Received: 4 December 2023 | Revised: 2 February 2024 | Accepted: 3 February 2024

DOI: 10.37917/ijeee.20.2.8 Vol. 20 | Issue 2 | December 2024

Open Access

Iraqi Journal for Electrical and Electronic Engineering

Review Article

IJEEE University of Basrah College of Engineering

Study of Chaotic-based Audio Encryption Algorithms: A Review

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

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

Correspondance
*Alaa Shumran
Electrical Engineering Department, University of Basrah, Basrah, Iraq
Email: pgs.alaash@uobasrah.edu.iq

Abstract

Nowadays, multimedia communication has become very widespread and this requires it to be protected from attackers and transmitted securely for reliability. Encryption and decryption techniques are useful in providing effective security for speech signals to ensure that these signals are transmitted with secure data and prevent third parties or the public from reading private messages. Due to the rapid improvement in digital communications over the recent period up to the present, the security of voice data transmitted over various networks has been classified as a favored field of study in earlier years. The contributions to audio encryption are discussed in this review. This Comprehensive review mainly focuses on presenting several kinds of methods for audio encryption and decryption the analysis of these methods with their advantages and disadvantages have been investigated thoroughly. It will be classified into encryption based on traditional methods and encryption based on advanced chaotic systems. They are divided into two types, continuous-time system, and discrete-time system, and also classified based on the synchronization method and the implementation method. In the fields of information and communications security, system designers face many challenges in both cost, performance, and architecture design, Field Programmable gate arrays (FPGAs) provide an excellent balance between computational power and processing flexibility. In addition, encryption methods will be classified based on Chaos-based Pseudo Random Bit Generator, Fractional-order systems, and hybrid chaotic generator systems, which is an advantageous point for this review compared with previous ones. Audio algorithms are presented, discussed, and compared, highlighting important advantages and disadvantages. Audio signals have a large volume and a strong correlation between data samples. Therefore, if traditional cryptography systems are used to encrypt such huge data, they gain significant overhead. Standard symmetric encryption systems also have a small key-space, which makes them vulnerable to attacks. On the other hand, encryption by asymmetric algorithms is not ideal due to low processing speed and complexity. Therefore, great importance has been given to using chaotic theory to encode audio files. Therefore, when proposing an appropriate encryption method to ensure a high degree of security, the key space, which is the critical part of every encryption system, and the key sensitivity must be taken into account. The key sensitivity is related to the initial values and control variables of the chaotic system chosen as the audio encryption algorithm. In addition, the proposed algorithm should eliminate the problems of periodic windows, such as limited chaotic range and non-uniform distribution, and the quality of the recovered audio signal remains good, which confirms the convenience, reliability, and high security.

Keywords

Audio encryption, chaotic systems, FPGA, Synchronization, and Fractional-order Systems.

I. Introduction

Securing speech communication is critical to many businesses, including corporate, military, voice-over IP, and private voice conferences. For the purpose of ensuring data confidentiality, integrity, and authentication, a strong, responsive, and trustworthy security system has to be developed. Accordingly, a variety of encryption algorithms have been created by researchers to accommodate the advancement of communication technologies. To guarantee high data solidity, high data confidentiality, and trusted data, the security system needs to be incredibly fast, robust, and secure. In this regard, scientists have developed a number of encryption algorithms that are reliant on advancements in wireless communication techniques. Encryption methods can be classified into encryption based on traditional methods such as (AES), (DES), (RSA), and encryption based on advanced chaotic systems method. A chaotic system with chaotic behavior can be classified into two types: continuous time and discrete time (map). Chaos with continuous systems depends on ordinary differential equations such as the Lorenz system and the Chen system, which are widely used in the field of signal encryption, while chaos with a discrete function depends on a recurring function such as the logistic map and the quadratic map, which are widely used in communications systems and digital signal encryption. They can also be classified based on synchronization methods and the method of implementation by FPGA, DSP, or Raspberry Pi. The data encryption standard (DES) and the advanced encryption standard (AES), which are examples of standard symmetric encryption programs, can achieve very high levels of guarantee. However despite the fact that the majority of these algorithms are used to encrypt binary data, they are not ideal for real-time audio encryption for the reasons listed below [1–6],:

1) The Standard symmetric cryptographic schemes suffer from a small key space, which leaves them vulnerable to brute force attacks, in addition to high specimen redundancy, bandwidth-dependent amplification of the ciphered signal, and a decline in the output signal-to-noise ratio performance degradation preclude their use in real-time speech encryption.

2) The intricate permutation process of these algorithms necessitates a longer computation time and more processing power.

3) These algorithms require a high level of computing power and more computational time due to their complex permutation process. Asymmetric encryption algorithms are also unsuitable for encryption due to their complexity and slow speed.

Therefore, it's imperative to investigate cutting-edge speech encryption methods that can offer a high degree of security, speed, and excellent audio quality in the decrypted speech signal. Numerous scholars have recognized the potential for utilizing chaotic systems' disordered behaviors and nonlinear dynamics in encryption. These chaotic systems exhibit remarkable qualities like high security, simplicity, , and high sensitivity to initial conditions and system parameters. They are a novel and effective means of delivering low-complexity secured speech communication because of their subtle nonlinear properties. Nevertheless, there are certain difficulties to be overcome when applying chaos theory to encryption. A few of them use different kinds of one-dimensional (1D) chaotic maps when creating speech security systems. One basic, predictable chaotic orbit is the outcome of 1D chaotic maps. This makes it simple for the attacker to acquire the chaotic map's initial states and/or system parameters. Furthermore, weak security and small key space plague one-dimensional chaotic maps. However, if the dimension is increased, the nonlinearity will also increase and security will be improved. Because they have more positive Lyapunov exponents and are difficult to predict time series, higher dimensional (HD) chaotic maps are frequently employed in multimedia encryption. A chaotic system is a cryptography practice that applies the mathematical theory of chaos. Because of the sensitivity of chaotic systems to the initial condition and random-like properties, it is suitable for encrypting multimedia. Lately, the use of chaotic theory for audio signal encryption has received a lot of attention [7–9]. One of the main areas of focus for chaos theory's methods is undoubtedly the dynamic aspect of modern cryptography:

1) Unauthorized individuals can be tricked by the random behavior of chaotic systems without the need for a special mechanism to produce them.

2) The chaotic map evolution time produces an extremely remarkable time evolution, contingent upon control parameters, initial conditions, and minute variations in these amounts. This implies that these initial conditions and control parameters can be used as keys in a cipher system. The cipher chaos method is a crucial, necessary, and effective encryption technique for the security of audio systems. The enormous size of audio data encryption has an impact on the suggested algorithm method that is selected.

II. Scholarly Review

In this work, we cover a general review of various forms of audio encryption and decryption methods, including those based on sophisticated chaotic methods and traditional encryption techniques. Fig. 1.shows a diagram of the methods and tech-

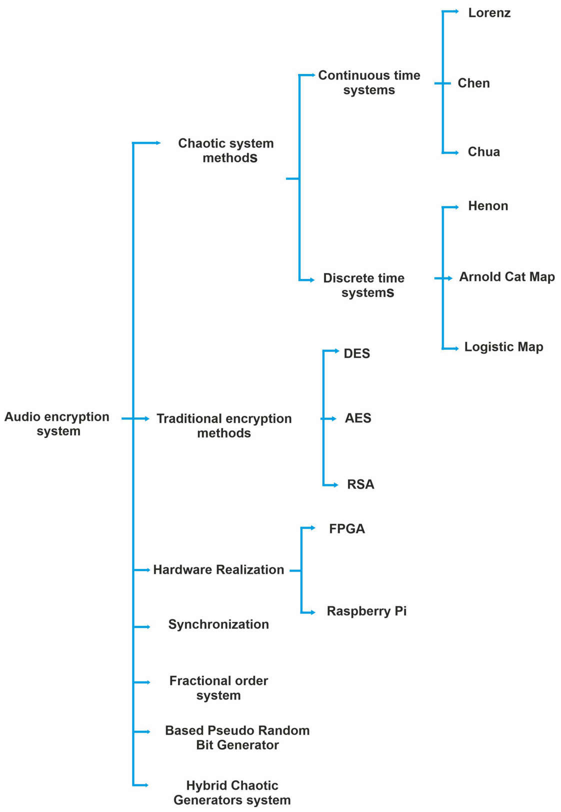


Fig. 1. Scheme of audio encryption techniques.

niques used in encryption processes, where we classified the methods into encryption based on traditional methods such as (DES, AES, RSA) and encryption based on chaotic systems, which are divided into two types: continuous-time systems such as (Lorenz, Chen, Chua) and discrete time systems such as (Henon, Arnold Catt map, logistic map). As well as classifications based on different implementation methods, such as (FPGA, Raspberry Pi), types of synchronization systems, chaotic systems based on fractional order systems, and hybrid chaotic generator systems, as shown in Fig. 1.

A. Traditional Methods:

In 2012,by Rahman et al [10], the authors proposed an effective way to encrypt and decrypt speech data using the RSA algorithm. The maximum number of characters that can be encrypted at once is constrained by the requirement that the integer representation of the message to be encrypted must lie within the range given by the modulus (i.e., M lies in the range $[0, n-1]$). With their continued efforts, all of this algorithm's drawbacks have been eliminated, and speech communication systems will use the RSA digital signature scheme.

In 2016, Khalil [11], they proposed and evaluated two distinct encryption/decryption algorithms that are applied to the audio signal in real-time. The first is the conventional RSA encryption and decryption method, and the second is a newly proposed algorithm built on the idea of symmetric cryptography. The suggested algorithms are simulated and the real-time audio signal is obtained using the MATLAB Simulink simulator tool. Given the mathematical nature of the audio signal, the experimental results demonstrated that the recommended algorithm produces an audio signal with high quality that is identical to the original signal, while the RSA method produces an audio signal with low quality.

In 2020, Sura F .Yousif [12], proposed sound signal encryption and decryption using the RSA algorithm. The algorithm's performance was evaluated through an experimental implementation. Using MATLAB simulations, the results indicated that the Cepstral Distance Measure (CD), Linear Predicative Code Measure (LPC), and Segmental Spectral Signal to Noise Ratio (SSSNR) reached values of 6.8781, 4.9614, and -21.5563 dB, respectively. The approach demonstrated high intelligibility of the recovered audio signal and was found to be safe, dependable, and effective when used in secure audio communications. . The suggested approach is divided into two phases: first, the audio signal is encrypted, and then it is decrypted using the RSA algorithm. The obtained voice or audio samples are encrypted at the transmitter using the public key, which was previously produced together with the private key. The audio samples that have been ciphered or encrypted are transferred one after the other across a communication channel to the recipient, who uses the secret key to decrypt each sample. In the interest of simplicity, it is assumed that the communication or transmission channel is perfect or noise-free. Fig. 2. displays the block diagram of the approach that is being described.

In 2016, El Bakri et al [13], the security of voice calls was maintained by employing the RSA encryption technique. Using an analog-to-digital converter circuit, the voice call is transformed from analog to digital in this method after it is received from the microphone. The output signal is then encrypted using RSA and sent to a digital-to-analog converter circuit to be converted back to analog. The original voice call will be obtained by the receiver by applying the reverse decryption procedures.

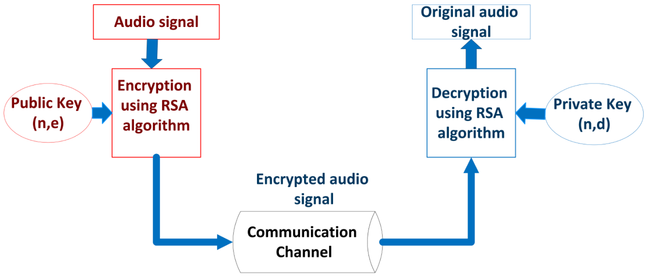


Fig. 2. Block diagram of the presented methodology, adapted from [12].

The investigation for more safe and efficient ways to preserve speech confidentiality began after it became evident from our study of traditional encryption methods that these techniques were ineffective for encrypting speech due to their small key space, high sampling frequency, and complicated switching process, which needed a larger processing unit and more computation time.

B. *New Chaotic Methods:*

Over the past 40 years, the scientific, mathematical, and engineering communities have conducted a great deal of research on chaos, a very fascinating and complex nonlinear phenomena. Consequently, creating chaos has emerged as a prominent field of study.chaotic systems are of high importance in engineering [14–16], and medical [17], applications.In this section, a general method of chaotic encryption will be provided as follows:

1) *Continuous Time Chaotic Systems:*

In 2021, Wanying Dai et al [18], proposed an audio encryption algorithm based on Chen memristor chaotic system. The core idea of the algorithm is to encrypt the audio signal into the color image information. Most of the traditional audio encryption algorithms are transmitted in the form of noise, which makes it easy to attract the attention of attackers. To achieve greater security, the authors employed a unique encryption technique. First, the signal is compressed and denoised using the Fast Walsh-Hadamard Transform (FWHT). The Discrete Cosine Transform (DCT) and the Fast Fourier Transform (FFT) lack the good energy compression characteristics of the FWHT. Additionally, the rectangular basis function of the Fast Fourier Transform (FWHT) can be implemented in the digital circuit more effectively than the triangular basis function, allowing it to transform the reconstructed dual-channel audio signal into the R and B layers of the digital image matrix, respectively. Moreover, the limited chaos range and nonuniform distribution of the periodic window problems are resolved by a novel Chen memristor chaotic system. Ultimately, the overlapping diffusion encryption of the cryptographic block is employed to fill the speech signal's silence period, resulting in the audio ciphertext. The primary audio signal, compression and de-noising, and audio image conversion procedure are the three basic components of the encryption technique. In a memristor chaotic system, the overlapping diffusion encryption process and interactive channel shuffle are used to generate the mask and cipher blocks. Fig. 3. depicts the algorithm encryption process design.

In 2023, ShiMing Fu et al [19], examined a novel four-dimensional hyperchaotic system showed its fundamental dynamic behavior, such as its bifurcation diagram, equilibrium point stability, chaotic attractor, and Lyapunov exponent spectrum. To stabilize the hyperchaotic system until it reaches equilibrium, a linear feedback control technique was presented. The efficacy of this technique was demonstrated using both Multisim circuit simulation and embedded hardware STM32 implementation. In addition, this paper applies the designed hyperchaotic system to audio encryption. The cross-XOR operation method, which has a certain degree of complexity and is easy to implement, is used by the audio encryption algorithm. The results of the experiment demonstrate that, in the time domain, the encrypted audio sequence is exactly the same as the original sequence; however, in the frequency domain, it appears as random noise, making it impossible to decipher the actual information carried by the audio. This demonstrates the efficacy of the hyperchaotic key sequence-based cross-XOR operation method for audio encryption.

An innovative 4D hyperchaotic system given by system (1) [19],:

$$\begin{aligned} \frac{dx}{dt} &= a(y-x)+w \\ \frac{dy}{dt} &= cy-10xz \\ \frac{dz}{dt} &= -bz+10xy \\ \frac{dw}{dt} &= dy+x^2 \end{aligned} \tag{1}$$

the state variables in this case are x,y,z and w and the derivatives of these variables are, in turn, dx/dt,dy/dt ,dz/dt and dw/dt.

In 2020, Ehab Abdul Razzaq Hussein et al. [20], Based on the double chaotic masking technique, an active secure communication system was applied to the information signal. From this study, the following conclusions can be made:

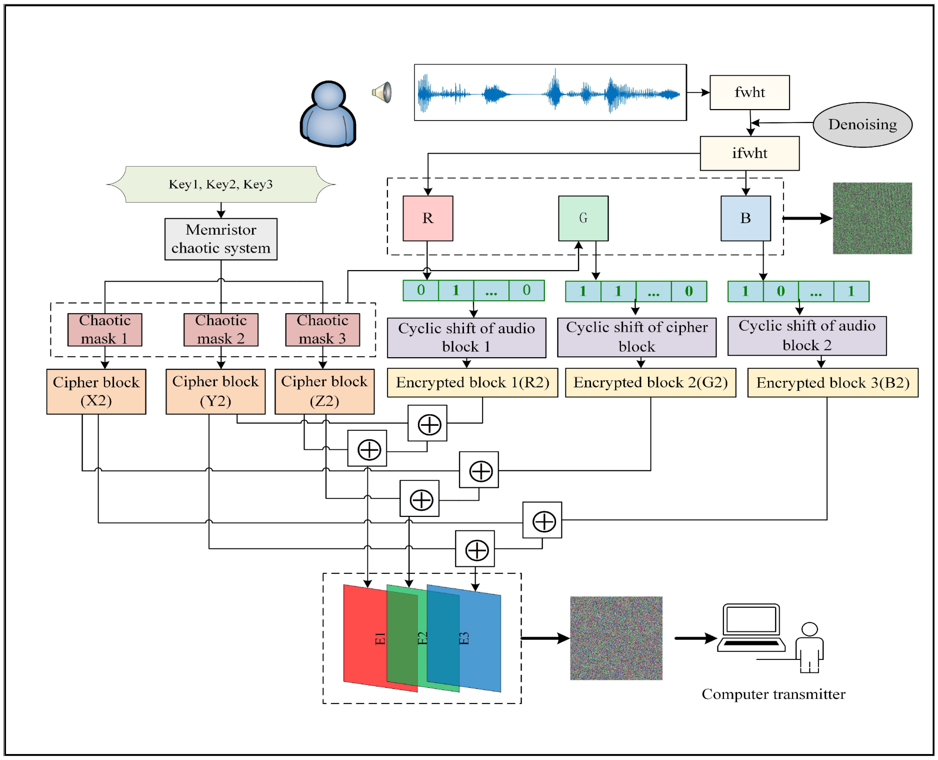


Fig. 3. Encryption flow chart, adopted from [18].

1) Two stages of chaotic masking were applied to the signal in order to implement the recommended security approach: the first stage was created using the Lorenz system as shown in Fig. 4., and the second stage was created using the Roessler chaotic flow system as shown in Fig. 5.

2) The suggested system was tested over an AWGN channel for usage applications, and the results indicated that the quality of the recovered information starts to be clear at a minimum SNR value of 37 dB with an MSE of 0.0061.

3) This strategy has been coupled with the digital processing method (DPM) to lessen the impact of noise on the information that has been recovered.In this way, the suggested method was able to function correctly at a signal-to-noise ratio (SNR) of 21 dB and a mean square error (MSE) of 3.7135 10-6. However, although the system's complexity increased as a result of this combination, which is very helpful in improving the quality of the recovered signal, the channel's bandwidth will need to be increased because the data type has changed from analog to binary. The Lorenz Attractor shown in Fig. 4., is a famous nonlinear three dimensional system of differential equations. The system is described by the following differential equations (2) [20],:

$$\begin{aligned}\frac{dx}{dt} &= \alpha(y-x)\\ \frac{dy}{dt} &= x(\rho-z-y)\\ \frac{dz}{dt} &= \beta z+xy\end{aligned} \tag{2}$$

where (α , ρ and β) are the system parameters.

The Rossler Attractor shown in Fig. 5. is another three dimensional system of differential equations. The system is described by the following differential equations (3) [20],:

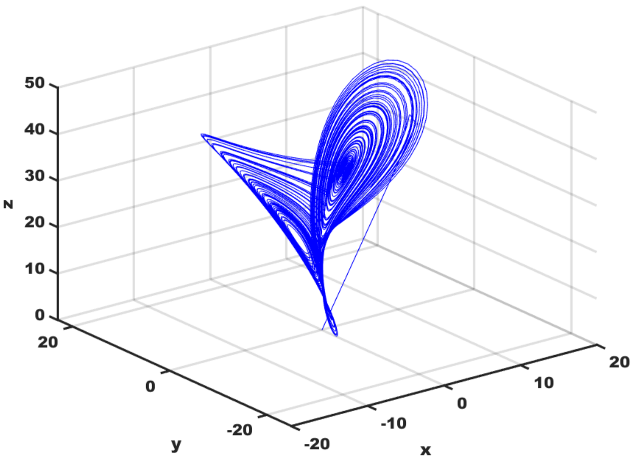


Fig. 4. Lorenz chaotic Attractor.

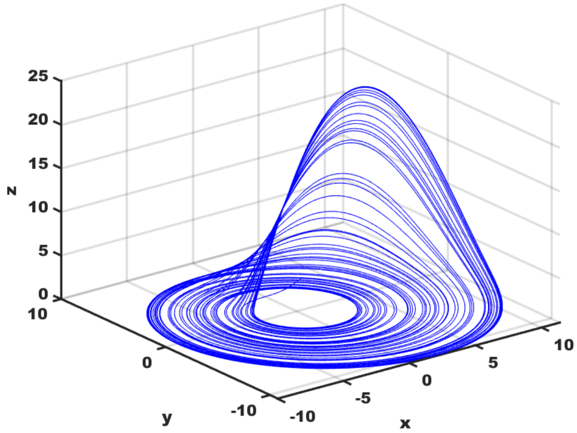


Fig. 5. Roessler chaotic Attractor.

$$\begin{aligned}\frac{dx}{dt} &= -y-x\\ \frac{dy}{dt} &= x+ay\\ \frac{dz}{dt} &= b+z(x-c)\end{aligned} \tag{3}$$

Where a, b , c are the system parametersa and the state variables in this case are x , y and z.

In 2018, Saad S. Hreshee et al. [21], the suggested system is creating a two-level encrypted high-security system. Information permutation, or scrambling, is the first stage. The chaotic map system is used to carry out this procedure. Masking of jumbled information is the second level. The Lorenz system for chaotic flow is responsible for this process. This study's objectives were:

1) Learn about the properties of chaotic systems and use chaos to create safe communication schemes.

2) Create a two-level security system based on Lorenz's chaotic flow and chaotic map to encrypt voice signals.

3) Apply a non-coherent detection receiver to the signal that is masked by chaos. That is, creating a synchronization algorithm that is effective for chaotic sequences at both the transmitter and the receiver.

4) Utilizing MATLAB simulations, assess how well the suggested system performs in the presence of noise.

Fig. 6.displays the suggested system's block diagram. Initially, the speech signal is encrypted using a chaotic map method that has start circumstances that are understood by the sender and the recipient. The disorganized speech will be covered up in the second phase by a disorganized flow signal. A synchronized version of the chaotic signal is initially used at the receiver side to remove the mask. After that, the voice recovery and demystification are carried out appropriately.

2) *Discrete-time Chaotic Systems (maps):*

All the previous encryption methods depend on continuous systems, in the following other methods will be reviewed based on discrete chaotic systems that may provide simpler digital realization.

In 2016, Mohamoud F. El Zaher et al [22], introduced a voice encryption system based on substitution and permutation of voice signal depends on secret keys that generated by utilizing the Henon and Arnold Cat maps. First, the speech signal is converted from 1D to 2D then using the Arnold cut map shown in the Fig. 7. it's used to permute the blocks and return to the 1D format and use the henon map as a masking key. Two scenarios are used to generate the mask key: the first one uses the Henon map, and the second uses a modified Henon map to alter the initial parameter. The analysis and the results show that the key size of the proposed secret key is about 10128.

1) The two equations that represent the double-dimensional chaotic system are known as the Arnold

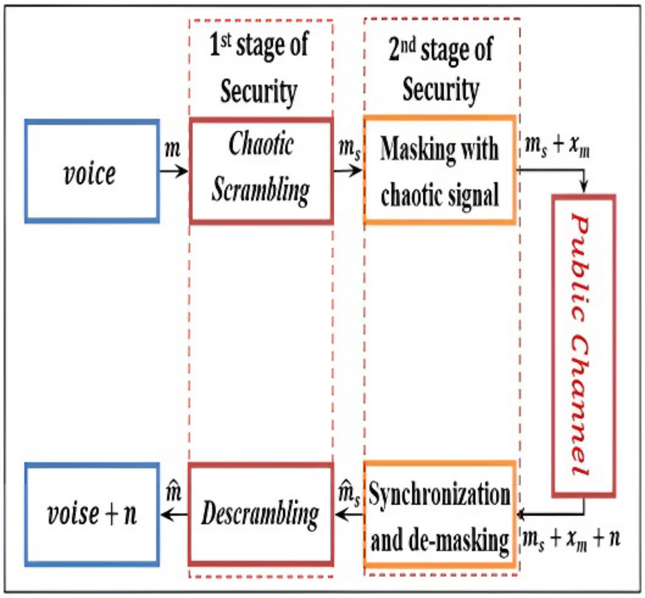


Fig. 6. Block diagram of the two chaotic levels secure proposed system, adopted from [21].

Cat Map, which was first proposed by Vladimir Arnold in 1960. Arnold Cat Map system given by (4) [22]:

$$
\begin{aligned}
X_n + 1 &= X_n + AY_n \quad \text{mod } (N)\\
Y_n + 1 &= BX_n + ABY_n \quad \text{mod } (N)
\end{aligned}
\tag{4}
$$

where, samples' positions in the matrix $(N * N)$are represented by X_n,Y_n and the transformed positions following the cat map are represented by $(n = 1, 2, 3, ..., N_1)$ and $(X_n + 1, Y_n + 1)$ and A are two positive integer control parameters. The cat map is used to iterate through the encryption process. After a total of M iterations, T positive integers exist such that $(X_n + 1$, $Y_n + 1) = (X_n,\ Y_n)$. The parameters A, B and the sample matrix's size $(N * Nmatrix)$ determine the period, T.

2) The Henon Map is a dynamical system with discrete time. It is among the most researched illustrations of chaotic behavior in dynamical systems. A point (X_i, Y_i) in the plane is taken and mapped to a new point using the Henon map. An equation describes a Henon Chaotic system given by (5) [22],:

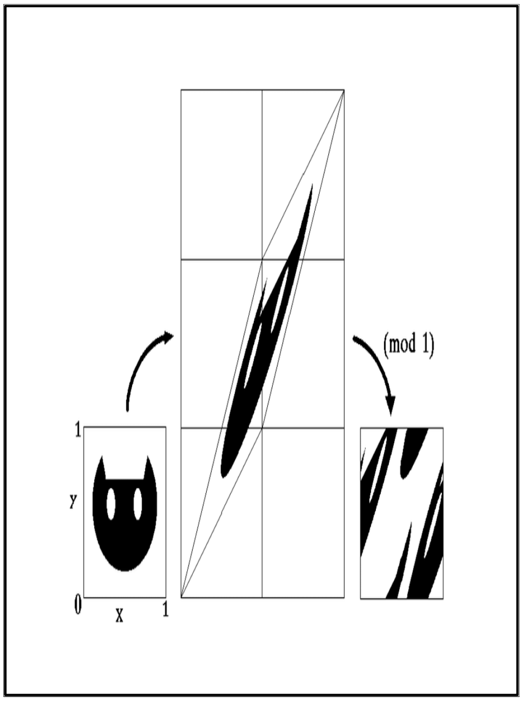


Fig. 7. Map of Arnold Cats, adopted from [23].

$$
\begin{aligned}
X_i + 1 &= 1 + aX_i^2 + Y_i\\
Y_n + 1 &= bX_i
\end{aligned}
\tag{5}
$$

The map displays a basic 2-D chaotic map with quadratic nonlinearity, contingent on parameters a, b initial values(X_0, X_1). The value of a is between 1.07 and 1.4. Fig. 8. displays the bifurcation of X in relation to parameter a, while Fig. 9. illustrates the iteration property at $a = 1.4$.

In 2019, Krasimir Kordov [24], studied a cryptographic algorithm that relies on permutation-substitution architecture realized by using a chaotic circle map and modified rotation equations. The encryption technique is based on traditional symmetric models and makes use of a pseudo-random number generator made of altered rotation equations and a chaotic circle map. A novel pseudo-random generator scheme is introduced and utilized as the foundation for erratic bit-level permutations and substitutions applied to the structure of audio files in order to achieve successful encryption. The encryption process diagram can be illustrated as in Fig. 10. and Fig. 11. illustrates the decryption process.

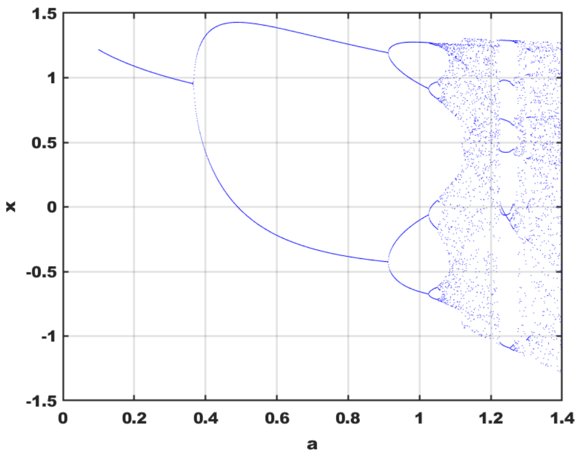


Fig. 8. Diagram showing the bifurcation of $a \in [0, 1.4]$. Henon Map with $a = 1.4$

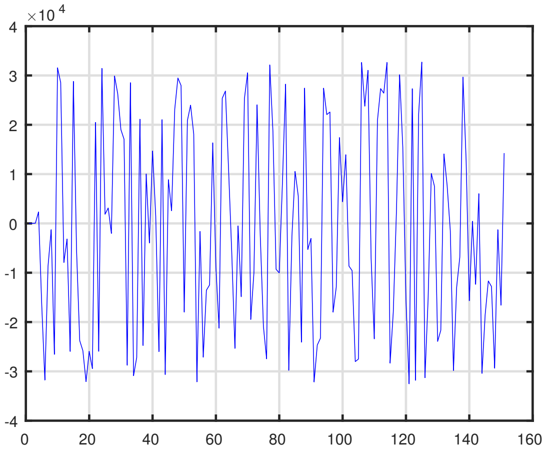


Fig. 9. The time waveform of the signal of the chaotic Henon function.

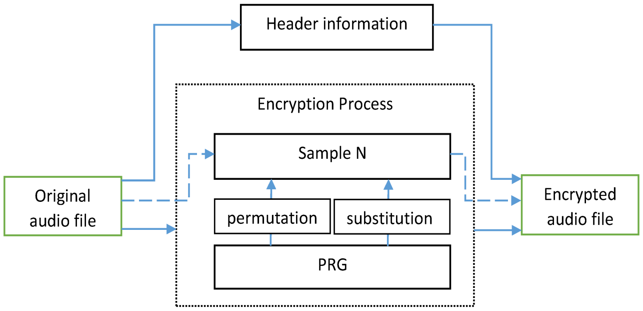


Fig. 10. Encryption scheme, adopted from [24].

In 2021 Haris Aziz [25], a new encryption method is offered for audio applications that require real-time processing. Principles of confusion and diffusion form the foundation of the proposed scheme's framework. Mordell elliptic curves (MEC) and a symmetric group of permutations S8 are applied to the confusion to incorporate nonlinearity. The utilization of chaotic maps enhances the proposed scheme's durability even more. In defense applications, especially in conflict zones, the suggested scheme is meant to meet the needs of real-time voice communications. Multiple S-box applications have resulted in more robust cryptosystems with substantial confusion and dispersion. The multiple S8 MEC S-box collection enhances the security of the suggested scheme and is very relevant to the current target application case. Fig. 12. illustrates the case, in which eight identical pixel values are modified using eight distinct S-boxes and one single S-box. The graphic shows that whereas several S-box transformations result in unique values and improved correlation, transformation with a single S-box had no effect on correlation. By utilizing numerous S-boxes to create a transformation effect, the cryptosystem may be optimized to meet the necessary security level with fewer rounds.

In 2018, M.Y. Mohamed Parvees, et al [26], created a method for efficiently shuffling audio bytes by utilizing several chaotic maps. The audio encryption method creates sequences using the chaotic economic map and the Henon map. The sequences become interdependent with one another because of the system's efficient algorithm. The suggested algorithm will become more sensitive and complex as a result of this interdependency.

In 2017, S. J. Sheela [27], proposed a new audio cryptosystem based on chaotic maps, hybrid chaotic shift transform (HCST), and deoxyribonucleic acid (DNA) encoding rules. The scheme uses chaotic maps such as two-dimensional modified Henon map (2D-MHM) and standard map. An additional tool that improves the cryptosystem's security is DNA encoding technology. Using distinct encryption/decryption quality metrics, the algorithm's performance is assessed for a range of speech signals. Nonetheless, diverse analyses indicated that the algorithm is appropriate for narrow-band radio transmission. .To improve the algorithm's security performance and key space, two chaotic maps are employed. Diffusion and confusion are used, respectively, to alter the speech samples' values and shuffle their locations at random. Fig. 13. displays the encryption scheme's whole design.

In 2016, Amina Mahdi et al [28], a new stream cipher system has been presented in which the bit stream is generated from the Henon map by using three different methods so as to achieve a sequence of zeros and ones similar in properties to Pseudo Random Number (PRN) code. The first method is the analog-to-digital convertor method (ADC) which is used

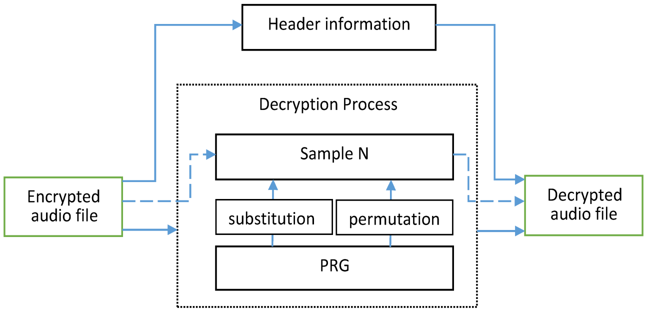


Fig. 11. decryption scheme, adopted from [24].

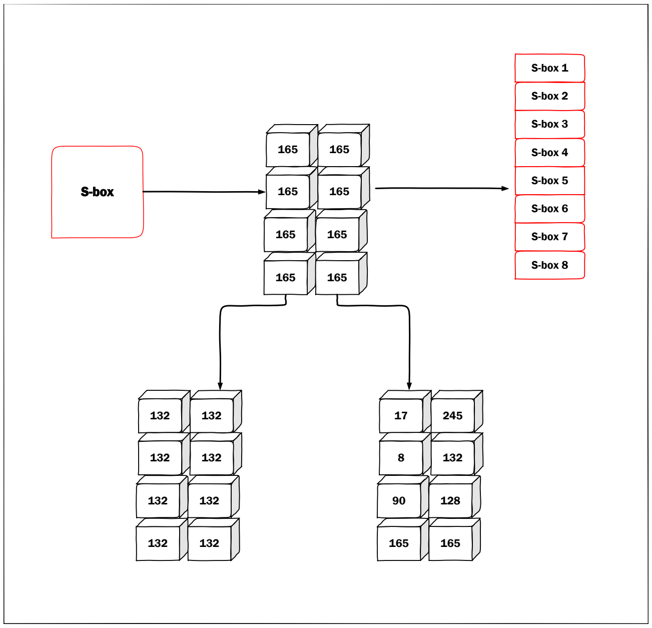


Fig. 12. Transformation effect through S-box, adapted from [25].

to convert each sample to a number of bits. In the second method, the sample of the henon map is limited with a real value threshold then it is converted to binary sequence bits. The last method is the comparator method which mainly depends on the comparison between the output of the two henon maps in order to convert the real value to binary bits.

In 2017, Ardalan Ghasemzadeh et al [29], introduced a speech encryption system by using three chaotic methods namely; the logistic map, the nonlinear chaotic algorithm map (NCA), and the tangent-delay ellipse reflecting cavity-map system (TD-ERCS). The encrypted process is done by multiplying the audio signal by a constant value, each part then is converted to a binary form and divided into three chunks, also each part of the divided chunk is XORed with the generated value from one of the three chaotic methods. Finally, the data is put with each other to produce the encrypted signal. The result shows that the key is 144-bit long, with the best scores of the residual intelligibility measure using correlation coefficients which is about (-0.0082).

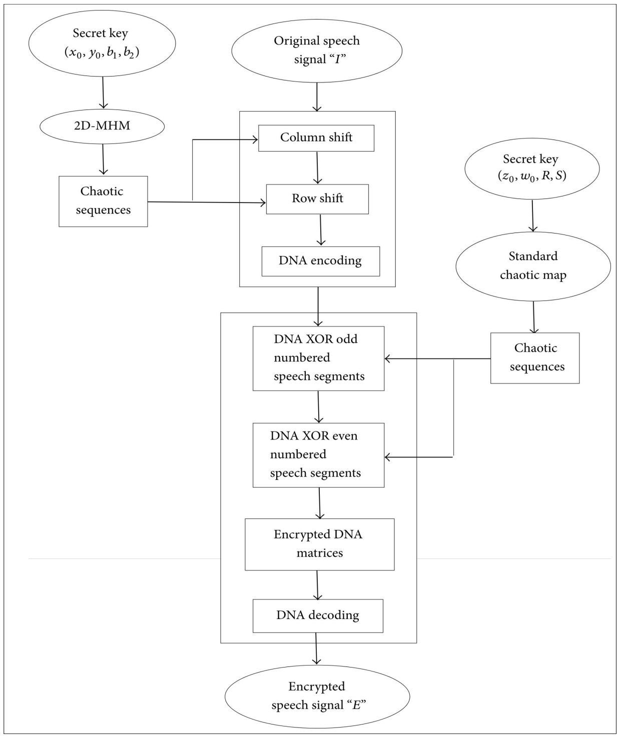


Fig. 13. Proposed encryption scheme flow diagram, adapted from [27].

In 2017, P. Sathiyamurthi et al [30], presented the four chaotic maps used in the speech encryption system: the quadratic map, the tent map, the logistic map, and Bernoulli's map, which serves as a chaotic shift key technique. The original speech is separated into four levels, and the four attractors produced by the chaotic maps are used to permute each level of the speech.

In 2018, Wafaa S. Sayed et al [31], proposed a new speech encryption by using the generalized modified transition map, the main idea behind this map is the conjugacy between two maps which are the tent and logistic map. The encrypted speech signal is generated by XORing the unsecured digital speech signal after passing through the bit permutation with the PRBG key. The findings indicate that the System's key space is 2128.

C. Encryption Methods Depending on Method of Realizations:

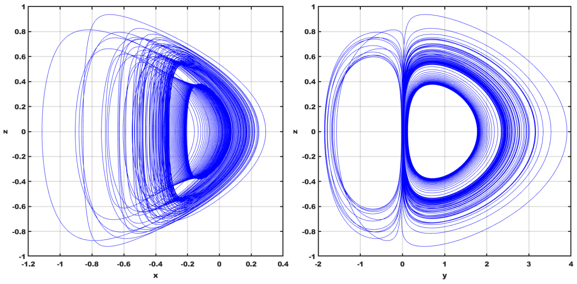
1) The Field Programmable Gates Array (FPGA)

The Field Programmability Gates Array (FPGA) is a technique used for analog and digital implementation and it has become one of the most digital implementations ever, used with a different application to achieve high speed and low cost with a short time to mark the features [32, 33].

In 2023, Mohamad Afendee Mohamed et al [34], proposed a novel chaotic dynamic system in three dimensions with an equilibrium curve shaped like a capsule. Because the proposed chaotic system has an infinite number of equilibrium points, it is noted that it has a hidden attractor. Additionally, it is proven that for the same parameter values but different initial states, the suggested chaotic system displays multi-stability with two coexisting chaotic attractors. The suggested speech cryptosystem is put into practice using an FPGA (Field Programmable Gate Array) platform. According to experimental findings, the suggested encryption scheme uses 33% of the FPGA, with a maximum clock frequency of 178.28 MHz.
A six-term chaotic dynamical system in three dimensions given by (6) [34],:

$$\begin{aligned} \dot{\xi} &= \zeta \\ \dot{\eta} &= -\zeta(\alpha\eta+\beta\eta^2+\xi\zeta) \\ \dot{\zeta} &= \xi^4-(0.1\xi^2\eta^2)+\eta^2-0.5 \end{aligned} \tag{6}$$

In the system (6),as shown in Fig. 14. the state is designated by the three dimensional vector $k=(\xi,\zeta,\eta)$ noteworthy, the dynamics (6) consists of six nonlinear terms. It is assume that all system constantsα,and β, are positive.



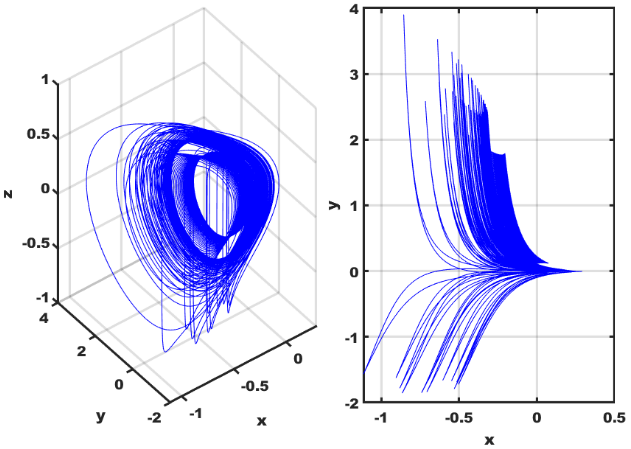


Fig. 14. The signal plots for the proposed 3-D chaotic system.

In 2018, Eduardo Rodríguez-Orozco et al. [35], proposed a cryptosystem consisting of three technologies: (i) a Spartan 3E-1600 FPGA from Xilinx; (ii) a 64-bit Raspberry Pi 3 single board computer; and (iii) a voice recognition chip manufactured by Sun plus.a chaotic pseudo-random binary generator whose decimal numerical values are converted to an 8-bit binary scale under the VHDL description of $mod(255)$. A block diagram of the hardware components used to build up the primary control subsystem and the procedures pertaining to the encryption and decryption of digital pictures is presented in fig.15. The access authorization and XOR encrypter are two sub-entities that work with the FPGA to establish control over the operations. Additionally, it displays the CPRBG entity, which is in charge of producing binary chaotic states in relation to a chosen mapping. Through the UART 1 and UART 2 communication ports, the primary control subsystem simultaneously maintains communication in parallel with the capture, display, and recognition subsystems. Five algorithms govern how the whole system operates.

In 2018, Munawar A. Riyadi et al [36], proposed Using Spartan-3 FPGA boards and a chaotic cryptography algorithm, a secure voice channel prototype with cipher feedback mode has been implemented. Lastly, the Spartan-3 FPGA provides options for additional voice channel security because it can process chaotic cryptography algorithms for data at audio frequencies.

In 2021, Fethi Dridi et al. [37], researchers assessed the hardware implementation performance in terms of computational complexity and security on an FPGA board that was designed as a secure chaos-based stream cipher (SCbSC) using VHDL. The suggested secure pseudo-chaotic number generator (SPCNG) is the core component of the system. The suggested SPCNG's architecture consists of three first-order recursive filters, each of which has an internal pseudo-random number (PRN) mixing technique and a discrete chaotic map. An FPGA platform called Xilinx XC7Z020 PYNQ-Z2 was used to implement the suggested system. A good trade off between efficiency and security was demonstrated by logic resources, throughput, and cryptanalytic and statistical tests.Fig. 16. shows the block diagram of a stream encryption/decryption system. The stream encryption/decryption technique, as we can see, basically involves an XOR operation between the ciphertext and the key-stream for decryption and the plaintext and the key-stream for encryption. The key-stream that the key-stream generator provides determines how secure the system is.

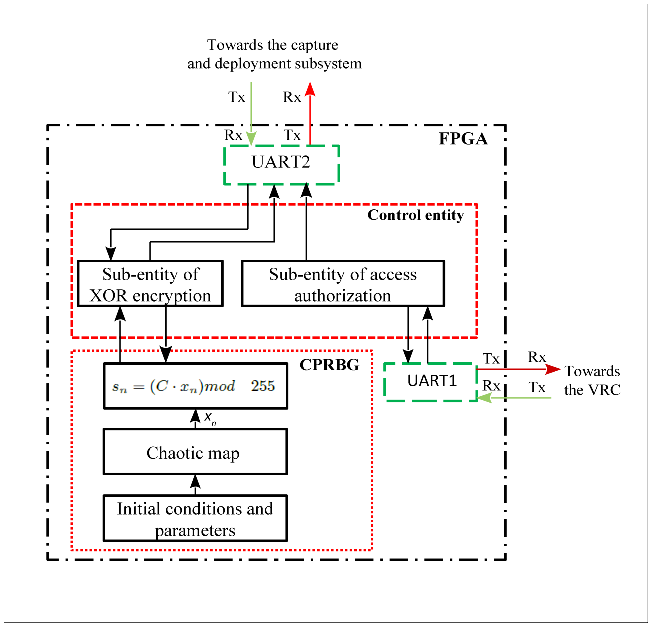


Fig. 15. Block diagram of the main control subsystem implemented in FPGA Spartan 3E, adopted from [35].

In 2019, Heba M. Yassin et al [38], suggested a novel method for creating a dynamic S-box that improved security by relying on the concepts of a chaotic system and DNA modules. The proposed design incorporates a Lorenz chaotic generator to handle chaos. Real-time offline speech encryption and decryption tests are conducted with this design on the Field Programmable Gate Array (FPGA). The oscilloscope is used to display the experimental results. Tests conducted on MATLAB also validate the system's security.

In 2018, Mohammed F. Tolba et al [39], offers a chaotic speech encryption and decryption system based on bit permutations, designed and implemented using FPGA technology. Methods for minimizing both area and delay are employed. To enhance the efficiency of the encryption scheme design,

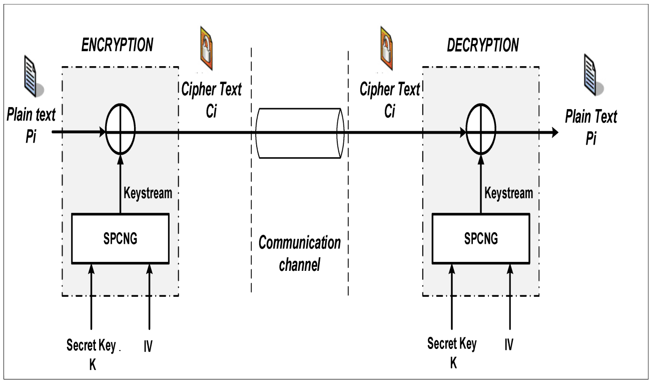


Fig. 16. Block diagram of a stream encryption/decryption system, adopted from [37] .

carry look-ahead adder, multi-operand adder, and booth multiplier are added. There's an introduction to the state of the art and a comparison of the various encryption architectures. It is possible to use the suggested systems for speech telecommunication because of the results, which show that they have good security. The designs were implemented on an FPGA Xilinx Virtex-5 xc5lx50T after being simulated with Xilinx ISE 14.7. In comparison with 1.1 Gbit/sec and 1.49 Gbit/sec for prior work, 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.

2) *Implementation Using Raspberry Pi's*

The Raspberry Pi is a tiny computer board that can be completely programmed and customized. Analyzing the Raspberry Pi's essential components and performance in comparison to some of the IoT prototype platforms already in use has revealed that, despite a few drawbacks, it is still a reasonably priced computer that is used extremely effectively in a wide range of IoT vision research applications. The benefits of the Raspberry Pi may be summed up as follows: The Raspberry Pi is a tiny, self-contained computer that can be configured to run any Linux operating system and can run several distributions. Moreover, its working memory (RAM memory) is quite huge. To save the data, it includes expandable memory that can hold up to 64GB. and its frequency range of operation is 700 MHz to 1000 MHz.Because it supports USB 2.0, a wide range of accessories may be added to it. WiFi and Bluetooth adapters can be added to the Raspberry Pi, depending on the demands. It may run on a sollar cell or a battery.

In 2022, Guillén-Fernández, et al [40], proposed fractional- and integer-order chaotic systems were used to encrypt color images sent over Message Queue Telemetry Transport (MQTT)

for the Internet of Things protocol using Raspberry Pi's connected to Wi-Fi. The NIST and Test U01 tests were used to assess the random binary string generation process of the Chen system. Using XOR for post-processing allowed for the creation of the optimal random sequence. The encryption process over MQTT used this random sequence, and two synchronization techniques—Hamiltonian forms and the OPCL method—were used to synchronize the publisher and subscriber. This is a summary of the encryption technique that the authors suggested. The subscriber that is embedding the same chaotic system can only decrypt the encrypted image sent by the publisher; in the absence of this, the subscriber can only read data that resembles noise. More privacy and security are offered by this, and the average synchronization time was found to be This provides more privacy and security, and the average time for synchronization was measured to be 2.1 s over MQTT using Raspberry Pis over Wi-Fi.
The suggested MQTT-implemented system is shown in Fig. 17. The broker is in charge of facilitating communication between nodes that have the ability to operate as publishers (transmitters) or subscribers (receivers), but they also include an embedded chaotic oscillator that can have various topologies, state variables, parameters, and step sizes. This offers a starting point for conducting private communication with any number of subscribers and a publisher. The fact that the chaotic systems may have various starting circumstances is another crucial point.

In 2019, Yugendra et al [41], the authors proposed, a robust and quick audio watermarking algorithm built on a Raspberry Pi that uses the patchwork method and base64 encoding. High imperceptibility is demonstrated by this methodology, which was assessed by PSNR, which yielded values of 30 dB for the audio signal and 40 dB for the picture. In addition, it is safe and does not require the original audio signal in order to extract the watermark. Bit error rate analysis is used to assess its robustness; it is a very small %0.036. The suggested approach might work well in real-time applications.

In 2016, J. K. SAHA, et al [42], suggested with the use of wired and wireless networks, an embedded system is developed that can transmit real-time video and synchronized audio. Complete audio-visual systematization is achieved by combining video communication with a half-duplex voice communication scheme. The extra features that the framework uses are image capture and video recording. An anonymous, random IP address that is only acknowledged by the users on both the transmitting and receiving ends protects the confidentiality of the communication method. This device is suitable for high-risk surveillance and remote monitoring due to its user-friendly interface, lightweight and compact design, easy maintenance, and impressive security features.

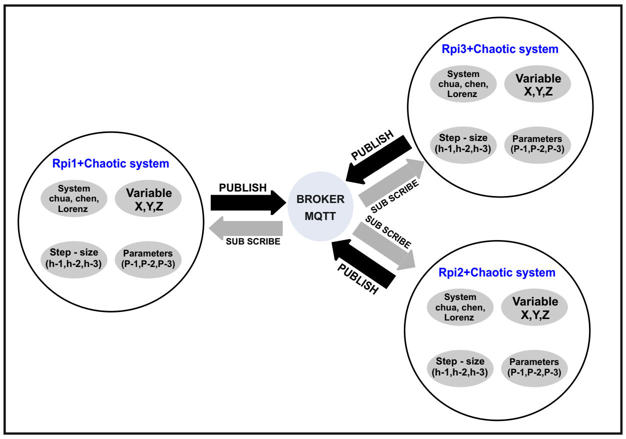


Fig. 17. The MQTT protocol encrypts images by using chaotic systems in the nodes that are under broker control.

D. *Based on Synchronization Methods*

In 2021, N. Ramesh Babu et al [43], proposed Encryption and decryption techniques that rely on the synchronization of 4-D nonlinear fractional-order hyperchaotic systems with external disturbances. When establishing finite-time control for sender and receiver system synchronization, the authors considered fractional orders of ($0 \leq \alpha \leq 1$). The study examines algorithms for audio encryption and decryption by transforming audio samples into image data. Both audio signal encryption and decryption are done using a random mask created from a chaotic mask. A fractional-order hyperchaotic system's error path is demonstrated to be significantly superior to a classical one.Fig. 18. represent the block diagram of proposed audio Encryption.

In 2022, Jianxiang Yang et al [44], suggested developing an adaptive sliding mode controller and applying it to secure communication, this work focuses on the finite-time generalized synchronization problem of non-identical fractional order chaotic (or hyper-chaotic) systems. Model uncertainties as well as the effects of disturbances are considered. It is possible to demonstrate the stability of a newly designed fractional order integral sliding mode surface to the origin within a finite time frame. the overall diagram of speech encryption–decryption process is depicted in Fig. 19.

In 2018, P. Muthukumar, et al. [45], a sliding mode control theory-based general robust synchronization technique has been studied and proposed to robustly synchronize fractional-order dynamical systems with uneven fractional derivatives,

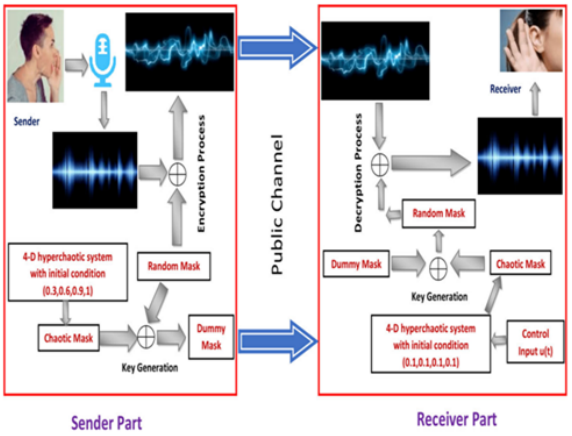


Fig. 18. Block diagram of proposed audio encryption, adopted from [43].

different configurations, and two different dimensions. The required condition for achieving and implementing the suggested synchronization scheme has been determined. The effectiveness of the suggested synchronization scheme has been demonstrated using two different systems: the three-dimensional fractional order reverse butterfly-shaped chaotic system and the four-dimensional fractional order hyper chaos Lorenz system.

E. Chaotic Systems Based on Fractional-order Calculus

The subsequent section will examine additional techniques that rely on the fractional order system. Fractional orders, or additional degrees of freedom, are introduced into the system by fractional calculus. This improves the system's controllability and increases its resistance to hacking.

In 2020, Abdulaziz H. Elsafty, et al. [46], presents a study investigating how the behavior of a chaotic system is affected by the use of various floating-point representations. Furthermore, it provides an analysis of the attractors in three distinct orders: fractional, mixed-order, and integer. This comparison illustrates how few bits are required in each case, for all parameters, to simulate the chaotic attractor. MATLAB-based numerical simulations for every chaotic system under discussion are provided. A hardware implementation for FPGA is suggested for all new Wang chaotic systems, including fractional, mixed-order, and integer ones. They are implemented on the Xilinx Vertix-5 FPGA kit using the Verilog hardware description language and simulated by Xilinx ISE 14.7.

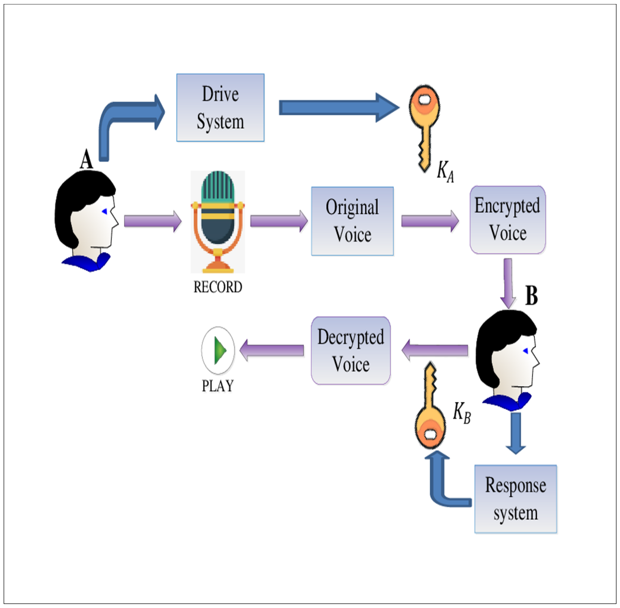


Fig. 19. The overall diagram of speech secure communication, adopted from [44].

In 2021, Abdullah Ali. [47],Suggested a fractional-order chaotic cryptosystem running on gear specific to the application, such as FPGA or DSP development boards. Fractional-order chaotic structures are valuable in data-secure communication because the security space key raises the fractional-order parameters and improves security. Further enhancing the level of communication security is the planned use of discrete time fractional-order chaotic schemes for the digital speech signal scrambling. In 2019, Zahraa M. Alroubaie, et al. [48], it is suggested using synchronized fixed-point chaotic map-based stream ciphers (SFPCM-SC) for speech encryption. The pseudo-random bit generator (PRBG) is created using a fixed-point converter after five chaotic maps—quadratic, henon, logistic, Lozi, and duffing—are synchronized using the master-slave synchronization technique. After creating the encrypted signal, the digital speech signal is XORed with the PRBG. The original speech signal is recovered on the other side by synchronizing the same map with the master map. Xilinx System Generator (XSG) is used to build the design and MATLAB is used to simulate the work initially. The FPGA SP605 XC6SLX45T device is used to implement hardware co-simulation for the proposed system.the general equations of master chaotic maps are given as follows in system (7), and the master system is the chaotic system on the transmitter side [48]:

$$\begin{aligned} X_i+1 &= f(X_i, Y_i) \\ Y_i+1 &= g(X_i, Y_i) \end{aligned} \tag{7}$$

The X signal at the receiver uses the following equations to get the slave system's synchronization with the two systems (8) [48] :

$$W_i+1=f(X_i,Y_i)$$
$$Z_i+1=g(W_i,Z_i) \tag{8}$$

The total voice encryption block diagram employing (SFPCM-SC) is shown in Fig. 20. For fixed- point PRBGs, five different kinds are created, namely FPQM-PRBG, FPHM-PRBG, FPDM - PRBG, FPLM-PRBG, and FPLoM-PRBG.Henon, Duffy, Lozi, quadratic, and logistic mapscorrespondingly. The spoken signal in analog format is sampled using $n=16$ resolution bits and a sample frequency of $f_s=8$ kHz is used. The pre-processing function is used to extract a fixed- point sequence with a length of 32 words for each sample from the sampled speech signal (S). After that, the 32-bit sample was XORed with the key stream bits $(K_i)$to produce the encryption bits (C_i). The original i-th bit(S) is recovered at the receiving end by XORing the encryption bits with the synchronized key stream bits produced on the deciphering side. In order to restore the original speech signal at the transmitter end, the conversion procedure is the inverse function of the pre-processing function.

In 2019, Abd El-Maksoud, et al [49], presented the FPGA implementation of the Ozoguz, Yalcin, and Tang chaotic systems, as well as fractional order multi-scrolls. The chaotic system equations were generalized into the fractional-order domain using the Grunwald-Letnikov (GL) definition. Additionally, each system's parameter variation was examined in relation to the GL definition's window size. To simulate the design under investigation, Xilinx ISE 14.5 was utilized, while Artix-7 XC7A100T FPGA was employed for systems realization. Every fractional system's FPGA summary was presented, and a comparative analysis was conducted. The respective throughputs of Yalcin, Ozoguz, and Tang were found to be $3.417GHz$,$1.513GHz$, and $2.425GHz$, respectively. Since Yalcin had the highest throughput and Ozoguz had the lowest, Yalcin was selected to be employed in the speech encryption system. Additionally, the encryption algorithm for speech encryption used the Yalcin system. One clock latency was used to implement the entire system on FPGA.

In 2016, Fadhil S. Hasan [50], The author presents the Fixed-Point Chaos-based Stream Cipher (FPC-SC), which is used to encrypt speech signals. The stream cipher system uses a fixed-point chaos-based pseudo-random bit generator (FPC-PRBG) as its key sequence. Gold FPC-PRBG is generated by combining two chaotic Lorenz and Chen systems. The outcomes demonstrate that FPC-PRBG can be used to generate high speech security levels and has good statistical randomness and encryption performance measures. The Xilinx System Generator (XSG) with Xilinx Virtex 4 FPGA device is used to implement FPC-PRBG. The system is accessed and routed in this device with throughputs of 818.64, 7978.88, and 780.24 Mbits/sec for Lorenz, Chen, and Gold FPC-PRBG, respectively, where 40 bits fixed-point operation is used.

In 2023, Girma Adam, et al. [51], a three-dimensional fractional-order chaotic system (FOCS) is created; the system has by adding a nonlinear function and the values of its parameters, equilibria can take on a variety of forms. A dynamical analysis is carried out using analytical and numerical methods in order to understand the behavior of the system under various situations and parameter values. Phase portraits, bifurcation analysis, Lyapunov spectra, and Lyapunov exponents (LEs) are some of the methods used in this investigation. The system exhibits more complex attractors than a standard chaotic system with an integer value, in particular when the fractional order q is set to 0.97. It is very suitable for creating secure communication networks because of its characteristic. To further demonstrate the system's viability, a working implementation built around an electrical circuit has been created. Two layers of encryption were used in the construction of a secure communication system.

F. Chaotic Systems Based Pseudo Random Bit Generator (PRBG)

The PRBG is widely used in many applications such as computer games, cryptography testing, numerical analysis, and integrated circuits. When creating pseudo-random numbers to create a binary key stream for encryption, the chaotic system's orbit's aperiodic, irregular, unpredictable, and sensitive dependence on initial conditions are useful properties to have:

In 2016, Farsana F J et al [2], suggested a new method for speech encryption by using diffusion and confusion processes of the speech samples using Zaslavsky map and cat transform. Firstly, the original speech signal is converted to the frequency domain by using discrete cosine transform (DCT) and its binary information is confused by XORing with the key stream generated from the two-dimensional chaotic Zaslavsky map. The result is confused and rearranged by using the cat transform and finally, the resulted signal is converted to the time

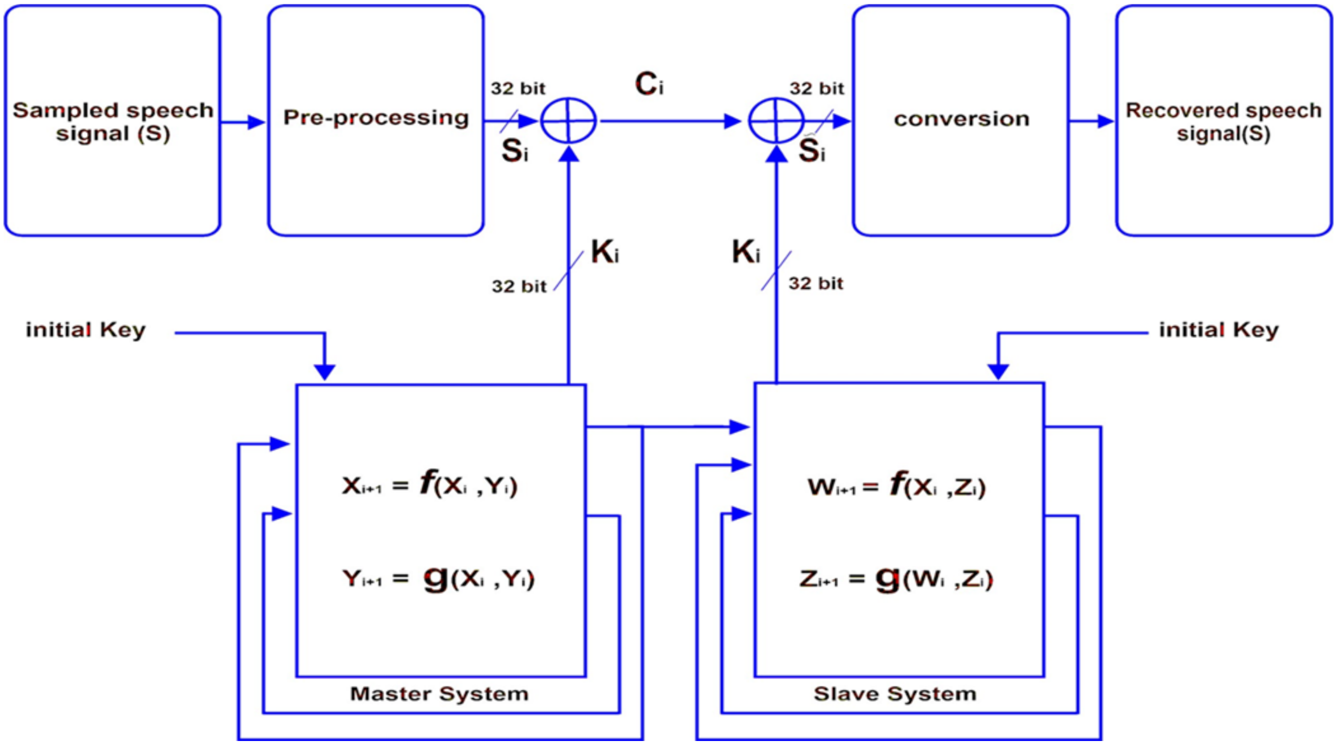


Fig. 20. Block diagram of speech encryption system using FPSCM-SC, adapted from [48].

domain by using the inverse discrete cosine transform (IDCT).

In 2017, Mahmood K. Ibrahem et al [52], introduced a voice-over-internet protocol (VOIP) speech encryption system by using Lorenz chaotic map as a pseudo-random number (PRN) by solving the three-dimensional equations of the Lorenz system using fourth-order Runge Kutta (RK4) and the output is converted to binary with 64 bits. By applying a different test for different voices, the best residual intelligibility measure results are MSE=172313540.6 and SNR= 1.385901466 and the throughput of the system is 1876 bps.

In 2015, Sattar B. Sadkhan et al [53], introduced a new stream cipher system by XORing the voice signal with PRBG that is generated from the random unified chaotic map (RUM) which is modified from the Unified chaotic map by using a uniform distribution to get expanded and other values of the map. To achieve random properties such as (nonlinear, sensitivity to the initial condition, and deterministic) the mod operation is used. Three PRBGs are generated and compared with each other. The results show that the Lyapunov exponents (LE), which is the most important tool that is used to measure the sensitivity to initial condition and the non-chaotic behavior for the non-linear system and which its value must be larger than zero are increased from (0.341353,0.346251,0.389717) in the unified chaotic map to (0.485935,0.481211,0.624137) in the proposed system.

G. Chaotic Systems Based on Hybrid Chaotic Generators systems

In 2013, Mohamed Salah Azzaz, et al [54], suggested an innovative chaotic pseudo-random number generator known as the Hybrid Continuous Chaotic System, or HDCCS. A new method for creating chaos-based cryptosystems can be developed thanks to this chaotic generator. approach is based on the perturbation technique, which uses two different kinds of chaotic systems: discrete (Henon Map, Logistic Map, etc.) and continuous (Lorenz, Chen, Chua, etc.) chaotic systems. Their scheme, the continuous chaotic system perturbs the discrete system and makes the transmitter and receiver synchronized. Chaotic encryption keys with intricate and erratic behaviors are generated by the disrupted discrete system. Real-time wireless chaos-based speech encryption based on the suggested HDCCS has been developed and implemented on FPGA technology in order to verify the efficacy and principle of their scheme encryption. Secure real-time embedded applications in digital cryptosystems heavily depend on the use of a good chaotic generator with desirable dynamical statistical properties and high performance (speed, cost, power, etc.).

In 2020, F.J. Farsana, et al [55], examined a keystream generated by the modified Lorenz-Hyperchaotic system, which is used to substitute audio samples after they have been permuted using a discrete modified Henon map. The authors suggested that in order to eliminate any remaining intelligibility in the transform domain, the audio file be first compressed using the Fast Walsh Hadamard Transform (FWHT). After that, the resultant file is encrypted twice. To reduce the correlation between neighboring samples, a modified discrete Henon map is used in the first phase of the permutation operation. The second phase fills in the silences in the speech conversation by using a modified Lorenz hyperchaotic system for substitution operation. To improve the correlation between encrypted and plaintext text, a mechanism for dynamic keystream generation is also introduced. An altered Henon map and perturbed Lorenz-hyperchaotic system are presented. The original and encrypted data samples' correlation eventually decreased as a result of the modified Henon map's maximizing of the permutation operation over its seed map. The adoption of a hyperchaotic system removed weak chaotic trajectories and smaller chaotic ranges, which are frequently found in chaotic systems with lower dimensions.

In 2014, Saad Najim Al Saad et al [56], proposed a hybrid system, that combines scrambling and stream cipher systems in which four levels of the encryption process are introduced. The time domain of the frame speech signal is permutated using a permutation key generated by the logistic map. The key generation in the first level is the diffusion using random permutation and it is used to scramble the discrete cosine transform (DCT) or separate wavelet transform (DWT) domain of speech signal, which is the second level of the encryption. Third, the mask key generated by using the logistic map is Xored with the speech samples after taking the inverse DCT or DWT. Finally, the speech samples are permutated using Arnold Cat Map.

III. Conclusion

In this paper, different types of techniques used in audio encryption are covered and encryption algorithms have been classified based on traditional symmetric encryption systems such as, (AES), (DES), (RSA), However, the small key space of these systems makes them vulnerable to brute force attacks. Because of the high level of sample repetition and the encryption signal's bandwidth distribution, these encryption algorithms cannot be used to encrypt speech. Regarding this. Numerous encryption algorithms have been developed by researchers to keep up with the advancements in wireless communication technologies. Many researchers have identified the possibility of applying nonlinear dynamics and turbulent behaviors of a chaotic system in encryption. Among the important classifications mentioned in our review of this encryption system is based on advanced chaotic systems, which are divided into two types: the continuous-time system, such as (Lorenz, Chua, and Chen,) and the discrete-time system, such as (Henon, Arnold cat, logistic and Tent map). which has amazing qualities like unpredictable behavior, high security, and high sensitivity to initial conditions and system parameters. We also classified them based on the synchronization method and the implementation method by FPGA or Raspberry Pi. We also studied and classified encryption systems based on Fractional-order systems and based on Hybrid chaotic generator systems.

Conflict of Interest

The authors declare that they have no conflicts of interest.

References

[1] 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.

[2] F. Farsana and K. Gopakumar, "A novel approach for speech encryption: Zaslavsky map as pseudo random number generator," *Procedia computer science*, vol. 93, pp. 816–823, 2016.

[3] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International journal of bifurcation and chaos*, vol. 16, no. 08, pp. 2129–2151, 2006.

[4] Z. Su, G. Zhang, and J. Jiang, "Multimedia security: a survey of chaos-based encryption technology," *Multimedia-A Multidisciplinary Approach to Complex Issues. InTech*, pp. 99–124, 2012.

[5] P. Gautam, M. D. Ansari, and S. K. Sharma, "Enhanced security for electronic health care information using obfuscation and rsa algorithm in cloud computing," *International Journal of Information Security and Privacy (IJISP)*, vol. 13, no. 1, pp. 59–69, 2019.

[6] M. D. Ansari, V. K. Gunjan, and E. Rashid, "On security and data integrity framework for cloud computing using tamper-proofing," in *ICCCE 2020: Proceedings of the 3rd International Conference on Communications and*

Cyber Physical Engineering, pp. 1419–1427, Springer, 2021.

[7] W. Dutta, S. Mitra, and S. Kalaivani, "Audio encryption and decryption algorithm in image format for secured communication," in *2017 International Conference on Inventive Computing and Informatics (ICICI)*, pp. 517–521, IEEE, 2017.

[8] M. Kalpana, K. Ratnavelu, and P. Balasubramaniam, "An audio encryption based on synchronization of robust bam fcnns with time delays," *Multimedia Tools and Applications*, vol. 78, pp. 5969–5988, 2019.

[9] H. Liu, A. Kadir, and Y. Li, "Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys," *Optik*, vol. 127, no. 19, pp. 7431–7438, 2016.

[10] M. M. Rahman, T. K. Saha, and M. A.-A. Bhuiyan, "Implementation of rsa algorithm for speech data encryption and decryption," *IJCSNS International Journal of Computer Science and Network Security*, vol. 12, no. 3, pp. 74–82, 2012.

[11] M. I. Khalil, "Real-time encryption/decryption of audio signal," *International Journal of Computer Network and Information Security*, vol. 8, no. 2, pp. 25–31, 2016.

[12] S. F. Yousif, "Encryption and decryption of audio signal based on rsa algorithn," *International Journal of Engineering Technologies and Management Research*, vol. 5, no. 7, pp. 57–64, 2018.

[13] A. E. Taki_El_Deen, "Implementation of an encryption scheme for voice calls," *International Journal of Computer Applications*, vol. 975, p. 8887.

[14] A.-B. A. Al-Hussein, F. R. Tahir, and O. Boubaker, "Chaos elimination in power system using synergetic control theory," in *2021 18th International Multi-Conference on Systems, Signals & Devices (SSD)*, pp. 340–345, IEEE, 2021.

[15] 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, pp. 1–13, 2021.

[16] A.-B. A. Al-Hussein, "Chaos phenomenon in power systems: A review.," *Iraqi Journal for Electrical & Electronic Engineering*, vol. 17, no. 2, 2021.

[17] 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.

[18] W. Dai, X. Xu, X. Song, and G. Li, "Audio encryption algorithm based on chen memristor chaotic system. symmetry 14 (1): 17," 2022.

[19] S. Fu, X. Cheng, and J. Liu, "Dynamics, circuit design, feedback control of a new hyperchaotic system and its application in audio encryption," *Scientific Reports*, vol. 13, no. 1, p. 19385, 2023.

[20] E. A. Hussein, M. K. Khashan, and A. K. Jawad, "A high security and noise immunity of speech based on double chaotic masking," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 4, pp. 4270–4278, 2020.

[21] S. S. Hreshee, H. N. Abdullah, and A. K. Jawad, "A high security communication system based on chaotic scrambling and chaotic masking," *Int. J. Commun. Antenna Propag*, vol. 8, no. 3, p. 257, 2018.

[22] M. F. Abd Elzaher, M. Shalaby, and S. H. El Ramly, "Securing modern voice communication systems using multilevel chaotic approach," *International Journal of Computer Applications*, vol. 135, no. 9, pp. 17–21, 2016.

[23] E. Avaroğlu, "Pseudorandom number generator based on arnold cat map and statistical analysis," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 25, no. 1, pp. 633–643, 2017.

[24] K. Kordov, "A novel audio encryption algorithm with permutation-substitution architecture," *Electronics*, vol. 8, no. 5, p. 530, 2019.

[25] H. Aziz, S. M. M. Gilani, I. Hussain, A. K. Janjua, and S. Khurram, "A noise-tolerant audio encryption framework designed by the application of s8 symmetric group and chaotic systems," *Mathematical Problems in Engineering*, vol. 2021, pp. 1–15, 2021.

[26] 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.

[27] S. Sheela, K. Suresh, D. Tandur, *et al.*, "A novel audio cryptosystem using chaotic maps and dna encoding," *Journal of Computer Networks and Communications*, vol. 2017, 2017.

[28] 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.

[29] A. Ghasemzadeh and E. Esmaeili, “A novel method in audio message encryption based on a mixture of chaos function,” *International Journal of Speech Technology*, vol. 20, pp. 829–837, 2017.

[30] P. Sathiyamurthi and S. Ramakrishnan, “Speech encryption using chaotic shift keying for secured speech communication,” *EURASIP Journal on Audio, Speech, and Music Processing*, vol. 2017, pp. 1–11, 2017.

[31] M. F. Tolba, W. S. Sayed, A. G. Radwan, and S. K. Abd-El-Hafiz, “Chaos-based hardware speech encryption scheme using modified tent map and bit permutation,” in *2018 7th international conference on modern circuits and systems technologies (MOCAST)*, pp. 1–4, IEEE, 2018.

[32] Z. A. O. Nasri Sulaiman, M. Marhaban, and M. Hamidon, “Design and implementation of fpga-based systems-a review,” *Australian Journal of Basic and Applied Sciences*, vol. 3, no. 4, pp. 3575–3596, 2009.

[33] W. S. Sayed, M. F. Tolba, A. G. Radwan, and S. K. Abd-El-Hafiz, “Fpga realization of a speech encryption system based on a generalized modified chaotic transition map and bit permutation,” *Multimedia Tools and Applications*, vol. 78, pp. 16097–16127, 2019.

[34] 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.

[35] E. Rodríguez-Orozco, E. E. García-Guerrero, E. Inzunza-Gonzalez, O. R. López-Bonilla, A. Flores-Vergara, J. R. Cárdenas-Valdez, and E. Tlelo-Cuautle, “Fpga-based chaotic cryptosystem by using voice recognition as access key,” *Electronics*, vol. 7, no. 12, p. 414, 2018.

[36] 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.

[37] 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.

[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] M. F. Tolba, W. S. Sayed, A. G. Radwan, and S. K. Abd-El-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.

[40] O. Guillén-Fernández, E. Tlelo-Cuautle, L. G. de la Fraga, Y. Sandoval-Ibarra, and J.-C. Nuñez-Perez, “An image encryption scheme synchronizing optimized chaotic systems implemented on raspberry pis,” *Mathematics*, vol. 10, no. 11, p. 1907, 2022.

[41] Y. Chincholkar and S. Ganorkar, “Audio watermarking algorithm implementation using patchwork technique,” in *2019 IEEE 5th International Conference for Convergence in Technology (I2CT)*, pp. 1–5, IEEE, 2019.

[42] B. Paul, “A novel design and implementation of a real-time wireless video and audio transmission device,” *WSEAS Transactions on Computer Research*, vol. 4, pp. 161–172, 2016.

[43] N. R. Babu, M. Kalpana, and P. Balasubramaniam, “A novel audio encryption approach via finite-time synchronization of fractional order hyperchaotic system,” *Multimedia Tools and Applications*, vol. 80, pp. 18043–18067, 2021.

[44] J. Yang, J. Xiong, J. Cen, and W. He, “Finite-time generalized synchronization of non-identical fractional order chaotic systems and its application in speech secure communication,” *Plos one*, vol. 17, no. 3, p. e0263007, 2022.

[45] P. Muthukumar, P. Balasubramaniam, and K. Ratnavelu, “Sliding mode control for generalized robust synchronization of mismatched fractional order dynamical systems and its application to secure transmission of voice messages,” *ISA transactions*, vol. 82, pp. 51–61, 2018.

[46] A. H. Elsafty, M. F. Tolba, L. A. Said, A. H. Madian, and A. G. Radwan, “Enhanced hardware implementation

of a mixed-order nonlinear chaotic system and speech encryption application," *AEU-International Journal of Electronics and Communications*, vol. 125, p. 153347, 2020.

[47] A. A. S. Alghamdi, "Design and implementation of a voice encryption system using fractional-order chaotic maps," *Int. Res. J. Modern. Eng. Technol. Sci*, vol. 3, no. 06, 2021.

[48] Z. M. Alroubaie, M. A. Hashem, and F. S. Hasan, "Fpga design of encryption speech system using synchronized fixed-point chaotic maps based stream ciphers," *International Journal of Engineering and Advanced Technology*, vol. 8, no. 6, pp. 1534–1541, 2019.

[49] A. J. Abd El-Maksoud, A. A. Abd El-Kader, B. G. Hassan, N. G. Rihan, M. F. Tolba, L. A. Said, A. G. Radwan, and M. F. Abu-Elyazeed, "Fpga implementation of sound encryption system based on fractional-order chaotic systems," *Microelectronics Journal*, vol. 90, pp. 323–335, 2019.

[50] F. S. Hasan, "Speech encryption using fixed point chaos based stream cipher (fpc-sc)," *Eng. &Tech. Journal*, vol. 34, no. 11, pp. 2152–2166, 2016.

[51] 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.

[52] M. K. Ibrahem and H. A. Qasim, "Implementation of voip speech encryption system using stream cipher with lorenz map key generator," *International Journal of Scientific and Engineering Research*, vol. 8, no. 7, pp. 533–541, 2017.

[53] 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.

[54] M. S. Azzaz, C. Tanougast, S. Sadoudi, and A. Bouridane, "Synchronized hybrid chaotic generators: Application to real-time wireless speech encryption," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 8, pp. 2035–2047, 2013.

[55] F. Farsana, V. Devi, and K. Gopakumar, "An audio encryption scheme based on fast walsh hadamard transform and mixed chaotic keystreams," *Applied Computing and Informatics*, vol. 19, no. 3/4, pp. 239–264, 2020.

[56] 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.