International Journal of Computational and Experimental Science and ENgineering
(IJCESEN)

Vol. 11-No.3 (2025) pp. 4535-4544
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Two Layers of Audio Security Utilizing the International Data Encryption Algorithm (IDEA) and Lorenz Chaotic Scrambler

Bushra W. Hussein AL Zahawy[1,2*], Saad S. Hreshee[3]

[1]Electric Engineering Department, College of Engineering, University of Babylon, Iraq.
[2]Water Resources Management Engineering Department, College of Engineering, Al-Qasim. Green University, Babylon, 51013, Iraq
M* Corresponding Author Email: eng322.bushra.hussien@student.uobabylon.edu.iq – **ORCID**: 0009-0005-8834-4261

[1]Electric Engineering Department, College of Engineering, University of Babylon, Iraq.
Email:saa2d@gmail.com - **ORCID:** 0009-0005-8834-4260

Article Info:

DOI: 10.22399/ijcesen.2183
Received : 05 February 2025
Accepted : 01 May 2025

Keywords

Voice Encryption,
IDEA,
Chaos,
Digital Chaotic Scrambler,
Lorenz System,
MSE,
Correlation Coefficients

Abstract:

Voice communication between individuals is an essential aspect of daily life. The significance of voice transmission security is increasing as digital communication channels become more prevalent. This paper suggests a secure and resilient voice encryption system that integrates traditional cryptography and chaotic systems. This paper introduces a digital chaotic scrambler (DCS) that is based on the Lorenz system and is designed to address the constraints of the International Data Encryption Algorithm (IDEA) in the context of voice encryption. The DCS also reinforces the resistance of the IDEA structure to many cryptographic attacks. The DCS and the strong mathematical operations of the IDEA establish a secure, efficiency, voice encryption system in real applications. The security metrics we define are used to quantify the performance of the proposed system; these include sensitivity to initial conditions, sensitivity to the key, and attack resistance. Keyspace analysis, Statistical analysis, MSE (mean square error), Signal-to-noise ratio (SNR), correlations and (Segmental spectral signal-to-noise ratio) SSSNR and Cepstral Distance (CD) analyses results. Statistical analyses and audio security tests performed on audio files of different sizes with a WAV file extension have shown that the algorithms proposed are resistant to brute force or statistical attacks and have a higher security level.

1. Introduction

The security of digital voice communications has become a major concern in the current connected world [1], [2], [3], [4]. We depend on digital platforms to run the show today, whether in e-commerce or social relations, the risk to our sensitive information is growing. Voice encryption: a cryptographic method used to convert understandable voice signals into an incomprehensible signal, which provides a strong protection against eavesdropping and unauthorized interception [1], [5]. Audio encryption literature survey of using chaotic systems to make the International Data Encryption Algorithm (IDEA) more secure. The previous study analyzed how chaotic maps help to increase kay space and resist attack. In [1], which proposed a digital chaotic scrambling for audio encryption based on the Duffing map. In [6], proposed a robust approach to encrypt audio messages, employing chaos theory and user-biometric images using SHA-256 hash technique and zig-zag traversal. In [7], a new audio encryption scheme uses chaotic systems and DNA coding to confuse and diffuse audio data, providing high security. In [8], [9], [10], proposed a speech encryption based on chaotic masking and noise reduction based on different methods and schemes. In [11], they showed a chaotic-based safe communication system that uses three levels of cryptography and a mix of chaos masking and encryption methods. The authors in [12], presented a secure chaos-based cryptosystem for communication systems, combining a conventional cryptography algorithm with two levels of chaotic masking technique. In [13], [14], [15], proposed a voice encryption using two layers based on chaos such as chaotic masking and chaotic scrambling. In

[16], proposed encryption algorithm, based on mathematical terms and operations, is a general-purpose symmetric encryption suitable for various file types.The IDEA has long been a popular symmetric encryption algorithm, including voice encryption [17], [18]. A balanced mix of arithmetic and Boolean operations underpins secure data transmission. IDEA, like any cryptographic algorithm, faces cryptanalytic threats [17], [18]. In [19], a proposed speech cryptosystem based on substitution and permutation. In [20] presented a chaos-based speech scrambling system. In [21] ,suggested an audio encryption crypto model that used a three different 3D Fibonacci-Lucas maps. The successful use of chaotic maps for large-scale data encryption, including image, audio, and video data, is attributed to their good properties, including pseudo-randomness, sensitivity to changes in initial conditions and system parameters, and aperiodicity. This paper uses two chaotic maps. Increasing computing power and cryptanalytic techniques have necessitated ongoing research to improve cryptographic system security. The DCS is especially important in the design of modern block ciphers such as IDEA. Encryption is complex and non-linear thanks to DCS, and thus the plaintext becomes almost impossible for the attacker to recover. We believe that the DCS of IDEA is well designed, but that like the Office of Indian Affairs, emerging threats require adjustments to better secure the networks of the DCS. This system is based on proposing a Lorenz chaotic based DCS, which adds confusion, diffusion, and utilizes the initial conditions and dynamics for this purpose. And the data to be encrypted is even better protected by the International Data Encryption Algorithm (IDEA), a commonly used block cipher that is also fast and secure. This research's main goals:

- In-depth IDEA algorithm analysis: A thorough analysis of IDEA's design concepts, strengths, and flaws.
- DCS design and implementation: Design of a Lorenz-based DCS featuring nonlinearity, diffusion, and differential and linear cryptanalysis resistance.
- To integrate the DCS into IDEA: Integrating the DCS into the IDEA algorithm to ensure efficiency and seamless integration.
- Performance evaluation: Thorough testing of the proposed system's security, efficiency, and resilience to differential power analysis and side-channel assaults.

1.1. Lorenz Chaotic System

Chaos in dynamic systems is influenced by initial conditions and control parameters, causing significant changes in behavior over time [22], [23], [24]. The definitions of chaos have changed they have been shifting mostly to nonlinearity and periodicity instead of complexity. Chaotic systems are prevalent in modeling complex and unpredictable systems such as weather, stocks and disease. Uneven attractor patterns are commonly found on them, illustrating the behavior of the system as time progresses [10], [25], [26]. Chaotic systems appear in many fields such as physics, chemistry, biology, mathematics, engineering and cryptography. Random or pseudo-random generators can produce random numbers and sequences that are indistinguishable from true random numbers by its non-regular behavior [24], [27]. Chaos is sensitive to initial conditions, nonlinear, gets periodic, and has strange attractors. These systems are extremely patient in terms of initial conditions, so even subtle perturbations in them are meaningful [28], [29]. They're also volatile, which makes it hard to forecast what they'll do over long stretches. They exhibit non-linear behavior; they are impossible to understand and model. Additionally, chaotic systems often have strange attractors, which are geometric patterns that represent the long-term behavior of the system [25], [30], [31].The first person to look at the Lorenz system, which is a set of ordinary differential equations (ODEs), was the meteorologist and mathematician Edward Lorenz. In 1963, a simpler mathematical model of convection in the atmosphere was made. The model consists of three ordinary differential equations called the Lorenz equations [9],[26], [32].

$$\dot{x} = \sigma(y - x) \quad (1)$$
$$\dot{y} = rx - y - xz \quad (2)$$
$$\dot{z} = xy - bz \quad (3)$$

Where the $\dot{x}, \dot{y}\ and\ \dot{z}$ are the state vectors of the Lorenz system. (σ, r, and b) are the Lorenz parameters equal to [10, 28, 8/3], respectively [33]. All the state vectors and the 3D strange attractors are shown in Figure . While Figure illustrate the sensitivity of the Lorenz system, to any slightly changing in initial condition and parameters.

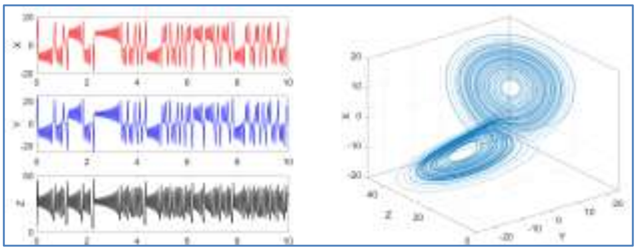

Figure 1. *Time series X, Y, and Z of the Lorenz system and 3D strange attractor* [24].

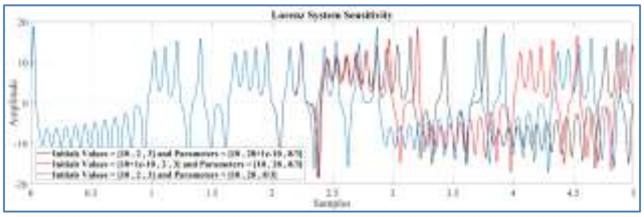

Figure 2. *Lorenz system parameter or initial value sensitivity to small changes.*

1.2. The Proposed Methodology

The digital voice signal is encrypted using IDEA and further scrambled with a DCS before transmission over a public channel. On 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. A diagram for a voice encrypts and decrypt process shown in Figure 1. It all starts with the original voice signal being digitized. IDEA (International Data Encryption Algorithm) is used to encrypt the digital voice signal, blocking symmetric-key which is one of the security and efficiency types. This encrypted signal is then disturbed via a DCS, where DCS stands for Digital Chaotic Signal, where chaotic principles are adopted to make it difficult to attack. The encrypted scrambled signal is sent through a public channel, such as the internet, radio waves, or satellite links. This is followed by the chaotic decryption approach to unscrambled the received signal that counteracts the effect of the DCS. The signal, once unscrambled, is decrypted using the IDEA decryption algorithm, recreating the original digital voice signal. The end result is the discrete form of original voice signal that can be played back. In this encryption scheme, the power of IDEA algorithm is combined with extra security offered by Digital Circuit Security (DCS). It aims to protect the confidentiality of the voice signal during transmission over a public channel.

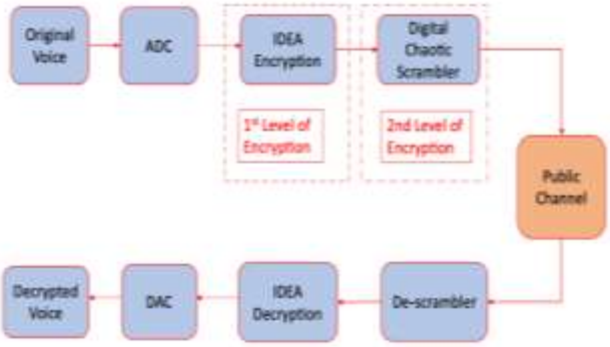

***Figure 1**. Block diagram for the proposed system.*

1.3. International Data Encryption Algorithm (IDEA)

A 128-bit key controls the block cipher IDEA, which uses 64-bit plaintext and cipher text blocks. Using operations from three algebraic groups is the key novelty in this algorithm. Available block ciphers avoid substitution boxes and Look Up Tables (LUTs). The algorithm structure makes encryption and decryption identical except for key sub-blocks. Figure shows the encryption process functionally. Eight identical encryption rounds and an output transformation comprise the method. The IDEA encryption processes are described as follow: The 64-bit plaintext block has four 16-bit subblocks: X1, X2, X3, X4. The 128-bit Key generates eight subkeys: Z1 to Z8 from eight 16-bit blocks. Six subkeys are utilized in the first round, while the remaining two are used in the second. Addition modulo 2^{16} and multiplication modulo $2^{16}+1$ mix the first four 16-bit key sub-blocks with two 16-bit plaintext blocks in the first encryption round. Further processing uses two further 16-bit key sub-blocks and the third algebraic group operator, the bit-by-bit exclusive OR. The second encryption round receives four 16-bit values in a somewhat modified order from the first encryption round. Following round one, each of the seven encryption rounds uses a different 16-bit key sub-block. Addition modulo 2^{16} and multiplication modulo $2^{16}+1$ combine the four 16-bit values from the eighth encryption round with the last four key sub-blocks to obtain the four 16-bit

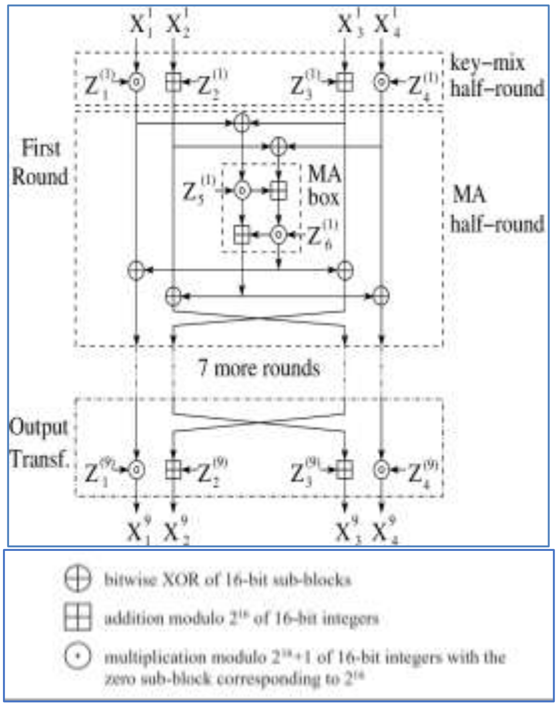
X1 X2 X3 X4
Z1(1) Z2(1) Z3(1) Z4(1)
key–mix half–round
First Round
Z5(1)
MA box
Z6(1)
MA half–round
7 more rounds
Output Transf.
Z1(9) Z2(9) Z3(9) Z4(9)
X1(9) X2(9) X3(9) X4(9)
⊕ bitwise XOR of 16-bit sub-blocks
⊞ addition modulo 2^16 of 16-bit integers
⊙ multiplication modulo 2^16+1 of 16-bit integers with the zero sub-block corresponding to 2^16

Figure 4. *The general structure of IDEA algorithm.*

ciphertext blocks. The distribution of the 52 subkeys for each round. These subkeys are used to encrypt all the data to be encrypted. Other subkeys can only be generated traditionally by changing the original key bits. Four 16-bit subblocks make up the 64-bit plaintext block since all encryption algebraic operations utilize 16-bit values. Another procedure generates six 16-bit key sub-blocks from the 128-bit Key per encryption round. The 128-bit Key must generate 52 (16-bit key-sub-blocks) for the output transformation, which requires four more. The 128-bit key generates 52 16-bit key sub-blocks:

1- Initial key sub-blocks are the first eight 16-bit sub-blocks of the 128-bit Key.
2- After cyclically shifting the 128-bit Key left by 25 positions, the block is partitioned again into eight 16-bit sub-blocks to be utilized as the following eight key sub-blocks.
3- Repetition of the cyclic shift technique generates all 52 16-bit key sub-blocks.

2. Digital Chaotic Scrambler (DCS) Based on Lorenz System

The process of designing of DCS scrambler to achieve the second step of security by hashing the 64 encrypted bits. DCS may be designed to achieve this goal by utilizing chaotic signals, which exhibit a random behavior. Because of the way this system is designed, it is assumed that the chaotic initial values and parameters are the same in both the transmitter and the receiver. The suggested algorithm for scrambling data is described by the following steps [33], [34]:

2.1. Chaotic System Initialization

The proposed encryption system starts with initializing chaotic systems and generating voice signal-length chaotic signals. Define the Lorenz chaotic system initial conditions and parameters.

2.2. Chaotic Signal Generation

In order to produce chaotic signals, the system equations are numerically integrated. There are numerical methods, such as Euler's, that can accomplish this, as demonstrated by the following equations [33], [34]:

$$\left.\begin{aligned} x_{n+1} &= x_n + hf_x(x_n\,, y_n\,, z_n) \\ y_{n+1} &= y_n + hf_y(x_n\,, y_n\,, z_n) \\ z_{n+1} &= z_n + hf_z(x_n\,, y_n\,, z_n) \end{aligned}\right\} \tag{4}$$

In the Lorenz system, $(f_x, f_y, and\ f_z)$ represented $(\dot{x}, \dot{y}, and\ \dot{z})$. In addition, the step size of the Ordinary Differential Equations (ODE) solver is denoted by h, and the present and next states are represented by (n, n+1 respectively). The chaotic samples that are adjacent to the signals that are generated exhibit a high degree of correlation.

2.3. Digitized Chaotic Signal

The following equation is used to convert a continuous signal to a semi-random and discrete-valued (SRDV) signal, disregarding the correlation between adjacent chaotic samples [33], [34]:

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

For example: if N is equal to 10, the generated SRDV signal is shown in the table 1.

Table 1. *SRDV signal*

n	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
SRDV	10330	63609	62729	31810	52448	9299	27641	60014	51919	62882

Table 2. *The sequence that was established in step 1*

6	1	7	4	9	5	8	3	10	2
9299	10330	27641	31810	51919	52448	60014	62729	62882	63609

Table 3. *Our sequence at step 4, N=10, DCS.*

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

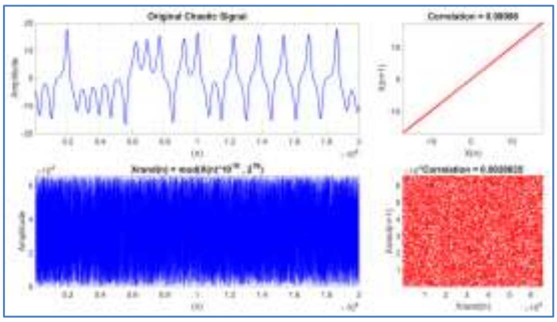

***Figure 2.** Digitized chaotic values and correlation neglecting.*

2.4. Ascending Sorting for SRDV

The resulting chaotic vector is arranged in ascending order. The sequence that was established in step 1 will provide the outcome given in table 2.

2.5. Generating Chaotic DCS Tables

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 permute data. Our sequence at step 4, N=10, DCS is given in table 3.

Simple designs with high scattering and low correlation are good. If the frame size is big, sorting N elements takes N(N-1)/2 comparisons, which can take a long time.

3. Measuring the Quality of Audio Signal

The proposed system performance will be evaluated by two types of testing: objective measurements, and subjective measurements. The objective testing, such as Mean Squared Error (MSE), Correlation (Corr), segmental spectral signal to noise ratio (SSSNR), Signal-to-Noise-Ratio (SNR), Linear Predictive Code (LPC) distance measure, and Cepstral Distance (CD) Measure. To resist the voice signal against the statistical attacks, (the correlation, SNR, SSSNR) for the encrypted signal should be reduced and the (MSE, DLPC, CD) should be increased.
Furthermore, the subjective testing mentioned above may be presented by some plots such as wave form of speech signal Fast Fourier Transform (FFT) plot, correlation plot, and spectrogram plot. These measures are defined as follows [10], [38], [39], [37]:

3.1. Mean Square Error (MSE)

The MSE value provides a way to analyze the accuracy of the model

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

The length of the original sound signal and the recovered or encrypted audio signal is equal to m.

3.2. The Correlation Coefficients (CC.)

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

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

X and Y refer to the original, recovered, or encrypted audio signals [35], [4], [39].

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

3.3. Segmental Spectral Signal to Noise Ratio (SSSNR)

The SSSNR is a quantity 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.

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

where Xi(k) & Yi(k) are the DFT of original signal & recovered signal respectively [8], [22].

3.4. Signal To Noise Ratio (SNR)

Utilized to ascertain the signal's quality. 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, and the signal will be considered more than noise once the value exceeds 0 dB

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

Where x is the voice signal that wasn't encrypted and y is the voice signal that was encrypted or decrypted [15], [40], [41].

3.5. Linear-Predicative-Code (LPC)

The LPC is a method that is primarily employed in the fields of audio signal processing and speech processing to represent the spectral envelope of a digital speech signal in compressed form. This methodology employs the information of a linear predictive model.

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

A and B vectors are the LPC coefficients for the original and encrypted or recovered audio signal. The autocorrelation matrix of the original audio signal block is V [15] [10].

3.6. Cepstral Distance Measure (CD):

In general, cepstral distance is applied to measure the similarity between two frames of speech signals

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

The cepstral coefficients are CC_x and CC_y for the original audio signal and the recovered or encrypted audio signal [37].

4. Simulation Results

This section delves into the simulation findings and system methodologies for voice encryption, utilizing the IDEA algorithm and enhancing encryption through the use of chaotic signals. We conducted two studies using Intel Core i7- 13700H laptop, 2.40 GHz CPU speed and 16GB of RAM. The simulation findings were developed using the MATLAB language (R2022a) and the Windows 11 operating system. Figure 3 displays the original voice signal for testing the proposed system.

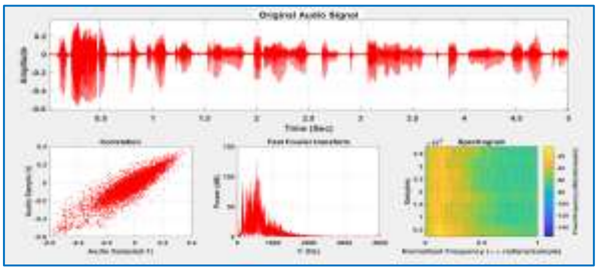

Figure 3. *Original audio signal used to testing the proposed system [1], [22], [42]*

4.1. Encryption Results Based on the Proposed System

Figure 7 shows 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.

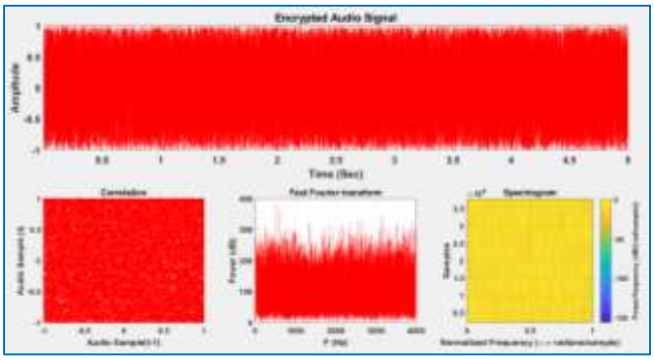

Figure 7. *Encryption first audio signal based on IDEA and chaotic flow system.*

Table 4. *Encryption results Based on IDEA and ChaoticFlow System.*

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

The simulation results in Table 1 showed some distortion (MSE=0.33783), almost no correlation (-0.00039), low signal-to-noise ratio (-22.78dB), and a delay that was fine (0.9252 sec).

Table illustrate the efficacy of the proposed encryption scheme that makes use of IDEA in conjunction with chaotic key generation. The decrypted audio signal has a low mean square error (MSE), a high signal-to-noise ratio (SNR), minimal distortion, strong correlation, and an acceptable delay. The achievement of these results demonstrates that the algorithm is capable of

4.2. Decryption Results Based on the Proposed System

Figure and

maintaining audio quality while simultaneously providing robust security.

Table 5. *Decryption results Based on IDEA and chaotic flow system.*

Audio Time	MSE	Corr.	SNR_{dB}	SSSNR_{dB}	Dlpc	CD	Delay (sec.)
5 sec	Zero	One	Infinity	Infinity	-Infinity	-Infinity	0.8622
10 sec	Zero	One	Infinity	Infinity	-Infinity	-Infinity	1.5822924
20 sec	Zero	One	Infinity	Infinity	-Infinity	-Infinity	2.909889
30 sec	Zero	One	Infinity	Infinity	-Infinity	-Infinity	4.5041742
50 sec	Zero	One	Infinity	Infinity	-Infinity	-Infinity	7.1939034

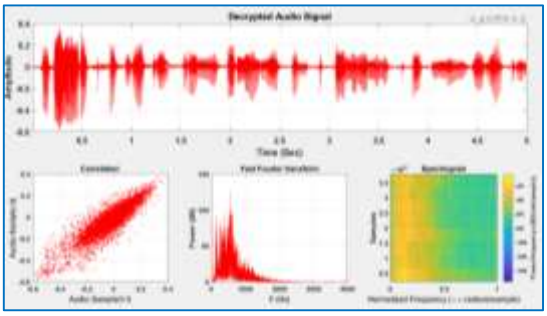

Figure 8. *Decryption first audio signal based on IDEA and chaotic flow system*

5. The Key Sensitivity and Key Space of the Proposed System

Table.

Table. Even changing one bit can have a big effect on decryption, changing MSE, correlation, and SNR. This level of security is very important for encryption systems. The results show that the algorithm is strong against brute-force attacks, which means it can be used for audio encryption.

6. The Proposed System's Key Space Calculation

The key space size is the total number of potential keys that can be employed with a cryptographic algorithm. The IDEA Key space is equivalent to 128 bits. However, the exact number of keys in chaotic systems cannot be determined, but it can be approximated in accurate largely, as demonstrated in the following equation:

$$Key\ Space(Henon) = \prod_{i=1}^{d} \frac{1}{S} * R(i) \qquad (12)$$

Where: d: The number of parameters and initial values for the chaotic system. S: Key Sensitivity for Chaotic Systems. R: The range of values for any parameter or initial value within which the system remains within the limits of chaos.

5.1. Key Sensitivity

Changing encryption keys affects both encryption and decryption, preventing decryption of the audio signal. A key bit change between encryption and decryption prevents audio signal retrieval, so sensitivity is essential for secure encryption. Any change in one bit of IDEA key bits or any slightly change in the initial value or parameters of the Lorenz chaotic system don't allow to recover the original audio signal, and remined the decrypted signals are similar to the encrypted audio signal, as shown in

The IDEA algorithm is very sensitive to changes in key bits or chaotic parameters, as shown in

In order 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. Lorenz system comprises three parameters (σ , r, and b) and three state vectors (x, y, and z).

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

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

Key Space over all the proposed system

$$All\ Keyds = \text{Key}_{IDEA} * Key_{\text{Lorenz}} \qquad (15)$$

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

A comparison of the key space size in bits for the proposed system and several other relevant articles is presented in **Hata! Başvuru kaynağı bulunamadı.**.Where TDS: is Time Domain Scrambling, FDS: is Frequency Domain Scrambling, 2DS: is Two-Dimensional Scrambling (combining between time TDS and FDS).**Hata! Başvuru kaynağı bulunamadı.** demonstrates that the suggested method utilizes a 427-bit key space, 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.

Table 6. *Key Sensitivity Results Based on Any Change in IDEA Key Bits or Chaotic Lorenz Parameters.*

Change Singel IDEA bit. Or Initial Condition or Parameter about 10^{-15}	**MSE**	**Corr.**	**SNR (dB)**	**SSNR (dB)**	**Dlpc**	**CD**
IDEA Key bit # 59	0.33921	-0.00275	- 9.232	-19.43	20.152	8.289
IDEA Key bit #2	0.33916	0.00239	-18.221	-19.441	20.164	8.293
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
$\Delta_x(\text{Lorenz}) = 10^{-15}$	0.33278	0.00168	-17.994	-19.332	20.151	8.282
$\Delta_y(\text{Lorenz}) = 2 * 10^{-15}$	0.33214	-0.00315	-19.882	-19.328	20.155	8.282
$\Delta_z(\text{Lorenz}) = 5 * 10^{-15}$	0.32869	0.00434	-17.32	-19.281	20.174	8.279
$\Delta_\sigma(\text{Lorenz}) = 10^{-15}$	0.32726	-0.00111	-14.696	-19.249	20.144	8.272
$\Delta_r(\text{Lorenz}) = 2 * 10^{-15}$	0.32864	0.00262	-18.683	-19.28	20.179	8.281
Without Change	0	1	Inf	Inf	-Inf	-Inf

Table 7. *Comparative analysis of the proposed system with other encryption schemes in terms of performance metrics and key-space.*

Ref.	Corr.	SNR_{dB}	SSSNR_{dB}	LPC	CD	Entropy	Key-space
IDEA	0.0043	-18.052	-19.423	20.155	8.2890	14.931	128 Bits
[1]	-	-	-1.944	0.6723	3.3369	15.113	212 Bits
[13]	-	-	- 20.7803	0.9998	4.2583	15.142	266 Bits
[32]	-	-14.009	-	-	-	14.891	280 Bits
[20]	-0.0017	-11.8707	-	-	-	-	$\mathbf{10^{84}}$
[43]	0.0032	-10.4925	-	-	-	-	180 Bits
[26]	0.00952	-17.182	-18.953	18.339	8.1936	15.323	328 Bits
TDS [5]	-	-	0.9754	0.6532	2.4273	-	-
FDS [5]	-	-	-0.2735	0.5823	2.5095	-	-
2DS [5]	-	-	-1.9543	0.6132	3.2369	-	-
Our	0.00433	-18.052	-19.423	20.172	8.2840	15.612	428 Bits

7. Conclusions

The proposed encryption system integrates the effectiveness of the IDEA algorithm with the enhanced security provided by 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 $(x_0, y_0, z_0, \sigma, r\ and\ b)$ 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 method may also be applied to additional block blades and integrated with other security measures, including information concealment or watermarking.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] A. Mahdi, A. K. Jawad, S. S. Hreshee, A. Mahdi, and A. K. Jawad, (2016). Digital Chaotic Scrambling of Voice Based on Duffing Map, *Commun. Eng. J.*, vol. 1(2), 16–21, doi: 10.11648/j.cej.20160102.11.

[2] M. J. Orceyre and R. M. Heller, (1978) An Approach to Secure Voice Communication Based on the Data Encryption Standard, *IEEE Commun. Soc. Mag.*, vol. 16(6), 41–50, doi: 10.1109/MCOM.1978.1089785.

[3] N. J. Corron and D. W. Hahs, (1997). A New Approach to Communications Using Chaotic Signals, *IEEE Trans. circuits Syst.*, vol. 4(1) , 373–382, doi: 10.17950/ijer/v3s7/711.

[4] A. K. Jawad, G. Karimi, and M. Radmalekshahi, (2024). A Novel Digital Audio Encryption Algorithm Using Three Hyperchaotic Rabinovich System Generators, ARO-The Sci. J. Koya Univ., vol. XII(2), 234–245, 2024, doi: 10.14500/aro.11869.

[5] M. J. M. Ameen and S. S. Hreshee, (2023) Security analysis of encrypted audio based on elliptic curve and hybrid chaotic maps within GFDM modulator in 5G networks, *Bull. Electr. Eng. Informatics,* vol. 12(6), 3467–3479, doi: 10.11591/eei.v12i6.4913.

[6] B. Rahul, K. Kuppusamy, and A. Senthilrajan, (2023). Chaos-based audio encryption algorithm using biometric image and SHA-256 hash algorithm, *Springer US.* vol. 82(28). doi: 10.1007/s11042-023-15289-x.

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

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

[9] H. N. Abdullah, S. S. Hreshee, and A. K. Jawad, (2015). Design of Efficient noise reduction scheme for secure speech masked by chaotic signals, *J. Am. Sci.*, vol. 11(7), 49–55.

[10] H. N. Abdullah, S. S. Hreshee, and A. K. Jawad, (2016). Noise Reduction of Chaotic Masking System using Repetition Method. https://www.researchgate.net/publication/291356303

[11] W. Al Nassan, T. Bonny, and A. Baba, (2020). A New Chaos-Based Cryptoystem for Voice Encryption, *2020 3rd Int. Conf. Signal Process. Inf. Secur. ICSPIS 2020,* 1–4, doi: 10.1109/ICSPIS51252.2020.9340132.

[12] T. Bonny, W. Al Nassan, and A. Baba, Voice encryption using a unified hyper-chaotic system, *Multimed. Tools Appl.,* vol. 82(1), 1067–1085, 2023.

[13] A. K. Jawad, H. N. Abdullah, and S. S. Hreshee, (2018). 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,* 7–12. doi: 10.1109/ICASEA.2018.8370947.

[14] E. A. R. E. A. E. A. R. Hussein, M. K. M. K. Khashan, and A. K. A. K. Jawad, (2020). A high security and noise immunity of speech based on double chaotic masking, *Int. J. Electr. Comput. Eng.*, vol. 10(4), 4270–4278, doi: 10.11591/ijece.v10i4.pp4270-4278.

[15] 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(3), 257–264, 2018, doi: 10.15866/irecap.v8i3.13541.

[16] M. Baykara, R. Das, and G. Tuna, (2017). A Novel Symmetric Encryption Algorithm and its Implementation Muhammet, *Turkish J. Sci. Technol.*, vol. 12(1), 5–9.

[17] S. Basu, (2011). International Data Encryption Algorithm (Idea) – *A Typical Illustration*, vol. 2(7), 116–118.

[18] S. Patil and V. Bhusari, (2014). An Enhancement in International Data Encryption Algorithm for Increasing Security, *Int. J. Appl. or Innov. Eng. Manag.*, vol. 3(8), 64–70.

[19] A. Mostafa, N. F. Soliman, M. Abdalluh, and F. E. Abd El-Samie, (2016). Speech encryption using two dimensional chaotic maps, *2015 11th Int. Comput. Eng. Conf. Today Inf. Soc. What's Next?, ICENCO 2015*, 235–240, doi: 10.1109/ICENCO.2015.7416354.

[20] S. M. H. Alwahbani and E. B. M. Bashier, (2013). Speech scrambling based on chaotic maps and one time pad, Proc. - *2013 Int. Conf. Comput. Electr. Electron. Eng. Research Makes a Differ. ICCEEE 2013*, 128–133, doi: 10.1109/ICCEEE.2013.6633919.

[21] S. Pati, M. Mishra, and J. Rout, (2024). Securing Audio with 3D-Chaotic Map Based Hybrid Encryption Technique, *Int. J. Comput. Digit. Syst.*, vol. 16(1), 1–11.

[22] A. Mahdi, A. K. Jawad, and S. S. Hreshee, (2016). Digital chaotic scrambling of voice based on duffing map, *Int. J. Inf. Commun. Sci.*, vol. 1(2), 16–21.

[23] I. Jomaa, W. M. Saleh, R. R. I. Hassan, and S. H. H. Wadi, (2023). Secured drone communication based on Esalsa20 algorithm and 1D logistic map, *Indones. J. Electr. Eng. Comput. Sci.,* vol. 29(2), 861–874, doi: 10.11591/ijeecs.v29.i2.pp861-874.

[24] Ameer k. Jawad; Gholamreza Karimi; Mazdak Radmalekshahi, (2024). 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*, 1–6. doi: 10.1109/AEST63017.2024.10959812.

[25] M. Khalid, E. A. E. A. R. Hussein, Ameer K. Jawad, and A. K. Jawad, (2019). Digital Image Encryption Based on Random Sequences and XOR Operation, *J. Eng. Appl. Sci.*, vol. 14(8), 10331–10334, 2019.

[26] B. W. H. A.-Z. S. S. Hreshee, (2024). 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,* 1–6.

[27] A. A. Abdul-Kareem and W. A. M. Al-Jawher, (2024). An image encryption algorithm using hybrid sea lion optimization and chaos theory in the hartley domain, *Int. J. Comput. Appl.*, 1–14.

[28] Zahra Saeidi, A. Yazdi, S. Mashhadi, and M. Hadian, (2023). Introducing a New Evaluation Criteria for EMD- Base Steganography Method, *Electron.*, vol. 12, 1–13, doi: 10.1007/978-3-642-19542-6_51.

[29] O. Elnoamy et al. (2023), “Dynamic Analysis and Robust Control of a Chaotic System with Hidden Attractor, *Int. J. Electr. Comput. Eng.*, vol. 13, 38–43, 2023, doi: 10.33971/bjes.23.1.8.

[30] M. Moghtadaei and M. R. Hashemi Golpayegani, (2012). Complex dynamic behaviors of the complex Lorenz system, *Sci. Iran.*, vol. 19(3), 733–738, doi: 10.1016/j.scient.2010.11.001.

[31] D. Raghuvanshi, K. Joshi, R. Nandal, H. Sehrawat, S. Singh, and S. Singh, (2024). Improved security with novel M-Log chaos steganography algorithm for huffman compressed english text, *Multimed. Tools Appl.*, 1–24.

[32] Ameer K. Jawad, Wa’il a. H. Hadi, and Hyayder F. Y. Husseain, (2016). Enhancement of Image Transmission Using Chaotic Interleaver over Wireless Sensor Network. www.ijntr.org

[33] X. Li, H. Yu, H. Zhang, X. Jin, H. Sun, and J. Liu, (2020). Video encryption based on hyperchaotic system, *Multimed. Tools Appl.*, vol. 79(33–34), 23995–24011, doi: 10.1007/s11042-020-09200-1.

[34] A. R. Alharbi et al. (2022), A New Multistage Encryption Scheme Using Linear Feedback Register and Chaos-Based Quantum Map, *Complexity*, 2022, doi: 10.1155/2022/7047282.

[35] A. H. Elsafty, M. F. Tolba, L. A. Said, A. H. Madian, and A. G. Radwan, (2018). FPGA Speech Encryption Realization Based on Variable S-Box and Memristor Chaotic Circuit, *IEEE, Int. Conf. Microelectron. ICM*, 152–155, doi: 10.1109/ICM.2018.8704019.

[36] A. H. ElSafty, M. F. Tolba, L. A. Said, A. H. Madian, and A. G. Radwan, (2021). Hardware realization of a secure and enhanced s-box based speech encryption engine, *Analog Integr. Circuits Signal Process.*, vol. 106(2), 385–397, , doi: 10.1007/S10470-020-01614-Z.

[37] S. B. Sadkhab, A. M. Raheema, and S. M. A. Sattar, (2019). Design and Implementation Voice Scrambling Model Based on Hybrid Chaotic Signals, IEEE, *1st Int. Sci. Conf. Comput. Appl. Sci. CAS 2019*, 193–198, doi: 10.1109/CAS47993.2019.9075626.

[38] W. A. Al-Musawi, M. A. A. Al-Ibadi, and W. A. Wali, (2023). Artificial intelligence techniques for encrypt images based on the chaotic system implemented on field-programmable gate array, *IAES Int. J. Artif. Intell.*, vol. 12(1), 347–356, doi: 10.11591/ijai.v12.i1.pp347-356.

[39] H. Wen, L. Ma, and L. Liu, (2022). High-quality restoration image encryption using DCT frequency-domain compression coding and chaos, *Sci. Rep.*, vol. 12(1), 1–17, doi: 10.1038/s41598-022-20145-3.

[40] F. J. Farsana, V. R. Devi, and K. Gopakumar, (2019). An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic keystreams, *Appl. Comput. Informatics*, doi: 10.1016/j.aci.2019.10.001.

[41] H. Elkamchouchi, W. M. Salama, and Y. Abouelseoud, (2020). New video encryption schemes based on chaotic maps, *IET Image Process.*, vol. 14(2), 397–406, doi: 10.1049/iet-ipr.2018.5250.

[42] Z. Ali, K. Saleem, R. Brown, N. Christofides, and S. Dudley, (2022) Performance Analysis and Benchmarking of PLL-Driven Phasor Measurement Units for Renewable Energy Systems, *Energies*, vol. 15(5), doi: 10.3390/en15051867.

[43] S. Mokhnache, M. E. H. Daachi, T. Bekkouche, and N. Diffellah, (2022). A Combined Chaotic System for Speech Encryption, *Eng. Technol. Appl. Sci. Res.*, vol. 12(3), 8578–8583, doi: 10.48084/etasr.4912