




New Approach in Steganography Algorithm by Using Audio and Image as Secure Information Based on Chaotic Method



Aliaa Sadoon Abd^{*}, Osama Qasim Jumah Al-Thahab[†], Ahmed A. Hamad[‡]

Department of Electrical Engineering, University of Babylon, Hilla 51002, Iraq

Corresponding Author Email: eng530.aliaa.sadoon@student.uobabylon.edu.iq

Copyright: ©2025 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ijssse.150216>

ABSTRACT

Received: 2 September 2024

Revised: 20 November 2024

Accepted: 27 December 2024

Available online: 28 February 2025

Keywords:

steganography, encryption, chaos, LSB, audio steganography, image steganography

In the modern era of digital communication, safeguarding sensitive information has become a critical concern due to increasing cyber threats and unauthorized data breaches. Two foundational techniques widely employed to enhance data security are steganography and cryptography. Cryptography transforms information into an unreadable format, securing it from unauthorized access but often signaling the presence of valuable data. Steganography, on the other hand, ensures that sensitive data is invisible to attackers by hiding the information's mere existence. A better level of security can be attained by combining these two methods. This study presents a new chaotic-based steganography technique in which images are used as the main information-hiding medium. Additionally, for the first time, a novel combination of audio and image as hidden data is suggested. Confidential information is better protected by this two-layered approach, which makes it more resistant to illegal eavesdropping and hacking attempts. Strong security is ensured by the suggested system's use of a high-precision chaotic map for encryption. With a Mean Squared Error (MSE) of 0.083 and a Peak Signal-to-Noise Ratio (PSNR) of 74.87, the simulation results demonstrate the algorithm's efficacy. These measurements attest to the algorithm's capacity to preserve data integrity while offering a high degree of imperceptibility, which qualifies it for real-world use in secure communication.

1. INTRODUCTION

Advanced algorithms that provide strong security and dependability have become necessary due to the quick development of computer systems and communication technologies. These algorithms are essential for shielding private information from outside threats and hiding its existence from unwanted parties. Steganography and encryption are two essential methods for securing data. Using a secret key, encryption converts data into an unintelligible format, protecting against hackers and brute force attacks. The process of recovering the original message from its encrypted state is known as decryption [1]. Conversely, the goal of steganography is to hide the existence of data. It entails enclosing confidential information such as words, images, or audio into a cover medium, like a picture or video, in a way that makes the content hidden. Steganography protects both the content and communication itself by ensuring the hidden message stays undetected, in contrast to encryption, which by its very nature may draw attention. Chaotic systems have drawn a lot of interest in the realm of information security in recent years. These systems are distinguished by their deterministic, nonlinear characteristics and their incredibly unexpected, seemingly random behavior. The extraordinary sensitivity of chaotic systems to initial conditions—even a little change in an input parameter can have radically different results—is one of their main characteristics. Because of this

special characteristic, chaotic systems are especially well-suited for steganography and encryption, which increase the complexity and security of methods. On the other hand, when initial values are changed, classical systems only exhibit slight variations in results [2].

Chaotic systems have been used to enhance a number of studies. Various studies have examined the application of chaotic systems in steganography and encryption, emphasizing both their advantages and disadvantages. Using hyper and logistic maps to jumble images, Patro and Acharya [3] created a chaos-based labeling system for color images. This method only addressed image encryption, restricting its use to multimedia situations involving audio or video, even though it showed excellent security and low repetition rates. A 3D chaotic logistic map-based picture encryption method with strong randomness and security properties including confusion and diffusion was proposed by Kanso et al. [4]. But instead of addressing how to include steganography to further hide the existence of the encrypted data, this approach focused solely on encryption. Image steganography methods utilizing chaotic maps, such as 3D Chebyshev and Logistic Maps, were first presented by ALabaichi et al. [5]. These investigations' reliance on single-layer cover media (such as photographs) poses a barrier in situations that call for multi-layered protection or multimodal data embedding, like mixing voice and image, even if they achieved good security and data hiding efficiency.

A steganography approach based on a 5D chaotic map was proposed by Shehab et al. [6] to embed private information into video frames. While this approach was successful in maintaining the quality of both the to further improve security, Elshoush et al. [7] recently introduced a novel chaotic map approach that generates encryption keys through elliptic curve cryptography using 2D-TFCDM and discrete fractional calculus.

This study suggests a unique method for information security utilizing chaotic systems that combines steganography with encryption. The technique offers a novel dual layer of security by using both audio and visuals as secret information. The suggested technique seeks to improve the security of transmitted data by combining chaotic systems and steganography, guaranteeing resistance against outside threats while preserving high performance and dependability. A common steganography scenario is depicted in Figure 1, which shows how to embed and extract private data into a cover medium [8, 9].

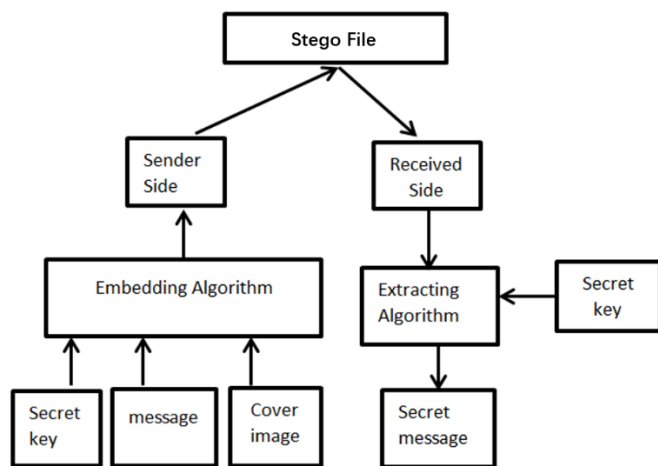


Figure 1. Data hiding system

2. ARNOLD CAT MAPPING (ACM)

Arnold transform (also called Arnold Cat mapping) (ACM) is a clipping transform presented by Pramanik et al. [10]. To enhance the safety and visual quality of the extracted message in the image hiding process, a shuffling operation is performed during embedding. This involves the successive mixing of the initial information, effectively spreading it throughout the available state space. Given the discrete nature of images and the ACM, which shares the same number of dimensions, ACM is particularly suitable for shuffling the hidden message across the appropriate sub-band of the cover image. As a result, recovering the original message without knowledge of the initial transformation or the secret key becomes exponentially more difficult [11]. The embedding locations within the proper sub-band are determined by the transformation via the Cat Map, rendering the secret message chaotic during the embedding process. To extract the secret message, the receiver must know the exact embedding locations used.

The map's action on a unit square is often illustrated with a picture of a cat, from which the map derives its name. The mathematical formula for this transformation is provided in Eq. (1) [12]:

$$C(x, y) = ((x + y_{mod1}), (x + 2y_{mod1})) = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod1 \quad (1)$$

where, mod 1 means the fractional part of "a" for any real "a", which also denoting to the square 2x2 matrix as A, the map can be written simply as:

$C(x, y) = A(x, y)^T mod 1$, where $(x, y)^T$ stands for a vector transpose these dynamical system. Figure 2 shows the flowchart of the algorithm that used for encryption audio.

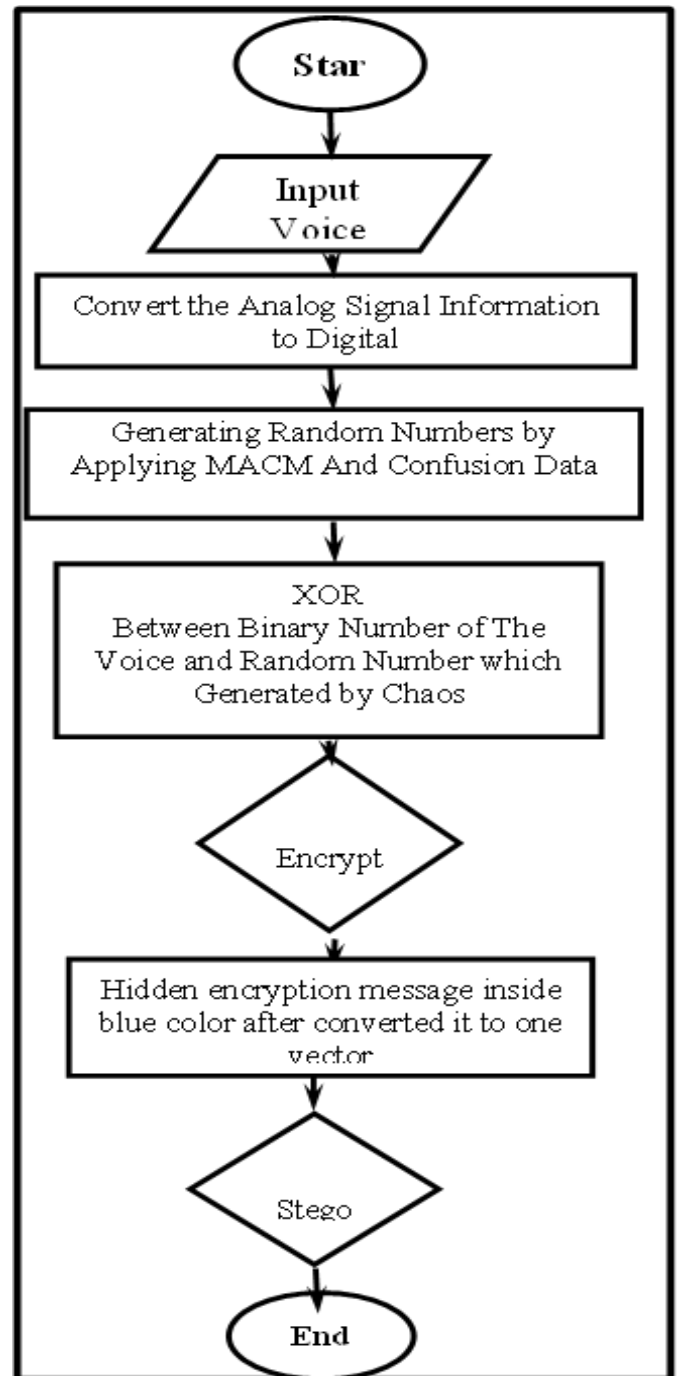


Figure 2. Encryption audio by using MACM

3. DUFFING MAP

The "Holmes map," also known as the Duffing map, is a type of chaotic map and a discrete-time dynamical system. It serves as an example of a system that exhibits chaotic behavior.

Eqs. (2) and (3) demonstrate how the Duffing map converts a point (X_n, Y_n) in the plane to a new point [13]:

$$X_{n+1} = Y_n \tag{2}$$

$$y_{n+1} = (-bX_n + aY_n + Y^3)^n \tag{3}$$

Because of its special qualities that make it especially useful for this application, the Duffing map was chosen for audio encryption in this study. Strong chaotic behavior and a high degree of randomness are characteristics of the Duffing map that are essential for guaranteeing the security of encrypted data. The Duffing map functions in a multi-dimensional phase space, which increases its sensitivity to initial conditions and offers a broader key space than more straightforward chaotic maps like Logistic or Chebyshev maps. This guarantees that the encrypted audio stream has better confusion and diffusion qualities and is impervious to brute force attacks. Furthermore, the Duffing map is a more reliable option for audio encryption than the discrete chaotic maps that are frequently employed for image encryption since it can handle the continuous nature of audio signals. Further confirming the Duffing map's efficacy in secure communication systems, simulation studies show that it generates encrypted audio signals with little correlation to the original signal [14].

In order to create chaotic behavior, parameters a and b are set to 2.75 and 0.2, respectively. The terms “trajectory” and “orbit” are commonly used to describe the evolution of these dynamic systems [15].

4. THEORY OF LEAST SIGNIFICANT BITS (LSB)

This method is considered one of the most direct and clearest ways to hide confidential data inside the cover file, (including confidential data in the image file). This is done in a way that is not clear to the naked eye the cover image is represented as an array of pixels, each pixel completes 1 byte and every byte equals 8 bits, meaning 256 colors between black and white (grayscale). LSB denotes a bit of location in binary integer. The basic idea is to replace the pixels of the data hidden in the least significant byte of the jacket matrix. When using a color image as a cover, 3 bits per pixel can be hidden [16].

5. PROPLEMS STATEMENT AND AIMS OF WORK

In the current technological development, there is a massive increase in the amount of data that is sent and shared over the various types of communication channels, especially the data that is exchanged on various internet platforms to reach the receiver was well as possible without losing their specification and secret information. Maintaining user data, especially the image file and audio file is one of the critical things that merely make people worry. The primary goals of this paper are:

- i. Design a security system that effectively protects hidden data from tampering by combining steganography techniques with chaos-based cryptography.
- ii. Create random locations in the cover image specifically to intentionally embed confidential data

within the RGB cover image without raising suspicion.

- iii. The proposed system proves its high efficiency in including data through:
 - a) Ensuring a high degree of similarity between the original image (the cover before the data is included) and the Stego image (the cover hidden inside the data).
 - b) High-quality hidden data extraction from the received Stego image when transmitted over different communication channels, even under different types of noise.
 - c) Perform careful analysis and necessary graph execution on input data, secured image and recovered data.

The proposed system was designed in MATLAB. In this system, duffing chaotic maps are used to encrypt the voice signal, and ACM to scramble the image signal. After the encryption processing the result value will be hidden in cover image. The procedure can be described in Figure 3.

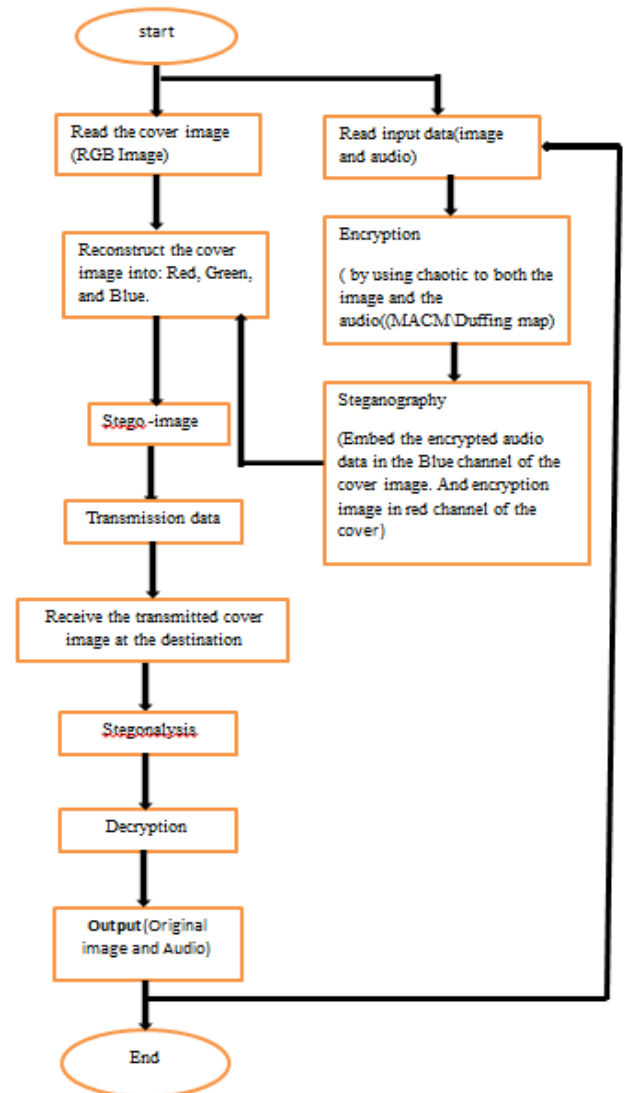


Figure 3. Flow chart of the proposed method

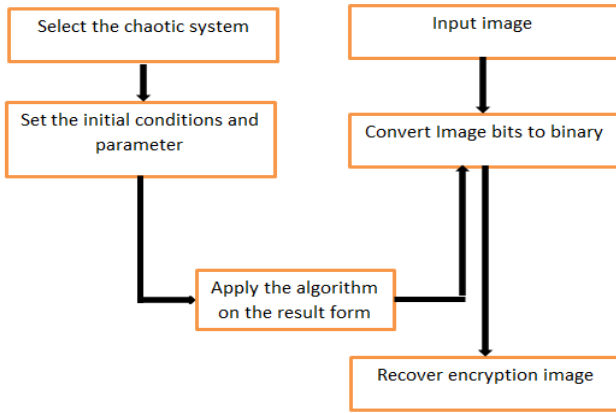


Figure 4. Block diagram of encryption image

The detailed steps of the research are summarized as follows:

First step: Read Input Data (color image and Audio with 8 KH sampling).

Second step: Encryption process is done by apply chaotic encryption to both the image and the audio file.

The audio is encrypted using Duffing chaotic map, and the process is clarified in steps.

- a) Audio Preprocessing: Read the audio and convert it to 2D (Two dimensions).
- b) Generated Duffing chaotic map and set initial condition Generated the chaotic map with length equal to audio length. Random numbers will be generated from (0-255).
- c) Make diffusion and confusion for data we get encryption audio.

The image message is also encrypted by using (ACM) and the procedure of encryption clarified as in Figure 4.

Third step: Read the cover image which used color image as cover to hide the encryption of the data in side it After that decompose the cover to its original channel (**R**: Red, **G**: Green, **B**: Blue).

Fourth step: Hide the encrypted audio data on the blue channel of the cover image. And hide the encrypted image data in the Red, ensuring minimal visual distortion.

Fifth step: Transmit the stego image (cover after hidden data), over a communication channel.

Sixth step: Data Extraction and extract the original message (Audio and image) after decryption and steganalysis.

6. PERFORMANCE EVALUATION

The primary purpose of steganography systems is to conceal secret data within a cover file (such as an image or video) in a way that cannot be detected by the human visual system. To determine whether the impact of data hiding on video quality falls within an acceptable range, various statistical tests are employed. This chapter will discuss several parameters such as Mean Squared Error (MSE), Structural Similarity Index (SSIM), and Peak Signal-to-Noise Ratio (PSNR) [17].

6.1 Mean-Squared Error (MSE)

Mean-Squared Error (MSE) is a statistical method used to assess the similarity between the stego image and the original image. The similarity is determined by measuring the error signal, which is obtained by subtracting the checked signal from the reference signal and then calculating the mean energy of the error signal. The formula for calculating MSE is shown in Eq. (4) [18]:

$$MSE = \frac{1}{m * n} \sum_{i=1}^{m*n} \sum_{j=1}^n (Pic1(i,j)_i - Pic2(i,j)_i)^2 \quad (4)$$

In this formula, Pic1 represents the original image, Pic2 represents the stego image, and $Pic1$ and $Pic2$ are the number of rows and columns in the input images, respectively (i.e., the dimensions of the image matrix).

6.2 Peak Signal-to-Noise Ratio (PSNR)

Peak Signal-to-Noise Ratio (PSNR) is defined as the ratio between the maximum power of a signal and the power of the noise that corrupts it. PSNR is typically expressed on a decibel scale and is commonly used to measure the quality of image reconstruction. The signal, in this case, is the original data, while the noise represents the error introduced. A high PSNR value indicates high image quality. PSNR can be calculated using Eq. (5) [19]:

$$PSNR(dB) = 10 \log_{10} \left[\frac{p^2}{MSE} \right] \quad (5)$$

Here, P is the maximum possible pixel value of the image, when pixels are represented using 8 bits per sample.

6.3 Structural Similarity Index (SSIM)

Structural Similarity Index (SSIM) is used in image processing to assess the quality of an image subject to various distortions that may reduce its accuracy. It is employed to estimate the change in media resolution before and after a steganography operation. The image altered after steganography must be compared to the image before the alteration. The equation for SSIM is presented in Eq. (6) [20]:

$$SSIM(\%) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \times 100 \quad (6)$$

In this equation, μ_x, μ_y represent the local means, $\sigma_x,$ and σ_y represent the standard deviations, and σ_{xy} represents the cross-covariance.

6.4 Histogram

A histogram is a graphical representation that organizes a group of data points into user-specified ranges, similar to a bar graph. The histogram condenses a data series into an easily interpreted visual by grouping many data points into logical ranges or bins. Figure 5 depicts a simplified diagram of a histogram [21].

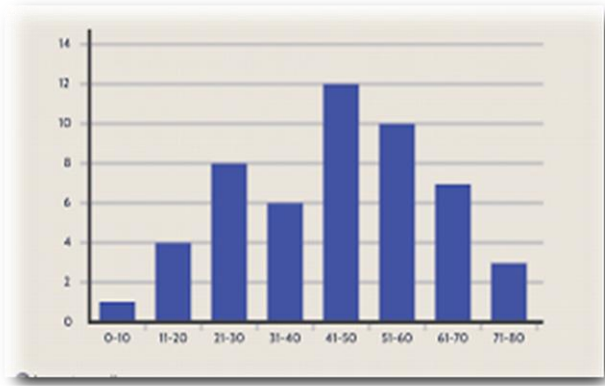


Figure 5. Histogram definition [19]

7.1 Encryption result

First, the result of the audio encoding is displayed. The voice clip used for testing purpose has 8KHz sampling frequency and 05:68 seconds length (45503 samples), as is shown in Figure 6.

In this section, the effect of audio encryption using the duffing chaotic map will be clarified. Also, the most prominent results obtained and the extent of the effect of chaos on the original sound will be clarified, Figure 6 shows the result of encryption algorithm. The parameter that is used in this process is $(a=-0.15, b=2.75)$. The result of encryption voice which clarified in Table 1.

Table 1 shows the objective results obtained by encoding the audio using the duffing chaotic map. The simulation results in this case are also shown in the Figure 7.

7. SIMULATION RESULT AND DISCUSSION

This section shows the results of simulations and discussions.

Table 1. Result of encryption voice

SSSNR (dB)	SNR (dB)	LPC	CD	MSE	CC
-12.07	-48.6	16.14	7.61	0.21	0.003

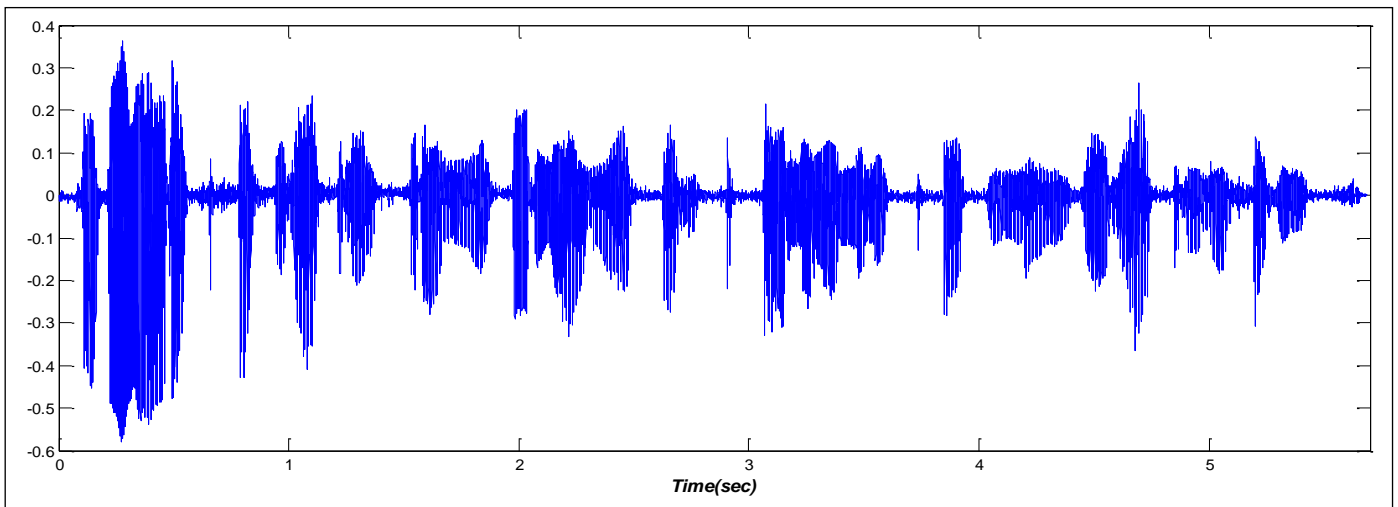


Figure 6. Original voice signal

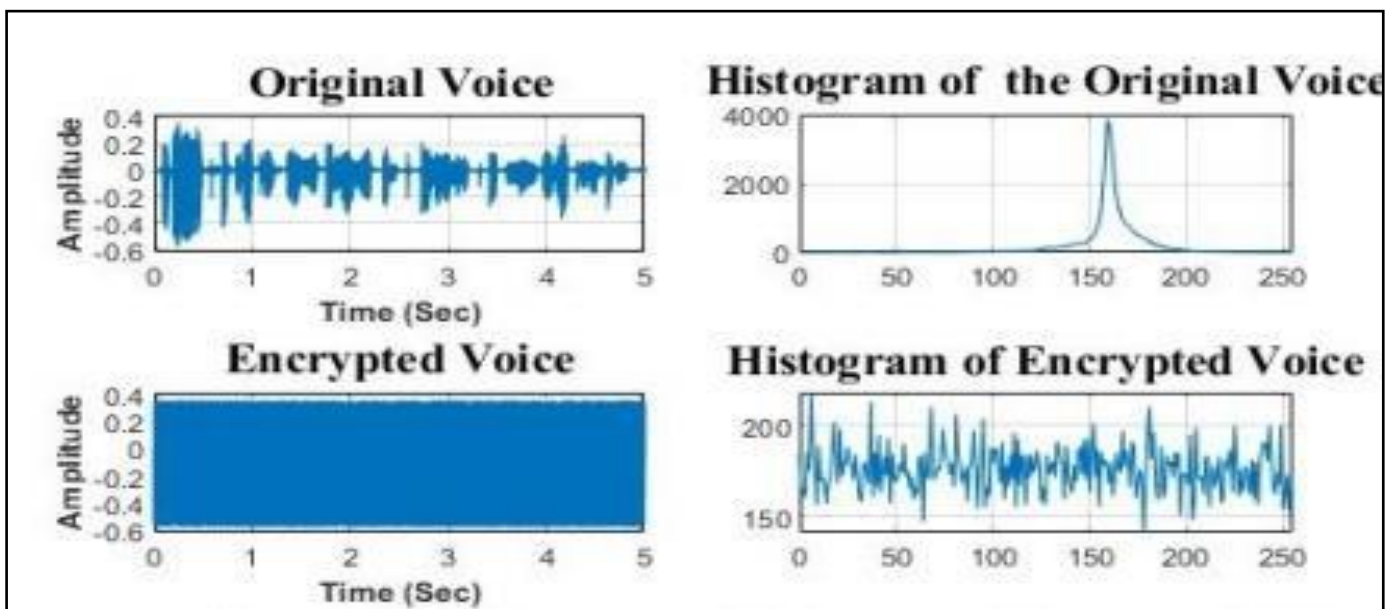


Figure 7. Audio encryption results

Table 2. Result of encryption algorithm for different size audio

Size of File	Encryption Audio			
	SSSNR	LPC	CD	MSE
8K	12.069	16.144	7.607	0.206
10K	-12.07	16.154	7.601	0.2033
16k	-12.001	16.145	7.599	0.203

Figure 7 shows the plot of the original audio, and its histogram also shows the encoder audio after applying the duffing chaotic map and its histogram. This figure shows that the histogram resulting from the encryption process is completely different from the original histogram.

This proves that the encryption used in this step doesn't leave a trace of the original voice. Rather, it shuffles the audio

sample in such a way that it is difficult to understand what has been encoded.

Voice messages of different sizes will be used to test the proposed encryption algorithm. The results of this procedure are shown in Table 2.

After viewing the results related to audio encoding, the results for image encoding (Encryption image), will be displayed. Because the confidential data that is sent within the protection system is represented by (image and sound). In this algorithm.

An image with a size of (192*192) is used as an example to test the proposed encryption algorithm. Figure 8 shows the original image and its histogram.

The image in Figure 8 is subject to an encryption process using the (MACM). The procedure for doing so was described in. Figure 8 shows the results of the image encryption process in addition to its histogram.

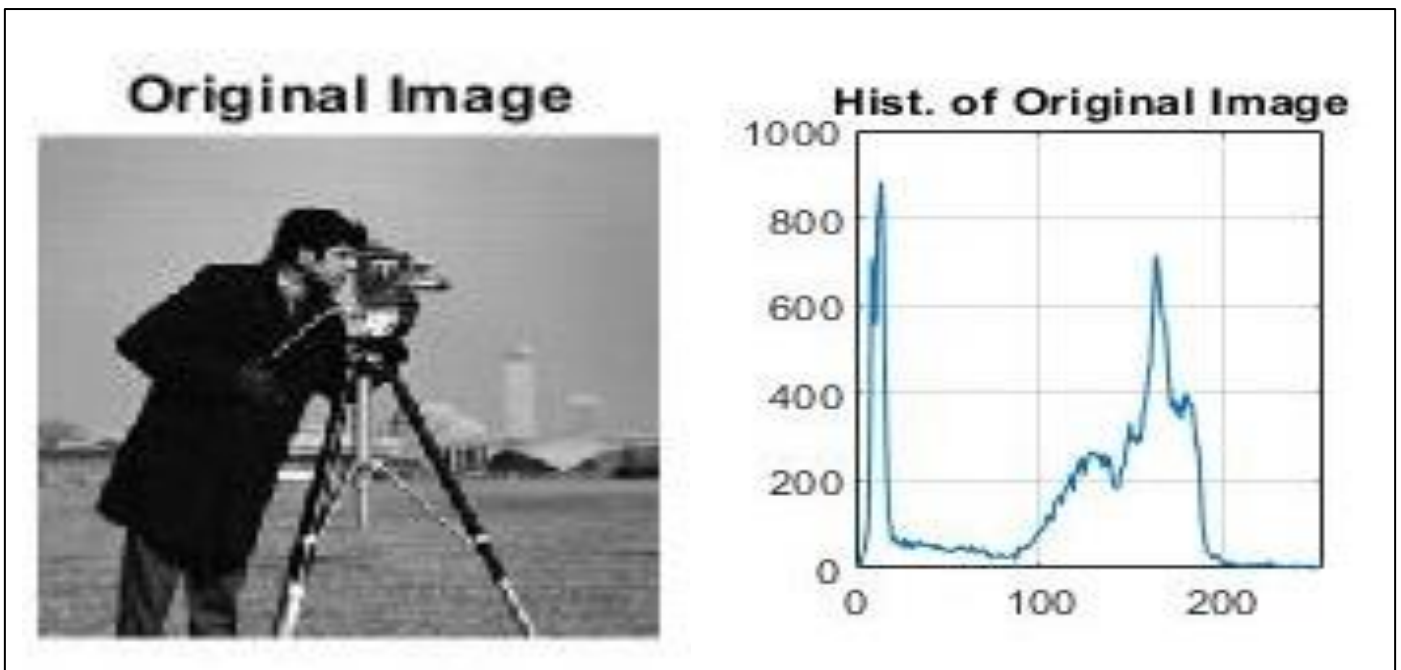


Figure 8. Original image and its histogram

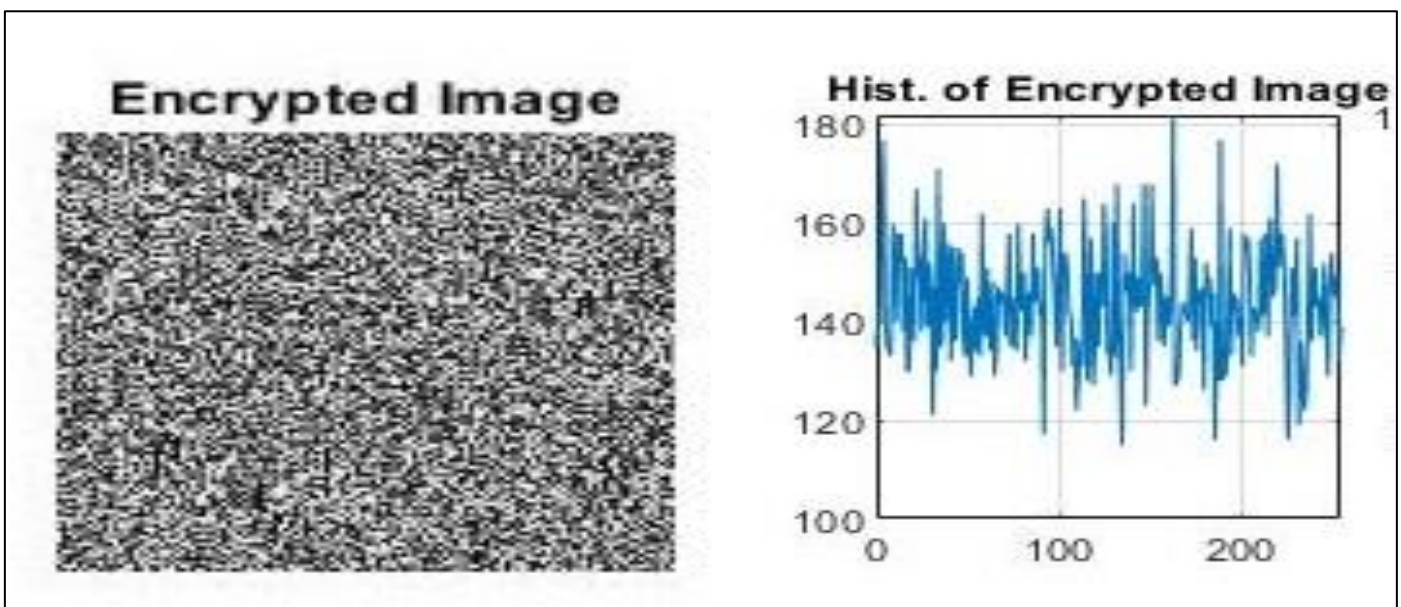


Figure 9. Encryption image and its histogram

Table 3. Encoder results for different size images

Size of Image	Encryption Image			
	MSE	PSNR	SNR	SSIM
32*32	6.432	3.01	0.0094	8.36 e+03
32*64	8.036	2.9	0.0075	9.51e+03
192*192	8.4680	3.691	0.008	9.25e+03

Figure 9 shows that the encryption process has been completed, where there are no features of the original image. This makes it difficult for hackers to decrypt and recover data unless the key to be used is specified. Here the keys used are represented by the parameters (A=2313, B=33311, C=43312) and they are known only to the sender and recipient. The histogram of an encrypted image is completely different from that of the original, secret image. This means that the bits of the original image are scattered in an image that is difficult to reconstruct unless the key used is known.

After viewing the encrypted image and its histogram, Table 3 shows the values obtained by comparing the encrypted image with the original.

7.2 Steganography results

After encrypting the audio by using duffing chaotic map and encryption the image using modify ACM. There is another level of security suggested by steganography. In this suggested steganography step, a colored image will be used as a cover, to hide confidential information inside it. The cover image size

is about (512*512). In this safety step, the cover image is segmented into its primary color (R, G, B). After the cover image has been segmented, the secret sound inside the blue color is hidden by occupying the least significant bits of that color. The encoded image is hidden within the red color of the cover image and the image bits are hidden inside LSB of that layer of the cover. Figure 10 shows the steganography process for a secret image with size (192*192) and a secret sound (16kb).

Figure 10 shows the amount of change in the cover image after hiding the data. Changes in the shell are barely perceptible and invisible to the human eye. This indicates that the proposed system is very effective, the results shown in Figure 10 prove the amount of congruence between the two images. In addition, it proves that the change in histogram between the two images isn't recognize in the human visual system.

Figure 11 proves that the effect of hiding data inside the cover image doesn't effect on it. Then the Stego image is sent over the internet channel (Viber, what's up, Email,) and received by the recipient. To stabilize the efficiency of the system, the received data must be like the transmitted data. On the receiving side, secret images and secret voices are received only by those who know the key, which only the sender knows. To test the efficiency of the proposed system, the data received should be the same as the data sent, with no distortion or loss. Figure 12 shows that the received secret image is the same as the transmitted image and hasn't changed any.

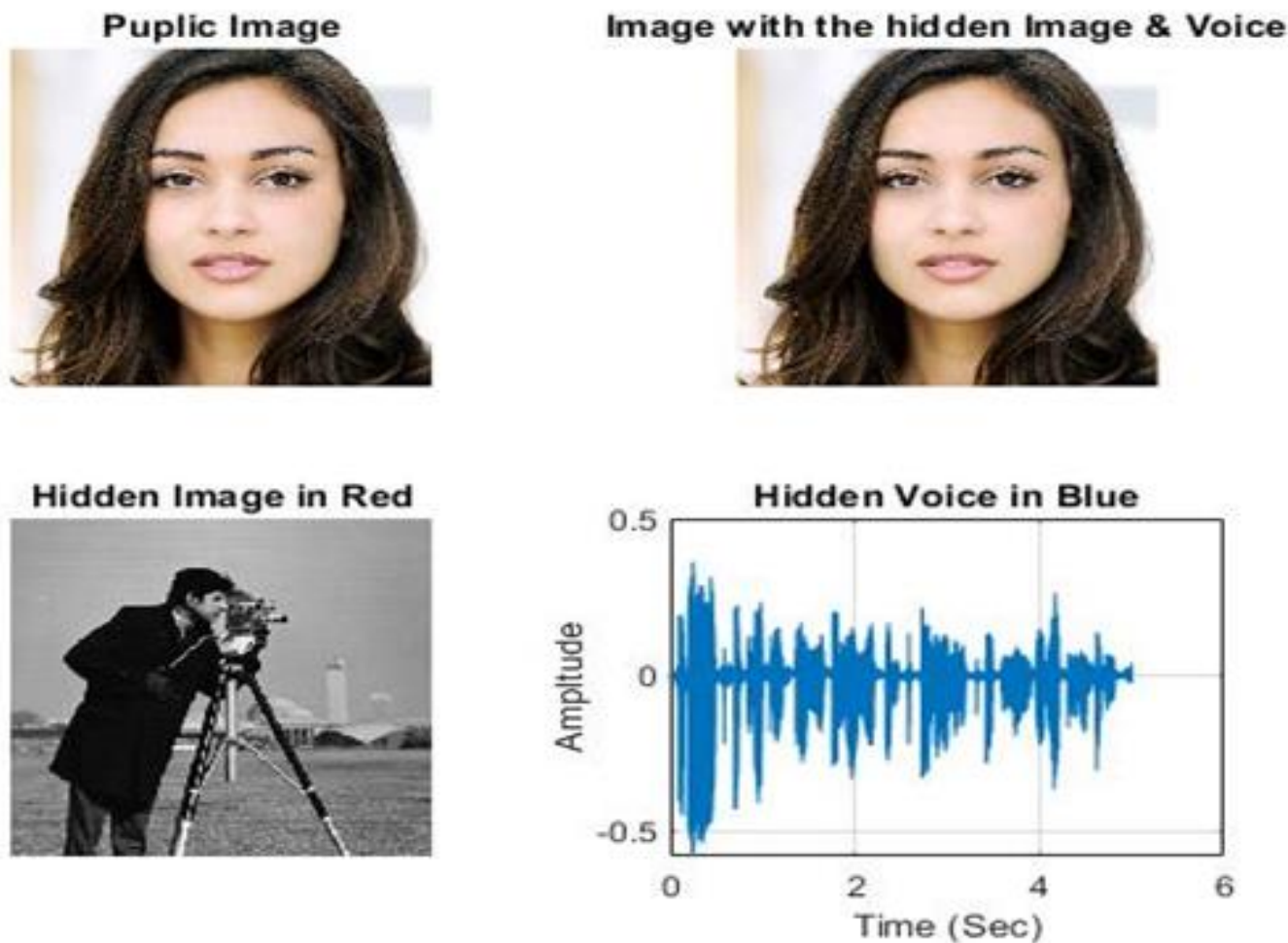


Figure 10. Image steganography process

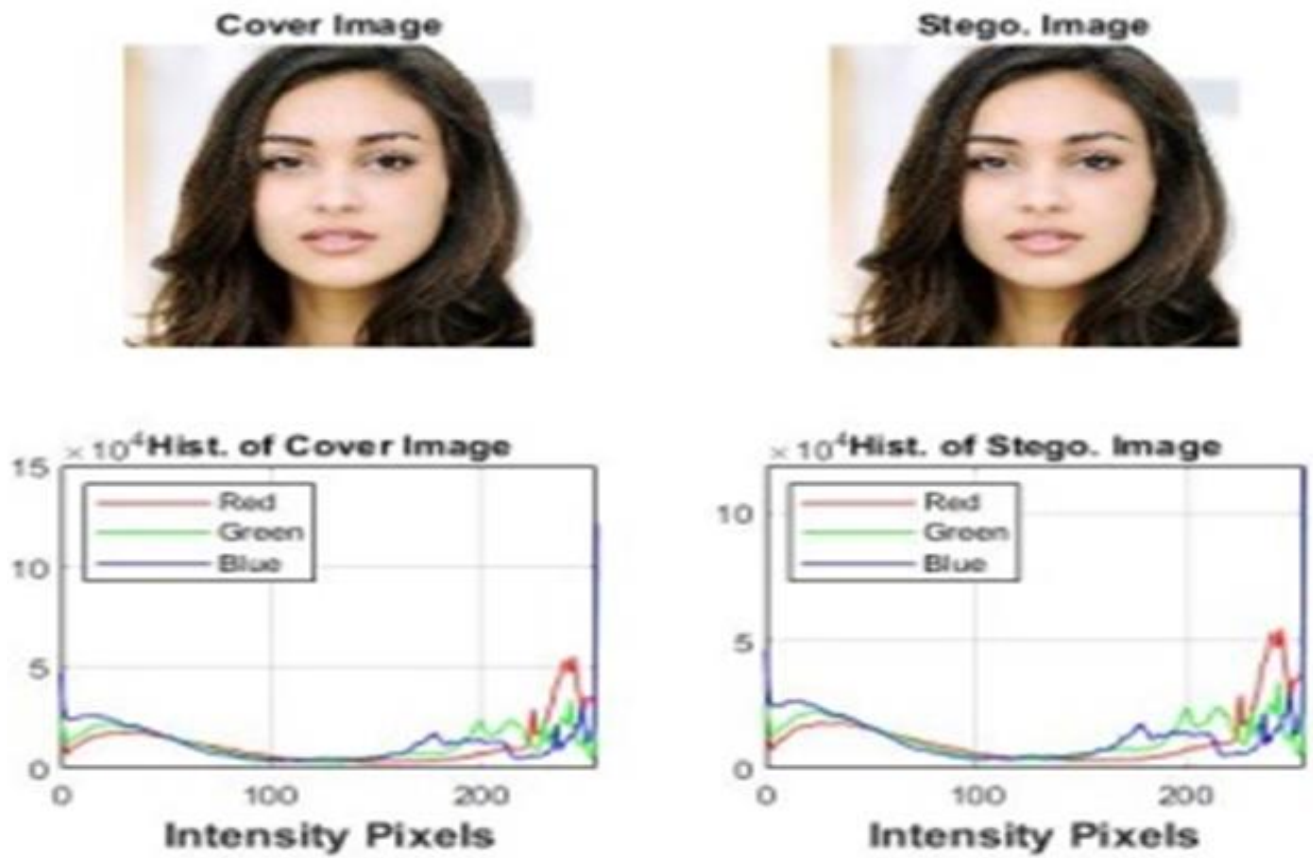


Figure 11. The results of hiding the secret audio and secret image inside the cover image

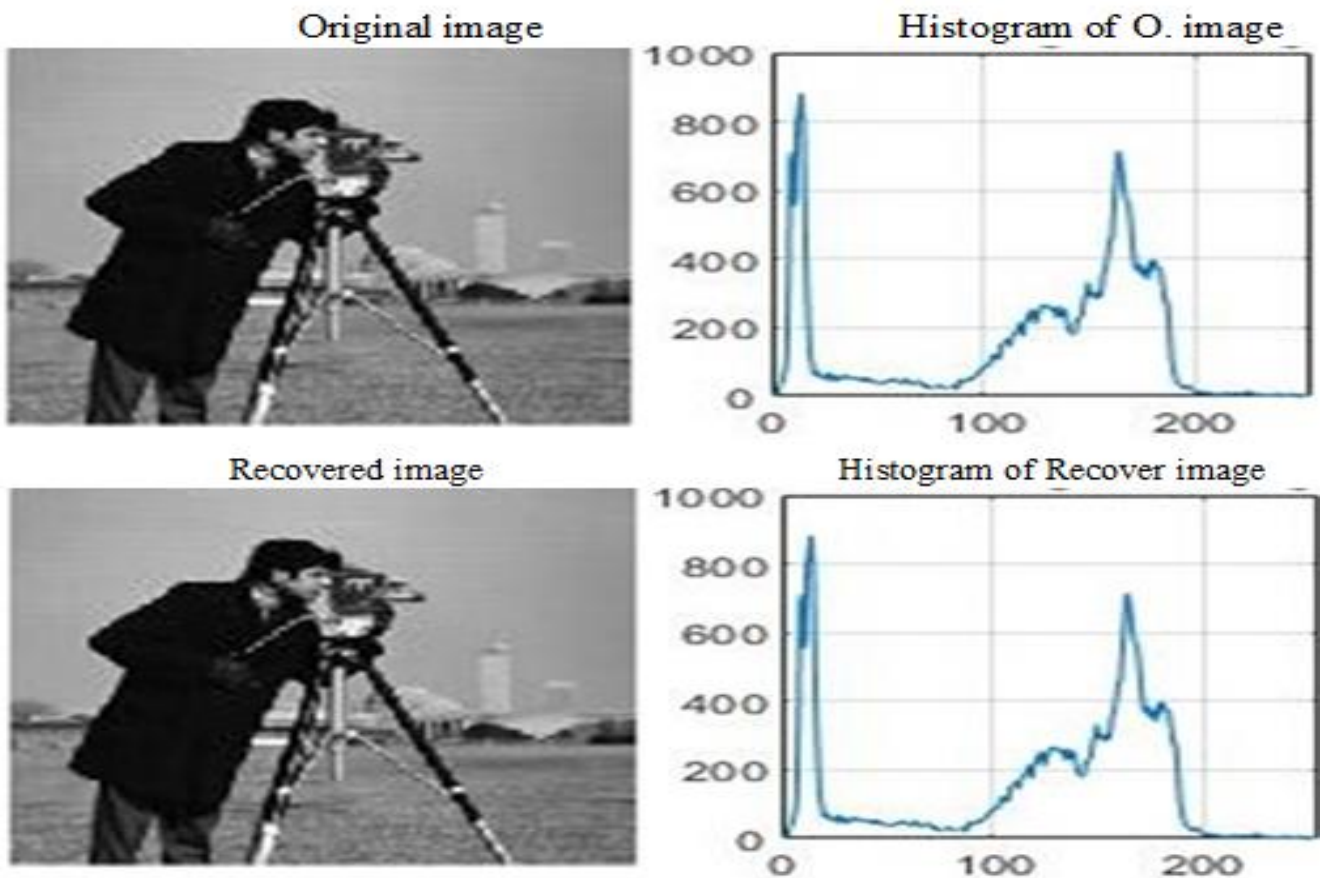


Figure 12. The received image histogram compared to the histogram of the original image

Table 4. Result of different recover image

Size of Secret Image	Recover Images			
	MSE	PSNR	SNR	SSIM
32*32	0	Inf	Inf	1
32*64	0	Inf	Inf	1
192*192	0	Inf	Inf	1

Table 5. Result of different recover audio

Size of Audio	Recover Audio			
	SSSNR	LPC	CD	MSE
8Kb	51.287	-18.82	-5.81	1.586 e-07
10Kb	51.3	-18.81	-5.809	1.5844 e-07
16kb	72,34	-59.14	-22.095	3.877 e-07

Table 4 displays the results obtained from comparing the sent and received image.

Table 4 proves that the sent images reach the recipient without any change when using the proposed system. After testing the system's efficiency in preserving the transmitted image, it will also be tested for the sent secret audio.

Through the values presented in Table 5, it was proved that the sound reaches the transmitter with a very small loss that can be bypassed in various ways in the future, such as filters to reduce noise and others.

The obtained results demonstrate the effectiveness of the proposed algorithm. For instance, the Peak Signal-to-Noise Ratio (PSNR) reached 74.87, which indicates high-quality reconstruction of the hidden data without noticeable distortion in the cover media. A higher PSNR value signifies better data fidelity, and values above 50dB are generally considered excellent for image and audio steganography.

Similarly, the Mean Square Error (MSE) was recorded at 0.083, indicating minimal difference between the original and the stego media. Lower MSE values are indicative of high data embedding quality and minimal perceptual changes, ensuring the cover media remains indistinguishable from its original form.

Values near 1 were displayed by the Structural Similarity Index (SSIM), which gauges perceived visual quality. This demonstrates how closely the steganographic media resembled the original cover media, demonstrating how well the suggested technique preserves both visual and aural quality.

The suggested algorithm performed better in terms of security and quality than earlier approaches, such as those that used linear techniques or simpler chaotic maps. These outcomes confirm the method's effectiveness and resilience, especially in terms of its capacity to withstand intrusions and preserve high fidelity in steganographic applications. The acquired results show how reliable and successful the suggested approach is at accomplishing safe data concealment. The distribution of pixel intensities for the encrypted image shows a notable change, as shown by the histogram analysis. It is difficult for an attacker to deduce the existence of hidden data because of this even distribution, which guarantees that no observable patterns are left behind. This outcome demonstrates the high degree of security provided by the suggested approach.

Furthermore, the remarkable quality retention of the cover image following the embedding of the secret data is shown in the computed PSNR value of 74.87. This suggests that minimal deformation is introduced during the embedding process, preserving the cover medium's visual integrity. The algorithm's dependability is further confirmed by the low MSE

value of 0.083, which emphasizes the small amount of error introduced during the embedding.

In addition, the changes in the histogram provide clear evidence of the effective scrambling and diffusion achieved by the chaotic encryption process. These changes validate the robustness of the algorithm against statistical and visual analyses, which are common techniques used in cryptanalysis. Overall, the combination of high PSNR, low MSE, and a transformed histogram demonstrates that the proposed method successfully achieves both secure data hiding and preservation of the cover medium's quality.

8. CONCLUSIONS

Security and reliability of the system are examined under various types of challenges. In addition, from all the output results of tests and simulations, it can be concluded some of the apparent points that proved the efficiency of the proposed system. In the method of data hiding using steganography, there are interesting primary objectives: the technique used in steganography should provide the maximum possible capacity, the data included should be imperceptible to the observer and the received data itself should be confidential data transmitted without any change. Here, a stego image was obtained with very close characteristics of the original cover image and the correlation was very close to that, so it is difficult to distinguish between them.

9. FUTURE WORKS

Future research can explore several directions to enhance and extend the proposed method. One potential area is testing the algorithm on larger and more diverse datasets, including images and audio files of varying formats and resolutions, to evaluate its robustness and adaptability under different conditions. Additionally, incorporating more advanced chaotic maps or hybrid encryption techniques could further improve the security and efficiency of the system.

Another promising avenue is applying the method in real-world scenarios, such as secure communication in IoT devices, medical image transmission, and multimedia streaming services, where data security and quality preservation are critical. Moreover, exploring the integration of machine learning techniques to dynamically optimize the embedding and extraction processes could provide a more intelligent and adaptive framework for steganography.

Finally, conducting comprehensive security analyses against emerging attacks, such as deep-learning-based steganalysis, would be essential to ensure the method's resilience and long-term reliability. These future directions not only aim to improve the proposed method but also contribute to advancing the broader field of secure data hiding.

REFERENCES

- [1] Rustad, S., Andono, P.N., Shidik, G.F. (2023). Digital image steganography survey and investigation (goal, assessment, method, development, and dataset). *Signal Processing*, 206: 108908. <https://doi.org/10.1016/j.sigpro.2022.108908>

- [2] Liu, Z., Xia, T. (2018). Novel two-dimensional fractional-order discrete chaotic map and its application to image encryption. *Applied Computing and Informatics*, 14(2): 177-185. <https://doi.org/10.1016/j.aci.2017.07.002>
- [3] Patro, K.A.K., Acharya, B. (2019). A simple, secure, and time-efficient bit-plane operated bit-level image encryption scheme using 1D chaotic maps. In *Innovations in Soft Computing and Information Technology: Proceedings of ICEMIT 2017, Singapore*: Springer Singapore, 3: 261-278. https://doi.org/10.1007/978-981-13-3185-5_23
- [4] Kanso, M.A., Piette, J.H., Hanna, J.A., Giacomini, A.J. (2020). Coronavirus rotational diffusivity. *Physics of Fluids*, 32(11): <https://doi.org/10.1063/5.0031875>
- [5] ALabaichi, A., Al-Dabbas, M.A.A.K., Salih, A. (2020). Image steganography using least significant bit and secret map techniques. *International Journal of Electrical & Computer Engineering* (2088-8708), 10(1): 935-946. <https://doi.org/10.11591/ijece.v10i1.pp935-946>
- [6] Shehab, J.N., Abdulkadhim, H.A., Al-Tameemi, T.F. (2021). Robust large image steganography using LSB algorithm and 5D hyper-chaotic system. *Bulletin of Electrical Engineering and Informatics*, 10(2): 689-698. <https://doi.org/10.11591/eei.v10i2.2747>
- [7] Elshoush, H.T., Mohammed, R.M., Abdelhameed, M.T., Mohammed, A.F. (2023). Mitigating man-in-the-middle attack in online payment system transaction using polymorphic AES encryption algorithm. *Journal of Information Hiding and Multimedia Signal Processing*, 14(3): 102-112.
- [8] Kumar, A., Rani, R., Singh, S. (2023). A survey of recent advances in image steganography. *Security and Privacy*, 6(3): e281. <https://doi.org/10.1002/spy2.281>
- [9] Easttom, W. (2021). Steganography. In *Modern Cryptography*, pp. 337-356. <https://doi.org/10.1007/978-3-030-63115-4>
- [10] Pramanik, S., Ghosh, R., Pandey, D., Samanta, D., Dutta, S., Dutta, S. (2021). Techniques of steganography and cryptography in digital transformation. In *Emerging Challenges, Solutions, and Best Practices for Digital Enterprise Transformation*. IGI Global, pp. 24-44. <https://doi.org/10.4018/978-1-7998-8587-0.ch002>
- [11] Hamidouche, B., Guesmi, K., Essounbouli, N. (2024). Mastering chaos: A review. *Annual Reviews in Control*, 58:100966. <https://doi.org/10.1016/j.arcontrol.2024.100966>
- [12] Choudhary, U., Agarwal, P. (2024). Image steganography combined with cryptography for covert communication. In *Proceedings of The 2024 Sixteenth International Conference on Contemporary Computing*, pp. 207-212. <https://doi.org/10.1145/3675888.3676053>
- [13] Abdulla, A.A. (2024). Digital image steganography: Challenges, investigation, and recommendation for the future direction. *Soft Computing*, 28(15): 8963-8976. <https://doi.org/10.1007/s00500-023-09130-8>
- [14] Li, C., Tan, K., Feng, B., Lü, J. (2021). The graph structure of the generalized discrete Arnold's cat map. *IEEE Transactions on Computers*, 71(2): 364-377. <https://doi.org/10.1109/TC.2021.3051387>
- [15] Hasan, M.M., Faruqi, T.M., Tazrean, M., Chowdhury, T.H. (2017). Biometric encryption using Duffing map. In *4th International Conference on Advances in Electrical Engineering (ICAEE)*, Dhaka, Bangladesh, pp. 737-742. <https://doi.org/10.1109/ICAEE.2017.8255452>
- [16] Ashari, I.F., Nugroho, E.D., Andrianto, D.D., Yusuf, M.A.N.M., Alkarkhi, M. (2024). The evaluation of LSB steganography on image file using 3DES and MD5 key. *Journal of Information Technology and Computer Engineering*, 8(1): 8-18.
- [17] Mandal, A.K., Prakash, C., Tiwari, A. (2012). Performance evaluation of cryptographic algorithms: DES and AES. In *IEEE Students' Conference on Electrical, Electronics and Computer Science, Bhopal, India*, pp. 1-5. <https://doi.org/10.1109/SCEECS.2012.6184991>
- [18] Himanshu, H., Hooda, R., Poply, V. (2024). Image enhancement in Fourier domain using MSE and PSNR. In *AIP Conference Proceedings*. AIP Publishing, 3081(1). <https://doi.org/10.1063/5.0196118>
- [19] Canales, C.M., Olea, G., Jurado, V., Espindola, M. (2024). Management Strategies Evaluation (MSE) in a mixed and multi-specific fishery based on indicator species: An example of small pelagic fish in Ecuador. *Marine Policy*, 162: 106044. <https://doi.org/10.1016/j.marpol.2024.106044>
- [20] Reznik, Y. (2023). Another look at SSIM image quality metric. *Electronic Imaging*, 35: 1-7. <https://doi.org/10.2352/EI.2023.35.8.IQSP-305>
- [21] Chaki, J., Dey, N. (2021). Histogram-based image colour features. In *Image Colour Feature Extraction Techniques*, Springer, Singapore, pp. 29-41. <https://doi.org/10.1007/978-981-15-5761-3>