DOI: https://doi.org/10.52436/1.jutif.2025.6.1.4007
p-ISSN: 2723-3863
e-ISSN: 2723-3871

AN ENHANCED MULTI-LAYERED IMAGE ENCRYPTION SCHEME USING 2D HYPERCHAOTIC CROSS-SYSTEM AND LOGISTIC MAP WITH ROUTE TRANSPOSITION

Zahrah Asri Nur Fauzyah[1], Adhitya Nugraha[2], Ardytha Luthfiarta[3], Muhammad Naufal Erza Farandi[4]

[1,2,3,4]Informatics Engineering, University Dian Nuswantoro, Indonesia
Email: [1]itszaraaa317@gmail.com, [2]adhitya@dsn.dinus.ac.id, [3]ardytha.luthfiarta@dsn.dinus.ac.id, [4]erza.naufal@gmail.com

(Article received: October 13, 2024; Revision: November 16, 2024; published: February 20, 2025)

Abstract

In the rapidly evolving digital era, image encryption has become a crucial technique to protect visual data from the threat of information leakage. However, the main challenge in image encryption is improving security against cryptanalysis attacks, such as brute-force and differential attacks, which can compromise the integrity of the encrypted image. Additionally, the creation of efficient and fast encryption schemes that do not degrade image quality remains a significant challenge. This research proposes a multi-layer image encryption scheme that integrates the Logistic Map algorithm, Cross 2D Hyperchaotic (C2HM) system, and Route Transposition techniques. The method aims to enhance the security of digital image encryption by combining chaotic and hyperchaotic systems. The Logistic Map is used to generate a sequence of random values with high chaotic properties, while C2HM contributes to increasing complexity and variability. The Route Transposition technique is applied to scramble pixel positions, further strengthening the encryption's randomness. The encryption key is derived from a combination of the image hash and user key, which are then used to calculate the initial seed in the chaotic algorithm. Experiments were conducted using standard images with a resolution of 512×512 pixels. The security analysis includes evaluations of NPCR, UACI, histogram analysis, and information entropy. The experimental results show that NPCR consistently exceeds 99.5%, while UACI ranges between 33.23% and 33.56%, indicating high sensitivity to minor changes. Histogram analysis demonstrates an even intensity distribution, and the information entropy value of 7.999 reflects an exceptionally high level of randomness. Robustness tests also indicate that this method can maintain image integrity even when subjected to damage or data loss.

Keywords: *Chaotic, C2HM, Hyperchaotic, Image Encryption, Logistic Map, Transposisi Route*

1. INTRODUCTION

In the rapidly evolving digital era, internet technology plays a crucial role in transforming various aspects of human life[1]. Significant advancements in internet technology, big data, artificial intelligence, and 5G communication have been key drivers of global digitalization and information transmission[2]. Information, which was once conveyed solely through text, can now be easily communicated in various formats such as audio, video, and especially images. Image-based digital communication has increasingly become a preferred choice due to its ability to convey more complex information compared to plain text [3]. However, as society's reliance on the internet for information exchange grows, the risk of cyberattacks, such as data theft and information interception, also increases [4]. One effective way to address these challenges is by implementing comprehensive security strategies, including the use of virtual private networks (VPNs), firewalls, secure key exchange, and cryptographic techniques. Cryptography is a technique used to protect information from unauthorized access by transforming it into an unrecognizable form without the correct key or algorithm [5], [6], [7]. This technique involves the use of complex mathematical algorithms and cryptographic keys to encrypt data, including digital images.

In image encryption, chaotic systems exhibit characteristics such as pseudorandomness, sensitivity to initial conditions, unpredictability in trajectory, and the ability to explore bounded intervals randomly [8]. These nonlinear properties make chaotic systems inherently suitable for cryptographic applications. Various chaotic algorithms have been employed in image encryption, including Henon Map, Arnold Map, Lorenz System, Tent Map, and Logistic Map [9]. One of the commonly used chaotic algorithms for image encryption is the logistic map [10], which offers the advantage of a simple structure while effectively generating a significant degree of chaos. The logistic map also exhibits controllable autocorrelation and cross-correlation properties, making it ideal for enhancing the security of digital images. According to research by Rizki et al. [11], the logistic map has been successfully applied in the encryption and decryption of digital images. This study demonstrates that the parameters within the logistic map significantly influence encryption outcomes, where higher parameter values result in improved encryption quality. However, with the growing demand for higher data security, chaotic systems alone may no longer be sufficient. Modern cryptographic challenges necessitate more complex approaches to counter sophisticated attacks such as brute-force and differential attacks. In response to this need, the concept of hyperchaotic systems has emerged [12].

Hyperchaotic systems offer the capability to generate more varied random sequences and possess a larger key space [13]. These systems are characterized by having more than one positive Lyapunov exponent, indicating more complex chaos distributed across multiple dimensions [14]. The high sensitivity to initial conditions, combined with the complexity of multidimensional dynamics, makes hyperchaotic systems highly suitable for adding an extra layer of security in image encryption [15]. This research introduces the Cross 2D Hyperchaotic System (C2HM), a two-dimensional dynamic system exhibiting hyperchaotic behavior, distinguished by having more than one positive Lyapunov exponent. This characteristic leads to highly unstable, nonlinear, and unpredictable system behavior [16]. C2HM is modeled through nonlinear equations that describe the evolution of variables in a two-dimensional phase space, with high sensitivity to initial conditions that further increases the unpredictability of its dynamics. The pseudorandom number sequences it generates are highly unpredictable, providing a high level of confidentiality.

Next, the route transposition algorithm is applied as a permutation method for image pixels. This algorithm works by determining a specific route through which the pixel positions in the image will be altered, resulting in a completely random pixel sequence. By using the route transposition algorithm, the spatial relationships between adjacent pixels in the original image are disrupted, thereby enhancing the confusion and diffusion within the original image.

Each of the three algorithms Logistic Map, C2HM, and route transposition has its own strengths. The Logistic Map generates a simple yet robust chaotic pattern, while C2HM produces more complex and unpredictable multidimensional chaos. On the other hand, the route transposition algorithm randomizes the pixel order of the image, further increasing the level of confusion and diffusion in the encrypted image. The combination of these three methods provides a significant enhancement in the security layers of image encryption.

This research aims to further strengthen digital image security by integrating these chaotic and hyperchaotic algorithms into a multilayer encryption scheme. The proposed approach not only enhances the randomness and unpredictability of the encryption process but also provides a solution capable of addressing emerging cyber threats in the digital age. The implementation of user-specific keys as an additional layer of security further ensures that the encryption remains resistant to various forms of cryptographic attacks. Ultimately, the research seeks to contribute to the development of more robust and efficient encryption techniques that can safeguard digital imagery in an increasingly interconnected world.

2. RESEARCH METHOD

This research proposes an encryption scheme that integrates chaotic and hyperchaotic systems, emphasizing encryption techniques that adhere to the principles of obfuscation and diffusion. The selected technique involves using the Logistic map as the foundation to generate a sequence of random values with high chaotic properties. Meanwhile, the Cross 2D Hyperchaotic Map (C2HM) is introduced to enhance the complexity and variability of the generated random sequence. These two systems are then combined with the route transposition technique to scramble the pixel positions in the image. Below, we detail the proposed method, including the fundamental principles, step-by-step algorithm, and key components, supported by a flowchart. For an initial illustration of the proposed method, see Figure 1.

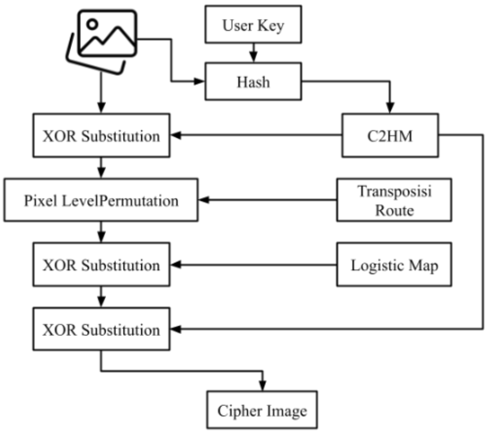


Figure 1. Proposed Method

2.1. Cross 2D Hyperchaotic Map

The Cross 2D Hyperchaotic Map is a two-dimensional nonlinear dynamic system that describes the evolution of two interacting variables, *x* and *y*, which engage in complex interactions. This system maps the two interrelated variables that dynamically evolve within a two-dimensional space, generating complex chaotic patterns [16]. Thus, the C2HM is capable of producing highly efficient hyperchaotic properties, where the interaction between the two variables over time results in unpredictable random patterns. This system employs two mathematical equations, which can be found in Equation (1). A sample trajectory from the C2HM with control parameters is α = 8, β = 3 is presented in Figure 2.

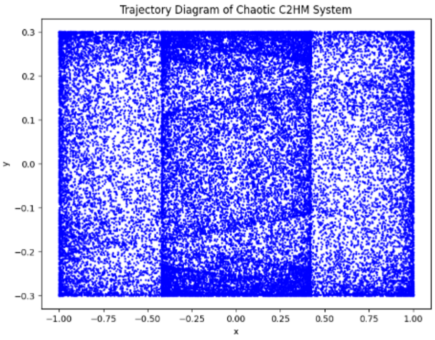


Figure 2. Sample Of Trajectory C2HM

$$\begin{cases} x_{n+1} = \sin\left[\dfrac{\alpha}{\sin(y_n)}\right] \\ y_{n+1} = \beta \sin[\pi(x_n + y_n)] \end{cases} \qquad (1)$$

where with its control parameter $\alpha \neq 0$, $\beta \in [0, 3]$, the initial value $y_0 \neq 0$, the system acquires the best chaotic performance at $\alpha \in [0, 8]$ and $\beta \in [0, 3]$. In Equation (1), the interaction, or what is referred to as cross coupling, between the two variables is depicted, where the value of one variable in the subsequent iteration is influenced by the value of the other variable, and vice versa.

The hyperchaotic properties generated by this system make it highly complex and sensitive to initial conditions. The incorporation of C2HM into the image encryption process creates variations in data transformations that are random and difficult to predict, making it particularly suitable for image encryption that requires a high level of security.

2.2. Logistic Map

The logistic map exhibits various types of system dynamics simply by altering the value of the parameter *r*, which can result in stability toward a fixed point, periodicity, and even chaotic characteristics that are highly sensitive to initial conditions[10]. The strength of the logistic map in cryptography lies in its simplicity. Despite its straightforward structure, the logistic map can produce highly complex and dynamic behavior. Additionally, the logistic map offers high computational efficiency, as it only involves basic operations such as multiplication and subtraction This makes the logistic map computationally efficient and ideal for implementation in various cryptographic schemes. The sensitivity to the parameter *r* is visualized in Figure 3, and the mathematical function of the logistic map is shown in Equation (2).

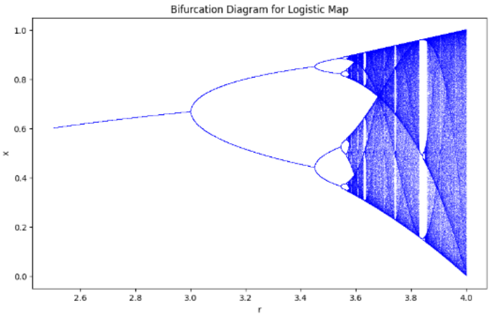


Figure 3. Bifurcation Logistic Map

$$x_{n+1} = rx_n(1 - x_n) \qquad (2)$$

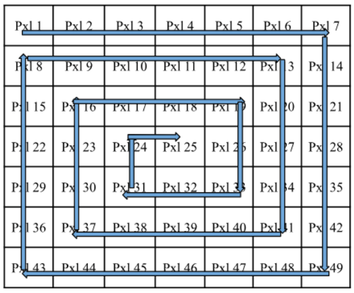
where $x0$ is the initial condition, the control parameter $r \in [0,4]$, dan $x \in [0,1]$.

The logistic map exhibits chaotic behavior when $r > 3.57$. Within this range, the system becomes highly sensitive to initial conditions, which is a key characteristic of chaotic systems. Small changes in the initial value x_0 can lead to significantly different outcomes after several iterations, emphasizing the importance of precision in determining initial conditions when analyzing this system.

2.3. Route Transposition

Route transposition is an effective technique for enhancing image encryption. In this context, route transposition is employed as one of the stages to scramble the image after it has been converted into a matrix. By randomly rearranging the positions of the pixels, this algorithm disrupts the spatial relationship between adjacent pixels, which was previously well-structured in the original image. As a result, this information becomes concealed and much harder to analyze. This process creates two fundamental principles of cryptography, namely confusion and diffusion, which aim to obscure the relationship between the original data and the encrypted data.

Confusion arises from the random rearrangement of pixels, making it extremely difficult to predict the relationship between the original and encrypted pixel positions without the encryption key. Meanwhile, diffusion refers to the spreading of changes that occur in one pixel throughout the entire image, affecting the overall structure. Thus, this algorithm ensures that a change in one pixel will influence many other pixels, creating a uniform distribution of changes across the entire image. This adds an extra layer of security, significantly increasing the difficulty of analyzing the encrypted image and providing added protection against potential attacks. An example of the implementation process for encryption using the route transposition algorithm on a 7x7 pixel image can be seen in Figure 4.



Pxl 1	Pxl 2	Pxl 3	Pxl 4	Pxl 5	Pxl 6	Pxl 7
Pxl 8	Pxl 9	Pxl 10	Pxl 11	Pxl 12	Pxl 13	Pxl 14
Pxl 15	Pxl 16	Pxl 17	Pxl 18	Pxl 19	Pxl 20	Pxl 21
Pxl 22	Pxl 23	Pxl 24	Pxl 25	Pxl 26	Pxl 27	Pxl 28
Pxl 29	Pxl 30	Pxl 31	Pxl 32	Pxl 33	Pxl 34	Pxl 35
Pxl 36	Pxl 37	Pxl 38	Pxl 39	Pxl 40	Pxl 41	Pxl 42
Pxl 43	Pxl 44	Pxl 45	Pxl 46	Pxl 47	Pxl 48	Pxl 49

Figure 4. Illustration Route Of Transposisi Route

2.4. Preparation, Key and Initial Seed

The key is a crucial component in the image encryption process to enhance security layers. In this study, the key is obtained from the combination of the image hash and the user key. This combination is used to compute the initial seed in the chaotic algorithms employed, such as C2HM and the logistic map. The following are the steps in the process :

1. Perform hashing using the SHA-512 algorithm, which will produce a hash value.
2. The hash value is then converted into an array of 8-bit unsigned integers
3. Next, perform a modulo 256 operation to obtain $hash_{key}$ which will be used to create the initial seed. The mathematical formulation can be seen in Equation (3).

$$hash_{key} = (user_{key}) \; mod \; 256 \qquad (3)$$

4. To calculate the initial seed for C2HM and the logistic map using $hash_{key}$. the standard deviation (std) function is used to measure the variation in the data. Next, normalization is performed by dividing by 10 raised to the power of the logarithm base 10 of the standard deviation, rounded down. The initial seed for C2HM is calculated using Equation (4), while the initial seed for the logistic map is computed using Equation (5).

$$x_1 = \frac{std(hash_{key1},\ldots,hash_{key16})}{10^{\lfloor \log_{10}(std(hash_{key1},\ldots\ldots,hash_{key16})) \rfloor}} - 1 \qquad (4)$$

$$y_1 = \frac{std(hash_{key16},\ldots,hash_{key32})}{10^{\lfloor \log_{10}(std(hash_{key16},\ldots\ldots,hash_{key32})) \rfloor}} - 1 \qquad (5)$$

Where initial seed values are in the range of 0 to 9, and the maximum number of decimal places is 14, *i* in $hash_{key(i)}$ represents the index.

5. The result of this stage is the generation of two initial seed values, one for C2HM and the other for the logistic map. These seeds will be used as the starting points for the respective chaotic systems in the image encryption process.

2.5. Encryption Process

In this section we provide a detailed, step by step explanation of the encryption process, as illustrated in figure 1. The encyption process consist of the following steps :

1. Convert the image into a one-dimensional format.
2. Initial image encryption begins by performing an XOR operation on each pixel value using the values generated from the C2HM chaotic function with sequence y from Equation (5), based on the initial seed (y_1) and parameters $\alpha = 0.8$ and $\beta = 0.3$.
3. Next, the encrypted result undergoes permutation using the route transposition technique, which scrambles the pixel positions in the image based on a movement pattern starting from the top-left corner in a clockwise direction.
4. The image that has passed through the route transposition is further encrypted using the logistic map according to Equation (1), with parameter r = 3.954 to generate new chaotic values. These chaotic values are then used to perform an XOR operation on each pixel of the image.
5. The final encryption step uses the values from the C2HM chaotic function generated by sequence x from Equation (4), based on the initial seed (x_1) and parameters $\alpha = 0.8$ and $\beta = 0.3$. The chaotic x values produced are then used to perform an XOR operation on the image pixels.
6. The final result of this process is the fully encrypted image, secured by multiple layers of encryption, known as the final cipher.

2.5. Histogram Analysis

A histogram is a graphical representation used to illustrate the distribution of pixel intensities in a digital image. On the horizontal x-axis, the histogram displays the range of pixel intensity values, from 0 to 255 for an 8-bit depth image. Meanwhile, the vertical y-axis shows the number or frequency of pixels with a specific intensity value. In the context of image encryption, the histogram plays a crucial role as an indicator of the success of the encryption process [17], [18]. Prior to encryption, the original image's histogram typically exhibits an uneven distribution, with certain pixel intensity values dominating and forming distinct peaks. However, after an effective encryption process, the pixel intensity distribution is expected to become more uniform and even.

2.6. Number of Pixels Change Rate (NPCR)

NPCR is an important metric used to measure the sensitivity of an encryption algorithm to small changes in the input image or slight variations in the encryption key. NPCR calculates the percentage of pixels that change between two encrypted images generated from two nearly identical original images or with a small difference in the encryption key [19], [20]. A high NPCR value indicates that the encryption algorithm is highly effective in producing significant changes in the encrypted image, making the original pattern difficult to recognize or analyze by unauthorized parties. The NPCR is calculated using Equation (6) and Equation (7).

$$\delta(i,j)\begin{cases}0 \; if \; E_1(i,j) = E_2(i,j)\\ 1 \; if \; E_1(i,j) \neq E_2(i,j)\end{cases} \quad (6)$$

$$NPCR = \left[\frac{1}{N\times M}\sum_{i=1}^{N}\sum_{j=1}^{M}\delta(i,j)\right]\times 100\% \quad (7)$$

E_1 is the encrypted image, while E_2 represents the encrypted image with a 1-bit modification in the original image. N represents the number of pixels in the columns, and M represents the number of pixels in the rows. Variables i and j indicate the position of each pixel individually, with 255 as the maximum value for pixel intensity in the image.

2.7. Unified Average Changing Intensity (UACI)

UACI is an essential metric used to quantify the extent of pixel value changes between two encrypted images resulting from small variations in the encryption key. UACI measures the average intensity of pixel changes between two nearly identical images or images with slight differences in the encryption key. A high UACI value indicates that even minimal changes in the encryption key lead to significant and unpredictable variations in pixel values, thereby enhancing the security of the encryption algorithm against differential analysis[21].

$$UACI = \left[\frac{1}{N\times M}\sum_{i=1}^{N}\sum_{j=1}^{M}\frac{|E_1(i,j) - E_2(i,j)|}{255}\right]\times 100\% \quad (8)$$

Symbol N represents the number of pixels in the columns, and M represents the number of pixels in the rows. Variables i and j indicate the position of each pixel individually, with 255 as the maximum value for pixel intensity in the image. E_1 is the encrypted image, while E_2 represents the encrypted image with a 1-bit modification in the original image.

2.8. Information Entropy (IE)

Information Entropy (IE) measures the level of uncertainty or randomness in a data source. For an efficient image encryption technique, the entropy of an encrypted 8-bit image should approach the value of 8 [22], indicating that the encryption process has effectively randomized the data. Conversely, a low IE value suggests weaker encryption, making patterns or information more easily detectable. The IE calculation is performed using equation (9).

$$H(x) = -\sum_{i=1}^{n} P(x_i)\log_2 P(x_i) \quad (9)$$

In this equation, $H(x)$ represents the Information Entropy (IE) value of the random variable *x*, while $P(x_i)$ denotes the probability of occurrence of the value x_i in the random variable. The variable *n* refers to the total number of possible values of *x*. The negative sign is used to ensure that the entropy value is positive. The more diverse and evenly distributed the values of *x* are, the higher the IE value will be. Conversely, if a single value dominates with a high probability, the entropy value will be low.

3. RESULT

This section presents the results of the experiments conducted. This research implements a combination of the logistic map algorithm, C2HM, and route transposition using the Python programming language, with Google Colab as the text editor. Additionally, we utilized a user input key that was hashed using the SHA-512 algorithm to enhance the encryption security of each image. The images used in this experiment are standard 512×512 pixel images, commonly used in various image encryption studies. Furthermore, detailed security analyses are conducted and accompanied by visualizations, as explained in Sections 3.1-3.4.

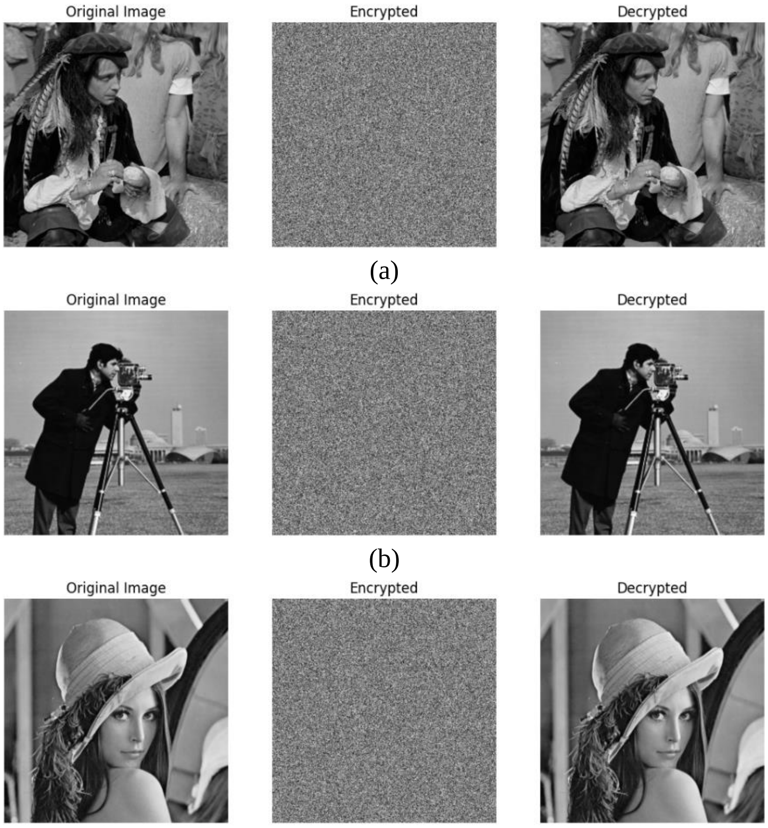
(a) (b) (c)

(d) (e) (f)

Figure 5. Standard Imaged Used For Testing; (a) Pirate, (b) Cameraman, (c) Lena, (d) Boats, (e) Tank, (f) Stream and Bridge

Before testing, the five standard images shown in figure 5, undergo an encryption process using a combination of the Cross 2D Hyperchaotic Map (C2HM), logistic map, and route transposition. The Original Image represents the initial state prior to encryption, serving as the basis for generating the encrypted image and acting as a reference in the decryption process. The original image is displayed clearly, without any alterations or distortions, making it easily recognizable. Next, the original image is encrypted using the combination of the Cross 2D Hyperchaotic Map (C2HM), logistic map, and route transposition. This encryption process results in a fully randomized image that appears as random noise, making it visually unrecognizable. The purpose of this encryption is to protect the image information from unauthorized access. The final image shows the outcome of decrypting the encrypted image using the correct key. This decryption process successfully restores the image to its original form, identical to the initial image, demonstrating that the implemented encryption-decryption method accurately maintains data integrity. The comparison between the original image, encrypted image, and decrypted image is presented in Figure 6.

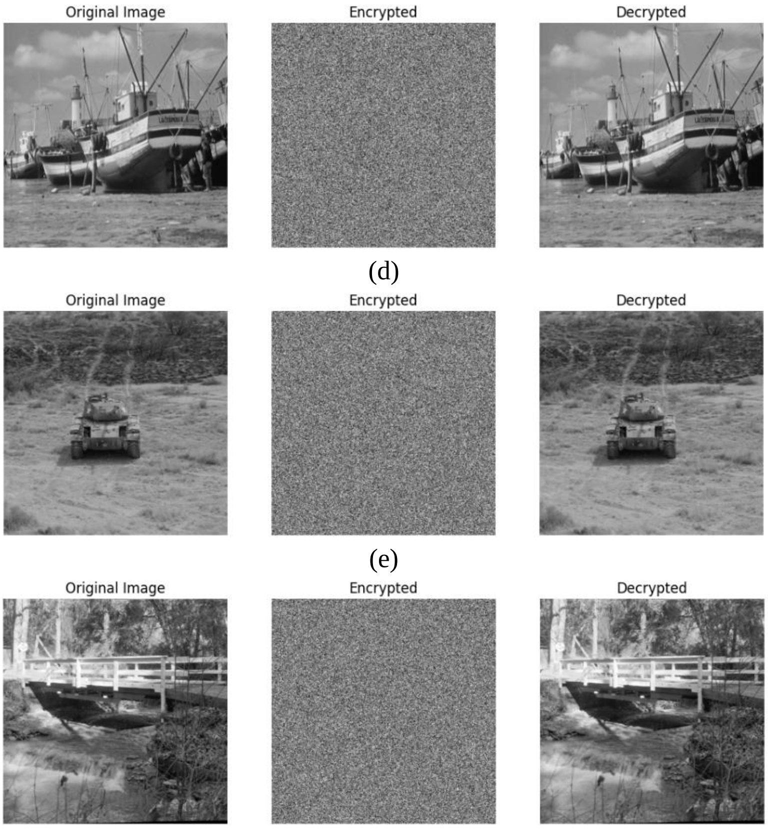
After performing the encryption and decryption processes using the Cross 2D Hyperchaotic Map (C2HM) algorithm, logistic map, and route transposition, the standard image used for testing will be further analyzed to evaluate the performance of these algorithms. The test results are presented in sections 3.1 through 3.4.



(a)

(b)

(c)



(d)

(e)

(f)

Figure 6. Original, Encrypted, Decrpyted Image; (a) Pirate, (b) Cameraman, (c) Lena, (d) Boats, (e) Tank, (f) Stream and Bridge

3.1 Different Analysis Testing

NPCR (Normalized Pixel Change Rate) and UACI (Unified Average Changing Intensity) are two key indicators used to measure how effectively an encryption algorithm protects an image from differential analysis. These metrics assess the algorithm's sensitivity to small changes in the input image, ensuring that even minor modifications result in significantly different encrypted outputs. According to the research cited in [23], an effective image encryption algorithm should ideally have an optimal NPCR value exceeding 99% and a UACI value within the range of 33% to 34%. The NPCR measurement results are presented in Table 1, and the UACI measurement results are shown in Table 2.

Table 1. NPCR results and its comparison with related works

Image	**Size (Pixel)**	**Method**[24]	**Proposed**
Pirate	512×512	-	99.61
Tank	512×512	-	99.62
Lena	512×512	-	99.60
Stream Bridge	512×512	-	99.59
Boat	512×512	99.61	99.61
Cameraman	512×512	99.60	99.61

Table 2. UACI results and its comparison with related works

Image	**Size (Pixel)**	**Method**[24]	**Proposed**
Pirate	512×512	-	33.41
Tank	512×512	-	33.42
Lena	512×512	-	33.49
Stream Bridge	512×512	-	33.40
Boat	512×512	33.40	33.47
Cameraman	512×512	33.37	33.41

The results of this study demonstrate the good performance of the proposed algorithm, as reflected by NPCR values exceeding 99%, indicating high sensitivity to key changes and a significant level of pixel variation in the encrypted images. Furthermore, the UACI values, falling within the optimal range of 33% to 34%, further validate the ability of the algorithm to maintain unpredictability and consistently generate a high level of randomness.

3.2 Histogram Testing

This test utilizes the image in figure 5 to compare the histogram of the original image, the encrypted image, and the decrypted image. The analysis aims to evaluate the effectiveness of the encryption scheme in producing a uniform pixel value distribution.

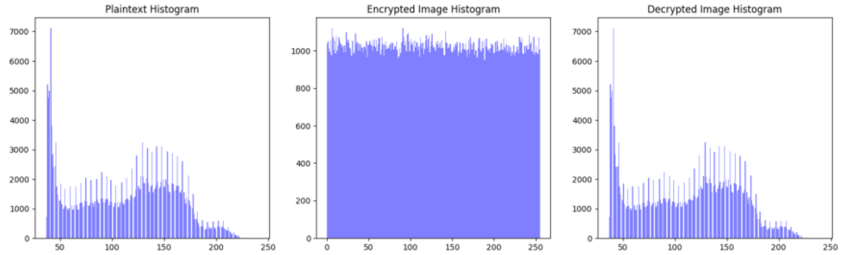


Figure 7. Original, Encrypted, And Decrypted Pirate Histogram

Based on figure 7, the original histogram shows a highly varied distribution of pixel intensity in the original image, with several significant peaks, especially in the low to mid-intensity range. This reflects the diversity of colors or intensities in the original image. After encryption, the encrypted histogram shows an almost uniform intensity distribution across the full range (0-255), indicating that the encryption algorithm successfully scrambled the pixel distribution. This pattern suggests a high level of encryption security, as the original image structure is entirely obscured. In the decrypted histogram, the intensity distribution closely resembles that of the original image, indicating that the decryption process can restore visual information accurately, preserving the image quality.

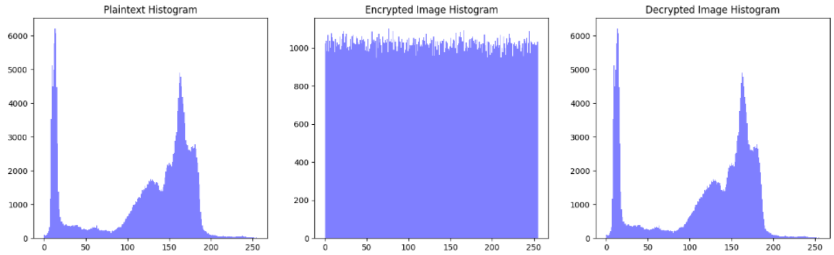


Figure 8. Original, Encrypted, And Decrypted Cameraman Histogram

Based on figure 8 the intensity distribution in the original histogram has notable peaks in the low to mid-intensity range, with a decline at higher intensities. This indicates a concentration of lower-intensity pixels in the original image. After encryption, the encrypted histogram displays a uniform distribution across all intensity levels, reflecting the algorithm's success in effectively obfuscating the original visual pattern. The decrypted histogram then closely matches the original image's distribution, confirming that the decryption process accurately restores the image to its original state without losing information, thus preserving the overall image integrity and quality.

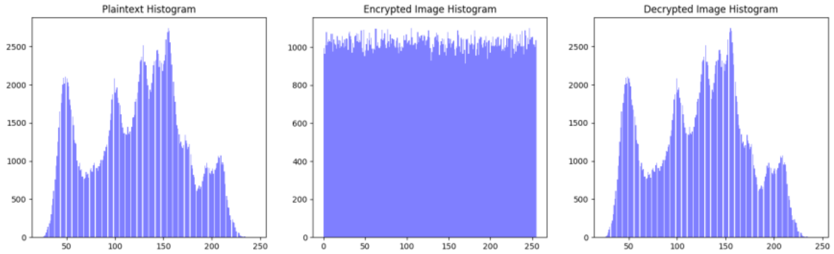


Figure 9. Original, Encrypted, And Decrypted Lena Histogram

Based on figure 9, the original histogram shows a relatively even distribution with peaks scattered across various intensity ranges, indicating a high intensity variation in the original image. After encryption, the encrypted histogram shows a uniform intensity distribution across the 0-255 range, demonstrating the encryption's effectiveness in scrambling pixel data and obscuring the original image pattern. The decrypted histogram then returns to a distribution that closely resembles the original image, indicating that the encryption-decryption algorithm can restore the image without significant changes, preserving the visual authenticity of the image.

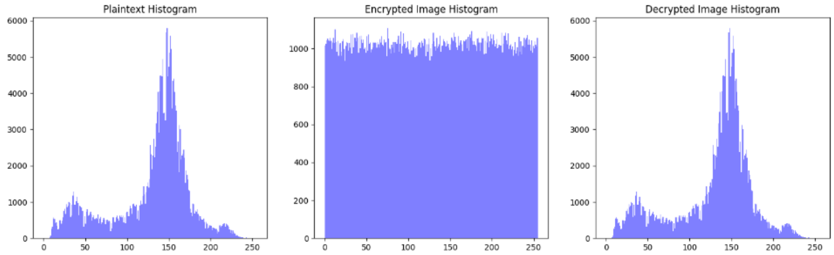


Figure 10. Original, Encrypted, And Decrypted Boats Histogram

Based on figure 10, the intensity distribution in the original image is concentrated around the 100-150 range, indicating a prevalence of mid-intensity pixels in the original image. This distribution reveals a characteristic visual pattern of the original image. After encryption, the encrypted histogram displays a uniform intensity distribution, suggesting that the encryption algorithm effectively concealed the original pattern. In the decrypted histogram, the intensity distribution returns to resemble the plaintext image, confirming that the decryption process restores the image to its original state without loss of visual information.

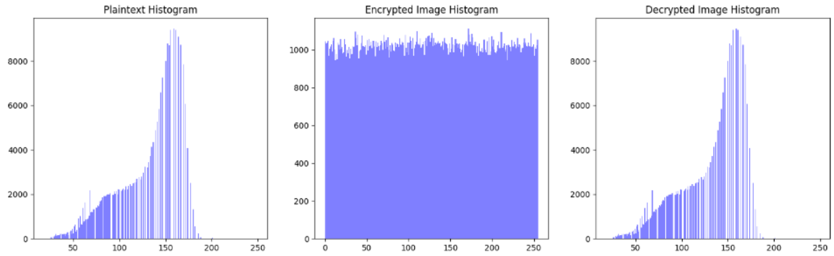


Figure 11. Original, Encrypted, And Decrypted Tank Histogram

Based on figure 11, the plaintext image's intensity distribution is concentrated between 100 and 200, with the highest peak around intensity 150. This shows that the original image has a somewhat narrow intensity variation. After encryption, the encrypted histogram shows a uniform distribution of intensity, indicating that the encryption algorithm effectively randomized the pixels and obscured the original pattern. The decrypted image histogram then closely matches the plaintext distribution, showing that the decryption process successfully preserves the original visual integrity, with the highest peak remaining in the same range.

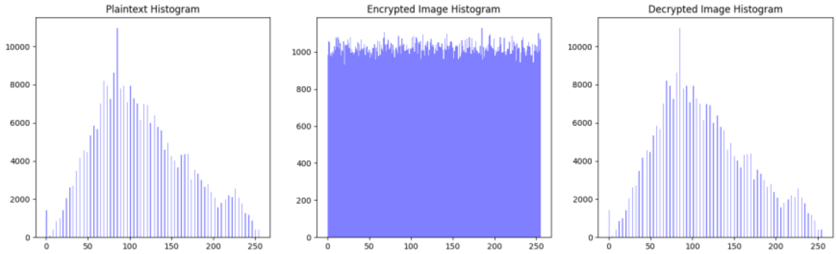


Figure 12. Original, Encrypted, And Decrypted Stream And Bridge Histogram

Based on figure 12, the original image shows a high peak at around intensity 100, suggesting many low-intensity pixels, which is typical for images with significant dark areas. After encryption, the encrypted histogram shows a uniform distribution across the entire range, indicating that the algorithm effectively scrambled the pixels and concealed the original pattern. In the decrypted histogram, the intensity distribution returns to resemble the plaintext image, demonstrating the encryption-decryption algorithm's effectiveness in restoring the original image without losing important visual details.

The proposed method successfully achieves this, as visually demonstrated by the relatively uniform histogram of the encrypted image [25], as show in figure 7-12.

3.3 Information Entropy Testing

In this test, entropy values were calculated for the original image, the encrypted image, and the decrypted image to assess the extent to which the encryption algorithm can produce an image with a high level of randomness. Table 3 presents the results of the information entropy (IE) calculation.

Table 3. IE results and its comparison with related works

Image	**Size (Pixel)**	**Method**[24]	**Proposed**
Pirate	512×512	-	7.9993
Tank	512×512	-	7.9992
Lena	512×512	-	7.9992
Stream Bridge	512×512	-	7.9992
Boat	512×512	7.9973	7.9992
Cameraman	512×512	7.9973	7.9992

The test results show that the entropy value of the encrypted image approaches the maximum value of 8 bits per pixel, with an overall excellent result of 7.999.

3.4 Robustness Test

The robustness testing of image encryption aims to assess the effectiveness of an encryption algorithm in maintaining the integrity of an image when part of its data is lost or corrupted. This test is crucial given the potential for partial data loss in encrypted images in real-world situations, such as due to poor data transmission or damaged storage media. In this test, a portion of the encrypted image data is intentionally deleted or corrupted, and the image is then decrypted to evaluate the extent to which the original image can be recovered [26]. A strong encryption algorithm is expected to produce an image that remains recognizable even after data loss. In this study, the proposed method was further tested, with the robustness test results shown in Figure 13.

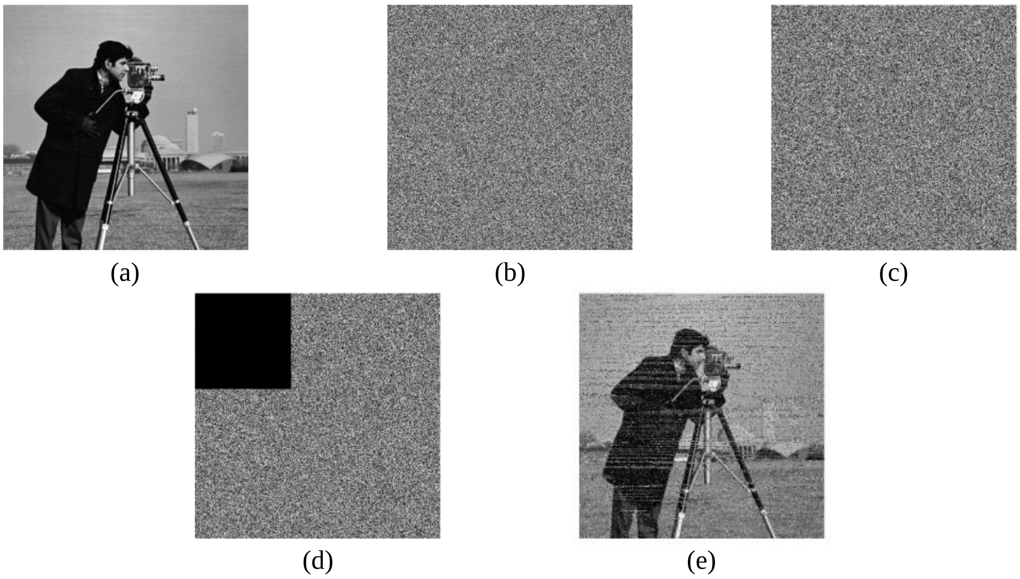


Figure 13. Robustness Test Using 200×200 Pixels Attack; (a) Original Image Of Pirate, (b) Encrypted Result, (c) Noise Attack Result, (d) Crop + Attack Result, (e) Decrypted Result

4. DISCUSSION

Based on previous research [24]. the experimental results in this study show excellent performance in measuring the security of image encryption using a combination of the Logistic Map, Cross 2D Hyperchaotic Map (C2HM), and route transposition algorithm. The results indicate that the NPCR value of 99.61% for the encryption of the cameraman and boat images demonstrates very high sensitivity to small changes in the image and encryption key. This suggests that even the smallest change in the image or key will result in a significant difference in the encrypted image, which enhances resistance to differential analysis between the original and encrypted images, as well as differential cryptanalysis attacks. This result is an improvement over previous studies, which often report lower NPCR values, indicating that the proposed scheme is more effective in creating encryption that is random and difficult to predict.

Furthermore, the UACI values obtained for the cameraman (33.41%) and boat (33.47%) images indicate significant and uniform changes in pixel intensity in the encrypted images. This suggests that the algorithm used not only produces noticeable changes in the image but also ensures that these changes are evenly distributed throughout the image. The high UACI value also indicates that this encryption scheme effectively increases confusion between adjacent pixels, which prevents statistical analysis techniques from detecting patterns in the image.

The information entropy value of 7.999 indicates a highly random distribution of pixels in the encrypted image, making statistical analysis on the encrypted image extremely difficult. This shows that the encryption produced by this method has a very high level of randomness, nearly approaching perfect random distribution. This result supports the claim that the proposed scheme offers a level of security comparable to encryption methods that use advanced cryptographic techniques.

Histogram analysis also shows that the pixel intensity distribution of the encrypted image is very uniform, unlike the histogram of the original image. This proves that the route transposition algorithm is effective in shuffling pixel positions, eliminating patterns that could be used for further analysis by unauthorized parties.

In addition to security testing, robustness testing shows that the proposed encryption scheme can maintain the integrity of the image even in the presence of data loss or corruption in parts of the image. In this test, despite disturbances or minor data damage, the decrypted image remains recognizable with a controlled degradation in quality. This result demonstrates that the proposed encryption scheme is resilient to real-world conditions, such as interference or data loss during transmission. This makes the method highly relevant for applications involving data transmission under imperfect conditions.

5. CONCLUSIONS

This research successfully proposes a multi-layer image encryption scheme that integrates the Logistic Map, Cross 2D Hyperchaotic Map (C2HM), and the route transposition algorithm, significantly enhancing image encryption security. The experimental results demonstrate excellent performance, with NPCR values reaching 99.61%, UACI values within the optimal range of 33%-34%, and information entropy achieving 7.999. These metrics indicate a high level of confusion and diffusion, essential for robust encryption. Histogram analysis further confirms the effectiveness of route transposition in scrambling pixel positions, thereby eliminating recognizable patterns that could be exploited by unauthorized parties.

Additionally, the proposed scheme proves to be robust against conditions of partial data loss or corruption, making it highly applicable in environments with imperfect data transmission. The use of a User Key hashed with the SHA-512 algorithm to generate the Initial Seed enhances security by adding resistance to brute-force attacks. Overall, the proposed encryption scheme offers a reliable, robust, and efficient solution for digital image security, with extensive potential applications in fields requiring high-level visual data protection.

REFERENCES

[1] A. K. Jain, S. R. Sahoo, and J. Kaubiyal, “Online social networks security and privacy: comprehensive review and analysis,” *Complex and Intelligent Systems*, vol. 7, no. 5, pp. 2157–2177, Oct. 2021, doi: 10.1007/S40747-021-00409-7/FIGURES/10.

[2] S. Sugiyatno, P. Sidiq, and I. F. Edrisy, “Pengaruh Teknologi 5G pada Evolusi Komunikasi: Sebuah Kajian Terhadap Perkembangan dan Implikasinya di Bidang Sains,” *NUCLEUS*, vol. 4, no. 2, pp. 115–120, Feb. 2024, doi: 10.37010/nuc.v4i2.1448.

[3] S. Zhao and M. Zappavigna, “Beyond the self: Intersubjectivity and the social semiotic interpretation of the selfie,” *New Media Soc*, vol. 20, no. 5, pp. 1735–1754, May 2018, doi: 10.1177/1461444817706074.

[4] N. Kshetri, “The evolution of cyber-insurance industry and market: An institutional analysis,” *Telecomm Policy*, vol. 44, no. 8, Sep. 2020, doi: 10.1016/j.telpol.2020.102007.

[5] A. Setyono, D. R. I. M. Setiadi, and Muljono, “StegoCrypt method using wavelet transform and one-time pad for secret image delivery,” *Proceedings - 2017 4th International Conference on Information Technology, Computer, and Electrical Engineering, ICITACEE 2017*, vol. 2018-January, pp. 203–207, Jul. 2017, doi: 10.1109/ICITACEE.2017.8257703.

[6] A. Singh, K. B. Sivangi, and A. N. Tentu, “Machine Learning and Cryptanalysis: An In-Depth Exploration of Current Practices and Future Potential,” *Journal of Computing Theories and Applications*, vol. 1, no. 3, pp. 257–272, Feb. 2024, doi: 10.62411/JCTA.9851.

[7] D. R. I. M. Setiadi, R. Robet, O. Pribadi, S. Widiono, and M. K. Sarker, “Image Encryption using Half-Inverted Cascading Chaos Cipheration,” *Journal of Computing Theories and Applications*, vol. 1, no. 2, pp. 61–77, Oct. 2023, doi: 10.33633/jcta.v1i2.9388.

[8] B. Zhang and L. Liu, “Chaos-Based Image Encryption: Review, Application, and Challenges,” *Mathematics 2023, Vol. 11, Page 2585*, vol. 11, no. 11, p. 2585, Jun. 2023, doi: 10.3390/MATH11112585.

[9] P. N. Andono and D. R. I. M. Setiadi, “Improved Pixel and Bit Confusion-Diffusion Based on Mixed Chaos and Hash Operation for Image Encryption,” *IEEE Access*, vol. 10, pp. 115143–115156, 2022, doi: 10.1109/ACCESS.2022.3218886.

[10] J. Oravec, L. Ovsenik, and J. Papaj, “An image encryption algorithm using logistic map with plaintext-related parameter values,” *Entropy*, vol. 23, no. 11, Nov. 2021, doi: 10.3390/e23111373.

[11] Muhammad Rizki, Erik Iman Heri Ujianto, and Rianto Rianto, "Digital Image Encryption Using Logistic Map," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 7, no. 6, pp. 1292–1299, Nov. 2023, doi: 10.29207/resti.v7i6.5389.

[12] S. Zhu and C. Zhu, "Secure image encryption algorithm based on hyperchaos and dynamic DNA coding," *Entropy*, vol. 22, no. 7, Jul. 2020, doi: 10.3390/e22070772.

[13] M. Kaur, D. Singh, and V. Kumar, "Improved seven-dimensional (i7D) hyperchaotic map-based image encryption technique," *Soft comput*, vol. 26, no. 6, pp. 2689–2698, Mar. 2022, doi: 10.1007/S00500-021-06423-8.

[14] M. Jin, K. Sun, and H. Wang, "Hyperchaos, extreme multistability, and hidden attractors in the novel complex nonlinear system and its adaptive hybrid synchronization," *Nonlinear Dyn*, vol. 110, no. 4, pp. 3853–3867, Dec. 2022, doi: 10.1007/S11071-022-07770-3/METRICS.

[15] T. Nestor *et al.*, "A New 4D Hyperchaotic System with Dynamics Analysis, Synchronization, and Application to Image Encryption," *Symmetry 2022, Vol. 14, Page 424*, vol. 14, no. 2, p. 424, Feb. 2022, doi: 10.3390/SYM14020424.

[16] L. Teng, X. Wang, F. Yang, and Y. Xian, "Color image encryption based on cross 2D hyperchaotic map using combined cycle shift scrambling and selecting diffusion," *Nonlinear Dyn*, vol. 105, no. 2, pp. 1859–1876, Jul. 2021, doi: 10.1007/s11071-021-06663-1.

[17] X. Xue, D. Zhou, and C. Zhou, "New insights into the existing image encryption algorithms based on DNA coding," *PLoS One*, vol. 15, no. 10, Oct. 2020, doi: 10.1371/journal.pone.0241184.

[18] X. Huang, Y. Dong, G. Ye, W. S. Yap, and B. M. Goi, "Visually meaningful image encryption algorithm based on digital signature," Feb. 01, 2023, *KeAi Communications Co.* doi: 10.1016/j.dcan.2022.04.028.

[19] A. Susanto, A. Sari, E. H. Rachmawanto, M. Doheir, W. Bagus Nugroho, and C. A. Sari, "A ROBUST AND IMPERCEPTIBLE FOR DIGITAL IMAGE ENCRYPTION USING CHACHA20," vol. 5, no. 2, pp. 397–404, 2024, doi: 10.52436/1.jutif.2024.5.2.1470.

[20] P. Parida, C. Pradhan, X. Z. Gao, D. S. Roy, and R. K. Barik, "Image Encryption and Authentication with Elliptic Curve Cryptography and Multidimensional Chaotic Maps," *IEEE Access*, vol. 9, pp. 76191–76204, 2021, doi: 10.1109/ACCESS.2021.3072075.

[21] O. Dişkaya, E. Avaroğlu, H. Menken, and A. Emsal, "A New Encryption Algorithm Based on Fibonacci Polynomials and Matrices," *Traitement du Signal*, vol. 39, no. 5, pp. 1453–1462, Oct. 2022, doi: 10.18280/TS.390501.

[22] M. Kaur, D. Singh, V. Kumar, B. B. Gupta, and A. A. Abd El-Latif, "Secure and energy efficient-based E-Health care framework for green internet of things," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 3, pp. 1223–1231, Sep. 2021, doi: 10.1109/TGCN.2021.3081616.

[23] X. Qian, Q. Yang, Q. Li, Q. Liu, Y. Wu, and W. Wang, "A Novel Color Image Encryption Algorithm Based on Three-Dimensional Chaotic Maps and Reconstruction Techniques," *IEEE Access*, vol. 9, pp. 61334–61345, 2021, doi: 10.1109/ACCESS.2021.3073514.

[24] X. Gao, "Image encryption algorithm based on 2D hyperchaotic map," *Opt Laser Technol*, vol. 142, Oct. 2021, doi: 10.1016/j.optlastec.2021.107252.

[25] S. Zhou, Y. Wei, Y. Zhang, and L. Teng, "Novel Chaotic Image Encryption Using Dynamic DNA Coding," 2023, doi: 10.21203/rs.3.rs-2650537/v1.

[26] E. Winarno, K. Nugroho, P. W. Adi, and D. R. I. M. Setiadi, "Combined Interleaved Pattern to Improve Confusion-Diffusion Image Encryption Based on Hyperchaotic System," *IEEE Access*, vol. 11, pp. 69005–69021, 2023, doi: 10.1109/ACCESS.2023.3285481.