Improving Voice Communication Security with Chaos-Based Encryption and DCSK

Mohammed Jasim Mohammed[1] and Aqeel Majeed Breesam[2]*

[1]Department of Physics, College of Education, University of Samarra, Salah Al-dein, Iraq
[2]Institute of Medical Technology/ Baghdad, Middle Technical University, Baghdad, Iraq
*Corresponding author: aqeelmajeed@mtu.edu.iq

Abstract: This study proposes a novel voice encryption system that synergistically combines chaos-based encryption with Differential Chaotic Shift Keying (DCSK) modulation to significantly enhance security and communication reliability. Key contributions include: (1) the integration of two distinct chaotic systems (Tinkerbell map and Lorenz system) for robust key generation, ensuring high encryption confidentiality via XOR-based operations. (2) The utilization of DCSK modulation for secure and noise-resilient transmission of the encrypted voice signals over Additive White Gaussian Noise (AWGN) channels, leveraging its inherent robustness to channel impairments.

Simulation results demonstrate the system's effectiveness: encryption yields significant signal transformation (MSE of 0.33, PSNR of 4.5 dB, and entropy of 15.899), while decryption accurately restores the original signal (MSE of 2.1×10^{-10}, PSNR of 96.6 dB). Security analysis confirms high key sensitivity (10^{-15}) and a vast key space (2^{300} for Tinkerbell, 2^{309} for Lorenz), making it highly resistant to brute-force attacks. Furthermore, the DCSK integration notably improves transmission performance, achieving a low Bit Error Rate (BER) (3.6×10^{-3} at SF=24 and SNR=6 dB). This integrated approach offers superior security and noise tolerance compared to existing methods, making it highly suitable for secure real-world voice communication applications.

Keywords: Voice communication security; chaos encryption; DCSK; MSE; PSNR

1. Introduction

A cryptographic algorithm scrambles voice data to make it unintelligible to unauthorized listeners [1]. Voice encryption are used in a diversity of applications, such as secure mobile communication, teleconferencing, and military communications [2]. Many encryption algorithms are using in voice are available, each with its own strengths and weaknesses. Some common voice encryption algorithms include the Advanced Encryption Standard (AES), Rivest Cipher 4 (RC4), and Twofish. The AES is a symmetric block cipher widely used for data encryption [3], [4], [5]. Recently, there has been growing interest in using chaotic signals for voice encryption. Chaotic signals are random and unpredictable, rendering cryptanalysis difficult [6], [7]. Additionally, chaotic signals can be generated using a variety of simple electronic circuits, making them suitable for low-cost and low-power applications using a variety of simple electronic circuits, making them suitable for low-cost and low-power applications.

A. Related Work

In [8], The study assesses the performance of a non-coherent differential chaotic shift keying communication system in an AWGN, focusing on bit error rate and power spectral density, finding comparable security and performance compared to conventional OFDM with index modulation. In [9], The study presents a four-dimensional two-scroll hyperchaotic system with quadratic nonlinearities and conducts bifurcation analysis. An electrical circuit is designed using MultiSim, and the system is implemented in a field-programmable gate array using two numerical approaches. In [10], [11], [12], proposed a speech encryption based on chaotic masking and noise reduction based on different methods and schemes. A speech-encryption technique was developed by combining modified chaotic maps from logistic and

Received: December 5th, 2024. Accepted: June 23rd, 2025
DOI: 10.15676/ijeei.2025.17.2.13

cubic maps, resulting in a confusion and diffusion architecture with superior performance in various chaotic behaviors. In [13], A secure communication system with two layers of encryption for voice signals has been developed, using chaotic masking phases from the Lorenz system and Rossler chaotic flow. In [14], A secure communication system with two degrees of encryption is used to protect speech signals using the Lorenz system and Rossler chaotic flow. The system uses two steps of chaotic masking to minimize noise. Additive white Gaussian noise (AWGN) channels were used for evaluation. Simulation studies show the quality of reconstructed voice signals depends on the signal-to-noise ratio (SNR). In [15], The proposed cryptosystem involves randomly rearrangement of speech components using Hénon state variables, with the index being toggled between them based on the toggle bit. In [16], The FH-OFDM-NR-DCSK system enhances BER and security performance by generating randomness samples and duplicating them P times. It creates a new frequency-hopping pattern based on a chaotic map. Simulations show it outperforms DCSK and FH-OFDM-DCSK, reducing noise variance and improving BER without complexity. In [17], The proposed MIMO communication system uses frequency hopping and orthogonal frequency division multiplexing differential chaotic shift keying (OFDM-DCSK) modulation to enhance security. These modules encrypt and conceal user data, preventing eavesdropping and malicious attacks.

B. Chaotic systems: definitions and key properties

Chaos is a dynamical system that changes extensively over time due to initial conditions and control parameters. Chaos has nonlinearity and periodicity, but early definitions focused on its sensitive dependence on initial conditions. Chaos is sensitive to initial conditions, unpredictable long-term behavior, nonlinear dynamics, periodicity, and strange attractors. [11], [18]. Modeling complex systems like weather, stock markets, and disease spread with chaotic systems is common. Strange attractors, geometric patterns that represent the system's long-term behavior, are common. Strange attractors are hard to spot and don't repeat. Chaotic systems occur in physics, chemistry, biology, mathematics, engineering, and cryptography. They can also generate random numbers due to their unpredictability [10], [19].

B.1. Lorenz system

Edward Lorenz discovered it in 1963 while modeling atmospheric convection, the Lorenz system exhibits all classic chaotic behavior [12], [20]. Mathematicians and physicists have long studied the beautiful and complex Lorenz attractor [10], [21]. The Lorenz system is defined by the following equations:

$$\begin{aligned}\dot{x} &= \sigma(y - x)\\ \dot{y} &= rx - y - xz\\ \dot{z} &= xy - bz\end{aligned} \tag{1}$$

Where the $\dot{x}, \dot{y}$ and $\dot{z}$ are the state vectors, and σ, r, and b are parameters for the Lorenz system [22], the state vectors and the 3D (X, Y, Z) strange attractors are shown in Figure 1.

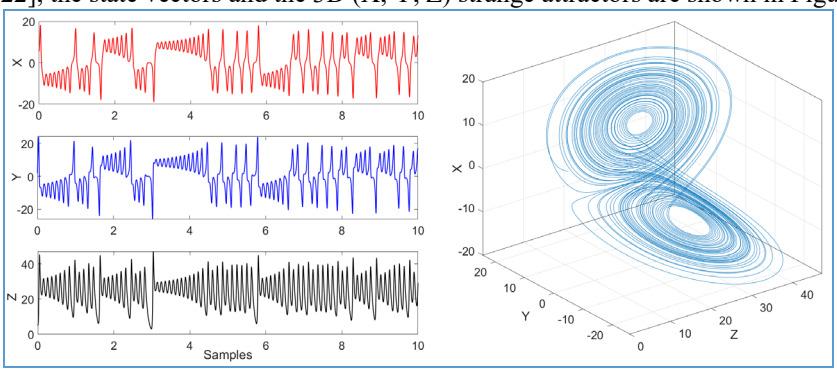

Figure 1. Lorenz System X, Y, and Z time series and $\boldsymbol{3D}$ ($\boldsymbol{X}$, $\boldsymbol{Y}$, $\boldsymbol{Z}$) Strange Attractors

B.2. Tinkerball Map

Mark J. Roberts introduced the discrete-time Tinkerbell chaotic system in 1992. These equations define the system: [23], [24]:

$$x_{n+1} = x_n^2 - y_n^2 + ax_n + by_n$$
$$y_{n+1} = 2x_n y_n + cx_n + dy_n \quad (2)$$

Where x_n & y_n are the values of the system at time n. While a, b, c, and d are constants parameters. The system's simplicity and power make it useful for understanding chaotic behavior and generating random numbers [23], [24]. Figure 2 displays the state vectors and the 2D (X, Y) strange attractors.

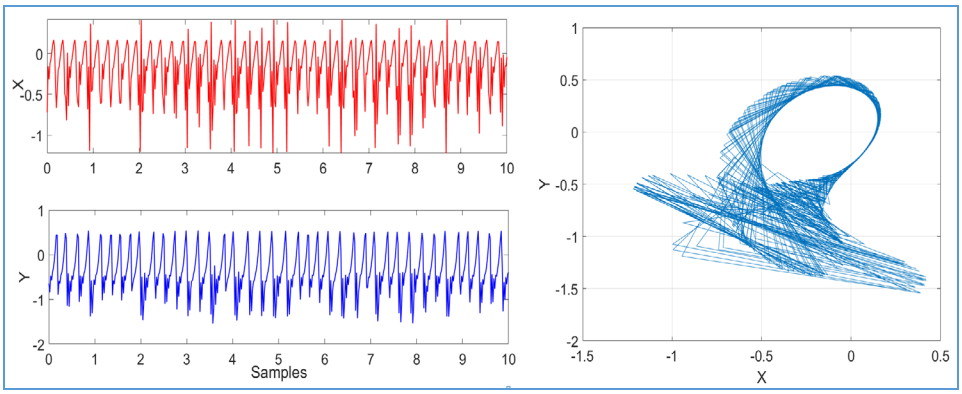

Figure 2. Time Series and (x, y) Strange attractor, of Tinkerbell Map

A common challenge in implementing chaotic systems in digital environments is the potential for digital chaos degradation, where finite precision arithmetic can lead to a loss of chaotic properties and periodicity over time. Researchers have addressed this through various techniques, including the use of high-precision arithmetic [10], [25], design of complex chaotic maps robust to quantization [1], [26], or hybrid analog-digital implementations. In our proposed system, while digital implementation is utilized, the combination of two distinct chaotic maps (Lorenz and Tinkerbell) and their careful parameter selection, along with the inherent robustness provided by DCSK modulation, helps mitigate such degradation effects, ensuring the sustained chaotic behavior essential for cryptographic strength.

C. Novelty and contributions

While traditional encryption algorithms (e.g., AES, RSA) are robust for general data, their computational overhead can limit real-time voice applications, and they often do not inherently address transmission challenges in noisy channels. Chaotic systems, conversely, offer properties like high sensitivity to initial conditions and pseudo-random behavior, making them attractive for lightweight, high-speed encryption tailored for multimedia. However, standalone chaotic encryption schemes often lack inherent robustness against channel impairments. This study bridges this gap. Chaos-based encryption and DCSK modulation have individually demonstrated significant potential for secure communication, their synergistic integration for voice encryption, as proposed in this study, represents a novel approach addressing the combined challenges of security and transmission robustness. The primary contributions of this research are summarized as follows:

- Development of a comprehensive voice encryption system that uniquely combines chaotic encryption (utilizing both Lorenz and Tinkerbell maps for enhanced key diversity and unpredictability) with DCSK modulation, ensuring both high confidentiality and robust transmission over noisy channels.

- Demonstrating superior security through rigorous analysis of key sensitivity and a significantly large key space, providing strong resistance against brute-force and differential attacks.
- Quantifying the performance benefits of integrating DCSK, showing significantly lower Bit Error Rates (BER) across various Signal-to-Noise Ratios (SNRs) and spreading factors, which is critical for reliable voice communication in real-world noisy environments.
- Providing simulation-based evidence that the proposed integrated system offers competitive or superior performance in terms of security and noise tolerance compared to standalone chaotic encryption schemes or conventional modulation techniques found in existing literature.

2. Proposed System Model Architecture

The Differential Chaotic Shift Keying (DCSK) modulation scheme is an integral component of the proposed secure voice communication system, serving a dual purpose: robust transmission of the encrypted voice signal over noisy channels and an additional layer of security due to its inherent chaotic nature. After the voice signal undergoes chaos-based XOR encryption, the resulting encrypted bitstream is modulated using DCSK. DCSK utilizes chaotic signals as carriers, which makes the transmitted signal highly resilient to additive noise and multipath fading, commonly encountered in wireless communication environments. This robust modulation ensures that the securely encrypted voice data can be reliably transmitted and recovered at the receiver, even under adverse channel conditions. Furthermore, the chaotic properties of DCSK carriers contribute to the overall unpredictability of the transmitted signal, thereby implicitly enhancing the system's security profile. The extensive explanation on DCSK and spreading factor (SF) is thus warranted to detail this critical aspect of the system's design and its contribution to the system's overall performance and resilience. Figure 3 shows a block diagram of an audio encryption system that uses a chaotic XOR operation and then sends the encrypted audio over an AWGN channel.

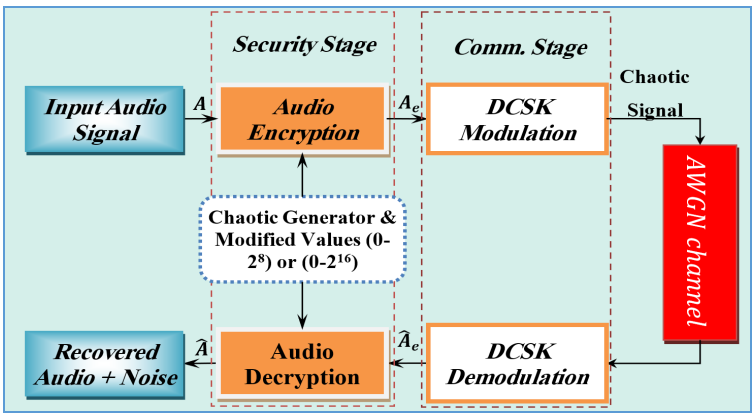

Figure 3. The General Block Diagram of the Proposed System Model

The security stage encrypts audio input with chaos and XOR bitwise. DCSK digital modulation transmits data using chaotic signals in the Communication Stage. We use the AWGN Channel to secure data transmission by modeling noise in communication channels with a random and Gaussian distribution.

A. Random Number Generator by Chaotic Signal

Following are the steps that are involved in this process, which converts the chaotic signal into a random integer number:

- Taking the chaotic value and multiplying it by the highest possible number (for example, 10^8).
- When you have the result, round it up to the nearest whole number.
- Apply the mod operation on the number to 2^{16}. (The result will be between 0 and 65535), as shown in the equation:

$$CRIN = \text{round}(\text{ChaoticNum} * 10^8) \,\%\, 2^n \quad (3)$$

Where $CRIN$ is a Chaotic Random Integer Number, n is 8 or 16 bits. In Equation (3), the '%' symbol denotes the modulo operation. This operation returns the remainder of the division of one number by another. For example, 'a % b' calculates the remainder when 'a' is divided by 'b'.

- The encryption and decryption process are based on XOR bitwise between chaotic random integer numbers and audio samples.

B. Differential Chaotic Shift Key (DCSK)

DCSK is a digital modulation technique that uses chaos theory to enhance communication systems. It uses a chaotic signal as the carrier wave, encoding data by introducing small changes. DCSK is resistant to noise and interference, unlike traditional methods like ASK or FSK, which directly encode data onto the carrier wave. Figure 3 displays the basic diagram of DCSK.

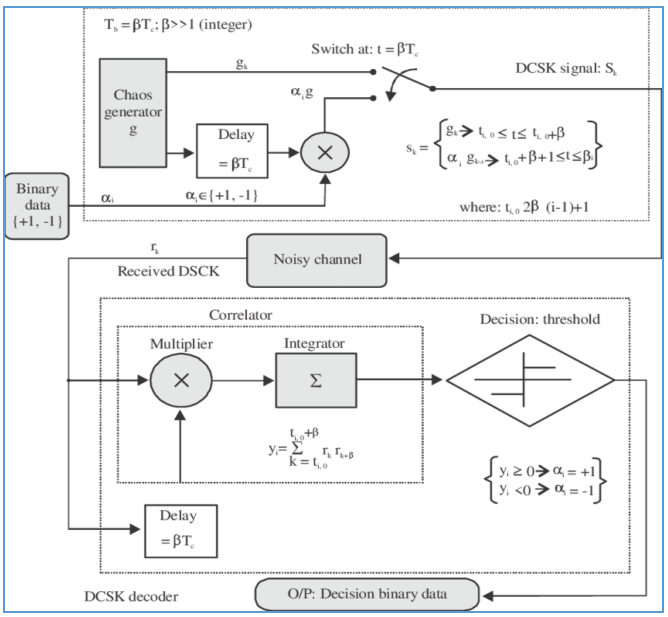

Figure 4. DCSK Basics Diagram

DCSK is a communication system that generates and modulates a chaotic signal with information, using systems like Logistic Map to create complex waveforms and differentially encode data. At the receiver end, we perform demodulation to extract differential changes and recover the original data, ensuring it remains robust against noise. Figure 5 illustrates the modulating bits, modulation signal, and recovery signals in the receiver.

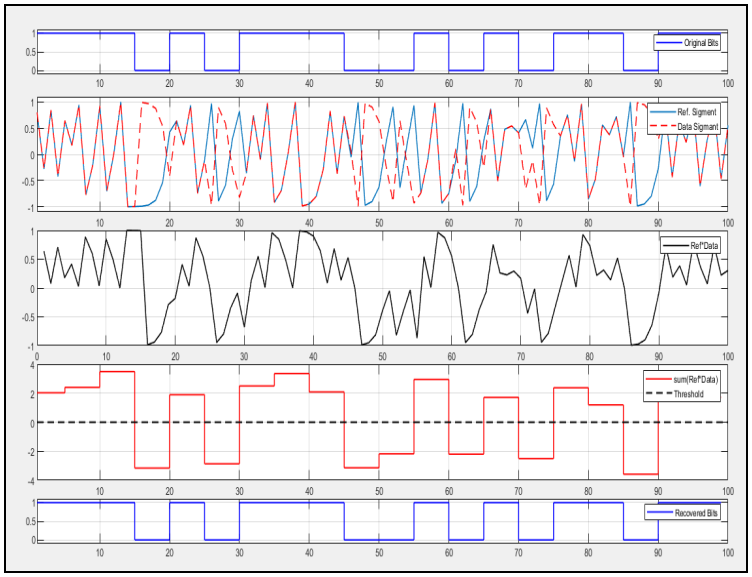

Figure 5. DCSK Modulation Signals: Original Random Bits, Reference and Data Segments, and Recovered Bits

3. Evaluation Metrics For Voice Signal Quality

Two types of testing will evaluate the proposed system performance: numeric and graphical measurements (Fast Fourier Transform plot (FFT plot), The Histogram Plot, The Correlation Plot). These measures are defined as follows:

A. The Correlation Coefficients (CORR)

$$\mathrm{CORR} = \frac{\sum_{i=1}^{m}(X_i - E(X))(Y_i - E(Y))}{\sqrt{\sum_{i=1}^{m}((X_i - E(X)))^2}\sqrt{\sum_{i=1}^{m}((Y_i - E(Y)))^2}} \quad (4)$$

X & Y are the original, recovered, or encrypted audio signals [27].

And $E(X) = \frac{\sum_{i=1}^{m} X}{m}$ $E(Y) = \frac{\sum_{i=1}^{m} Y}{m}$

B. Mean Square Error (MSE)

$$\mathrm{MSE} = \frac{\sum_{i=1}^{m}(x_i - y_i)^2}{m} \quad (5)$$

Where m is an equal length of the original voice signal. x & y original and recovered or encrypted voice signal [26], [28].

C. Peak Signal-to-Noise Ratio (PSNR)

$$\mathrm{PSNR\,(dB)} = 10 * \log_{10}\left[\frac{(\mathrm{NBits}^2 - 1)^2}{\mathrm{MSE}}\right] \quad (6)$$

NBits is the Number of Bits used for converting analog voice signals to digital. In this paper, NBits typically equals 8 or 16 bits for each sample [29], [30].

D. Entropy

$$E = \sum_{i=0}^{2^n-1} \left[p(i) * \log_2 \left(\frac{1}{p(i)} \right) \right] \quad (7)$$

In encryption, the entropy should be closs to 8 for 256 levels or 16 for 65536 levels, confirming predictability and resisting entropy attacks [31] .

E. Bit Error Rate (BER)

$$BER = \frac{\text{Incorrectly Received Bits}}{\text{All Transmitted Bits}} \quad (8)$$

Bit error rate (BER) is a digital communication system's error rate, indicating the ratio of incorrectly received bits to total transmitted bits. A lower BER indicates better quality, while a BER of less than 10^{-6} is generally acceptable. Factors affecting BER include noise, interference, distortion, and attenuation [32].

F. Key Space and Key Sensitivity

This section details the evaluation of the proposed system's cryptographic strength, specifically focusing on its key space and key sensitivity. These metrics are crucial in assessing the system's resistance against various cryptographic attacks [1], [26].

F.1. Key Sensitivity

The security of a chaotic encryption system is significantly dependent on its key space, which represents the total number of possible distinct keys. A larger key space makes brute-force attacks computationally infeasible [1], [26].

F.2. Key Sensitivity Calculation

Key sensitivity measures a cipher's sensitivity to changes in the key. High sensitivity indicates that a small change in the key results in a large change in the ciphertext, while low sensitivity indicates that a small change in the key results in a small change in the ciphertext [1], [26].

$$\text{Key Space} = \prod_{i=1}^{d} \frac{1}{S} * R(i) \quad (9)$$

Where: d: Number of Parameters and initial values for a chaotic system. S: Key Sensitivity for a chaotic system. R: The range between the most significant and most minor value for any parameter or initial value that the system remains within the limits of chaos. To facilitate the solution, we assume that the R is 1, although it is much more than 1 in most cases. In this case, the number of keys will be greater than the number now calculated.

4. Simulation Results and Performance Evaluation

The study evaluates a voice encryption system using various metrics, including correlation between voice signal samples, bandwidth spread, mean squared error, signal-to-noise ratio, and bit error rate. The simulation was conducted on a laptop with an Intel Core i7 12700H processor, 3.1 GHz CPU speed, 32 GB RAM, MATLAB language (R2022a), and Windows 11 operating system. The results show the system effectively protects against unauthorized access to encrypted voice signals. Four voice signals with difference frequency sampling (FS), time length, and Entropy are used to evaluate the performance of the proposed systems, as shown in Figure 6.

A. Encryption Results

In this section, the results of voice encryption using various systems of chaos (Tinkerbell Map and Lorenz System) will be presented, and the performance of each of them in the encryption process will be evaluated. This paper will present the numerical and graphic results of each chaotic system. The next section then discusses the encryption and decryption results.

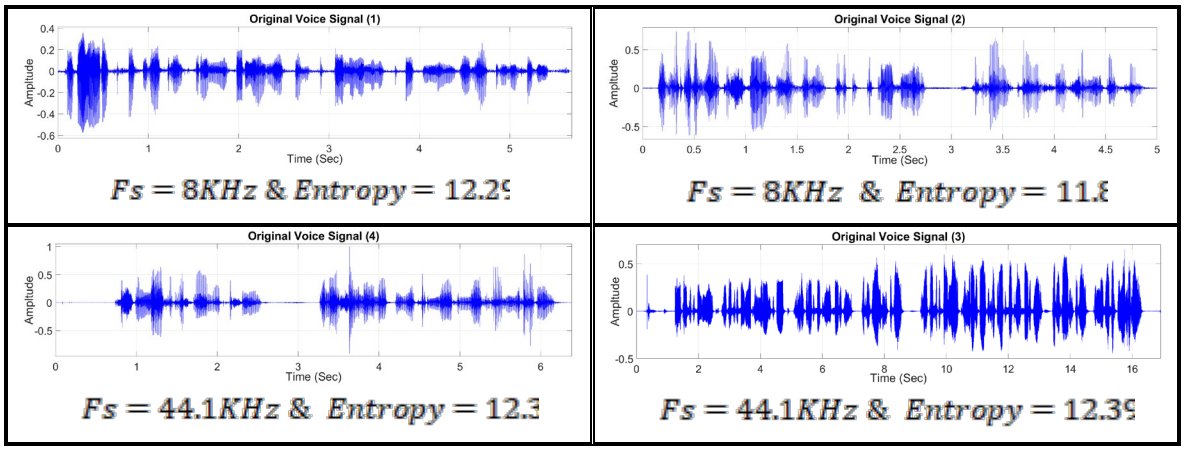

Figure 6. The Properties of the Original Voice Signals

Table 1. Simulation Results of Voice Encryption Signals Based on Tinkerbell Map

Voice Signal	MSE	PSNR (dB)	Correlation	Entropy	Delay (Sec)
#1	0.33820	4.7083	0.00536	14.8676	0.0072
#2	0.34215	4.6578	0.00588	14.7414	0.0042
#3	0.33867	4.7022	0.00099	15.9355	0.0269
#4	0.33939	4.6931	0.00127	15.8215	0.0118

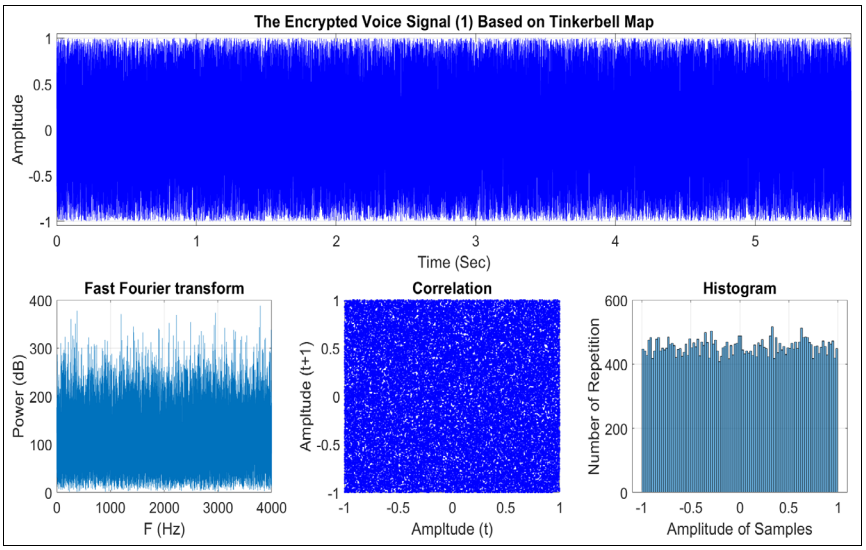

Figure 7. Encryption Results of Voice Signal (1) Based on Tinkerbell Map

Table 2 Simulation Results of Voice Encryption Signals Based on Lorenz System

Voice Signal	MSE	PSNR (dB)	Correlation	Entropy	Delay (Sec)
#1	0.33811	4.7095	0.00595	14.8652	0.0046
#2	0.34286	4.6489	0.00118	14.7487	0.0058
#3	0.33879	4.7008	0.00011	15.9357	0.0369
#4	0.33916	4.6959	0.00134	15.8211	0.0165

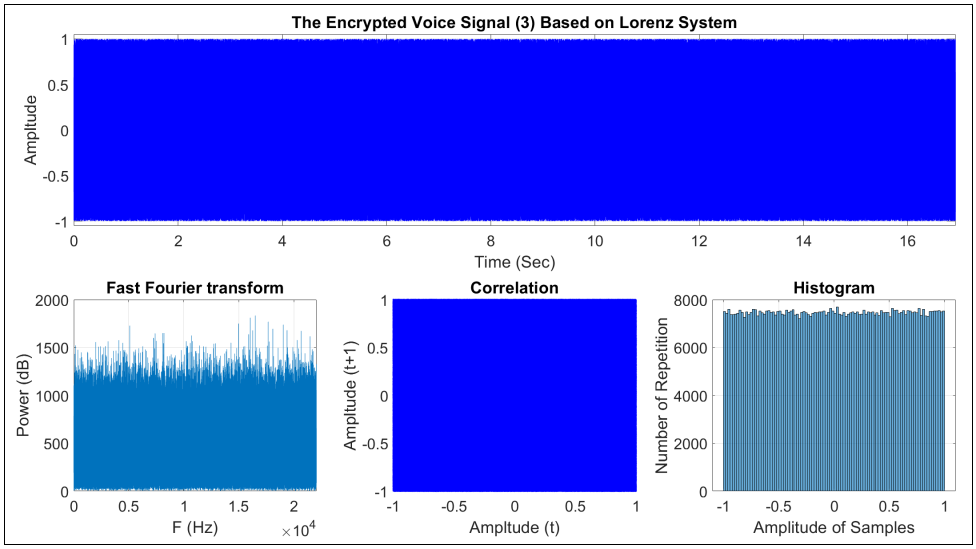

Figure 8. Encryption Results of Voice Signal (3) Based on Lorenz System

The simulation results of voice encryption demonstrate their efficacy in safeguarding voice data against unauthorized interception and eavesdropping attempts. The encryption process yielded signals that exhibited complete unrecognizability, attesting to the effectiveness of the encryption methodology. The encrypted signals exhibit high distortion, spectral complexity, low correlation, high entropy, and minimal time delay, rendering them impervious to decryption attempts and suitable for real-time voice communication security.

B. Decryotion Results

Table 3 Simulation Results of Decryption Voice Signals Based on Tinkerbell Map

Voice Signal	MSE	PSNR (dB)	Correlation	Entropy	Delay (Sec)
#1	$2.1625*10\text{-}^{10}$	96.650	1	12.2406	0.0068
#2	$2.1181*10\text{-}^{10}$	96.741	1	11.8904	0.0073
#3	$2.1461*10\text{-}^{10}$	96.683	1	12.39	0.0394
#4	$2.1469*10\text{-}^{10}$	96.682	1	12.2932	0.0191

Table 4. Simulation Results of Decryption Voice Signals Based on Lorenz System

Voice Signal	MSE	PSNR (dB)	Correlation	Entropy	Delay (Sec)
#1	$2.1625*10\text{-}^{10}$	96.659	1	12.2406	0.0083
#2	$2.1181*10\text{-}^{10}$	96.741	1	11.8904	0.0078
#3	$2.1461*10\text{-}^{10}$	96.683	1	12.39	0.0437
#4	$2.1469*10\text{-}^{10}$	96.682	1	12.2932	0.0203

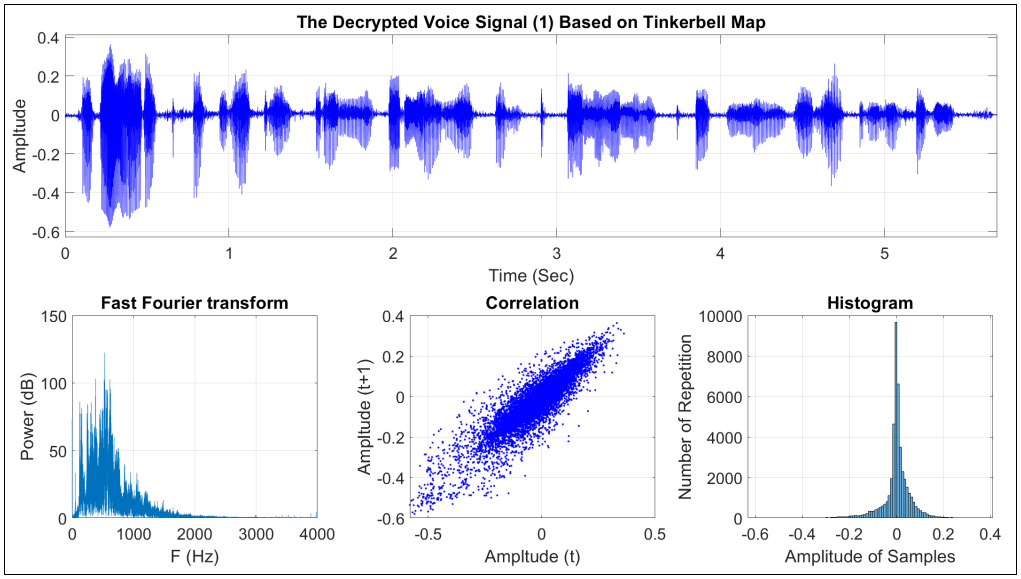

Figure 9. Decryption Results of Voice Signal (1) Based on Tinkerbell Map

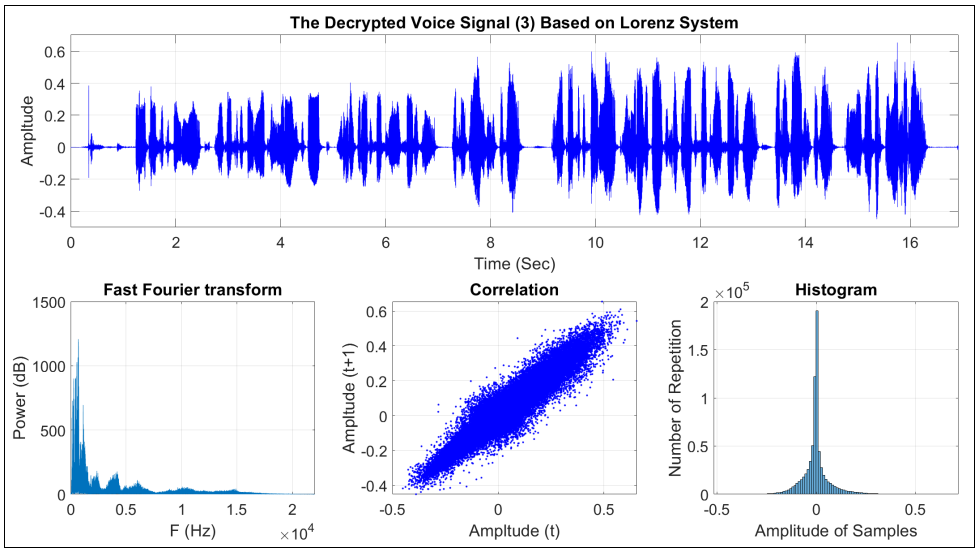

Figure 10. Decryption Results of Voice Signal (3) Based on Lorenz System

The previous results showed that the decryption algorithm accurately recovered the original voice signal from the encrypted signal without distortion or noise and a very small decryption delay.

C. Cryptanalysis of the Proposed System (Key Sensitivity and Key Space)

C.1. Key Sensetivity Analysis

The proposed encryption algorithm, based on chaotic signals, is highly sensitive to changes in the initial conditions, meaning that even a small change in the key will cause a significant change in the ciphertext, as shown in the following Table 5.

Table 5 Simulation Results for Key Sensitivity Analysis during Decryption

Chaotic Systems	Voice Signal	Changing	MSE	PSNR (dB)	Corr.	Entropy
Tinkerbell Map	#2	$y_1 = y_1 \pm 10^{-15}$	0.3416	4.6646	0.0025	14.7388
Tinkerbell Map	#4	$a = a \pm 10^{-15}$	0.3399	4.6861	0.00172	15.8205
Lorenz System	#1	$b = b \pm 10^{-15}$	0.3288	4.8312	0.00273	14.8605
Lorenz System	#2	$z_1 = z_1 \pm 10^{-15}$	0.3311	4.8007	0.0031	14.6963
Lorenz System	#3	$r = r \pm 10^{-15}$	0.3387	4.7017	0.0036	16.9354
Lorenz System	#4	$x_1 = x_1 \pm 10^{-15}$	0.3386	4.7029	0.00097	15.9264

Table 5 demonstrate that when any parameter or initial condition of any of the three chaotic systems changes by $\pm 10^{-15}$ or above, the decryption process remains interrupted (the voice signal's decryption remains fully encrypted); this indicates that the encryption algorithm is highly sensitive to changes in the key. It is resistant to both brute-force attacks and attacks that exploit the sensitivity of chaotic systems to changes in their initial conditions.

C.2 Key Space Calculation

In this section, we calculate the key space of the proposed system based on the precision of the chaotic system parameters.

Case 1: Key space of Tinkerbell Map:

Tinkerbell Map has two initial values (x and y) and four parameters (a, b, c, and d).

$$Key(\text{Tinkerbell Map}) \approx \prod_{i=1}^{6} \frac{1}{10^{-15}} = \left(\frac{1}{10^{-15}}\right)^{6} = 10^{90} \quad (10)$$

$$Key(\text{Tinkerbell Map}) \approx 2^{299} \approx 299\ bits \quad (11)$$

Case 2: Key space of the Lorenz System:

Lorenz system also has the same dimensions as the Tinkerbell map, but Lorenz has three initial values (x, y, and z) and three parameters (σ, r, and b).

$$Key(Lorenz\ System) = \mathrm{R}_x * R_y * R_z * 10^{90} \quad (12)$$

Where R_x, R_y, R_z range of the Lorenz system's x, y, and z state vectors, the values of R_x, R_y, R_z:

$$\mathrm{R}_x \approx (-18\ to\ 18) = 36, \mathrm{R}_y \approx (-18\ to\ 18) = 36\ and\ \mathrm{R}_z \approx (8\ to\ 42) = 34$$

$$Key(Lorenz\ System) \approx 10^{93} \approx 2^{309} \approx 309\ \text{bits} \quad (13)$$

D. Comparative analysis with existing works

Comparing the proposed system's performance and security to chaotic voice encryption and secure communication works highlights its advances. This section highlights the strengths of our integrated approach, as direct one-to-one comparisons can be difficult due to different experimental setups and measurements across research. Table 6 compares the proposed system's key space size in bits to many relevant papers.

Table 6 Comparative analysis of the proposed system with other encryption schemes in terms of performance metrics and key-space

Ref	MSE	PSNR (dB)	Correlation	Entropy	Key-space
[19]	-	-	-	15.113	212 Bits
[10]	0.1521	-	0.00812	-	215 Bits
[33]	-	-	-	15.142	266 Bits
[34]	0.33142	5.1254	0.00952	15.323	328 Bits
Our Tinkerbell	0.33939	4.6931	0.00127	15.8215	300 Bits
Our Lorenz	0.33916	4.6959	0.00134	15.8211	309 Bits

Table 6 demonstrates that the suggested method utilizes key space 300 for Tinkerbell map and 309 for Lorenz system, exceeding that of the majority of relevant literature. The enlarged key space improves system security by making brute-force attacks more difficult for potential adversaries.

E. Simulation Results of DCSK

To test DCSK's performance, a voice signal was transmitted using DCSK modulation with different spreading factors over an additive white Gaussian noise channel with different signal-to-noise ratios (SNRs).

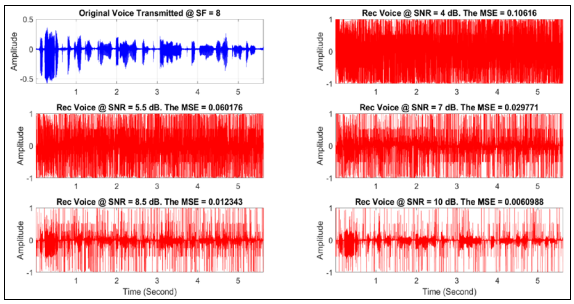

Figure 11. Transmission of voice signals in DCSK at SF=8 and multiple SNRs

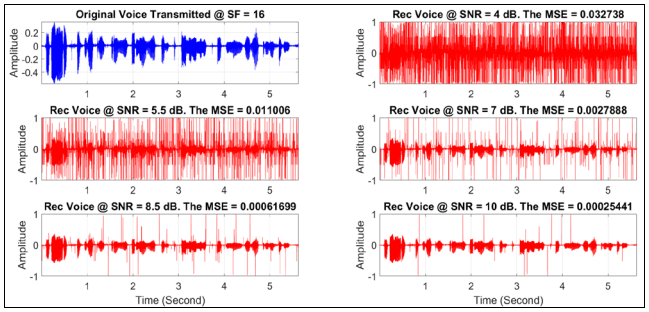

Figure 12. Transmission of voice signals in DCSK at SF=16 and multiple SNRs

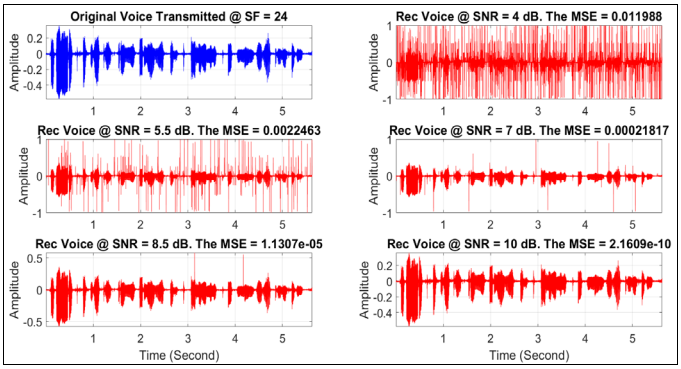

Figure 13. Transmission of voice signals in DCSK at SF=24 and multiple SNRs

The DCSK system's performance improves at a spreading factor (SF) of 8, which is not enough to provide adequate protection against noise (See Figure 11). A higher SF is needed to achieve better performance. The DCSK signal becomes more robust to noise at a spreading factor (SF) of 16, but this reduces bandwidth efficiency. The choice of SF depends on the system's specific requirements. The simulation results show that at an SNR of 4 dB, the received voice signal is noisy and difficult to understand, but the main features are still recognizable. At an SNR of 5.5 dB, the signal is less noisy and easier to understand, but still contains some noise. At the SNR value is 7 dB, the received voice signal have a good quality and easy to understand. And at SNR is equal 8.5 dB and 10 dB, the received voice signal have excellent quality and indistinguishable from the original voice signal. The bit error rate (BER) results for The DCSK at various SF and SNR values are shown in Figure 14.

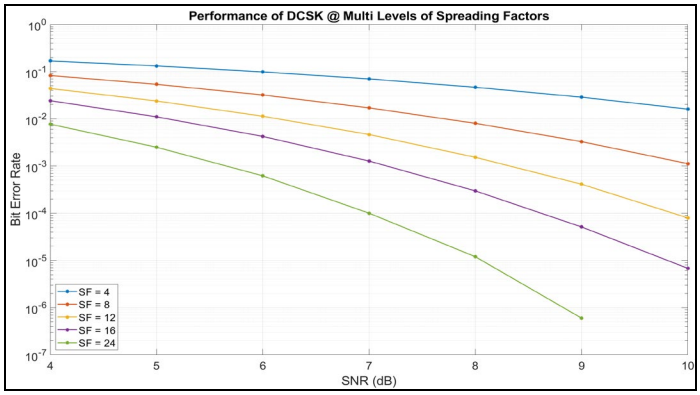

Figure 14. Bit Error Rate (BER) Performance of DCSK at Various Spreading Factors (SFs) and Signal-to-Noise Ratios (SNRs)

Figure 14 shows that at 6 dB SNR, BER values range from 0.1 at SF = 4, $2.3*10^{-2}$ at SF = 8, $1.001*10^{-2}$ at SF = 12, $4*10^{-3}$ at SF = 16, and $3.6*10^{-3}$ at SF = 24. When SF rises, DCSK performance improves at the same SNR. Also, DCSK BER improves with SNR; at SF=16, SNR=4 dB BER is $2.5*10^{-2}$, but SNR=10 dB is $7.3*10^{-6}$. The DCSK performs poorly with low SF or SNR. Higher SF or SNR improves system performance. With increasing SF and SNR, DCSK performance improves according to BER. The BER for SF=24 is $7.5*10^{-3}$, while the BER for SF=4 is 10^{-1} at SNR of 4 dB. This means that the DCSK system with SF=24 can transmit data with a much lower error rate. System bandwidth efficiency decreases with higher spreading factors. DCSK system spreading factors must balance noise robustness and bandwidth efficiency.

5. Conclusion

Without distortion or noise, the encryption algorithm can recover the original voice signal from the encrypted signal. The encrypted and decrypted voice signals have a very small delay compared to the original voice signal, providing real-time voice communications. The encryption algorithm scrambles voice data to make it unintelligible to eavesdroppers while recovering the original voice signal without distortion or noise during reception. Eavesdroppers had trouble intercepting and decrypting encrypted voice signals because the FFT plot spans many frequencies. Uniformly distributed histograms are hard to analyze and decrypt without the encryption key. The encrypted voice signal does not correlate with the original voice signal, making it difficult to recover without the encryption key. Due to the chaotic signal, the proposed encryption algorithm has high key sensitivity and a large key space. This makes brute-force attacks difficult. However, cryptanalysis attacks can still target the algorithm. The system's performance improves with increasing spreading factor or SNR. The proposed system is suitable for real-world voice signal transmission in noisy wireless environments, enhancing data integrity and noise resistance.

The proposed integrated system offers a robust and secure solution for voice communication. The synergy between chaos-based encryption and DCSK modulation effectively addresses the dual challenges of data confidentiality and reliable transmission in noisy environments. Looking forward, the demonstrated strengths of this approach, particularly its high security and noise resilience, make it highly promising for a wide array of practical applications beyond just voice, including secure multimedia communication (e.g., video conferencing), encrypted data streaming, and potentially even secure sensor networks or military communications where data integrity and confidentiality are paramount.

6. References

[1]. A. K. Jawad, G. Karimi, and M. Radmalekshahi, “A Novel Digital Audio Encryption Algorithm Using Three Hyperchaotic Rabinovich System Generators,” *ARO-The Sci. J. Koya Univ.*, vol. XII, no. 2, pp. 234–245, 2024, doi: 10.14500/aro.11869.

[2]. Y. Alemami, M. A. Mohamed, S. Atiewi, and M. Mamat, “Speech encryption by multiple chaotic maps with fast fourier transform,” *Int. J. Electr. Comput. Eng.*, vol. 10, no. 6, pp. 5658–5664, 2020, doi: 10.11591/ijece.v10i6.pp5658-5664.

[3]. Z. Rahman, X. Yi, M. Billah, M. Sumi, and A. Anwar, “Enhancing AES Using Chaos and Logistic Map-Based Key Generation Technique for Securing IoT-Based Smart Home,” *Electron.*, vol. 11, no. 7, 2022, doi: 10.3390/electronics11071083.

[4]. E. Mosa, N. W. Messiha, O. Zahran, and F. E. Abd El-Samie, “Encryption of speech signal with multiple secret keys in time and transform domains,” *Int. J. Speech Technol.*, vol. 13, no. 4, pp. 231–242, 2010, doi: 10.1007/s10772-010-9081-1.

[5]. M. A. Alrammahi and H. Kaur, “Development of Advanced Encryption Standard (AES) Cryptography Algorithm for Wi-Fi Security Protocol,” *Int. J. Adv. Res. Comput. Sci.*, vol. 5, no. 3, pp. 62–67, 2014.

[6]. K. Ganesan, R. Muthukumar, and K. Murali, “Look-up table based chaotic encryption of audio files,” *IEEE Asia-Pacific Conf. Circuits Syst. Proceedings, APCCAS*, vol. 00, pp. 1951–1954, 2006, doi: 10.1109/APCCAS.2006.342243.

[7]. M. Samimi, M. H. Majidi, and S. Khorashadizadeh, “Secure communication based on chaos synchronization using brain emotional learning,” ELSEVIER, AEU - *Int. J. Electron. Commun.*, vol. 127, no. September, p. 153424, 2020, doi: 10.1016/j.aeue.2020.153424.

[8]. S. H. Hussien and H. A. Abdullah, “Chaotic-based Orthogonal Frequency Division Multiplexing with Index Modulation,” *Technology*, p. 33, 2022.

[9]. S. Vaidyanathan, A. Sambas, E. Tlelo-Cuautle, C. F. Bermudez-Marquez, K. Benkouider, and S. A. Safaan, “A New Hyperchaotic Two-Scroll System: Bifurcation Study, Multistability, Circuit Simulation, and FPGA Realization,” Discret. Dyn. Nat. Soc. Hindawi, vol. 2022, no. 1, pp. 1–17, 2022, doi: 10.1155/2022/6604684.

[10]. H. N. Abdullah, S. S. Hreshee, G. Karimi, and A. K. Jawad, “Performance Improvement of Chaotic Masking System Using Power Control Method,” in *International Middle Eastern Simulation and Modelling Conference* 2022, MESM 2022, 2022, pp. 19–23.

[11]. H. N. Abdullah, S. S. Hreshee, and A. K. Jawad, “Design of Efficient noise reduction scheme for secure speech masked by chaotic signals,” *J. Am. Sci.*, vol. 11, no. 7, pp. 49–55, 2015.

[12]. H. N. Abdullah, S. S. Hreshee, and A. K. Jawad, “Noise Reduction of Chaotic Masking System using Repetition Method,” 2016. [Online]. Available: https://www.researchgate.net/publication/291356303

[13]. E. A. R. Hussein, M. K. Khashan, and A. K. Jawad, “A high security and noise immunity of speech based on double chaotic masking,” *Int. J. Electr. Comput. Eng.*, vol. 10, no. 4, 2020, doi: 10.11591/ijece.v10i4.pp4270-4278.

[14]. S. Hashemi, M. A. Pourmina, S. Mobayen, and M. R. Alagheband, “Multiuser wireless speech encryption using synchronized chaotic systems,” Springer, *Int. J. Speech Technol.*, vol. 24, no. 3, pp. 651–663, 2021, doi: 10.1007/s10772-021-09821-3.

[15]. F. S. Hasan, M. F. Mosleh, and A. H. Abdulhameed, “FPGA implementation of LDPC soft-decision decoders based DCSK for spread spectrum applications,” *Int. J. Electr. Comput. Eng.*, vol. 11, no. 6, pp. 4794–4809, 2021, doi: 10.11591/ijece.v11i6.pp4794-4809.

[16]. M. L. Mohammed and F. S. Hasan, “Design and performance analysis of frequency hopping OFDM based noise reduction DCSK system,” *Bull. Electr. Eng. Informatics*, vol. 11, no. 3, pp. 1438–1448, 2022, doi: 10.11591/eei.v11i3.3836.

[17]. W. Qiu, Y. Yang, Y. Feng, L. Zhang, and Z. Wu, “Secure Mimo Communication System with Frequency Hopping Aided OFDM-DCSK Modulation,” *Electron.*, vol. 11, no. 19, pp. 1–14, 2022, doi: 10.3390/electronics11193029.

[18]. Ameer K. Jawad, Wa’il a. H. Hadi, and Hyayder F. Y. Husseain, “Enhancement of Image Transmission Using Chaotic Interleaver over Wireless Sensor Network,” 2016. [Online]. Available: www.ijntr.org

[19]. A. Mahdi, A. K. Jawad, S. S. Hreshee, A. Mahdi, and A. K. Jawad, “Digital Chaotic Scrambling of Voice Based on Duffing Map,” *Commun. Eng. J.*, vol. 1, no. 2, pp. 16–21, 2016, doi: 10.11648/j.cej.20160102.11.

[20]. 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, pp. 257–264, 2018, doi: 10.15866/irecap.v8i3.13541.

[21]. M. M. Sepantaie, V. Bui, E. El-Araby, A. M. Sepantaie, G. Nehmatallah, and N. M. Namazi, "Secure communication systems using synchronized Lorenz strange attractor on reconfigurable hardware," in *Modeling and Simulation for Defense Systems and Applications* X, 2015, p. 947802. doi: 10.1117/12.2177589.

[22]. X. Li, H. Yu, H. Zhang, X. Jin, H. Sun, and J. Liu, "Video encryption based on hyperchaotic system," *Multimed. Tools Appl.*, vol. 79, no. 33–34, pp. 23995–24011, 2020, doi: 10.1007/s11042-020-09200-1.

[23]. A. Dinu and M. Frunzete, "Singularity, Observability and Statistical Independence in the Context of Chaotic Systems," *Mathematics*, vol. 11, no. 2, p. 305, 2023, doi: 10.3390/math11020305.

[24]. S. Bensid Ahmed, A. Ouannas, M. Al Horani, and G. Grassi, "The Discrete Fractional Variable-Order Tinkerbell Map: Chaos, 0–1 Test, and Entropy," *Mathematics*, vol. 10, no. 17, pp. 0–1, 2022, doi: 10.3390/math10173173.

[25]. M. Khalid, E. A. E. A. R. Hussein, Ameer K. Jawad, and A. K. Jawad, "Digital Image Encryption Based on Random Seguences and XOR Operation," *J. Eng. Appl. Sci*., vol. 14, no. 8, pp. 10331–10334, 2019.

[26]. Ameer k. Jawad; Gholamreza Karimi; Mazdak Radmalekshahi, "A Novel Lorenz-Rossler-Chan (LRC) Algorithm for Efficient Chaos-Based Voice Encryption," in 2024 3rd *International Conference on Advances in Engineering Science and Technology (AEST), IEEE*, 2024, pp. 1–6. doi: 10.1109/AEST63017.2024.10959812.

[27]. W. A. Al-Musawi, M. A. A. Al-Ibadi, and W. A. Wali, "Artificial intelligence techniques for encrypt images based on the chaotic system implemented on field-programmable gate array," *IAES Int. J. Artif. Intell.*, vol. 12, no. 1, pp. 347–356, 2023, doi: 10.11591/ijai.v12.i1.pp347-356.

[28]. A. M. Breesam, Y. M. Hussein, and M. J. Mohammed, "Fractal compression of digital image processing," in *AIP Conference Proceedings, AIP Publishing*, 2024.

[29]. P. Rashmi, M. C. Supriya, and Q. Hua, "Enhanced lorenz-chaotic encryption method for partial medical image encryption and data hiding in big data healthcare," *Secur. Commun. Networks,* vol. 2022, pp. 1–9, 2022.

[30]. A. M. Breesam, A. M. Zalzala, and E. Najjar, "Walsh Transform-based Image Compression for Less Memory Usage and High Speed Transfer," *Majlesi J. Electr. Eng.*, vol. 18, no. 1, 2024.

[31]. U. Erkan, A. Toktas, and Q. Lai, "2D hyperchaotic system based on Schaffer function for image encryption," *Expert Syst. Appl.*, vol. 213, p. 119076, 2023.

[32]. K. Altun and E. Günay, "A novel chaos-based modulation scheme: Adaptive threshold level chaotic on-off keying for increased BER performance," *Turkish J. Electr. Eng. Comput. Sci*., vol. 28, no. 2, pp. 606–620, 2020, doi: 10.3906/elk-1904-186.

[33]. A. K. Jawad, H. N. Abdullah, and S. S. Hreshee, "Secure speech communication system based on scrambling and masking by chaotic maps," in *IEEE, International Conference on Advances in Sustainable Engineering and Applications, ICASEA* 2018 - Proceedings, 2018, pp. 7–12. doi: 10.1109/ICASEA.2018.8370947.

[34]. B. W. H. A.-Z. S. S. Hreshee, "Encryption Audio Signal with IDEA Technique Enhanced by Chaotic System," in 2024 *3rd International Conference on Advances in Engineering Science and Technology (AEST), Babil, Iraq: IEEE*, 2024, pp. 1–6.

Mohammed Jasim Mohammed was born in Salah Aldein in 1988. He received the B.S degree in computer science from University of Tikrit College of computer and mathematics science department computer science in 2011. And M.S from UPM University putra Malaysia faculty of computer sciences and information technology major in network.He has been a full time lecturer in physics department at university of Samarra since September 2019. He can be contacted via email: mohammed.j.m@uosamarra.edu.iq.

Aqeel Majeed Breesam in the Institute of Medical Technology/ Baghdad – Middle Technical University, Baghdad, Iraq. I have a BSc degree in Computer Technologies Engineering in 2016 and a Master's Degree in Computer Technologies Engineering from the College of Electrical Engineering Technologies in 2021. My research areas are Image Processing, Computer Vision, Deep Learning, and Machine Learning.
He can be contacted at Email: aqeelmajeed@mtu.edu.iq