A novel multi-image cryptosystem based on weighted plain images and using combined chaotic maps

Ahmad Pourjabbar Kari1 · Ahmad Habibizad Navin2 · Amir Massoud Bidgoli1 · Mirkamal Mirnia3

Received: 18 January 2021 / Accepted: 26 February 2021 / Published online: 13 March 2021 © The Author(s), under exclusive licence to Springer-Verlag GmbH Germany, part of Springer Nature 2021

Abstract
This paper introduces a new multi-image cryptosystem based on modified Henon map and non-linear combinations of chaotic seed maps. Based on the degree of correlation between the adjacent pixels of the plain images, a unique weight is assigned to the plain images. First, the coordinates of plain images are disrupted by modified Henon map as confusion phase. In the first step of diffusion phase, the pixels content of images are changed separately by XOR operation between confused images and matrices with suitable non-linear combination of seed maps sequences. These combinations of seed maps are selected depending on the weight of plain images as well as bifurcation properties of mentioned chaotic maps. After concatenating the matrices obtained from the first step of diffusion phase, the bitwise XOR operations are applied again between newly developed matrix and the other produced matrix from the chaotic sequences of the Logistic–Tent–Sine hybrid system, as second step of diffusion phase. The encrypted image is obtained after applying shift and exchange operations. The results of the implementation using graphs and histograms show that the proposed method requires an average of 49.31 ms less processing time than the best time of some previous methods for 1024 × 1024 images. The entropy is close to the ideal value of 8, and the values of the correlation coefficient of the encrypted images are close to 0. The histogram of the encrypted images is uniform and the value of peak signal to noise ratio (PSNR) is about 5 dB more than some compared methods for 50% cropping attack. Therefore, compared to some of the existing methods, the proposed method can also be used as a secure method for encrypting gray-scale digital images.

Keywords Multimedia security · Image encryption · Information entropy · Noise attack · Chaotic maps · Henon map

1 Introduction

With the explosive growth of image data [1], multimedia data security, including digital images and videos, is one of the most basic requirements of computer and telecommunication networks [2]. Among the various protection methods, image encryption is one of the most effective and common methods for data protection [3]. Although traditional cryptographic methods such as AES, DES, and RSA are also used for image encryption, image data have some features that make these cryptographic methods inefficient, especially if a large number of images are to be sent, such as videos [4]. Some of the unique features of the image are: the volume of image data is very large compared to textual data [5, 6], there is a high correlation between the pixel content of the image, the volume of duplicate data in an image is larger than the text [7], and real-time image data transmission should be maintained due to the high volume of data [8]. Especially, in the multi-view video systems, various cameras
are producing a huge amount of video and image content around the clock [9] which makes it difficult in real time to manage and encrypt the huge amount of data [10, 11] by traditional cryptographic methods.

In recent years, various methods have been proposed for effective image encryption. A new design for image encryption was presented in Ref. [12]. In the first step, the original image is confused with two keys obtained from a pseudo-random Lorenz sequence. In the second step, by performing rotation operations on the confused matrix, the diffusion operation is performed and the OR operation is performed to decode the matrix with a binary key and the encrypted image is obtained. With the emergence of deep learning, machines are now outperforming humans [13]. Deep learning-based neural networks and chaotic systems have provided some advantages in the field of computer vision, image processing [14] and cryptography. To encrypt a complex image, Zhang et al. in [15] proposed a chaotic system with deep learning-based neural networks and rotation operations simultaneously to DNA sequences. The diffusion of pixels is done through DNA code, and the selection of coding rules is done with the decimal string generated by Chen’s chaotic system. To increase the complexity and security of cryptography, the Lorenz system is used to weaken the correlation power between adjacent pixels of the image. The diffusion effect is amplified by rotational operations for DNA sequences and the XOR operator is performed between the decoding matrix and the binary matrix with the chaotic system. A secure multimedia technique over cloud where the role of the prime numbers is exposed to provide the security for multimedia data was introduced in Ref. [16]. In the proposed method, the authors have been motivated by the solution of cubic congruence and polynomial congruence.

For simultaneous encryption of RGB components of a color image, a new encryption method based on logistic map was introduced in Ref. [17]. In this method, the randomness of the chaotic sequences produced by logistic map was not appropriate. A new encryption algorithm has been put forward in Ref. [18] based on multi-secret sharing scheme along with temporal reordering of image frames. Cryptography involving traditional encryption algorithms like DES and AES are found computationally infeasible in real time due to the use of block ciphers where 128-bit data are broken into blocks. Same transformation is applied to each block and later recombined resulting expensive to use. However, the \( V \oplus \text{SEE} \) encryption process requires less bandwidth and computational power as compared to AES and DES. Li et al. proposed a new scheme based on precision limited chaotic system in Ref. [19]. They introduced a novel precision limited piecewise linear and logistic chaotic map, and also they proposed an image encryption system which is robust against statistical attacks, differential attacks and brute force attacks.

One of the most popular image denoising and encryption algorithms is based on wavelet transform, which is a transform-domain filtering method. Besides the wavelet transform, Fourier transform and mean filter are also the common methods in image denoising and encryption [20]. Wang et al. proposed an adaptive image encryption based on lifting wavelet optimization in Ref. [21]. In their proposed method, based on the adaptive wavelet, the improved wavelet optimization scheme based on improved threshold method and particle swarm optimization algorithm was proposed to improve the evaluating parameters. A novel encryption algorithm for quantum images based on chaotic maps was proposed in Ref. [22]. In this method, the image is converted into a scrambled state using quantum circuits using the principle of quantum Hilbert image scrambling algorithm. The confused image is encrypted using the quantum XOR using the chaotic maps algorithm.

A non-linear optical multi-image encryption scheme based on chaotic system and two-dimensional linear canonical transform was proposed in Ref. [23]. In this method, low-frequency sub-bands of the four gray-scale images are extracted with the contourlet transform, and the phase truncation and the bitwise XOR operation, as non-linear processes, improve the robustness of the presented multi-image encryption scheme against chosen-plaintext attack. A new image encryption scheme based on hybrid chaotic maps was proposed in Ref. [24]. In the proposed method, the confusion phase is based on Arnold’s two-dimensional map and the diffusion operation is performed using hybrid chaotic maps. The composition of the chaotic maps is selected based on the correlation coefficient of the original image as well as the characteristics of the bifurcation diagram of the combined chaotic maps.

In Ref. [25], an optimized version of the genetic algorithm is employed through modeling the simplified version of genetic processes. It is used to generate a frame sequence such that the correlation between any two frames is minimized. The frame sequence determines the randomization in order of frames of a video. The proposed method is not only fast but also more accurate to enhance the efficiency of an encryption process. Mondal et al. proposed an image encryption scheme based on a novel two-dimensional sine–cosine crosschaotic map in Ref. [26]. The proposed chaotic map generates two pseudo-random sequence which are used in permutation, and diffusion phase. The confusion layer is implemented by shuffling the image pixels, and the diffusion layer is designed by bitwise XOR operation. In Ref. [27], an image encryption algorithm based on parallel permutation-and-diffusion scheme was proposed. In the parallel row step, first, permuting each row and then performing row forward diffusion and row reverse diffusion on each row are implemented. In the parallel column step, first, permuting each column and then conducting column forward diffusion...
A novel multi-image cryptosystem based on weighted plain images and using combined chaotic…  909

and column reverse diffusion to obtain the cipher image are implemented. Yang et al. introduced a new algorithm in Ref. [28], based on fractional order hyper-chaotic system and DNA approach for double-image encryption. The proposed algorithm provides a variety of DNA coding and operation modes. Chaotic sequences are used to control the coding and operation mode to improve the complexity of the encryption process. Fractional order and initial values of fractional order hyper-chaotic system are used as the key of the proposed algorithm.

A pseudo-random number generator based on multiple chaotic maps (i.e., Logistic map, Sine map and Chebyshev map) was proposed in Ref. [29]. Subsequently, a pseudo-random sequence, whose size is the same length as plain image, was produced by the generator. The index sequence obtained by sorting the pseudo-random sequence is used to shuffle the image vector, and the original pseudo-random sequence is used to diffuse the shuffled vector by the addition modulus operations. Then, the diffused vector is circularly left-shifted to get the ciphered image vector.

Chaos has received a lot of attention in recent years for its unique features for image encryption [30, 31]. Some reasons for researchers to use chaos for image encryption are the randomness of the generated sequences, high sensitivity to the initial conditions, ergodicity, and simplicity of implementation [32, 33]. Chaotic maps are divided into one-dimensional and high-dimensional categories [34–36]. Implementation of one-dimensional chaotic maps are simple but not very secure and can be easily hacked [37, 38]. High-dimensional chaotic maps have higher security, but are difficult to implement and have high processing overhead [39, 40].

As mentioned earlier, there are many challenges to process and encrypt such massive data [30, 31]. Some reasons for researchers to use chaos for image encryption and diffusion are the randomness of the generated sequences, high sensitivity to the initial conditions, ergodicity, and simplicity of implementation [32, 33]. Chaotic maps are divided into one-dimensional and high-dimensional categories [34–36]. Implementation of one-dimensional chaotic maps are simple but not very secure and can be easily hacked [37, 38]. High-dimensional chaotic maps have higher security, but are difficult to implement and have high processing overhead [39, 40].

This paper is organized as follows:

Section 2 presents a brief survey on Logistic, Tent, Sine, and Henon chaotic maps. Section 3 gives complete description and discussion of the proposed cryptographic method, which is followed by experimental verification results in Sect. 4. Finally, Sects. 5 and 6 discuss the conclusion and future scope of the work, respectively.

2 Preliminaries

In this section, modified Henon map, three simple chaotic maps (Logistic, Tent, and Sine maps), and non-linear combinations of these simple maps are described briefly. We call these simple maps as seed maps.

2.1 Henon map

Henon map is a two-dimensional, reversible, discrete, and non-linear chaotic map [48]. Henon map transforms a point \( (x_q, y_q) \) into \( (x_{q+1}, y_{q+1}) \) by Eq. (1):
\[
\begin{align*}
    x_{q+1} &= 1 - ax_q^2 + y_q, \\
    y_{q+1} &= bx_q,
\end{align*}
\]

where \(a\) and \(b\) are the Henon map parameters. The behavior of the Henon map depends on the value of \(a\) and \(b\). For \(a \in (0.54, 2)\), and \(b \in (0, 1)\), it shows chaotic behavior [48, 49].

In this paper, Henon map is employed for confusion phase and changing the coordinates of the image pixels, so for the \(N \times N\) image:

\[
x_q, y_q, x_{q+1}, y_{q+1}, \ldots \in \{0, 1, 2, \ldots, N-1\}. \]

Therefore, to keep the coordinates of the pixels in this range, we use the modified Henon map according to Eq. (2):

\[
\begin{align*}
    x_{q+1} &= \left[ \left( 1 - ax_q^2 + y_q \right) \times 10^d \right] \mod N, \\
    y_{q+1} &= \left[ bx_q \times 10^d \right] \mod N,
\end{align*}
\]

where \(d\) is the number of floating points, and \(N\) is the size of \(N \times N\) image.

### 2.2 Logistic map

Logistic map is a one-dimensional and discrete chaotic map. This map is one of the simplest chaotic maps, and is defined mathematically as follows [24]:

\[
m_{n+1} = 4dm_n \left( 1 - m_n \right),
\]

where \(d\) is the control parameter also known as bifurcation parameter. According to the bifurcation diagram of Logistic map, when \(d\) is in the range of \([0.9, 1]\), the map will behave chaotically [48]. \(d_0 \in (0, 1)\) is initial value for \(m_n\).

### 2.3 Tent map

Tent map is another one-dimensional chaotic map that is used in many applications [48]. This map is also known as triangular map. The definition of Tent map [48] is presented as Eq. (4):

\[
e_{n+1} = \begin{cases} 2ze_n & 0 \leq e_n \leq 0.5 \\ 2z(1 - e_n) & 0.5 < e_n < 1. \end{cases}
\]

where \(z\) is the control parameter and according to the bifurcation diagram of Tent map, if \(z \in [0.5, 1]\), then the map will have chaotic behavior [48]. \(z_0 \in (0, 1)\) is the initial value for \(e_n\).

### 2.4 Sine map

Sine map is one of the most widely used one-dimensional chaotic maps [24], that can produce complex chaotic sequences with a range of \([0, 1]\). The definition of Sine map is:

\[
k_{n+1} = w \times \sin (\pi k_n),
\]

where \(w\) is the control parameter and according to the bifurcation diagram [24], \(w \in [0.87, 1]\) and \(w_0\) is the initial value for \(k_n\).

### 2.5 Combined chaotic maps

To increase the unpredictability of chaotic sequences, we use seven non-linear combinations of simple Logistic, Tent, and Sine maps, shown in Table 1. These non-linear systems are used to generate complex chaotic sequences.

The cascade operator is applied to seed maps, which improves complexity level of the chaotic structure, and the mod operation ensures the output is restricted to \([0, 1]\).

In this paper, to quantify all the produced chaotic sequences between 0 and 255, except for modified Henon map, Eq. (13) is employed:

\[
U_i = \left[(10^d \times V_i)\right] \mod 256,
\]

where \(V_i\) is the generated chaotic sequence, \(f\) is the number of floating point, and \(U_i\) is the chaotic sequence between 0 and 255.

### 3 Proposed scheme

Figure 1 shows the block diagram of the proposed scheme. For simplicity, the proposed method is implemented for two \(N \times N\) gray images, but it can be generalized to more than two color images of any size. The introduced method has been structured in such a way that it can be used in parallel in multiprocessor systems. This method uses two basic parts for cryptography: confusion and diffusion. The confusion operation is used to disrupt the pixel coordinates, and the diffusion operation is used to change the content of the pixels. One of the main goals in image encryption is to keep the correlation between the pixels in the encrypted image.

| Combined system | Equation |
|-----------------|----------|
| LL system: \(x_{n+1} = \text{Logistic (Logistic (}x_n)\)) \mod (1) | (6) |
| TT system: \(x_{n+1} = \text{Tent (Tent (}x_n)\)) \mod (1) | (7) |
| SS system: \(x_{n+1} = \text{Sine (Sine (}x_n)\)) \mod (1) | (8) |
| LT system: \(x_{n+1} = \text{Logistic (Tent (}x_n)\)) \mod (1) | (9) |
| LS system: \(x_{n+1} = \text{Logistic (Sine (}x_n)\)) \mod (1) | (10) |
| ST system: \(x_{n+1} = \text{Sine (Tent (}x_n)\)) \mod (1) | (11) |
| LTS system: \(x_{n+1} = \text{Logistic (Tent (Sine (}x_n)\)) \mod (1) | (12) |
as small as possible and close to zero. In our scheme, to enhance efficiency, we proposed that a certain weight be assigned to the input images according to the degree of correlation of the adjacent pixels, and these weights be effective in the cryptographic process. Plain images with smaller correlation coefficients close to zero should be lighter encoded and have lower weights. So different images are encrypted in different ways. Low-correlation images are encrypted with simpler maps, and vice versa.

The proposed algorithm is summarized in seven steps as follows:

**Step 1:** The absolute values of correlation coefficient for 2000 random horizontally, vertically and diagonally adjacent pixels for two images $I_1, I_2$ with a size of $N \times N$ are calculated separately, and are called $r_1$ and $r_2$, respectively.

**Step 2:** The coordinates of the pixels of the two plain images $I_1, I_2$ are changed separately, using the modified Henon map using Eq. (2), so the $H_1$ and $H_2$ matrices of size $N \times N$ are generated.

**Step 3:** Using the correlation coefficients calculated in step 1 ($r_1, r_2$), the appropriate weight ($w$) for each image is assigned according to Table 2, and also the proper combination of chaotic maps are selected to produce the appropriate chaotic sequences and formation of $C_1, C_2$ combined chaotic matrices of size $N \times N$. These weights are selected based on bifurcation diagram of seed and hybrid chaotic maps, and also the correlation rate of plain images.

After quantizing the values of $C_1$ and $C_2$ matrices at $[0, 255]$ by Eq. (13), bitwise XOR operation is performed between $H_1$ and $C_1$, and also between $H_1$ and $C_2$ separately. The matrices of $I'_1$ and $I'_2$ are produced as Eqs. (14, 15):

$$I'_1 = H_1 \oplus C_1,$$

$$I'_2 = H_2 \oplus C_3.$$  

**Step 4:** In this step, $I'_1$ and $I'_2$ matrices with size $N \times N$ are concatenated and a new matrix ($R$) with size $2N \times N$ is produced.

**Step 5:** Suppose the weight of the first image is $w_1$ and the weight of the second image is $w_2$. The value of $t$ is calculated by Eq. (16):

$$t = \left(\frac{w_1 - w_2}{2}\right) + 1.$$  

---

**Table 2** Assigned weights to images with different correlations, and corresponding chaotic maps

| Absolute value of plain image correlation coefficient | Weight ($w$) | Selected combined chaotic map to generate chaotic sequences (combined chaotic matrices $C_{1, N \times N}$) |
|-------------------------------------------------------|--------------|--------------------------------------------------------------------------------------------------|
| $0.0 \leq r < 0.2$                                   | $w = 1$      | Logistic map                                                                                    |
| $0.2 \leq r < 0.3$                                   | $w = 2$      | Tent map                                                                                        |
| $0.3 \leq r < 0.4$                                   | $w = 3$      | Sine map                                                                                       |
| $0.4 \leq r < 0.5$                                   | $w = 4$      | Combination of Logistic and Logistic maps (LL system)                                           |
| $0.5 \leq r < 0.6$                                   | $w = 5$      | Combination of Tent and Tent maps (TT system)                                                   |
| $0.6 \leq r < 0.7$                                   | $w = 6$      | Combination of Sine and Sine maps (SS system)                                                   |
| $0.7 \leq r < 0.8$                                   | $w = 7$      | Combination of Logistic and Tent maps (LT system)                                               |
| $0.8 \leq r < 0.9$                                   | $w = 8$      | Combination of Logistic and Sine maps (LS system)                                               |
| $0.9 \leq r \leq 1.0$                                | $w = 9$      | Combination of Sine and Tent maps (ST system)                                                   |
For all $2N \times N$ components of 8-bit gray-scale pixels in the $R$, the left circular shift operation is performed for $t$ time, and matrix $S$ is produced.

**Step 6:** For all $2N \times N$ components of the $S$ matrix, the contents of the bits in the $\left[\frac{n}{2}\right]$ and $\left[\frac{n}{2}\right]$ positions are swapped together and matrix $P$ is obtained.

**Step 7:** In this step, a new $2N \times N$ matrix $Z$ containing chaotic sequences generated by the non-linear combination of three Logistic, Tent and Sine maps (LTS system) is achieved. After quantizing the values of matrix $Z$ in the range $[0, 255]$ by Eq. (13), the bitwise XOR operation between $P$ and the new $2N \times N$ matrix $Z$ is performed and final encrypted matrix $E$ is produced.

Since all operations performed for encryption are reversible, so the decryption operation is similar to the encryption operation that must be performed in reverse.

### 3.1 Theoretical analysis

To prove the effectiveness of the proposed method, and to prove why we used Table 2 for different correlation coefficients, Lyapunov’s exponent (LE) analysis is employed. Maps with a larger positive Lyapunov exponent have a larger chaotic range [24, 49, 50]. Here, we prove the efficiency of the proposed method for ST (combined of Sine and Tent maps), and there is a similar proof for other combined maps. We represent the Lyapunov exponent value of Sine map with $\lambda_{S(x)}$, and Tent map with $\lambda_{T(x)}$, and the Lyapunov exponent value of the combined ST map with $\lambda_{U(x)}$. Let $x_0, y_0$ be two initial values with small difference. $x_1$, $y_1$ are the next iteration of $x_0$, and $y_0$. $S(x)$, $T(x)$ are Sine and Tent maps, respectively. We have:

$$|x_1 - y_1| = \frac{|S(T(x_0)) - S(T(y_0))|}{|T(x_0) - T(y_0)|}. $$

If $x_0 \to y_0$ then $T(x_0) \to T(y_0)$ and we have:

$$\frac{d(S)}{dx} \approx \lim_{T(x_0) \to T(y_0)} \frac{|S(T(x_0)) - S(T(y_0))|}{|T(x_0) - T(y_0)|}. $$

So we have:

$$|x_1 - y_1| \approx \left( \frac{d(S)}{dx} \right)_{T(x_0)} \left| \frac{d(T)}{dx} \right|_{x_0} |x_0 - y_0|. $$

After $n$ iteration, we have:

$$|x_1 - y_1| \approx \left( \prod_{i=0}^{n-1} \frac{d(S)}{dx} \right) \left( \prod_{i=0}^{n-1} \frac{d(T)}{dx} \right) |x_0 - y_0|. $$

Suppose $\Delta U(x)$ is the average change in each iteration from $|x_1 - y_1|$ to $|x_n - y_n|$, so we have:

$$\Delta U(x) \approx \left( \prod_{i=0}^{n-1} \frac{d(S)}{dx} \right) \left( \prod_{i=0}^{n-1} \frac{d(T)}{dx} \right) |x_0 - y_0|.$$ 

Based on Lyapunov’s exponent definition (LE), we can calculate LE of $U(x)$ as:

$$\lambda_{U(x)} = \ln(\Delta U(x)) = \lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left( \frac{d(S)}{dx} \left| \frac{d(T)}{dx} \right| \right).$$

We know the larger value of a positive LE has better chaotic performance, so $\lambda_{S(x)}$ and $\lambda_{T(x)}$ must be positive numbers, and it is clear that $\lambda_{U(x)} \geq \lambda_{S(x)}$ and $\lambda_{U(x)} \geq \lambda_{T(x)}$.

As mentioned earlier, in order for Logistic, Tent, and Sine maps to have chaotic properties, their Lyapunov exponent values must be positive. For this purpose, their control parameters, $d, z$, and $w$, must be in certain intervals ($d \in [0.9, 1], z \in [0.5, 1], w \in [0.87, 1]$). Therefore, to determine LE threshold, we use a random number generator at specified intervals to generate random numbers as control parameters. These control parameters are secret keys.

### 3.2 Motivation

One of the goals of image encryption is to make the correlation between adjacent pixels in the encrypted image as small as possible and close to zero. Therefore, as an motivation, if the plain image has a small correlation coefficient, it should be encrypted with simpler methods. As an innovation, we proposed to assign a weight to the plain images. We assigned less weight to low-correlation images and more weight to high-correlation images. In addition, these weights are used
in the cryptographic process and are effective in the cryptographic process. Therefore, images with different correlations are encrypted in different ways. This innovation makes the encryption method unpredictable and images with low correlation have less processing time and vice versa. Furthermore, due to the simultaneous and parallel encryption of two images, the performance increases.

4 Performance analysis and discussion

Evaluation measures are necessary to confirm the effectiveness of image encryption technique. In this section, the various characteristics of an image encryption algorithm are explored using these parameters.

4.1 Differential attack

Two evaluation parameters are used to show the effectiveness of the cryptographic method against differential attacks [50]: number of pixel change rate (NPCR) and unified average changing intensity (UACI). Differential attack shows the sensitivity of the cryptographic method to small changes in the original image. High sensitivity indicates that if a small change, such as a change of only one least significant bit in the original image occurs, different encrypted images are obtained [51]. Table 3 shows the values obtained for these two evaluation parameters for standard images. In Table 4, the NPCR and UACI values of the proposed method are compared with some of the previous methods.

4.1.1 Number of pixel change rate (NPCR)

This evaluation parameter indicates the percentage difference between the original encrypted image and the original encrypted image with only one bit difference [52, 53]. The maximum value of NPCR is 100%, and the values closer the maximum value indicate that the cryptographic method is more resistant to differential attacks [54, 55]. The value of NPCR is calculated using Eq. (17):

\[
\text{NPCR} = \frac{\sum_{i,j} f(i,j)}{M \times N} \times 100%,
\]

\[
\begin{align*}
   f(i,j) &= 0 \text{ if } P_1(i,j) = P_2(i,j) \\
   f(i,j) &= 1 \text{ if } P_1(i,j) \neq P_2(i,j),
\end{align*}
\]

\[
\text{UACI} = \frac{1}{M \times N} \left[ \sum_{i,j} \left| P_1(i,j) - P_2(i,j) \right| / 255 \right] \times 100%.
\]

\[
P_1 \text{ is the original encrypted image and } P_2 \text{ is the original encrypted image with only one bit difference. } M \text{ is the width of the image and } N \text{ is the height of the image.}
\]

4.1.2 Unified average changing intensity (UACI)

After creating a bit difference in the original image, two images are encrypted. UACI shows the average intensity of difference between two encrypted images [56, 57]. The value of the parameter is calculated by Eq. (19).

High values are suitable for this evaluation parameter, because it indicates that the average difference between two encrypted images is large and the cryptographic method is resistant to differential attacks [58].

| Method | Image | Size   | NPCR (%) | UACI (%) |
|--------|-------|--------|----------|----------|
| Proposed | Lena  | 512×512 | 99.6895  | 33.5964  |
| Ref. [24] | Lena  | 512×512 | 99.6461  | 33.6252  |
| Ref. [50] | Lena  | 512×512 | 99.6200  | 33.4100  |
| Ref. [73] | Lena  | 512×512 | 99.6100  | 33.4590  |
| Ref. [74] | Lena  | 512×512 | 99.6110  | 33.4509  |
| Ref. [75] | Lena  | 512×512 | 76.1681  | 24.5234  |
| Ref. [51] | Lena  | 512×512 | 99.6052  | 33.4111  |
| Ref. [52] | Lena  | 512×512 | 99.6215  | 33.4954  |
| Proposed | Lena  | 256×256 | 99.6100  | 33.4600  |
| Ref. [24] | Lena  | 256×256 | 99.6226  | 33.4156  |
| Ref. [53] | Lena  | 256×256 | 99.5941  | 33.5021  |
| Ref. [54] | Lena  | 256×256 | 99.6101  | 33.4354  |
| Proposed | Lena  | 256×256 | 99.7126  | 33.4864  |
| Ref. [24] | Lena  | 256×256 | 99.6236  | 33.4311  |
| Ref. [58] | Lena  | 256×256 | 99.6017  | 33.6287  |
| Proposed | Baboon | 512×512 | 99.6255  | 33.4215  |
| Ref. [24] | Baboon | 512×512 | 99.6234  | 33.4156  |
| Ref. [51] | Baboon | 512×512 | 99.3504  | 33.4520  |
| Ref. [56] | Baboon | 512×512 | 99.6048  | 33.4554  |
| Ref. [57] | Baboon | 512×512 | 99.6101  | 33.4354  |
| Proposed | Baboon | 256×256 | 99.7126  | 33.4864  |
| Ref. [24] | Baboon | 256×256 | 99.6236  | 33.4311  |
| Ref. [58] | Baboon | 256×256 | 99.6017  | 33.6287  |
4.2 Statistical analysis

One of the main goals of image encryption is to reduce the correlation between adjacent pixels as much as possible, and also to make the histogram of the encrypted image uniform [59, 60]. In statistical analysis of a cryptographic method, the uniformity of the histogram as well as the value of the correlation coefficient between adjacent pixels in the encrypted image is examined [61, 62].

4.2.1 Histogram analysis

The image histogram shows the number of pixels that have the same gray-scale level [63]. For 8-bit gray-scale images, the horizontal axis of the histogram represents the gray levels from 0 to 255, and the vertical axis represents the number of pixels that have specific gray levels. The plain images usually do not have a uniform histogram, and one of the important purposes of cryptography is to make the encrypted image histogram uniform, so that there are approximately equal numbers of pixels on each gray-scale level [64, 65]. The uniformity of encrypted histograms makes difficult for the attacker to guess the true gray levels of the plain image. Figures 2, 3, 4 and 5 show the non-uniformity of the plain images histogram, as well as the uniformity of the encrypted images.

4.2.2 Correlation coefficient

In the original images, usually there is a high correlation between adjacent pixels in three directions: horizontal, vertical, and diagonal [66, 67]. High correlation makes it easy for the attackers to guess the pixel values of the original image [68]. Therefore, another goal of an effective encryption method is to reduce the correlation coefficient between adjacent pixels in the encrypted image as close as possible to zero [69, 70]. Using Eq. (23), the correlation coefficient can be calculated:

\[
E(x) = \frac{1}{K} \sum_{i=1}^{K} x_i, \tag{20}
\]

\[
D(x) = \frac{1}{K} \sum_{i=1}^{K} [x_i - E(x_i)]^2, \tag{21}
\]

\[
Cov(x, y) = \frac{1}{K} \sum_{i=1}^{K} [x_i - E(x_i)] [y_i - E(y_i)], \tag{22}
\]

\[
r_{xy} = \frac{Cov(x, y)}{\sqrt{D(x)D(y)}}, \tag{23}
\]

where Cov(x, y) is the covariance between samples x and y. (x, y) are the coordinates of an image. K is the number of

**Fig. 2** a Standard 256×256 “Lena” plain image, b standard 256×256 “Camera man” plain image, second column, c, d are plain images with non-uniform histograms, respectively, e the 512×256 two plain image single encrypted image, f the uniform histogram of double encrypted images
A novel multi-image cryptosystem based on weighted plain images and using combined chaotic…

pixel pairs \((x_i, y_i)\). \(D(x)\) and \(D(y)\) are the standard deviation of \(x\) and \(y\), respectively. \(E(x)\) is the mean of \(x\) pixel values. The range of correlation coefficient is \([-1, 1]\), and the value of an encrypted image should be near to 0 \([71, 72]\). To test the correlation, we randomly select 3000 pixels adjacent horizontally, vertically, and diagonally from the images, and use

Fig. 3 First column a, d are two 256 × 256 plain images, second column b, e are decrypted images, respectively, c the 512 × 256 two plain image single encrypted image, f the uniform histogram of double encrypted images

Fig. 4 a Standard 256 × 256 “Baboon” plain image, b standard 256 × 256 “Peppers” plain image, c the 512 × 256 two plain image single encrypted image, d the uniform histogram of encrypted images
Fig. 5  a 512 × 256 merged two 256 × 256 plain images, b the 512 × 256 two plain image single encrypted image, c the histogram of two concatenated plain images, d the uniform histogram of encrypted images, e the decrypted image.

Fig. 6  a Standard 256 × 256 “Female” plain image, c standard “Male” 256 × 256 plain image, b the 512 × 256 two plain image single encrypted image, d the uniform histogram of encrypted images.

Table 5  Correlation test results for some 256 × 256 standard images

| Test image | Original image | Encrypted image |
|------------|---------------|-----------------|
|            | Horizontal   | Vertical        | Diagonal | Horizontal | Vertical | Diagonal |
| Lena       | 0.9711       | 0.9853          | 0.9853   | 0.0015     | 0.0041   | 0.0057   |
| Camera man | 0.9163       | 0.9732          | 0.9042   | 0.0075     | 0.0055   | -0.0083  |
| Baboon     | 0.6111       | 0.6589          | 0.5211   | 0.0087     | -0.0073  | 0.0041   |
| Female     | 0.9812       | 0.9370          | 0.9420   | 0.0073     | 0.0075   | 0.0074   |
| Peppers    | 0.8547       | 0.8961          | 0.8862   | 0.0041     | 0.0056   | 0.0024   |
| Male       | 0.9124       | 0.9327          | 0.9125   | 0.0067     | 0.0081   | 0.0061   |
A novel multi-image cryptosystem based on weighted plain images and using combined chaotic...

Eq. (23) to calculate the value of the correlation coefficient. When the histogram of the encrypted image is uniform, the correlation between adjacent pixels also decreases dramatically (Fig. 6).

Table 5 shows the results of the correlation coefficients of the original images and the encrypted images using the proposed scheme. Table 6 also compares the results of the proposed method with some of the recently introduced methods.

4.3 Information entropy

Information entropy is another criterion for evaluating the performance of a cryptographic method [73–75]. For 8-bit gray images, the information entropy value is in the range of 0 and 8, and the optimal value for this parameter is 8. If all 256 Gy levels of the image have the same probability \( P(s_i) = \frac{1}{256} \) in all image pixels, we will reach the maximum value. The information entropy value of an image is calculated using Eq. (24):

\[
H(s) = - \sum_{i=0}^{255} \left( P(s_i) \log_2 P(s_i) \right),
\]

where the \( P(s_i) \) indicates the existence probability of a \( s_i \) gray level in the image. It is clear that if the histogram of the encrypted image is more uniform, then the entropy value of the encrypted image is closer to the ideal value of 8.

Table 7 compares the proposed method with some of the previous methods, and Table 8 shows the results for some of the standard images.

### Table 6: Comparison of correlations with some recent image encryption schemes

| Reference  | Image          | Correlation  |
|------------|----------------|--------------|
|            |                | Horizontal | Vertical | Diagonal |
| Proposed   | Lena           | 0.0015      | 0.0041   | 0.0057   |
| Ref. [24]  | Lena           | 0.0054      | 0.0049   | 0.0042   |
| Ref. [73]  | Lena           | 0.0026      | 0.0051   | 0.0264   |
| Ref. [74]  | Lena           | 0.0016      | 0.0020   | 0.0014   |
| Ref. [75]  | Lena           | 0.0001      | 0.0015   | 0.0013   |
| Ref. [76]  | Lena           | 0.0012      | 0.0003   | 0.0010   |
| Proposed   | Baboon (Mandrill) | 0.0087      | −0.0073  | 0.0041   |
| Ref. [16]  | Baboon (Mandrill) | 0.0016      | −0.0011  | −0.0002  |
| Proposed   | Male (Pirate)  | 0.0067      | 0.0081   | 0.0061   |
| Ref. [16]  | Male (Pirate)  | 0.0122      | 0.0077   | 0.0047   |
| Proposed   | Female (Woman) | 0.0073      | 0.0075   | 0.0074   |
| Ref. [16]  | Female (Woman) | 0.0090      | 0.0085   | 0.0002   |

### Table 7: Comparison of the entropy value between proposed scheme and other methods

| Encryption scheme | Image  | Size  | Cipher images entropy |
|-------------------|--------|-------|-----------------------|
| Proposed          | Lena   | 512×12 | 7.999893              |
| Ref. [24]         | Lena   | 512×12 | 7.999918              |
| Ref. [75]         | Lena   | 512×12 | 7.902733              |
| Ref. [77]         | Lena   | 512×12 | 7.899111              |
| Ref. [78]         | Lena   | 512×12 | 7.902487              |
| Ref. [53]         | Lena   | 512×12 | 7.999338              |
| Ref. [59]         | Lena   | 512×12 | 7.999319              |
| Ref. [50]         | Lena   | 512×12 | 7.999324              |
| Ref. [51]         | Lena   | 512×12 | 7.999301              |
| Ref. [52]         | Lena   | 512×12 | 7.999286              |
| Proposed          | Lena   | 256×256| 7.996237              |
| Ref. [24]         | Lena   | 256×256| 7.998834              |
| Ref. [53]         | Lena   | 256×256| 7.996951              |
| Ref. [60]         | Lena   | 256×256| 7.997000              |
| Ref. [54]         | Lena   | 256×256| 7.997200              |
| Ref. [55]         | Lena   | 256×256| 7.997300              |
| Proposed          | Baboon | 512×12 | 7.999921              |
| Ref. [24]         | Baboon | 512×12 | 7.999896              |
| Ref. [53]         | Baboon | 512×12 | 7.999350              |
| Ref. [51]         | Baboon | 512×12 | 7.999263              |
| Ref. [61]         | Baboon | 512×12 | 7.999300              |
| Ref. [57]         | Baboon | 512×12 | 7.999345              |

### Table 8: Information entropy test results for standard images

| Test images   | Image size | Cipher images entropy |
|---------------|------------|-----------------------|
| Camera man    | 256×256    | 7.997325              |
| Lena          | 256×256    | 7.996237              |
| Baboon        | 256×256    | 7.999069              |
| Female        | 256×256    | 7.999158              |
| Male          | 256×256    | 7.998912              |
| Peppers       | 256×256    | 7.999124              |
keys to get the correct key, while if the key space is $10^{10}$, then the attacker must test more keys and spend more time to find correct key, so it will be actually impossible to find the right key in a reasonable time for enough larger key space. In this paper, the secret keys are: parameters $a, b$ in Henon map, parameters $d, d_0$ in Logistic map, parameters $z, z_0$ in Tent map, parameters $w, w_0$ in Sine map, correlation coefficient of plain images $r_1, r_2$, and finally iter is the number of iterations of the cryptographic process. Since the number of secret keys is 11, if the accuracy of the decimal numbers is 14 floating points, then the key space will be $10^{154}$, which is sufficiently resistant to attacks.

In key sensitivity analysis, for a high-performance cryptographic method, two items are considered. First, with a very small change of $10^{-14}$ in the secret key, a completely different encrypted image should be obtained. Second, if the encrypted image is decrypted with an incorrect key that has a very small difference of $10^{-14}$ with the correct key, the original image will not be obtained [77, 78]. Figure 7 shows the results of key sensitivity analysis for two secret keys. Parameter $a$ in Henon map is considered as the first secret key $K_{a1}$, and parameter $b$ in Henon map is considered as the second secret key $K_{a2}$, and the other secret keys are the same. The implementation results show that the original images can only be retrieved and decrypted with only the correct keys.

## 4.5 Noise and cropping attack

An attacker may make noise to destroy the original image, or cut part of the image information that causes the data to be lost [79]. An effective cryptographic method must be able to withstand noise and cropping attacks. Usually, to evaluate the cryptographic method against cropping attacks, $\frac{1}{16}, \frac{1}{4}, \frac{1}{2}$, and $\frac{1}{3}$ sizes of the encrypted image are cropped, then the cropped image is decrypted, and finally the quality of the decrypted image is evaluated compared to the plain image. To evaluate the cryptographic method against noise attacks, we add 5% salt and pepper noises to the encrypted image and then the noisy image is decrypted, and its quality is evaluated compared to the original image. Figures 8, 9 and 10 show the results of different cropping attacks. To evaluate

![Fig. 7](image_url)

Fig. 7  a, b 256×256 plain images, c the 512×256 encrypted image of two plain images with secret key $K_{a_1}=0.78$, d the 512×256 encrypted image of two plain images with secret key $K_{a_2}=0.83$, e the 512×256 decrypted image of two plain images with secret key $K_{a_1}=0.78 + 10^{-14}$, f the 512×256 decrypted image of two plain images with secret key $K_{a_2}=0.83 + 10^{-14}$, g the 512×256 decrypted image of two plain images with secret key $K_{a_1}=0.93$, h the 512×256 decrypted image of two plain images with secret key $K_{a_2}=0.63$, i the decrypted image of plain image (a) with correct secret key $K_{a_1}=0.78$, j the decrypted image of plain image (b) with correct secret key $K_{a_2}=0.83$.
A novel multi-image cryptosystem based on weighted plain images and using combined chaotic...

Fig. 8  a, d 256×256 plain images, b the decrypted image for (a) after $\frac{1}{16}$ cropping attack in one round, e the decrypted image for (d) after $\frac{1}{16}$ cropping attack in one round, c the 512×256 two plain image single encrypted image after $\frac{1}{16}$ cropping attack, f is the histogram of (c)

Fig. 9  a, d 256×256 plain images, b the decrypted image for (a) after $\frac{1}{4}$ cropping attack, e the decrypted image for (d) after $\frac{1}{4}$ cropping attack, c the 512×256 two plain image single encrypted image after $\frac{1}{4}$ cropping attack, f the histogram of (e)
the quality of noisy and cropped images compared to the original image, four parameters: peak signal to noise ratio (PSNR), signal to distortion ratio (SDR), signal to noise ratio (SNR) and structural similarity index (SSIM), have been introduced [79], which are explained in the following sections.

Figure 8 and Table 9 demonstrate the result of evaluating parameters for different iterations and $\frac{1}{16}$ cropping attack.

Figure 9 and Table 10 show the results of evaluating parameters for different iterations and 25% cropping attack.

Figure 10 and Table 11 illustrate the results of evaluating parameters for different iterations and 50% cropping attack.

Implementation results show that higher value of cropping attacks causes lower evaluating parameters, and in some iterations, some parameters have better values. In Table 11, it is clear that the value of PSNR in 1st iteration is better.

Figure 11 shows the results after 5% salt and pepper attack, and Table 12 shows the comparison of PSNR for different cropping attacks in some references and maximum

| Fig. 10 | a, d 256×256 plain images, b the decrypted image for (a) after $\frac{1}{2}$ cropping attack, e the decrypted image for (d) after $\frac{1}{2}$ cropping attack, f the 512×256 two plain image single encrypted image after $\frac{1}{2}$ cropping attack, f the histogram of (e) |
| --- | --- |

Table 9 Encryption evaluating parameters for $\frac{1}{16}$ cropping attack and different iterations

| Cropping value | Iteration | PSNR | SDR | SSIM | SNR |
| --- | --- | --- | --- | --- | --- |
| $\frac{1}{16}$ | 1 | 22.2157 | 14.2357 | 0.5342 | 16.0524 |
| 5 | 23.6981 | 14.6951 | 0.5874 | 16.2154 |
| 10 | 22.9264 | 14.3281 | 0.5318 | 16.8724 |
| 15 | 21.3281 | 14.8547 | 0.6286 | 15.9687 |
| 20 | 21.6581 | 14.1237 | 0.5682 | 16.3587 |

Table 10 Encryption evaluating parameters for 25% cropping attack and different iterations

| Cropping value | Iteration | PSNR | SDR | SSIM | SNR |
| --- | --- | --- | --- | --- | --- |
| $\frac{1}{4}$ | 1 | 19.3251 | 9.9825 | 0.2895 | 10.2354 |
| 5 | 19.2014 | 9.3258 | 0.2965 | 10.8951 |
| 10 | 19.0219 | 10.1206 | 0.3019 | 11.0124 |
| 15 | 18.6522 | 10.1125 | 0.2932 | 11.1267 |
| 20 | 19.2573 | 9.6528 | 0.2735 | 10.3257 |

Table 11 Evaluating parameters for different iterations and 50% cropping attack

| Cropping value | Iteration | PSNR | SDR | SSIM | SNR |
| --- | --- | --- | --- | --- | --- |
| $\frac{1}{2}$ | 1 | 16.3258 | 6.6584 | 0.1425 | 8.5516 |
| 5 | 16.1204 | 6.3284 | 0.1458 | 8.0324 |
| 10 | 15.8695 | 6.2574 | 0.1521 | 7.6951 |
| 15 | 16.1254 | 6.3874 | 0.1326 | 7.9824 |
| 20 | 16.2517 | 6.8921 | 0.1635 | 8.2514 |
A novel multi-image cryptosystem based on weighted plain images and using combined chaotic…

values of proposed method. Results show that the value of PSNR is more appropriate and for 50% cropping attack the PSNR value is about 5 dB more than some compared methods.

Figures 12, 13 and 14 show the PSNR, SSIM, SDR, and SNR evaluating parameters for different value of cropping attacks and various iterations.

4.5.1 Peak signal to noise ratio (PSNR)

This parameter is used to evaluate the effect of noise and cropping attack on the encrypted image. Higher value of
PSNR is good [79], because it shows that the noise and cropping attack has low effect on the decrypted image [24]. The maximum value for PSNR is infinite. PSNR is calculated by Eq. (25):

$$\text{PSNR} = 10 \log_{10} \left( \frac{255}{\sqrt{\text{MSE}}} \right)^2 \text{ (dB)},$$  (25)

$$\text{MSE} = \frac{1}{MN} \sum_{y=1}^{M} \sum_{x=1}^{N} \left[ I(x, y) - I'(x, y) \right]^2,$$  (26)

$I$ is plain image and $I'$ is decrypted image after cropping attack, and MSE is mean square error. If $I$ and $I'$ were exactly the same, then the value of PSNR value will be infinite.

### 4.5.2 Signal to distortion ratio (SDR)

Another parameter for evaluating the quality of a decoded image after a cropping attack is SDR. Higher value of SDR is suitable [24], because it indicates that the cropping attack has low effect on the decrypted image [79]. The maximum value for SDR is infinite. The SDR in dB (decibel) is calculated by Eq. (27):

$$\text{SDR} = 10 \log_{10} \frac{\sum_{x,y} I(x,y)^2}{\sum_{x,y} \left( I(x,y) - I'(x,y) \right)^2} \text{ (dB)},$$  (27)

$I$ is plain image, and $I'$ is decrypted image after cropping attack. If $I = I'$, then SDR will be infinite.

### 4.5.3 Signal to noise ratio (SNR)

This parameter is also used to evaluate the effect of noise and cropping attacks [79]. The amount of SNR is in the range of 1 and $\infty$. High values are suitable for SNR because it indicates that noise and cut have little effect on the encrypted image. If the two original and decoded images after cutting and noise attacks are the same, the value of SNR is infinite. The SNR value is calculated using Eq. (28):

$$\text{SNR} = \frac{\sum_{x,y} \left[ O(x,y) \right]^2}{\sum_{x,y} \left( O(x,y) - L(x,y) \right)^2},$$  (28)

where $O$ is the original image, and $L$ is decrypted image after noise and cropping attacks.

### 4.5.4 The structural similarity (SSIM) index

This parameter is used to measure the similarity between two images [79]. In this research, we use SSIM index between plain image and decrypted image after cropping attack. The resultant SSIM index is a decimal value between $-1$ and 1. If two images are exactly the same, the value of this parameter is equal to 1. SSIM is defined as Eq. (29):

$$\text{SSIM}(x,y) = \frac{(2\mu_x \mu_y + C_1) (2\sigma_{xy} + C_2)}{\left( \mu_x^2 + \mu_y^2 + C_1 \right) \left( \sigma_x^2 + \sigma_y^2 + C_2 \right)}.$$

$\mu_x$ is the average of $x$, $\mu_y$ is the average of $y$, $\sigma_x^2$ is the variance of $x$, $\sigma_y^2$ is the variance of $y$, $\sigma_{xy}$ is the covariance of $x$ and $y$, $C_1 = (k_1 L)^2$, $C_2 = (k_2 L)^2$, $L$ the dynamic range of the pixel values, $k_1 = 0.01$ and $k_2 = 0.03$.

### 4.6 Execution time

Another important factor in evaluating the performance of an encryption method is the processing time for encrypting an image in one round. To show the speed performance, implementation results are given in this section. The test was performed via the MATLAB R2016b on a computer running 64-bit Windows 10, the Intel (R) Core (TM) i7-6700 @ 3.60 GHz CPU, and 8 GB of RAM. All 26 images in the USC SIPI image Database (http://sipi.usc.edu/database) are selected as experimental images. Table 13 shows the average processing time for each image sizes and various correlation coefficients. It is clear that plain images with less correlation have less processing time and vice versa. Table 14 compares the average execution time for the proposed method with some references.

### Table 13 Average processing time for each image size and various correlation coefficients

| Correlation Coefficient | Processing time (ms) |
|--------------------------|----------------------|
| Plain image correlation  | Processing time (ms) |
| 256×256                  | 54.20                |
| 512×512                  | 81.57                |
| 1024×1024                | 116.38               |
| 0.0 ≤ r < 0.2            | 58.60                |
| 0.2 ≤ r < 0.3            | 85.36                |
| 0.3 ≤ r < 0.4            | 93.42                |
| 0.4 ≤ r < 0.5            | 101.12               |
| 0.5 ≤ r < 0.6            | 246.85               |
| 0.6 ≤ r < 0.7            | 298.33               |
| 0.7 ≤ r < 0.8            | 356.94               |
| 0.8 ≤ r < 0.9            | 452.69               |
| 0.9 ≤ r ≤ 1.0            | 510.37               |

Average processing time (ms) for each image size

| Image size             | Average processing time (ms) |
|------------------------|------------------------------|
| 256×256                | 90.97                        |
| 512×512                | 122.72                       |
| 1024×1024              | 301.69                       |
Table 14 Comparison between the average execution time for proposed method and some other methods (ms)

| Image size   | Ref. [67] | Ref. [24] | Ref. [53] | Ref. [69] | Ref. [70] | Ref. [71] | Ref. [72] | Proposed |
|--------------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|----------|
| 256×256      | 178       | 92        | 48        | 7641      | 189       | 569       | 109       | 90.97    |
| 512×512      | 663       | 109       | 139       | 34,768    | 758       | 2251      | 390       | 122.72   |
| 1024×1024    | 3142      | 351       | 481       | 151,709   | 3096      | 8986      | 1482      | 301.69   |

5 Conclusions

This paper introduces a new method for encrypting digital gray-scale multi-images. The confusion process is implemented using the modified Henon map, and the diffusion process is implemented using two-step XOR operation, also shift and exchange operations. Initially, the coordinates of two images are disrupted by the modified Henon map, and the confusion process is implemented.

As the first step of diffusion process, bitwise XOR operations are applied between the content of the confused images in confusion stage, and proper combined chaotic sequences. These chaotic sequences are selected according to the correlation values of the original images as well as the characteristics of the bifurcation diagram of the Logistic, Tent, and Sine chaotic maps. Depending on the correlation value of the original images, one weight is given to each image. Images with less correlation have less weights and vice versa. Furthermore, lighter images are encrypted with simpler chaotic maps and have less processing time. After the first stage of the diffusion process, two achieved matrix are concatenating together to form an expanded matrix. Due to the weight of the images, shift and exchange operations are applied as the second and third steps of the diffusion process, respectively. Finally, as the fourth step of the diffusion process, the second bitwise XOR operations are applied between the matrix obtained from the previous stages and combined chaotic sequences obtained from the LTS (Logistic–Tent–Sine) system with proper initial values, and the encrypted matrix is obtained.

According to the implementation results, processing time is proper, the information entropy value is close to the maximum value 8, and the correlation between adjacent pixels in encrypted images is close to zero. The histogram of the encrypted images are also uniform, the value of peak signal to noise ratio (PSNR) is about 5 dB more than some compared methods for 50% cropping attack, and the scheme is resistant to ordinary attacks. So, the proposed method can be used as a secure method for encrypting digital images.

6 Future work

As a suggestion for future work, we intend to use artificial intelligence to present a new cryptographic method using multi-criteria decision-making.

Declarations

Conflict of interest The authors have no relevant financial or non-financial interests to disclose. The authors have no conflicts of interest to declare that are relevant to the content of this article. All authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript. The authors have no financial or proprietary interests in any material discussed in this article.

References

1. Yan, C., Gong, B., Wei, Y., Gao, Y.: Deep multi-view enhancement hashing for image retrieval. In: IEEE transactions on pattern analysis and machine intelligence. PubMed ID: 32091992 (2020)
2. Xingyuan, W., Lin, T., Xue, Q.: A novel colour image encryption algorithm based on chaos. Signal Process. 92(4), 1101–1108 (2012). https://doi.org/10.1016/j.sigpro.2011.10.023
3. Pareek, N.K., Vinod, P., Sud, K.K.: Diffusion-substitution based gray image encryption scheme. Digit. Signal Process. 23(3), 894–901 (2013). https://doi.org/10.1016/j.dsp.2013.01.005
4. Alireza, J., Xin-Wen, W., Pallipuram, M.: Comments on the security of diffusion substitution based gray image encryption scheme. Digit. Signal Process. 32, 34–36 (2014). https://doi.org/10.1016/j.dsp.2014.05.011
5. Chengqing, L., Kwok-Tung, L.: Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Process. 91(4), 949–954 (2011). https://doi.org/10.1016/j.sigpro.2010.09.014
6. Kumar, K., Shrimankar, D.D., Singh, N.: Event BAGGING: a novel event summarization approach in multi view surveillance videos. In: 2017 International conference on innovations in electronics, signal processing and communication (IIESC), IEEE. (2017). https://doi.org/10.1109/IIESPC.2017.8071874
7. HONGJUN, L., ABDURAHMAN, K.: Asymmetric color image encryption scheme using 2D discrete-time map. Signal Process. 113, 104–112 (2015). https://doi.org/10.1016/j.sigpro.2015.01.016
8. Jun-xin, C., Zhi-liang, Z., Chong, F., Hai, Y., Yushu, Z.: Reusing the permutation matrices dynamically for efficient image cryptographic algorithm. Signal Process. 111, 294–307 (2015). https://doi.org/10.1016/j.sigpro.2015.01.003
9. Kumar, K., Shrimankar, D.D.: Deep event learning boost-up approach: DELTA. Multimed. Tools Appl. (2018). https://doi.org/10.1007/s11042-018-5882-z
10. Kumar, K., Shrimankar, D.D.: F-DES: fast and deep event summarization, proceedings of 2nd international conference on computer vision & image processing. IEEE Trans. Multimed. 20(2) 51–62 (2018)
11. Sharma, S., Kumar, K., Singh, N.: Deep eigen space based ASL recognition system. IETE J. Res. (2020). https://doi.org/10.1080/03772063.2020.1780164
12. Solak, E.: Cryptanalysis of a multi-chaotic systems based image cryptosystem. IEEE Opt. Commun. 283(2), 232–236 (2017)
13. Sharma, S., Shrivhare, S.N., Singh, N., Kumar, K.: Computationally efficient ANN model for small-scale problems, part of the advances in intelligent systems and computing, conference paper book series (AISC, volume 748). Mach. Intell. Signal Anal. 423–435 (2018)
14. Singh, M., Govil, M.C., Pilli, E.S., Vipparthi, S.K.: SOD-CED: salient object detection for noisy images using convolution encoder–decoder. IET Comput. Vis. (2019). https://doi.org/10.1049/iet-cvi.2018.5814
15. Zhang, Q., Guo, L., Wei, X., P.: Image encryption using DNA addition combining with chaotic maps. Math. Comput. Model. 52(11), 2028–2035 (2015)
16. Krishna, R.K., Kumar, K.: P-MEC: polynomial congruence based multimedia encryption technique over cloud. IEEE Consum. Electron. Mag. (2020). https://doi.org/10.1109/MCE.2020.3003127
17. Wang, X., Teng, L., Qin, X.: A novel colour image encryption algorithm based on chaos. Signal Process. 92(4), 1101–1108 (2012)
18. Manupriya, P., Sinha, S., Kumar, K.: V@SEE: video secret sharing encryption technique. In: In 2017 Conference on information and communication technology (CICT). IEEE. (2018). https://doi.org/10.1109/INFOCOMTECH.2017.8340639
19. Li, H., Deng, L., Gu, Z.: An image encryption scheme based on precision limited chaotic system. Multimed. Tools Appl. (2020). https://doi.org/10.1007/s11042-020-08826-5
20. Yan, C., Li, Z., Zhang, Y., Liu, Y., Ji, X., Zhang, Y.: Depth image denoising using nuclear norm and learning graph model. ACM Trans. Multimedia Comput. Commun. Appl. (2020). https://doi.org/10.1145/3404374
21. Wang, J., Liu, W., Zhang, S.: Adaptive encryption of digital images based on lifting wavelet optimization. Multimed. Tools Appl. (2019). https://doi.org/10.1007/s11042-019-7704-3
22. Diab, H., El-semary, A.M.: Secure image cryptosystem with secret sharing. In: Proceedings of 2nd international conference on computer vision & image processing, pp. 51–62 (2018)
23. Huang, Z.-J., Cheng, S., Gong, L.-H., Zhou, N.-R.: Nonlinear optics chaotic system and communication technology (CICT). IEEE. (2018). https://doi.org/10.1109/INFOCOMTECH.2017.8340639
24. Pourjabbar Kari, A., Habibizad Navin, A., Bidgoli, A.M., et al.: A new image encryption scheme based on hybrid chaotic maps. Multimed. Tools Appl. (2020). https://doi.org/10.1007/s11042-020-09043-w
25. Chen, J., Zhu, Z.-L., Zhang, L.-b, Zhang, Y., Yang, B.-Q.: Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption. Signal Process. (2017). https://doi.org/10.1016/j.sigpro.2017.07.034
26. Cao, C., Sun, K., Liu, W.: A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map. Signal Process. (2017). https://doi.org/10.1016/j.sigpro.2017.08.020
27. Wang, H., Xiao, Di., Chen, X., Huang, H.: Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map. Signal Process. (2017). https://doi.org/10.1016/j.sigpro.2017.11.005
28. Dhali, S., Pal, S.K., Sharma, K.: Cryptanalysis of image encryption scheme based on a new 1D chaotic system. Signal Process. (2017). https://doi.org/10.1016/j.sigpro.2017.12.021
29. Amina, S., Mohamed, F.K.: An efficient and secure chaotic cipher algorithm for image content preservation. Commun. Nonlinear Sci. Numer. Simul. (2017). https://doi.org/10.1016/j.cnsns.2017.12.017
30. Lan, R., He, J., Wang, S., Tianlong, Gu., Luo, X.: Integrated chaotic systems for image encryption. Signal Process. (2018). https://doi.org/10.1016/j.sigpro.2018.01.026
31. Kumar, K., Shrimankar, D.D., Singh, N.: SOMES: an efficient SOM technique for event summarization in multi-view surveillance videos. In: Recent findings in intelligent computing techniques, pp. 383–389, conference paper. (2018)
32. Kumar, K.: EVS-DK: event video skimming using deep keyframe. J. Vis. Commun. Image Represent. 58, 345–352 (2019). https://doi.org/10.1016/j.jvcir.2018.12.009
33. Kumar, K., Kumar, A., Bahuguna, A.: D-CAD: deep and crowded anomaly detection. In: ICCIT-2017: proceedings of the 7th international conference on computer and communication technology, pp. 100–105, November 2017. https://doi.org/10.1145/3154979.3154998
34. Yan, C., Shao, B., Zhao, H., Ning, R., Zhang, Y., Feng, X.: 3D room layout estimation from a single RGB image. IEEE Trans. Multimed. (2020). https://doi.org/10.1109/TMM.2020.2967645
35. Kumar, K.: Text query based summarized event searching interface system using deep learning over cloud. Multimed. Tools Appl. (2020). https://doi.org/10.1007/s11042-020-10157-4
36. Kumar, K., Shrimankar, D.D.: ESUMM: event summarization on scale-free networks. IETE Tech. Rev. 36(3), 265–274 (2019). https://doi.org/10.1080/02564602.2018.1454347
37. Atrish, A., Singh, N., Kumar, K., V.: An automated hierarchical framework for player recognition in sports image. In: ICVIP 2017: proceedings of the international conference on video and image processing, pp. 100–105, December 2017. https://doi.org/10.1145/3177404.3177432
38. Ali, T.S., Ali, R.: A novel medical image signcryption scheme using TLTS and Henon chaotic map. IEEE Access (2020). https://doi.org/10.1109/ACCESS.2020.2987615
39. Ibrahim, S., Alharbi, A.: Efficient image encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptography. IEEE Access (2017). https://doi.org/10.1109/ACCESS.2020.3032403
A novel multi-image cryptosystem based on weighted plain images and using combined chaotic…