Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

A Novel Image Encryption Framework Using Multiple Chaotic Maps, Image Steganography and CNN Filters

Ahmed Makram

am.abuelmaaty025@egma.edu.eg

1Department of Comunication, Air Defence College, Egyptian Military Academy, New Capital, 4804004,

Abeer Saber

Damietta University

Azhar. A. Hamdi

Zagazig University

Rania A. Elsayed

Zagazig University

Wael A. Awad

Damietta University

Article

Keywords: Image Encryption-Decryption, Skew tent map, Piecewise Linear Chaotic Map, CNNs, median Filter, gaussian Filter, Chosen-plaintext attack Security analysis

Posted Date: April 24th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9260826/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

A Novel Image Encryption Framework Using Multiple Chaotic Maps, Image Steganography and CNN Filters

Ahmed Makram[1*], Abeer Saber [2], Azhar. A. Hamdi[3], Rania A. Elsayed[3], Wael A. Awad [4]

[1]Department of Comunication, Air Defence College, Egyptian Military Academy, New Capital, 4804004
. am.abuelmaaty025@egma.edu.eg

[2]*Information Technology Department,* Faculty of Computers and Artificial Intelligence, Damietta University, Damietta 34517, Egypt.
Abeer_saber@du.edu.eg

[3]Department of Electronics and Communications Engineering, Zagazig University, Zagazig44519, Egypt.

azharhamdi@zu.edu.eg, rania_ahmed@zu.edu.eg

[4]*Computer Science Department,* Faculty of Computers and Artificial Intelligence, Damietta University, Damietta 34517, Egypt.

Wael_abdelkader@du.edu.eg

ABSTRACT- *Image encryption is paramount for safeguarding sensitive visual data from unauthorized access and ensuring privacy. By transforming images into unintelligible codes, encryption prevents the misuse or disclosure of confidential information. This paper introduces a novel paradigm for image coding that leverages chaotic maps and steganography to enhance security and privacy. The proposed system employs a two-step encryption process. First, the original image is concealed within another image (cover image) using the Discrete Cosine Transform (DCT). Second, a robust chaotic map is generated by combining different chaotic maps: a cosine-square logistic map is used to generate a variable key to create new chaotic maps. These enhanced chaotic map algorithms are then used to encrypt the DCT coefficients of the hidden image. To further improve the quality of the decrypted image, convolutional neural networks (CNNs) with various filters are applied. We demonstrate the effectiveness of the proposed method through extensive numerical experiments on gray-scale images. By comparing our approach to established techniques like circular mapping, S-box, and S-box combined with Arnold transform, we show that our method offers superior security, low correlation coefficients, and excellent information entropy. We contrasted our approaches with well-established ones, such as circular mapping, the S-box, and the S-box combined with the Arnold Transform. The overall results indicate that the suggested method is superior to existing methods and that it has high security and low correlation coefficients.*

Keywords*: Image Encryption-Decryption, Skew tent map, Piecewise Linear Chaotic Map, CNNs, median Filter, gaussian Filter, Chosen-plaintext attack Security analysis.*

1- INTRODUCTION

Encryption, the act of transforming data from one form to another to guarantee that only authorized parties may access it, has become a vital foundation in today's digital world. With the exponential expansion in the flow of sensitive information across many platforms, safeguarding this data has never been more vital. Among the different forms of data that need comprehensive security, pictures retain special relevance because to their extensive usage in communications, multimedia, medical imaging, and other sectors. Image encryption, in recent years, has attracted substantial interest as an important field of study, with several approaches being developed to preserve the confidentiality and integrity of digital photographs. Many of these solutions employ chaos theory, which offers a good foundation for picture encryption owing to its ability to manage enormous data capacities and the strong correlation between pixels in digital images [1]. Chaos-based picture encryption methods are especially successful because they add a high degree of randomness and unpredictability core characteristics of a safe encryption process[2]. The expanding number of electronic device users, together with the proliferation of services on smartphones, tablets, and personal digital assistants (PDAs), has generated an urgent demand for safe, efficient means to store and transfer multimedia material, including photos[3].

The S-box approach has also emerged as a notable method for accelerating encryption by eliminating the need for multiple circular keys [4]. This method is particularly suitable for high-speed networks, where fast data transfer is essential. However, encryption methods based entirely on S-boxes have been criticized for their potential vulnerability to certain cryptographic attacks, especially in signal processing and image transmission. To address these limitations, more complex solutions have been proposed, such as combining substitution boxes (S-boxes) with the Arnold transform, which scrambles pixel locations in a chaotic manner. While this approach enhances security, it often requires a large key space, leading to increased computational demands and longer encryption times.

The S-box approach has also emerged as a notable method for accelerating encryption by eliminating the need for multiple circular keys [4]. This method is particularly suitable for high-speed networks, where fast data transfer is essential. However, encryption methods based entirely on S-boxes have been criticized for their potential vulnerability to certain cryptographic attacks, especially in signal processing and image transmission. To address these limitations, more complex solutions have been proposed, such as combining substitution boxes (S-boxes) with the Arnold transform, which scrambles pixel locations in a chaotic manner. While this approach enhances security, it often requires a large key space, leading to increased computational demands and longer encryption times.

In contrast to these earlier methods, our proposed approach uses dynamic key generation for each pixel through a sine-square logistic map, paired with multiple chaotic maps [5]. This combination significantly enhances security by ensuring that the encryption key for each pixel is unique and continuously changing, making it extremely difficult for attackers to predict or reverse the encryption process. Our study has shown that this technique offers greater protection against differential attacks and exhibits high sensitivity to changes in the plaintext image—two key factors in generating strong encryption [6]. Furthermore, statistical analysis demonstrates that our method results in a lower mean square error (MSE) and higher correlation coefficients compared to other existing techniques. Unlike many previous systems that select a random set of pixels for correlation analysis, our method evaluates all nearby pixels, ensuring a comprehensive assessment of the image's properties. This careful approach not only strengthens the security of the encrypted image but also highlights the effectiveness and reliability of the proposed encryption system.

Overall, our method represents a significant advancement in secure image encryption, making it well-suited for modern digital communication systems where both speed and security are crucial [7]. The current interconnected digital environment, characterized by the integration of emerging technologies, pervasive connectivity, and continuous data generation, has ushered in a new era of unprecedented opportunities and challenges. The following complex issues underscore the difficulties of managing privacy, security, and national interests in the digital age [8].

1. Privacy in the Surveillance Capitalist Era: Privacy rights and autonomy have been compromised by surveillance capitalism, which involves tech firms and digital platforms collecting, analyzing, and monetizing personal data. The monetization of personal data poses serious ethical and social problems regarding privacy and trust in digital ecosystems, from targeted advertising and behavioral profiling to algorithmic decision-making [9-16].
2. Threats and vulnerabilities in cybersecurity: Cyber hazards including malware, phishing, and ransomware threaten people, corporations, and governments globally. Advanced hackers and state-sponsored actors exploit weaknesses in digital infrastructure, networks, and IoT devices to disrupt essential services and steal sensitive data. The rising frequency and severity of cyber-attacks underline the critical need for effective cybersecurity solutions and proactive threat intelligence to preserve digital assets and reduce risks [17].
3. National Security and Data Sovereignty: Balancing national security imperatives with the preservation of people's rights to privacy and data sovereignty provides a complicated policy problem for governments and regulatory agencies. In an age of geopolitical tensions and information warfare, governments deal with the twin responsibility of preserving national security interests while upholding civil rights and democratic norms [12]. The rise of state-sponsored cyber-attacks, misinformation operations, and surveillance capabilities highlights the requirement for open, responsible, and rights-respecting approaches to cybersecurity and intelligence collection [13].
4. Regulatory Frameworks and Compliance Challenges: The developing regulatory environment, typified by the adoption of severe data privacy legislation such as the GDPR, CCPA, and the impending Digital Services Act (DSA), offers compliance issues for enterprises, technology organizations, and digital service providers. Navigating the complex regulatory frameworks, ensuring data transparency and accountability, and upholding consumer privacy rights require proactive governance, robust data management practices, and investment in privacy-enhancing technologies (PETs) such as encryption, anonymization, and differential privacy [14].
5. Ethical Dilemmas and Technological Disruptions: As AI, machine learning, and biometric identification systems continue to transform digital ecosystems and society norms, ethical issues are becoming increasingly important in conversations about digital rights, privacy, and security. The moral quandaries around data ownership, algorithmic prejudice, and the use of surveillance technologies prompt significant inquiries about the appropriate application of technology, safeguarding human rights, and upholding democratic principles in the digital era [15].

This research distinguishes itself through a novel approach to image encryption, moving beyond traditional S-box and static key methods. Its core innovation lies in the dynamic generation of encryption keys for each individual pixel, achieved through the synergistic application of a sine-square logistic map and multiple chaotic maps. This pixel-specific, continuously evolving an encryption strategy significantly elevates security, rendering it exceptionally resistant to differential attacks and enhancing sensitivity to plaintext alterations. Furthermore, the methodology's comprehensive correlation analysis, evaluating all neighboring pixels rather than a random subset, provides a more robust assessment of image properties. This meticulous approach not only strengthens the encrypted image's integrity but also contributes valuable insights into the effective utilization of chaotic systems for cryptographic purposes. By addressing the limitations of existing techniques and demonstrating superior performance in crucial security metrics, this work offers a substantial contribution to the field of image encryption, with direct relevance to securing sensitive visual data in modern digital communication systems.

The following sequence determines the remaining portions of this article. Some other previously used methods are presented in Section No. 2, some methods and frames are presented in Section No. 3, and the innovative image encryption method and its details, which will be used in the new chaotic system, are explained in Section 4 after a brief examination of several existing chaotic maps. Section 5 offers performance metrics. The findings of our system constructed utilizing the MATLAB environment for computer simulation are provided in Section 6. The findings obtained are given forth in Section 7.

2- PRELIMINARY LITERATURE REVIEW

With the widespread adoption of smart devices and high-speed networks, researchers are focusing on securing digital image applications, such as those in social media, healthcare, education, business, and defense, from unauthorized use. Additionally, with the fast increase of electronic data transmission, unlawful access to data is expanding. Information security against unwanted access is becoming increasingly vital in both data storage and data transit. Images are a common sort of information utilized in practically every part of life, making the security of image data against unwanted access vital [16].

Jamal et al. [12] presented a brand-new method for encrypting medical pictures. The key concepts are outlined as follows: the first. S-Boxes are Dynamic, the process creates substitution boxes (S-Boxes), which increase security and introduce unpredictability with each encryption session. Because of its dynamic nature, attackers find it challenging to predict the encryption pattern. The Second: Encryption Based on ROI, The Region of Interest (ROI), which contains important medical data, is the focus of encryption rather than the complete medical picture. By leaving the remainder of the picture, which is usually a black backdrop, unencrypted, encryption time and computing effort are decreased .

Third: Managing Big DICOM Pictures, the quantity of data handled is significantly reduced by encrypting just the ROI because DICOM pictures are often huge in size. This increases effectiveness without sacrificing the critical protection that sensitive areas require. Essentially, the study presents a novel method for medical picture encryption that addresses the unique difficulties associated with huge DICOM data. Through the use of dynamic S-Boxes and ROI encryption, the technique guarantees improved security and computational effectiveness. There may also be drawbacks to consider. While there is a computational cost savings when the black backdrop is left unencrypted, there may also be security risks. For instance, an attacker could be able to determine the kind of medical picture being utilized or infer details about the Region of Interest (ROI) if they get to view the image's unencrypted portions. The exposed background may also turn into an area of vulnerability for side-channel attacks [17]. In such assaults, attackers might extract important information about the encrypted sections of the picture by analyzing parameters such as processing time, power usage, or even electromagnetic emissions during the encryption process. This emphasizes how crucial it is to properly weigh security against computing performance when using selective encryption techniques.

Kumari et al. [9] developed an encryption method that combines DNA computation with Nonlinear Feedback Shift Registers (NLFSR). In this method, the NLFSR generates a pseudorandom sequence during the image permutation phase, which is essential for concealing the original image. The substitution process uses DNA computation to modify pixel values based on DNA-based operations in cipher block chaining mode. This approach enhances security by making the substitution dependent not only on the current pixel but also on the preceding ciphertext block. Due to the complexity of DNA operations and the unpredictable nature of NLFSR, this combination provides a high level of security, making it difficult to decrypt the encrypted image. Although this method is innovative, particularly with its use of DNA computation, it entails computational overhead, especially when processing large images. Furthermore, its practical implementation may be challenging due to financial and technological constraints.

Si et al. [10] presented a novel approach to medical image encryption that combines dynamic S-Boxes with ROI-based encryption. The use of dynamic S-Boxes enhances security by making the encryption process more resilient to attacks. On the other hand, encrypting only the Region of Interest (ROI), which is the critical part of the image, reduces the computational burden and improves efficiency. Since only the encrypted ROI needs to be stored, this method also saves storage space. However, there are potential drawbacks, including the risk of missing sensitive information if the ROI is incorrectly identified, the computational overhead associated with generating dynamic S-Boxes and determining the ROI, and possible incompatibilities with existing software and standards for medical imaging.

Gupta et al. [8] proposed an encryption methodology that combines watermarking and cryptographic algorithms. This approach breaks down an image into frequency bands using the Discrete Wavelet Transform (DWT) and embeds a hidden watermark in the image. To generate a session key, the secret image is first encrypted using a hybrid cryptographic method based on logistic chaotic maps and crossover. The watermark, which is the encrypted secret image, is then DWT-embedded within the original image. To further enhance security, the entire watermarked image is encrypted again using the same hybrid approach. The combination of watermarking and encryption increases security and is well-suited for Internet of Things (IoT) devices, as it enables error correction and detection while maintaining computational efficiency. However, its complexity, vulnerability to attacks, and potential processing costs are challenges that require further investigation and evaluation.

Niu et al. [14] implemented an encryption solution that uses symmetric encryption. The first step involves generating a random number generator, which is then used to rotate both the plain image and the key image reagreed upon by the sender and receiver. To create the encrypted image, the plain image and the permuted key are combined using an XOR technique. The computational efficiency of the XOR operation, along with the simplicity of the method, makes it ideal for smaller images, offering both efficiency and ease of use. The encryption is further strengthened by dynamic pixel permutation, which makes it more difficult for attackers to predict the process. However, the confidentiality of the key image is critical to the security of the technique; if it is compromised, the encryption can be easily broken. More advanced encryption methods and additional security layers would enhance overall security, as the XOR operation is inherently simple. Table .1 summarizes and compares different cryptographic methods.

Table 1: Comparison between different cryptographic methods

References	Method Description	Pros.	Cons.	Results (%)
Jamal,et al.2024) [12]	The study uses dynamic S-Boxes to encrypt just the ROI of medical pictures, improving security and efficiency. This method lowers data processing, making it suited for huge DICOM files while guaranteeing encryption unpredictability.	The technique enhances security using dynamic S-Boxes and increases efficiency by encrypting just the area of interest (ROI), making it optimal for processing extensive DICOM medical pictures.	The approach poses a risk of data exposure via unencrypted regions and may incur computational complexity due to dynamic S-Box formation and ROI detection.	NPCR 99.55 UACI 33.45 PSNR 8.39 COOR 0.003
Kumari, et al.2024 [9]	This encryption technique uses three main parts: a DNA computation for pixel value substitution, a Nonlinear Feedback Shift Register (NLFSR) to generate a pseudorandom sequence for image permutation, and Cipher Block Chaining (CBC) to guarantee that each encrypted block depends on the preceding ciphertext block. By adding unpredictability and interdependency between encryption blocks, this combination improves security.	The approach provides great security by combining NLFSR's unexpected pseudorandom sequence with the complexity of DNA computing. This revolutionary application of DNA computing for picture encryption offers a distinct and unique layer of safety.	The approach challenges computational cost because of the expensive nature of DNA-based processes, especially for big pictures. Additionally, applying DNA computations in real- world applications offer practical hurdles, including technological restrictions and high prices.	NPCR 99.59 UACI 33.35 PSNR 8.69 COOR 0.0004
Si, Zhao et al.2023 [10]	The paper offers a technique for encrypting big DICOM medical pictures utilizing dynamic S-boxes and region-of-interest (ROI) encryption, boosting security and minimizing computing effort by concentrating on essential image regions. However, it poses possible weaknesses, such as assaults on unencrypted parts. While promising, additional study is necessary to overcome these security vulnerabilities.	The approach boosts security by leveraging dynamic S-Boxes, making it more resistant to assaults. It also enhances efficiency by encrypting just the area of interest (ROI), which saves computational overhead. Additionally, the technique decreases storage requirements because only the encrypted ROI must be saved.	The approach introduces concerns of information leakage if the ROI is misinterpreted, possibly leaving sensitive data unprotected. It may also incur computational costs from producing dynamic S-Boxes and potentially encounter compatibility concerns with current medical imaging standards and software	NPCR 99.43 UACI 33.35 PSNR 28.69 COOR 0.0004

Gupta, Shukla et al.2022 [8]	The research study offers a unique encryption approach for picture transmission in Internet of Things (IoT) contexts, boosting security and error detection by integrating watermarking and cryptographic algorithms. It leverages Discrete Wavelet Transform (DWT) to breakdown pictures, embeds a secret watermark, and combines hybrid cryptography using logistic chaotic maps to produce a session key. The procedure comprises encrypting the secret picture, embedding it into the original image as a watermark, and finally encrypting the complete watermarked image for safe transmission.	The approach strengthens security by merging watermarking with encryption, offering a solid layer of protection. It also permits detection of mistakes and repair via the encoded watermark, assuring data integrity throughout transmission. Furthermore, the combination of Discrete Wavelet Transform (DWT) and a lightweight cryptographic algorithm provides computing efficiency, making the technique well- suited for IoT devices.	The method's complexity rises owing to the integration of numerous methodologies, making implementation more complicated. Its efficacy is also subject to the choice of wavelet coefficients and embedding techniques, while the encryption and decryption operations may add computing cost, lowering speed.	NPCR 99.56 UACI 33.22 PSNR 9.69 COOR 0.002
Niu, Ying, and Xuncai Zhang et al.2020 [14]	The encryption approach security using symmetric encryption paired with dynamic pixel permutation. It employs an XOR operation to mix the plain picture with the key image, while a random number generator shuffles the pixels before the XOR procedure. The total technique comprises generating random numbers, permuting the pictures, and performing the XOR function to generate the encrypted image.	The technique has various advantages, such as simplicity from the efficient XOR operation, making it especially ideal for tiny pictures. Additionally, dynamic pixel permutation helps security by increasing complexity, making the encryption more resistant against prospecti ve assaults.	The approach has considerable limitations, notably its dependence on the secrecy of the key image; if the key is compromised, the encryption may be quickly cracked. Furthermore, the simplicity of the XOR technique restricts the complexity of the encryption, possibly exposing it to flaws despite the improved protection from dynamic permutation.	NPCR 99.75 UACI 33.32 PSNR 9.23 COOR 0.003

3- METHODS AND FRAMEWORK

In our quest to achieve high levels of security and privacy, and to build a robust system that effectively encrypts images while protecting them from various attacks and unauthorized access, we have designed a strong encryption system. Initially, we use image masking, where the image to be encrypted is hidden within another image as a cover for the original. For example, we employ a masking method such as Discrete Cosine Transformation (DCT), then integrate these cover images into our encryption system[18].

Next, we designed a hybrid approach that utilizes multiple chaotic maps. According to chaos theory [11,19], a known nonlinear dynamic system behaves in a predictable manner but exhibits dynamics that are highly sensitive to initial conditions. Two fundamental characteristics of chaotic systems are the mixing feature and the sensitivity to initial conditions [3,20]. To control the encryption process and generate the chaotic sequence, a chaotic map is employed. Chaos streams are produced using various chaotic maps (CMs). We examine two specific maps and evaluate their behaviors. We used several CMs to generate these maps. The decoding of these maps is provided below[21].

3. 1. Logistic Map

One of the moderately nonlinear chaotic discrete systems, the logistic map, displayed chaotic behavior. The following are some characteristics of 1D CS. [1, 13, 22]:

$$X_{n+1} = \mu X_n (1 - X_n) \quad (1)$$

Where μ the control parameter $\mu \in [0, 4]$, When n is the total number of duplicates, $X \in [0, 1]$, The disorderly behavior is acknowledged when $\mu \in [3.57, 4]$.

3.2 Tent Map

Tent maps are the second form of map used in our concept. In mathematics, the tent map [1,2,23] is a repeating function in the shape of a tent that forms a discrete-time dynamical system. It translates a point X_(n) on the real line to another point.

$$X_{n+1} = \begin{cases} \mu X_n & \text{for} \quad X_n < 0.5 \\ \mu(1 - X_n) & \text{for} \quad 0.5 \leq X_n \end{cases} \tag{2}$$

where μ is a positive real chaotic constant. The tent map demonstrates a range of dynamical behavior ranging from predictable to chaotic relied on the value of μ.

3.3 Quadratic Map

Because it is a second order non-linear equation, the quadratic map is one of the sorts of systems that exhibit chaotic behavior. Ref. [1,2, 24] provides a description of the traditional quadratic map equation.

$$X_{n+1} = f_c(X_n) = X_n^{\,2} + c \tag{3}$$

Where the amount of iterations is n and X∈ [0, 1]. Critical points for an analytic map are positions where $f'(X_C) = 0$. Every stable cycle attracts at least one critical point. $X_C = 0$ is recognized as the lone crucial point in quadratic map. Therefore, it can have only one appealing cycle and XC is used as the beginning point to discover the cycle. The second fixed point is always repulsive. For |x| > x2 iterations go to infinity. For |x| < x2 they travel to the attractive fixed point x1. This gap is the foundation of attraction of the point [25].

3.4 Bernoulli Map

Another common map for encryption is the Bernoulli map, sometimes known as the 2 x mod1 maps [8,9]. A Bernoulli process is a discrete random process that consists of an infinite or finite sequence of independent stochastic variables X1, X2, X3,... such that for each i, the value of Xi is either 1 or 0. For all values of i, the probability of Xi =1 is the same amount. The Bernoulli process, at each given time, is a future trial independent of previous trials. The Bernoulli map [26] is defined as:

$$X_{n+1} = \begin{cases} 2X_n & 0 \leq X_n < 0.5 \\ 2X_n - 1 & 0.5 \leq X_n < 1 \end{cases} \tag{4}$$

3.5 Cubic Map

One of the discrete systems and small nonlinear chaotic that best exemplify chaotic method is a cubic map [1–5,27]. It is described by

$$X_{n+1} = f(X_n) = \mu X_n^{\,3} + (1 - \mu) X_n \tag{5}$$

where μ is the chaotic factor and the number of iterations is n. When x ∈ [0, 1], μ ∈ [0, 4] in which, the chaotic procedure is recognized when μ ∈ [3.57,4].

3. 6. Skew Maps.

The asymmetric skew tent map also was configured to be a skew map and is written as

$$X_{n+1} = \begin{cases} B_{Sk}\, X_n & ;\ \mathrm{Xn} \in [0, \beta\mathrm{sk}] \\ (1 - \mathrm{Xn})/(1 - \beta\mathrm{sk}) & ;\ \mathrm{Xn} \in [\,\beta\mathrm{sk}, 1] \end{cases} \quad (6)$$

The control parameter, βsk, can range from 0 to 1. These maps have a larger dispersion rate than tent maps and sine maps. As a result, these maps are widely used in the bulk of cryptographic applications [15, 28].

3.7. Piecewise Linear Chaotic Map.

The piecewise chaotic map is expressed as

$$X_{n+1} = \begin{cases} \mathrm{Xn}/\gamma\,, & 0 \le \mathrm{Xn} < \gamma \\ \mathrm{Xn} - \gamma/0.5 - \gamma, & \gamma \le \mathrm{Xn} \end{cases} \quad (7)$$

The control parameter γ , which has a range of values from 0 to 1, is where. When (0,1) such that can be used as the secret key, the map behaves chaotically[16,29].

4- PROPOSED IMAGE ENCRYPTION AND DECRYPTION SYSTEMS

The maps' advantages include superior random sequence creation and uniform invariant distribution, which makes this map more appropriate for picture encryption. Instead of being utilized for the confusion and diffusion process, this map is more suited for creating a key with a bigger key space[30].

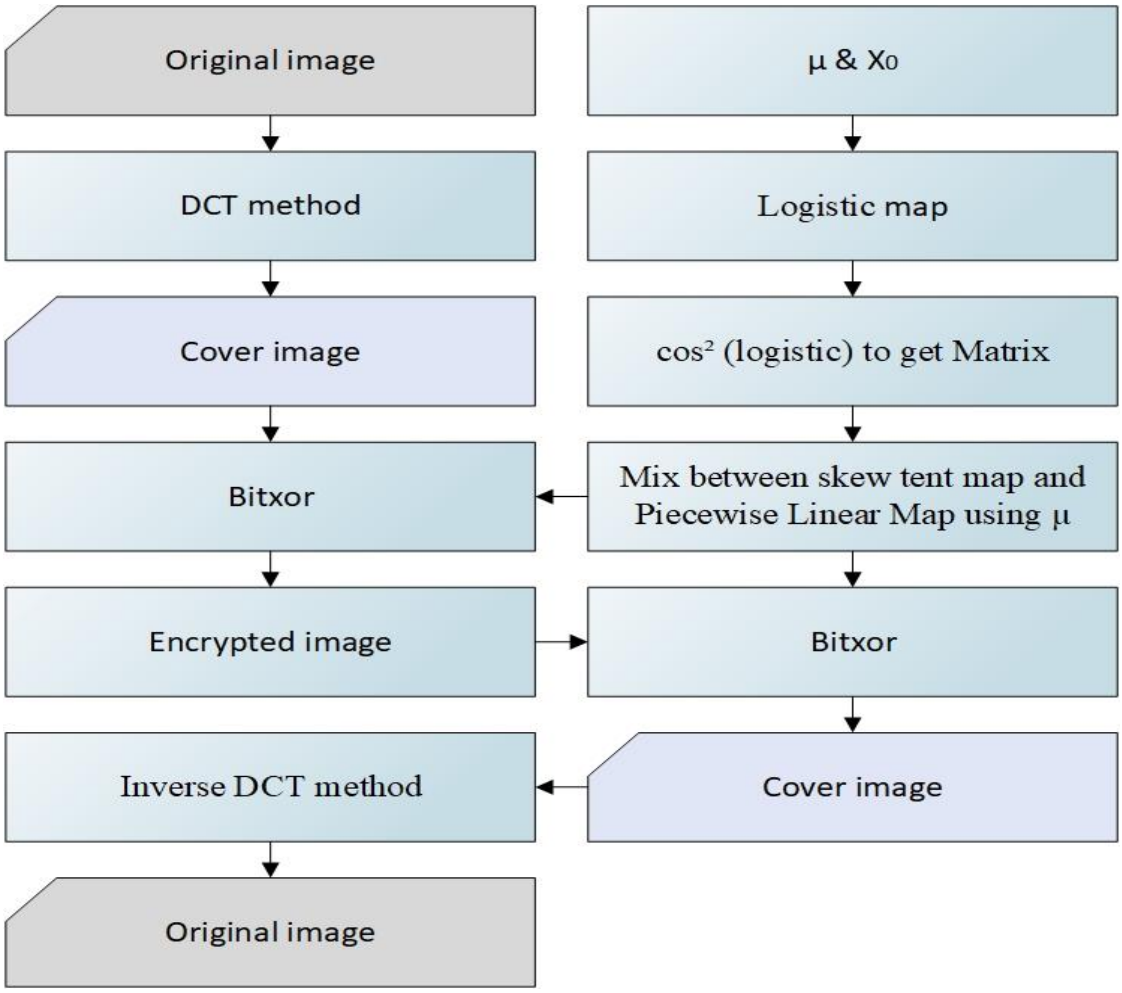


Figure1: Scheme of suggestion Chaotic map system with initials condition μ = 3.99999 and X_0 = 5.333

Detailed in the flowchart that follows. It summarizes the explanations provided in the equations above. Figure 1 illustrates how to obtain a logistic map using the fundamental values = 3.99999 and X (0) = 5.333. After that, As the values on the resulting logistic map run from 0 to 255, we calculated $\cos^2$, giving us a range of 0 to 0.96., from which we obtained variable control parameter' ranging from 0 to 0.96. The next stage is to create a new map by combining the pieces of a skew tent map and a piecewise linear chaotic map. In the end, this new chaotic map was chosen to multiply with the original image using XOR to produce the encrypted image. In a similar manner, we multiplied the encrypted image with the new chaotic map to produce the original image [31].

4.1 Steganography Algorithm System.

Figure 2 illustrates the procedure for masking the original picture in various dimensions, concealed behind another counterfeit image of equal or greater size. Given an size $(u * v)$ plain gray image P , the cover image C and the Steganography image S .The Steganography and encryption steps are shown as follows:

Step 1: Image Acquisition

Input: Obtain the cover image C (u, v) and the secret image P (u, v) that will be hidden inside the cover image.

Step 2: Apply Discrete Cosine Transform (DCT)

Apply the Discrete Cosine Transform (DCT) on the cover picture to transfer it into the frequency domain. This decomposes the picture into distinct frequency components as in Eq (8).

cover = imresize(cover image, [u, v])

secret = imresize(secret image, [u, v]

originalImage = double(cover)

secretImage = double(secret)

dctOriginal = dct2(originalImage);

alpha = 0.09

*dctStego = dctOriginal + alpha * secretImage*

$$S(u, v) = DCT(C(u, v)) + \alpha * P(u, v)) \quad (8)$$

Where

S (u, v) is the steganography image (the cover picture containing the concealed message).

C (u, v) is the Discrete Cosine Transform of the cover picture.

α is the embedding strength parameter which we used it equal 0.097

P (u, v) is the secret image (the hidden message). We initially hide the original image inside another fake image as a cover for the original image.

Step 3: Determine Embedding Locations

Determine the embedding locations within the DCT coefficients. Typically, coefficients in the low-frequency range are selected as they are less sensitive to changes and can better withstand noise. Create the steganography image (the cover picture containing the concealed message) S (u, v). *steoImage = idct2(dctStego)* transform the type of chaotic matrices from double to uint8.

4.2 Encryption algorithm system

Our plan uses a combination of the chaotic maps outlined above for increased security and effectiveness. Figure 2 depicts our hybrid pipeline, which comprises of numerous successive phases using various chaotic maps. With the initial conditions of x and the control parameter μ .

Input: the steganography image S (u, v) that the cover picture containing the concealed message.

Step 4: Generate the logistic map using the following equation where n represents the number of iterations and μ is the control parameter $0 \leq \mu \leq 4$, $Xn \in [0,1]$ using Eq. (9) which has the same size of original image ($u * v$).

$$X_{n+1} = \mu X_n (1 - X_n) \quad (9)$$

Step 5: Produced variable control parameter B'_{Skn} with size ($u * v$) by finding cos² for the every values of logistic map's pixels that will be given by Eq. (10) to obtained values from 0 to 1, $B'_{Skn} \in [0, 1]$. Acquiring variable keys for the development of novel chaotic maps that address the deficiencies of existing approaches, and the challenges associated with key identification or prediction.

$$B'_{Skn} = cos^2 (\mu X_n (1 - X_n)) \quad (10)$$

where n is the number of iterations and μ is the chaotic factor. The chaotic process is identified when $\mu \in [3.57,4]$, where $x \in [0,1]$, and $\mu \in [0, 4]$.

Step 6: establishing the variable control parameter γ'_n with size (u ∗ v) by as in step 5 but using cos² cubic map which given by Eq. (11) which produce values from 0 to 1, $\gamma \in [0, 1]$,

$$\gamma'_n = cos^2\ \mu X_n{}^3 + (1-\mu)\, X_n \tag{11}$$

where μ is the chaotic factor and the number of iterations is n. When x ∈[0, 1], μ∈[0, 4] in which, the chaotic procedure is recognized when μ ∈ [3.57,4].

Step 7: We have done many experiments to come up with the best mix between both maps in Eq (6) and Eq (7) to give the best results and discover a new chaotic map and new equation that is following by Eq(12), corresponding matrix **A** using the variable control parameter that produced in step 5and step 6. Consequently, enhanced security rates are seen while using encryption compared to earlier conventional methods.

$$X_{n+1} = \begin{cases} B'_{Sk1}\, X_n & 0 < X_n \le B_{Sk} \\ Xn/\gamma'1 & B_{Sk} < X_n \le \gamma'1 \\ (1-Xn)/(1-\ B'_{Sk2}) & B_{Sk2} < X_n \le \gamma'2 \\ Xn-\gamma'2/0.5-\gamma'2 & \gamma 2\ < X_n < 1 \end{cases} \tag{12}$$

Where $\beta'_{sk}1$ is the first control parameter and it takes any value from 0 to 0.25, $\beta'_{sk1} \in (0,0.25)$, and $\beta'_{sk}2$ is the second control parameter and it takes any value from 0.5 to 0.75, $\beta'_{sk1} \in (0.5,0.75)$,also where γ'_1 is the control parameter and it takes any value from 0.25 to 0. 5 , $\gamma'_1 \in (0.25,0.5)$, and γ'_2 is the second control parameter and it takes any value from 0.75 to 1, $\gamma'_2 \in (0.75,1)$.

Step 8: developed the output of step 7 (the new chaotic map **A**) and create the best mix of maps in Eq (2), Eq (3), Eq (6) and Eq (7) to generate the new robust chaotic map corresponding matrix **B** that produced using Eq(13).

$$X_{n+1} = \begin{cases} \mu' X_n{}^2 & 0 < X_n \le 0.25 \\ Xn/\gamma' & 0.25 < X_n \le \gamma' \\ (1-Xn)/(1-\ B'_{Sk}) & B'_{Sk} < X_n \le 0.75 \\ \mu'(1-X_n) & 0.75\ < X_n < 1 \end{cases} \tag{13}$$

Where μ' the control parameter μ∈[0, 4], When n is the total number of duplicates, X∈ [0, 1], and where γ' is the control parameter for second part in Eq (13) and it takes any value from 0.25 to 0. 5, $\gamma' \in (0.25,0.5)$, also where β'_{sk} is the control parameter for third part in Eq(13) and it takes any value from 0.5 to 0.75. Then used again μ' in the last part in Eq (13).

Step 9: apply the encryption process for the steganography image S (u, v) which contained the original image inside using Bit XOR with one of two matrix **A , B** that we developed in step 7and step 8 . The chouse between two map depended on the best result of correlation for each one (Comparison the result of correlation and feedback)
correlation = min ([corr1, corr2]).

```
for u = 1: u
    for v = 1: v
      Encrypted image (u,v) = bitxor (S(u,v),A(u,v));
      Encrypted image (u,v) = bitxor (S(u,v),B(u,v));
    end
end
```

Table2:Summary of the adapted equations used in the proposed image encryption algorithm

Algorithms	Previous Methods	Proposed Methods
Logistic Map	$X_{n+1} = \mu X_n (1 - X_n)$	$B'_{Skn} = cos^2 (\mu X_n (1 - X_n))$
Cubic Map	$X_{n+1} = f(X_n) = \mu {X_n}^3 + (1 - \mu) X_n$	$\gamma'_n = cos^2 \mu {X_n}^3 + (1 - \mu) X_n$
Tent Map	$X_{n+1} = \begin{cases} \mu X_n & \text{for } X_n < 0.5 \\ \mu(1 - X_n) & \text{for } 0.5 \le X_n \end{cases}$	$X_{n+1} = \begin{cases} \mu' {X_n}^2 & 0 < X_n \le 0.25 \\ Xn/\gamma' & 0.25 < X_n \le \gamma' \\ (1 - Xn)/(1 - B'_{Sk}) & B'_{Sk} < X_n \le 0.75 \\ \mu'(1 - X_n) & 0.75 < X_n < 1 \end{cases}$
Quadratic Map	$X_{n+1} = f_c(X_n) = {X_n}^2$	
Bernoulli Map	$X_{n+1} = \begin{cases} 2X_n & 0 \le X_n < 0.5 \\ 2X_n - 1 & 0.5 \le X_n < 1 \end{cases}$	
Skew Maps	$X_{n+1} = \begin{cases} B_{Sk} X_n & ; Xn \in [0, \beta sk] \\ (1 - Xn)/(1 - \beta sk) & ; Xn \in [\beta sk, 1] \end{cases}$	$X_{n+1} = \begin{cases} B'_{Sk1} X_n & 0 < X_n \le B_{Sk} \\ Xn/\gamma'1 & B_{Sk} < X_n \le \gamma'1 \\ (1 - Xn)/(1 - B'_{Sk2}) & B_{Sk2} < X_n \le \gamma'2 \\ Xn - \gamma'2/0.5 - \gamma'2 & \gamma 2 < X_n < 1 \end{cases}$
Piecewise Linear Chaotic Map	$X_{n+1} = \begin{cases} Xn/\gamma, & 0 \le Xn < \gamma \\ Xn - \gamma/0.5 - \gamma, & \gamma \le Xn \end{cases}$	

In the following table 2, we provide a summary of the equations that were utilized in the process of deriving the new formulas that are utilized in our cutting-edge encryption system, which is designed to achieve high efficiency and robust security.

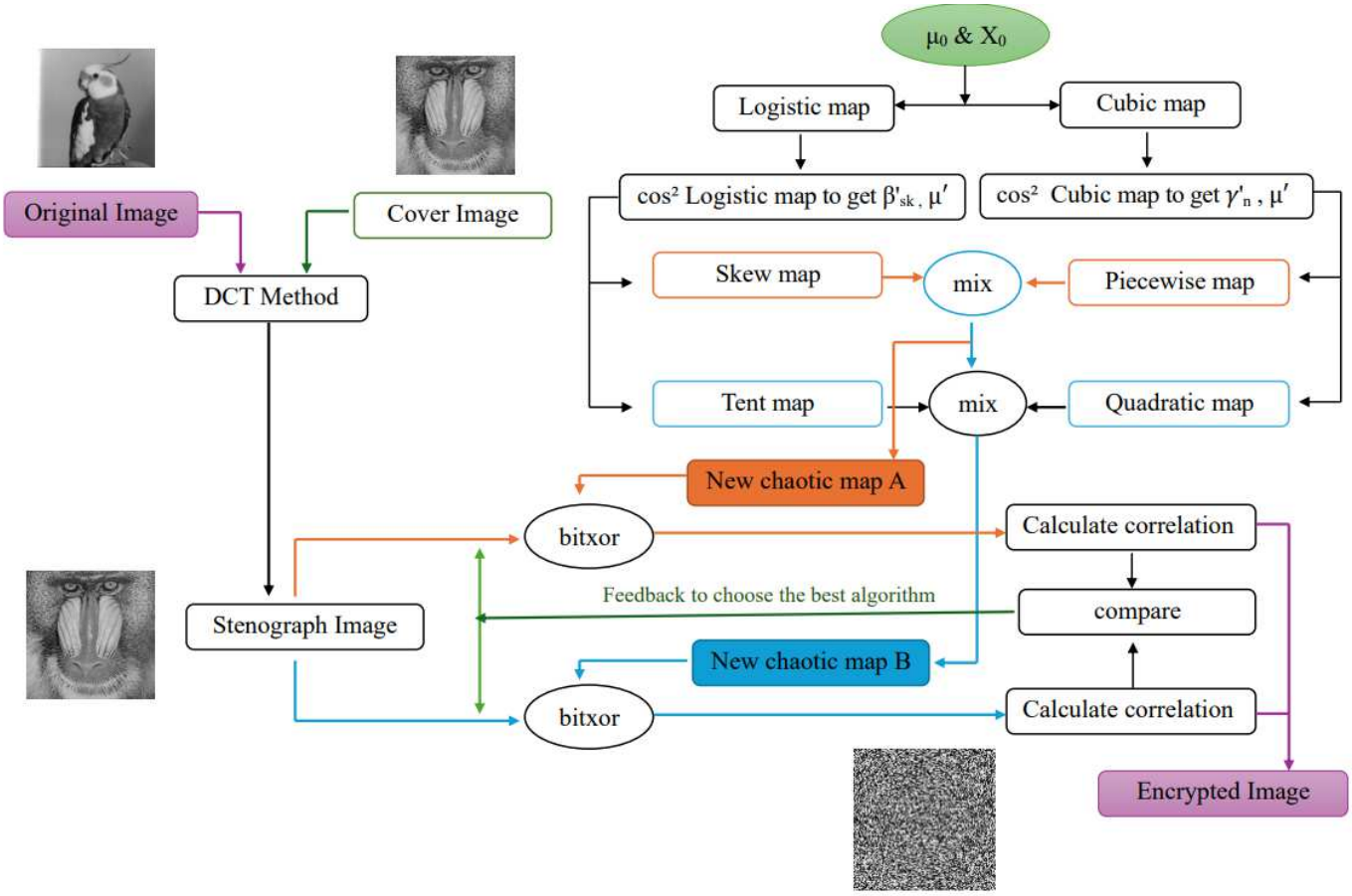


Figure2: Scheme of suggestion Encryption Chaotic map system with initials condition μ = 3.99999 and X_0 = 5.333

Figure .2 illustrates the algorithm steps explained in the Encryption System, how various chaotic maps, such as the Logistic, Cubic, Skew, Piecewise Tent and Quadratic maps, were utilized to generate stronger new maps such as A and B maps. These new maps were then applied to encrypt the input image within the system we designed based on our proposed approach. Additionally, the original images intended for encryption were concealed within other decoy images to enhance security. The selection of a specific chaotic map is based on achieving the best correlation output among all the tested maps, to ensure the most effective encryption and achieve optimal system performance, the selection of the new chaotic map can be based on various criteria such as execution time, entropy, PSNR and MSE. This flexibility allows the system to dynamically adapt its choice depending on the desired optimization parameter.

4.3 Decryption algorithm system

Figure 3 will depict the decryption process and the extraction of the original picture from the cover image, along with our purification method intended to eliminate noise and any interference from the extracted image. These steps will be reviewed as follows.

Step 10: apply the decryption process by multiple the encryption image (that have the secret image inside) BitXOR with the proposed chaotic maps **A** or **B** that are used in the encryption algorithm to generate S (u, v) which is the steganography image (the cover picture containing the concealed message).

for u = 1: u

for v = 1: v

Decrypted image (u,v) = bitxor (Encrypted image (u,v) ,A(u,v));

Decrypted image (u,v) = bitxor (Encrypted image (u,v),B(u,v));

end

end

4.4 Invers Steganography Algorithm System

Step 11: We apply the inverse DCT method to extract the original image P (u, v) that is hidden inside the fake image C (u, v) that we used in step 1 to Retrieved Secret image R (u, v) from the steganography image S(u,v).

Retrieved decryption = dct2(Decrypted image)
R (u, v) = *(Retrieved decryption - dctOriginal) / alpha;*

4.5 Filter Algorithm System

Many filters have been applied to the image in Figure 3 to get the best result with autoencoder (CNNs).

Step 12: we used autoencoder (CNNs) convolution neural networks with different filters like the median filter, gaussian filter and combined between them to improve the image extracted and denoising image after the masking process to avoid any interference with it

Input: the noisy image R (u, v).

Step 13: Employ convolutional layers (Conv2D) to extract features from the corrupted picture. Every convolutional layer utilizes filters to identify patterns in images.

First Convolution Layer:

$$FeatureMap1(u, v) = ReLU(Conv2D(R(u,v)))$$

Max Pooling (optional) is used to reduce the dimensionality of the feature map:

$$PooledMap1(u, v) = MaxPooling(FeatureMap1(u,v))$$

Step 14: The noisy image is encoded into a latent space (low-dimensional representation) via additional convolutional and pooling layers.

$$LatentRepresentation\ (u,v)=Conv2D(PooledMap1(u,v))$$

Step 15: This step restores the picture by undoing the compression, returning it to its original resolution.

$$UpsampledMap1(u,v)=UpSampling2D(LatentRepresentation(u,v))$$
$$ReconstructedImage(u,v)=Conv2DTranspose(UpsampledMap1(u,v))$$

Step 15: These filters assist in eliminating various forms of noise from the reconstructed picture to enhance its quality.

Median Filter: Reduces salt-and-pepper noise.

$$DenoisedImage(u,v)=MedianFilter(ReconstructedImage(u,v))$$

Gaussian Filter: Smooths the image and reduces Gaussian noise.

$$DenoisedImage(u,v)=GaussianFilter(ReconstructedImage(u,v))$$

Combined Filters: Use both filters sequentially to enhance the image:

$$EnhancedImage(u,v)=Combine(MedianFilter,GaussianFilter,ReconstructedImage(u,v))$$

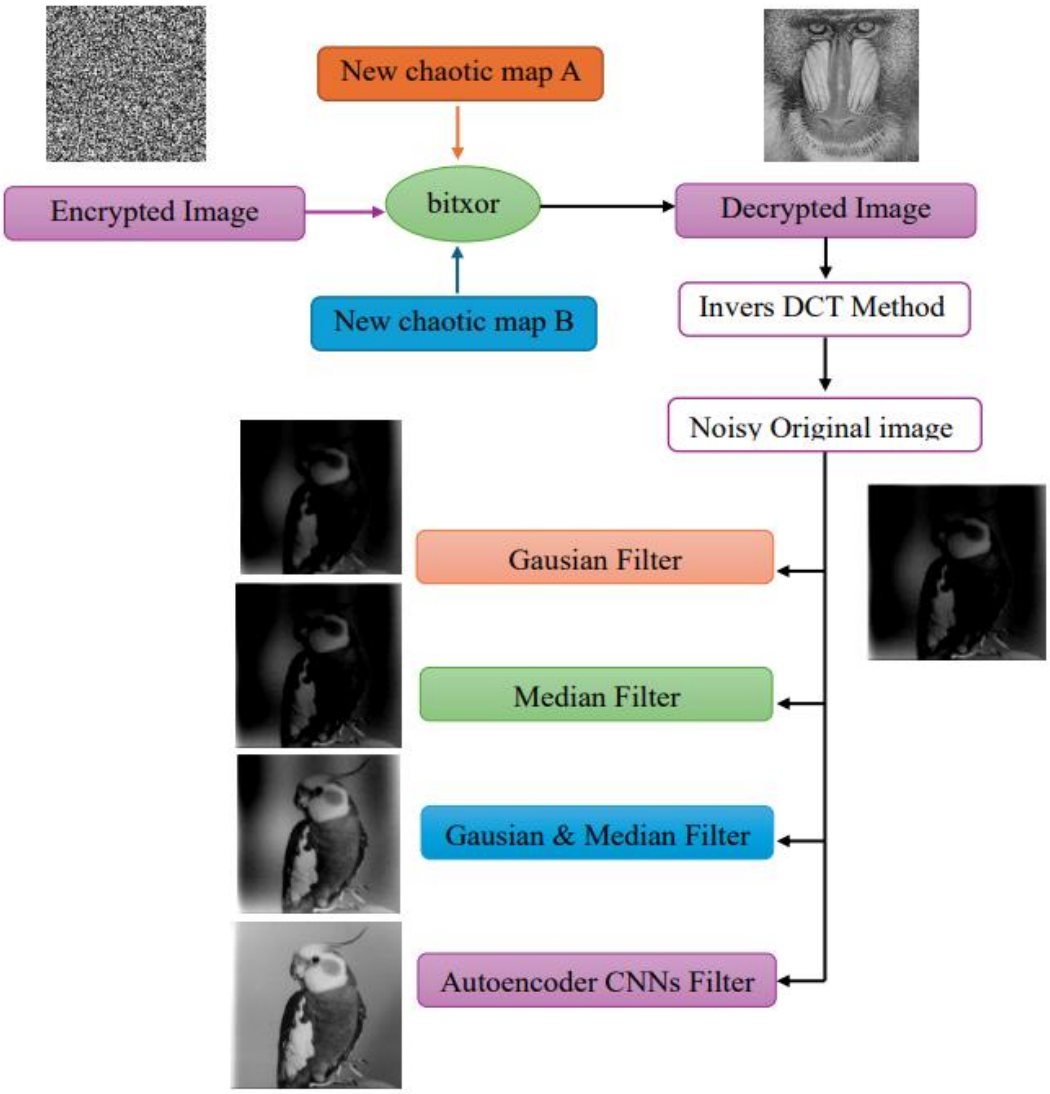


Figure 3: Scheme of suggestion Decryption Chaotic map system and its filter system

5. PERFORMANCE METRICS

To evaluate how effectively our system worked, we used plaintext sensitivity analysis (Differential analysis) as a unified average changing intensity and net pixel change rate[18,19,32]. Also, in order to demonstrate the effectiveness of our system, we employed deferential attacks such correlation coefficient, peak signal to noise ratio (PSNR), and mean absolute error (MAE).

5.1. Plaintext sensitivity analysis.

The cryptographic tool modifies one bit, or often one pixel, to compare the altered plain and cryptographic images to build a beneficial link between them and to ascertain the secret key. In an effort. basic visual. Differential cryptanalysis [7,12,33] is the term used in cryptography to describe this type of analysis. Such differential analysis may become useless if a small change in the normal image results in big changes to the encrypted image. Two of the most popular measurements, net pixel changes rate (NPCR) and unified average changing intensity (UACI), are used to examine the effects of a single pixel alteration on the entire cypher image. Let's call two encrypted photos CI1 and CI2, whose related original images only differ by one pixel. Please identify the grayscale values for the grid(i,j) pixels in CI1(i,j) and CI2(i,j) as well. Give the pictures CI1 and CI2 the same size as the bipolar array d. Then, Diff(i,j)is determined by CI1 (i,j) and CI2 (i,j), namely, if CI1(i,j) $\neq$ CI2 ((i,j) then Diff(i,j)= 1; otherwise, Diff(i,j)= 0.The NPCR [5,2,34] is realized as :

$$NPCR = \frac{\sum_{i,j} Diff(i,j)}{W \times H} \times 100\% \quad (9)$$

where the images' height and width, respectively, are H and W. The UACI, on the other hand, entails altering the intensity of the relevant pixels in both the plain image and the cypher image. The encryption technique is more resistant to the differential attack the larger the UACI. According to the UACI [4,22,35],

$$UCAI = \frac{I}{W \times H} \sum_{i,j} \left[\frac{CI1(i,j) - CI2(i,j)}{255} \right] \times 100\% \quad (10)$$

The values of 99.69 and UACI 33.4653 provide the NPCR value for two random pictures, a foreseeable approximation for a well-known encryption algorithm. The NPCR value and UCAI for the suggested approach are determined to be 99.698 and 34.28, respectively. The suggested image encryption method appears to be extremely sensitive to plaintext, hence it is immune to differential assaults [23,36].

5.2. Mean absolute error (MAE).

The grey levels (GLs) in the photographs are specific and represented by C(i, j) [37]. Moreover, the GLs that each individual pixel at a specific place obtains are shown as P (i, j). The cypher has the following measurements: WH. With two pictures, Get the sum of the subtractions and the resulting MAE is defined as:

$$MAE = \frac{I}{W \times H} \sum_{j=1}^{W} \sum_{i=1}^{H} |C(i,j) - P(i,j)| \quad (11)$$

5.3. Peak signal to noise ratio (PSNR).

The peak signal-to-noise ratio (PSNR) [9,15,38] of the original and encrypted images is calculated as follows.

$$PSNR = 10 \log_{10} \frac{W \times H \left[\max_{1 \le i \le m, 1 \le j \le n} \{Pi,j\} \right]^2}{\sum_{j=1}^{W} \sum_{i=1}^{H} (Pi.j - P\prime i,j)^2} \quad (12)$$

where the original image's height and width are w and h, and the original image's and the cypher image's respective values of pixels are Pij and Pij. PSNR is an estimation of an encryption planner that reflects the goodness of encryption [24,39]. A lower PSNR number results in higher-quality encryption. In the suggested plan, it is roughly 8.3.

5.4 Correlation coefficient analysis.

The histogram analysis and entropy analysis both demonstrate the overall unpredictability of an image. We must examine surrounding pixels to pinpoint the differences between the structure's characteristics before and after encryption. can be used to figure out how two pixels that are pointing in different directions are related [25,40].

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)\sqrt{D(y)}}} \quad (13)$$

Where

$$cov(x,y) = \frac{1}{N} \sum_{j=1}^{N} (X_j - E(X))(Y_j - E(Y)) \quad (14)$$

Where the number of selected neighboring pixels N is calculated as W×H, where H and W are the image sizes required to display the entire scrambling image, and cov (x, y) is covariance of random variables X and Y. A decreased correlation between adjacent pixels must be achieved for effective encryption and impedance qualities. The definition of the coefficient correlation is,

$$D(x) = \frac{1}{N} \sum_{j=1}^{N} (X_j - E(X))^2 \quad (15)$$

$$D(y) = \frac{1}{N} \sum_{j=1}^{N} (Y_j - E(y))^2 \quad (16)$$

$$E(X) = \frac{1}{N}\sum_{j=1}^{N} X_j \quad (17)$$

$$E(Y) = \frac{1}{N}\sum_{j=1}^{N} Y_j \quad (18)$$

For random variables X and Y, the standard deviations are denoted as (D(x)) and (D(y)) respectively. where x and y are the neighboring pixel intensities. N is the number of surrounding pixels selected. In our experiments, we selected each adjacent pixel to determine connectivity [26,41].

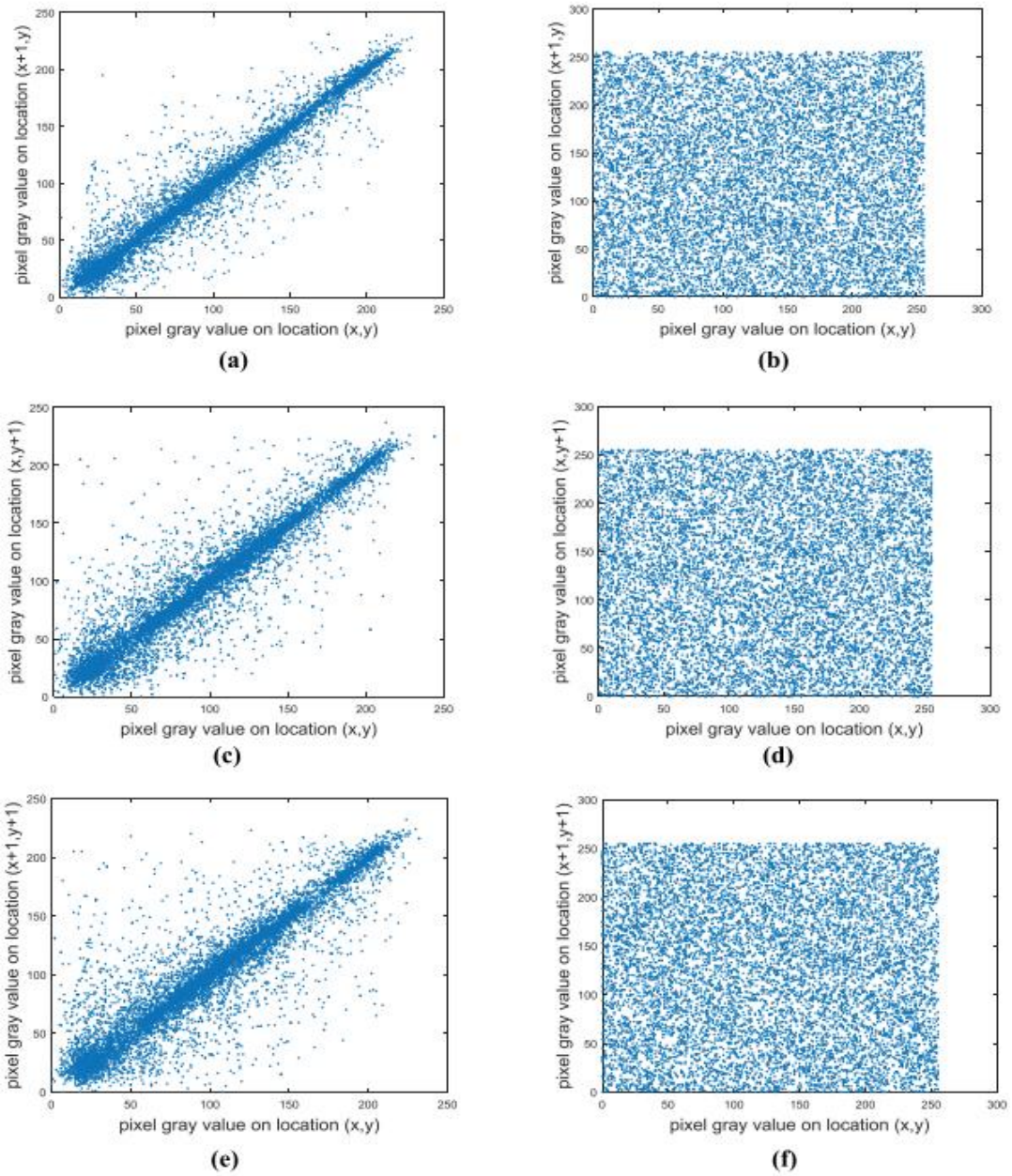


Figure 4: The correlation between colored-Lena plain-image (a–c) and equivalent ciphered-image (d–f)

The correlations of two neighboring pixels will be shown in Figure 4. There will be a horizontal correlation in the plain image Lena and a cipher image, a vertical correlation in the plain image and a cipher image, a diagonal correlation in the plain image, and a cipher image diagonal correlation.

5.5 Structural similarity index measure (SSIM)

When comparing a decrypted image to its original input image, SSIM is used to measure image quality [41.42]. The recovery of a high-quality picture is related with an SSIM value of one. The SSIM value ranges from -1 to 1. The following formula is used to calculate similarity.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2 \quad +\sigma_y^2 \quad +C_2)} \tag{19}$$

where μ_x and μ_y are the corresponding pixel sample means of images X and Y. The variances of X and Y are denoted by σ^2_x and σ^2_y, respectively. The cross-correlation between X and Y is denoted by σ_xy. $C_1=(k_1L)^2$ and $C_2=(k_2L)^2$ are variables. With L being the dynamic range of the pixel value (L=2Numberofbitsperpixel−1) and k1=0.01 and k2=0.03 as default values, stabilizes the division with weak denominator. A visualization of SSIM with a variable noise factor using 1000 iterations is shown in Figure 5. The plot indicates that when the noise factor (k) increases, the SSIM value drops [43].

The plotted graph depicts the connection between the Structural Similarity Index (SSIM) and the noise factor for the original, encrypted, and denoised image after using CNN autoencoder, giving an important assessment of the encryption system's strength. The original picture curve is used as a baseline, demonstrating the natural loss of image quality due to noise. The encrypted picture curve shows very unstable SSIM values, suggesting successful encryption by making the content unidentifiable. The decrypted picture curve, which is ideally near to the original, demonstrates the system's ability to properly reconstruct the image after decryption. This research is critical for assessing encryption performance, noise resistance, and the balance between security and picture quality. A robust encryption technique should guarantee that the decrypted picture has high SSIM values despite noise, exhibiting resilience while keeping critical features. The findings inform the development of encryption algorithms, improving their noise resistance and providing safe but accurate picture reconstruction, which is especially important in optical encryption and secure image transmission applications.

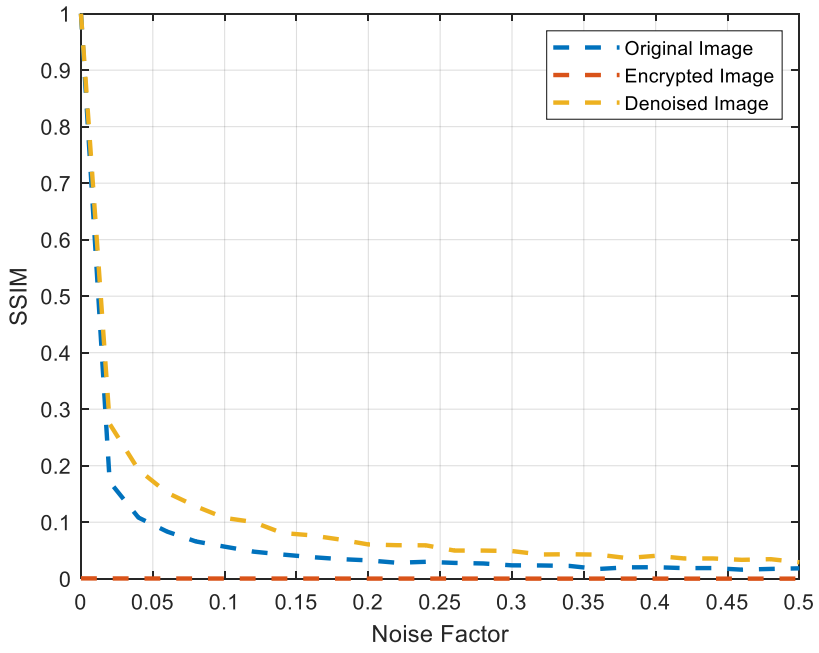


Figure 5: SSIM plot the images of Lena and Baboon with the noise-factor (k)

5.6 Pixels cropped analysis

The development of more resilient encryption algorithms that can effectively handle data loss and improve the security of encrypted information depends on this study, which is crucial for assessing an encryption system's resistance to partial interference and assaults. This connection evaluates the resilience of the system against partial deterioration or noise. A very robust and dependable encryption strategy is demonstrated if the Mean Squared Error (MSE) stays low even as the occluded region grows. This shows that the system can successfully recover the picture even in the event of data loss [44]. On the other hand, if the MSE rises significantly with the occluded area, it indicates that the system is extremely susceptible to data loss, which makes it less appropriate for use in high-noise or less-than-ideal settings. To verify the authenticity of the encrypted picture loss, our method has been tested against occlusion attacks. The occlusion attack causes some of the encrypted image's pixels to get blocked. The degree of encryption loss is determined by the size of the restricted region and is then analyzed through simulation. When a picture is hidden or masked during encryption, its quality is reduced. The MSE with occluded region are shown in Figures 6. It is clear that the quality of the recovered image steadily declines as the encrypted image's occlusion percentage rises and shows the various occlusion percentages of the encrypted and corresponding decoded images

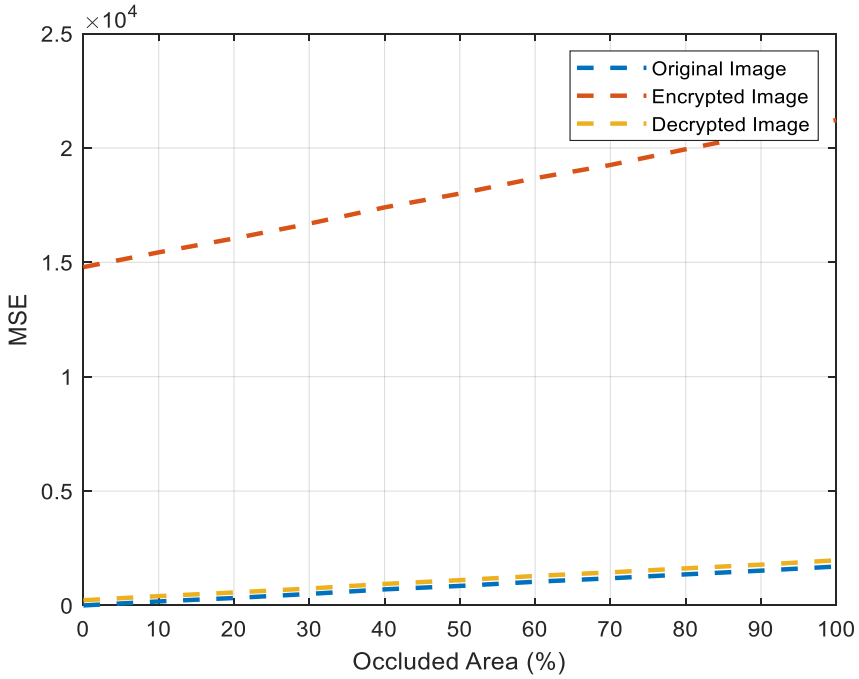


Figure 6: MSE plot with percentage occluded area

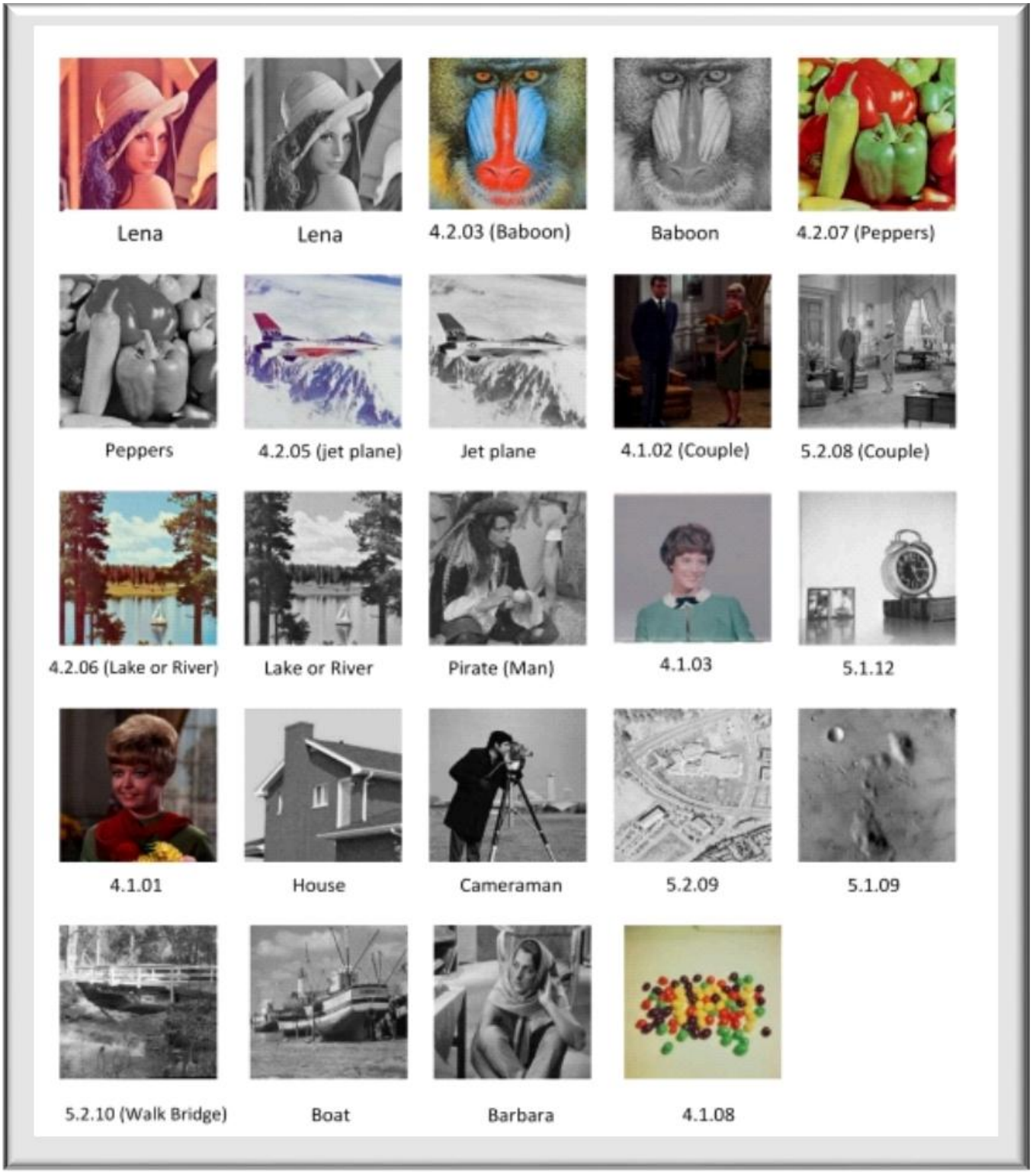


Figure 7: Test images

Various testing images of different sizes were utilized as data set in the implemented system , as illustrated in Figure 7, to obtain diverse results and compare them with previously employed methods. This comparison aimed to evaluate the efficiency of our proposed system[2,10,45].

6. EXPERIMENTAL RESULTS

The proposed encryption algorithm was implemented in the MATLAB simulation environment. During subsequent tests, various grayscale images of different sizes, such as Baboon, Cameraman, Lena, Bridge, Airplane, etc., were considered to validate and test the robustness of the proposed method, as shown in Figure 8. We used the suggested workflow to encrypt these images. The algorithm was also validated to test its resilience against the impact of image noise. Finally, several comparisons between the proposed algorithm and other algorithms were made [27, 46].

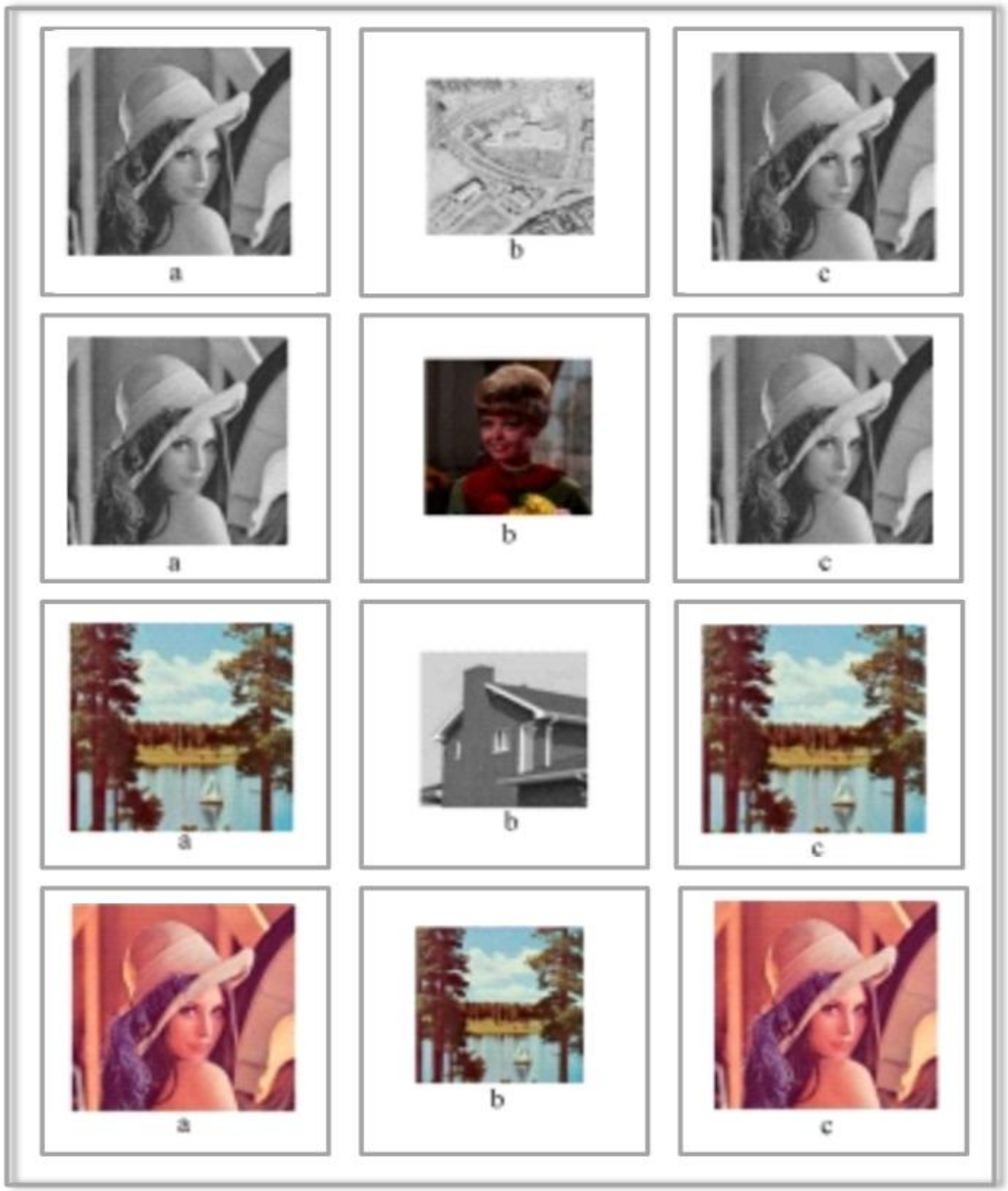


Figure 8(a) Cover image, (b) secret message, and (c) steganographic image



Figu**re 9: We show the cover image of Lena , the original image of airplane,the steganographic original image and retrieval it and vice versa**

In Figure 9(A), we show our use of Lena's image as a fake image, we hide inside it the image to be encrypted as an Airplane image, which contains a lot of black color in most parts of the image, to introduce how good the method used to hide it inside an image that does not contain this many black pixels. Then, in figure. 9 (B), we do the reverse and use the picture of Airplane that includes a lot of black color as a false image and conceal the other image inside, both of us are much less than in the black fault) [47]. This is to increase the security and Privacy rate of the image to be preserved from hacking or unauthorized access from any party or person. Because if the encrypted image is hacked and may be decrypted, the hacker will see a fake image and the real image is hidden inside [48].

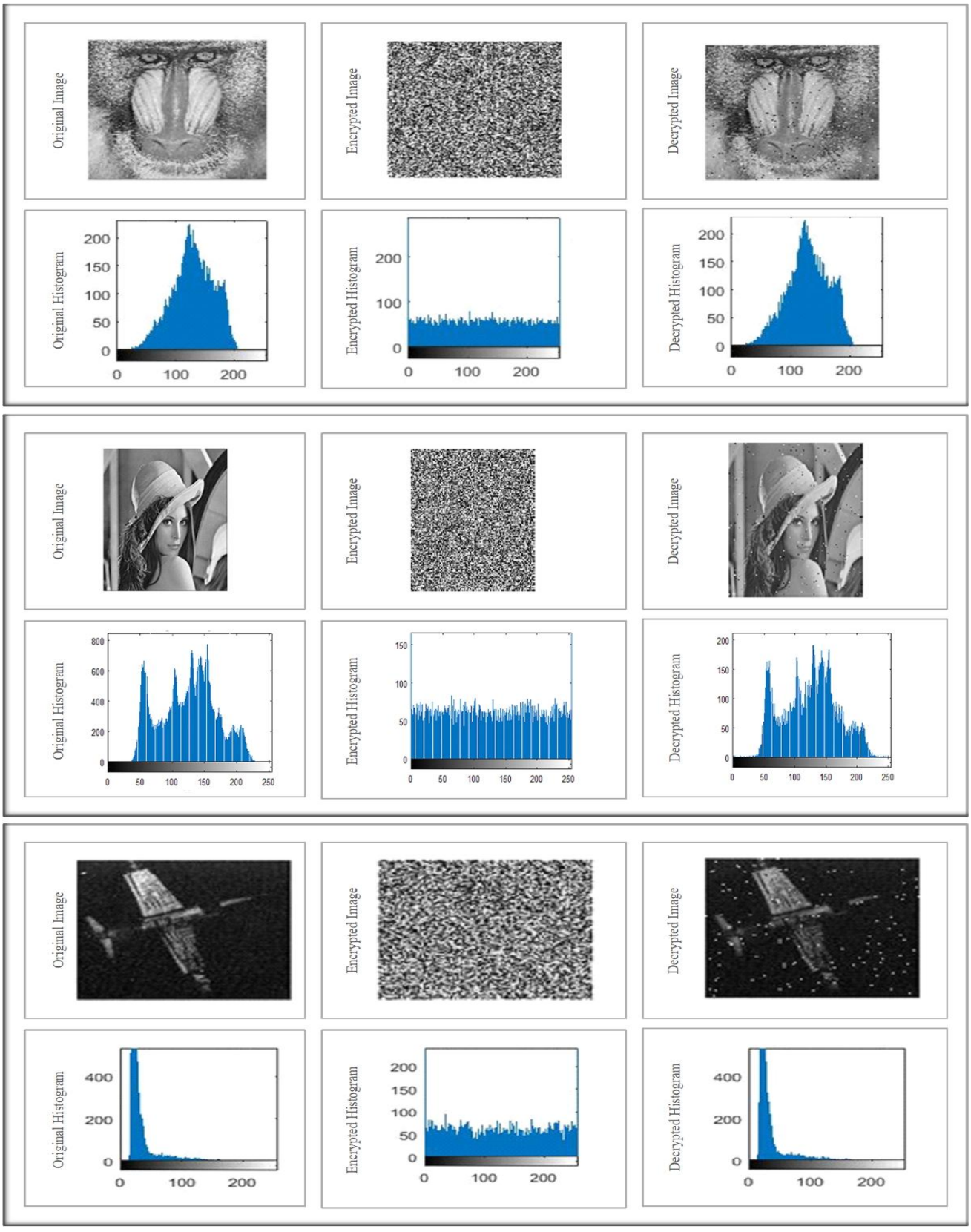


Figure 10: The fake image of Baboon and its histogram which has original image of LENA inside it with 2%salr&pepper noise and its histogram

The provided images in Figure.10 and its associated histograms illustrate the exceptional effectiveness and resilience of the encryption technology utilized for photos of diverse sizes and complexities. The method proficiently obscures the actual visual material during encryption and precisely restores it during decryption, even amidst noise [49]. The encryption procedure for the Baboon picture alters the original material into an almost unrecognizable format, as seen by the histogram's homogeneity. This signifies a robust encryption method that eradicates all discernible patterns. The decryption algorithm effectively recovers the Baboon picture, despite the introduction of 2% salt-and-pepper noise, demonstrating the system's robustness to noise and excellent fidelity. Likewise, for the Lena image, the encryption procedure equally disperses the pixel intensity values, so concealing the original information [50]. The decoded image keeps its clarity despite the presence of noise, further showing the method's durability. The histogram illustrates the system's capacity to recreate the image while preserving the original distribution of intensity levels. The Airplane picture, measuring 1024 × 1024, has a highly jumbled appearance post-encryption, accompanied by a uniform histogram, so illustrating the method's scalability for bigger datasets. The encrypted picture, albeit exhibiting 3.5% salt-and-pepper noise, preserves the fundamental information, as seen by its recovered histogram [51].

Overall, the histograms across all cases show the system's potential to encrypt successfully by attaining pixel uniformity and to decode with high accuracy, despite noise and variable picture sizes. This highlights the dependability and quality of the suggested encryption technology for safe picture processing [52].

Table 3 presents the results of the differential attack and sensitivity analysis of the plaintext when we used various original Lena images to show the change in the results as the image size changed. We confirmed the relationship between the size of the encoded Lena image and its results for the differential attack and plaintext sensitivity analysis of the encryption process [51].

Table 3: Comparative Analysis of Encryption Performance on Different Image Sizes (Lena)

analysis	CORR	UACI	PNCR	MAE	PSNR	Entropy	Time/sec
128×128	0.00006	33.43	99.94	10130	8.36	7.72	6.45
256 × 256	0.000046	33.45	99.96	10663	8.24	7.72	5.66
512 × 512	0.00004	33.67	99.93	10424	8.22	7.71	4.72

Table 4 shows how the findings from our coding approach differed from those of various other methods [4-23] that used the Lena image to illustrate the difference between those methods for performance analysis (NPCR, UACI, CORR, and entropy). We obtained preferential values of the correlation coefficient and convergence of values in other findings [22, 23, 53].

Table 4: Comparison of Encryption Performance on Lena Image

Performance analysis		NPCR	UACI	CORR	Entropy
Image Lena	[4]	99.59	33.45	0.0033	7.99
	[6]	99.62	33.46	-0.00054	7.99
	[8]	99.56	33.22	0.002	7.9
	[10]	99.59	33.45	0.0004	7.9
	[12]	99.5	33.22	0.0041	7.9
	[15]	99.61	33.47	-0.0021	7.9
	[22]	99.71	33.45	0.0009	7.9
	[23]	100	33.44	0.0008	7.9
	present work	99.93/100	33.36/33.67	0.000029	7.71

Moreover, comparison on performance analysis between the suggested methodology and the method provided [2] is shown in table.5, showed that by determining the findings of NPCR, UACI, CORR, MAE, PSNR and entropy, two pictures Lena and Baboon, as demonstrated the lowest result and the maximum result emerged utilizing given approach technique. Note that convergence of

findings and their resemblance in NPCR, UACI, and entropy. As we are not a clear and considerable rise in MAE, PSNR and "CORR" correlation accordingly. This illustrates the benefit of our approach employed in encryption of the method given in reference [2,53]. Table 5 uses Lena and Baboon to compare between the results of our method and methods introduced.

Table 5: Comparison of Encryption Performance on Lena and Baboon Images

Metrics	Image					
	Lena				Baboon	
	[9]	[42]	[44]	present work	[14]	present work
NPCR	99.68	---	---	99.46/100	99.66	99.46/100
UACI	33.28	---	---	33.06/33.48	33.32	33.2/33.82
MSE	7735	1.07e-19	6.04e-14	9395/9532	7391	7132/7429
PSNR	22.121	286.26	312.11	8.33/8.4	23.224	9.33/9.4
CORR	0.0107	0.2727	---	0.00002/ 0.00009	0.0141	0.00016/ 0.00004
Entropy	7.9953	7.52	7.92	7.716	7.9872	7.753

When we used larger images with multiple sizes, the results for the differential attack and plaintext sensitivity analysis significantly and favorably improved, as evident in Table 6. The UACI value increased significantly to 36.42, surpassing previous techniques, and the PSNR value decreased significantly to 6.92, a result of increased MAE. These substantial improvements strongly favor our proposed approach [57].

Table 6: Differential Attack Results for Different Airplane Image Sizes

analysis	CORR	UACI	MAE	PSNR
256 × 256	0.0000052	40.22	101.29	7.49
512 × 512	0.0000003	40.62	103.16	7.12
1024×1024	0.0000018	41.42	105.75	6.92

Table 7: Comparative Analysis of Encryption Performance on Different Fruit Image Sizes

analysis	CORR	UACI	PNCR	MAE	PSNR	Entropy	Time/sec
128×128	0.00007	33.53	99.92	8072	8.87	7.72	11.14
256 × 256	0.00005	33.45	99.95	8544	8.63	7.72	6.23
512 × 512	0.00003	33.84	99.94	8792	8.43	7.71	5.39

In Table 7 we illustrate the effect of our approach utilized on different sizes of Fruit. We prove this by the outcomes of the differential attack and Plaintext sensitivity analysis. And thus, it has occurred to us that there is a link between the outcomes and the size of the image. It becomes evident to us that the higher the picture size, the better results we receive for COOR, UACI, PSNR and Entropy [14,55].

Table 8 that is created shows the differences in the results that were obtained by utilizing our way of coding in comparison to some other approaches that were presented by employing camcorder images of varying sizes. Entropy, UACI, CORR, and NPCR are the four methodologies that are used for performance analysis in table.8, to highlight the differences between these methods. Within the other results, we discovered the preferred values of the correlation coefficient as well as the convergence of values [56,57].

Table 8: Summary results of the sample image of Cameraman with several sizes

analysis	CORR	UACI	PNCR	MAE	PSNR	Entropy	Time/sec
128×128	0.00008	33.34	98.89	10142	8.31	7.71	6.24
256 × 256	0.000044	33.76	99.95	10473	8.14	7.71	5.43

Table 9 provides a comparison of our technique with other encryption methods based on the correlation coefficient (CORR) metric. The results demonstrate a significant improvement in the CORR value, indicating a higher level of security and preference for our proposed algorithm. Additionally, a comparison with methods presented in [6,7,10,12] further highlights the superior performance of our approach in terms of the correlation coefficient, as confirmed by references [10, 58-61].

Table 9: Summary results of the correlation coefficient of image Elaina.

analysis	[6]	[7]	[10]	[12]	present work
CORR	0.0097	-0.0017	-0.0004938	0.0003	- 0.0000019

Using photographs of the Cameraman, Elaina, and Airplane, Table 10 compares the outcomes of our proposed methodology with those described in references [7, 10, 12]. When using the Airplane and Elaina images, PSNR, Entropy, CORR, and UACI values are significantly better than those of the methods used in References [12, 62], which all employed Chaos Maps but in different forms and techniques. While using the Cameraman image, we observe close values for NPCR, UACI, and entropy, as well as a clear preference for PSNR, MAE, and CORR values. This consistently affirms and creates a positive impression that we employed chaos maps as a special technique to achieve the objective of this paper [63, 64].

Table 10: Comparison of the Method's Analysis on 256x256 Images (Cameraman, Elaina, Airplane)

performance analysis	Image with size 256x256						
	Cameraman			Elaina		Airplane	
	[10]	[12]	Present work	[7]	present work	[7]	present work
NPCR	99.55	99.6	99.99	99.66	99.99	99.66	99.99
UACI	33.45	33.44	34.88	33.69	35.18	33.69	36.42
MAE	47.98	83.45	85.95	83.45	88.3	47.37	105.57
PSNR	28.69	8.39	7.76	27.12	7.37	26.01	6.92
CORR	0.003	0.0034	0.0000012	-0.0017	0.0000048	-0.0045	0.0000018
Entropy	7.9	7.99	7.99	7.98	7.99	7. 97	7.99

The results of encoding several images are shown in Table 10. The NPCR attained a value of 100, the UACI measured 36.42, the MAE measured 105.75, the PSNR measured 6.92 dB, the CORR measured 18 × 10^-8, and the entropy measured around 7.99. This clearly indicates a preference for our approach over other previous methods [65]. These findings also demonstrate the performance analysis of the proposed algorithm on a large number of 256x256-pixel images. By utilizing chaotic maps in various ways and employing changeable initial condition values, we were able to create a highly secure encryption system resistant to a wide range of attacks [66-68].

Table 11: Comparative Analysis of Encryption Performance on Different Image Sizes

image	NPCR	UACI	MAE	PSNR	CORR	ENTR	TIME m sec
cameraman	99.99	33.88	85.17	7.76	0 .000012	7.99	6.24
Lena	99.99	34.82	79.77	7.69	0.0000008	7.99	4.45
Bridge	99.99	33.56	81.16	8.31	-0.00005	7.99	4.07
Fruit	99.99	33.50	80.72	7.73	0.000024	7.99	5.14
Airplane	**100**	**36.42**	**105.75**	**6.92**	**- 0.00000018**	**7.99**	**3.14**
Baboon	99.99	35.86	77.29	8.21	0.0000004	7.99	7.07
Elaina	99.99	35.18	88.30	7.37	0.0000048	7.99	8.43

In Table 11, we summarized the best results obtained from our innovative method in the encryption system. The highest NPCR value achieved was 100 with the image of an Airplane, while the minimum value was 99.99. The highest value produced for UACI was 36.42, also with the image of an Airplane, and the lowest value was 33.50. The best value for MAE was 105.75, but the minimum value was 77.29. Also, the best result for PSNR equalled 6.92. The system achieved more best values, such as 0.00000018 for correlation, because our proposed hybrid system was designed based on correlation results to choose which chaotic map to use in the encryption process. We can also choose other performance metrics [69-74]. The maximum Entropy was 7.99, and the minimum time was 3.14 milliseconds.

It was essential to develop a system that would disinfect and enhance the resultant photos of our encryption technology because the picture exhibits distortions post-extraction. It is customary to encounter noise during transmission from sender to receiver, as seen in Figure 9. We have developed a purification, disinfection, and noise removal system using a sample of photos from the previously suggested encryption system to determine the most effective way for purification and noise removal in our novel system [75].

We have developed an image filtering system using many kinds, including a Gaussian filter, a Median filter, and a hybrid filter that combines both Gaussian and Median filters to enhance efficiency [71, 76]. We enhance image illumination by adjusting brightness and subsequently utilize convolutional neural network CNNs (autoencoders) as a novel and effective method, following extensive training to determine optimal parameters for improving the image depicted in Figure 9.6 per photograph.

The most significant outcomes for improving concealed pictures, after their extraction from the cover image, were seen when using kernel neural network filters (KNN) [77-82]. To demonstrate the distinctions in Figure 11, we utilized an image of a baboon in varying sizes to obtain different levels of noise and distortions, alongside a larger image of Lena, which possessed greater data and contrast in gray levels than the former, as well as an image of a cameraman with small size and different gray levels from Lena [83].

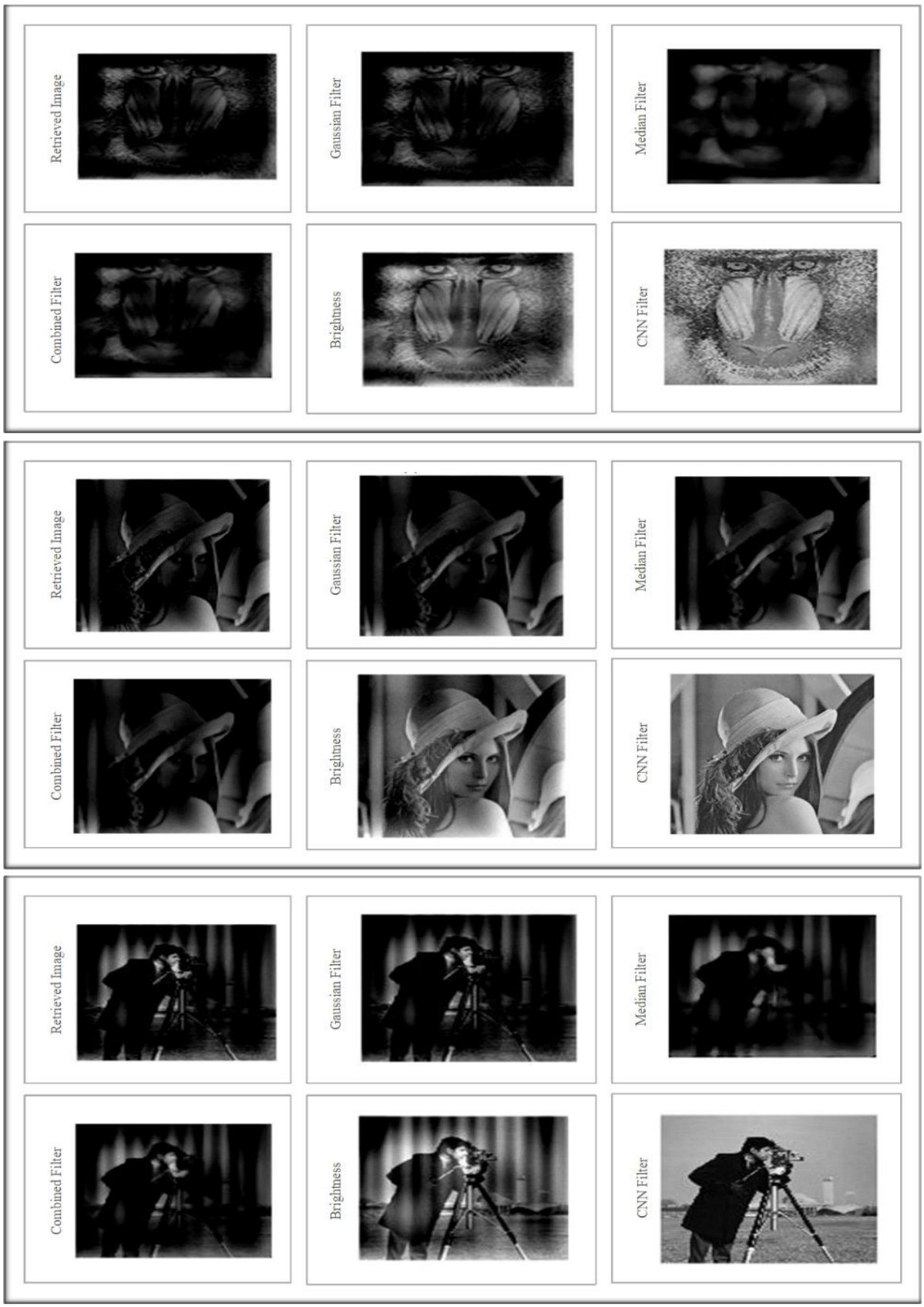


Figure 11: shows the result of different filters for retrieved secret image of Baboon

7- CONCLUSION

Our lives have become intertwined with vast amounts of digital data, with the ability to file, share, and transfer it, often without limitations on privilege or privacy. This places an obligation on system administrators to ensure all systems maintain an acceptable level of data security. As a result, there is continuous development in data security techniques and various encryption algorithms [23,80]. On the other hand, intruders continuously develop cryptanalysis techniques to breach these systems. Medical data is highly sensitive and requires a high level of security, especially when transmitted wirelessly. Protection methods such as steganography and cryptography are often employed. In this work, we enhanced security by hiding the original images inside another "fake" image using the steganographic DCT method. We then generate variable keys for each pixel using chaotic maps created by combining two maps in the encryption process with a cosine square logistic map. Furthermore, by mixing multiple chaotic maps, we achieve robust image encryption. Additionally, we propose a filtering system using various filters, with the Convolutional Neural Networks (CNN) filter being the most effective. Our results demonstrate an excellent level of security and high efficiency in performance, as indicated by plaintext sensitivity analysis and differential attacks. Statistical analysis shows a lower Mean Square Error (MSE) and higher correlation than the proposed algorithm. By utilizing various chaotic mappings, we present a new algorithm for image encryption and decryption. The keys are generated using the sine-square logistic map, which creates additional chaotic maps, further enhancing security to protect privacy. Comparative results with state-of-the-art algorithms show that the proposed approach outperforms the compared methods based on metrics such as PSNR, CORR, MAE, UACI, NPCR, and entropy. The algorithm integrates multiple chaotic maps to achieve a highly secure encrypted image with low computational complexity, making it ideally suited for real-time video communication applications with high security.

Data availability

"As the same of many papers in the same research direction, we also use the several standard images as Lena , cameraman , baboon , bird and others from the site of Image Processing Place Image Databases"

Funding:
The authors declare that no external funding was received for this research.

REFERENCES

[1] G. A. Sathishkumar, K. Bhoopathy, N. Sriram et al. “Image Encryption Based On Diffusion And Multiple Chaotic Maps,” in International Journal of Network Security & Its Applications (IJNSA), vol. 3, no. 15, pp. 181-194, March 2011.

[2] M. Khan et al. “A novel Image Encryption Scheme Based on Multiple Chaotic S-boxes,” in Nonlinear Dyn, vol. 82, no. 7, pp. 527–533, 28 May 2015.

[3] I. Amr, M. Amin, H. Diab et al. “A digital Image Encryption Algorithm Based a Composition of Two Chaotic Logistic Maps” in International Journal of Network Security, vol. 11, no. 11, pp. 1-10, 2010.

[4] S. Farwa, T. Shahy, N. Muhammad, N. Bibiz, A. Jahangir, S. Arshady et al. “An Image Encryption Technique Based On Chaotic S-Box And Arnold Transform Applications,” in International Journal of Advanced Computer Science and application (IJACSA), vol. 8, no. 5,pp. 360-264, 2017.

[5] Y. Zhou, L. Bao, C. L. Philip et al. “A new 1D Chaotic System for Image Encryption,” in Signal Processing Journal, vol. 00, no. 22, pp 1-21, 2014.

[6] M. Kanaf, B. Fathi et al. “A novel Image Encryption Scheme Based On Clifford Attractor And Noisy Logistic Map For Secure Transferring Images In Navy,” in International Journal of e-Navigation and Maritime Economy, vol. 6, no. 21, pp. 053–063, 2017.

[7] M. Mokhtar, N. M.Sadek, A. Mohamed et al. “Design of Image Encryption Algorithm Based on Different Chaotic Mapping,” in (NRSC), vol. 13, no. 8, pp. 197-204, 2017.

[8] Z. Hua, Y. Zhou, C. Pun, C. L. Philip et al. “2D Sine Logistic Modulation Map For Image Encryption,” in Information Sciences Journal, vol. 297, no. 15, pp. 80-94, 2015.

[9] X. Wang, Sh. Gu, Y. Zhang et al. “Novel Image Encryption Algorithm Based on Cycle Shift and Chaotic System,” in Optics and Lasers in Engineering Journal, vol. 68, no. 7, pp. 126-134, 2014.

[10] X. Wang, X. Zhu, Y. Zhang et al. “An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map,” in IEEE Access, vol. 6, no. 14, PP. 23733-23746, 2018.

[11] K. Shankar, M. El Hoseny, E. Dhirvida, S. K. Lakshmanaprabu, W. Wu et al. “An Efficient Optimal Key Based Chaos Function For Medical Image,” in IEEE Access, vol. 6, no. 10 ,pp. 77145-77154 , 2018,

[12] Mansouri, Ali, and Xingyuan Wang. "A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme." Information Sciences, vol.520, pp.46-62, 2020.

[13] Kolivand, Hoshang, Sabah Fadhel Hamood, Shiva Asadianfam, and Mohd Shafry Rahim. "Image encryption techniques: A comprehensive review." Multimedia Tools and Applications, pp.1-36,2024.

[14] Yousif, Bedir, Fahmi Khalifa, Ahmed Makram, and Ali Takieldeen. "A novel image encryption/decryption scheme based on integrating multiple chaotic maps." AIP Advances, vol.10, no. 7, pp.1-10 ,2020.

[15] Zia, Unsub, Mark McCartney, Bryan Scotney, Jorge Martinez, Mamun AbuTair, Jamshed Memon, and Ali Sajjad. "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains." International Journal of Information Security, vol.21, no.4 pp. 917-935, 2022.

[16] Hu, Guozhen, and Baobin Li. "Coupling chaotic system based on unit transform and its applications in image encryption." Signal Processing,vol. 178,pp. 107790,2021.

[17] Li, Yuan-Min, Mingjie Jiang, Deyun Wei, and Yang Deng. "A Novel Image Encryption Algorithm Based on Compressive Sensing and a Two-Dimensional Linear Canonical Transform." Fractal and Fractional, vol.8, no. 2, pp. 92 ,2024.

[18] Wang, Xingyuan, and Yining Su. "Image encryption based on compressed sensing and DNA encoding." Signal Processing: Image Communication, vol.95, pp. 116246, 2021.

[19] Gupta, Manish, Vibhav Prakash Singh, Kamlesh Kumar Gupta, and Piyush Kumar Shukla. "An efficient image encryption technique based on two-level security for internet of things." Multimedia Tools and Applications 82, no. 4, pp.5091-5111,2023.

[20] Kumari, Punam, and Bhaskar Mondal. "Lightweight image encryption algorithm using NLFSR and CBC mode." The Journal of Supercomputing 79, no. 17, pp. 19452-19472 2023.

[21] Si, Yuanyuan, Hongjun Liu, and Mengdi Zhao. "Constructing keyed strong S-Box with higher nonlinearity based on 2D hyper chaotic map and algebraic operation." Integration, vol.88, pp. 269-277,2023.

[22] Singh, Monu, and Amit Kumar Singh. "A comprehensive survey on encryption techniques for digital images." Multimedia Tools and Applications, vol.82, no. 8, pp. 11155-11187, 2023.

[23] Jamal, Sajjad Shaukat, Mohammad Mazyad Hazzazi, Muhammad Fahad Khan, Zaid Bassfar, Amer Aljaedi, and Zain ul Islam. "Region of interest-based medical image encryption technique based on chaotic S-boxes." Expert Systems with Applications, vol.238, pp. 122030, 2024.

[24] Kong, Xinxin, Fei Yu, Wei Yao, Cong Xu, Jin Zhang, Shuo Cai, and Chunhua Wang. "A class of 2n+ 1 dimensional simplest hamiltonian conservative chaotic systems and fast image encryption schemes." Applied Mathematical Modelling, vol.125, pp.351-374, 2024.

[25] Niu, Ying, and Xuncai Zhang. "A novel plaintext-related image encryption scheme based on chaotic system and pixel permutation." IEEE Access, vol. 8, pp. 22082-22093, 2020.

[26] Toktas, Abdurrahim, Uğur Erkan, Suo Gao, and Chanil Pak. "A robust bit-level image encryption based on Bessel map." Applied Mathematics and Computation, vol.462, pp. 128340, 2024.

[27] Wang, Xingyuan, and Yining Su. "Image encryption based on compressed sensing and DNA encoding." Signal Processing: Image Communication, vol.95, pp. 116246, 2021.

[28] Gupta, Manish, Vibhav Prakash Singh, Kamlesh Kumar Gupta, and Piyush Kumar Shukla. "An efficient image encryption technique based on two-level security for internet of things." Multimedia Tools and Applications 82, no. 4, pp.5091-5111,2023.

[29] Kumari, Punam, and Bhaskar Mondal. "Lightweight image encryption algorithm using NLFSR and CBC mode." The Journal of Supercomputing 79, no. 17, pp. 19452-19472 2023.

[30] Si, Yuanyuan, Hongjun Liu, and Mengdi Zhao. "Constructing keyed strong S-Box with higher nonlinearity based on 2D hyper chaotic map and algebraic operation." Integration, vol.88, pp. 269-277,2023.

[31] Singh, Monu, and Amit Kumar Singh. "A comprehensive survey on encryption techniques for digital images." Multimedia Tools and Applications, vol.82, no. 8, pp. 11155-11187, 2023.

[32] Jamal, Sajjad Shaukat, Mohammad Mazyad Hazzazi, Muhammad Fahad Khan, Zaid Bassfar, Amer Aljaedi, and Zain ul Islam. "Region of interest-based medical image encryption technique based on chaotic S-boxes." Expert Systems with Applications, vol.238, pp. 122030, 2024.

[33] Kong, Xinxin, Fei Yu, Wei Yao, Cong Xu, Jin Zhang, Shuo Cai, and Chunhua Wang. "A class of 2n+ 1 dimensional simplest hamiltonian conservative chaotic systems and fast image encryption schemes." Applied Mathematical Modelling, vol.125, pp.351-374, 2024.

[34] Niu, Ying, and Xuncai Zhang. "A novel plaintext-related image encryption scheme based on chaotic system and pixel permutation." IEEE Access, vol. 8, pp. 22082-22093, 2020.

[35] Toktas, Abdurrahim, Uğur Erkan, Suo Gao, and Chanil Pak. "A robust bit-level image encryption based on Bessel map." Applied Mathematics and Computation, vol.462, pp. 128340, 2024.

[36] Hedayati, Razieh, and Seyedakbar Mostafavi. "A lightweight image encryption algorithm for secure communications in multimedia Internet of Things." Wireless Personal Communications, vol.123, no. 2, pp. 1121-1143 2022.

[37] Arthi, G., V. Thanikaiselvan, and Rengarajan Amirtharajan. "4D Hyperchaotic map and DNA encoding combined image encryption for secure communication." Multimedia Tools and Applications, vol.81, no. 11, pp. 15859-15878,2022.

[38] Agarwal, Abhinav, and Sandeep Malik. "A Brief Review on Various Aspects of Steganography Followed by Cryptographic Analysis." In 2022 IEEE 7th International conference for Convergence in Technology (I2CT), pp. 1-10. IEEE, 2022.

[39] Alexan, Wassim, Dina El-Damak, and Mohamed Gabr. "Image Encryption Based on Fourier-DNA Coding for Hyperchaotic Chen System, Chen-Based Binary Quantization S-box, and Variable-Base Modulo Operation." IEEE Access ,2024.

[40] Wen, Heping, and Yiting Lin. "Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding." Expert Systems with Applications, vol.237, pp. 121514, 2024.

[41] Abdulameer, Saad A. "Choosing the Right Chaotic Map for Image Encryption: A Detailed Examination." Journal Of Theoretical and Applied Information Technology, vol.102, No. 3, 2024.

[42] A watermarking-based asymmetric cryptosystem using gyrator transform, QZ modulation, and fractional vortex toroidal phase mask. J Opt (2024).

[43] An asymmetric hybrid cryptosystem based on triple random phase encoding using polar decomposition, QZ modulation, and gyrator domain, Optik , 171602 (2024) .

[44] Hukum Singh ,R Girija,Manoj Kumar,A cryptoanalysis of elliptic curve cryptography based on phase truncation in the domain of hybrid gyrator Hartley transform. Opt Quant Electron 55, 487 (2023).

[45] X. Liu, D. Xiao, Y. Xiang et al. “Quantum Image Encryption Using Intra and Inter Bit Permutation Based on Logistic Map,” in IEEE Access, vol. 7, no. 10, pp. 6937-6946, 2018.

[46] H. Ren, J. Wang, Q. Wang et al. “An Image Encryption Scheme Of Logistic Modulation Using Computer-Generated Hologram And Chaotic Map,” in Journal of Electrical and Computer Engineering, vol. 6, no. 8, pp. 1-7, 2018.

[47] H. Pan, Y. Lei, C. Jian et al. “Research on Digital Image Encryption Algorithm Based on Double Logistic Chaotic Map,” in EURASIP Journal on Image and Video Processing, vol. 124, no. 11, pp. 1-10, 2018.

[48] T. Gopalakrishnan, S. Ramakrishnan et al. “Image Encryption In Bin Block-Wise With Multiple Chaotic Maps For Permutation And Diffusion,” in ICTACT Journal on Image and Video Processing, vol. 6, no. 8, PP. 1220-1227, 2016.

[49] S. Liansheng, Z. Bei, N. Xiaojuan, T. Ailing, et al. “Optical Multiple-Image Encryption Based on the Chaotic Structured Phase Masks under the Illumination of A vortex Beam in the Gyrator Domain,” in Optics Express Journal, vol. 24, no. 18, pp. 1-17, 2016.

[50] F. K. Tabash, M. Q. Rafiq, M. Izharrudin et al. “Image Encryption Algorithm Based On Chaotic Map,” in International Journal of Computer Applications, vol. 64, no. 13, PP. 1-14, 2013

[51] R. Ye et al. “A highly Secure Image Encryption Scheme Using Compound Chaotic Maps,” in Journal of Emerging Trends in Computing and Information Sciences, vol. 4, no. 6, pp. 532-544, 2013.

[52] H. Alsafasfeh, A. Arfoa et al. “Image Encryption Based On The General Approach For Chaotic Systems,” in Journal of Signal and Information Processing, vol. 2, no. 7, pp. 238-244, 2011.

[53] S. Behnia, A. Akhshani, H. Mahmodi, A. Akhavan et al. “A novel Algorithm for Image Encryption Based on Mixture of Chaotic Maps,” in Chaos Solutions and Fractals Journal, vol. 35, no. 13, pp. 408–419, 2006.

[54] A. A. El-Latif, L .L. Zhang et al. “Digital Image Encryption Scheme Based on Multiple Chaotic Systems,” in Sensing and Imaging an International Journal, vol. 13, no. 12, pp. 67-88, 2012.

[55] X. Wu, B. Zhu, Y. Hu, Y. Ran et al. “A novel Color Image Encryption Scheme Using Rectangular Transform-Enhanced Chaotic Tent Maps, “in IEEE Access, vol. 5, no. 8, pp. 6429-6436, 2017.

[56] C. Zhu, K. Sun et al. “Cryptanalyzing And Improving A novel Color Image Encryption Algorithm Using RT-Enhanced Chaotic Tent Maps,” in IEEE Access, vol. 6, no. 12, pp. 18759-18770, 2018.

[57] M. Li, D. Lu, W. Wen, H. Ren, Y. Zhang et al. “Cryptanalyzing A color Image Encryption Scheme Based on Hybrid Hyper-Chaotic System and Cellular Automata,” in IEEE Access, vol. 6, no. 10, pp. 47102-47111, 2018.

[58] W. Feng, Y. He, H. Li, C. LI et al. “Cryptanalysis And Improvement Of The Image Encryption Scheme Based On 2D Logistic-Adjusted-Sine Map,” in IEEE Access, vol. 7,no. 14, pp. 12584-12597, 2019.Bibliography of authors

[59] Marakumbi Prakash R, A Survey on Image Encryption Using Chaotic MapsInternational Journal of Progressive Research in Science and Engineering ,Volume-2, Issue-2, February-2021.

[60] Battelle (2020) The future of security: zeroing in on un-hackable data with quantum key distribution https://www.wired.com/ insights/2014/09/quantum-key-distribution/. Accessed 20 Feb 2020.

[61] Ahmed Makram , Bedir Yousif, Fahmi Khalifa, Ali Takieldeen. "A novel image encryption/decryption scheme based on integrating multiple chaotic maps" , AIP Advances, 2020.

[62] Sameh S Askar, Abdelrahman A Karawia, and Fatmah S Alammar. Cryptographic Algorithm Based on Pixel Shuffling and Dynamical Chaotic Economic Map. IET Image Processing, 12(1):158–167, 2017.

[63] NJ Gogtay and UM Thatte. Principles Of Correlation Analysis. Journal of the association of physicians of India, 65:78–81, 2017.

[64] Omar Farook Mohammad, MohadShafryMohad Rahim, SubhiRafeeq Mohammed Zeebaree, and FY Ahmed. A Survey and Analysis of The Image Encryption Methods. International Journal of Applied Engineering Research, 12(23):13265–13280, 2017.

[65] Stefan Kölbl, Christian Rechberger, and Lars Ramkilde Knudsen. Design And Analysis of Cryptographic Algorithms. PhD thesis, Technical University of Denmark (DTU), 2017

[66] Hu G., Li B. Coupling Chaotic System Based on Unit Transform and Its Applications in Image Encryption. Signal Process. 2021; 178:107790.

[67] Mansouri A., Wang X. A Novel One-Dimensional Sine Powered Chaotic Map and Its Application in A New Image Encryption Scheme. Inf. Sci. 2020; 520:46–62.

[68] Wang X., Su Y. Image Encryption Based on Compressed Sensing and DNA Encoding. Signal Process. Image Communication. 2021; 12:116246.

[69] Muhammad Faheem Mushtaq, Sapiee Jamel, Abdulkadir Hassan Disina, Zahraddeen A Pindar, N Shafinaz Ahmad Shakir, and Mustafa Mat Deris. A Survey on The Cryptographic Encryption Algorithms. International Journal of Advanced Computer Science and Applications, 8(11):333–344, 2017.

[70] Ahmed Eltengy, SamaaShohieb, Ali Takieldeen, and M. Ksasy. A New Advanced Cryptographic Algorithm System for Binary Codes by Means of Mathematical Equation. ICIC Express Letters, 12(2):117–123, 2018.

[71] Rajvir Kaur and Gauravdeep. Statistical based DDOS detection methods: A review. International Journal of Engineering Technology, Management and Applied Sciences, 5(4):521–525, 2017.

[72] Sameh S Askar, Abdel A Karawia, Abdulrahman Al-Khedhairi, and Fatemah S Al-Ammar. An Algorithm of Image Encryption Using Logistic and Two-Dimensional Chaotic Economic Maps. Entropy, 21(1):44, 2019.

[73] W. Feng, Y. He, H. Li, C. LI et al. “Cryptanalysis and Improvement of The Image Encryption Scheme Based On 2D Logistic-Adjusted-Sine Map,” in IEEE Access, vol. 7, no. 14, pp. 12584-12597, 2019.

[74] Mahmoud, Amena, Nancy Awadallah Awad, Najah Alsubaie, Syed Immamul Ansarullah, Mohammed S. Alqahtani, Mohamed Abbas, Mohammed Usman, Ben Othman Soufiene, and Abeer Saber. "Advanced Deep Learning Approaches for Accurate Brain Tumor Classification in Medical Imaging." Symmetry 15, no. 3 (2023): 571.

[75] Alnowaiser, Khaled, Abeer Saber, Esraa Hassan, and Wael A. Awad. "An optimized model based on adaptive convolutional neural network and grey wolf algorithm for breast cancer diagnosis." PloS one 19, no. 8 (2024): e0304868.

[76] Esraa Hassan, Abeer Saber, Samar Elbedwehy, Knowledge distillation model for Acute Lymphoblastic Leukemia Detection: Exploring the impact of nesterov-accelerated adaptive moment estimation optimizer, Biomedical Signal Processing and Control, Volume 94, 2024, https://doi.org/10.1016/j.bspc.2024.106246.

[77] Batra, Reenu, Shakti Arora, Mayank Mohan Sharma, Sonu Rana, Kanishka Raheja, Abeer Saber, and Mohd Asif Shah. "Integration of LSTM networks with gradient boosting machines (GBM) for assessing heating and cooling load requirements in building energy efficiency." Energy Exploration & Exploitation (2024): 01445987241268075.

[78] Esraa Hassan, M. Shamim Hossain, Samir Elmuogy, Ahmed Ghoneim, Khalid AlMutib, Abeer Saber, Ultimate pose estimation: A comparative study, Expert systems, 2024, https://doi.org/10.1111/exsy.13586.

[79] Hassan, E., Hossain, M. S., Saber, A., Elmougy, S.Ghoneim, A.Muhammad, (2024). A quantum convolutional network and ResNet (50)-based classification architecture for the MNIST medical dataset. Biomedical Signal Processing and Control, 87, 105560.

[80] Saber, A.Hussien, A. G., Awad, W. A., Mahmoud, A. Allakany, A. (2023). Adapting the pre-trained convolutional neural networks to improve the anomaly detection and classification in mammographic images. Scientific Reports, 13(1), 14877.

[81] Zheng, Rong, Abdelazim G. Hussien, Raneem Qaddoura, Heming Jia, Laith Abualigah, Shuang Wang, and Abeer Saber. "A multi-strategy enhanced African vultures optimization algorithm for global optimization problems." Journal of Computational Design and Engineering 10, no. 1 (2023): 329-356.

[82] Saber, A. Sakr, M. Abo-Seida, O. M. Keshk, A. Chen, H. (2021). A Novel Deep-Learning Model for Automatic Detection and Classification of Breast Cancer Using the Transfer- Learning Technique. IEEE Access, 9, 71194-71209.

[83] Hussien, A. G. Abualigah, L. Abu Zitar, R., Hashim, F. A., Amin, M., Saber, A., Gandomi, A. H. (2022). Recent Advances in Harris Hawks Optimization: A Comparative Study and Applications. Electronics, 11(12), 1919.