Received: August 10, 2023. Revised: October 3, 2023.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Hybrid Image Encryption Technique for Securing Color Images Transmitted Over Cloud Networks

Suhad Abbas Yassir[1] **Haidar Raad Shakir[2]***

[1]*Southern Technical University, Shatra Technical Institute, Iraq*
[2]*University of Thi-Qar, Thi-Qar, Iraq*
* Corresponding author's Email: haidar.raad@utq.edu.iq

Abstract: Information is an asset that profoundly affects every aspect of our lives and requires protection from malicious attacks. Although storing it in a repository can safeguard this information, techniques to maintain confidentiality during transmission over communication networks are essential. Due to the advent of digital technologies and easy communication channels, most of the information now exists in images or other multimedia formats. To safeguard such formats, it is crucial to encrypt information before transmitting it over a network. Encryption transforms the data such that only the intended recipients can reconstruct it. Image encryption is a widely researched topic and various methods have been proposed. As traditional methods often fail to provide adequate protection, advanced encryption standards are currently being investigated. Chaos-based techniques are strong contenders for cryptography because they ensure confidentiality, nonperiodicity, and randomness and are easy to implement. Therefore, they are frequently utilized and can be combined with other methods to bolster protection. In this study, we developed a hybrid image-encryption technique that leverages hyperchaotic maps and elliptic-curve cryptography to guard data against security vulnerabilities. The proposed method achieves an average entropy information value of 7.99%, indicating its resilience to entropy attacks. Furthermore, it showed a net pixel change rate of over 99% for all the test images acquired from the final diffusion stage. It also recorded peak security values of 0.9897, 0.9848, and 0.9676 in the horizontal, vertical, and diagonal directions, respectively. Overall, the scheme demonstrated a satisfactory performance across nearly all evaluation criteria.

Keywords: Image encryption, Chaotic maps, Elliptic-curve cryptography, Decryption, Cloud networking.

1. Introduction

Over the last decade, "cloud" computing has become one of the most frequently used terms in computer science research. This technology allows both individuals and organizations to store vast amounts of multimedia data, including documents, images, and videos. Moreover, it enables easy sharing and access across networks, thereby addressing the constraints of individual computer storage and computation. However, because multimedia files may contain sensitive information, securing them against unauthorized access is imperative [1, 2]. Therefore, image-encryption techniques have been developed to enhance data security. While various encryption algorithms, such as the data encryption standard, advanced encryption standard, and Rivest–Shamir–Adleman, have been employed in data-security methods to provide better data protection [3], they face several limitations that compromise their effectiveness. These algorithms convert data into a seemingly incomprehensible format; however, their predictability, attack vulnerability, and limited keyspace raise security concerns. Nonetheless, these methods have provided a good technical foundation [4] for text data encryption. The digital age has also exacerbated these challenges, given the massive influx of multimedia data that require encryption before transmission. Hence, various enhanced techniques, such as S-Box, DNA coding, and chaotic mapping, have been proposed [5, 6], but they still struggle to provide sufficient protection for multimedia data.

Among these, chaos-based methods, characterized by pseudo-randomness, sensitivity to initial conditions, and ergodicity, are promising for multimedia encryption [7]. Pseudo-random sequences make chaotic maps very complex and difficult to analyze, thereby making them difficult to hack. Various chaos-based algorithms have been proposed, including 1D to 3D chaotic cat map conversion, to develop encryption schemes that provide real-time security. Advanced 3D chaotic methods permute the image pixel positions, and the permuted image is diffused using a logistic chaotic system [3]. For example, a chaos-based quantum encryption method was used in [8] to encrypt healthcare images. As the exchange of medical images between healthcare professionals and patients may occur over cloud platforms, stringent security mechanisms are required. In the proposed technique, the image is scrambled and encrypted using a quantum XOR operation based on a key generator controlled by a chaotic logistic map [9]. However, quantum encryption is not yet widely available, and is still a relatively new technology that limits its applicability in real-world scenarios.

Researchers have also attempted to hybridize different methods to transform images into more secure and unrecognizable formats. In [10], two chaotic maps (logistic and tent maps) were combined to increase chaotic performance and produce new strong image ciphers that are highly resistant to various cryptanalytic attacks, but are not very secure owing to their relative simplicity, making it possible to predict their behaviors. To enhance the security features in chaos-based cryptography [11], pseudo-random bit sequences were designed to increase the randomness during post-processing to blur symbol boundaries. However, the security of this approach is compromised due to the potential predictability of the pseudo-random sequence obtained by analyzing its statistical features. As a result, despite existing security mechanisms that protect image information and various research advancements, there is scope for further research.

Recently, neural networks have been proven to be cost-effective optimization techniques for securing images [12]. Although they can be used efficiently with chaotic map techniques to evaluate simple encryption methods, implementing neural networks to protect images from diverse attacks may be computationally expensive and impractical for encrypting large images.

Several researchers believe that chaos theory-based cryptographic techniques are useful for developing novel and efficient image-encryption techniques. Most image-encryption models involve four steps: image preprocessing, key generation, image encryption, and decryption. Two chaotic maps have been hybridized [13] for parameter tuning, which improved the performance and confirmed that it is an effective and secure method for image-transfer tasks. Continuous efforts are being made to improve the performance of image-encryption cryptosystems. In [14], an image-encryption system was developed by fusing a machine learning algorithm (support vector machine) and a chaotic system, wherein a hash function was used for chaotic map initialization. However, SVMs are not well suited for image encryption because they cannot effectively encrypt images without compromising quality.

The fusion of a chaotic sequence and k-medoids clustering machine learning algorithm has been used to scramble original/plain images; this method can resist various classical attacks. In [15], a hybrid 2D-chaotic-map-based method was proposed, which included a sine-cosine cross-chaotic map in the confusion phase. For diffusion, this method uses a 1D logistic chaotic map to produce a chaotic self-diffusion matrix that is bitwise XORed and finally generates the cipher image [16]. Hence, it combines 1D and 2D chaotic maps and is claimed to be more unpredictable and secure; however, this map has not been very well studied, and its security properties are not fully understood.

To further enhance secure communications and data protection in cloud-based storage systems, the exploration of novel hybrid chaos-based image-encryption schemes has emerged as a notable trend in the recent literature. These algorithms frequently combine multiple chaotic systems to improve algorithmic performance and security, particularly for color images. For example, Salman et al. proposed using dual chaotic systems and hash functions to encrypt images [17]. These approaches typically involve two crucial phases, confusion and diffusion. In the confusion phase, both the plain image and private key collaboratively generated unpredictable sequences, which were then used to shuffle and rotate the image. However, these methods rely on one-dimensional logistic maps; therefore, their efficacy in ensuring secure communication is questionable [18]. Another study investigated the encryption of color images using an S-Box-based one-dimensional logistic map [19]. While innovative, the technique exhibited a significant following drawback: the potential for complete image decryption and suboptimal performance for secure communication. Zareai et al. also incorporated Arnold's cat map, logistic mapping, and image blocking for image encryption [20]. This approach succeeded in encrypting images, but the decrypted

images retained all the original information, which is a significant limitation in image encryption [21]. Additionally, this technique has limitations in handling color images. In contrast, another study proposed a novel exploration utilizing the discrete fourier transform (DFT) for secure image encryption and decryption [22]. Good encryption results were obtained, but the approach could not address the shortcomings associated with two-dimensional Baker maps, that is, their vulnerability to statistical attacks [23]. Another interesting study integrated gray code, quantum walks, and the Henon map, which are commonly utilized in image encryption [24], to enhance encryption security. These methods generate encryption keys that are complexly correlated to the original image, thereby making them highly sensitive even to minor alterations. However, the Henon map can be predicted using finite chaotic sequences [25]. Furthermore, advancements in color image encryption, such as an approach based on a bit-plane and the Chen chaotic system outlined in [26], have demonstrated promising potential for better image protection but with vulnerabilities. Recent findings have shown that without access to encryption keys, encrypted images can be fully retrieved [27]. Another intriguing method employs AES and the Rossler chaotic map for image encryption [28]. These two methods improve the effectiveness of the model but are sensitive to initial conditions and susceptible to statistical analysis, potentially compromising its security [29].

In summary, providing good data encryption, chaos-based image-encryption techniques have several limitations, including high computational complexity, which makes them slow to encrypt and decrypt images. The sensitivity of chaotic maps to initial conditions (butterfly effect) also renders them vulnerable to certain attacks. Furthermore, it is challenging to design chaotic maps that are both secure and efficient, leaving room for further investigation in addressing these limitations.

Therefore, this study introduces a novel hybrid image-encryption technique that combines hyperchaotic maps and elliptic-curve cryptography (ECC) to enhance data security and improve computational efficiency. This approach aims to provide a higher sensitivity, improved resistance to cryptanalysis, and robust protection against entropy attacks. By synergizing hyperchaotic maps and ECC, our proposed technique establishes a secure image-encryption model that addresses the shortcomings of traditional methods. By integrating these advanced cryptographic concepts, we presented a solution that contributes to the broader goal of securing multimedia data in cloud networks. Our evaluation results demonstrated the robustness of the proposed method against statistical and other attacks. Finally, the proposed approach offers a reduced correlation between adjacent pixels in encrypted images, enhancing the overall security and confidentiality.

The rest of this paper is organized as follows. The materials and methods section discusses the technical details of hyperchaotic maps and ECC, encryption process, and evaluation of the proposed scheme against state-of-the-art methods. The Results and Discussion section presents the evaluation outcomes, including histogram analysis, PSNR, MSE, entropy information, adjacent-pixel correlation, and resistance to differential attacks. The study concludes with the conclusion and future scope section, summarizing the contributions, reiterating the strengths of the proposed method, and suggesting potential research directions.

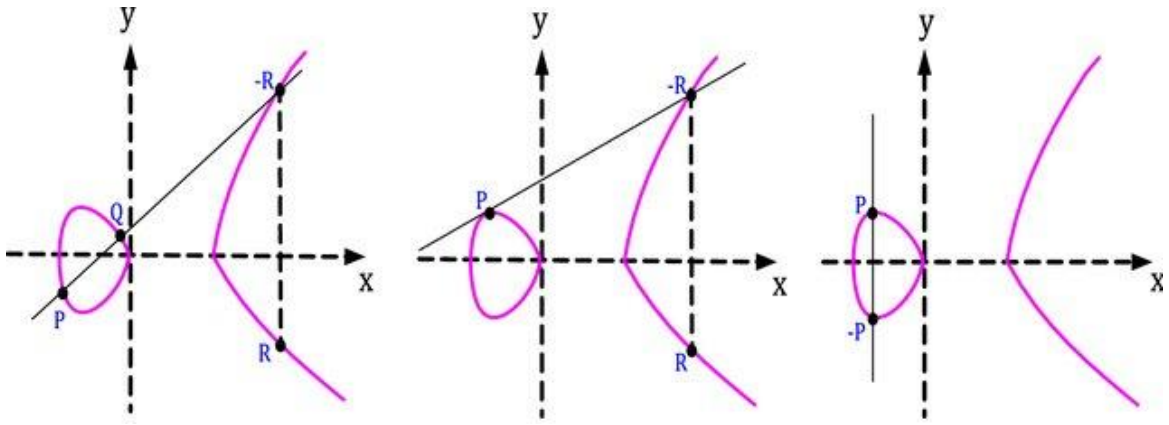
2. Materials and methods

2.1 Preliminaries

This section explains the principles of ECC and the 6D hyperchaotic system used to encrypt the digital images in the proposed scheme. Cryptographic systems can be broadly categorized into symmetric and asymmetric encryptions based on key distribution. Symmetric encryption uses the same key for both encryption and decryption, simplifying key management but posing risks if compromised. Asymmetric encryption involves separating public and private keys, making it challenging for intruders to breach security. ECC is a well-known asymmetric encryption technology owing to its computational efficiency, compact keys, and strong security. This enables secure communication, digital signatures, and authentication. Asymmetric encryption eliminates the need for secure key exchanges, benefiting from interactions with unknown or untrusted parties. ECC offers improved security, faster performance, and smaller key sizes and is gaining popularity across diverse applications.

2.1.1. Six dimensional (6D) hyperchaotic system

Mathematical analyses have shown that the typically used chaotic functions are nonlinear and exhibit dynamic behaviors, making their responses difficult to predict. Studies have shown that the dynamic behavior of hyperchaotic functions is considerably more complicated than that of low-dimensional chaotic functions [30]. A chaotic system must be comprised of at least four dimensions. Moreover, low-dimensional chaotic functions only have one positive Lyapunov exponent, whereas high-



(a) (b) (c)

Figure. 1 ECC processes: (a) point addition (R=P+Q) (b) point doubling (R=P+P) (c) point multiplication (R=P+(-P))

dimensional functions have at least two values.

Wang and Yu [31] defined a 6D hyperchaotic system as follows:

$$\begin{cases} x_1 = a(x_2 - x_{1)} + x_4 - x_5 - x_6 \\ x_2 = cx_1 - x_2 - x_1x_3 \\ x_3 = -bx_3 + x_1x_2 \\ x_4 = dx_4 - x_2x_3 \\ x_5 = ex_6 + x_3x_2 \\ x_6 = rx_1 \end{cases} \quad (1)$$

where a, b, c, d, e, and r are constants and x_1, x_2, x_3, x_4, x_5, and x_6 are the state variables of the 6D hyperchaotic system.

In this study, a = 10, b = 83, c = 28, d = 1, e = 8, and r = 3 were selected as constants. This ensures that the system has two positive Lyapunov exponents that satisfy the condition (the sum of all exponents is negative).

2.1.2. Elliptic-curve cryptography

Let F_p be the finite field of the modulo of large prime p. F_p is used to define an elliptic curve E as in the following formula:

$$Y^2\ X^3 + aX + b\ mod\ p \quad (2)$$

where a and b satisfy:

$$4a^3 + 27b^2\ mod\ p \neq 0 \quad (3)$$

The elliptic curve E with order n should have a base point P that meets N. $P = O$, where N is the order of P, and O is a point at the end of line E. Points of the elliptic curve E_p (a, b) comprise an additional cyclic group G_p of order p. The ECC comprises four tasks:

- Point addition: Consider an elliptic curve $E_p(a,b)$ with two points, P and Q, with coordinates (X_1,Y_1) and (X_2,Y_2), respectively. Adding these points yields a third point that falls on the elliptic curve. As shown in Fig. 1(a), these points are connected to a straight line. The elliptical curve exhibited X-axis symmetry. The reflection of the third point produces a new point on the curve with, negative X- and Y-coordinates. The coordinates of the two curved points are calculated as follows [32]:

$$\lambda = [(Y_2 - Y_1)(X_2 - X_1)] \quad (4)$$

$$X_3 = \lambda 2(X_1 + X_2) \quad (5)$$

$$Y_3 = \lambda(X_3 - X_3) - Y_1 \quad (6)$$

- Point doubling: During this process, a point is added. Domain parameters and slopes are required to determine this value. The slope under the condition $P = Q$ is computed as follows:

$$\lambda = [\frac{3{X_1}^2 + a}{2Y_1}] \quad (7)$$

$$X_3 = \lambda^2 - 2X_1 \quad (8)$$

$$Y_3 = \lambda(X_1 - X_3) - Y_1 \quad (9)$$

- Point multiplication: The repetitive addition of a point to itself creates multiplication on an elliptic curve. Consider a point on curve E_p denoted by $P(x,y)$ (a,b). This operation is also referred to as scalar multiplication if K is a scalar integer. The repeated addition is expressed as $k_P = P + P + P...k$ times.

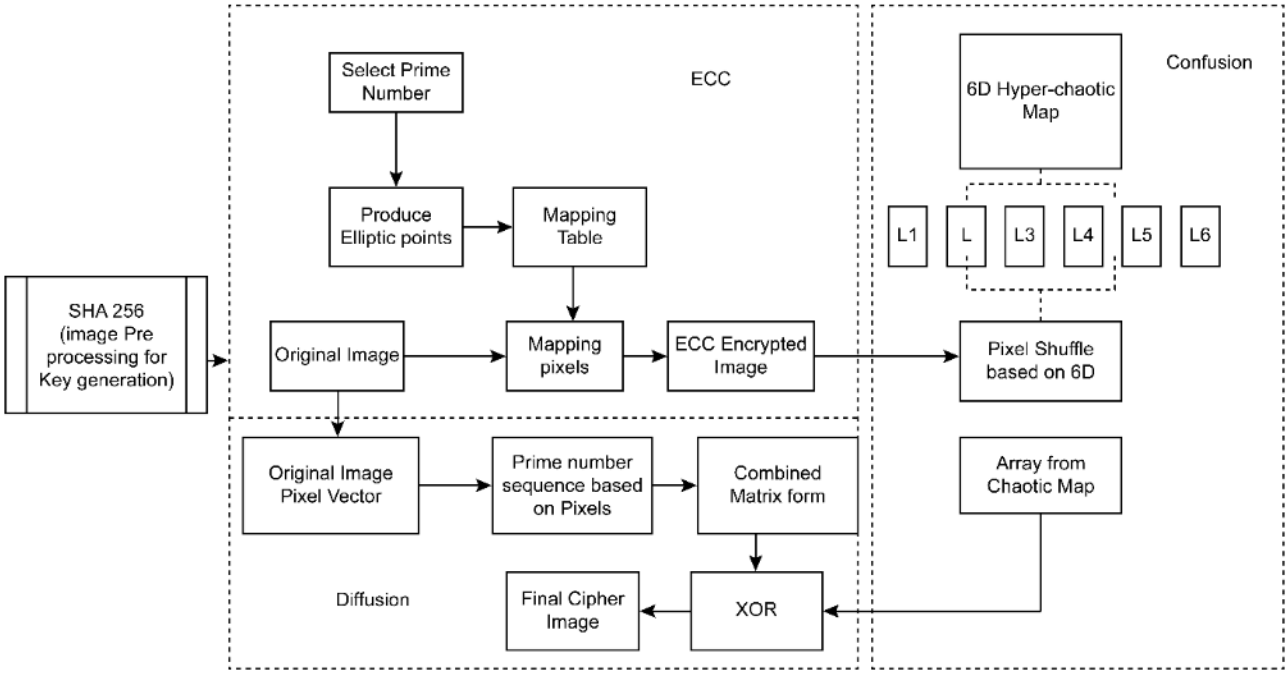


Figure. 2 Framework of the proposed cryptographic model for image security

$$\begin{cases} X_1(0) = mod(\left(x_1'(0) + \frac{mod(h_1+h_2+h_3+h_4+h_5,256)}{256}\right),1) \\ X_2(0) = mod(\left(x_2'(0) + \frac{mod(h_6+h_7+h_8+h_9+h_{10},256)}{256}\right),1) \\ X_3(0) = mod(\left(x_3'(0) + \frac{mod(h_{11}+h_{12}+h_{13}+h_{14}+h_{15},256)}{256}\right),1) \\ X_4(0) = mod(\left(x_4'(0) + \frac{mod(h_{16}+h_{17}+h_{18}+h_{19}+h_{20},256)}{256}\right),1) \\ X_5(0) = mod(\left(x_5'(0) + \frac{mod(h_{21}+h_{22}+h_{23}+h_{24}+h_{25},256)}{256}\right),1) \\ X_6(0) = mod\left(\left(x_6'(0) + \frac{mod(h_{26}+h_{27}+h_{28}+h_{29}+h_{30},256)}{256}\right),1\right) \end{cases} \quad (10)$$

Multiplication entails calculating k_P by conducting a series of point multiplications and adding to the product point.

2.2 Proposed framework

In this section, we explain the proposed cryptographic model shown in Fig. 2, which comprises the key generation, confusion, and diffusion processes.

2.2.1. SHA-256 key generation

Hybrid image encryption based on hyperchaotic maps and ECC was initialized with a key obtained using the SHA-256 hash algorithm. The SHA-256 hash value H of a plaintext image is divided into 32 8-bit groups and converted into decimal numbers. Hence, H can be expressed as $H = h_1, h_2, h_3,..., h_{32}$, where h_i is a decimal number in the range [0, 255]. The initial values and parameters of the chaotic system are as follows:

where $x_1(0)$, $x_2(0)$, $x_3(0)$, $x_4(0)$, $x_5(0)$, and $x_6(0)$ denote the preset initial values of the 6D hyperchaotic system. In this manner, the keys of the chaotic system were set.

2.2.2. Image encryption and decryption

The encryption procedure involves two processes: diffusion and confusion.

The diffusion process comprises the following steps.

- Consider an input image X with dimensions of $M \times N$.
- The elements of X are referred to as "messages" and denoted as m.
  m is transformed into a point on the curve (X_i,Y_i), denoted as $P_m = (X_i,Y_i)$. Similarly, all pixels are mapped to the (x,y) coordinate pairs created through ECC processes. By substituting the x value in the elliptic-curve equation into the general equation below, the

appropriate value of y can be determined using.

$$y_2 = \{(x_3 + a_x + b) \text{ (modulo } P)\} \quad (11)$$

where P is the large prime integer.

- The sender and receiver select the private keys K_a and K_b, respectively, which are large integers.
- The generator point $G = (G_x, G_y)$ is obtained from the curve.
- The sender generates public key P_a by multiplying its private key K_a by the generator point:

$$P_a = K_a \times (G_x, G_y) \quad (12)$$

- The receiver computes the public key K_b by multiplying its private key by the generator point:

$$P_b = K\text{b} \times (G_x, G_y) \quad (13)$$

- The public keys of both users are shared. P_m represents the mapped data of the original message to be encrypted, whereas P_c represents cipher data:

$$P_c = (P_a, P_m + K_a) \text{ and } P_b = P_c (X, Y) \quad (14)$$

This generated encrypted image is transmitted to the confusion process.

The diffusion process, which is based on a 6D hyperchaotic system, comprises the following steps:

- First, the initial condition of the system is obtained using Eq. (10), based on a plain image.
- Three different integer numbers, ranging between 1 and 6, were randomly generated to select the hyperchaotic sequence number. These numbers were stored as i_1, i_2, and i_3. For example, $i_1 = 1$, $i_2 = 5$, $i_3 = 6$.
- The hyperchaotic system is then iterated using Eq. (1) to produce a new vector, after which three sequences were selected (xi_1, xi_2, and xi_3). Each sequence was assigned a color channel for shuffling (red, green, or blue).
- The order of the sorted numbers in this vector was employed to confuse plain images.

After both processes were completed, the final encrypted image was obtained. For decryption, the following procedure was implemented. The decryption process is the reverse of the encryption process. The steps are summarized as follows:

- Six key streams are obtained by iterating the 6D hyperchaotic system.
- Thereafter, three cryptographic matrices (xi_1, xi_2, and xi_3) are obtained.
- The order of the sorted numbers in this vector is employed to decrypt the pixel positions in the plain image.
- At the receiver, the original information is retrieved by applying the receiver's private key K_b. The first point is multiplied by the receiver's private key K_b and added to the second point to restore the final image, as follows:

$$P_m = (P_m + K_a P_B - K_b P_a) = P_m (X_i, Y_i) \quad (15)$$

2.3 Evaluation setup

The proposed image-encryption scheme uses hyperchaotic maps and ECC and was implemented in MATLAB 2022b. Additionally, its performance was evaluated using 11 color images, as shown in Fig. 3.

The proposed scheme was validated against seven state-of-the-art models [17, 19, 20, 22, 24, 26, 28] established for image encryption. In [17], dual chaotic systems and hash functions were employed for image encryption. These approaches involved two key phases, confusion and diffusion. In the confusion phase, the plain image and a private key generated unpredictable sequences to shuffle and rotate the image. In the diffusion phase, a mathematical tool called a logistic map was used to further scramble the encrypted image. The study in [19] introduced a color image-encryption technique utilizing a one-dimensional logistic map. This technique employs chaotic sequences to construct S-boxes, which were used to compute the pixel values within small image blocks. In [20], the authors leveraged the Arnold cat map, logistic mapping, and image blocking. This unique algorithm divides the image into four blocks, independently relocating pixel values within each block and then globally displacing them using Arnold cat mapping. The authors of [22] utilized a discrete Fourier transform (DFT) technique for secure image encryption and decryption. This approach applies Baker's map to modified picture coefficients in the frequency domain. The study in [24] combined Gray code, quantum walks, and the Henon map, which are often used in image encryption. These algorithms create key streams tied to the plain image, introducing extreme sensitivity to even minute-bit changes in the original image. Additionally, [26]

Figure. 3 Test images used to evaluate the proposed scheme

introduced a bit-plane and Chen's chaotic system-integrated encryption model. The algorithm splits an RGB image into three channels, each representing an eight-bit binary integer. The upper and lower four bits of each pixel's binary gray value were swapped, and a logistic chaotic sequence was used to encrypt the position of each four-bit integer. The four-bit binary numbers were converted to hexadecimal values for the computation. Another logistic chaotic sequence was used to permute the modified image's position, and the Chen chaos sequence was used to compute the gray pixel values.

Finally, [28] proposed an image-encryption algorithm called AES&Rossler hyperchaotic modeling (ARHM). The algorithm uses the AES symmetric encryption algorithm and Rossler chaotic map to encrypt images. The ARHM algorithm first generates two-dimensional random chaotic sequences using the Rossler chaotic map. These chaotic sequences were then used to encrypt the image pixels using the AES algorithm.

Based on these comparisons, the proposed model's superiority and novelty is established.

3. Results and discussion

3.1 Histogram analysis

The pixel intensity values of the original and encrypted images were analyzed using a histogram. A graph can better represent a histogram by providing image information, such as the pixel count at every distinct intensity value. The image information does not change during the confusion process. Therefore, the pixels of an encrypted image histogram resemble those of the original image. However, the encrypted (cipher) images obtained from the diffusion stage do not contain the exact information of the original image during the transmission. The histograms in Fig. 4 show no similarities between the original and final encrypted images.

Fig. 4 shows that the pixel value distributions of several plaintext color channels have distinct

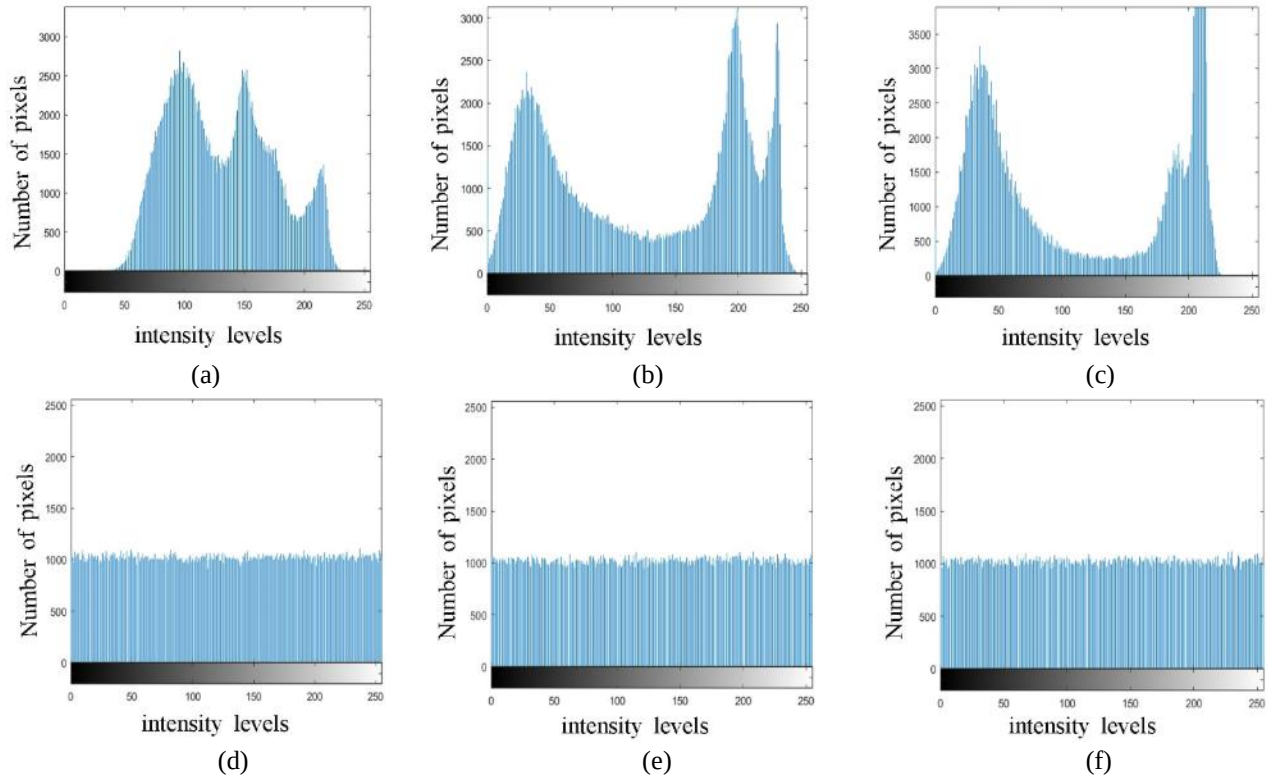


Figure. 4 Histograms of plain and cipher the Tree images of Tree: (a) red, (b) green, and (c) blue histograms of plain image; (d) red, (e) green, and (g) blue histograms of cipher image

Table 1. PSNR and MSE values

Image	PSNR	MSE
Airplane	7.9787	10356.4203
Baboon	8.7756	8620.3176
Bus	8.1673	9916.3257
Fruits	8.1053	10058.8507
Peppers	8.0737	10132.3038
Town	8.5698	9038.5086
Airport Tower	8.4456	9300.8207
Sailboat	8.0825	10111.8216
River	7.8779	10599.7331
Lena	8.6106	10486.1438
Statue	7.0816	12732.6626

properties, whereas their cipher text color histograms are evenly distributed. Additionally, an attacker cannot extract statistical information from a ciphertext image. Hence, the image-encryption technique presented in this study is resistant to statistical analysis attacks.

3.2 Peak signal-to-noise ratio and mean square error

An encrypted (cipher) image must be sensitive to minute variations in the original image. Observing attacks initiated by attackers is necessary to alter the image features. When an attacker performs a differential attack, a small amendment in the plain/original image would result in a significant transformation in the cipher image. If the security mechanism is highly sensitive, the attack would not have any impact. The MSE is used to calculate the differences between the original and encrypted images, and a high MSE value indicates a high difference.

The MSE is expressed as follows:

$$MSE = \frac{1}{M_x N_x f} \sum_{K=1}^{f} \sum_{i=1}^{M} \sum_{j=1}^{N} (P(i,j) - C(i,j))^2 \quad (16)$$

where *f* denotes the number of frames in an image, and *M* and *N* denote the rows and columns, respectively. The pixels in the original and encrypted images are denoted by *P (I, j)* and *C (i, j)*, respectively.

The PSNR for an image of size $M \times N$ is calculated as follows:

$$PSNR = 10\, log_{10}\left(\frac{Max_{01}^2}{MSE}\right) dB \quad (17)$$

where Max_{01}^2 is the maximum possible pixel value of the original image, and the PSNR calculated between the original and encrypted images indicates the efficiency of the encryption model.

Table 2. Information entropies of the original and cipher images

Image	Original Image			Cipher Image		
	R	G	B	R	G	B
Airplane	6.7178	6.7990	6.2138	7.9993	7.9992	7.9995
Baboon	7.7067	7.4744	7.7522	7.9992	7.9994	7.9993
Bus	7.5445	7.4588	7.5027	7.9991	7.9990	7.9990
Fruits	7.0556	7.3527	7.7134	7.9993	7.9993	7.9993
Peppers	7.3388	7.4963	7.0583	7.9993	7.9993	7.9993
Town	7.3908	7.4706	7.5112	7.9991	7.9992	7.9990
Airport	7.3263	7.0950	7.0473	7.9991	7.9990	7.9990
Tower						
Sailboat	7.3124	7.6429	7.2136	7.9993	7.9994	7.9992
River	7.4283	7.3365	7.1686	7.9991	7.9990	7.9989
Lena	7.2531	7.5952	6.9686	7.9993	7.9992	7.9993
Statue	7.6143	7.3993	7.1923	7.9992	7.9991	7.9990

Table 3. Information entropies obtained by the proposed and other encryption schemes

Encryption Scheme	Information Entropy
Ref. [17]	7.9998
Ref. [19]	7.9972
Ref. [20]	7.9994
Ref. [22]	7.1446
Ref. [24]	7.9997
Ref. [26]	7.9993
Ref. [28]	7.9971
Proposed Scheme	7.9992

Table 1 lists the PSNR and MSE values for the test images used in this study.

3.3 Entropy information

Entropy information was used to evaluate the randomness and uncertainty in the encrypted image.

Entropy information E is calculated as follows:

$$E = -\sum_{i=0}^{N-1} P(X)_i \log_2 X_i \qquad (18)$$

where $P(X_i)$ denotes the probability of the occurrence of a symbol.

Table 2 lists the entropy information of the original and final encrypted images of the red, green, and blue pixels. The results indicate that the entropy information values of the encrypted images are very close to the ideal value of 8 and are almost similar for all images, indicating that the chances of the images being corrupted by attacks are low.

Several encryption schemes have been appraised based on their information entropy, using the Lena color image as a benchmark. A higher entropy value indicated a more random image. The proposed scheme significantly outperformed the models of Salman et al. [19], adopting an S-Box with a chaotic map (7.9972), El-Sayed et al. [22] integrating chaotic baker map in DFT (7.1446), Yi and Cao [28], utilizing AES combined with Rossler hyperchaotic modeling (7.9971). In contrast, the entropy value of Budiman et al. [17], employing double-layer chaos with dynamic iteration and rotation pattern (7.9998), Zareai et al. [20], blending image blocking with the Arnold Cat and logistic mapping (7.9994), Xu et al. [26] applying a bit-plane with the Chen Chaotic System (7.9993), and Abd-El-Atty et al. [24], introducing a novel image cryptosystem using Gray code, Quantum Walks, and Henon map (7.9997), slightly surpassing the proposed method. The analysis emphasized therobustness and randomness of the proposed encryption technique against various new methods, with an entropy close to 8.

3.4 Adjacent-pixel correlation

In the original image, a pixel and its adjacent pixels are highly correlated in the horizontal, vertical, and diagonal directions. An ideal encryption model must produce a cipher image without correlating it with the adjacent pixels. Table 4 lists the correlations between the pixels of the original and encrypted images.

The correlation coefficients for horizontal, vertical, and diagonally adjacent pixels were computed. The correlation coefficient of the original image exhibits a linear relationship, and the value is close to 1; however, the correlation coefficient of the cipher image exhibits a stochastic relationship with a value close to 0.

These correlation coefficient values indicate that the implemented encryption scheme is highly secure against statistical attack.

Mathematically, pixel correlation can be calculated by the following:

$$r_{xy} = \frac{E\,(x-E(x))\,E\,(y-E(y))}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (19)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x(i) \qquad (20)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(\,x(i) - E(x))^2 \qquad (21)$$

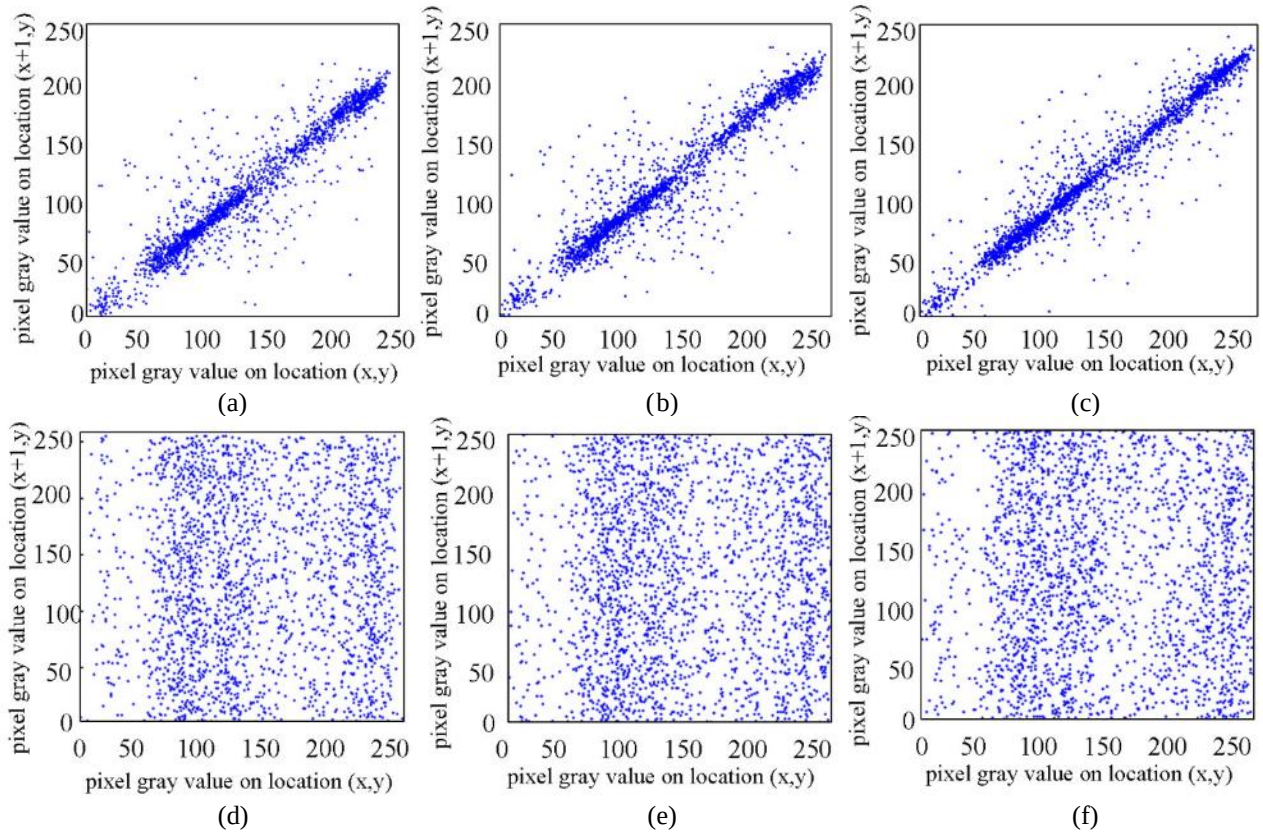


Figure. 5 Pixel distributions in the Lena image: (a), (c), and (e) show the vertical, horizontal, and diagonal correlation coefficients for the original image (Airplane), respectively; (b), (d), and (f) show the same correlation coefficients for the encrypted image

Table 4. Correlation coefficient values of the encrypted Lena image obtained through various encryption schemes

Scheme	**Horizontal**	**Vertical**	**Diagonal**
Lena (plain image)	0.9802	0.9885	0.9706
Proposed method	–0.0678	0.0088	−0.0155
Ref. [17]	-	-	-
Ref. [19]		0.0019 (avg.)	
Ref. [20]	−0.0012	−0.0012	−0.0012
Ref. [22]		−0.0947 (avg.)	−0.0947 (avg.)
Ref. [24]	−0.00007	−0.00007	−0.00007
Ref. [26]	0.0005	0.0005	0.0005
Ref. [28]	-	-	-

Table 5. NPCR and UACI values

Test images	**NPCR (%)**	**UACI (%)**
Airplane	99.6000	33.4902
Baboon	99.5903	33.5131
Bus	99.6051	33.4712
Fruits	99.6093	33.4446
Peppers	99.6086	33.5064
Town	99.6037	33.4789
Airport Tower	99.6047	33.5060
Sailboat	99.5990	33.5315
River	99.5763	33.4578
Lena	99.6544	33.4572
Statue	99.6139	33.3873

where N is a randomly selected adjacent-pixel pair, and x_i and y_i are depicted as gray values of the pixels.

Table 4 lists the correlation coefficient values of the encrypted Lena image obtained through various encryption schemes. The comparison indicates that the proposed model is highly sensitive. The correlation coefficients for the original image (Airplane) and the corresponding encrypted image are illustrated in Fig. 5.

Compared with the methods described in Table 3,

Table 6. NPCR and UACI values for the encrypted Lena image

Encryption algorithm	NPCR	UACI
Ref. [17]	99.5904	33.4517
Ref. [19]	99.601	33.56
Ref. [20]	99.6254	33.4660
Ref. [22]	99.4297	33.0529
Ref. [24]	99.6199	33.4557
Ref. [26]	99.6055	33.4822
Ref. [28]	99.36	33.26
Proposed method	99.65	33.45

the proposed encryption approach in Zareai et al. [8] and Zhao et al. [10] demonstrated lower correlation coefficients, indicating a more effective disruption structural patterns of the original image. Specifically, the average correlation coefficient for the proposed scheme, at −0.0815, falls below those of Salman et al. [6] and El-Sayed et al. [4], making it a robust choice against statistical attacks. Notably, this is consistent with the approach of Abd-El-Atty [12]. This strong resistance to structural correlation across different directions stems from the intricate shuffle process facilitated by the 7D chaotic map, significantly enhancing encryption complexity and bolstering the security of the method against potential decryption attempts.

3.5 Differential attacks

To protect an image from differential attacks, the encryption model must be robust and sensitive to the trivial deviations imposed on the plain/original image. Sensitivity was measured using the pixel variation in the original image. It is the effect of pixel variation on the image, that is, the net pixel change rate (NPCR). The results are expressed as a percentage.

If $X(i, j)$ and $Y(i, j)$ are the pixels of a ciphered image, and X and Y in row i and column j contain one-pixel variance with the original images, the NPCR is denoted as follows:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (22)$$

where W and H are the width and height, respectively, of X or B.

(i, j) is obtained as follows:

$$D(i,j) = \begin{cases} 1 \; if \; X(i,j) \neq (i,j) \\ 0 \; Otherwise \end{cases} \quad (23)$$

The NPCRs of the final encrypted images, which were obtained after implementing multiple hyperchaotic maps, are listed in Table 5. The NPCR analysis was considered positive because the NPCR value at the final diffusion stage was >99%, indicating the usefulness of chaotic maps. Unified averaged changed intensity (UACI) was also used to evaluate the impact of differential attacks on image encryption. The proposed scheme exhibited a stable and acceptable avalanche performance and was secure against differential attacks.

The UACI is expressed as follows:

$$UACI = \frac{1}{M_{np}} \left(\sum_{q,r} \frac{|L_a(q,r) - L_b(q,r)|}{2^{Gsp} - 1} \right) \times 100\% \quad (24)$$

where L_a and L_b denote the images and M_{np} denotes the pixel.

A comparison between this proposed scheme and other state-of-the-art algorithms is also presented in Table 6.

NPCR and UACI are crucial statistical metrics for assessing the quality of encrypted images. The NPCR quantifies the percentage of pixels that have undergone alteration between the original and encrypted images, whereas UACI gauges the average intensity change in the modified pixels. Remarkably, the proposed encryption method achieved the highest NPCR, an impressive 99.65%. This result signifies that a substantial number of pixels within the encrypted image have been distinctly transformed, attesting to the efficiency of the proposed method in effectively disarranging the image, thereby intensifying its resistance to decryption. Furthermore, the UACI value of 33.45 achieved by the proposed method falls within a comparable range to other methods, suggesting that the proposed method does not introduce any significant bias in the distribution of pixel intensities, ensuring that the average intensity changes remain consistent with the established encryption standards. In summary, the proposed encryption method outperforms the referenced methods in terms of NPCR and achieves consistent results in terms of UACI, indicating a higher degree of pixel value alteration and similar average intensity change in the encrypted image. These results confirm that the proposed model effectively disrupts the original image's structure and content, enhancing its security and resistance to decryption attempts. Thus, it was demonstrated that the proposed approach can successfully resist plaintext and differential attacks.

The superiority of the proposed scheme is also attributed to the asymmetric encryption technology of ECC, which enables secure communication, digital signatures, and authentication. This eliminates the need for secure key exchange, benefiting interactions with unknown or untrusted parties. ECC offers improved security, faster performance, and a smaller key size.

4. Conclusion and future scope

This study implemented a hybrid image-encryption technique that uses a hash function, hyperchaotic maps, and ECC to address the security flaws of conventional image cryptosystems. The proposed model combines confusion and diffusion processes initiated with a large keyspace using 6D hyperchaotic maps. An average entropy information value of 7.99% was obtained, indicating that it was robust against entropy attacks. Moreover, the NPCR was greater than 99% for all images obtained from the final diffusion stage. The maximum security values of the images obtained using the proposed scheme were 0.9897, 0.9848, and 0.9676 in the horizontal, vertical, and diagonal directions, respectively. Overall, the proposed encryption scheme performed satisfactorily for almost all the evaluation criteria. In the future, we will focus on developing more efficient encryption schemes in terms of evaluation parameters, fusing other encryption techniques, and improving embedding methods. Furthermore, hyperchaotic maps with more dimensions can be explored to achieve a greater efficiency.

Conflicts of interest

The authors declare that they have no conflicts of interest.

Author contributions

Haidar Raad Shakir developed the algorithm and codes, Suhad Abbas Yassir wrote the manuscript and prepared the figures. All authors approved the manuscript.

References

[1] M. Zanin and A. N. Pisarchik, “Gray Code Permutation Algorithm for High-Dimensional Data Encryption”, *Information Sciences*, Vol. 270, pp. 288–297, 2014.

[2] Y. Q. Zhang and X. Y. Wang, “A Symmetric Image Encryption Algorithm Based on Mixed Linear–Nonlinear Coupled Map Lattice”, *Information Sciences*, Vol. 273, pp. 329–351, 2014.

[3] B. Wang, Y. Xie, C. Zhou, S. Zhou, and X. Zheng, “Evaluating the Permutation and Diffusion Operations Used in Image Encryption Based on Chaotic Maps”, *Optik*, Vol. 127, No. 7, pp. 3541–3545, 2016.

[4] Q. Xu, K. Sun, S. He, and C. Zhu, “An Effective Image Encryption Algorithm Based on Compressive Sensing and 2D-SLIM”, *Optics and Lasers in Engineering*, Vol. 134, No. January, p. 106178, 2020.

[5] Z. Zhu, Y. Song, W. Zhang, H. Yu, and Y. Zhao, “A Novel Compressive Sensing-Based Framework for Image Compression-Encryption with S-Box”, *Multimedia Tools and Applications*, p. 2020.

[6] S. Ibrahim, H. Alhumyani, M. Masud, et al., “Framework for Efficient Medical Image Encryption Using Dynamic S-Boxes and Chaotic Maps”, *IEEE Access*, Vol. 8, pp. 160433–160449, 2020.

[7] M. Machkour, A. Saaidi, and M. L. Benmaati, “A Novel Image Encryption Algorithm Based on the Two-Dimensional Logistic Map and the Latin Square Image Cipher”, *3D Research*, Vol. 6, No. 4, pp. 1–18, 2015.

[8] A. A. A. E. Latif, B. A. E. Atty, and M. Talha, “Robust Encryption of Quantum Medical Images”, *IEEE Access*, Vol. 6, pp. 1073–1081, 2017.

[9] M. Roy, S. Chakraborty, and K. Mali, *A Chaotic Framework and Its Application in Image Encryption*, 2021.

[10] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, “A New Hybrid Digital Chaotic System with Applications in Image Encryption”, *Signal Processing*, Vol. 160, pp. 45–58, 2019.

[11] W. A. Halang, W. K. S. Tang, H. J. Lee, and J. G. B. Ramírez, “Hybrid-Time Chaotic Encryption and Sender Authentication of Data Packets in Automation Networks”, *IFAC Proceedings Volumes (IFAC-PapersOnline)*, Vol. 42, No. 3, pp. 179–184, 2009.

[12] S. R. Maniyath and T. V, “An Efficient Image Encryption Using Deep Neural Network and Chaotic Map”, *Microprocessors and Microsystems*, Vol. 77, p. 103134, 2020.

[13] S. Saravanan and M. Sivabalakrishnan, “A Hybrid Chaotic Map with Coefficient Improved Whale Optimization-Based Parameter Tuning for Enhanced Image Encryption”, *Soft Computing*, Vol. 25, No. 7, pp. 5299–5322, 2021.

[14] S. Zhou, X. Wang, Y. Zhang, B. Ge, M. Wang, and S. Gao, “A Novel Image Encryption Cryptosystem Based on True Random Numbers

and Chaotic Systems", *Multimedia Systems*, Vol. 28, No. 1, pp. 95–112, 2022.

[15] N. Khalil, A. Sarhan, and M. A. M. Alshewimy, "An Efficient Color / Grayscale Image Encryption Scheme Based on Hybrid Chaotic Maps", *Optics and Laser Technology*, Vol. 143, No. June, p. 107326, 2021.

[16] S. Kumar and R. K. Sharma, "Securing Color Images Using Two-Square Cipher Associated with Arnold Map", *Multimedia Tools and Applications*, Vol. 76, No. 6, pp. 8757–8779, 2017.

[17] F. Budiman, P. N. Andono, and M. Setiadi, "Image Encryption Using Double Layer Chaos with Dynamic Iteration and Rotation Pattern.", *International Journal of Intelligent Engineering & Systems*, Vol. 15, No. 2, p. 2022, doi: 10.22266/ijies2022.0430.06.

[18] H. Wang, D. Xiao, X. Chen, and H. Huang, "Cryptanalysis and Enhancements of Image Encryption Using Combination of the 1D Chaotic Map", *Signal Processing*, Vol. 144, pp. 444–452, 2018.

[19] R. S. Salman, A. K. Farhan, and A. Shakir, "Creation of S-Box Based One-Dimensional Chaotic Logistic Map: Colour Image Encryption Approach", *Int. J. Intell. Eng. Syst*, Vol. 15, No. 5, p. 2022, 2022, doi: 10.22266/ijies2022.1031.33.

[20] D. Zareai, M. Balafar, and M. R. F. Derakhshi, "A New Grayscale Image Encryption Algorithm Composed of Logistic Mapping, Arnold Cat, and Image Blocking", *Multimedia Tools and Applications*, Vol. 80, pp. 18317–18344, 2021.

[21] A. G. Radwan, S. H. A. E. Haleem, and S. K. A. E. Hafiz, "Symmetric Encryption Algorithms Using Chaotic and Non-Chaotic Generators: A Review", *Journal of Advanced Research*, Vol. 7, No. 2, pp. 193–208, 2016.

[22] H. S. E. Sayed, A. Afifi, M. A. A. Zain, and O. S. Faragallah, "An Image Cryptosystem Using Chaotic Baker Map in DFT", In: *Proc. of 2021 International Conference of Women in Data Science at Taif University (WiDSTaif)*, pp. 1–7, IEEE, 2021.

[23] A. Chamoli, J. Ahmed, M. A. Alam, and B. Alankar, "A Diffusion Model Based on the Features of the 3D Chaotic Baker Map for Image Encryption", *International Journal of Intelligent Systems and Applications in Engineering*, Vol. 11, No. 5s, pp. 173–180, 2023.

[24] B. A. E. Atty, M. E. Affendi, and A. A. A. E. Latif, "A Novel Image Cryptosystem Using Gray Code, Quantum Walks, and Henon Map for Cloud Applications", *Complex & Intelligent Systems*, Vol. 9, No. 1, pp. 609–624, 2023.

[25] H. Zhao, S. Xie, J. Zhang, and T. Wu, "A Dynamic Block Image Encryption Using Variable-Length Secret Key and Modified Henon Map", *Optik*, Vol. 230, p. 166307, 2021.

[26] J. Xu, B. Zhao, and Z. Wu, "Research on Color Image Encryption Algorithm Based on Bit-Plane and Chen Chaotic System", *Entropy*, Vol. 24, No. 2, p. 186, 2022.

[27] M. Li, Y. Guo, J. Huang, and Y. Li, "Cryptanalysis of a Chaotic Image Encryption Scheme Based on Permutation-Diffusion Structure", *Signal processing: Image Communication*, Vol. 62, pp. 164–172, 2018.

[28] G. Yi and Z. Cao, "An Algorithm of Image Encryption Based on AES & Rossler Hyperchaotic Modeling", *Mobile Networks and Applications*, pp. 1–9, 2023.

[29] D. S. Laiphrakpam and M. S. Khumanthem, "Cryptanalysis of Symmetric Key Image Encryption Using Chaotic Rossler System", *Optik*, Vol. 135, pp. 200–209, 2017.

[30] W. K. S. Tang and Y. Liu, "Formation of High-Dimensional Chaotic Maps and Their Uses in Cryptography", *Chaos-Based Cryptography: Theory, Algorithms and Applications*, pp. 99–136, Springer, 2011.

[31] J. Wang, W. Yu, J. Wang, Y. Zhao, J. Zhang, and D. Jiang, "A New Six-dimensional Hyperchaotic System and Its Secure Communication Circuit Implementation", *International Journal of Circuit Theory and Applications*, Vol. 47, No. 5, pp. 702–717, 2019.

[32]R. Balamurugan, V. Kamalakannan, G. D. Rahul, and S. Tamilselvan, "Enhancing Security in Text Messages Using Matrix Based Mapping and ElGamal Method in Elliptic Curve Cryptography", In: *Proc. of 2014 International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 103–106, 2014.