study the system's bifurcation in parameter space. While parameters a , b , and c are fixed at their respective values, parameter d is regarded as the bifurcation parameter. The first iteration's beginning conditions are $[0.5, 0.5, 0.5]$, and after each iteration, it is reinitialized to the end values of the state trajectories. Plotting the maxima of each state for each repetition replaces the initial transients. Fig. 4 shows the bifurcation charts of the system for the control parameter d . With the starting condition for the first iteration taken, as $[0.5, 0.5, 0.5]$ and the system reinitialized to the end values of the state variables, it displays the bifurcation of the system where the parameter d is increased from 0.57 to 0.65. For non-linear dynamic systems, Lyapunov exponents (LE) are an essential metric that distinguishes chaotic from non-chaotic motion and gauges the sensitivity of the system to initial conditions. It provides us with a quantifiable measure of chaos, namely the rate of divergence of neighboring trajectories. When LE has a positive value, chaotic behavior is attained. A dynamical system's chaotic nature is confirmed by the presence of a positive Lyapunov exponent [47, 48]. Calculating precise (LEs) is essential for identifying hyper- and chaos in dynamical systems. For both integer and fractional order systems, the Wolf algorithm [47], and the Jacobian approach are well-known time series-based methods for computing Lyapunov exponents. In this work, the Jacobian is employed.

Lyapunov exponents are calculated to propose a novel chaotic system using the Jacobian and found as shown in Fig. 5. Fig.5, shows Lyapunov exponents for the Chameleon chaotic system with the initial condition $[0.5, 0.5, 0.5]$ and using the system parameters ($a = -6, b = 0.8, c = 0.1, d = 0.605$).

B. Introduction and FPGA Architecture

High degrees of system integration and quick advancements in FPGA technology have made FPGAs the preferred plat-

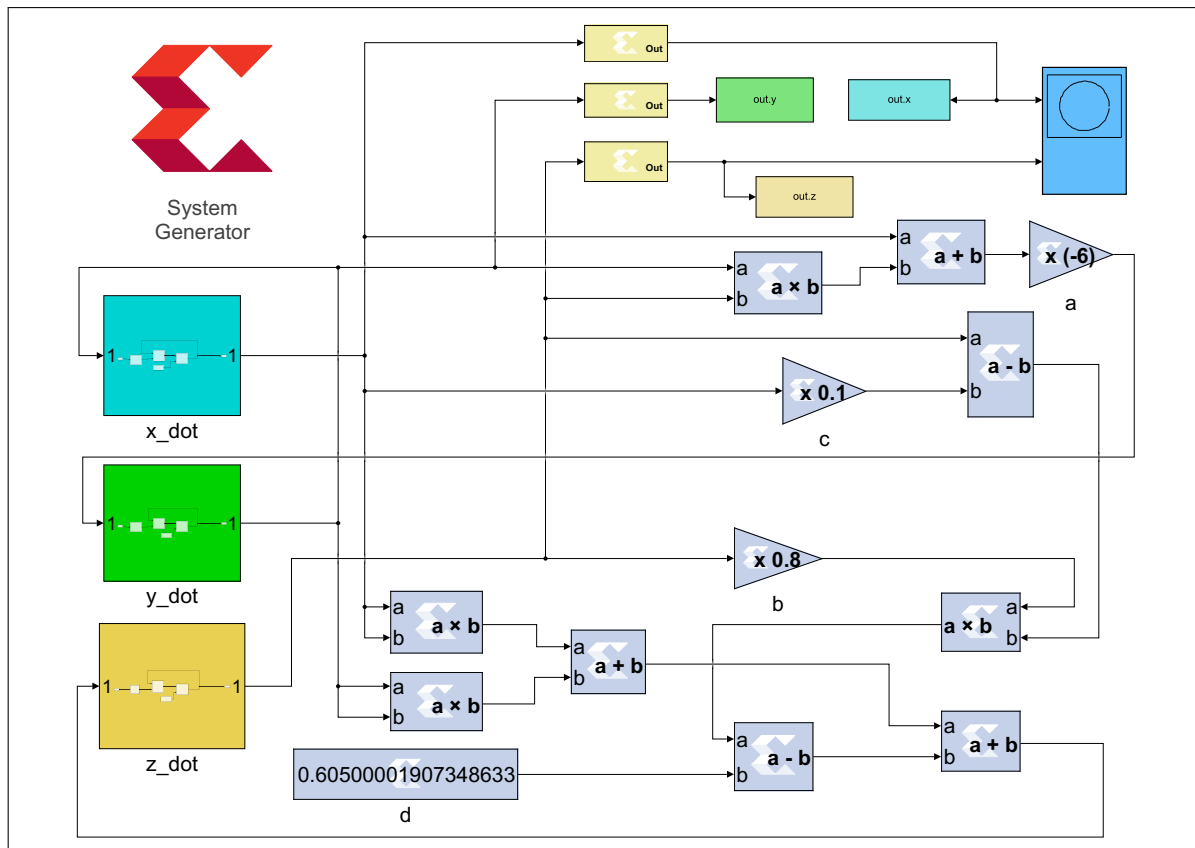


Fig. 1. The chaotic Chameleon system is designed under MATLAB-Simulink environment.

form for embedded digital system manufacturing as well as quick prototyping. Over the past 20 years, FPGAs' capabilities and uses have grown significantly. Recent developments in FPGA technology, which enable the integration of specialized functional blocks like processors, memory, clocking, and arithmetic units, justify the usage of FPGAs as keystones in a growing number of digital systems. Programmable integrated circuit chips, or FPGA chips, are used in the creation of digital circuits. FPGA chips are incredibly fast and capacious. A common moniker for these chips is System on a Chip (SOC). Due to its advantages, such as parallel operation and system-specific design, FPGA chips can perform tasks significantly quicker than personal computers, even though they have a lower operating frequency. Furthermore, FPGAs are widely utilized in several industries, including communications [49], and image processing [50].

C. Xilinx System Generator (XSG)

For FPGA design, the MathWorks model-based Simulink design environment can be used with System Generator, a DSP design tool from Xilinx. By covering the technical knowledge

required for FPGA and Register Transfer Level (RTL) design, design tools streamline design processes. Instead, to expedite the development process, the design is constructed utilizing Simulink's user-friendly visual environment, which makes use of multiple distinct sets of blocks. To create an FPGA executable file, the System Generator may also carry out the FPGA implementation processes of synthesis, mapping, location, and routing.

The System Generator block offers multiple options for clock speed, compilation type, and analysis in addition to specifying the kind of FPGA board to be utilized.

D. Zynq-7000 Family Description

The Zynq-7000 family provides the power, and performance, along with the flexibility and scalability of an FPGA. With a single platform and industry-standard tools, designers can target both high-performance and budget-conscious applications with the Zynq-7000 family of devices. Although all Zynq-7000 family devices have identical Processing Systems (PS), they differ in terms of Programmable Logic (PL) and I/O resources. The Zynq-7000 and Zynq-7000S SoCs can

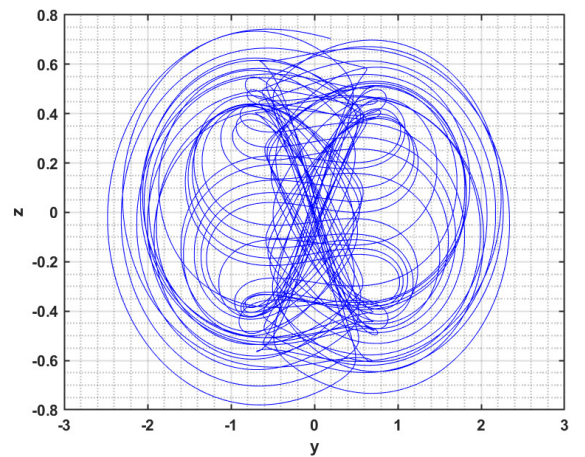
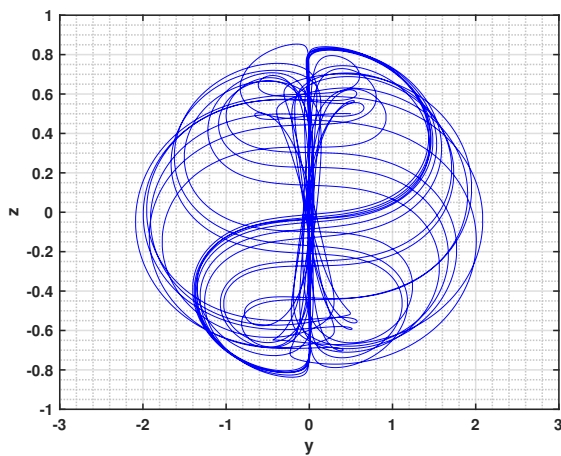
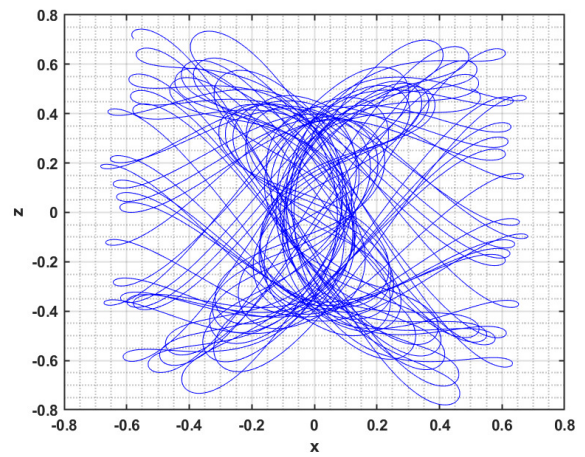
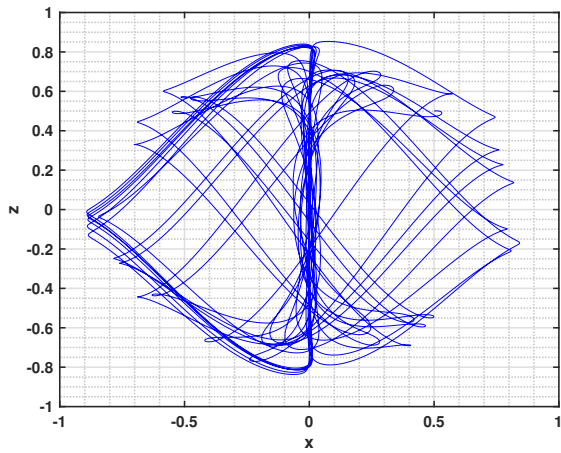
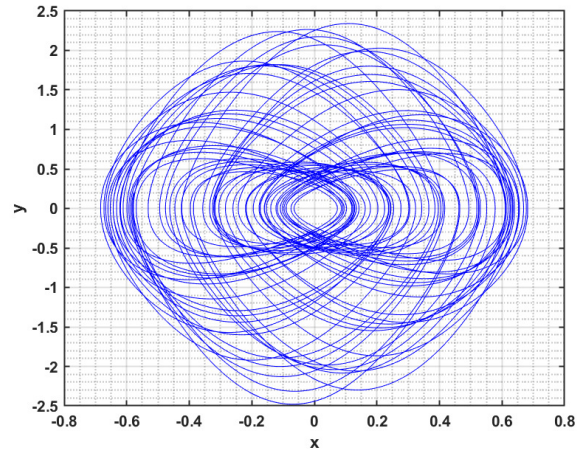
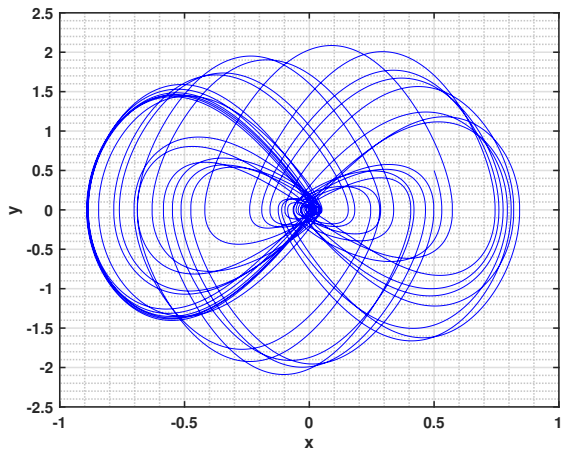


Fig. 2. The self-excited attractor of the chameleon chaotic system (1) at $b \neq 0$.

Fig. 3. The chameleon chaotic system (1) at $b = 0$.

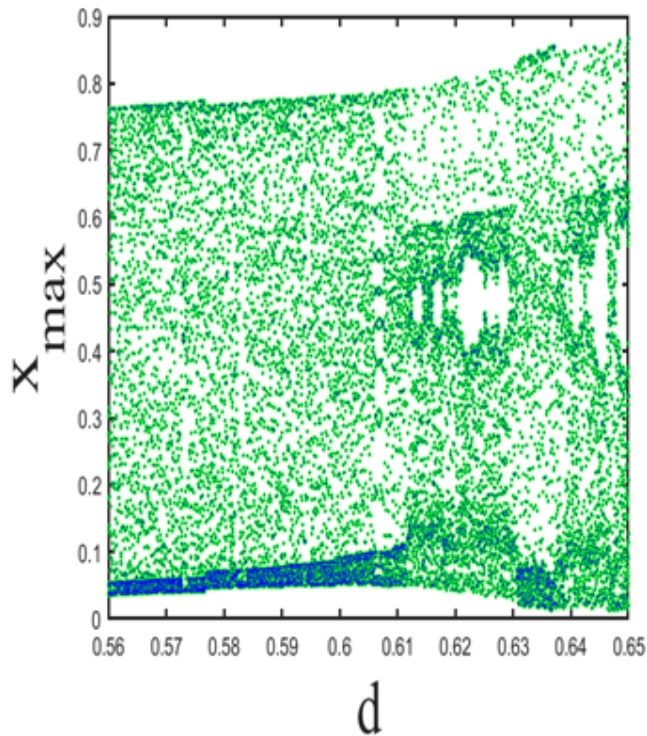


Fig. 4. The bifurcation diagram of the Chameleon system.

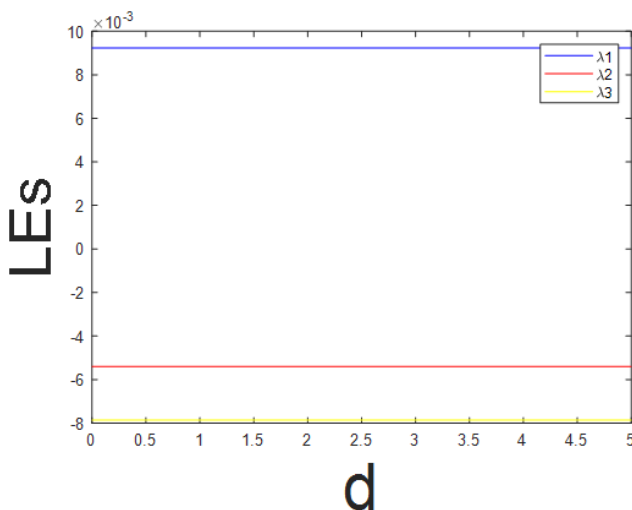


Fig. 5. Lyapunov exponents of the Chameleon system.

therefore be used for a variety of purposes, such as:

- 1) Broadcast cameras.
- 2) Medical diagnostics and imaging.
- 3) Multifunction printers.
- 4) LTE radio and baseband.
- 5) Industrial motor control.
- 6) Industrial networking, and machine vision.
- 7) IP and smart cameras, and more.

Custom software in the PS and custom logic in the PL are made possible by the Zynq-7000 architecture. It makes it possible to realize distinct and special system functionalities.

IV. AUDIO ENCRYPTION SYSTEM

This section illustrates the speech-based cryptosystem using the proposed chameleon system. The block diagram of the encryption system is displayed in Fig. 6. The source of the chaos-based key generators in this cryptosystem is the chameleon chaotic system. The output of the chaotic system is used to mask the voice signal in order to create the encrypted signal that must be sent across the channel. The wave file is read by the workspace using the signal from the workspace MATLAB function with 32-bit resolution and then converted to the system generator environment using an in-gateway block with 32Q24 format. After that, the 32 parallel bits are converted to serial bits to be scrambled with the chameleon chaotic system key using the XOR logical function. To recover the original speech signal, the received encrypted stream bits are XOR with a slave chameleon chaotic system key at the receiver, assuming that the synchronization with the transmitter side is completed and that the key at the receiver matches that at the transmitter. The speech-based cryptosystem has been implemented on the FPGA platform in this section of the study. Fig. 7, shows the system design in XSG First, MATLAB was used to simulate this work, and then Xilinx System Generator (XSG) was used to build the design. Finally, an FPGA Zynq-7000 device was used to create hardware co-simulation for the suggested system. Initially, the system generator design's VHDL code was used to create the recommended chaotic chameleon system diagram in MATLAB Simulink, utilizing

the Xilinx toolkit. With the Xilinx software environment, the VHDL code is then created. The gateway-in and gateway-out functions are used to convert from the Simulink/Matlab environment to the XSG environment and from XSG to the Simulink/Matlab environment respectively. In the first stage of encryption, parallel data is converted into serial data using the Pre-processing function. Which contains the following functions: (Reshape, Transpose, frame, and Unbuffer). This function is used to convert the array into sequential samples, each sample consisting of 32 bits. The sequential sample format is converted to the fixed point format FL=24, WL=32 using Getway-in. After obtaining the binary string, the key created by the chameleon system is encrypted using the XOR function. The binary data produced by this operation is encrypted. To recover the same original communicated data, the code is decoded using a key that is comparable to the sending key and synchronized with it during the decoding or receiving stage. The getaway-out function is used to return the binary data to the Simulink/Matlab environment. Next, the Post-processing function is used to transform the samples into a matrix that is the same size as the original matrix. The following functions are included in this function (buffer and shape).

A. FPGA Implementation Model

The Fix32 – 24 data format is used to build the XSG models with 1 sign bit, 24 fractional bits, and 7 integer bits. This model is used to generate the Vivado project's FPGA implementation. As shown in Fig. 8, below is a timing implementation report such as Worst Negative Slack (WNS), and it is valued is equal (5.2 ns), and the value must be positive. As well as the Utilization value as a percentage of (LUT, FF, DSP, IO, BUFG, and MMCM) and their values are respectively (4%, 1%, 15%, 65%, 6%, 25%) and the amount of power consumed such as (Clocks, Signals, Logic, DSP, MMCM, I/O) and their values are respectively (0.002 W, 0.013 W, 0.013 W, 0.024 W, 0.106 W, 0.023 W).

To calculate the maximum clock frequency using the clock period and Worst Negative Slack ($WNS = 5.2ns$) defined in the implementation timing report as in (2) [51]:

$$f_{max} = \frac{1}{T_s - WNS} \quad (2)$$

T_s is the clock time ($T_s = 35ns$), while f_{max} is the highest frequency ($f_{max} = 33.557MHZ$). If the implementation successfully satisfies all timing constraints, the value of WNS must be positive.

The results of plotting system signals before, after, and during encryption are shown in the following Fig. 9.

V. ANALYSIS OF SPEECH SECURITY

The encryption system's performance will be discussed in this section. The system is tested using a number of techniques, including statistical analysis, key sensitivity, mean square error (MSE), Correlation, histogram, spectrogram, and entropy analysis are examples of statistical analyses. Robust encryption needs to withstand all quantifiable examinations with great resilience. These tests consist of statistical studies, including information entropy analyses, correlation, and histogram analysis.

A. Correlation Analysis

This analysis is a statistical metric used to assess an encryption scheme's strength. For audio applications, correlation is quite helpful. The mutual association between identical segments in the original and encrypted audio samples is calculated by correlation. Audio samples are converted by a robust cryptosystem into a low-correlation random noise signal. The relationship between two audio files' matching sample values is expressed by the measurement of the correlation coefficient between them. This is an additional statistical assessment to examine the efficaciousness of the encryption methods. The correlation coefficient is a measure of the degree of correlation between two files and is always between -1 and 1. Samples from the plain files are comparable to samples from the encrypted file when the correlation between $|1-0.7|$ is strong, between $|0.7-0.3|$ is medium, and between $|0.3-0|$ is weak. The correlation coefficient can be calculated as follows given by (3) [51]:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \quad (3)$$

where $Cov(x,y)$ is the covariance between the original signal x and the encrypted signal y . $D(x)$ and $D(y)$ are the variances of the signals x and y .

The correlation coefficient results are shown in Table I, first for the original and encrypted speech and then for the input and decrypted speech. These findings show that the encrypted

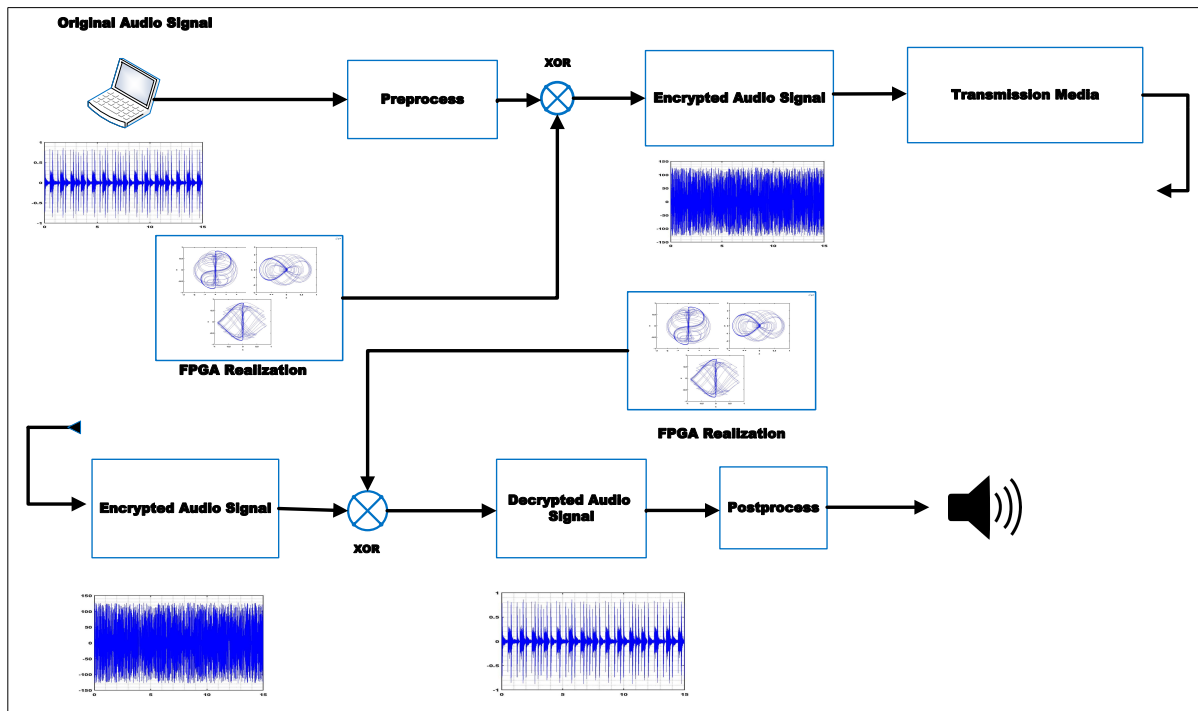


Fig. 6. Block diagram of the proposed audio encryption system.

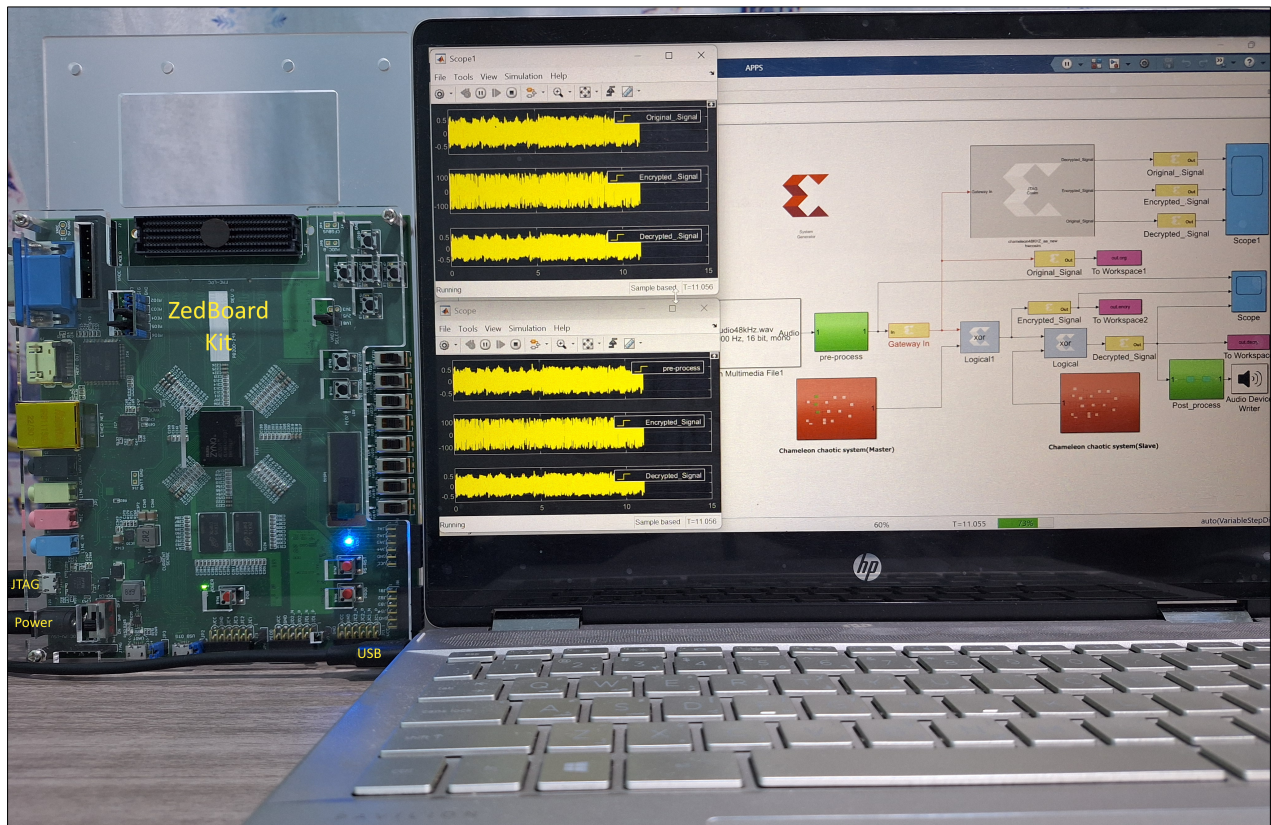


Fig. 7. XSG design of audio encryption and decryption based on the chameleon chaotic system.

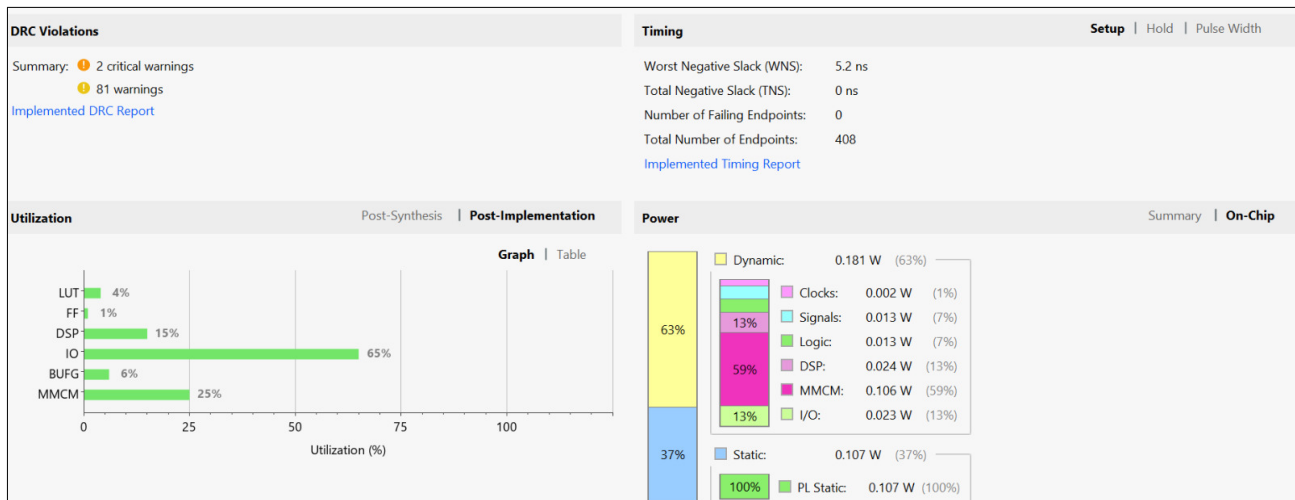


Fig. 8. FPGA resources utilization after model HW implementation using Vivado SW.

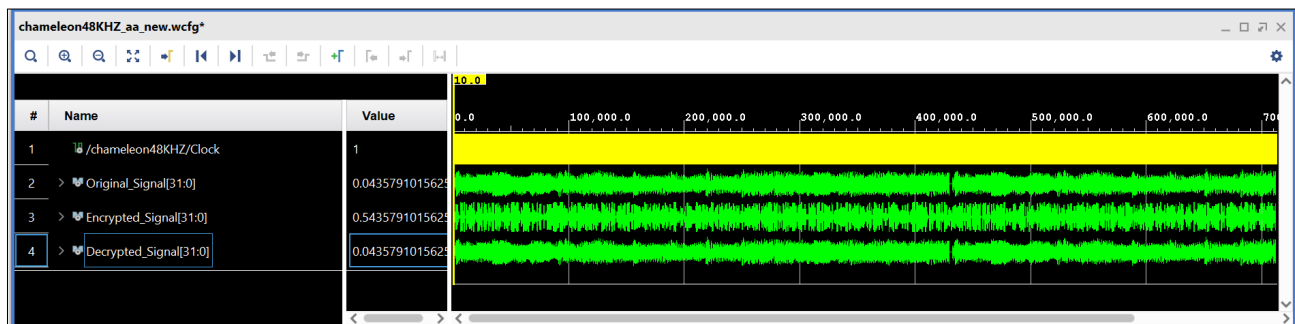


Fig. 9. The time waveform of original, encrypted, and decrypted speech signals respectively.

series has a high degree of correlation and is entirely random due to the extremely low correlation coefficient values. Since the correlation coefficient is one, the decrypted data is identical to the original. We will draw the correlation between the original speech signal and encrypted speech and also the Correlation between the original speech signal and decrypted speech as shown in Table II.

B. Histogram Analysis

Histogram analysis is a reliable technique for assessing the quality of an encrypted voice stream. Getting an encrypted voice file with equally likely sample values is preferable as a realistic encryption technique is likely to encrypt the original speech file into random-like noise. Consequently, no information that would enable statistical assaults on the encrypted area is provided by the encrypted speech. Table III, shows the histogram of the original and encrypted voice signal. The encrypted voice signal's uniformly distributed histogram, which shows the signal's unpredictability, is shown in Table III. The histogram makes it evident that the suggested technique has excellent security against a range of statistical threats. A

popular technique for calculating value distribution is the histogram. Histogram diagrams are a great tool for analyzing audio signals and figuring out how the sample values in the audio files are distributed. Strong encryption is shown by the consistent and close distribution of values in Table III. Additionally, resistance to assaults is shown by the near readings.

C. Audio Spectrogram Analysis

It is a graphic depiction of how the audio frequency spectrum changes over time. Time and frequency are the two geometric dimensions that make up the spectrum. The sampled data is divided into overlapping blocks in the time domain, and each block's spectrum size is determined by performing a Fourier transform on each block. The decibels of audio transmissions at various frequencies and times are represented by distinct colors in the spectrum. High decibels are represented by the dark yellow area and low decibels by the dark blue area. An audio spectrogram is used to provide important information about the relationship between audio signal and frequency and

TABLE I. CORRELATION RESULT FOR ENCRYPTED AND DECRYPTED SPEECH.

No.	Speech file	Correlation between original speech signal and encrypted speech	Correlation between original speech signal and decrypted speech
1	Audio1 (48kHz)	0.0266	1
2	Audio2 (8kHz)	0.0244	1
3	Audio3 (44.1 kHz)	0.0051	1

time. The spectrogram of an original, ciphered, and decoded audio dataset is shown in Table IV), below. The energy distribution in the time-frequency plane of the spectrogram can be used to visually examine the suggested voice cryptosystem. As can be seen in Table IV, the encrypted signal's spectrogram differed significantly from the original signals' spectrogram. As a result, the initial signal lost its meaning. Furthermore, we can infer from the spectrogram plots that the decrypted speech signal in Table IV), is the same as the original speech signal. The results make it very obvious that encrypted audio files are uniform and do not share any commonalities with original audio files. Fourier transform is used to construct the spectrum diagram in the time domain signal.

Table IV), displays the spectrum graphs for the unencrypted, encrypted, and decrypted audio. The amplitude diagram and the spectrum diagram of the original audio exhibit consistent distribution characteristics for high decibels, as demonstrated in Table IV). The equally scattered frequency spectrum of encrypted audio shows that all of the sounds are high decibels, suggesting that the audio signal was effectively dispersed and that the encrypted audio is high decibel noise without any noticeable characteristics. Plotting spectrograms is yet another crucial method for audio signal analysis. In this instance, the sound's frequency in relation to the time domain is the primary focus.

D. Entropy Analysis

It's a statistic for assessing how uncertain encrypted audio data is. The entropy analysis establishes the randomness. The entropy is a measure of an audio cipher's unpredictability. The following equation is used to compute the entropy given by (4) [52]:

$$H(m) = \sum_{i=1}^M p(m_i) \log \frac{1}{p(m_i)} \quad (4)$$

where $p(m_i)$ is the probability that a symbol m_i will occur, and m is the information source and M is the total number of symbols $m_i \in m$. data that has been ciphered is measured for unpredictability using entropy analysis. It is employed to demonstrate the unpredictable nature of encrypted data and the degree to which it resembles white noise. The encrypted data is seen as more random the closer the entropy value is to the number of bits per symbol. Table V, shows the entropy value for the original and encrypted audio signal.

E. Mean Squared Error (MSE)

The Mean Square Error (MSE) tests might be used to evaluate how sensitive the examined decryption system was to minute fluctuations in the encryption key. A mathematical method called MSE is used to evaluate an encryption system's effectiveness. This is accomplished by outlining how the encrypted signal differs from the original. MSE is used to diverge the incorrectly decrypted signals from the original signal when the key is utilized incorrectly. Table VI shows the MSE values of the audio data as a result of our proposed technique. The avalanche effect is measured by the mean square error (MSE), which finds the total squared delay between two encoded audio files. The MSE between these two audio streams can be calculated by taking two vectors X and Y , each containing two audio streams. N is the vector length of X (or Y). The formula for calculating MSE is as follows given by (5) [52]:

$$MSE = \frac{1}{N} \sum_{i=1}^N ((X) - (Y))^2 \quad (5)$$

where N is the length of the original and encrypted signals, X is the original speech signal, and Y is the encrypted signal. These values are used to compute the mean square error (MSE). While it is often the goal of design to minimize Mean Square Error (MSE), encryption systems function better when the MSE value is larger.

F. Number of Sample Change Rate (NSCR) and Unified Average Changing Intensity (UACI) Analysis

Robustness tests like UACI and NSCR are used to examine how well an encryption system performs. In mathematics,

Both UACI and NSCR are calculated by the two equations (6), (7) and (8) [53]:

$$MSE = \frac{1}{N} \left[\frac{\sum_i X_i - X'_i}{2Q - 1} \right] * 100\% \quad (6)$$

$$NSCR = \sum_i \frac{D_i}{N} * 100\% \quad (7)$$

$$\begin{aligned} D_i = 1 & \quad X_i \neq X'_i \\ D_i = 0 & \quad X_i = X'_i \end{aligned} \quad (8)$$

Where X_i and X'_i are the representations original audio signal and encrypted. The audio segment's length, N and Q represents the bit required to describe the audio. The UACI and NSCR results are presented in Table VII, demonstrating that the encryption method is secure and optimal for maintaining the confidentiality of information.

G. Signal-to-Noise Ratio (SNR) and Peak Signal-to-Noise Ratio (PSNR)

Signal-to-noise ratio (SNR) and peak signal-to-noise ratio (PSNR) are used to assess the quality of the signal. The amount of noise present in the encrypted data stream is gauged by the signal-to-noise ratio. Cryptographic analyzers constantly attempt to encrypt the signal's information by increasing the noise. The signal-to-noise ratio is larger than 0dB, meaning that the signal is clearer than the noise, while the encrypted signal is veiled by maximization. A lower PSNR value is necessary for the encrypted audio file since it indicates that the file has a high amount of noise and strong antiattack capabilities. One simple way to confirm the effectiveness of a data encryption scheme is to measure the signal to noise ratio. The signal's noise level in the encrypted data is measured by SNR. Ratio of Signal to Noise (SNR). SNR is used to gauge the quality of the decrypted signal and the encrypted signal's remaining intelligibility. In general, a high SNR number indicates a high-quality decrypted signal, whereas a low SNR value indicates an encrypted signal with higher noise levels than the original voice signal.

PSNR is calculated as follows (9) [53]:

$$PSNR = 10 \log \frac{MAX^2}{MSE} \text{ dB} \quad (9)$$

Where MAX is the maximum possible value of audio stream and MSE is the mean square error between the original and encrypted audio signal. The results from our PSNR tests are shown in the Table VIII.

VI. CONCLUSION

In the chaos literature, a chameleon system is described as a chaotic system in which the chaotic attractor can vary between a hidden attractor and a self-excited attractor depending on the parameter values. This is one of the most important features of this system because it increases the complexity of the system's dynamics compared to other types of chaotic systems. Phase images, bifurcation diagrams, and Lyapunov exponents are used in this research to analyze the continuous chaotic chameleon system. Self-excitation (SA) and hidden attractor (HA) are the main characteristics of the system. Also, it is the first time to implement and use this system in an FPGA platform. FPGA has become an extremely valuable platform due to advances in this field and the creation of sophisticated and efficient modeling, simulation, and synthesis tools. The simulation results confirm that the proposed chaotic systems are effective in encoding and decoding voice communications. Spectrograms, correlation coefficients, and histograms are used to evaluate the security of a cryptosystem. MATLAB Xilinx tool and Vivado software have been used to show the obtained results. The proposed technique can encode many types of audio signals at a high-security level and withstand many attacks, according to comprehensive simulation results. In addition, the algorithm has a high PSNR value and can tolerate many kinds of noise. Three different audio samples were tested referred to as "audio 48kHz," "audio 8kHz," and "audio 44.1kHz" The corresponding PSNR values are as follows: 67.2689, 73.4442, and 61.6569. These high PSNR values indicate good encoding quality. Additionally, the correlation between the original signal and the encoded one is very close to zero, suggesting a strong and effective encryption system. For the three samples, the correlation values are 0.0266, 0.0244, and 0.0051, respectively. Based on the obtained results for UACI and NSCR, we can conclude that the proposed method is both efficient and highly secure for maintaining information confidentiality.

TABLE II. CORRELATION BETWEEN ORIGINAL AUDIO AND ENCRYPTED AND BETWEEN ORIGINAL AUDIO AND DECRYPTED AUDIO.

No.	Speech file	Correlation between original speech signal and encrypted speech	Correlation between original speech signal and decrypted speech
1	Audio1 (48kHz)		
2	Audio2 (8kHz)		
3	Audio3 (44.1 kHz)		

TABLE III. Histogram analysis of an original, encrypted and decrypted audio signal

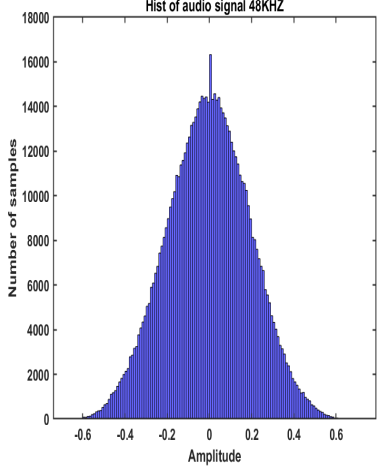
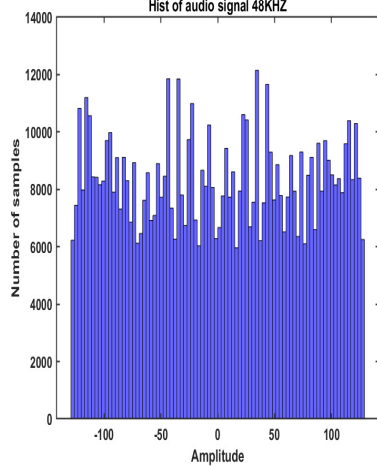
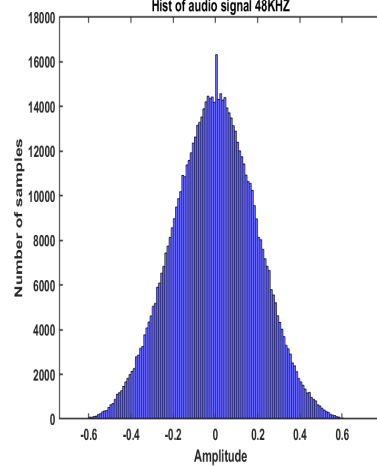
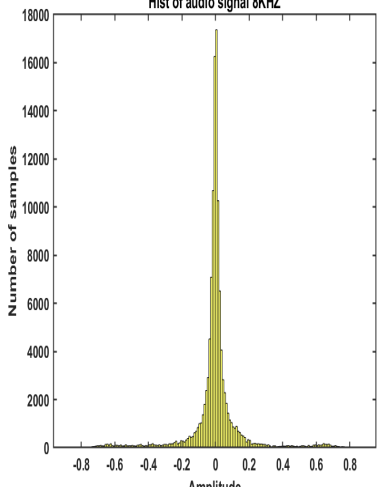
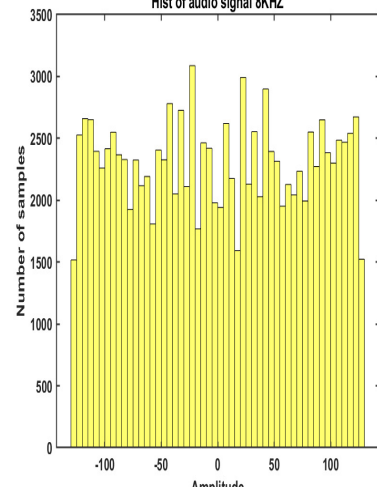
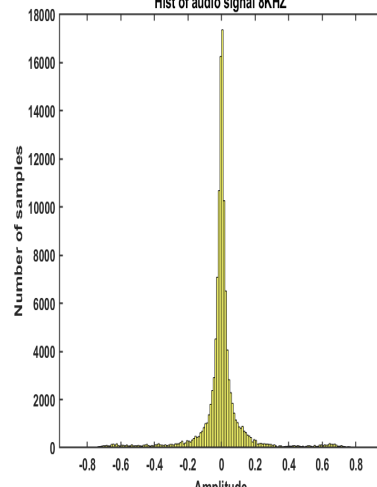
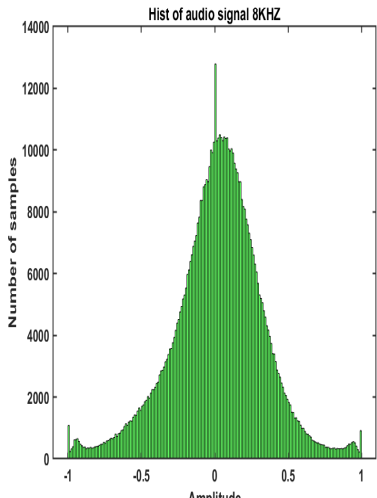
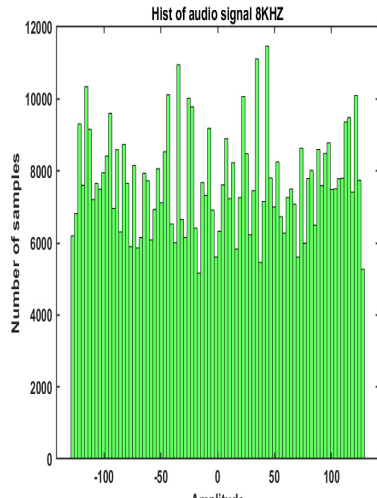
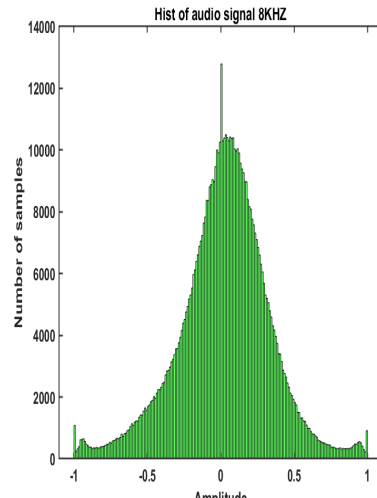
No.	Original audio signal	Encrypted audio signal	Decrypted audio signal
1	 <p>Hist of audio signal 48KHZ</p>	 <p>Hist of audio signal 48KHZ</p>	 <p>Hist of audio signal 48KHZ</p>
2	 <p>Hist of audio signal 8KHZ</p>	 <p>Hist of audio signal 8KHZ</p>	 <p>Hist of audio signal 8KHZ</p>
3	 <p>Hist of audio signal 8KHZ</p>	 <p>Hist of audio signal 8KHZ</p>	 <p>Hist of audio signal 8KHZ</p>

TABLE IV. Spectrogram analysis of an original, encrypted and decrypted audio signal.

No.	Original audio signal	Encrypted audio signal	Decrypted audio signal
1			
2			
3			

TABLE V. THE ENTROPY VALUES OF THE AUDIO ORIGINAL SPEECH SIGNAL AND ENCRYPTED SPEECH.

No.	Speech file	The entropy of the original signal	The entropy of the encrypted signal
1	Audio1 (48kHz)	0.6364	1
2	Audio2 (8kHz)	0.1723	0.9999
3	Audio3 (44.1 kHz)	0.98908	0.99998

TABLE VI. MSE VALUES OF THE AUDIO BETWEEN ORIGINAL SPEECH SIGNAL, ENCRYPTED AND DECRYPTED SPEECH.

No.	Speech file	MSE between original speech signal and encrypted speech	MSE between original speech signal and decrypted speech
1	Audio1 (48kHz)	$2.2123 * 10^3$	0
2	Audio2 (8kHz)	88.9546	0
3	Audio3 (44.1 kHz)	$7.4005 * 10^3$	0

TABLE VII. UACI AND NSCR VALUES

No.	Speech file	UACI(%)	NSCR (100%)
1	Audio1 (48kHz)	38.54586	100
2	Audio2 (8kHz)	47.581	100
3	Audio3 (44.1 kHz)	24.19487	100

TABLE VIII. PEAK SIGNAL-TO-NOISE RATIO.

No.	Speech file	PSNR
1	Audio1 (48kHz)	67.2689
2	Audio2 (8kHz)	73.4442
3	Audio3 (44.1 kHz)	61.6569

CONFLICT OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

- [1] A. Mahdi and S. S. Hreshee, "Design and implementation of voice encryption system using xor based on hénon map," in *2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)*, pp. 1–5, IEEE, 2016.
- [2] S. N. Al Saad and E. Hato, "A speech encryption based on chaotic maps," *International Journal of Computer Applications*, vol. 93, no. 4, pp. 19–28, 2014.
- [3] E. Mosa, N. W. Messiha, O. Zahran, and F. E. Abd El-Samie, "Chaotic encryption of speech signals," *International Journal of Speech Technology*, vol. 14, pp. 285–296, 2011.
- [4] S. B. Sadkhan and R. S. Mohammed, "Proposed random unified chaotic map as prbg for voice encryption in wireless communication," *Procedia computer science*, vol. 65, pp. 314–323, 2015.
- [5] O. El bied, M. A. T. Turbí, A. García-Valero, Á. F. Cano, and J. A. Acosta, "Mitigating ammonia, methane, and carbon dioxide emissions from stored pig slurry using chemical and biological additives," *Water*, vol. 15, no. 23, p. 4185, 2023.
- [6] M. Talbi and M. S. Bouhalel, "Application of a lightweight encryption algorithm to a quantized speech image for secure iot," 2018.
- [7] A. Kulkarni, S. Kulkarni, K. Haridas, and A. More, "Proposed video encryption algorithm v/s other existing algorithms: A comparative study," *arXiv preprint arXiv:1303.3485*, 2013.
- [8] A.-B. A. Al-Hussein, F. Rahma, L. Fortuna, M. Bucolo, M. Frasca, and A. Buscarino, "A new time-delay model for chaotic glucose-insulin regulatory system," *International Journal of Bifurcation and Chaos*, vol. 30, no. 12, p. 2050178, 2020.
- [9] A.-B. A. Al-Hussein, "Chaos phenomenon in power systems: A review," *Iraqi Journal for Electrical & Electronic Engineering*, vol. 17, no. 2, 2021.
- [10] A.-B. A. Al-Hussein, F. R. Tahir, and K. Rajagopal, "Chaotic power system stabilization based on novel incommensurate fractional-order linear augmentation controller," *Complexity*, vol. 2021, no. 1, p. 3334609, 2021.

- [11] G. A. Beyene, F. Rahma, K. Rajagopal, A.-B. A. Al-Hussein, and S. Boulaaras, "Dynamical analysis of a 3d fractional-order chaotic system for high-security communication and its electronic circuit implementation," *Journal of Nonlinear Mathematical Physics*, vol. 30, no. 4, pp. 1375–1391, 2023.
- [12] O. E. Rössler, "An equation for continuous chaos," *Physics Letters A*, vol. 57, no. 5, pp. 397–398, 1976.
- [13] G. Chen and T. Ueta, "Yet another chaotic attractor," *International Journal of Bifurcation and chaos*, vol. 9, no. 07, pp. 1465–1466, 1999.
- [14] Q. Lai, P. D. K. Kuate, F. Liu, and H. H.-C. Iu, "An extremely simple chaotic system with infinitely many coexisting attractors," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 6, pp. 1129–1133, 2019.
- [15] C. Li, W. J.-C. Thio, H. H.-C. Iu, and T. Lu, "A memristive chaotic oscillator with increasing amplitude and frequency," *IEEE Access*, vol. 6, pp. 12945–12950, 2018.
- [16] S. H. Strogatz, *Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering*. CRC press, 2018.
- [17] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Physical review letters*, vol. 64, no. 8, p. 821, 1990.
- [18] L. M. Pecora and T. L. Carroll, "Driving systems with chaotic signals," *Physical review A*, vol. 44, no. 4, p. 2374, 1991.
- [19] C. Li, K. Rajagopal, F. Nazarimehr, and Y. Liu, "A non-autonomous chaotic system with no equilibrium," *Integration*, vol. 79, pp. 143–156, 2021.
- [20] S. Ren, S. Panahi, K. Rajagopal, A. Akgul, V.-T. Pham, and S. Jafari, "A new chaotic flow with hidden attractor: The first hyperjerk system with no equilibrium," *Zeitschrift für Naturforschung A*, vol. 73, no. 3, pp. 239–249, 2018.
- [21] V.-T. Pham, C. Volos, S. Jafari, and T. Kapitaniak, "Coexistence of hidden chaotic attractors in a novel no-equilibrium system," *Nonlinear Dynamics*, vol. 87, pp. 2001–2010, 2017.
- [22] V.-T. Pham, S. Jafari, C. Volos, T. Gotthans, X. Wang, and D. V. Hoang, "A chaotic system with rounded square equilibrium and with no-equilibrium," *Optik*, vol. 130, pp. 365–371, 2017.
- [23] V. MD, A. Karthikeyan, J. Zivcak, O. Krejcar, and H. Namazi, "Dynamical behavior of a new chaotic system with one stable equilibrium," *Mathematics*, vol. 9, no. 24, p. 3217, 2021.
- [24] K. Zhang, M. Vijayakumar, S. S. Jamal, H. Natiq, K. Rajagopal, S. Jafari, and I. Hussain, "A novel megastable oscillator with a strange structure of coexisting attractors: Design, analysis, and fpga implementation," *Complexity*, vol. 2021, no. 1, p. 2594965, 2021.
- [25] Y. Yang, L. Huang, J. Xiang, H. Bao, and H. Li, "Design of multi-wing 3d chaotic systems with only stable equilibria or no equilibrium point using rotation symmetry," *AEU-International Journal of Electronics and Communications*, vol. 135, p. 153710, 2021.
- [26] X. Wang, V.-T. Pham, S. Jafari, C. Volos, J. M. Munoz-Pacheco, and E. Tlelo-Cuautle, "A new chaotic system with stable equilibrium: From theoretical model to circuit implementation," *Ieee Access*, vol. 5, pp. 8851–8858, 2017.
- [27] S. Mobayen, C. K. Volos, S. Kaçar, Ü. Çavuşoğlu, and B. Vaseghi, "A chaotic system with infinite number of equilibria located on an exponential curve and its chaos-based engineering application," *International Journal of Bifurcation and Chaos*, vol. 28, no. 09, p. 1850112, 2018.
- [28] K. Rajagopal, S. Jafari, A. Karthikeyan, A. Srinivasan, and B. Ayele, "Hyperchaotic memcapacitor oscillator with infinite equilibria and coexisting attractors," *Circuits, Systems, and Signal Processing*, vol. 37, no. 9, pp. 3702–3724, 2018.
- [29] V.-T. Pham, C. Volos, S. T. Kingni, T. Kapitaniak, and S. Jafari, "Bistable hidden attractors in a novel chaotic system with hyperbolic sine equilibrium," *Circuits, Systems, and Signal Processing*, vol. 37, pp. 1028–1043, 2018.
- [30] V.-T. Pham, C. Volos, S. Jafari, and T. Kapitaniak, "A novel cubic–equilibrium chaotic system with coexisting hidden attractors: analysis, and circuit implementation," *Journal of circuits, Systems and Computers*, vol. 27, no. 04, p. 1850066, 2018.
- [31] H. Bao, N. Wang, B. Bao, M. Chen, P. Jin, and G. Wang, "Initial condition-dependent dynamics and transient period in memristor-based hypogenetic jerk system with four line equilibria," *Communications in Nonlinear Science and Numerical Simulation*, vol. 57, pp. 264–275, 2018.

- [32] C. Eroglu and F. A. Savaci, "Implementation of partial synchronization of different chaotic systems by field programmable gate array," in *2009 European Conference on Circuit Theory and Design*, pp. 559–562, IEEE, 2009.
- [33] S. Sadoudi, M. S. Azzaz, M. Djeddou, and M. Benssalah, "An fpga real-time implementation of the chen's chaotic system for securing chaotic communications," *International Journal of Nonlinear Science*, vol. 7, no. 4, pp. 467–474, 2009.
- [34] L. Merah, A. Ali-Pacha, N. H. Said, and M. Mamat, "Design and fpga implementation of lorenz chaotic system for information security issues," *Applied Mathematical Sciences*, vol. 7, no. 5, pp. 237–246, 2013.
- [35] L. Ding, Q. Chen, and Q. Ding, "The hardware circuit design, generation, download and tests of chaotic sequence model," *International Journal of Hybrid Information Technology*, vol. 8, no. 4, pp. 97–104, 2015.
- [36] M. F. Tolba, W. S. Sayed, A. G. Radwan, and S. K. Abdel-Hafiz, "Fpga realization of speech encryption based on modified chaotic logistic map," in *2018 IEEE International Conference on Industrial Technology (ICIT)*, pp. 1412–1417, IEEE, 2018.
- [37] M. A. Riyadi, N. Pandapotan, M. R. A. Khafid, and T. Prakoso, "Fpga-based 128-bit chaotic encryption method for voice communication," in *2018 International Symposium on Electronics and Smart Devices (ISESD)*, pp. 1–5, IEEE, 2018.
- [38] H. M. Yassin, A. T. Mohamed, A. H. Abdel-Gawad, M. F. Tolba, H. I. Saleh, A. H. Madian, and A. G. Radwan, "Speech encryption on fpga using a chaotic generator and s-box table," in *2019 Fourth International Conference on Advances in Computational Tools for Engineering Applications (ACTEA)*, pp. 1–4, IEEE, 2019.
- [39] F. Dridi, S. El Assad, W. El Hadj Youssef, M. Machhout, and R. Lozi, "The design and fpga-based implementation of a stream cipher based on a secure chaotic generator," *Applied Sciences*, vol. 11, no. 2, p. 625, 2021.
- [40] M. A. Mohamed, T. Bonny, A. Sambas, S. Vaidyanathan, W. A. Nassan, S. Zhang, K. Obaideen, M. Mamat, M. Nawawi, and M. Kamal, "A speech cryptosystem using the new chaotic system with a capsule-shaped equilibrium curve.," *Computers, Materials & Continua*, vol. 75, no. 3, 2023.
- [41] G. Leonov, N. Kuznetsov, and V. Vagitsev, "Hidden attractor in smooth chua systems," *Physica D: Nonlinear Phenomena*, vol. 241, no. 18, pp. 1482–1486, 2012.
- [42] G. Leonov, N. Kuznetsov, and V. Vagitsev, "Localization of hidden chua's attractors," *Physics Letters A*, vol. 375, no. 23, pp. 2230–2233, 2011.
- [43] D. Dudkowski, S. Jafari, T. Kapitaniak, N. V. Kuznetsov, G. A. Leonov, and A. Prasad, "Hidden attractors in dynamical systems," *Physics Reports*, vol. 637, pp. 1–50, 2016.
- [44] G. Leonov, N. Kuznetsov, and T. Mokaev, "Homoclinic orbit and hidden attractor in the lorenz-like system describing the fluid convection motion in the rotating cavity," *arXiv preprint arXiv:1412.7667*, 2014.
- [45] G. Leonov, N. Kuznetsov, and T. Mokaev, "Homoclinic orbits, and self-excited and hidden attractors in a lorenz-like system describing convective fluid motion: Homoclinic orbits, and self-excited and hidden attractors," *The European Physical Journal Special Topics*, vol. 224, pp. 1421–1458, 2015.
- [46] A.-H. A. Abdul-Basset, T. R. Fadhil, A. Hamzah, A. Girma, and R. Karthikeyan, "Plc implementation of a new chaotic chameleon system," *IEICE Proceedings Series*, vol. 76, no. B2L-41, 2023.
- [47] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, "Determining lyapunov exponents from a time series," *Physica D: nonlinear phenomena*, vol. 16, no. 3, pp. 285–317, 1985.
- [48] S. Ellner, A. R. Gallant, D. McCaffrey, and D. Nychka, "Convergence rates and data requirements for jacobian-based estimates of lyapunov exponents from data," *Physics Letters A*, vol. 153, no. 6-7, pp. 357–363, 1991.
- [49] R. Bittner, E. Ruf, and A. Forin, "Direct gpu/fpga communication via pci express," *Cluster Computing*, vol. 17, pp. 339–348, 2014.
- [50] A. H. Nguyen, M. R. Pickering, and A. Lambert, "The fpga implementation of a one-bit-per-pixel image registration algorithm," *Journal of Real-Time Image Processing*, vol. 11, pp. 799–815, 2016.
- [51] L. Zhang, "System generator model-based fpga design optimization and hardware co-simulation for lorenz chaotic generator," in *2017 2nd Asia-Pacific Conference on Intelligent Robot Systems (ACIRS)*, pp. 170–174, IEEE, 2017.
- [52] M. M. Parvees, J. A. Samath, and B. P. Bose, "Audio encryption—a chaos-based data byte scrambling technique," *International Journal of Applied Systemic Studies*, vol. 8, no. 1, pp. 51–75, 2018.

- [53] W. Dai, X. Xu, X. Song, and G. Li, "Audio encryption algorithm based on chen memristor chaotic system," *Symmetry*, vol. 14, no. 1, p. 17, 2021.