International Journal of Safety and Security Engineering
Vol. 13, No. 6, December, 2023, pp. 1127-1134
Journal homepage: http://iieta.org/journals/ijsse

Enhancing Key Exchange Security: Leveraging RSA Protocol in Encryption Algorithm Based on Hyperchaotic System

Hadeel J. Shnaen*, Sadiq A. Mehdi

Computer Science, College of Education, Mustansiriyah University, Baghdad 10052, Iraq

Corresponding Author Email: hadeel.albahadili@gmail.com

https://doi.org/10.18280/ijsse.130616

Received: 24 October 2023
Revised: 29 November 2023
Accepted: 15 December 2023
Available online: 25 December 2023

Keywords:
chaotic system, correlation, decryption, delta feature, encryption, initial conditions, RSA, sensitivity

ABSTRACT

This investigation delineates an innovative approach to fortify the secure key exchange process by integrating the robustness of the RSA algorithm with the unpredictability of a chaotic system, thereby advancing the security framework for color image encryption. Within this scheme, encryption keys are derived from a chaotic system, the initial conditions of which are dynamically modulated by the delta feature extracted from the source image. Such a design ensures that the system's behavior inherently adapts to the input image. The initial values and parameters governing the five-dimensional chaotic system are securely transmitted from sender to recipient via the RSA algorithm. Subsequently, diffusion and confusion processes are orchestrated through the application of two uniquely computed key matrices, which operate on the image at the column and row levels, respectively. This mechanism is instrumental in altering pixel values throughout the image. Performance evaluation of the proposed algorithm is quantified by several metrics: a high Number of Pixels Change Rate (NPCR) value of 99.621% illustrates its efficacy in pixel value modification, while a Peak Signal-to-Noise Ratio (PSNR) value of 8.898 implies the retention of image quality post-encryption. Furthermore, an Unified Average Changing Intensity (UACI) value of 33.823% signifies the algorithm's proficiency in introducing substantial variations in pixel intensities. The results corroborate the algorithm's competency in encrypting color images, underpinning its utility in diverse applications that necessitate stringent data and image protection measures against unauthorized access.

1. INTRODUCTION

Image encryption has emerged as a pivotal tool for the preservation of privacy across various domains, particularly within realms handling sensitive data such as medical imaging or personal photographs [1]. The application of encryption methodologies precludes unauthorized access to visual content, thereby ensuring the integrity of privacy [2, 3]. Cryptographic techniques are broadly categorized into symmetric and asymmetric systems. Symmetric Key Cryptography utilizes a singular key, which is consensually established between the sender and receiver. In contrast, Asymmetric Key Cryptography assigns unique public and private keys to each user [4]. Public keys are disseminated among all conversational participants, whereas private keys remain confidential to the individual user. The encryption process leverages the receiver's public key for message encryption, and the recipient uses their private key for decryption [5]. In the pursuit of heightened data security, researchers have advocated for the use of extensive keys within various cryptographic algorithms. While an enlarged key size is synonymous with fortified data protection, the complexity inherent in key management cannot be overlooked [6]. The RSA algorithm, a cornerstone in public-key cryptography, was introduced to the public domain in 1978 and represents a significant advancement in the field [7]. The fusion of chaotic system-based encryption with the RSA key exchange mechanism harnesses the intrinsic benefits of both systems. Chaotic systems are distinguished by their inherent stochasticity and unpredictability [8], whereas RSA offers a strong cryptographic framework predicated on public-key encryption techniques. By implementing a dual-layered security strategy, the integrity of image transmission and storage is substantially reinforced [9]. Therefore, the proposed research seeks to amalgamate the RSA algorithm with a chaos-based encoding system for color image encryption. The RSA framework, which employs a dual-key system, facilitates secure key exchanges. This integration strives to strike an optimal balance between the efficacy of protection measures and the security of key exchange protocols.

2. RELATED WORKS

In the domain of image encryption, significant strides have been made to enhance the security of visual data. In 2018, a novel encryption system was introduced, leveraging the virtual optical approach of phase-shifted digital holography in conjunction with RSA public key exchange [10]. The encryption keys are composed of multiple parameters, including the wavelength of the laser beam, the focal length of the test lens, the defocusing distance, and a scaling factor. The encryption process is executed by employing a holographic function that incorporates phase shifting, transforming a plaintext image into its encrypted counterpart. The RSA key exchange protocol is then employed to securely transmit cryptographic keys between the communicating parties.

The following year, a groundbreaking image encryption technique was proposed that merges the robust principles of RSA with chaotic maps [9]. This innovative method was designed to handle images of various sizes, initiating the encryption process with a permutation applied via 1D Skew tent maps and 1D Sin maps. This process served to rearrange the pixels of the input image, thereby contributing to the encryption's complexity.

In 2020, the evolution of image encryption methodologies witnessed the introduction of a technique that utilized the RSA algorithm to generate a pair of public and private keys [11]. During the encryption phase, a transformation map generated the initial key, which was derived from the cipher text key. Subsequently, this original key was input into a fractional hyperchaotic system equation to calculate the keystream, further complicating the encryption process and enhancing security.

In the ongoing quest to safeguard visual data, 2021 witnessed the introduction of a public-key image encryption technique predicated on pixel information and the insertion of random numbers [12]. During this process, two prime numbers were randomly selected and, in tandem with the public key, utilized for the synthesis of the private key. The plaintext data were encrypted via the RSA algorithm and subsequently subjected to key transformation mapping. The culmination of this process, involving diffusion and XOR operations, yielded the final encrypted image.

Concurrently, a distinct approach to image encryption was presented, which amalgamated the RSA algorithm with the dynamics of the Lorenz hyperchaotic system [13]. The RSA method was initially employed to generate starting values, which were then iteratively processed to produce the keystream. Additive mode diffusion was applied to alter the grey scale values and pixel locations, with the ultimate goal of dispersing pixel information uniformly across the encrypted image.

Upon comparison, it is evident that the studies of Abbas et al. [9] and Lin and Li [13] closely align with the system proposed herein; however, notable distinctions exist in the deployment of the RSA algorithm, as shown in Table 1. While both approaches integrate RSA within their respective frameworks, the intricacies of key generation and the subsequent encryption processes diverge, reflecting the unique contributions of each methodology to the field of image encryption. These innovations underscore the significance of RSA as a foundational element in the development of secure image encryption systems.

Table 1. Comparison between the proposed system and related works

References	Encryption Method	Key Used	RSA Algorithm Recruitment Site
Proposed	Chaotic mapping system 5D with RSA.	Shared public and private key with chaotic mapping system 5D.	Protect the secure key exchange and transfer of initial values and parameters.
[9]	Chaotic mapping system with RSA.	The shared public and private keys with the chaotic mapping system.	Integrating RSA principles with chaotic maps.
[10]	Virtual optical method with RSA.	Sharing a public and private key with other information such as focal length, laser wavelength, and blur distance.	RSA public key exchange using virtual optical control, and digital holography.
[11]	a hyper-chaotic fractal system with RSA.	Using a transformation map and a chaotic hyper-fractal system with a public and private key.	Image encryption technique using transform map, hyper-chaotic fractal system, and RSA algorithm.
[12]	Use RSA to insert pixel information and random numbers.	Using RSA and key transformation with shared public and private keys.	Image encryption using RSA to insert pixel information and random numbers.
[13]	Lorenz Hyperchaotic System with RSA.	Lorenz Hyperchaotic System with Shared Public and Private Key.	Image encryption technology using Lorenz Hyperchaotic system and RSA algorithm.

3. STRUCTURE OF NEW 5D CHAOTIC SYSTEM

A unique chaotic system based on a 5D framework was used with fourteen positive parameters and complicated, chaotic dynamics features. This system's fundamental attributes and dynamic properties are examined. According to the conclusions of the research, the new system has five Lyapunov exponents, which means that the system shows non-predictive behavior and two unstable equilibrium points. Estimated the values for Kaplan Yorke and maximum positive Lyapunov exponent (MLE) are 3.12204 and 4.45994, respectively, which indicates the complexity of the structure of chaos within the system. The novel system demonstrates unpredictably unstable, highly complicated, and inconsistent features. The acquisition of the innovative five-dimensional autonomous system is accomplished by the following:

$$\begin{aligned}
\frac{dx}{dt} &= ayu - byw + cy - \lambda x\\
\frac{dy}{dt} &= -bxz - exu + fx - gy\\
\frac{dz}{dt} &= h_1xy + kuw - l(z - x)\\
\frac{du}{dt} &= -pw(y + z) - qu - bw\\
\frac{dw}{dt} &= bxy - rzu + t_1u - lw
\end{aligned} \tag{1}$$

where, x, y, z, u, w, and t€R^+ referred to the states of sys a, b, c, λ, e, f, g, h_1, k, l, p, q, r and t_1 are positive system parameters. The chaotic attractor of the 5D system "(1)" is observed when specific values are assigned to the system parameter. a=10, b=2, c=25, λ=40, e=0.5, f=30, g=0.1, h_1=9, k=3, l=4, p=15, q=19, r=.3 and t_1=34 And we assume that X(0)=1, Y(0)=0.5, *Z*(0)=5, *U*(0)=0.6, and *W*(0)=0.4 are the initial circumstances. The result of the Lyapunov exponent is obtained as follows: L_1=4.45994, L_2=0.4620, L_3=-2.75930, L_4=-17.72055, L_5=-48.55465 Intricate and plentiful chaotic behaviors characterize the observed dynamics of this nonlinear system. Figure 1 depicts the 3D representation of the peculiar attractor, which resembles the motion of a butterfly in flight, which shows the chaotic nature and complexity of behavior [14]. The system exhibits complex and rich chaotic properties, and it contributes to understanding the nature of high-dimensional dynamical systems that exhibit chaotic behavior and instability.

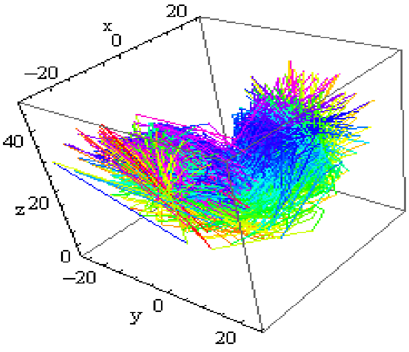


Figure 1. Chaotic attractor three-dimensional view (x-y-z)

It is widely recognized that the waveform of a chaotic system exhibits a lack of periodicity. To establish the chaotic nature of the suggested system, it is necessary to provide evidence [15]. The graphic in Figure 2 illustrates the relationship between time and the state variable as generated from the simulation conducted using the MATHEMATICA software. The time domain representation of x(t) is depicted in Figure 2, illustrating its aperiodic nature.

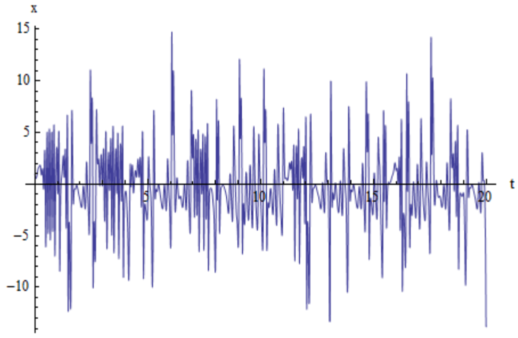


Figure 2. Time versus *x* of the novel chaotic system

4. PROPOSED ENCRYPTION ALGORITHM

An efficient algorithm for securely encrypting color images using a 5D chaotic system is presented. The encryption keys are generated using differences extracted from the original image, which makes them difficult to predict, and enhances the security of the system. RSA technology is used to encode the different feature and initial parameters of the chaotic system during the transmission process. The process of decrypting the parameters is done using the RSA private key derived from the key values (p and q) chosen from the keys generated by the chaotic system. When conducting a set of experiments using different images using standards such as NPCR, UACI, Correlation Coefficient, MSE, PSNR, Information Entropy, and encryption and decryption time, the results showed the strength of the algorithm in achieving effective and secure encryption of color images. Comparing the performance of the proposed algorithm with some other algorithms, the proposed algorithm achieved superior results in many criteria as shown in Figure 3.

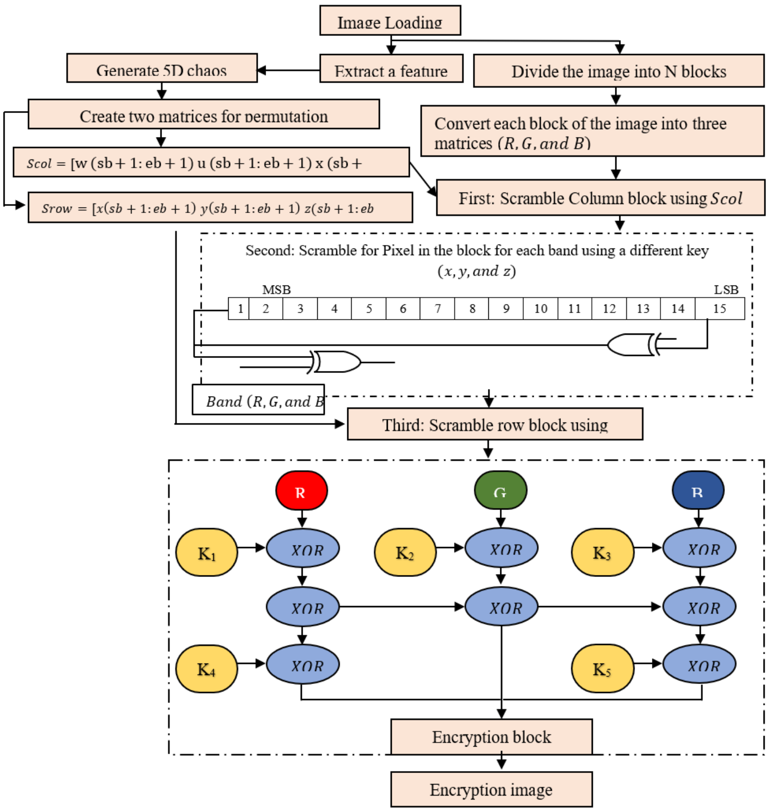


Image Loading
Generate 5D chaos
Extract a feature
Divide the image into N blocks
Create two matrices for permutation
Convert each block of the image into three matrices (*R*, *G*, *and B*)
Scol = [w (sb + 1: eb + 1) u (sb + 1: eb + 1) x (sb +
Srow = [*x*(*sb* + 1: *eb* + 1) *y*(*sb* + 1: *eb* + 1) *z*(*sb* + 1: *eb*
First: Scramble Column block using *Scol*
Second: Scramble for Pixel in the block for each band using a different key (*x*, *y*, *and z*)
MSB
LSB
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Band (*R*, *G*, *and B*
Third: Scramble row block using
R
G
B
K1
K2
K3
K4
K5
XOR
XOR
XOR
XOR
XOR
XOR
XOR
XOR
Encryption block
Encryption image

Figure 3. The diagram of the proposed encryption algorithm

Table 2. The algorithm of the delta feature

```
Algorithm 1. Compute delta feature value
Input: r(row), image
Output: Value of delta E
Begin
Step1: Extract the reference L*a*b* and measured RGB color values
Step 2: Convert the measured RGB colors to the L*a*b* color space
        I_lab=rgb2lab(image);
Step 3: initialize the deltaE variable to 0
        dE=0;
Step 4: iterate over image rows        for i=1: r-1
Step 5: compute deltaE for the entire block of pixels
        block1=I_lab (i: i+1, 1:2, :);
        block2=I_lab (i:i+1, 2:3, :);
        deltaE_block = deltaE (block1, block2);
Step 6: sum up the deltaE values for this block dE = dE + sum(deltaE_block);
Step 7: Normalize the delta features
              fet = mod(sum(dE),256);
End algorithm
```

Table 3. Utilize the computed delta feature value

```
Algorithm 2: Utilization of the computed delta feature value (fet)
        x (1) = initial value x (0) + fet * 0.002
        y (1) = initial value y (0) + fet * 0.002
        z (1) = initial value z (0) + fet * 0.002
        u (1) = initial value u (0) + fet * 0.002
        w (1) = initial value w(0) + fet * 0.002
```

4.1 Compute delta feature value from image

Delta Features refer to the differences between two images or image regions. This can be calculated as the absolute or relative changes in pixel values, color channels, or texture features [16]. Computing the delta feature from an image and using it to change the initial condition in a chaotic system is an interesting approach to generating encryption keys. Chaotic systems are susceptible to initial conditions, so even a small change can lead to significantly different trajectories [14]. This property can be harnessed to create a unique and unpredictable sequence of values, serving as an encryption key. Algorithm 1 describes steps to extract the feature from an image in Table 2. For implementation, see Table 3.

4.2 Chaotic sequence generator

The state values of chaotic systems are often expressed as floating-point integers, and the sequences composed of these state values are not directly applicable in image cryptosystems [13]. In this specific phase, five unordered sequences are generated by employing the initial conditions and attributes linked to the recently established 5-D hyper-chaotic system (1). The mechanism under test is a hyper-chaotic system that generates five sequences (xi, yi, zi, ui, wi) made up of real numbers The given sequences are subsequently converted into five vectors (key1, key2, key3, key4, key5) using the chaotic sequence.

4.3 Encryption image stage

The encryption algorithm employs the exclusive (XOR) operation to generate disorderly sequences within a five-dimensional chaotic environment. The procedure commences by selecting a prominent image, which is subsequently partitioned into blocks of a specified size, denoted as SB. The sequences are created using a confidential key, and the image is partitioned into three vectors (R, G, and B) for every block. The block image undergoes scrambling through the utilization of pseudocode, while the plain image is subjected to encryption via the use of five chaotic sequences formed during step 2. The generation of the encrypted image involves the merging of the red (R), green (G), and blue (B)Components inside each block lead to the creation of the ultimate encrypted image (Table 4).

Table 4. The proposed image encryption algorithm

Algorithm 3: Encryption algorithm	
INPUT	Image, SB (Size Block), the Secret key: The initial conditions, parameters, and iteration for a 5D chaotic system.
OUTPUT	Encrypted Image
BEGIN	
STEP 1	Compute the feature image using Table 1 and Table 2
STEP 2	Iterate the proposed hyperchaotic system with a secret key to create five chaotic sequences [{K1},{K2},{K3},{K4},{K5}] • Using the secret key, initialize the hyperchaotic system with the proposed initial conditions and parameters. • Iterate the system to generate the five chaotic sequences {K1}, {K2}, {K3}, {K4}, and {K5} such that the size of the sequences is greater than or equal to the size of the image.
STEP 3	Divide the Image into Blocks and Create Vectors (R, G, B) • Divide the image into blocks of size SB • Create three vectors, R, G, and B, containing the red, green, and blue pixel values, respectively, for each block.
STEP 4	Scrambled Block Image sb (start block) eb(end block) Create two matrices for rows and column permutation Scramble Column = [w (sb+1: eb+1) u (sb+1: eb+1) x (sb+1: eb+1)]; first stage Scramble Row = [x(sb+1: eb+1) y(sb+1:eb+1) z(sb+1:eb+1)]; third stage Calculate the MSB (most significant bit) as the XOR of the first two bits of the jth element of the x component of the key as seen in Figure 3 second stage
STEP 5	Encrypt plain Image with keys from 5D Hyper-Chaotic System using XOR operation Use the five chaotic sequences {K1}, {K2}, {K3}, {K4}, and {K5} generated in step 2 to encrypt the plain image using the XOR operation
STEP 6	Combine the R, G, and B components for each block into the final encrypted image. Combine the R, G, and B components obtained in step 5 to form the encrypted image.
STEP 7	Output the encrypted image
END	

Table 5. Creates an RSA public/private key

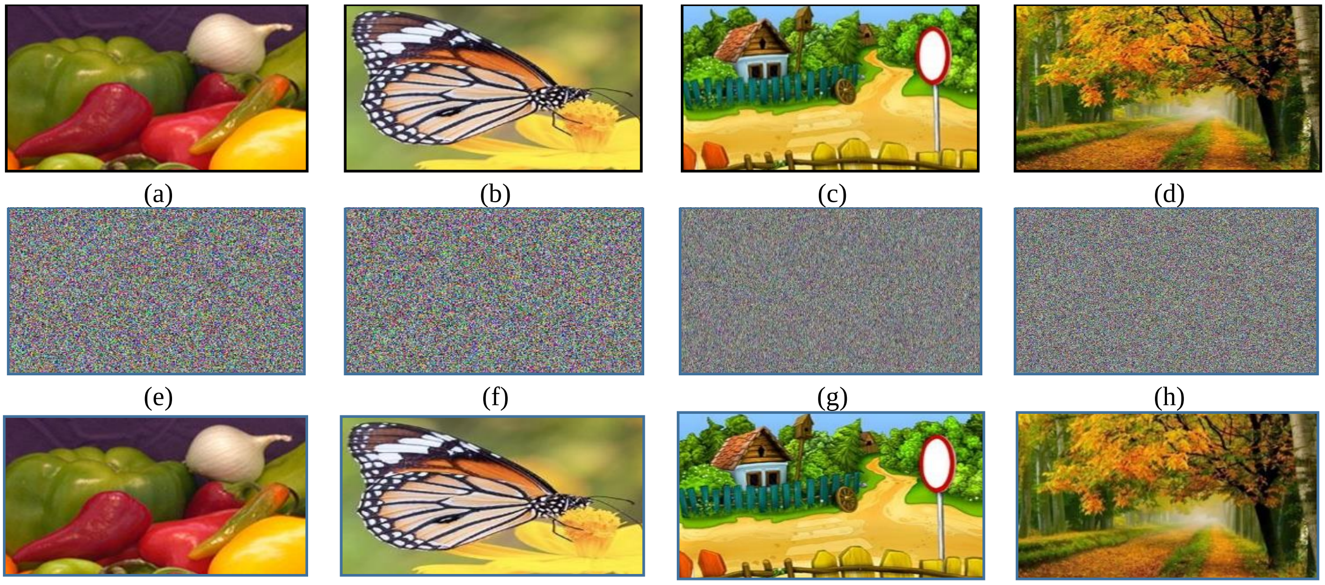
```
Algorithm (4): Generated RSA Key
Input: Initial condition, parameters, delta feature, (x,y,z): chaotic system keys
Ooutput: public &rivate key
begin
            Initialization and Setup:
Step 1          • Set 'n 'to 10 (the number of keys are generated)
                • Create matrix keyt =n X3
                • Compute the nearest integer (key1) by scaling the values in(keyt) to 1000 and take the absolute value.
                • Initialize 'nn' to 0.
            Main Loop to Generate Key Components:
Step 2          • Nested loop checks each value in 'key1' if it is prime using the 'isprime ()' function.
                • TP is a matrix to store the prime number, If the number is not prime, it advances until a prime is discovered.
            Generate RSA Key Components
Step 3          • Select the prime number (p,q)from TP.
                • Euler's totient function is computed 'oy1'.
                • e1 is the public exponent.
                • Calculate the privet key 'd1' by multiplicative inverse of e1 mod oy1
            Storing Key Components
Step4           • Check the 'tt' array, if contains 4 values (p,q,e,d), then the 'nn' counter increases.
                • The 'KDC'matrix stores the array 'tt'.
            Retrieve user input and RSA key components
Step 5          • User interface elements supply strings, which are converted to doubles, np1.
                • Selecting a KDC matrix row with RSA key components p, q, e, and d using np1.
                • Multiple p and q provide RSA modulus nn.
End
```

5. RSA FOR KEY EXCHANGE

This study uses RSA technology to encrypt the delta feature and initial parameters of the chaotic system throughout the transmission process from the transmitter to the receiver. The recipient decrypts the parameters using their RSA key, derived from the prime values (p and q) selected from the keys created by the chaotic system (refer to Table 5). Implementing these steps guarantees the preservation of confidentiality and integrity, hence bolstering the security of color picture encryption.

6. DECRYPTION IMAGE STAGE

The decoding procedure is initiated when RSA is used to transfer the original values and parameters of a five-dimensional chaotic system from the sender to the receiver and then reconstruct it at the receiving end. The system can adapt based on the original image. Decrypting the encrypted image involves using the initial values, delta feature, and keys generated within the decryption process and back XOR operation in reverse order. This process ensures security by incorporating precise details and maintaining the privacy of keys and information shared between the sender and the recipient (Figure 4).


(a) (b) (c) (d)

(e) (f) (g) (h)

(i) (j) (k) (l)

Figure 4. Results of the test images: Plain images of (a) peppers, (b) butterfly, (c) village, (d) autumn landscape. Encrypted images of (e) peppers, (f) butterfly, (g) village, (h) autumn) landscape. Decrypted images of (i) peppers, (j) butterfly, (k) village, (l) autumn landscape

7. EVALUATION AND ASSESSMENT

To assess the credibility and robustness of the method, a series of simulations were conducted utilizing the Matlab platform on the Windows 10 operating system. The chosen sample photos consist of "Peppers" and "Butterfly," both color images measuring 256×256 in size. The images titled "The Village" and "Autumn" have dimensions of 512×512 pixels. Several metrics and criteria are used to evaluate the effectiveness of the encryption method [10]. As shown in Table 6, reviewing the most common metrics.

7.1 Histogram analysis

A histogram is employed as a visual representation to illustrate pixel intensity distribution within an image. An encrypted image that meets the ideal conditions has a consistent frequency distribution, which means that potential attackers can't use it to learn anything useful about statistics. The histogram distribution of photos before and after encryption is depicted in Figure 5 [15].

7.2 The experiment results of the proposed system

As shown in Table 7, the NPCR value means that the attacker will have difficulty distinguishing patterns between the images and the encrypted images. The ideal UACI value would be close to 33.823%, a positive result indicating effective encryption. The correlation coefficient values indicate a very weak linear relationship, which is a positive result for the coding. A higher PSNR value indicates better image quality because the decoded image closely matches the original image. An ideal encryption process should result in maximum entropy, which indicates that the image is highly random and difficult to predict. The value of entropy 7.6981 indicates good randomness. Execution times are important to evaluate the efficiency of an algorithm, especially in real-time or resource-constrained applications.

Table 6. Image encryption evaluation procedure

Metric	Characterizations	Equations	Outline
Number of Changing Pixel Rate (NPCR), Unified Averaged Changed Intensity (UACI) [17].	The NPCR technique, with an ideal range of 0-1, is highly suitable for encryption, while an ideal UACI value of 34 is recommended for a 512×512-pixel image.	$NPCR = \frac{\sum_{i,j} I(i,j)}{M\times H} \times 100\%$ $\mathrm{UACI} = \frac{1}{\mathrm{M}\times\mathrm{H}}\left[\frac{\sum_{\mathrm{i,j}} \mathrm{D(i,j)} - \mathrm{D(\acute{i},j)}}{255}\right] \times 100\%$ D and D’ are encrypted images before and after a single pixel change, with L representing the maximum supported value and T representing the total number of pixels.	An NPCR value of 0.9 and a UACI value of approximately 0.33 are essential.
Correlation Coefficient (CC)[14]	defines the connection between original and encoded image pixels. The analysis includes horizontal, diagonal, and vertical components. CC scale can be negative or positive.	$cc = \frac{\sum_{im}\sum_{jn}(AA_{ijn} - \overline{AA})(BB_{mij-}\overline{BB})}{\sqrt{(\sum_{im}\sum_{jn}(AA_{ijn} - \overline{AA})^2(\sum_{im}\sum_{j}(BB_{ijn} - B\bar{B})^2)}}$ where, *A* and *B* are matrices of comparable dimensions, where (Ā=mean(A), B̄=mean(B)).	The cross-correlation (CC) value for an encrypted image is expected to be almost equal to zero.
Mean Squared Error (MSE)[8]	Validating error values that distinguish encrypted and plain images The MSE range is 0 to ∞.	$\mathrm{MSE} = \frac{1}{\mathrm{M}\times\mathrm{N}}\sum_{\mathrm{i=0}}^{\mathrm{m-1}}\sum_{\mathrm{j=0}}^{\mathrm{n-1}}[\mathrm{A(i,j)} - \mathrm{B(i.j)}]^2$ where, *A* and *B* are the encrypted and unencrypted images. In a m×n image size, pixels with coordinates (i, j)	Images with a low (MSE) are often regarded as superior quality.
Peak Signal to Noise Ratio (PSNR)[7]	compare the quality of plain images with their encrypted counterparts. The Range of (PSNR) is quantified in decibels (dB) and spans from zero to infinity (∞).	$\mathrm{PSNR} = \frac{10 \times \log_{10}(2XX - 1)^2}{MSE}$ where, *X* is the number of bits allocated per pixel.	PSNR between original and decrypted images must be high.
Information Entropy (IE)[14]	It's the average data per image pixel. Pixels have different values. IE 0 TO +8.	$H(m) = -\sum_{i=0}^{N-1} P(m_i)log[P(m_i)]$ *H*(*m*) is the entropy of a message m, where p(m$_i$) is the probability of the symbol appearing.	The IE value for an 8-bit image should be closer to 8.
Execution Time (ET) [18]	It defines image-encryption time. Sum of compile and run times. Measurements are ms, secs, and minutes.	---------	ET should affect the encryption scheme value less.

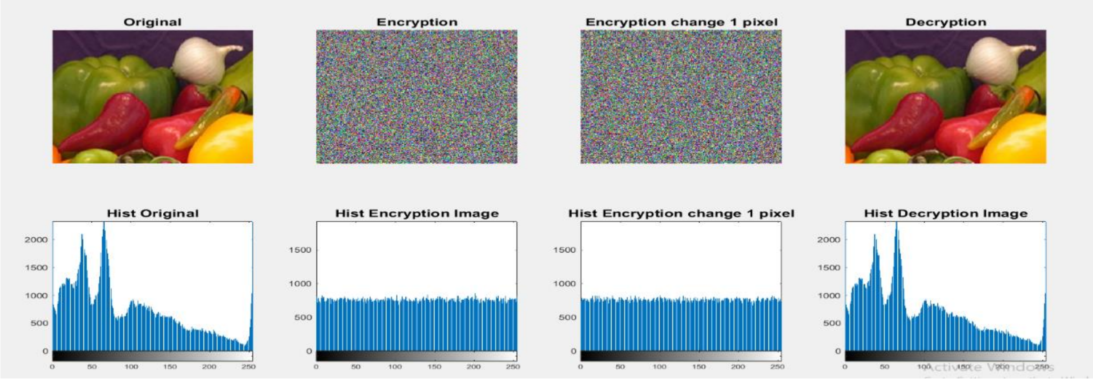


Figure 5. The histogram for the original and encryption image using the proposed algorithm

Table 7. The experiment results of the proposed system

Images Metrics		Peppers	Butterfly	Village	Autumn
NPCR		99.617	99.5911	99.5977	99.6202
UACI		% 33.82	% 32.323	% 34.9335	% 33.6567
Correlation Coefficient		0.00532	-0.0014	0.0014	-0.0013
(MSE)	**Encryption**	8651.05	7555.80	9273.46	8394.69
	Decryption	0	0	0	0
(PSNR)	**Encryption**	8.7601	8.0566	8.4584	8.8908
	Decryption	∞	∞	∞	∞
Information Entropy	**Original**	7.6981	7.8353	7.8307	7.6681
	Encryption	7.9991	7.9990	7.9998	7.9997
	Decryption	7.6981	7.8353	7.8307	7.6681
Execution Time	**Key generate**	0.380580	0.34499	0.93776	0.90332
	Encryption	0.52734	0.52772	2.16187	2.02593
	Decryption	0.52288	0.53269	2.21767	2.09913

Table 8. A comparison between the proposed study and other systems

Ref. Metrics	Proposed	Ref. [7]	Ref. [19]
NPCR	99.621	100%	99.706
UACI	% 33.65	% 38.14	33.461
Correlation Coefficient	0.0014	0.367	0.0075
PSNR	8.8908	-41.27	8.0132
Information Entropy	7.9998	2.747	7.9974

Table 9. Comparison of the proposed system with other systems for Lena (256×256) and (512×512)

Metrics	Lena 256×256			Lena 512×512		
	Propose	Ref. [20]	Ref. [21]	Propose	Ref. [20]	Ref. [21]
NPCR	99.615	99.6114	99.766	99.611	99.608	99.7470
UACI	31.452	33.4954	36.7148	31.352	33.4558	36.7368
CC	0.0011	0.0072	0.0029	0.0011	0.0028	0.0015
IE	7.9993	7.9974	7.9955	7.9998	7.9993	7.9989
PSNR	8.6251	/	36.3461	8.6262	/	35.3924

To correctly identify and quantify these leverage points, it's critical to undertake a comprehensive examination and comparison of the proposed encryption method and current systems, as shown in Tables 8 and 9. Several comparison criteria could be employed depending on the objectives and specifications of the encryption system and the environment in which it will be utilized. Additionally, a thorough evaluation of security, performance, and other pertinent variables should be used to determine the best encryption method.

8. CONCLUSIONS

The results of the image encryption algorithm presented in this paper demonstrate its effectiveness in providing secure and dynamic color image encryption. The algorithm leverages a five-dimensional chaotic system with tested features such as unpredictability and sensitivity to initial values, supported by a positive Lyapunov exponential. Key generation dynamically adapts based on delta feature values extracted from the original image, enhancing the system's security. The high NPCR value of 99.621 indicates that the encryption algorithm induces significant changes in pixel values between the original and encrypted images. This is a positive sign of the algorithm's ability to perturb the image data effectively. An ideal UACI value of 33.823% suggests that the encryption algorithm introduces substantial changes in pixel intensities, reinforcing that it effectively obfuscates the image content. A low correlation coefficient value of 0.00532 between the original and encrypted images indicates a minimal similarity, further confirming the algorithm's ability to obscure the original content. The increase in information entropy from the original to the encrypted image (7.6981 to 7.9991) signifies that our encryption algorithm introduces a high level of randomness and unpredictability into the data, a desirable characteristic in encryption. However, the decrypted image also has an entropy value of 7.6981, which indicates the decryption. process effectively restores the original information content, as the entropy value returns to a level similar to that of the original image. Regarding execution time, we observed the following values (in seconds): Key Generation: 0.38058, Encryption: 0.52734, and Decryption: 0.52288. These execution time results indicate that our encryption algorithm is efficient and practical for real-world applications. essential for secure communication. Encryption and decryption times are also reasonably quick, making the algorithm suitable for use in scenarios where real-time or near-real-time processing is required.

ACKNOWLEDGMENT

This effort was made possible with assistance from Mustansiriyah University.

REFERENCES

[1] Yousif, N.A., Mahdi, G.S., Hashim, A.T. (2022). Medical image encryption based on frequency domain and chaotic map. International Journal of Safety and Security Engineering, 12(4): 467-473. https://doi.org/10.18280/ijsse.120407

[2] Sumathy, S., Kumar, B.U. (2010). Secure key exchange and encryption mechanism for group communication in wireless ad hoc networks. arXiv preprint arXiv:1003.3564. https://doi.org/10.5121/jgraphhoc.2010.2102

[3] Sahoo, A., Mohanty, P., Sethi, P.C. (2022). Image encryption using RSA algorithm. Lecture Notes in Networks and Systems, 431: 641-652. https://doi.org/10.1007/978-981-19-0901-6_56

[4] Hussain, S.M., Al-Bahadili, H., Al-Bahadili, H. (2016). A DNA-based cryptographic key generation algorithm master thesis view project using mobile learning to evaluate success factors of mobile learning view project a DNA-based cryptographic key generation algorithm. https://www.researchgate.net/publication/308366247.

[5] Somkunwar, R.K., Nawghare, S., Shaikh, Z. (2023). A novel approach for ticket generation and validation using RSA and Keccak algorithms. Revue d'Intelligence Artificielle, 37(3): 761–772. https://doi.org/10.18280/ria.370325

[6] Mahdi, M.H., Abdulrazzaq, A.A., Mohd Rahim, M.S., Taha, M.S., Khalid, H.N., Lafta, S.A. (2019). Improvement of image steganography scheme based on LSB value with two control random parameters and multi-level encryption. IOP Conference Series: Materials Science and Engineering, 518(5): 052002. https://doi.org/10.1088/1757-899X/518/5/052002

[7] Jaswanth, P.V., Reddy, B.R., Kumar, M.S.P., Priyadarsini, M.J.P. (2020). Color image encryption using AES and RSA. International Journal of Engineering and Advanced Technology, 9(5): 547–550. https://doi.org/10.35940/ijeat.E9648.069520

[8] Shakir, H.R., Mehdi, S.A.A., Hattab, A.A. (2022). Chaotic-DNA system for efficient image encryption. Bulletin of Electrical Engineering and Informatics, 11(5): 2645-2656. https://doi.org/10.11591/eei.v11i5.3886

[9] Abbas, E.A., Karam, T.A., Abbas, A.K. (2019). Image cipher system based on RSA and chaotic maps. Eurasian Journal of Mathematical and Computer Applications, 7(4): 4-17. https://doi.org/10.32523/2306-6172-2019-7-4-4-17

[10] Chatterjee, A., Dhanotia, J., Bhatia, V., Prakash, S. (2018). Virtual optical encryption using phase shifted digital holography and RSA algorithm. In 2018 3rd International Conference on Microwave and Photonics (ICMAP), pp. 1-2. https://doi.org/10.1109/ICMAP.2018.8354560

[11] Ye, G., Jiao, K., Wu, H., Pan, C., Huang, X. (2020). An asymmetric image encryption algorithm based on a fractional-order chaotic system and the RSA public-key cryptosystem. International Journal of Bifurcation and Chaos, 30(15): 2050233. https://doi.org/10.1142/S0218127420502338

[12] Wu, H., Zhu, H., Ye, G. (2021). Public key image encryption algorithm based on pixel information and random number insertion. Physica Scripta, 96(10): 105202. https://doi.org/10.1088/1402-4896/ac0bcf

[13] Lin, R., Li, S. (2021). An image encryption scheme based on lorenz hyperchaotic system and RSA algorithm. Security and Communication Networks, 2021: 5586959. https://doi.org/10.1155/2021/5586959

[14] Ahmed, S.S., Mehdi, S.A. (2022). Image encryption algorithm based on a novel 5D chaotic system. In 2022 8th International Conference on Contemporary Information Technology and Mathematics (ICCITM), pp. 249-255. https://doi.org/10.1109/ICCITM56309.2022.10031883

[15] Jasem, N.N., Mehdi, S.A. (2023). Multiple random keys for image encryption based on sensitivity of a new 6D chaotic system. International Journal of Intelligent Engineering and Systems, 16(5): 576-585. https://doi.org/10.22266/ijies2023.1031.49

[16] Fave, X., Zhang, L., Yang, J., Mackin, D., Balter, P., Gomez, D., Followill, D., Jones, A. K., Stingo, F., Liao, Z., Mohan, R., Court, L. (2017). Delta-radiomics features for the prediction of patient outcomes in non-small cell lung cancer. Scientific Reports, 7(1): 588. https://doi.org/10.1038/s41598-017-00665-z

[17] Saidi, R., Cherrid, N., Bentahar, T., Mayache, H., Bentahar, A. (2020). Number of pixel change rate and unified average changing intensity for sensitivity analysis of encrypted inSAR interferogram. Ingenierie Des Systemes d'Information, 25(5): 601-607. https://doi.org/10.18280/ISI.250507

[18] Petrenko, K., Mashatan, A., Shirazi, F. (2019). Assessing the quantum-resistant cryptographic agility of routing and switching IT network infrastructure in a large-size financial organization. Journal of Information Security and Applications, 46: 151-163. https://doi.org/10.1016/j.jisa.2019.03.007

[19] Mehdi, S.A., Jabbar, K.K., Abbood, F.H. (2018). Image encryption based on the novel 5D hyper-chaotic system via improved AES algorithm. International Journal of Civil Engineering and Technology, 9(10): 1841-1855.

[20] Jasim, O.A., Hussein, K.A. (2021). A hyper-chaotic system and adaptive substitution box (S-Box) for image encryption. In 2021 International Conference on Advanced Computer Applications (ACA), pp. 144-149. https://doi.org/10.1109/ACA52198.2021.9626793

[21] Setyaningsih, E., Wardoyo, R., Sari, A.K. (2020). Securing color image transmission using compression-encryption model with dynamic key generator and efficient symmetric key distribution. Digital Communications and Networks, 6(4): 486-503. https://doi.org/10.1016/j.dcan.2020.02.001