Merging the International Data Encryption Algorithm and Digital Chaotic Scrambler (DCS) to Enhance Audio Security

Bushra W. Hussein Al Zahawy
Electric Engineering Department, College of Engineering, University of Babylon, Iraq
eng322.bushra.hussien@student.uobabylon.edu.iq (corresponding author)

Saad S. Hreshee
Electric Engineering Department, College of Engineering, University of Babylon, Iraq
eng.saad.saffah@uobabylon.edu.iq

Received: 28 March 2025 | Revised: 4 May 2025 and 16 May 2025 | Accepted: 17 May 2025

 DOI: https://doi.org/10.48084/etasr.11191

ABSTRACT

Voice communication is a daily necessity, and as digital communication channels become increasingly widespread, the importance of voice transmission security is increasing. This paper proposes a robust and secure voice encryption system that combines chaotic systems and traditional cryptography. Specifically, it introduces a Digital Chaotic Scrambler (DCS) based on the Lorenz system to overcome the limitations of the International Data Encryption Algorithm (IDEA) in voice encryption. Incorporating the DCS into the IDEA structure enhances its resilience to cryptographic attacks. The DCS and IDEA's robust mathematical operations create a secure and efficient voice encryption system for real-time applications. Security metrics such as initial condition sensitivity, key sensitivity, and attack resistance quantify the proposed system's performance. Additional analyses, including key space analysis, statistical analysis, Mean Square Error (MSE), Signal-to-Noise Ratio (SNR), Segmental Spectral Signal-to-Noise Ratio (SSSNR), and Cepstral Distance (CD) demonstrate the effectiveness of the approach. Experimental results using audio files of various sizes in WAV format confirm that the suggested algorithms are not vulnerable to brute force or statistical attacks and achieve a higher level of security.

Keywords-voice encryption; IDEA; chaos; digital chaotic scrambler; Lorenz system; MSE; correlation coefficient

I. INTRODUCTION

In today's digitally interconnected world, the security of voice communications has become paramount. As our reliance on digital platforms for various aspects of life—from e-commerce to social interactions—continues to grow, so too does the risk of unauthorized access to sensitive information [1-5]. Voice encryption, a cryptographic technique that transforms intelligible voice signals into a scrambled form, serves as a robust defense against eavesdropping and unauthorized interception [1, 6-10].

Several studies have explored the integration of chaotic systems with the International Data Encryption Algorithm (IDEA) to enhance audio encryption by examining how chaotic maps increase key space and attack resistance. In [1], authors proposed a digital chaotic scrambling used for audio encryption based on the Duffing map. In [11], authors presented a robust audio encryption method using chaos theory and user-biometric images, employing the SHA-256 hash technique and zig-zag traversal. In [12], authors presented a new audio encryption scheme the uses chaotic systems and DNA coding to confuse and diffuse audio data, providing high security. In [13-15], authors proposed various speech encryption methods and schemes based on chaotic masking and noise reduction. In [16], authors presented a chaotic-based safe communication system that uses three levels of cryptography and a mix of chaos masking and encryption methods. Authors in [17] presented a secure chaos-based cryptosystem for communication systems, combining a conventional cryptography algorithm with two levels of the chaotic masking technique. In [18-20], authors proposed dual-layer voice encryption methods based on chaotic masking and chaotic scrambling. In [21], authors proposed a general-purpose symmetric encryption algorithm based on mathematical transformations and operations, suitable for various file types.

The IDEA has long been a popular symmetric encryption algorithm, including applications for voice encryption [22, 23]. A balanced mix of arithmetic and Boolean operations facilitates secure data transmission. Like any cryptographic algorithm, IDEA faces cryptanalytic threats [22, 23]. To address such vulnerabilities, various studies have proposed enhanced encryption schemes. In [24], a speech cryptosystem based on

substitution and permutation was proposed. In [25] authors presented a chaos-based speech time domain scrambling. In [26], authors suggested an audio encryption crypto model that used three different 3D Fibonacci-Lucas maps.

Chaos in dynamic systems results from the influence of initial conditions and control parameters, causing significant changes in behavior over time [27-29]. Chaos definitions have evolved to focus on nonlinearity, periodicity, and strange attractors, which are often used to model complex and unpredictable systems like weather, stocks, and diseases [15, 30-32]. Chaotic systems are found in various fields such as physics, chemistry, biology, mathematics, engineering, and cryptography, where they are utilized to generate unpredictable random numbers and sequences [33, 34]. Chaos is characterized by sensitivity to initial conditions, which makes even small changes significant [31, 35], as well as by unpredictable behavior over time, nonlinear dynamics, periodicity, and strange attractors. Chaotic systems are challenging to predict over long periods and are not proportional to inputs, which makes them difficult to understand and model. They often have strange attractors, which are geometric patterns that represent long-term system behavior [34, 34, 36].

In 1963, meteorologist and mathematician Edward Lorenz was the first person to study the Lorenz system, a set of Ordinary Differential Equations (ODEs), as a simpler mathematical model of atmospheric convection. The model consists of three ODEs, known as the Lorenz equations [14, 37]:

$$\dot{x} = \sigma(y - x) \quad (1)$$

$$\dot{y} = rx - y - xz \quad (2)$$

$$\dot{z} = xy - bz \quad (3)$$

where $\dot{x}$, $\dot{y}$, and $\dot{z}$ are the state vectors of the Lorenz system. The constants σ, r, and b are the Lorenz parameters, set to 10, 28, 8/3, respectively [38]. Figure 1 shows all the state vectors and the 3D strange attractors. Figure 2 illustrates the sensitivity of the Lorenz system to slight changes in initial conditions and parameters.

Chaotic maps are effective for large-scale data encryption due to their properties such as pseudo-randomness, sensitivity to initial conditions changes, and aperiodicity. This paper uses two chaotic maps to improve the security of cryptographic systems. While modern block ciphers like IDEA offer strong encryption, they can benefit from increased nonlinearity and confusion. To address this, the proposed system uses a Lorenz-based Digital Chaotic Scrambler (DCS), which introduces confusion and diffusion into encryption, exploiting initial conditions and complex dynamics. The encrypted data are further secured using IDEA. The main goals of this research are: First, the study focuses on analyzing the IDEA algorithm, including its design concepts, strengths, and flaws. The study also discusses the design and implementation of a Lorenz-based DCS integrated into the IDEA algorithm to improve efficiency and ensure seamless integration. A performance evaluation is conducted to assess the system's security and resilience.

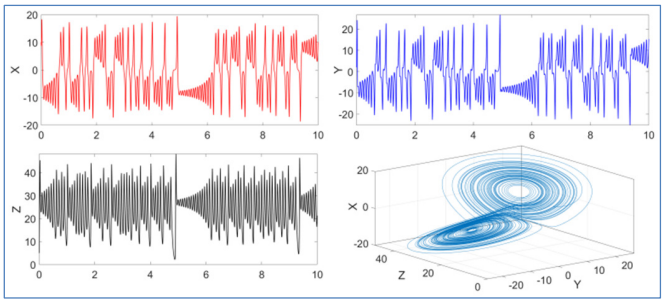

Fig. 1. Time series of X, Y, and Z and the 3D strange attractor of the Lorenz system.

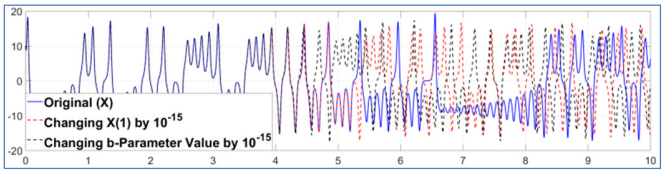

Fig. 2. Sensitivity of the Lorenz system to small changes in parameters or initial conditions.

II. PROPOSED METHODOLOGY

The digital voice signal is first encrypted using IDEA, then scrambled using a DCS, and finally transmitted over a public channel. At the receiving end, the signal is unscrambled and decrypted to recover the original voice signal. This scheme aims to secure voice communication over public channels.

Figure 3 illustrates the voice encryption and decryption process. The process begins by converting the original voice signal into a digital format. Then, the digital voice signal is encrypted using IDEA, a symmetric-key block cipher known for its security and efficiency. Then, the encrypted signal is scrambled using a DCS, a chaotic principle designed to add complexity and resistance to attacks. The encrypted and scrambled signal is transmitted over a public channel, such as the internet, radio waves, or satellite links. Once received, the signal is unscrambled using a chaotic decryption process that reverses the effects of the DCS. Next, the unscrambled signal is decrypted using the IDEA decryption algorithm, which restores the original digital voice signal. The final output is the original voice signal in its digital form, ready for playback. This encryption scheme combines the strength of the IDEA algorithm with the added security provided by the DCS. The goal is to protect the confidentiality of the voice signal during transmission over a public channel.

A. International Data Encryption Algorithm

The block cipher IDEA employs 64-bit plaintext and ciphertext blocks using a 128-bit key. Unlike many traditional block ciphers, IDEA is innovative in using three algebraic groupings, avoiding substitution boxes and Lookup Tables (LUTs). The encryption and decryption processes in IDEA are identical, differing only in key sub-blocks. The method comprises eight identical encryption rounds and an output transformation. Figure 4 provides a functional overview of the encryption process, which is described in detail below.

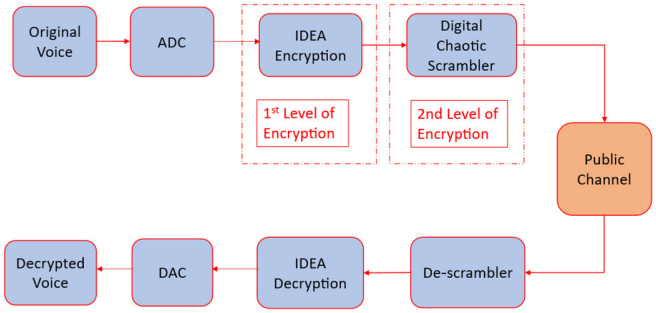

Fig. 3. Block diagram of the proposed voice encryption and decryption system.

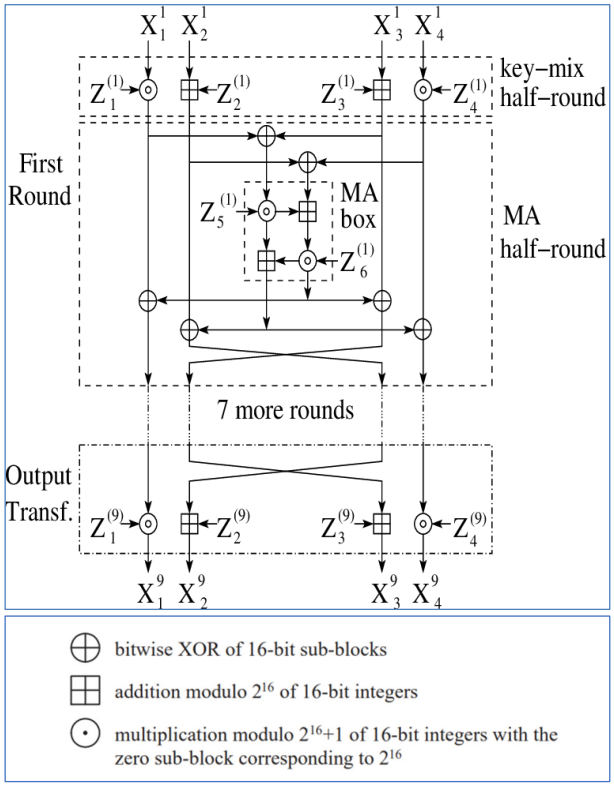

Fig. 4. General structure of the IDEA algorithm.

The 64-bit plaintext block is divided into four 16-bit sub-blocks: X1, X2, X3, X4. The 128-bit key generates eight 16-bit subkeys: Z1 to Z8. Six of these subkeys are utilized in the first round, and the remaining two are used in the second.

The first encryption round uses four 16-bit subkeys and two 16-bit plaintext blocks. The second round uses two additional 16-bit subkeys and the bit-by-bit exclusive OR operator. The eighth encryption round uses four 16-bit values and the last four subkeys to obtain four 16-bit ciphertext blocks. IDEA uses a total of 52 subkeys, across its eight encryption rounds and the final output transformation. Each round utilizes six 16-bit subkeys and the final transformation step requires an additional four subkeys. The subkey generation process works as follows:

1. The first eight 16-bit subkeys are generated by dividing the 128-bit key.
2. After cycling the 128-bit key left 25 places, the block is partitioned again into eight 16-bit sub-blocks for the next eight subkeys.
3. Cyclic shift repetition creates all 52 16-bit subkeys.

B. Digital Chaotic Scrambler based on Lorenz System

DCS is incorporated to achieve the second step of security by hashing the 64 encrypted bits from the IDEA algorithm. It achieves this goal by utilizing chaotic signals that exhibit a random behavior. Moreover, it is assumed that the chaotic initial values and parameters are securely shared and identical in both the transmitter and the receiver. The proposed DCS algorithm is described by the following steps [36, 37, 39]:

- Step 1: Chaotic system initialization

  Initialize the Lorenz chaotic system by defining its initial conditions and parameters and generate voice signal-length chaotic signals.

- Step 2: Chaotic signal generation

  To produce the chaotic signals required for scrambling, the system equations are numerically integrated using methods such as Euler's method [36, 37]. The iterative update equations are:

$$\left.\begin{aligned} x_{n+1} &= x_n + h f_x(x_n, y_n, z_n) \\ y_{n+1} &= y_n + h f_y(x_n, y_n, z_n) \\ z_{n+1} &= z_n + h f_z(x_n, y_n, z_n) \end{aligned}\right\} \quad (4)$$

  Here, f_x, f_x, and f_x represent the Lorenz system's $\dot{x}$, $\dot{y}$, and $\dot{z}$, and h is the ODEs solver's step size (typically $h \approx 0.001$) The present and next states are n and $n+1$, respectively. Due to the smooth nature of the Lorenz system, the nearby chaotic samples are highly correlated.

- Step 3: Digitized chaotic signal

  The continuous nature of the Lorenz signal, coupled with the small step size (h), results in minimal variation between consecutive samples. This inherent smoothness leads to a very high correlation approaching unity, visually represented by the near-diagonal line in the correlation plot. To enhance randomness and sensitivity to distant values, a transformation involving multiplication by a large constant (such as 1010) followed by a modulo operation with a smaller value (such as 216=65536) is applied [5, 37]. This process decorrelates adjacent samples effectively, as evidenced by the scattered distribution and near-zero Correlation Coefficient (CC) in the transformed signal's correlation plot illustrated in Figure 5. The transformation is mathematically expressed as:

$$\mathrm{Xmod}(n) = \mathrm{mod}(X_L(n) * 10^{10}, 2^{16}) \quad (5)$$

  For example, if $n = 10$ is equal to 10, the generated $\mathrm{Xmod}(n)$ signal is shown in Table I.

- Step 4: Ascending sorting of Xmod

  The chaotic vector is arranged in ascending order, resulting in Table II.

TABLE I. GENERATED XMOD VALUES FOR N = 10

n	Xmod
1	10,330
2	63,609
3	62,729
4	31,810
5	52,448
6	9,299
7	27,641
8	60,014
9	51,919
10	62,882

TABLE II. ASCENDING SORTING OF XMOD VALUES AND CORRESPONDING INDEX

n	Sorted Xmod
6	9,299
1	10,330
7	27,641
4	31,810
9	51,919
5	52,448
8	60,014
3	62,729
10	62,882
2	63,609

- Step 5: Chaotic DCS table generation

  As presented in Table III, changing element indices follows sorting the chaotic vector in step 4. Both the transmitter and receiver use these new DCS table indexes to encrypt and decrypt data.

TABLE III. GENERATED CHAOTIC DCS MAPPING TABLE FOR N = 10

Input index	1	2	3	4	5	6	7	8	9	10
Output index	6	1	7	4	9	5	8	3	10	2

Simple designs with high scattering and low correlation are preferred. However, for large frame sizes, sorting N elements requires $N(N-1)/2$ comparisons, which can lead to significant computational delays.

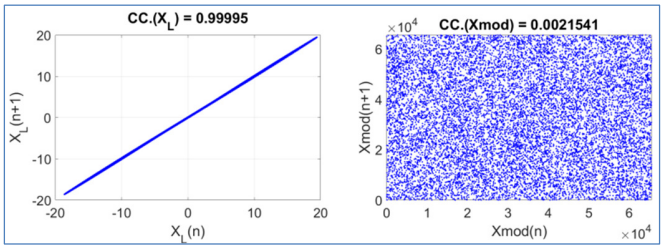

Fig. 5. Scatter plots and CCs of X_L and Xmod.

III. MEASURING THE QUALITY OF AUDIO SIGNAL

The performance of the proposed system will be evaluated using two types of testing: objective measurements and subjective measurements. These measures are defined as follows [10, 38-44].

A. Mean Square Error

The Mean Square Error (MSE) provides a way to analyze the accuracy of the model:

$$MSE = \frac{\sum_{i=1}^{m}(x_i - y_i)^2}{m} \quad (6)$$

where m is the length of the original and recovered (or encrypted) audio signals.

B. Correlation Coefficient

Calculating the correlation between adjacent samples is one method of assessing the efficacy of encryption algorithms. The CC is one of the analyses conducted to assess the resilience of a cryptosystem against a variety of statistical attacks.

$$CC = \frac{\sum_{i=1}^{m}(X_i - E(X))(Y_i - E(Y))}{\sqrt{\sum_{i=1}^{m}((X_i - E(X)))^2}\sqrt{\sum_{i=1}^{m}((Y_i - E(Y)))^2}} \quad (7)$$

where X and Y refer to the original and recovered (or encrypted) audio signals [35, 45, 46], and $E(X) = \frac{\sum_{i=1}^{m} X}{m}$, $E(Y) = \frac{\sum_{i=1}^{m} Y}{m}$.

C. Segmental Spectral Signal-to-Noise Ratio

The Segmental Spectral Signal-to-Noise Ratio (SSSNR) is the amount of noise in a specific signal. It is a collective measurement of the residual clarity of the encrypted speech and the clarity of the reconstructed speech.

$$SSSNR_i(dB) = 10 * \log_{10}\left(\frac{\sum_{k=1}^{N}|X_i(k)|}{\sum_{k=1}^{N}[|X_i(k)| - |Y_i(k)|]}\right) \quad (8)$$

where $X_i(k)$ and $Y_i(k)$ are the Discrete Fourier Transforms (DFTs) of the original and recovered signals, respectively [27].

D. Signal-to-Noise Ratio

Signal-to-Noise Ratio (SNR) is a metric that quantifies the amount of noise present in the encrypted data signal. Negative SNR values suggest that noise signals are more intense than the original audio signal.

$$SNR\ (dB) = 10 * \log10\left(\frac{\sum x^2}{\sum (x-y)^2}\right) \quad (9)$$

where x is the original voice signal and y is encrypted or decrypted voice signal [20, 47, 48].

E. Linear Predicative Coding

Linear Predicative Coding (LPC) is a method that is primarily employed in the fields of audio signal processing and speech processing to represent the spectral envelope of the speech signal. This methodology employs the information of a linear predictive model.

$$d_{lpc} = \ln\left(\frac{AVA^T}{BVB^T}\right) \quad (10)$$

where A and B vectors are the LPC coefficients for the original and encrypted or recovered audio signals, and V is the autocorrelation matrix of the original audio signal block [20, 15, 49]

F. Cepstral Distance

In general, Cepstral Distance (CD) is applied to measure the similarity between two frames of speech signals:

$$CD = 10\log_{10}\left[2\sum_{n=1}^{p}\{CC_x(n) - CC_y(n)\}^2\right]^{\frac{1}{2}} \quad (11)$$

where CC_x and CC_y are the cepstral coefficients for the original and the recovered or encrypted audio signals, respectively [43].

IV. SIMULATION RESULTS

This section presents the simulation findings and system methodologies for voice encryption utilizing the IDEA algorithm, further enhanced by chaotic signals. We conducted two studies using an Intel Core i7-13700H laptop with a 2.40 GHz CPU speed and 16 GB of RAM. The simulation findings were developed using the MATLAB (R2022a) and the Windows 11 operating system. Figure 6 shows the original voice signal used to test the proposed system [1, 27, 50].

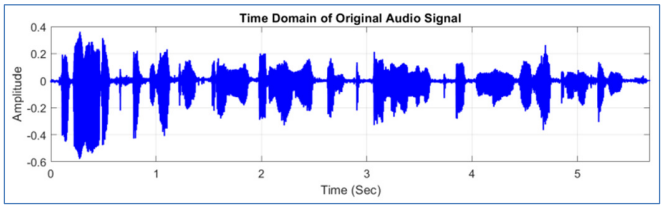

Fig. 6. Original audio signal used to test the proposed system.

A. Simulation Results of Classical International Data Encryption Algorithm

1) Audio Encryption Results

Figure 7 illustrates the encrypted audio signal, which appears as random noise, indicating the process has obscured the original content. The low correlation between consecutive samples suggests a high degree of randomness, making it difficult to exploit statistical relationships for decryption. The broad and relatively flat spectrum of both Fast Fourier Transform (FFT) and spectrogram plots indicates that the encryption process has effectively spread signal energy across a wide range of frequencies, making it challenging for attackers to identify characteristic frequencies.

The simulation results in Table IV indicate moderate distortion with an MSE of 0.33783, correlation close to zero, low SNR (less than -16dB), and an acceptable delay of 0.4524 s for the 5 s signal. These results indicate that the encryption scheme provides reasonable security; however, further optimization may be needed to improve audio quality and reduce noise.

2) Audio Decryption Results

Figure 8 shows the results of decrypting an audio signal using the IDEA algorithm. The decrypted audio signal appears to be a reasonably accurate reconstruction of the original, with minimal distortion. The correlation plot demonstrates a strong positive correlation between consecutive samples, indicating that the temporal relationships in the original signal have been preserved. The FFT and spectrogram plots resemble the original audio signal's frequency content, suggesting that the decryption process has successfully recovered the original signal's characteristics. The simulation results in Table V demonstrate a perfect decryption with zero MSE, perfect correlation, infinite SNR, and minimal delay. The findings confirm that the proposed encryption method is effective in maintaining the quality of the audio and ensuring the safety of the data transfers.

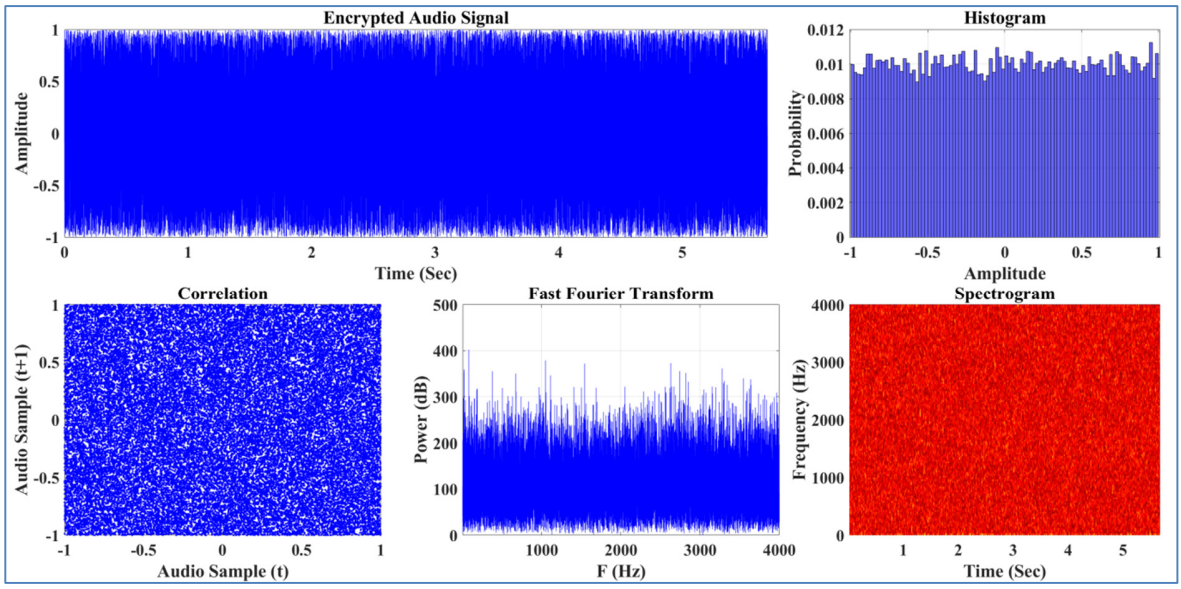

Fig. 7. Encrypted audio signal using the IDEA algorithm.

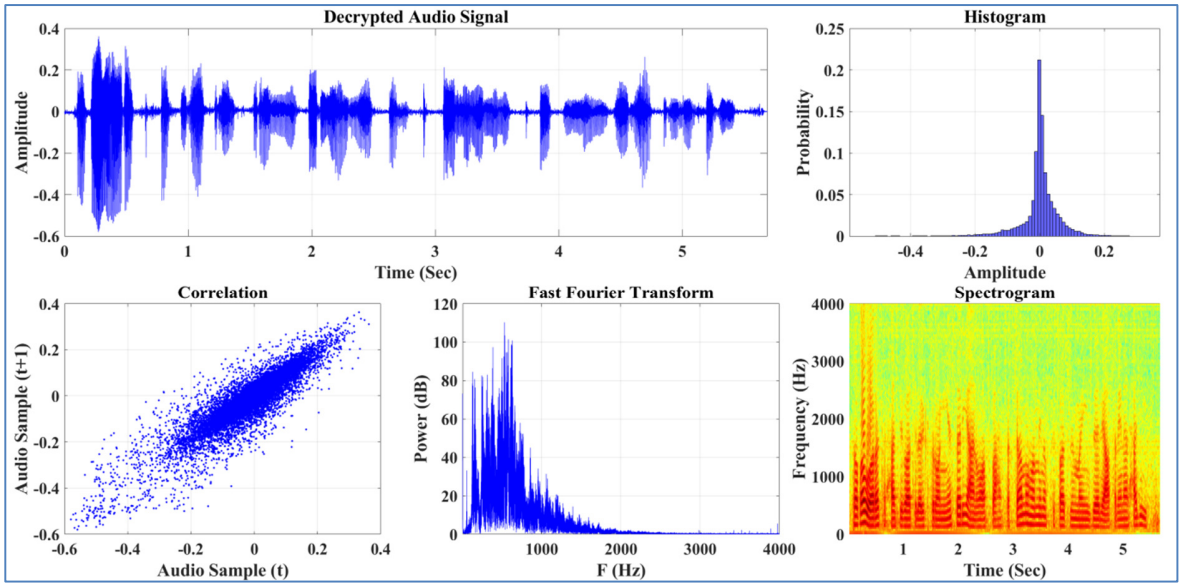

Fig. 8. Decrypted audio signal using the IDEA algorithm.

TABLE IV. SIMULATION RESULTS OF AUDIO ENCRYPTION BASED ON IDEA

Audio time (s)	MSE	CC	SNR (dB)	SSSNR (dB)	LPC	CD	Delay (s)
5	0.3378	0.00433	-18.052	-19.423	20.155	8.289	0.4524
10	0.3385	0.0008	-16.695	-19.43	23.18	8.289	0.9695
20	0.3378	0.00433	-24.072	-19.423	26.176	8.289	1.8121
30	0.3380	0.0001	-28.657	-19.418	27.935	8.287	2.7360
50	0.3391	-0.0046	-16.239	-19.424	30.145	8.291	4.7402

TABLE V. SIMULATION RESULTS OF AUDIO DECRYPTION BASED ON IDEA

Audio time (s)	MSE	CC	SNR (dB)	SSSNR (dB)	LPC	CD	Delay (s)
5	0	1	∞	∞	−∞	−∞	0.9059
10	0	1	∞	∞	−∞	−∞	1.7592
20	0	1	∞	∞	−∞	−∞	3.197
30	0	1	∞	∞	−∞	−∞	5.2445
50	0	1	∞	∞	−∞	−∞	8.4770

B. Simulation Results of the Proposed Method

As illustrated in Figure 3, the DCS is implemented subsequent to the IDEA block to encrypt the output of the IDEA using chaotic sequences.

1) Audio Encryption Results

Figure 9 demonstrates that the encrypted audio signal appears as random noise, obscuring the original content. The low correlation between consecutive samples suggests high randomness, making statistical decryption difficult. The broad and relatively flat spectrum of FFT and spectrogram plots shows that the encryption process has spread signal energy across a wide range of frequencies, making it difficult for attackers to identify characteristic frequencies.

The simulation results in Table VI demonstrate some distortion (MSE=0.33783), almost no correlation (-0.00039), low SNR (-22.78dB), and an acceptable delay (0.9252 s).

2) Audio Decryption Results

Figure 10 and Table VII illustrate the efficacy of the proposed encryption scheme, which makes use of IDEA in conjunction with chaotic key generation. The decrypted audio signal has a low MSE, a high SNR, minimal distortion, strong correlation, and an acceptable delay. These results demonstrate that the algorithm is capable of maintaining audio quality while providing robust security.

C. Key Sensitivity and Key Space Analysis of the Proposed System

1) Key Sensitivity

Changing the encryption key affects both the encryption and decryption processes, preventing the decryption of the audio signal. A key bit change between encryption and decryption prevents retrieval of the audio signal, so key sensitivity is essential for secure encryption. Any change to one IDEA key bit, or any slight change to the initial value or parameters of the Lorenz chaotic system, prevents recovery of the original audio signal. The output remains indistinguishable from the encrypted signal, as demonstrated in Table VIII.

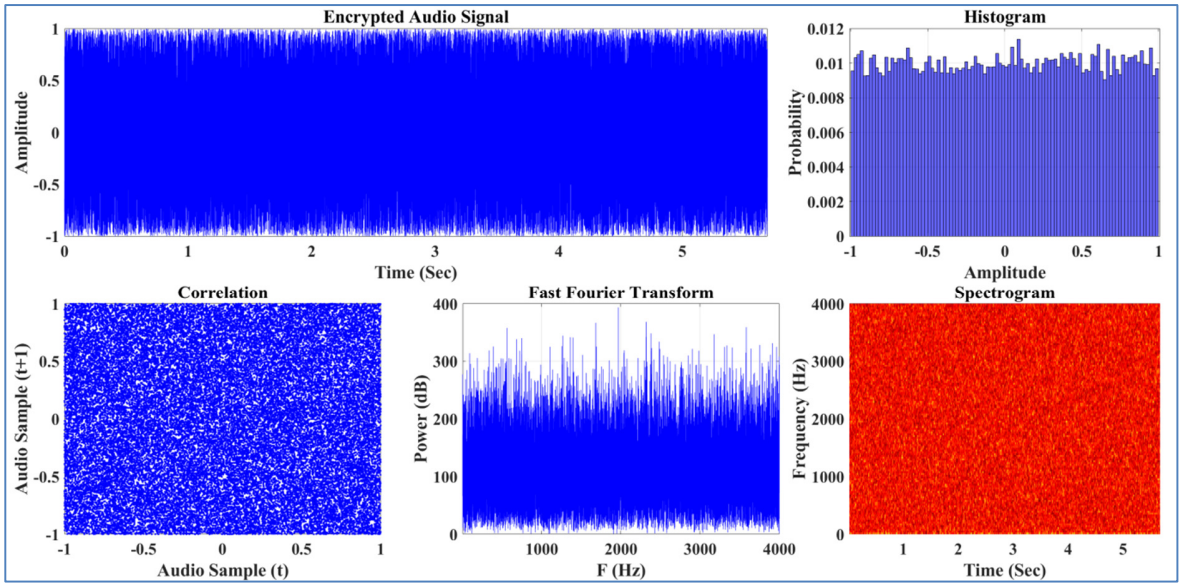

Fig. 9. Encrypted audio signal using IDEA and chaotic flow system.

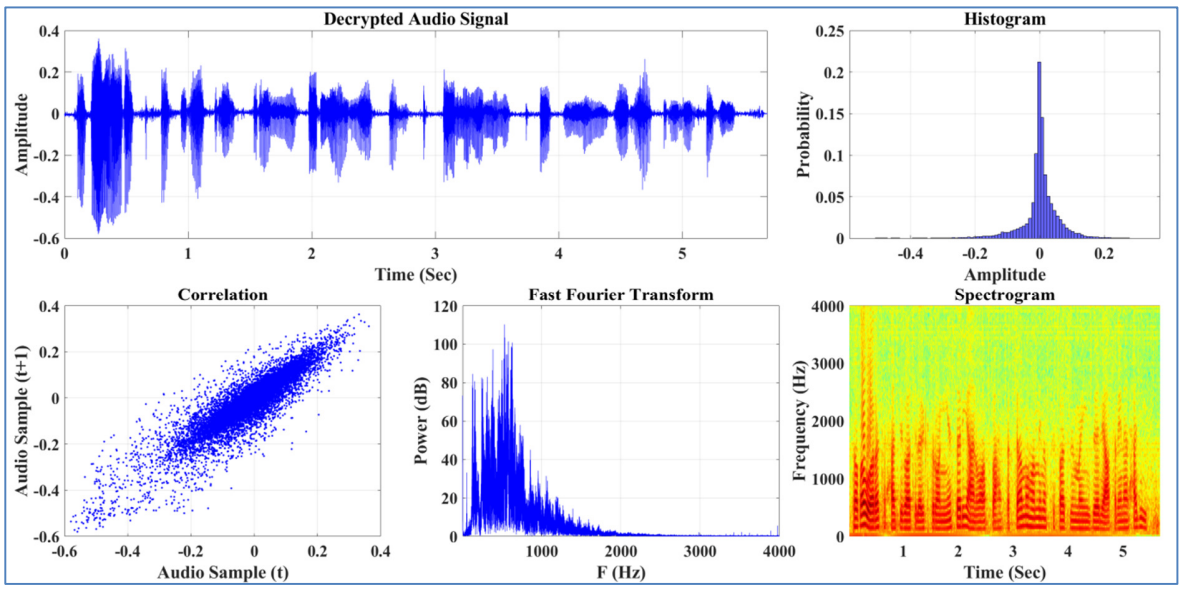

Fig. 10. Decrypted audio signal using IDEA and chaotic flow system.

TABLE VI. SIMULATION RESULTS OF AUDIO ENCRYPTION BASED ON IDEA AND CHAOTIC FLOW SYSTEM

Audio time (s)	MSE	CC	SNR (dB)	SSSNR (dB)	LPC	CD	Delay (s)
5	0.3378	-0.00039	-22.78	-19.417	20.172	8.284	0.9252
10	0.3390	0.00393	-20.751	-19.434	23.183	8.288	1.6734
20	0.3369	-0.00461	-12.501	-19.398	26.184	8.288	3.3439
30	0.3395	0.00202	-12.463	-19.44	27.935	8.29	4.8966
50	0.3374	-0.00246	-12.068	-19.407	30.162	8.289	8.1310

TABLE VII. SIMULATION RESULTS OF AUDIO DECRYPTION BASED ON IDEA AND CHAOTIC FLOW SYSTEM

Audio time (s)	MSE	CC	SNR (dB)	SSSNR (dB)	LPC	CD	Delay (s)
5	0	1	∞	∞	−∞	−∞	0.8622
10	0	1	∞	∞	−∞	−∞	1.5822924
20	0	1	∞	∞	−∞	−∞	2.909889
30	0	1	∞	∞	−∞	−∞	4.5041742
50	0	1	∞	∞	−∞	−∞	7.1939034

TABLE VIII. KEY SENSITIVITY RESULTS BASED ON CHANGES IN IDEA KEY BITS OR CHAOTIC LORENZ PARAMETERS

Change (single IDEA bit or initial condition/parameter ~10^{-15}	MSE	CC	SNR (dB)	SSSNR (dB)	LPC	CD
IDEA key bit #59	0.33921	-0.00275	- 9.232	-19.430	20.152	8.289
IDEA key bit #79	0.33665	0.0099	-14.941	-19.405	20.15	8.283
IDEA key bit #49	0.33836	-0.00103	-19.098	-19.415	20.148	8.281
$\Delta_x = 2 * 10^{-15}$	0.33278	0.00168	-17.994	-19.332	20.151	8.282
$\Delta_y = 1 * 10^{-15}$	0.33214	-0.00315	-19.882	-19.328	20.155	8.282
$\Delta_z = 1 * 10^{-15}$	0.32869	0.00434	-17.32	-19.281	20.174	8.279
$\Delta_\sigma = 2 * 10^{-16}$	0.32726	-0.00111	-14.696	-19.249	20.144	8.272
$\Delta_r = 2 * 10^{-16}$	0.32864	0.00262	-18.683	-19.280	20.179	8.281
Without change	0	1	∞	∞	$-\infty$	$-\infty$

The simulation results confirm that the IDEA algorithm, especially when combined with the Lorenz chaotic system, is extremely sensitive to key modifications. Even changing one bit can have a big effect on decryption and affect MSE, correlation, and SNR. This level of security is very important for encryption systems. The results demonstrate that the algorithm is strong against brute-force attacks, indicating its suitability for audio encryption.

2) Key Space Calculation for the Proposed System

The key space size is the total number of potential keys that can be employed with a cryptographic algorithm. The IDEA key space is fixed at 128 bits. In contrast, the exact number of keys in chaotic systems cannot be determined, but it can be approximated with a high degree of accuracy, as demonstrated in the following equation:

$$\text{KeySpace} = \prod_{i=1}^{d} \frac{1}{S} * R(i) \quad (12)$$

where d is the number of parameters and initial conditions of the chaotic system, S is the key sensitivity, and R is the range of values for any parameter or initial value within which the system remains within the limits of chaos.

To simplify the solution, we assume that R is 1, despite the fact that it is typically significantly greater than 1. In this scenario, the actual number of keys will exceed the current calculation. The Lorenz system is comprised of three parameters (σ, r, and b), and three state vectors (x, y, and z). The key space can be approximated as:

$$\text{Key(Lorenz)} \approx \prod_{i=1}^{6} \frac{1}{10^{-15}} \approx \left(\frac{1}{10^{-15}}\right)^6 \quad (13)$$

$$\text{Key(Lorenz)} = (10^{15})^6 = 10^{90} \approx 2^{299} \quad (14)$$

The total key space of the proposed system is:

$$\text{All Keys} = \text{Key}_{\text{IDEA}} * \text{Key}_{\text{Lorenz}} \quad (15)$$

$$\text{All Keys} \approx 2^{128} * 2^{299} \approx 2^{427} \quad (16)$$

A comparison of the key space size in bits for the proposed system and several other relevant studies is presented in Table IX. This table demonstrates that the proposed method utilizes a 427-bit key space, exceeding that of the majority of relevant literature. This expanded key space improves system security by significantly increasing resistance to brute-force attacks.

TABLE IX. PERFORMANCE COMPARSION BETWEEN THE PROPOSED SYSTEM AND OTHER METHODS

Reference	MSE	Corr.	SNR (dB)	SSSNR (dB)	LPC	CD	Key space (bits)
[1]	-	-	-	-1.944	0.6723	3.3369	212
TDS [18, 20]	-	-	-	0.9754	0.6532	2.4273	-
FDS[18, 20]	-	-	-	-0.2735	0.5823	2.5095	-
2DS[18, 20]	-	-	-	-1.9543	0.6132	3.2369	-
[25]	-	-0.0017	-11.8707	-	-	-	280
[32]	-	0.0032	-10.4925	-	-	-	180
[39]	-	0.0004	-	-	-	-	240
[42]	0.32647	-0.0038	-	-	-	-	175
[43]	0.3477	-	-	-	0.3187	7.8765	-
[49]	-	-	-	-12.8760	0.8877	3.6963	-
Ours (classical IDEA)	0.33782	0.0043	-18.052	-19.423	20.155	8.2892	128
Ours (proposed system)	0.33783	0.00433	-19.253	-20.124	20.817	8.2840	427

V. CONCLUSION

The proposed encryption system integrates the effectiveness of the International Data Encryption Algorithm (IDEA) algorithm with the enhanced security provided by a Digital Chaotic Scrambler (DCS) derived from the Lorenz system. Its objective is to safeguard the audio signal during transmission across any public channel. The simulation outcomes of audio encryption utilizing IDEA are highly favorable; however, the key space of 128 bits is regarded as relatively limited. Chaotic key generation is a technique that markedly enhances the security of IDEA for audio encryption. Expanding the key space renders brute-force attacks computationally impractical and introduces nonlinearity via chaotic maps, thereby enhancing resistance to cryptanalytic assaults. Any alteration to the parameters of the Lorenz map or initial conditions (x_0, y_0, z_0, σ, r, and b) will yield an unpredictable trajectory, which enhances encryption strength regarding key sensitivity. Moreover, any alteration of any

component within IDEA's keys during encryption and decryption precludes the recovery of the original audio signal from the encrypted audio signal. This method's robust security can enhance the development of audio encryption systems that surpass traditional methods in reliability and strength. Furthermore, its outcomes can be utilized in other domains necessitating secure voice data transmission. The proposed method may also be applied to additional block blades and integrated with other security measures, including information concealment or watermarking.

REFERENCES

[1] A. Mahdi, A. K. Jawad, and S. S. Hreshee, "Digital Chaotic Scrambling of Voice Based on Duffing Map," *International Journal of Information and Communication Sciences*, vol. 1, no. 2, pp. 16–21, Aug. 2016, https://doi.org/10.11648/j.ijics.20160102.11.

[2] M. Orceyre and R. Heller, "An approach to secure voice communication based on the data encryption standard," *IEEE Communications Society Magazine*, vol. 16, no. 6, pp. 41–50, Nov. 1978, https://doi.org/10.1109/MCOM.1978.1089785.

[3] N. J. Corron and D. W. Hahs, "A new approach to communications using chaotic signals," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 44, no. 5, pp. 373–382, May 1997, https://doi.org/10.1109/81.572333.

[4] A. K. Jawad, G. Karimi, and M. Radmelkshahi, "A Novel Digital Audio Encryption Algorithm Using Three Hyperchaotic Rabinovich System Generators," *ARO-The Scientific Journal Of Koya University*, vol. 12, no. 2, pp. 234–245, Dec. 2024, https://doi.org/10.14500/aro.11869.

[5] A. k. Jawad, G. Karimi, and M. 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*, Babil, Iraq, 2024, pp. 114–119, https://doi.org/10.1109/AEST63017.2024.10959812.

[6] W. Dai, X. Xu, X. Song, and G. Li, "Audio Encryption Algorithm Based on Chen Memristor Chaotic System," *Symmetry*, vol. 14, no. 1, Jan. 2022, Art. no. 17, https://doi.org/10.3390/sym14010017.

[7] P. Sathiyamurthi, S. Ramakrishnan, S. Shobika, N. Subashri, and M. Prakavi, "Speech and Audio Cryptography System using Chaotic Mapping and Modified Euler's System," in *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, Coimbatore, India, 2018, pp. 606–611, https://doi.org/10.1109/ICICCT.2018.8473183.

[8] M. J. M. Ameen and S. S. Hreshee, "Hyperchaotic Modulo Operator Encryption Technique for Massive Multiple Input Multiple Output Generalized Frequency Division Multiplexing system," *International Journal on Electrical Engineering and Informatics*, vol. 14, no. 2, pp. 311–329, Jun. 2022, https://doi.org/10.15676/ijeei.2022.14.2.4.

[9] M. J. M. Ameen and S. S. Hreshee, "Security analysis of encrypted audio based on elliptic curve and hybrid chaotic maps within GFDM modulator in 5G networks," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 6, pp. 3467–3479, Dec. 2023, https://doi.org/10.11591/eei.v12i6.4913.

[10] W. Wei and J. Kim, "Modeling and Analysis of Chaos-based Spread Spectrum Scheme using Irregular LDPC Code and Non-Coherent 16-DCSK under Fading and Jamming," *Engineering, Technology & Applied Science Research*, vol. 9, no. 6, pp. 5080–5087, Dec. 2019, https://doi.org/10.48084/etasr.3232.

[11] B. Rahul, K. Kuppusamy, and A. Senthilrajan, "Chaos-based audio encryption algorithm using biometric image and SHA-256 hash algorithm," *Multimedia Tools and Applications*, vol. 82, no. 28, pp. 43729–43758, Nov. 2023, https://doi.org/10.1007/s11042-023-15289-x.

[12] X. Wang and Y. Su, "An Audio Encryption Algorithm Based on DNA Coding and Chaotic System," *IEEE Access*, vol. 8, pp. 9260–9270, 2020, https://doi.org/10.1109/ACCESS.2019.2963329.

[13] A. K. Jawad, H. N. Abdullah, S. S. Hreshee, and G. Karimi, "Performance Improvement of Chaotic Masking System using Power Control Method," in *International Middle Eastern Simulation and Modelling Conference*, Baghdad, Iraq, 2022, pp. 19–23.

[14] H. N. Abdullah, S. S. Hreshee, and A. K. Jawad, "Design of Efficient Noise Reduction Scheme for Secure Speech Masked by Chaotic Signals," *Journal of American Science*, vol. 11, no. 7, pp. 49–55, Jul. 2015.

[15] H. N. Abdullah, S. S. Hreshee, and A. K. Jawad, "Noise Reduction of Chaotic Masking System using Repetition Method," *Unpublished*, Feb. 2015, https://doi.org/10.13140/RG.2.1.4023.7209.

[16] W. A. Nassan, T. Bonny, and A. Baba, "A New Chaos-Based Cryptoystem for Voice Encryption," in *2020 3rd International Conference on Signal Processing and Information Security*, Dubai, United Arab Emirates, 2020, pp. 1–4, https://doi.org/10.1109/ICSPIS51252.2020.9340132.

[17] T. Bonny, W. A. Nassan, and A. Baba, "Voice encryption using a unified hyper-chaotic system," *Multimedia Tools and Applications*, vol. 82, no. 1, pp. 1067–1085, Jan. 2023, https://doi.org/10.1007/s11042-022-13317-w.

[18] A. K. Jawad, H. N. Abdullah, and S. S. Hreshee, "Secure speech communication system based on scrambling and masking by chaotic maps," in *2018 International Conference on Advance of Sustainable Engineering and its Application*, Kut, Iraq, 2018, pp. 7–12, https://doi.org/10.1109/ICASEA.2018.8370947.

[19] 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, Aug. 2020, https://doi.org/10.11591/ijece.v10i4.pp4270-4278.

[20] S. S. Hreshee, H. N. Abdullah, and A. K. Jawad, "A High Security Communication System Based on Chaotic Scrambling and Chaotic Masking," *International Journal on Communications Antenna and Propagation (IRECAP)*, vol. 8, no. 3, pp. 257–264, Jun. 2018, https://doi.org/10.15866/irecap.v8i3.13541.

[21] M. Baykara, R. Daş, and G. Tuna, "A Novel Symmetric Encryption Algorithm and its Implementation," *Turkish Journal of Science and Technology*, vol. 12, no. 1, pp. 5–9, Mar. 2017.

[22] S. Basu, "International Data Encryption Algorithm (IDEA) – A Typical Illustration," *Journal of Global Research in Computer Science*, vol. 2, no. 7, pp. 116–118, Jul. 2011.

[23] H. P. Singh, S. Verma, and S. Mishra, "Secure-International Data Encryption Algorithm," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 2, no. 2, pp. 780–792, Feb. 2013.

[24] A. Mostafa, Naglaa. F. Soliman, M. Abdalluh, and F. E. Abd El-samie, "Speech encryption using two dimensional chaotic maps," in *2015 11th International Computer Engineering Conference*, Cairo, Egypt, 2015, pp. 235–240, https://doi.org/10.1109/ICENCO.2015.7416354.

[25] S. M. H. Alwahbani and E. B. M. Bashier, "Speech scrambling based on chaotic maps and one time pad," in *2013 International Conference on Computing, Electrical and Electronic Engineering*, Khartoum, Sudan, 2013, pp. 128–133, https://doi.org/10.1109/ICCEEE.2013.6633919.

[26] S. Pati, M. Mishra, and J. Rout, "Securing Audio with 3D-Chaotic Map Based Hybrid Encryption Technique," *International Journal of Computing and Digital Systems*, vol. 18, no. 1, pp. 1–15, Aug. 2024, https://doi.org/10.12785/ijcds/1571111843.

[27] H. A. Ismael and S. B. Sadkhan, "Security enhancement of speech scrambling using triple Chaotic Maps," in *2017 Annual Conference on New Trends in Information & Communications Technology Applications*, Baghdad, Iraq, 2017, pp. 132–137, https://doi.org/10.1109/NTICT.2017.7976141.

[28] I. Jomaa, W. M. Saleh, R. R. I. Hassan, and S. H. H. Wadi, "Secured drone communication based on Esalsa20 algorithm and 1d logistic map," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 29, no. 2, pp. 861–874, Feb. 2023, https://doi.org/10.11591/ijeecs.v29.i2.pp861-874.

[29] H. Mahalingam, T. Veeramalai, A. R. Menon, S. S., and R. Amirtharajan, "Dual-Domain Image Encryption in Unsecure Medium—

A Secure Communication Perspective," *Mathematics*, vol. 11, no. 2, Jan. 2023, Art. no. 457, https://doi.org/10.3390/math11020457.

[30] M. Khalid, E. A. Hussein, and A. K. Jawad, "Digital Image Encryption Based on Random Sequences and XOR Operation," *Journal of Engineering and Applied Sciences*, vol. 14, no. 8, pp. 10331–10334, Nov. 2019, https://doi.org/10.36478/jeasci.2019.10331.10334.

[31] H. Tian, Z. Wang, P. Zhang, M. Chen, and Y. Wang, "Dynamic Analysis and Robust Control of a Chaotic System with Hidden Attractor," *Complexity*, vol. 2021, no. 1, Jan. 2021, Art. no. 8865522, https://doi.org/10.1155/2021/8865522.

[32] S. Mokhnache, M. E. H. Daachi, T. Bekkouche, and N. Diffellah, "A Combined Chaotic System for Speech Encryption," *Engineering, Technology & Applied Science Research*, vol. 12, no. 3, pp. 8578–8583, Jun. 2022, https://doi.org/10.48084/etasr.4912.

[33] A. A. Abdul-Kareem and W. A. M. Al-Jawher, "An image encryption algorithm using hybrid sea lion optimization and chaos theory in the hartley domain," *International Journal of Computers and Applications*, vol. 46, no. 5, pp. 324–337, May 2024, https://doi.org/10.1080/1206212X.2024.2313300.

[34] D. Raghuvanshi, K. Joshi, R. Nandal, H. Sehrawat, S. Singh, and S. Singh, "Improved security with novel M-Log chaos steganography algorithm for huffman compressed english text," *Multimedia Tools and Applications*, vol. 84, no. 2, pp. 665–688, Jan. 2025, https://doi.org/10.1007/s11042-024-18889-3.

[35] H. Rafiee, M. Mahdavi, and A. NaghshNilchi, "Introducing a New Evaluation Criteria for EMD-Base Steganography Method." arXiv, Aug. 15, 2023, https://doi.org/10.48550/arXiv.2308.07970.

[36] M. Moghtadaei and M. R. Hashemi Golpayegani, "Complex dynamic behaviors of the complex Lorenz system," *Scientia Iranica*, vol. 19, no. 3, pp. 733–738, Jun. 2012, https://doi.org/10.1016/j.scient.2010.11.001.

[37] W. A. H. Hadi, H. F. Y. Hussein, and A. K. Jawad, "Enhancement of Image Transmission Using Chaotic Interleaver over Wireless Sensor Network," *International Journal of New Technology and Research*, vol. 2, no. 7, pp. 24–28, 2016.

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

[39] A. Elsharkawi, R. M. El-Sagheer, H. Akah, and H. Taha, "A Novel Image Stream Cipher Based On Dynamic Substitution," *Engineering, Technology & Applied Science Research*, vol. 6, no. 5, pp. 1195–1199, Oct. 2016, https://doi.org/10.48084/etasr.729.

[40] A. R. Alharbi *et al.*, "A New Multistage Encryption Scheme Using Linear Feedback Register and Chaos-Based Quantum Map," *Complexity*, vol. 2022, no. 1, Apr. 2022, Art. no. 7047282, https://doi.org/10.1155/2022/7047282.

[41] A. H. Elsafty, M. F. Tolba, L. A. Said, A. H. Madian, and A. G. Radwan, "FPGA Speech Encryption Realization Based on Variable S-Box and Memristor Chaotic Circuit," in *2018 30th International Conference on Microelectronics*, Sousse, Tunisia, 2018, pp. 152–155, https://doi.org/10.1109/ICM.2018.8704019.

[42] A. H. ElSafty, M. F. Tolba, L. A. Said, A. H. Madian, and A. G. Radwan, "Hardware realization of a secure and enhanced s-box based speech encryption engine," *Analog Integrated Circuits and Signal Processing*, vol. 106, no. 2, pp. 385–397, Feb. 2021, https://doi.org/10.1007/s10470-020-01614-z.

[43] S. B. Sadkhab, A. M. Raheema, and S. M. Abdul Sattar, "Design and Implementation Voice Scrambling Model Based on Hybrid Chaotic Signals," in *2019 First International Conference of Computer and Applied Sciences*, Baghdad, Iraq, 2019, pp. 193–198, https://doi.org/10.1109/CAS47993.2019.9075626.

[44] 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 International Journal of Artificial Intelligence*, vol. 12, no. 1, pp. 347–356, Mar. 2023, https://doi.org/10.11591/ijai.v12.i1.pp347-356.

[45] H. Wen *et al.*, "High-quality restoration image encryption using DCT frequency-domain compression coding and chaos," *Scientific Reports*, vol. 12, no. 1, Oct. 2022, Art. no. 16523, https://doi.org/10.1038/s41598-022-20145-3.

[46] P. V. S. Reddy and M. N. R, "Reduction of Correlation in 2D Image Encryption using Novel Gingerbreadman Chaotic Map in Comparison with Tinkerbell Map," *Baltic Journal of Law & Politics*, vol. 15, no. 4, pp. 147–158, Dec. 2022, https://doi.org/10.2478/bjlp-2022-004015.

[47] F. J. Farsana, V. R. 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, Jun. 2023, https://doi.org/10.1016/j.aci.2019.10.001.

[48] H. Elkamchouchi, W. M. Salama, and Y. Abouelseoud, "New video encryption schemes based on chaotic maps," *IET Image Processing*, vol. 14, no. 2, pp. 397–406, Feb. 2020, https://doi.org/10.1049/iet-ipr.2018.5250.

[49] M. K. M. AlAzawi and J. Q. Kadhim, "Speech Scrambling Employing Lorenz Fractional Order Chaotic System," *Journal of Engineering and Sustainable Development*, vol. 17, no. 4, pp. 195–211, Oct. 2013.

[50] Z. Ali, K. Saleem, R. Brown, N. Christofides, and S. Dudley, "Performance Analysis and Benchmarking of PLL-Driven Phasor Measurement Units for Renewable Energy Systems," *Energies*, vol. 15, no. 5, Mar. 2022, Art. no. 1867, https://doi.org/10.3390/en15051867.