Journal of King Saud University – Computer and Information Sciences 35 (2023) 238–248

HOSTED BY

ELSEVIER

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

An image encryption scheme based on a seven-dimensional hyperchaotic system and Pascal's matrix

Ammar Ali Neamah

Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq

ARTICLE INFO

Article history:
Received 27 September 2022
Revised 13 February 2023
Accepted 14 February 2023
Available online 17 February 2023

Keywords:
Image encryption
Hyperchaotic system
Pascal's matrix
Security

ABSTRACT

The transmission of an excessive number of images between users via the Internet and other communication media necessitates the use of effective techniques to protect the images from unauthorized usage. Encryption is one of the most effective methods for protecting both images and data. This paper presents a new grayscale image encryption method that integrates a seven-dimensional hyperchaotic system with Pascal's matrix. The algorithm used the hyperchaotic system to first confuse the original image before diffusing the permuted image using Pascal's matrix. To assess the image encryption performance, the suggested algorithm used histogram, correlation coefficient, differential attack, information entropy, and noise attack. Simulation results indicate that the suggested algorithm has a high level of security and is resistant to a variety of attacks.

1. Introduction

Rapid advances in network communications in recent years have led to high demand for the secure transmission of images over the Internet and other networks. Protecting images, particularly medical and military images, is critical in light of the increasing frequency of harmful cyber-attacks. Therefore, securing the content of images has become a critical matter.

Image watermarking, image steganography, and image encryption are all common methods for protecting images' content. Image encryption techniques are the most efficient means of ensuring image security since it converts the original image into an unreadable one utilizing a private key. Recently, various image encryption techniques based on chaotic maps have been introduced to increase image security. Chaotic maps are important in cryptography because they create arbitrary numbers that are used as encryption keys. These maps are mostly classified as one-dimensional and higher-dimensional chaotic maps. Many of these techniques rely on two fundamental stages. Confusion is the initial stage that relies on changing the position of pixels. The following stage is diffusion in which the pixels values are changed.

Many techniques for digital image encryption were proposed by researchers such as chaotic-based (Wang and Lingfeng, 2022; Wang et al., 2019; Ye et al., 2020; Hua et al., 2019; Xu et al., 2022; Lyle et al., 2022; Zheng and Zeng, 2022; Almalkawi et al., 2019; Alghamdi et al., 2022), elliptic curve-based (Hayat et al., 2022; Banik et al., 2019; Laiphrakpam and Khumanthem, 2018), Cellular automata-based (Mondal et al., 2019; Zhang et al., 2019; Li et al., 2022; Ping et al., 2022), DNA (Wu et al., 2018; Nematzadeh et al., 2020; Uddin et al., 2021; Wang and Du, 2022), and compressive sensing (Gong et al., 2019; Zhang et al., 2018; Ye et al., 2022; Shi et al., 2021). Yu et al. (Yu et al., 2020) suggested an image encryption technique that relies on a hyperchaotic system and a short-time fractional Fourier transform. However, the method cannot efficiently retrieve the images when the ciphered image is attacked with statistical attacks. Luo et al. (Luo et al., 2020) suggested a new image encryption technique that combines a hyper-chaotic system with quantum coding. The classic image data is mapped to the quantum state, ensuring that this image is extracted accurately. But this technique is still in the study stage due to a lack of quantum hardware. Wu et al. (Wu et al., 2016) developed a color image encryption method merging a six-dimensional hyperchaotic system and a two-dimensional discrete wavelet transform to achieve a better encryption result. However, this technique increases the cost of data storage and transmission. Chai et al. (Chai et al., 2016) used a four-dimensional memristive

Peer review under responsibility of King Saud University.

ELSEVIER Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2023.02.014
1319-1578/© 2023 The Author. Published by Elsevier B.V. on behalf of King Saud University.

hyperchaotic map with genetic recombination in image encryption. The map's sensitivity to the initial key and complicated dynamical behavior makes it a suitable choice for image encryption. Despite having a high level of security, the image encryption algorithm's temporal complexity is large. Tsafack et al. (Tsafack et al., 2020) developed a four-dimensional chaotic circuit and used it to encrypt images. This approach provides a large keyspace but is vulnerable to noise assaults. Hosny et al. (Hosny et al., 2021) designed a new image encryption technique that depends on Fibonacci Q-matrix and a six-dimensional hyperchaotic system. This technique effectively withstands differential assaults but require a long time to process. Lu et al. (Lu et al., 2021) suggested utilizing a 4D conservative hyperchaotic system to create a chaotic sequence as secret keys, combining it with image DNA encoding to encrypt the plain images. The approach is highly secure; however, the speed of DNA encoding operation has to be improved. Kaur et al. (Kaur et al., 2022) designed a new image encryption technique that based on a dual local search-based evolutionary algorithm to use to adjust the initial values of an improved 7D hyperchaotic system to creat large private keys. However, the authors concentrated only on the encryption process and paid less attention to computational complexity.

Hyperchaotic approaches are utilized to overcome the limitations of low-dimension chaotic systems. These methods perform better than the low ones in terms of nonlinearity, randomness, unpredictability, and created key sequences, which have a big keyspace. In general, the level of security can be increased by the use of hyper-chaotic systems. Seven-dimensional hyperchaotic systems have a complex structure and multiple parameters, which provides better dynamic behavior as compared to the 4,5, and 6D systems. These 7D systems can be used in secure communications due to their complicated dynamic behavior. These characteristics allow these systems to outperform low dimension systems' drawbacks. There are some drawbacks to related works, such as low keyspace, encryption methods that cannot retrieve the original image when the ciphered image is attacked with a salt and pepper noise attack, and failure to withstand differential and statistical attacks. These weaknesses motivated us to suggest a novel method for encrypting images. To secure the content of digital images, this work offers an image encryption technique based on Pascal's matrix and seven-dimensional hyperchaotic system. This combination not only efficiently removes the correlation between nearby pixels in the ciphered image, but also increases the degree of randomness and uncertainty for encrypted images. In other words, the correlations between neighboring pixels in an image and their pixel values are simultaneously cracked. Thus, our approach will further increase resistance to differential and statistical assaults and reduce the processing time. This combination can also achieve the best results compared with other approaches if using a symmetric Pascal matrix of order 4.

The following is a summary of this paper's contributions:

- The first use to combine a seven-dimensional hyperchaotic system with Pascal's matrix in image encryption.
- Integration of Pascal's matrix and the seven-dimensional hyperchaotic system provides a high level of security.
- A seven-dimensional hyperchaotic system is employed to produce the private key needed for scrambling the original image, with the initial conditions (initial key values) of the system dependent on the original image.
- The size of the key of the suggested algorithm is big enough to resist brute-force attacks.
- The suggested approach for image encryption is extremely resistant to most attacks.
- The experimental findings and algorithm evaluations show that the proposed method efficiently encrypts grayscale images with excellent performance.

The remainder of the article is structured as follows: The preliminaries of this study are introduced in Section 2. The third section primarily describes the proposed technique and lists the detailed steps. Section 4 includes various analysis in addition to the simulated experiments. Section 5 provides the security evaluation and results. Section 6 concludes with a summary of the entire work.

2. Preliminaries

This section explains two key tools that are the foundation of our proposed approach. The first tool is a symmetric Pascal matrix, which is defined. Following that, a seven-dimensional hyperchaotic system is described.

2.1. Symmetric Pascal matrix

Consider the square $n \times n$ matrix $P(n)$ with entries

$$P_{i,j} = \binom{i+j}{i} = \frac{(i+j)!}{i!j!},\ 0 \le i,j < n. \tag{1}$$

We call $P(n)$ the symmetric Pascal matrix of order n. The coefficients of $P(n)$ satisfy the following recurrence relation (Bacher and Chapman, 2004)

$$p_{i,j} = p_{i-1,j} + p_{i,j-1} \tag{2}$$

The first four matrices of Pascal (Zhang et al., 2022), for example, are

$$P(1) = [1],\ P(2) = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix},\ P(3) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 3 & 6 \end{bmatrix},\ P(4) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 6 & 10 \\ 1 & 4 & 10 & 20 \end{bmatrix}. \tag{3}$$

The inverse of these matrices can be found. For instance,

$$P^{-1}(4) = \begin{bmatrix} 4 & -6 & 4 & -1 \\ -6 & 14 & -11 & 3 \\ 4 & -11 & 10 & -3 \\ -1 & 3 & -3 & 1 \end{bmatrix}. \tag{4}$$

In this paper, we are interested in the symmetric Pascal matrix of order 4 and its inverse. This matrix will utilize to change image pixel values in the diffusion stage because it has a simple structure, fast, and capable of diffusing scrambled images. These features can fulfill image encryption requirements. Thus, this matrix can protect image content effectively and safely when used for encryption and decryption purposes.

2.2. Seven-Dimensional hyperchaotic system

M. Varan, A. Akgul (Zhang et al., 2022) defined the seven-dimensional hyperchaotic system as:

$$\begin{aligned}
\dot{x_1} &= -ax_1 + ax_5 - bx_5x_6x_7, \\
\dot{x_2} &= -cx_2 - dx_6 + x_1x_6x_7, \\
\dot{x_3} &= -ax_3 + ax_5 - gx_1x_2x_7, \\
\dot{x_4} &= -ax_4 + ex_1 + x_1x_2x_3, \\
\dot{x_5} &= -ax_5 + ex_7 - x_2x_3x_4, \\
\dot{x_6} &= -ex_6 + ex_5 + x_3x_4x_5, \\
\dot{x_7} &= -bx_7 + fx_2 - hx_4x_5x_6,
\end{aligned} \tag{5}$$

where a, b, c, d, e, f, g, h are the system parameters; $x_1, x_2, x_3, x_4, x_5, x_6, x_7$ are the state variables of this system. In this system, the chosen parameters values are $a = 15$, $b = 5$, $c = 0.5$, $d = 25$, $e = 10$, $f = 4$, $g = 0.1$, and $h = 1.5$ (Trejo-Guerra et al., 2013). The parameter d represents the control parameter, with the other values remaining constant. The bifurcation diagram of the seven-dimensional hyperchaotic system with respect to $d \in [7.6, 27.4]$ is given in Fig. 1. When $d \in (23.8, 24)$, the system (5) has a chaotic behavior with two positive Lyapunov exponents (Varan and Akgul, 2018).

3. The proposed algorithm

This section outlines the major steps of the suggested technique for protecting grayscale images. The input image is encrypted and turned into a noise image in the first stage. The decryption phase is then used to retrieve the original image. Fig. 2 illustrates a diagram of the proposed image encryption and decryption algorithm.

3.1. The process of encryption

The steps for image encryption are as follows:

Step1: import the grayscale image G.

Step2: convert G to vector V.

Step3: compute the hyperchaotic system's initial key values

$$x_1 = \frac{\sum_{i=1}^{MN} V(i) + MN}{2^{23} + MN} \tag{6}$$

$$x_i = \mathrm{mod}\left(10^7 x_{i-1}, 1\right),\ i = 2, 3, 4, 5, 6, 7 \tag{7}$$

where mod(•) represents the modulus after division and MN denotes the image vector V's length.

Step4: generate the sequence S by iterating the seven-dimensional hyperchaotic system and choosing the sequences (x_1, x_2, and x_7).

Step5: sort S in ascending order and then return the positions of the sorted pixels in vector SS.

Step6: compute the permuted vector $B = V(SS)$.

Step7: reshape the vector B into matrix D with size MN.

Step8: split the matrix D into submatrices of order 4.

Step9: get matrix E by multiplying each submatrix with the Pascal matrix of order 4 as follows:

$$\begin{bmatrix} E_{i,j} & E_{i,j+1} & E_{i,j+2} & E_{i,j+3} \\ E_{i+1,j} & E_{i+1,j+1} & E_{i+1,j+2} & E_{i+1,j+3} \\ E_{i+2,j} & E_{i+2,j+1} & E_{i+2,j+2} & E_{i+2,j+3} \\ E_{i+3,j} & E_{i+3,j+1} & E_{i+3,j+2} & E_{i+3,j+3} \end{bmatrix} = \begin{bmatrix} D_{i,j} & D_{i,j+1} & D_{i,j+2} & D_{i,j+3} \\ D_{i+1,j} & D_{i+1,j+1} & D_{i+1,j+2} & D_{i+1,j+3} \\ D_{i+2,j} & D_{i+2,j+1} & D_{i+2,j+2} & D_{i+2,j+3} \\ D_{i+3,j} & D_{i+3,j+1} & D_{i+3,j+2} & D_{i+3,j+3} \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 6 & 10 \\ 1 & 4 & 10 & 20 \end{bmatrix} \mathrm{mod}\, 256, \tag{8}$$

$i = 1 : 4 : M,\ j = 1 : 4 : N$

Step10: obtain the ciphered image E by using two rounds of the encryption process.

In order to get better encryption results, only two rounds of scrambling and diffusion processes is enough to modify the positions and remove the correlations between neighboring pixels in the encrypted image.

3.2. The process of decryption

The steps for image decryption are as follows:

Step1: The ciphered image E is split into sub-matrices of order 4, and then the following equation is used for the sub-matrices of the image by multiplying each sub-matrix with the inverse of the Pascal matrix:

$$\begin{bmatrix} D_{i,j} & D_{i,j+1} & D_{i,j+2} & D_{i,j+3} \\ D_{i+1,j} & D_{i+1,j+1} & D_{i+1,j+2} & D_{i+1,j+3} \\ D_{i+2,j} & D_{i+2,j+1} & D_{i+2,j+2} & D_{i+2,j+3} \\ D_{i+3,j} & D_{i+3,j+1} & D_{i+3,j+2} & D_{i+3,j+3} \end{bmatrix} = \begin{bmatrix} E_{i,j} & E_{i,j+1} & E_{i,j+2} & E_{i,j+3} \\ E_{i+1,j} & E_{i+1,j+1} & E_{i+1,j+2} & E_{i+1,j+3} \\ E_{i+2,j} & E_{i+2,j+1} & E_{i+2,j+2} & E_{i+2,j+3} \\ E_{i+3,j} & E_{i+3,j+1} & E_{i+3,j+2} & E_{i+3,j+3} \end{bmatrix} \begin{bmatrix} 4 & -6 & 4 & -1 \\ -6 & 14 & -11 & 3 \\ 4 & -11 & 10 & -3 \\ -1 & 3 & -3 & 1 \end{bmatrix} \mathrm{mod}\, 256, \tag{9}$$

$i = 1 : 4 : M,\ j = 1 : 4 : N$

Step2: The image D attained from the earlier phase is turned into vector U.

Step3: The following calculation uses the vector S created during the encryption phase to return the pixels to their original positions:

$$O(S_k) = U_k,\ k = 1 : MN \tag{10}$$

Step4: Convert O's vector into matrix to attain the deciphered image G'.

Step5: To attain the deciphered image, a twice decryption process is required.

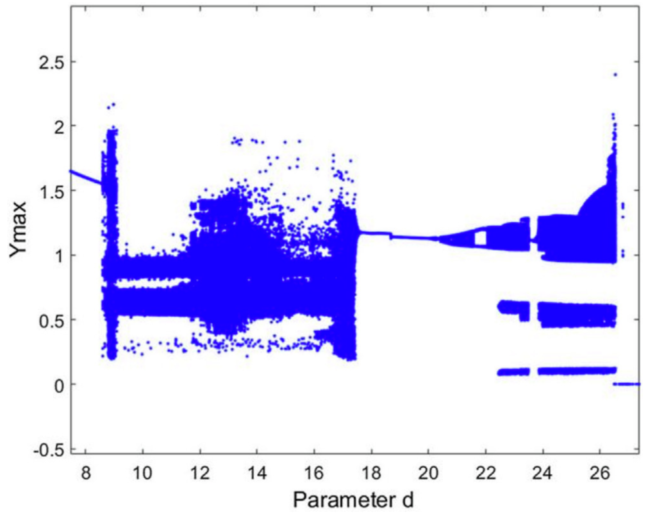

Fig. 1. Bifurcation diagram of system (5) with (a, b, c, e, f, g, h) = (15, 5, 0.5, 10, 4, 0.1, 1.5) and $d \in [7.6, 27.4]$.

4. Simulation results

4.1. Experiment platform

To demonstrate the encryption and decryption capabilities of our technique, we used a laptop computer with an Intel i7-1065G7 processor running at 1.30 GHz and memory of 8 GB. The algorithm described above was executed in a program written in MATLAB (R2018A).

4.2. Experiment results

Different sorts of experiments have been presented in this section to examine and validate the suggested method's performance. In these experiments, the effectiveness of the suggested method was evaluated using various typical grayscale images (Airplane,

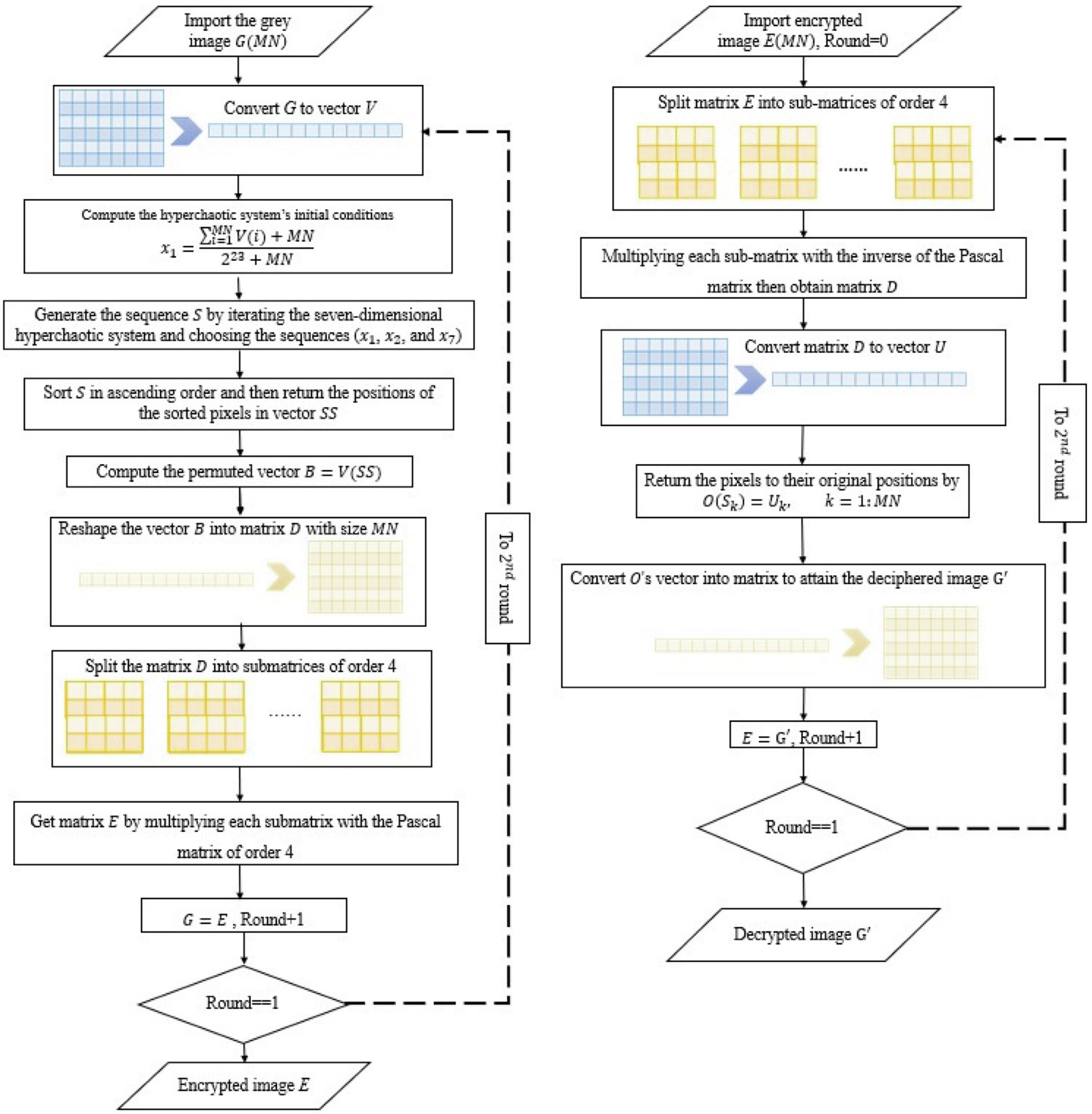
Import the grey image $G(MN)$
Convert G to vector V
Compute the hyperchaotic system's initial conditions
$x_1 = \frac{\sum_{i=1}^{MN} V(i) + MN}{2^{23} + MN}$
Generate the sequence S by iterating the seven-dimensional hyperchaotic system and choosing the sequences (x_1, x_2, and x_7)
Sort S in ascending order and then return the positions of the sorted pixels in vector SS
Compute the permuted vector $B = V(SS)$
Reshape the vector B into matrix D with size MN
Split the matrix D into submatrices of order 4
......
Get matrix E by multiplying each submatrix with the Pascal matrix of order 4
$G = E$, Round+1
Round==1
Encrypted image E
To 2^{nd} round
Import encrypted image $E(MN)$, Round=0
Split matrix E into sub-matrices of order 4
......
Multiplying each sub-matrix with the inverse of the Pascal matrix then obtain matrix D
Convert matrix D to vector U
Return the pixels to their original positions by $O(S_k) = U_k$, $k = 1{:}MN$
Convert O's vector into matrix to attain the deciphered image G′
E = G′, Round+1
Round==1
Decrypted image G′
To 2^{nd} round

Fig. 2. The encryption and decryption flowchart of the proposed algorithm.

Baboon, Boat, and Peppers) with sizes of 512 × 512 and 256 × 256. These images can be found in SIPI datasets (USC-SIPI Image Database, 2022). The plain images of size 512 × 512, corresponding encrypted images, and decrypted images are shown in Fig. 3.

5. Security Analysis

This section describes several well-known measures that are commonly used to assess new algorithms' security. To evaluate the performance and security aspects of the proposed algorithm, we give some analysis of the implemented method below. The speed of the proposed algorithm is also addressed in the last subsection.

5.1. Keyspace analysis

The size of the key matters in the encryption process. This key must be sufficiently large to resist brute force attacks. In the suggested encryption algorithm, the private key is created by the values a, b, c, d, e, f, g, h, x_1, x_2, x_3, x_4, x_5, x_6, x_7 and N_0 of the 7D hyperchaotic system. If we consider the estimation precision of the initial value equals 10^{16}, hence the total private key is $N_0 \times 10^{240}$, which is big enough to resist brute-force attacks.

5.2. Key sensitivity

A well-designed encryption method has to be highly sensitive to any small change in initial conditions of the used private key. When this key is slightly altered, the restored image becomes noisy and unintelligible. For this purpose, we decrypted the Boat image by modifying x_1 in the initial conditions tox_1 + 0.0000001; the results are shown in Fig. 4c. The correct private key will only recover the original image, as shown in Fig. 4d. Boat's plain and cyphered images are shown in Fig. 4a,b.

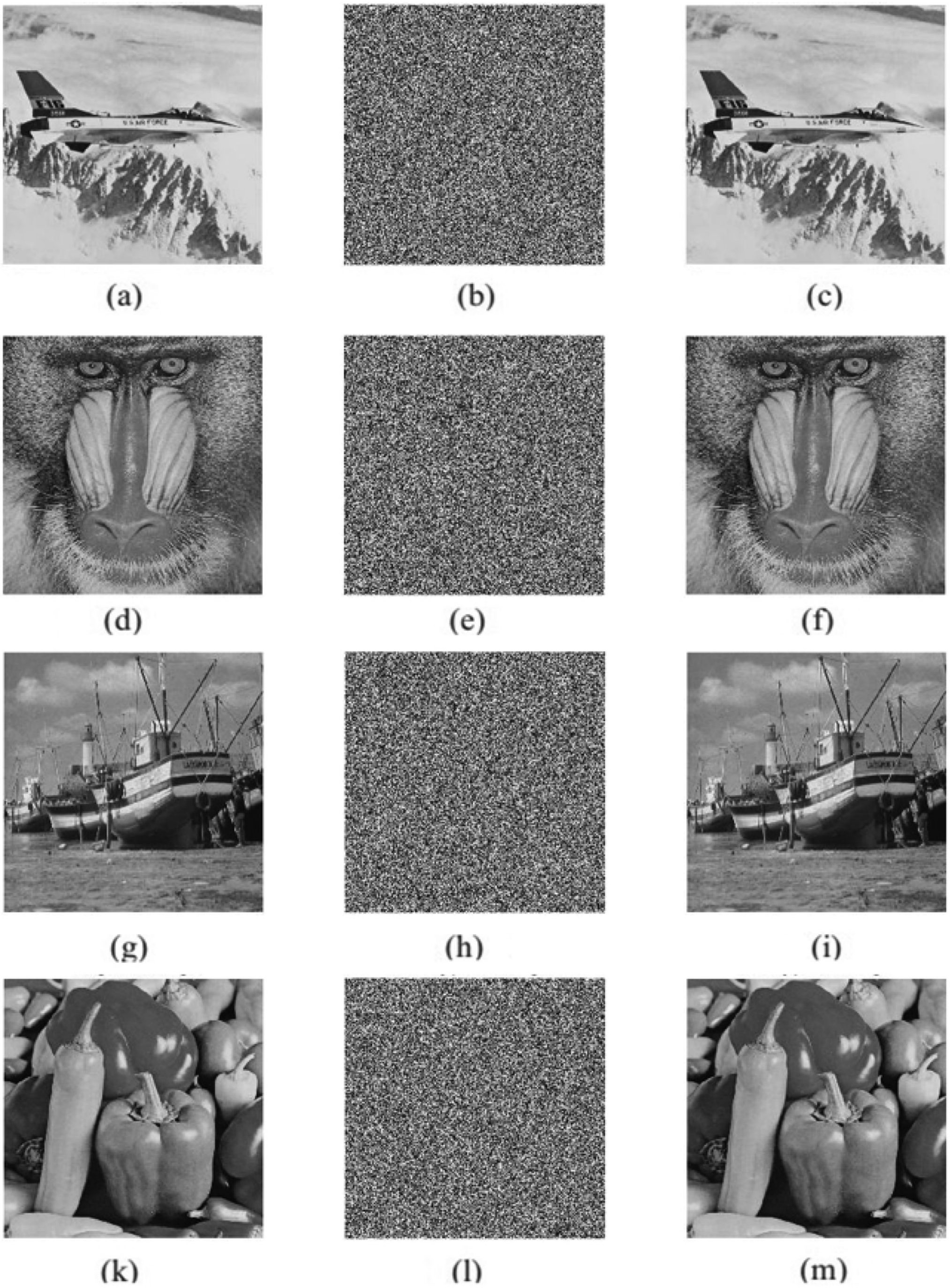

Fig. 3. (a), (d), (g) and (k) Plain images; (b), (e), (h) and (l) The corresponding encrypted images; (c),(f),(i) and (m) The decrypted images.

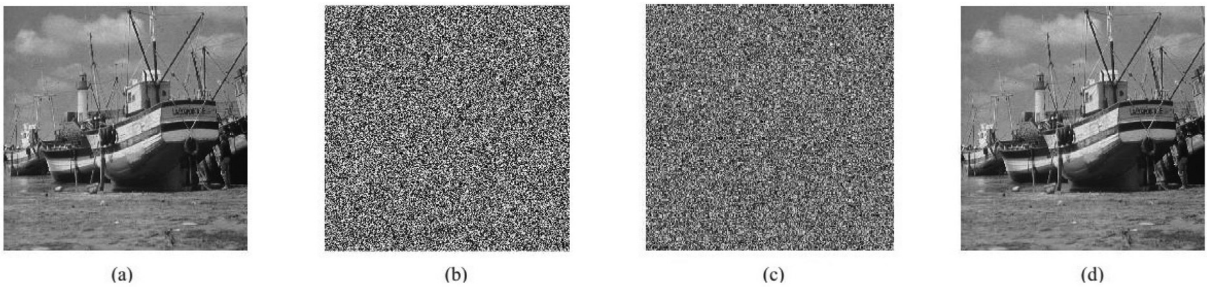

Fig. 4. (a) Plain image. (b) Encrypted image with the actual key. (c) Decrypted image of (b) with the modifed key. (d) Decrypted image of (b) with the actual key.

5.3. Histogram analysis

An image's histogram shows the frequency of each pixel value. If the histogram of the ciphered image is uniformly distributed, the cryptographic scheme can efficiently resist statistical attacks. Fig. 5 shows histogram plots for the original images and the encrypted images used in the simulation. The proposed method produces scrambled images with a desirable uniform distribution of pixels.

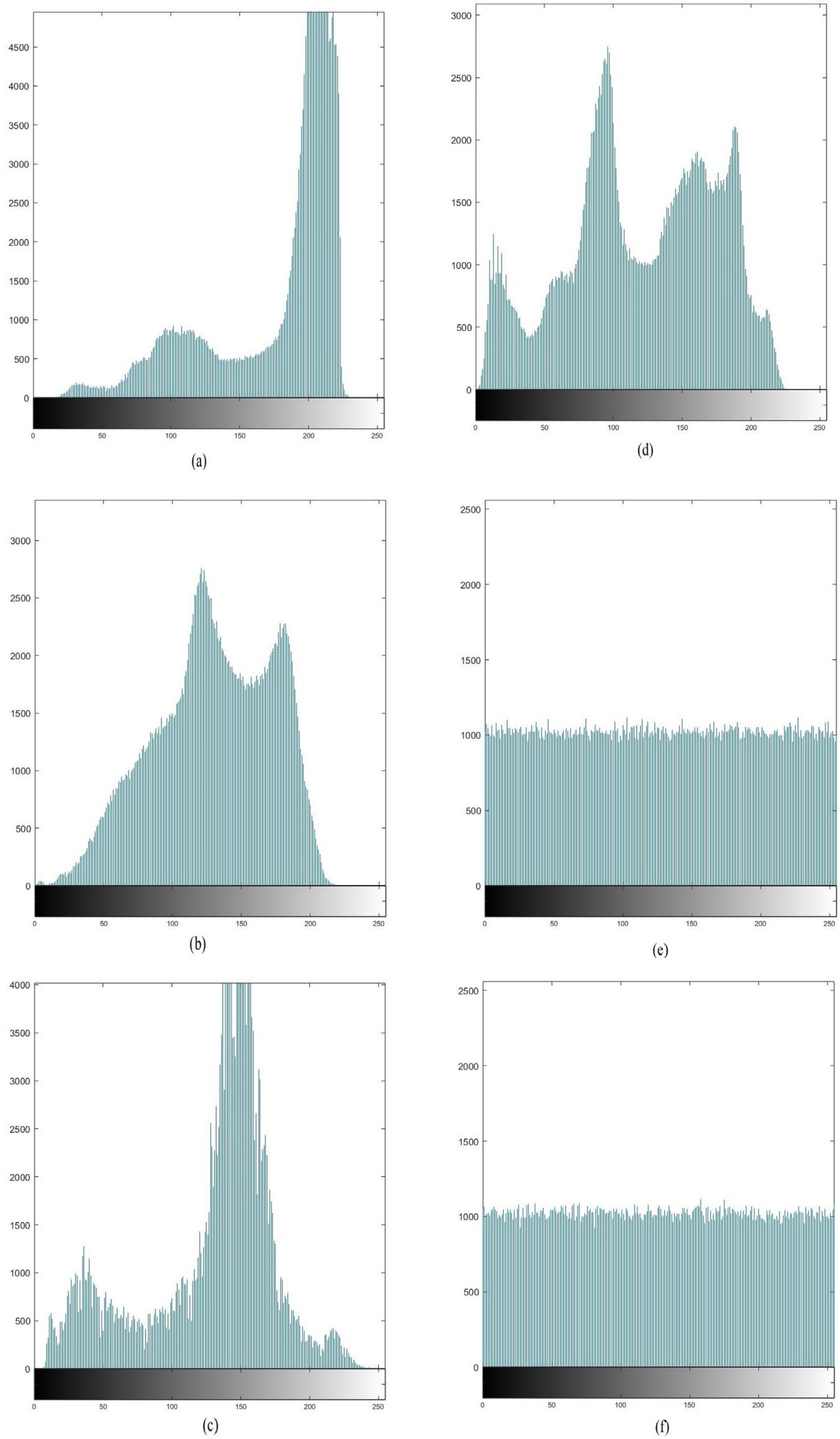

Fig. 5. Histograms of the plain and encrypted images: (a), (b), (c), and (d) The plain images histograms in Fig. 3a,d,g,k, respectively; (e), (f), (g), and (h) The encrypted images histograms in Fig. 3b,e,h,l, respectively.

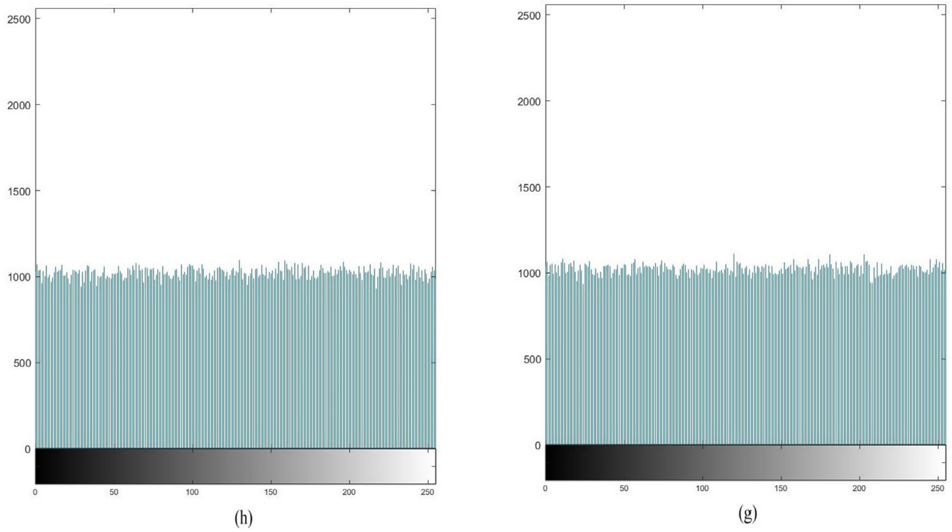

Fig. 5 (*continued*)

Fig. 5a,b,c,d illustrates the plain images histograms in Fig. 3a,d,g,k, and Fig. 5e,f,g,h depicts the encrypted images histograms in Fig. 3b, e,h,l, respectively.

The chi-square test is used as a measure for determining a histogram's uniformity (Andono and Setiadi, 2022). It is mathematically expressed as:

$$\chi^2 = \sum_{i=1}^{256} \frac{(\mathrm{V}_i - F)^2}{F}, \tag{11}$$

where V_i is the observed occurrence frequency of the i-th gray level and F represents the expected occurrence frequency of each gray level $\left(F = \frac{V}{255}\right)$. Assuming a 0.05 significance level, $\chi^2(255.05)$ = 293.2478. If the value of χ^2 is less than 293, encrypted image's histogram is confirmed to be uniform (Setiadi et al., 2022). Table 1 shows the chi-square test results that are less than 293. These findings validate the new algorithm's efficiency. Thus, the suggested method is more resistant to statistical assaults.

5.4. Correlation coefficient analysis

One of the most important characteristics in the field of image encryption is the correlation between any two adjacent pixels. Pixels in a plain image have high correlation coefficients with their neighbors. To reduce the possibility of attacks, the correlation between neighboring pixels of a cipher image must be highly close to zero. The vertical, horizontal, and diagonal correlation between each pair of pixels, x and y, can be computed by

$$R_{x,y} = \frac{cov(x,y)}{\sqrt{D(x)} \times \sqrt{D(y)}}, \tag{12}$$

where $cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y - E(y_i))$, $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$, $E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i$ and N is the total number of pixels involved in the calculations. Table 1 illustrates the computed correlation coefficients for ciphered images using our method. The proposed encryption technique's average coefficient correlations are very near zero. The findings in this study indicate that the proposed technique can efficiently remove the correlation between nearby pixels in the ciphered image while protecting the original image's content. Table 2 shows the correlation between the vertical, horizontal, and diagonal directions of the Airplane, Baboon, Boat and Peppers images before and after encryption. The proposed method, compared with previous methods (Hua et al., 2019; Wu et al., 2018; Luo et al., 2020; Hosny et al., 2021), and (Kaur et al., 2022), has better results.

Table 1
The values of chi-square test.

Size	Airplane	Baboon	Boat	Peppers
256 × 256	248.9688	270.5781	253.0859	260.3359
512 × 512	260.5436	259.7125	255.1092	243.2378

5.5. Differential attack analysis

The cryptanalysts' purpose in this attack is to crack the cipher images without needing the key by identifying the connection between the ciphered and original images. As a result, minor pixel changes in the plain images have a substantial influence on the ciphered image, making it more challenging for cryptanalysts to break the ciphered images. The Unified Average Changing Intensity (UACI) and Number of Pixels Change Rate (NPCR) are used to assess the ability to access the differential attack. The values for UACI and NPCR are computed as follows:

$$\mathrm{UACI} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|C_2(i,j) - C_1(i,j)|}{255 \times M \times N} \times 100\%, \tag{13}$$

$$\mathrm{NPCR} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}h(i,j)}{M \times N} \times 100\%, \tag{14}$$

where $C_2(i,j)$ and $C_1(i,j)$ are the cipher images formed by two plain images that differ by only one pixel, and $h(i,j)$ is defined by

$$h(i,j) = \begin{cases} 0, & if\ C_2(i,j) = C_1(i,j) \\ 1, & if\ C_2(i,j) \neq C_1(i,j). \end{cases} \tag{15}$$

To ensure the algorithm's security, the UACI value of the image cryptographic algorithms must be larger than 0.33 and the NPCR value must be greater than 0.99. For cryptographic algorithm validation, Table 3 presents the average UACI and NPCR values of images tested. It can be seen that the suggested approach is extremely sensitive to even little changes in the plain-image. The findings show that the suggested technique can successfully withstand differential assaults.

Table 2
Correlation coefficient values.

Images	Size	Directions	Correlation for Plain Image	Proposed Algorithm	Hua et al. (Hua et al., 2019)	Wu et al. (Wu et al., 2018)	Luo et al. (Luo et al., 2020)	Hosny et al. (Hosny et al., 2021)
Airplane	512 × 512	V	0.9641	– 0.0013	0.0089	0.0050	– 0.0040	0.0196
		H	0.9663	– 0.0004	0.0154	0.0025	0.0055	0.0296
		D	0.9370	– 0.0020	0.0031	0.0012	0.0080	0.0260
Baboon	512 × 512	V	0.7587	0.0035	0.0251	0.0033	0.0012	0.0040
		H	0.8665	– 0.0006	0.0132	0.0029	– 0.0023	0.0251
		D	0.7262	0.0030	0.0040	0.0062	– 0.0015	0.0231
Boat	512 × 512	V	0.9713	0.0034	0.0330	0.0034	0.0003	0.0011
		H	0.9381	– 0.0011	0.0003	0.0003	0.0072	0.0041
		D	0.9222	0.0001	0.0214	0.0011	0.0005	0.0113
Peppers	512 × 512	V	0.9792	– 0.0013	0.0038	0.0038	0.0028	0.0077
		H	0.9768	0.0001	0.0010	0.0006	0.0089	0.0044
		D	0.9639	0.0018	0.0006	0.0010	0.0023	0.0067
Airplane	256 × 256	V	0.9302	0.0036	0.0014	0.0041	0.0034	0.0103
		H	0.9364	0.0040	0.0055	0.0028	0.0040	0.0229
		D	0.8819	0.0032	0.0083	0.0010	0.0018	0.0100
Baboon	256 × 256	V	0.8261	0.0005	0.0005	0.0009	0.0021	0.0337
		H	0.8736	– 0.0040	0.0113	0.0026	– 0.0019	0.0065
		D	0.7843	0.0015	0.0136	0.0052	– 0.0038	0.0244
Boat	256 × 256	V	0.9452	0.0007	0.0181	0.0031	0.0011	0.0093
		H	0.9268	0.0047	0.0014	0.0001	0.0072	0.0138
		D	0.8833	0.0007	0.0066	0.0015	– 0.0017	0.000003
Peppers	256 × 256	V	0.9703	0.0084	0.0165	0.0059	0.0045	0.0129
		H	0.9633	– 0.0038	0.196	0.0016	0.0054	0.0211
		D	0.9362	– 0.0017	0.0210	0.0034	– 0.0038	0.0013

5.6. Information entropy

Information entropy test measures the degree of randomness and uncertainty in an image. It is defined as usual by

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i)\log\frac{1}{p(m_i)}, \tag{16}$$

where N denotes the number of bits for each symbol m_i, $p(m_i)$ represents the probability of m_i. The perfect entropy value of an encrypted image is eight. In this work, the entropy of tested images is listed in Table 4, in which the entropy of encrypted images is highly near to the ideal value of eight. This indicates that there may not even be any information leaking within the technique. As a result, the suggested method may survive entropy assaults. Our approach performs the best in terms of information entropy when compared to earlier techniques (Hua et al., 2019; Wu et al., 2018; Luo et al., 2020; Hosny et al., 2021; Kaur et al., 2022). Hence, the proposed algorithm is resistant to statistical attacks.

5.7. Salt and Pepper noise attack

Encrypted Images are susceptible to noise or interference when transferred through physical communications channels. Therefore, the cipher encryption technique must be resilient enough to decipher the ciphered images despite the accumulation of noise. The difference between the original image and the ciphered image is measured using the peak signal-to-noise ratio (PSNR). It can be calculated by

$$\mathrm{PSNR} = 10\,log_{10}\left(\frac{max^2}{\mathrm{MSE}}\right), \tag{17}$$

where max is the grayscale's maximum scale value of 8 bits and MSE is formally defined by

$$\mathrm{MSE} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(O(i,j) - D(i,j))^2, \tag{18}$$

where $O(i,j)$ is the original image and $D(i,j)$is the decipher image (Setiadi, 2021).

The proposed technique is resistant to "salt and peppers" noise of a density of 0.001, with average PSNR values of 26.97db. When the noise level was raised to 0.002 and 0.005, the average dropped to 23.96db and 20.2db. Table 5 shows the PSNR for the tested images of dimension 512 × 512 after being attacked by noise.

Fig. 6 shows the decrypted results when the encrypted Boat image is disrupted by Salt and Pepper noise at densities of 0.001, 0.002, 0.005, respectively. The decrypted findings are all identifiable, as illustrated in Fig. 6. This indicates that noisy encryption of data is acceptable. According to Fig. 6, the suggested system can withstand noise assault.

Table 3
Differential Attack test.

Images	Size	Proposed Algorithm		Hua et al. (Hua et al., 2019)		Wu et al. (Wu et al., 2018)		Luo et al. (Luo et al., 2020)		Hosny et al. (Hosny et al., 2021)	
		UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR
Airplane	512 × 512	0.3341	0.9960	0.3343	0.9961	0.3357	0.9962	0.3340	0.9961	0.3345	0.9960
Baboon	512 × 512	0.3345	0.9960	0.3352	0.9959	0.3352	0.9959	0.3347	0.9958	0.3347	0.9960
Boat	512 × 512	0.3350	0.9962	0.3347	0.9960	0.3358	0.9961	0.3349	0.9962	0.3346	0.9961
Peppers	512 × 512	0.3345	0.9960	0.3355	0.9961	0.3352	0.9961	0.3350	0.9960	0.3340	0.9958
Airplane	256 × 256	0.3351	0.9961	0.3346	0.9962	0.3363	0.9962	0.3351	0.9953	0.3350	0.9960
Baboon	256 × 256	0.3335	0.9958	0.3345	0.9963	0.3338	0.9959	0.3350	0.9958	0.3346	0.9959
Boat	256 × 256	0.3340	0.9961	0.3336	0.9956	0.3366	0.9961	0.3345	0.9942	0.3341	0.9941
Peppers	256 × 256	0.3342	0.9958	0.3368	0.9962	0.3349	0.9960	0.3347	0.9960	0.3342	0.9942

Table 4
The values of entropy with sizes 512 × 512 and 256 × 256 for the scheme and other schemes.

Images	Size	Proposed Algorithm	Hua et al. (Hua et al., 2019)	Wu et al. (Wu et al., 2018)	Luo et al. (Luo et al., 2020)	Hosny et al. (Hosny et al., 2021)
Airplane	512 × 512	7.9993	7.9993	7.9992	7.9991	7.9993
Baboon	512 × 512	7.9993	7.9991	7.9992	7.9992	7.9992
Boat	512 × 512	7.9994	7.9993	7.9994	7.9992	7.9992
Peppers	512 × 512	7.9993	7.9993	7.9993	7.9993	7.9992
Airplane	256 × 256	7.9976	7.9971	7.9970	7.9975	7.9972
Baboon	256 × 256	7.9973	7.9974	7.9971	7.9974	7.9973
Boat	256 × 256	7.9975	7.9974	7.9971	7.9974	7.9976
Peppers	256 × 256	7.9974	7.9971	7.9974	7.9973	7.9970

Table 5
The values of PSNR for noise attack.

Images	Airplane	Baboon	Boat	Peppers
Salt and Pepper noise (0.001)	25.7422	27.5560	27.4344	27.1557
Salt and Pepper noise (0.002)	23.1938	24.4331	24.0149	24.2025
Salt and Pepper noise (0.005)	19.4081	20.9707	20.4745	19.9845

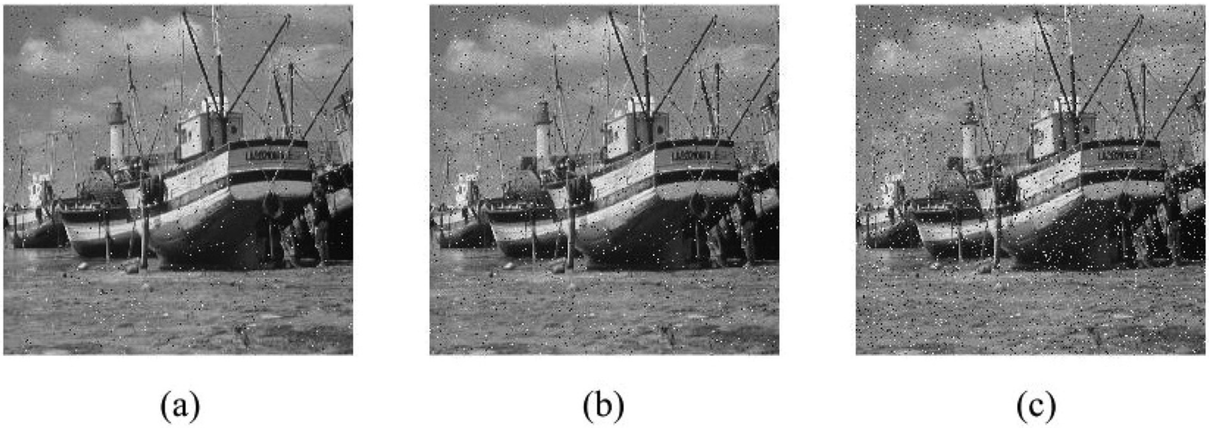

Fig. 6. Decrypted data from a salt and pepper noise attack with densities of (a) 0.001, (b) 0.002, and (c) 0.005.

Table 6
The values of MAE of images encrypted by the proposed algorithm.

Images	Airplane	Baboon	Boat	Peppers	Airplane	Baboon	Boat	Peppers
Size	512 × 512	512 × 512	512 × 512	512 × 512	256 × 256	256 × 256	256 × 256	256 × 256
MAE	87.3422	86.6811	87.4284	84.0717	87.3638	85.5810	87.3023	84.0655

5.8. Mean absolute error (MAE)

MAE test measures the statistical difference between the encrypted image $C(i,j)$ and the original image $O(i,j)$. It is mathematically defined by

$$\mathrm{MAE} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}|O(i,j) - C(i,j)| \tag{19}$$

The higher the MAE is, the more increased the security of proposed cryptographic system. Table 6 shows the MAE for the tested images with sizes of 512 × 512 and 256 × 256.

5.9. Gray level Co-Occurrence matrix (GLCM) analysis

It is a method of analyzing the texture of an image, measuring the frequency with which different combinations of gray levels in a given spatial relationship appear in a given area of an image or throughout the entire image. The normalized GLCM can be used to derive metrics like those for contrast, energy and homogeneity.

In contrast analysis, higher contrast levels reflect the degree of unpredictability in the ciphertext image that increases security. The following equation is used to determine the intensity of contrast between a pixel and all of its neighboring pixels over the entire image:

$$C_n = \sum_{i,j}|i - j|^2 p(i,j), \tag{20}$$

where $p(i,j)$ represents the gray-level co-occurrence matrices in GLCM.

Another metric that can be computed using the GLCM is energy. The energy analysis in this situation measures squared components and is mathematically expressed as:

$$E_n = \sum_{i,j} p(i,j)^2, \tag{21}$$

Table 7
Analysis of plain and encrypted images.

Images	Size	Properties	Plain Images	Encrypted Images
Airplane	512 × 512	C_n	0.2121	10.4977
		E_n	0.3808	0.0156
		H_n	0.9287	0.3894
Baboon	512 × 512	C_n	0.6178	10.4866
		E_n	0.0890	0.0156
		H_n	0.7873	0.3894
Boat	512 × 512	C_n	0.3800	10.5250
		E_n	0.1890	0.0156
		H_n	0.8753	0.3887
Peppers	512 × 512	C_n	0.2561	10.4773
		E_n	0.1107	0.0156
		H_n	0.8989	0.3890
Airplane	256 × 256	C_n	0.3222	10.4587
		E_n	0.3604	0.0156
		H_n	0.9071	0.3904
Baboon	256 × 256	C_n	0.5133	10.4644
		E_n	0.1030	0.0156
		H_n	0.8018	0.3896
Boat	256 × 256	C_n	0.3966	10.4860
		E_n	0.2023	0.0156
		H_n	0.8813	0.3891
Peppers	256 × 256	C_n	0.3004	10.4838
		E_n	0.1133	0.0156
		H_n	0.9004	0.3870

Table 8
Required time (seconds) for encrypting and decrypting images.

Images	Size	Encryption time	Decryption time
Airplane	512 × 512	0.710758 *sec.*	0.128318 *sec.*
Baboon	512 × 512	0.684918 *sec.*	0.135599 *sec.*
Boat	512 × 512	0.707523 *sec.*	0.137447 *sec.*
Peppers	512 × 512	0.688577 *sec.*	0.122551 *sec.*
Airplane	256 × 256	0.253159 *sec.*	0.037650 *sec.*
Baboon	256 × 256	0.250984 *sec.*	0.034726 *sec.*
Boat	256 × 256	0.259434 *sec.*	0.035883 *sec.*
Peppers	256 × 256	0.253761 *sec.*	0.034905 *sec.*

where $p(i,j)$ signifes the overall number of gray-level co-occurrence matrices.

Homogeneity analysis can measure the closeness of gray-level co-occurrence matrices (GLCM) elements in this system. The encryption technique is better if the homogeneity values are as small as possible. It can be computed as follows:

$$H_n = \sum_{i,j} \frac{p(i,j)}{1+|i-j|}, \tag{22}$$

where $p(i,j)$ represents the gray-level co-occurrence matrices in GLCM. Table 7 demonstrates that the suggested system has larger contrast values and smaller homogeneity values than the other schemes in (Alghamdi et al., 2022), indicating that it is more secure.

5.10. Speed test

When developing a robust image encryption method, running speed is just as crucial as security concerns. Our algorithm is run on the Airplane, Baboon, Boat, and Peppers images with sizes of 512 × 512 and 256 × 256. Table 8 outlines the required times for the encryption and decryption process.

6. Conclusions

In this work, we suggested a novel grayscale image encryption technique. Pascal's matrix of order 4 is combined with a seven-dimensional hyperchaotic system in this technique. We initially employed a seven-dimensional hyperchaotic system to produce random sequences, and then we chose three of these sequences to modify the position of the pixel. The diffused grayscale image is split into a set of 4 × 4 sub-blocks, and Pascal's matrix is utilized to change the values of pixels for each sub-block. To boost security, twice, confusion and diffusion processes are implemented. The proposed technique's security and robustness testing revealed high sensitivity to any pixel or key change and robustness in facing all frequent attacks. In this article, we used the novel approach to grayscale images, and in future work, the suggested technology will be studied to be utilized for RGB images.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Alghamdi, Y., Munir, A., Ahmad, J., 2022. A Lightweight Image Encryption Algorithm Based on Chaotic Map and Random Substitution. Entropy 24 (10), 1344. https://doi.org/10.3390/e24101344.

Almalkawi, I.T., Halloush, R., Alsarhan, A., Al-Dubai, A., Al-karaki, J.N., 2019. A lightweight and efficient digital image encryption using hybrid chaotic systems for wireless network applications. J. Inf. Secur. Appl. 49. https://doi.org/10.1016/j.jisa.2019.102384.

Andono, P.N., Setiadi, D.R.I.M., 2022. Improved Pixel and Bit Confusion-Diffusion Based on Mixed Chaos and Hash Operation for Image Encryption. IEEE Access 10, 115143–115156. https://doi.org/10.1109/ACCESS.2022.3218886.

Bacher, R., Chapman, R., 2004. Symmetric Pascal matrices modulo p. European Journal of Combinatorics. 25 (4), 459–473. https://doi.org/10.1016/j.ejc.2003.06.001.

Banik, A., Shamsi, Z., Laiphrakpam, D.S., 2019. An encryption scheme for securing multiple medical images. Journal of Information Security and Applications 49. https://doi.org/10.1016/j.jisa.2019.102398.

Chai, X.-L., Gan, Z.-H., Lu, Y., Zhang, M.-H., Chen, Y.-R., 2016. A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system. Chinese Physics B 25 (10). Article ID 100503.

Gong, L., Qiu, K., Deng, C., Zhou, N., 2019. An image compression and encryption algorithm based on chaotic system and compressive sensing. Optics & Laser Technology 115, 257–267. https://doi.org/10.1016/j.optlastec.2019.01.039.

Hayat, U., Ullah, I., Azam, N.A., Azhar, S., 2022. A Novel Image Encryption Scheme Based on Elliptic Curves over Finite Rings. Entropy 24 (5), 1–24. https://doi.org/10.3390/e24050571.

Hosny, K.M., Kamal, S.T., Darwish, M.M., Papakostas, G.A., 2021. New image encryption algorithm using hyperchaotic system and fibonacci Q-matrix. Electronics 10 (9), 1066. https://doi.org/10.3390/electronics10091066.

Hua, Z., Zhou, Y., Huang, H., 2019. Cosine-transform-based chaotic system for image encryption. Inf. Sci. 480, 403–419. https://doi.org/10.1016/j.ins.2018.12.048.

Kaur, M., Singh, D., Kumar, V., 2022. Improved seven-dimensional (i7D) hyperchaotic map-based image encryption techniquem. Soft Computing 26 (6), 2689–2698. https://doi.org/10.1007/s00500-021-06423-8.

Laiphrakpam, D.S., Khumanthem, M.S., 2018. A robust image encryption scheme based on chaotic system and elliptic curve over finite field. Multimedia Tools and Applications 77 (7), 8629–8652. https://doi.org/10.1007/s11042-017-4755-1.

Li, L., Luo, Y., Qiu, S., Ouyang, X., Cao, L., Tang, S., 2022. Image encryption using chaotic map and cellular automata. Multimed. Tools and Applications, 1–19. https://doi.org/10.1007/s11042-022-12621-9.

Lu, Q., Yu, L.L., Zhu, C.X., 2021. A New conservative hyperchaotic system-based image symmetric encryption scheme with DNA coding. Symmetry 13 (12). https://doi.org/10.3390/sym13122317.

Luo, Y., Tang, S., Liu, J., Cao, L., Qiu, S., 2020. Image encryption scheme by combining the hyper-chaotic system with quantum coding. Optics and Lasers in Engineering 124. https://doi.org/10.1016/j.optlaseng.2019.105836.

Lyle, M.M., Sarosh, P., Parah, S.A., 2022. Adaptive image encryption based on twin chaotic maps. Multimedia Tools and Applications 81 (6), 8179–8198. https://doi.org/10.1007/s11042-022-11917-0.

Mondal, B., Singh, S., Kumar, P., 2019. A secure image encryption scheme based on cellular automata and chaotic skew tent map. Journal of Information Security and Applications 45, 117–130. https://doi.org/10.1016/j.jisa.2019.01.010.

Nematzadeh, H., Enayatifar, R., Yadollahi, M., Lee, M., Jeong, G., 2020. Binary search tree image encryption with DNA. Optik 202. https://doi.org/10.1016/j.ijleo.2019.163505.

Ping, P., Zhang, X., Yang, X., et al., 2022. A novel medical image encryption based on cellular automata with ROI position embedded. Multimed. Tools Appl. 81 (5), 7323–7343. https://doi.org/10.1007/s11042-021-11799-8.

Setiadi, D.R.I.M., 2021. PSNR vs SSIM: imperceptibility quality assessment for image steganography. Multimedia Tools and Applications 80 (6), 8423–8444. doi.org/10.1007/s11042-020-10035-z.

Setiadi, D.R.I.M., Rachmawanto, E.H., Zulfiningrum, R., 2022. Medical image cryptosystem using dynamic Josephus sequence and chaotic-hash scrambling. Journal of King Saud University-Computer and Information Sciences 34 (9), 6818–6828. https://doi.org/10.1016/j.jksuci.2022.04.002.

Shi, M., Guo, S., Song, X., Zhou, Y., Wang, E., 2021. Visual Secure Image Encryption Scheme Based on Compressed Sensing and Regional Energy. Entropy 23 (5), 570. https://doi.org/10.3390/e23050570.

Trejo-Guerra, R., Tlelo-Cuautle, E., Carbajal-Gómez, Victor Hugo, Rodriguez-Gomez, G., 2013. A survey on the integrated design of chaotic oscillators. Applied Mathematics and Computation 219 (10), 5113–5122. https://doi.org/10.1016/j.amc.2012.11.021.

Tsafack, N., Kengne, J., Abd-El-Atty, B., Iliyasu, A.M., Hirota, K., El-Latif, A.A.A., 2020. Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption. Inf. Sci. 515, 191–217. https://doi.org/10.1016/j.ins.2019.10.070.

Uddin, M., Jahan, F., Islam, M.K., et al., 2021. A novel DNA-based key scrambling technique for image encryption. Complex Intell. Syst. 7 (6), 3241–3258. https://doi.org/10.1007/s40747-021-00515-6.

USC-SIPI Image Database. Available online: http://sipi.usc.edu/database/database.php (accessed on 10 July 2022).

Varan, M., Akgul, A., 2018. Control and synchronisation of a novel seven-dimensional hyperchaotic system with active control. Pramana 90 (4), 1–8. https://doi.org/10.1007/s12043-018-1546-9.

Wang, X., Du, X., 2022. Chaotic image encryption method based on improved zigzag permutation and DNA rules. Multimedia Tools and Applications, 1–27. https://doi.org/10.1007/s11042-022-13012-w.

Wang, J., Lingfeng, L., 2022. A Novel Chaos-Based Image Encryption Using Magic Square Scrambling and Octree Diffusing. Mathematics 10 (3), 457. https://doi.org/10.3390/math10030457.

Wang, X., Zhao, H., Feng, L., Ye, X., Zhang, H., 2019. High-sensitivity image encryption algorithm with random diffusion based on dynamic-coupled map lattices. Optics and Lasers in Engineering 122, 225–238. https://doi.org/10.1016/j.optlaseng.2019.04.005.

Wu, X., Wang, D., Kurths, J., Kan, H., 2016. A novel lossless color image encryption scheme using 2d dwt and 6d hyperchaotic system. Information Sciences 349–350, 137–153. https://doi.org/10.1016/j.ins.2016.02.041.

Wu, J., Xiaofeng, L., Yang, B., 2018. Image encryption using 2D Hénon-Sine map and DNA approach. Signal processing 153, 11–23. https://doi.org/10.1016/j.sigpro.2018.06.008.

Xu, J., Zhao, B., Wu, Z., 2022. Research on color image encryption algorithm based on bit-plane and Chen Chaotic System. Entropy 24 (2), 186. https://doi.org/10.3390/e24020186.

Ye, G., Min, L., Mingfa, W., 2022. Double image encryption algorithm based on compressive sensing and elliptic curve. Alexandria Engineering Journal 61 (9), 6785–6795. https://doi.org/10.1016/j.aej.2021.12.023.

Ye, X., Wang, X., Gao, S., Mou, J., Wang, Z., Yang, F., 2020. A new chaotic circuit with multiple memristors and its application in image encryption. Nonlinear Dynamics 99 (2), 1489–1506. https://doi.org/10.1007/s11071-019-05370-2.

Yu, S.S., Zhou, N.R., Gong, L.H., Nie, Z., 2020. Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system. Opt. Laser Eng. 124. https://doi.org/10.1016/j.optlaseng.2018.105816.

Zhang, Y., Hua, Z., Bao, H., Huang, H., Zhou, Y., 2022. An $ n $-Dimensional Chaotic System Generation Method Using Parametric Pascal Matrix. IEEE Transactions on Industrial Informatics 18 (12), 8434–8444. https://doi.org/10.1109/TII.2022.3151984.

Zhang, D., Liao, X., Yang, B., Zhang, Y., 2018. A fast and efficient approach to color-image encryption based on compressive sensing and fractional Fourier transform. Multimed. Tools Appl. 77 (2), 2191–2208. https://doi.org/10.1007/s11042-017-4370-1.

Zhang, W., Zhu, Z., Yu, H., 2019. A symmetric image encryption algorithm based on a coupled logistic-Bernoulli map and cellular automata diffusion strategy. Entropy 21 (5), 504. https://doi.org/10.3390/e21050504.

Zheng, J., Zeng, Q., 2022. An image encryption algorithm using a dynamic S-box and chaotic maps. Applied Intelligence 52 (13), 15703–15717. https://doi.org/10.1007/s10489-022-03174-3.