

Speech Encryption by Splitting Data and Applying Chaotic Image Encryption Algorithms

Nagham Malik Abd Ali^{1*}, and Dr. Tarik Zeyad Ismaeel²

^{1*} Department of Electrical Engineering, College of Engineering, University of Baghdad, Baghdad, Iraq. nagham.abd2402m@coeng.uobaghdad.edu.iq, <https://orcid.org/0009-0006-4548-6093>

² Professor, Department of Electrical Engineering, College of Engineering, University of Baghdad, Baghdad, Iraq. tarik.z@coeng.uobaghdad.edu.iq, <https://orcid.org/0000-0002-4003-9968>

Received: September 15, 2025; Revised: October 21, 2025; Accepted: December 17, 2025; Published: February 27, 2026

Abstract

The rapid growth of computer communications and multimedia has created a pressing need for the safeguarding of this information instantaneously. For safeguarding the information carried from hackers and maintaining its confidentiality unbroken, audio signal security has been one of the leading fields of research in recent times. A new speech signal coding is introduced in this paper. This coding has been done on the principle of converting the audio signal into a digital image and then encrypting it for ensuring confidentiality of data and prevention from tampering or interception. This operation employs different chaotic systems (e.g., the logistical map, Henon map, and Lorenz system) that are highly sensitive to minor conditions. To ensure that the image is secured to be sent, encryption techniques are used such that it becomes hard for an attacker to decrypt the encrypted image. Upon decoding the encrypted image with the inverse encoding algorithm, the system restores the original sound signal. It reconverts digital information into an aural signal through restored keys. The basis of system strength and search method for encryption is the integration of voice signal processing technologies and chaotic encryption based on chaotic systems. The proposed approach possesses the ability to improve resistance to cryptanalysis attacks and improve security during transmission.

Keywords: Audio Encoder, Voice-To-Picture, Chaotic System, EX-OR, Chaotic Logistic Map, Henon Map, Lorenz System, Encrypt Images.

1 Introduction

Multimedia has gained increasing significance with the development of communication technology. Greater security for digital information is urgently needed. Building more robust systems to be capable of fending off cyberattacks has been a priority. Many researchers have been involved in using encryption with chaotic systems and applications to images and signals. On top of that, they highlighted the usefulness of a logistics map in building robust encryption keys. It is very difficult to forecast the action of this map. The researchers enhanced the level of security by gathering numerous techniques. Mansor tested the chaotic system encryption method application to image security in 2016. showing the manner

through which various encryption techniques could be integrated with the logistics map for enhancing communication systems' security (Mansor, 2016).

Munir, (2024) noted that the integration of different chaotic systems, say, the Lorenz system and the Henon map, would enhance the level of security during the encryption process. The integration of the two technologies, they noted in their research, further boosts the level of complexity entailed in resisting cyberattacks and attempted unauthorized modification or retrieval. Alaklabi et al., (2024) confirmed that encryption processes ought to be based on complex algorithms. To provide greater security while working with sensitive information, they used swap networks.

Some experiments were also conducted to utilize chaotic systems in encrypting sound signals, has a study where these techniques were applied to secure information during transmission through digital networks, as quoted by Sathiyamurthi & Ramakrishnan, (2017). It demonstrated that it was possible to preserve the quality of the recovered signal unaltered by using chaotic encryption methods. It also improved the secrecy level. Mohi et al., (2025) also suggested a model in which they employed the Henon system and nonlinear encryption methods. They strengthened the regime's cybersecurity measures here (Herbadji et al., 2024).

A comprehensive review of the latest advances in data encryption from random systems was provided by Luo et al., (2024). It focused on reducing computation resource consumption and improving encryption efficiency.

According to current studies, using three-dimensional maps might be the way forward. It enhances encryption techniques with more strength and efficiency. According to Hosny et al.'s study (Hosny et al., 2024).

The purpose of the work presented here is to create a strong sound signal encryption technique. Chaotic systems, which are thoroughly penetrating and very sensitive even to minor changes in their initial parameters, are utilized by them. Therefore, they are difficult to hack and decrypt if the hacker is not aware of the encryption scheme's parameters.

Relishing the most widely accepted ideas discussed in recent research was the main goal of the project outlined here. This process involves transforming the audio signal into an 8-bit image. The image is subjected to encoding procedures. One system split the image information into two parts, and each was processed by a different system.

The information is decrypted. It retrieves the original sound image. The decrypted image is then converted to an audio signal (Maazouz et al., 2022).

This integrated system shows a new concept of making use of the properties of chaotic systems, which have been used successfully in recent studies. Besides its function in the security of audio signals.

2 Methodology

All steps of the process are performed in MATLAB 2024 software.

1. Convert Sound to Image

- i. Digitally sampling the signal once it has been loaded. As the process should be kept as basic as possible, it is performed on a mono channel. with reference to keeping a mount of samples in consideration.

- ii. The initial signal levels are typically in the range $[-1,1]$. They are normalized to the range $[0,1]$ and further normalized by multiplication with 255. Then, the values so obtained are rounded off and are made into integer values to accommodate the pixel value scheme. This is the dynamic range of the 8-bit digital image's pixel values. Thus, audio data can be employed as pixel values for the image.
- iii. To transform the information into an image. The no. of samples must be calculated. The square root of the number of samples is used in order to calculate the area of a square picture. If missing, zeros are padded as the alternative.
- iv. A square monochromatic matrix is formed by reconstructing resultant vector.
- v. Accordingly, we place each original sample in its rightful position throughout the image. During a process of transforming an image, it is absolutely necessary that there be neither data loss nor distortion.
- vi. To prepare it for subsequent procedures, the matrix is scanned as an image and saved as shown in figure 1.

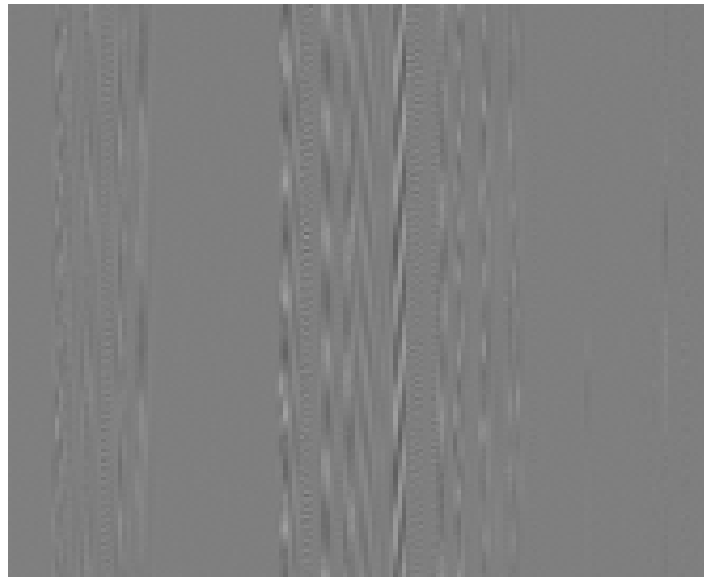


Figure 1: Input speech image

2. Split Image Data

Such a split process complicates the process of encryption. Thus, increasing the system's power and threat-advantageous efficacy improves its security.

To Split the Image Data

- i. The resulting image from the audio is accessed in matrix form first.
- ii. The matrix is then transformed into a vector (Talib Mangi et al., 2023).
- iii. Such a vector is split into two varied groups:

L_1 : represents the pixels of the odd index.

L_2 : Represents the pixels of the even index.

In preparation for applying a distinct encryption process to every cluster, this segmentation is the essential first step.

3. Encryption Stage

Chaotic Generators

The image is encoded using three chaotic systems:

a. Logistics Chaotic Map

- It is one of the chaotic maps that is widely used is a random nonlinear system. A random series of L1 and L2 is generated separately and with different values using the equation (Jerjees et al., 2020):

$$x_{n+1} = r \times x_n(1 - x_n) \quad (1)$$

Where:

x_n : the system range of (0-1).

$n = 1, 2, \dots, N$.

r : bifurcation parameter of the system with a range of (0-4) (Mansor, 2016).

Chaotic behavior depends on the value of r . where it behaves almost oscillatory when its value is from (0 - 3), then it begins to branch at range (3 - 3.75). Finally takes the chaotic behavior starting from (3.75) (Abdulameer et al., 2022). As it approaches(4), r increases to reach its peak value, as seen in figure 2 (Mansor, 2016; Sathiyamurthi & Ramakrishnan, 2017). The resulting values are converted to integers.

Figure 2 illustrates the dynamic behavior of the chaotic logistic map.

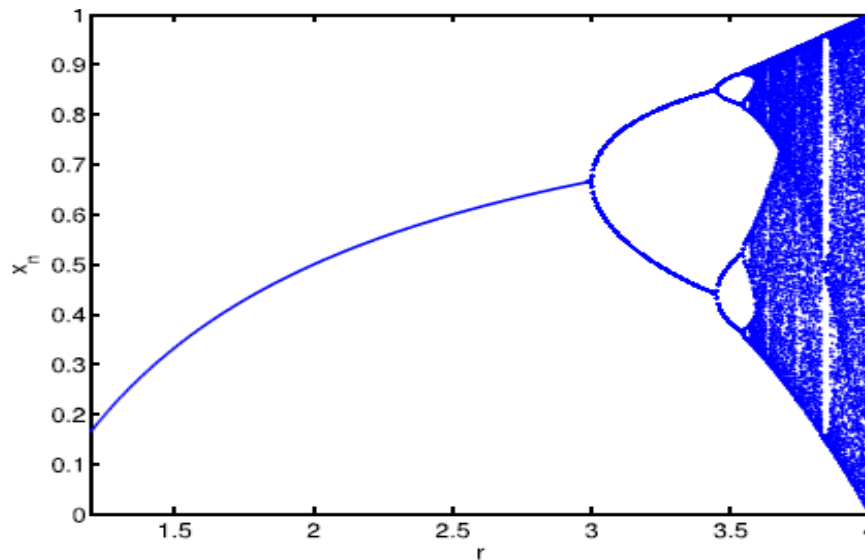


Figure 2: Logistic map bifurcation diagram (Jerjees et al., 2020; Raghuvanshi et al., 2020)

- Create a logistics chaos map (Talib Mangi et al., 2023).
 - Sequence Generation: The logistic map is employed to generate a sequence of real-valued numbers using Equation (1), where: $r = 3.99$, $x0_For_L1 = 0.5$, $x0_For_L2 = 0.7$.
 - This sequence is iterated to yield a number of elements equal to the total number of items in each group

- iii. Mapping and Folding: The real-valued outputs of the logistic map are scaled by multiplying them with 255. The resulting values are then folded using the modulus operation with respect to 255 to ensure that all values remain strictly within the range [0, 255].
- iv. Data Representation: To prepare the values for further encryption or embedding processes, the sequence is cast into an 8-bit unsigned integer format (uint8), which facilitates compatibility with standard image and multimedia data structures.

Henon Map

- Used to generate an additional encryption key for the L1 group. It is a chaotic two-dimensional map Figure 3 showing its equations below (Mansor, 2016):

$$x_{n+1} = 1 - a(x_n)^2 + y_n \quad (2)$$

$$y_{n+1} = bx_n \quad (3)$$

where a and b are the parameters of this map and (x_n, y_n) represents the state of the system at iteration n. The system will show chaotic behavior where:

a=0.3 and b=1.4 (Mansor, 2016).

That is, the Henon map works as a chaotic map with a range of (1.07 to 1.4). it is a fixed value in relation to other values (Hosny et al., 2024).

Figure 3 illustrates the dynamic behavior of the Henon chaotic map, as computed numerically in MATLAB.

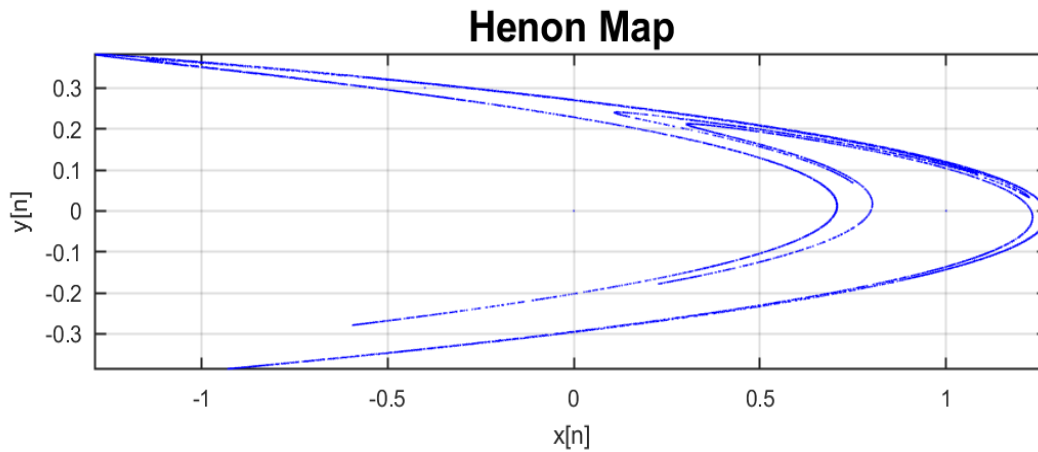


Figure 3: Chaotic behavior of henon map

- Generate an extra key from the 2D Henon map for Group 1.
 - i. Parameters a = 1.4 and b = 0.3 are used.
 - ii. Specifies the initial values $x_0_henon=0.1$ and $y_0_henon=0.3$.
 - iii. The `henon_key` function according to equations (2) and equation (3) generates a key corresponding to the number of L1 elements.

Parameters used in the Henon map were chosen to operate under the existing chaotic functionality of the system. The parameters a = 1.4 and b = 0.3 are recognized to produce a chaotic but stable attractor. The initial values $(x_0, y_0) = (0.1, 0.3)$ have been chosen in order not to converge to periodic orbits and ensure maximized randomness. These parameters are appropriate for encryption, since they generate

pseudo-random, non-cyclic responses with high initial condition sensitivity, which renders the cryptographic scheme more secure and robust.

Lorenz System

- The Lorenz system is used to create a second encryption key for the L2 set using numerical integration methods. The Lorenz system is governed by the following three first-order differential equations, which model the long-term evolution of the Lorenz attractor (Hosny et al., 2024; Mansor, 2016; Sathiyamurthi & Ramakrishnan, 2020).

$$\dot{x} = \delta(y - x) \quad (4)$$

$$\dot{y} = -xz + \rho x - y \quad (5)$$

$$\dot{z} = xy - \beta z \quad (6)$$

x , y , and z : state vectors of the system, β , ρ , and δ : System Parameters (Mansor, 2016).

Where the intervals for variables x , y , and z are given as $-60 \leq x \leq 60$, $-60 \leq y \leq 60$, and $-60 \leq z \leq 60$. For chaotic behavior, parameters δ , ρ , and β values are $\delta = 10$, $\rho = 28$, and $\beta = 8/3$, respectively (Hosny et al., 2024).

Lorenz's chaotic system has several advantages. including unpredictability, confusion, and proliferation-like characteristics.

Sensitivity to primary conditions and factors, complex dynamic behavior involving multiple control variables (Mansor, 2016).

As a result, Lorenz-based encryption has a high score of unpredictability and a huge master space (Hosny et al., 2024).

This system is produced by the so-called the butterfly effect, as shown in the figure 4. This means that minor causes produce large effects. i.e., any difference in the initial values to a large difference in subsequent values (Mansor, 2016).

Figure 4 illustrates the Lorenz system trajectory.

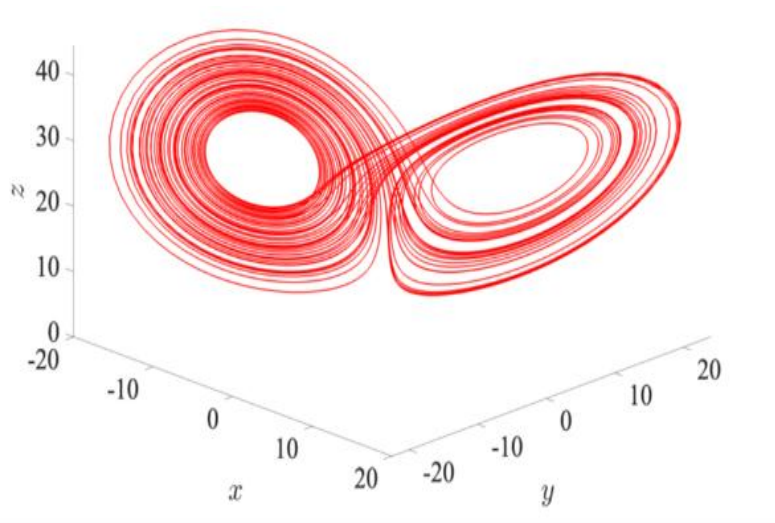


Figure 4: Lorenz system trajectory (Luo et al., 2025)

- Generate an extra key from the Lorenz 3D system for group 2:

- i. Determine the three system parameters: $\beta=8/3$, $\rho=28$, and $\delta=10$.
- ii. Determine the initial values of the system with a time integration step: $x_0=1$, $y_0=1$, $z_0=1$.
- iii. The Lorenz key function, according to equations (4), equation (5), and equation (6), produces dimensional keys corresponding to the number of L2 elements.

The initial conditions for the Lorenz system were selected such that a highly chaotic and random series was generated. That is, the default values of $\sigma = 10$, $\rho = 28$, and $\beta = 8/3$ (Hosny et al., 2024) were utilized since they are in the chaotic regime of the Lorenz system. Additionally, the initial values $(x_0, y_0, z_0) = (1.5, 2.5, 15)$ are adequate in ensuring sensitivity to initial values, which is important for efficient encryption. The values ensure that any slight change of the initial parameters yields significantly different chaotic sequences, ensuring security.

A. Merge Keys

The keys of logistics map and the Henon map are integrated together as well as logistics map with the Lorenz system as shown below:

- i. For L1: The logistics map key is combined with the Henon map key by the EX-OR process to produce the final key key_L1.
- ii. For L2: The second logistics map key is combined with the Lorenz key in the same way to produce the final key, key_L2.

B. Pixel Encoding

- i. Applies the EX-OR operation to the pixels specified by L1 using the key_L1 key to encode the group L1.
- ii. We apply the EX-OR operation to the pixels specified by L2 using the key_L2 key to encode the L2 group.

C. Image Reshaping

The resulting vector is reconstituted as an array with the same dimensions as the original image to produce the encoded image shown in figure 5.

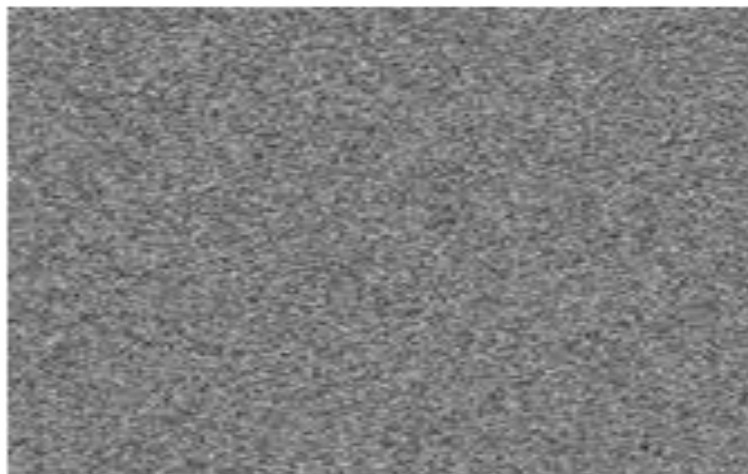


Figure 5: Encrypted speech image

4. Decryption Stage

- i. The encoded image is read and converted to a vector.
- ii. Regenerate the keys of each `key_L1_deckey` and `key_L2_deckey` group with the same transactions of the systems used in the encryption process.
- iii. Perform an EX-OR operation between the keys `key_L1_deckey` and `key_L2_deckey` and the groups of 1 and 2, respectively, where the original data of the image is retrieved.
- iv. Converts the resulting vector to a matrix to reproduce the image.

Figure 6 shows the resulting image from the decoding process.

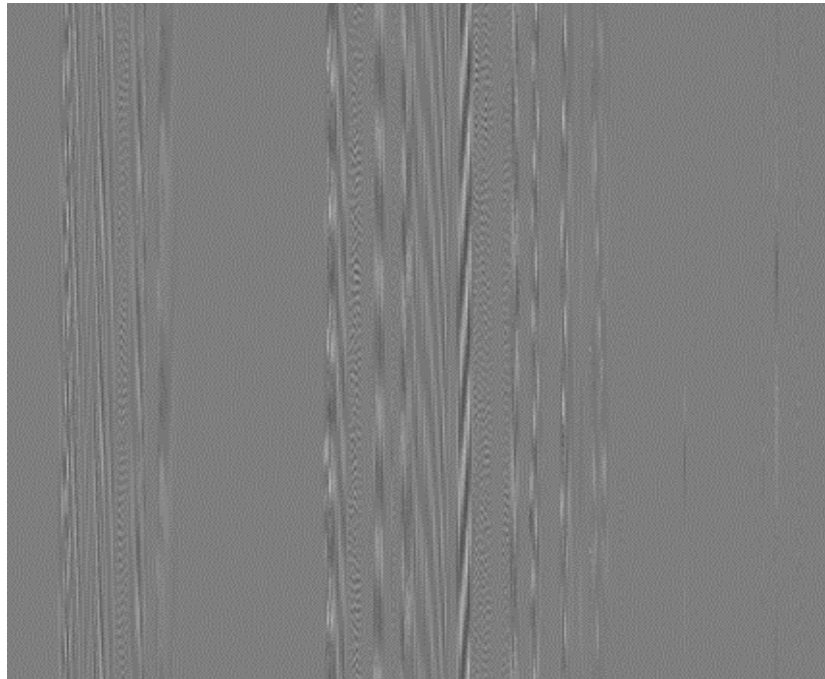


Figure 6: Decrypted speech image

5. Audio Retrieval Phase

The last stage of the system is to retrieve the sound from the decoded image and is done in several steps:

- i. The sound data is retrieved from the only channel in the image because the image is gray.
- ii. Converts a pixel matrix to a vector. The added zeros of the filling are omitted according to the number of original samples stored. Thus, none of the padding data is retained when retrieving the audio.
- iii. Resize numeric values to $[-1, 1]$ for voice data recovery.
- iv. Save audio within a specific file.

Figure 7 demonstrates the methodology of converting sound to image and encoding the resulting image using chaotic systems.

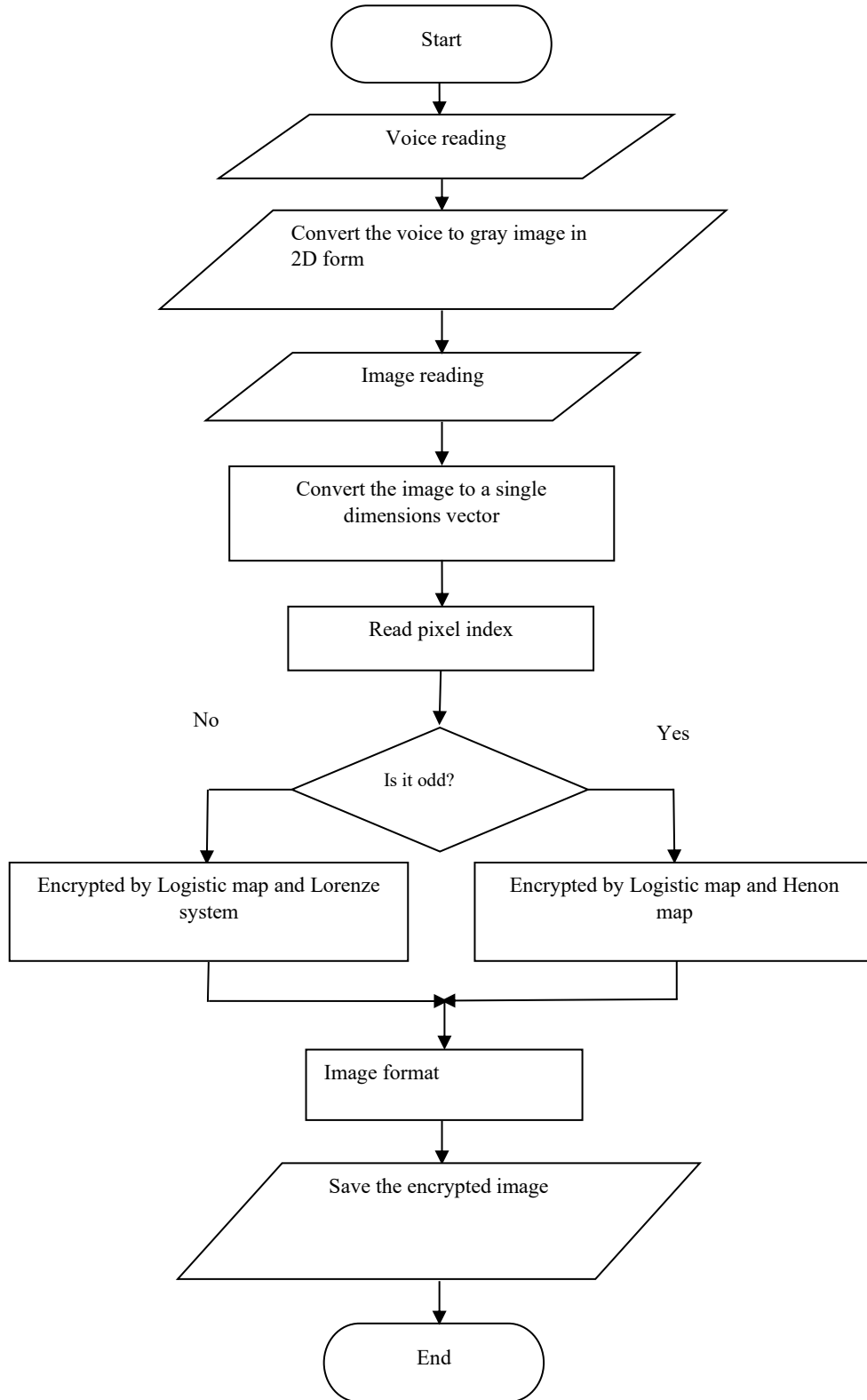


Figure 7: Flowchart of encrypted phase

Figure 8 demonstrates the methodology for decoding the encoded image that resulted from the encoding phase and retrieving the sound from the decoded image.

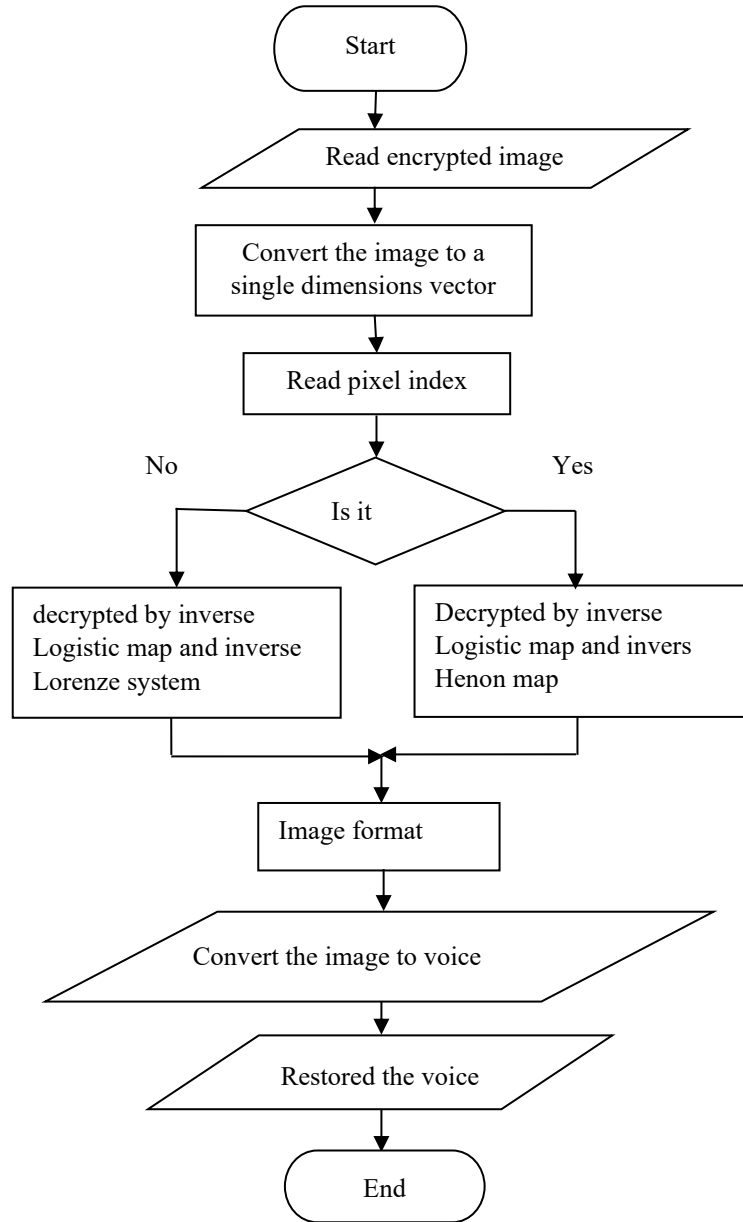


Figure 8: Flowchart of decrypted phase

6. Pseudo-Code

Input: Audio signal A of length L

Output: Encrypted image E, Decrypted audio A'

Step 1: Convert audio signal A to 8-bit unsigned integers

A_scaled = scale A from [-1,1] to [0,255]

Pad A_scaled with zeros to make a perfect square

Step 2: Reshape padded A_scaled into image matrix Img (dim x dim)

Save Img as PNG lossless image

Step 3: Read Img and flatten it into pixel vector P

Divide P into:

L₁: Odd-indexed pixels

L₂: Even-indexed pixels

Step 4: Generate encryption keys

For L₁:

Use Logistic Map and Henon Map → key_L₁

For L₂:

Use Logistic Map and Lorenz System → key_L₂

Step 5: Encrypt the image

P[L₁] = P[L₁] XOR key_L₁

P[L₂] = P[L₂] XOR key_L₂

Reshape encrypted P to form encrypted image E

Step 6: To decrypt:

Re-generate keys as in Step 4

Encrypted_P[L₁] = Encrypted_P[L₁] XOR key_L₁

Encrypted_P[L₂] = Encrypted_P[L₂] XOR key_L₂

Recover original image and reshape it

Step 7: Recover audio:

Flatten decrypted image and discard padded zeros

Convert values from [0,255] back to [-1,1]

Save as restored audio A'

7. Complexity Analysis

i. Rough analysis based on the steps:

Table 1 presents the complexity analysis of the steps.

Table 1: Complexity analysis

Stage	Operation	Approximate Time
Sound -to-Image Conversion	Scaling + Padding + Reshape	O(n)
Generating Hennon/Lorenz Logistics Keys	Loops For each element in L ₀ /L ₁	O(n)
Encryption using EX-OR	Loop over n	O(n)
Re-encoding and image decoding	Similar to encryption	O(n)
Image-to-Sound Conversion	Flatten + Normalize	O(n)

i. Time of the algorithm:

$O(n) = T(n)$

Where:

n : is the number of audio samples or the number of pixels.

ii. Memory Used

It stores images, switches, and arrays that are approximately n length, thus:

$O(n) = \text{Space}$

3 Experiments And Results

All the experiments performed using the suggested encryption algorithm were executed on a home machine with the below specifications:

Processor: Intel Xeon CPU E3-1505M v5 at a base clock speed of 2.81 GHz, and RAM: 16 GB.

The process, encryption and decryption functions, and time and statistical testing were performed for the software module on Windows 10 using MATLAB R2024a. After running the algorithm for a collection of sound samples, the following outcomes were achieved in terms of security, efficiency, and time efficiency:

1. It successfully converted audio into monochrome 8-bit image.
2. The sound obtained from the encrypted image is thoroughly unreadable based on the success of the encryption process such that the encrypted image cannot be written to except in the holder of the encryption keys.
3. The image was successfully recovered by the image decoding process having been solved. Furthermore, audio data can be precisely and distinctly obtained from the decrypted image.
4. System sensitivity: The result showed that the system was sensitive to a slight change in the initial values of the transaction. As a result, its data became harder to change or hack.

Tables 2, 3, 4, 5, 6 and 7 below also show the tests result:

- i. Correlation test (Mokhnache et al., 2022; Sathiyamurthi & Ramakrishnan, 2017):

Table 2 presents the test results of correlation for four speech samples.

Table 2: Correlation test

No	Speech sample in wav	Encryption speech	Decryption speech
1	Audio1	0.0020	0.9993
2	Audio2	-0.0018	0.9997
3	Audio3	-0.0015	0.9984
4	Audio4	-0.0003	0.9994

- ii. SNR & PSNR Tests (Sathiyamurthi & Ramakrishnan, 2017):

Table 3 presents the test results of SNR and PSNR for four speech samples.

Table 3: SNR & PSNR tests

No.	Speech sample in wav	Duration in second	SNR in dB	PSNR in dB
1	Audio1	5	28.2434	29.17
2	Audio2	4	32.9688	27.29
3	Audio3	3	24.9467	36.47
4	Audio4	1	29.4796	29.95

- i. Spectral Distortion (Sreedharan & Eswaran, 2019):

Table 4 presents the test results of spectral distortion for four speech samples.

Table 4: Spectral distortion

No.	Speech sample in wav	Spectral Distortion in dB
1	Audio1	27.46
2	Audio2	23.12
3	Audio3	24.02
4	Audio4	21.57

ii. MSE (Al-Rifae et al., 2023; Chicco et al., 2021):

Table 5 presents the test results of mean squared error for four speech samples.

Table 5: MSE test

No	Speech sample in wav	Encryption	Decryption
1	Audio1	0.3409	0.0000
2	Audio2	0.3494	0.0000
3	Audio3	0.3389	0.0000
4	Audio4	0.3406	0.0000

iii. Time efficiency (Gill et al., 2025):

Table 6 presents the test results of time efficiency for four speech samples.

Table 6: Time efficiency

No.	Speech sample in wav	Duration in second	The conversion time for audio to image in second	Encryption time in second	Decryption time in second
1	Audio1	5	0.0586	0.0702	0.1406
2	Audio2	4	0.0780	0.0718	0.1623
3	Audio3	3	0.0631	0.0636	0.1198
4	Audio4	1	0.0505	0.0442	0.0983

iv. Entropy (Mohi et al., 2025):

Table 7 presents the test results of entropy for four speech samples.

Table 7: Entropy

No.	Speech sample in wav	Entropy (bits / sample)
1	Audio1	7.9994
2	Audio2	7.9991
3	Audio3	7.9991
4	Audio4	7.9977

4 Comparison

A comparison between the new method and earlier methods was conducted in the form of test results on SNR, PSNR, and correlation, as shown in Table 8.

Table 8: Comparison

	Speech sample	SNR in Db	PSNR In dB	Correlation	
				Encryption	Decryption
The proposed method	1	28.24	46.97	0.0020	0.999
	2	32.97	50.48	0.0018	1.000
	3	24.95	44.86	0.0015	0.998
	4	29.48	47.59	0.0003	0.999
(Sathiyamurthi & Ramakrishnan, 2017)	1	33.7464	59.7989	0.0233	0.999
	2	32.5781	59.2281	0.0384	0.999
	3	33.0569	59.6304	0.0157	1
	4	34.7112	62.3189	0.0119	1
(Sathiyamurthi & Ramakrishnan, 2020)	1	-	-	0.0386	0.9958
	2	-	-	-0.0974	-0.9925
	3	-	-	0.0312	0.9917
	4	-	-	-0.0643	-0.9896
	5	-	-	0.0514	0.9899
	6	-	-	0.0458	0.9927

5 Conclusion

The paper proposes a complete coding scheme to represent speech signals by relating them to 8-bit gray images. Chaotic system-based encryption techniques (e.g., logistic map, Henon map, and Lorenz system) are used, where the image is divided into two subsets depending on the pixel positions (L1 and L2). Each group is separately encrypted with a technique that utilizes the keys produced by the chaotic systems, thus securing the system and making it resistant to intrusions. To provide further security support, a secure key distribution mechanism is suggested, with deterministic initial conditions of the chaotic systems being known only by the certified users. In case an attack or compromise is detected, the keys can be replaced securely by resetting the initial parameters of the chaotic maps, so the system is immune to known cryptanalytic attacks. This dynamically regenerating key process provides an extra layer of security and renders the system sensitive to live security threats. The experimental results confirmed the efficiency of the system to enhance audio data protection for information security in utilizing digital communication and secret storage. The system performed perfectly in the recovery of the signal where the implanted audio signal was recoverable from the image without degrading the quality of the received audio signal. This is quite critical to ensure that users are able to share confidential information without being hacked. Generally, the use of advanced encryption algorithms, alongside secure key generation and handling, considerably enhances the privacy and integrity of sound data in different digital media.

References

- [1] Abdulameer, L. F., Sripathi, U., & Kulkarni, M. (2022). BER Performance improvement of dual chaotic maps based on STBC communication system. *Al-Khwarizmi Engineering Journal*, 18(4), 32-44. <https://doi.org/10.22153/kej.2022.10.001>
- [2] Alaklabi, A., Munir, A., Hafeez, M. A., & Khatkhat, M. A. K. (2024). Z-crypt: Chirp z-transform-based image encryption leveraging chaotic logistic maps and substitution permutation network. *IEEE Access*, 12, 123401-123422. <https://doi.org/10.1109/ACCESS.2024.3453171>
- [3] Al-Rifae, Z. I., Abood, S. I., & Ismaeel, T. Z. (2023). Comparison hybrid techniques-based mixed transform using compression and quality metrics. *Indonesian Journal of Electrical Engineering and Computer Science*, 30(2), 807-816.
- [4] Chicco, D., Warrens, M. J., & Jurman, G. (2021). The coefficient of determination R-squared is more informative than SMAPE, MAE, MAPE, MSE and RMSE in regression analysis evaluation. *Peerj computer science*, 7, e623. <https://doi.org/10.7717/PEERJ-CS.623>
- [5] Gill, H. S., Amjad, M., Faheem, M., ur Rehman, A., Rana, U., Khan, A. R., & Bashir, R. (2025). A Normalized Exponential Piecewise Chaotic System (NEPCS) and DNA image cryptography using SHA-256. *IEEE Access*, 13, 110392-110417. <https://doi.org/10.1109/access.2025.3582318>
- [6] Herbadji, D., Herbadji, A., Kahia, H., Belmeguenai, A., & Derouiche, N. (2024). An enhanced logistic chaotic map based tweakable speech encryption algorithm. *Integration*, 97, 102192. <https://doi.org/10.1016/j.vlsi.2024.102192>
- [7] Hosny, K. M., Elnabawy, Y. M., Elshewey, A. M., Alhammad, S. M., Khafaga, D. S., & Salama, R. (2024). New method of colour image encryption using triple chaotic maps. *IET Image Processing*, 18(12), 3262-3276. <https://doi.org/10.1049/ipr2.13171>
<https://doi.org/10.11591/ijeecs.v30.i2.pp807-816>
- [8] Jerjees, S. A., Esttaifan, B. A., & Ismaeel, T. Z. (2020). Hybrid ciphering method based on chaos logistic map and fingerprint information. *Journal of Engineering Science and Technology*, 15(5), 3013-3024.

- [9] Luo, Y., Huang, Y., Yu, F., Liang, D., & Lin, H. (2024). Adaptive asymptotic shape synchronization of a chaotic system with applications for image encryption. *Mathematics*, 13(1), 128. <https://doi.org/10.3390/math13010128>
- [10] Maazouz, M., Toubal, A., Bengherbia, B., Houhou, O., & Batel, N. (2022). FPGA implementation of a chaos-based image encryption algorithm. *Journal of King Saud University-Computer and Information Sciences*, 34(10), 9926-9941.
- [11] Mangi, H. T., Ali, S. A., & Jawad, M. J. (2023). Encrypting of text based on chaotic map. *Journal of University of Babylon for Pure and Applied Sciences*, 25-39. <https://doi.org/10.29196/jubpas.v31i1.4526>
- [12] Mohi Ud Din, S., Shah, T., Alblehai, F., Nooh, S., & Jamal, S. S. (2025). A combinatory approach of non-chain ring and henon map for image encryption application. *Scientific reports*, 15(1), 1781. <https://doi.org/10.1038/s41598-025-85814-5>
- [13] Munir, R. (2024). Combining Two Chaos Maps and Determining Selective Methods for MSB Bits in a Digital Image Encryption Algorithm. *Journal of Multimedia Trend and Technology*, 3(3), 166-175. <https://doi.org/10.35671/jmtt.v3i3.63>
- [14] Raghuvanshi, K. K., Kumar, S., & Kumar, S. (2020). A data encryption model based on intertwining logistic map. *Journal of Information Security and Applications*, 55, 102622. <https://doi.org/10.1016/j.jisa.2020.102622>
- [15] Sathiyamurthi, P., & Ramakrishnan, S. (2017). Speech encryption using chaotic shift keying for secured speech communication. *EURASIP Journal on Audio, Speech, and Music Processing*, 2017(1), 20. <https://doi.org/10.1186/s13636-017-0118-0>
- [16] Sathiyamurthi, P., & Ramakrishnan, S. (2020). Speech encryption algorithm using FFT and 3D-Lorenz-logistic chaotic map. *Multimedia Tools and Applications*, 79(25), 17817-17835. <https://doi.org/10.1007/s11042-020-08729-5>
- [17] Sreedharan, S., & Eswaran, C. (2019). Speech encryption using advanced encryption standard for secured communication. *International Journal of Recent Technology and Engineering*, 8(3), 6515-6521.

Authors Biography



Nagham Malik Abd Ali is a Master's student in the Department of Electrical Engineering, specializing in Electronics and Communications, at the University of Baghdad, Iraq. Her current research interests include digital signal processing, audio and image encryption, and information security.



Prof. Dr. Tarik Zeyad Ismaeel has been a faculty member at a University of Baghdad, College of Engineering, Electrical Engineering Department since 1994. His research interest includes Communication, Information Security, Digital Signal and Image Processing.