Alexandria Engineering Journal (2022) 61, 6785–6795

HOSTED BY

Alexandria University

Alexandria Engineering Journal

www.elsevier.com/locate/aej
www.sciencedirect.com

Double image encryption algorithm based on compressive sensing and elliptic curve

Guodong Ye [a,*], Min Liu [a], Mingfa Wu [b]

[a] Faculty of Mathematics and Computer Science, Guangdong Ocean University, Zhanjiang 524088, China
[b] School of Management, Guangdong Ocean University, Zhanjiang 524088, China

Received 14 September 2021; revised 19 November 2021; accepted 7 December 2021
Available online 18 December 2021

KEYWORDS

Discrete wavelet transform;
Compressive sensing;
Chaotic systems;
Elliptic curve;
Security

Abstract A new improved three-dimensional continuous chaotic system (ImproBsys) is designed in this paper. It can achieve from an ordinary chaotic state to a hyperchaotic state, that is, chaotic behavior tends to become more complex. Furthermore, by using ImproBsys, this paper proposes a double image encryption algorithm based on compressive sensing and public key elliptic curve. First, the two plain images of the same size are excuted by discrete wavelet transformation (DWT), and then the DWT coefficients are thresholded. Second, the quantization matrix is compressed by compressive sensing, and the size is reduced to half of the original one, and then the two compressed matrices are spliced together to form a new matrix. Finally, the new matrix is encrypted by elliptic curve cipher to get the cipher image. Our contributions are: (1) A new ImproBsys is designed with better chaotic behavior, which has two positive Lyapunov exponents to show hyperchaos phenomenon. (2) Compressive sensing technique is employed to reduce the amount of data transmission for two single images, and then we use ImproBsys to control the measurement matrix. (3) The initial values of the ImproBsys depend on the information entropy of the plain image by a new constructed mathematical model.

1. Introduction

With the rapid development and popularization of the Internet, the transmission of digital information only by text content can not satisfy people's requirements. Consequently, the transmission and communication of image and video are increasing explosively. Among them, image as one of the most intuitive and easy way to understand the world, including medical image, weather image, educational image, etc., has been widely used in mobile communication. However, some images contain private information of individuals or organizations. It is inappropriate to make such images public. So, we should take some methohs to prevent unauthorized access. Moreover, people pay more and more attention to the protection of private information due to the arising of security awareness. As a result, the security of the image becomes an important issue [1]. For image privacy protection scheme, direct encryption is an effective method to protect image content. At present,

* Corresponding author at: Faculty of Mathematics and Computer Science, Guangdong Ocean University, Zhanjiang 524088, China.
E-mail address: guodongye@hotmail.com (G. Ye).
Peer review under responsibility of Faculty of Engineering, Alexandria University.

https://doi.org/10.1016/j.aej.2021.12.023
1110-0168

researchers and scholars over the world are designing and perfecting different types of image encryption algorithms.

Since the discovery of physical phenomena, namely, chaotic phenomena, chaotic systems and maps are widely used in image encryption [2] due to their ergodicity, unpredictability, randomicity and extreme sensitivity to initial values, etc. Hyperchaotic systems have more complex dynamic characteristics than general chaotic systems, and they are favored by researchers in image encryption [3]. For example, a modular fractional chaotic sine map (MFC-SM) [4] has been designed to achieve a high Lyapunov exponent value with enhanced chaotic behavior compared with other chaotic map. Moreover, NIST tests show that the MFC-SM can display better performance.

Ye et al. [5] proposed an asymmetric image encryption algorithm based on fractional-order chaotic system and RSA public key cryptosystem. Hosny et al. [6] suggested an image encryption algorithm based on hyperchaotic system and Fibonacci Q-matrix. According to the Nyquist theory, in the converting process of the analog information (or digital signal), when the sampling frequency is more than twice of the highest frequency in the signal, the digital signal after being sampled will be able to retain the information in the original signal completely. As to the digital image sampling, there will produce a lot of redundant information.

However, compressive sensing (CS) [7], as a new sampling theory, condition which is much less than Nyquist sampling rate. After obtaining the discrete sample of signal by the random sampling method, the original signal can be reconstructed almost perfectly by using nonlinear reconstruction algorithm or method. Compressive sensing technology tells us: if the sampled signal is sparse or can be sparsed on some basis, then it can be sampled by less than twice the highest frequency of the sampled signal. Moreover, it can restore the original signal in a more ideal from the sampled signal. In the field of image encryption, compressive sensing method has been used to compress images to reduce the encrypted data and speed up the encryption process. For example, Brahim et al. [8] proposed an image encryption algorithm based on compressive sensing and chaotic system. Wang et al. [9] designed a plaintext related image encryption algorithm based on compressive sensing and hyperchaotic system. In [10], an image encryption algorithm based on compressive sensing was presented with random measurement permutation. An improved reconstruction for compressive sensing based ECG acquisition and a compressive sensing framework for heart sound acquisition in Internet of medical things were proposed by Chen et al. [11,12].

Many other encryption algorithms or improved schemes have also been suggested to protect the content of the plain image by directly encrypting the image into meaningless cipher image similar to noise signal. On this basis, with the help of reversible information hiding methods, many researchers began to study how to hide secret plain image into meaningful carrier image so that it cannot be easily detected visually from carrier image, to better promise the security of the images. For example, Yang et al. [13] proposed a universal embedding model (UEM), and further designed a visual meaningful image encryption algorithm based on UEM. The plain image is pre-encrypted and dynamically embedded into the subband of integer wavelet transformation (IWT) for carrier image. An image encryption and hiding algorithm based on compressive sensing and random number insertion was proposed in Reference [14]. With the increase number of images, in order to encrypt secret images efficiently, multi-image encryption algorithm has attracted the attention of the researchers. Multi-image encryption is the combination of multiple images with a synchronous encryption, which makes the encrypted images related to each other, so as to improve the resistance of ciphertext to various attacks and reduce the amount of keys. For example, in order to protect the image content and improve the communication speed over Internet, Zhang et al. [15] presented a novel multi-image encryption algorithm based bit decomposition and DNA coding. By using compressive sensing and Schur decomposition, a multi-image visual meaningful encryption algorithm was designed in Reference [16]. Patro et al. [17] suggested an efficient multi-graph encryption algorithm based on two-level cross-coupled chaotic map.

However, there are still existing some problems in the above mentioned image encryption algorithms, namely: (1) Most multi-image encryption algorithms simply concatenate multiple images together to design encryption, which leads to the problem of increasing image data. (2) Most compressive sensing based single-image encryption methods require transmission of measurement matrix as secret key, which leads to extra transmission. To solve these problems, a double image encryption algorithm based on compressive sensing and public key elliptic curve encryption is designed in this paper. According to the Sprott's three-dimensional chaotic system (Bsys) [18], a new improved three-dimensional continuous chaotic system (ImproBsys) is proposed in this paper. In the process of encryption, two images of the same size are first performed by discrete wavelet transform (DWT), and the adaptive threshold processing is carried out. Then, the Hadamard matrix is selected and determined as measurement matrix according to the random sequence generated by the ImproBsys. Second, the two compressed coefficient matrices are directly spliced together, and then quantized to range of 0–255. Third, a public key elliptic curve encryption algorithm is employed to encrypt the quantized matrix by segments. Finally, the cipher image can be obtained after finish of above processes. In particular, we propose an improved ImproBsys whose number of positive Lyapunov exponent is increased from one to two, so that it has more complex chaotic behavior. In addition, the initial values of ImproBsys are related to the information entropy of the plain image, which further improves the security of the proposed algorithm.

By using the encryptoin algorithm proposed in this paper, one can encrypt two images at the same time, and furthermore let the size of the cipher image be smaller than that of cipher image obtaining form double images directly. Our method can also be extended to multi-image encryption scheme. There are many applications such as medical treatment, camera snap for traffic, and etc. For a specific example, after examining a patient, the doctor may need to send multiple medical images to the patient. So, doctors can simultaneously encrypt multiple medical images and transmit them to patients without the need for multiple times of encryption and transmission for each single image.

The organization of this paper is as follows: Section 2 introduces the related knowledges, including the new 3D hyperchaotic system ImproBsys, compressive sensing, elliptic curve, and Koblitz plaintext coding algorithm. In Section 3, we mainly describe the proposed algorithm and list the detailed steps. The simulation experiments are implemented in Section 4

with some analyses. Section 5 gives the security evaluation with corresponding results. Finally, the summary of whole paper is included in Section 6.

2. The related knowledges

2.1. ImproBsys chaotic system

Nonlinear chaotic systems are often used to produce pseudo-random sequences in the field of digital image encryption due to their distinct characteristics such as nonlinearity, high sensitivity to initial conditions, and etc.. Compared with ordinary chaotic systems, hyperchaotic systems can show more complex behabior (for example, the extension and folding of evolutionary orbits) due to more positive Lyapunov exponents. Moreover, it can produce multiple groups of pseudo-random sequences with good statistical performance simultaneously. Therefore, many imge encryption schemes using hyperchaotic system show better performance.

In Reference [18], Sprott gave some three-dimensional nonlinear chaotic systems, in which one of B series chaotic systems (Bsys) is as follows:

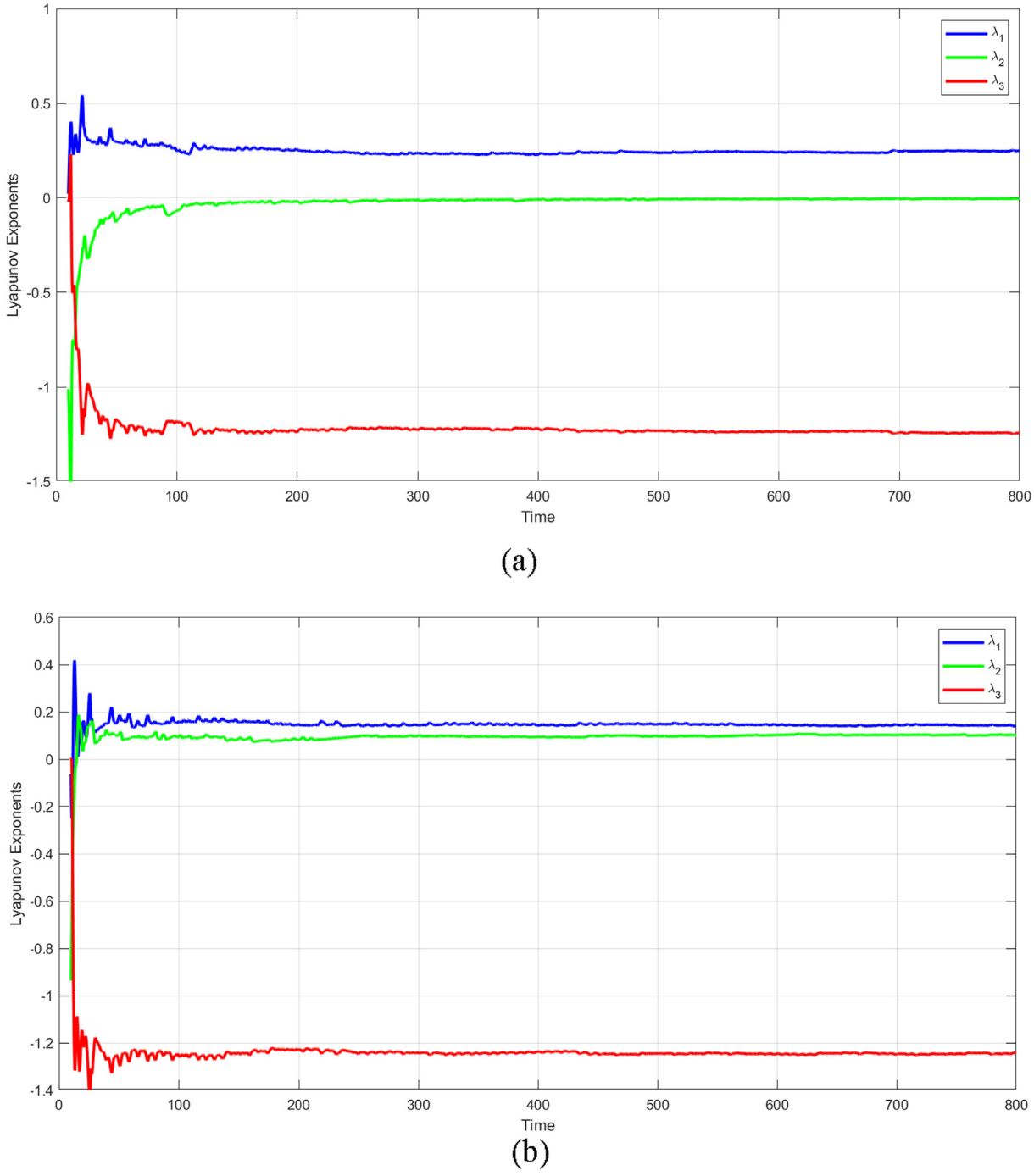

Fig. 1 Lyapunov exponents: (a) Bsys chaotic system, (b) ImproBsys chaotic system.

$$\begin{cases} \dot{x} = yz, \\ \dot{y} = x - y, \\ \dot{z} = 1 - xy, \end{cases} \tag{1}$$

where the Lyapunov exponents [18] of the Bsys chaotic system are: $\lambda_1 = 0.210, \lambda_2 = 0, \lambda_3 = -1.210$ as shown in Fig. 1(a). Based on the Bsys chaotic system, this paper adds a new function to make it become a hyperchaotic system (ImproBsys), as follows:

$$\begin{cases} \dot{x} = ayz, \\ \dot{y} = bx - cy, \\ \dot{z} = d - exy - f(xy), \end{cases} \tag{2}$$

Where
$f(x) = B \cdot sign(x) + B \cdot sign(x - 2A) + B \cdot sign(x + 2A)$,-
$A = 2, B = 0.25, a = 1, \quad b = 1, c = 1, d = 2, e = 1.$ Function $sign(x)$ is as

$$sign(x) = \begin{cases} 1, x > 0 \\ 0, x = 0 \\ -1, x < 0 \end{cases}, \tag{3}$$

where the Lyapunov exponents of the ImproBsys chaotic system are: $\lambda_1 = 0.1549, \lambda_2 = 0.0988, \lambda_3 = -1.2538$ as shown in Fig. 1(b) .

As can be seen from above Fig. 1(b), the ImproBsys chaotic system has two positive Lyapunov exponents. Thus, the ImproBsys chaotic system is a hyperchaotic system. The 3D trajectories of the Bsys chaotic system and the ImproBsys chaotic system are shown in Fig. 2.

2.2. Compressive sensing

Compressive sensing is a new sampling and reconstruction technique. It points out that if a signal is sparse or can be represented in a sparse domain, then the signal can be sampled at a sampling rate much lower than Nyquist's theory, and the original signal can be reconstructed in an ideal case. Suppose the length of the signal X is $N \times 1$, which can be represented by a sparse basis $\Psi$with size $N \times M$as follows:

$$X = \psi \times S, \tag{4}$$

where S is called the sparse representation on X. The signal S can be measured by a measurement matrix ϕ with size $H \times M$ as follows:

$$Y = \phi \times X = \phi \times \psi \times S = \theta \times S, \tag{5}$$

where $Y$is the compressed signal with size $H \times 1 (H < N)$. $\theta = \phi \times \Psi$ is called the measurement matrix.

In this paper, the image is first excuted by three layer of discrete wavelet transform (DWT) to get wavelet coefficients. Then, all the wavelet coefficients are thresholded. Before using the compressive sensing technology, suppose that the length of signal is n, which has r non-zero elements. Assume that the compression ratio $m \geqslant 4r$ is required to compress the signal to the length $m (m < n)$. In the proposed algorithm, the wavelet coefficient matrix is compressed to half of the original one, i.e., $m = n/2$, that is to say, $r \leqslant m/8$. So, about 88% of the wavelet coefficients need to be set to zero. After a number of tests, it is found that if 85% of the values in the wavelet coefficient matrix are set to zero, then it can reach the best effect. Thus, the wavelet coefficient matrix will become sparse after a threshold process. Finally, according to the pseudo random sequences generated by the ImproBsys chaotic system, some rows of the Hadamard matrix are selected to produce measurement matrix. Then, the sparse wavelet coefficient matrix is compressed. The detail steps will be described in the encryption algorithm.

2.3. Elliptic curve

Public Key (asymmetric) cryptography is an important part of technologies modern encryption and advanced signature. It can effectively avoid the problems of key management and distribution found in a symmetric cryptography. Among them, elliptic curve cryptography (ECC) is a classical public key cryptosystem based on finite field, which is defined as follows:

Definition: Let F_p denotes the field of prime numbers. The elliptic curve over it is defined as:

$$E : y^2 \equiv x^3 + ax + b (\ mod\ p), \tag{6}$$

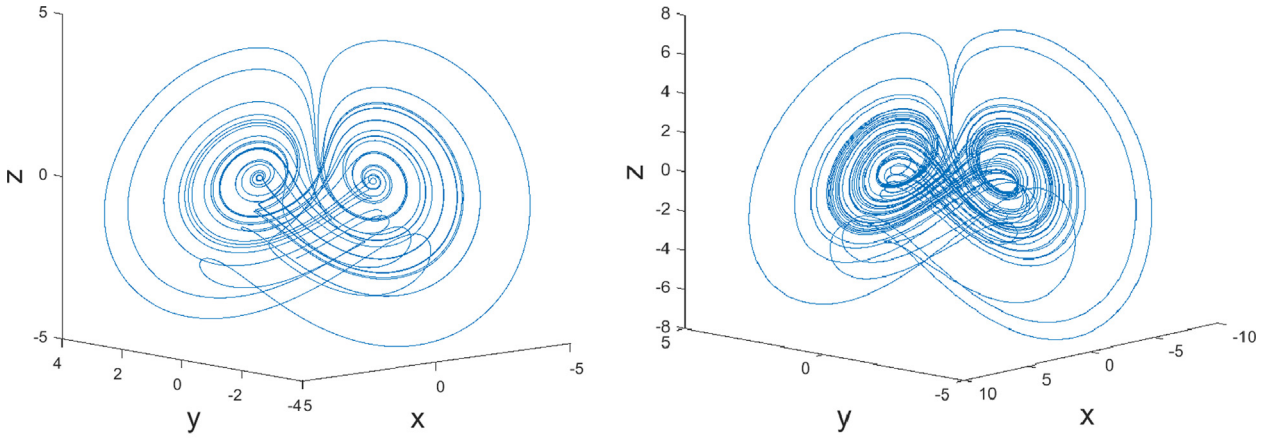

Fig. 2 The 3D trajectories of: (a) Bsys chaotic system, (b) ImproBsys chaotic system.

where $a, b \in F_p, p \neq 2, 3,\ 4a^3 + 27b^2 \neq 0$. A group of elliptic curves $E(F_p)$ represent the points that satisfy the elliptic curve equation (6) and a set of special points at infinity.

Elliptic curve cryptography: The encryption process based on elliptic curve is as following:

1) User A: choose a elliptic curve $E_p(a, b)$, and set a point Gas basis point in the curve.
2) User A: select a private key k, and compute public key $K = kG$.
3) User A: send $E_p(a, b)$,K and$G$to User B.
4) User B: encode a plain message m to a point M on the curve $E_p(a, b)$. Then, generate a random number $r(r < n)$, where n is the order of point G.
5) User B: compute cipher messages $C1 = M + rK$and $C2 = rG$.
6) User B: send $C1$and $C2$to User A.
7) User A: recover point $M = C1 - kC2$, and then decode Minto a plain message m.

2.4. Koblitz encoding algorithm

Operations of elliptic curve cryptography are performed on a discrete set of points, but the plain messages may not be the points on the elliptic curve. Therefore, these plain messages need to be encoded into points on the elliptic curve. In the proposed algorithm, Koblitz encoding algorithm [19] is employed to complete these processes as following:

Given an elliptic curve $E : y^2 \equiv x^3 + ax + b \bmod p$, suppose the plain message is $m(0 \leqslant m \leqslant p/1000 - 1)$, where $p$is a decimal number. Compute $x_j = 1000m + j$, and$s_j \equiv x_j^3 + ax_j + b \bmod p$. If $s_j^{(p-1)/2} \equiv 1 \bmod p$, then we get$y_j = s_j^{(p+1)/4} \bmod p$. So, the encoding result of the plain message $m$is $M_m = (x_j, y_j)$. The decoding can be easy obtained by $m = \lfloor x_j/1000 \rfloor$to get the plain message m.

3. The proposed algorithm

3.1. The encryption process

This algorithm takes the encryption of two plain images as an example. Other cases can be similarly extended. By using discrete wavelet transform, compressive sensing, elliptic curve cryptography, and ImproBsys chaotic system, the proposed image encryption algorithm is designed as follows:

Step 1: Given two plain images D and $F$with size $H \times L$. Do a three-layer discrete wavelet transform on each of them. Suppose the wavelet coefficient matrices are J and I for the images$D$and F respectively.

Step 2: Take the absolute values for all elements of the wavelet coefficient matrix J to get matrix N. Then, the elements of the matrix N are sorted in descending order to get an array O, in which the same numbers are arranged together. To speed up, we just sort the first 15% of the data. Therefore, for an image size of $H \times L$, only the first $index = \lfloor H \times L \times 15\% \rfloor$ numbers need to be excluded. Let $threshold = O_{index}$, and set the elements in matrix J less than$threshold = O_{index}$ by the absolute operation to be zeros, assuming that matrix Q is obtained. The operation can be seen as follows:

$$Q_{ij} = \begin{cases} 0, |J_{ij}| < threshold \\ J_{ij}, |J_{ij}| \geqslant threshold \end{cases}, i = 1, 2, 3, \cdots H, j = 1, 2, 3, \cdots L. \tag{7}$$

Step 3: Similarly, do the same operation to the matrix I, assuming that matrix R is got.

Step 4: Use the ImproBsys chaotic system to generate a chaotic sequence S of length$H$, where, the three initial values are calculated by the following formula:

$$\begin{cases} x_0 = ((entropy(D) \times 10^{10}) \bmod 1 + 0.36255) \bmod 1 \\ y_0 = ((entropy(F) \times 10^{10}) \bmod 1 + 0.45368) \bmod 1\ . \\ z_0 = (x_0 + y_0 + 0.24142) \bmod 1 \end{cases} \tag{8}$$

Then, sort the above chaotic sequence to get an index sequence T whose length is equal to the number of rows in the image. Generate a Hadamard matrix $U$of size $H \times H$, and select $\lfloor H/2 \rfloor$ row from it to get a matrix V according to the index T as follows:

$$[\sim, T] = sort(S). \tag{9}$$

$$V = U(T(1 : H/2), T(1 : H)). \tag{10}$$

Step 5: Do multiplication operation for matrix Q and $R$by matrix V to get matrix W and X respectively, i.e., $W = V \times Q$, $X = V \times R$. So, both the size of W and X are $\frac{H}{2} \times L$. These matrices are spliced together to get a new matrix Y of $H \times L$.

Step 6: Quantize the elements of matrix Yinto 0–255 to get a matrix Zas:

$$\max = \max(Y). \tag{11}$$

$$\min = \min(Y). \tag{12}$$

$$Z_{ij} = round\left(255 \times \frac{Y_{ij} - \min}{\max - \min}\right), i = 1, 2, 3, \cdots H, j = 1, 2, 3, \cdots L. \tag{13}$$

Step 7: Select a and b satisfying $4a^3 + 27b^2 \neq 0$ according to elliptic curve$E : y^2 \equiv x^3 + ax + b \bmod p$. In this paper, a, b, p , and $G$are randomly set for test as:

$$a = \text{0x6d810ae8c2030466cb34cdb4ffb217b6602907c6f796 babaa31779f63ae463f340f14ecd122f94e7954a9c30182ab6 7d5bc6edd7fe5a3ea17b049247df31677d}$$

$$b = \text{0xcabc0e234da7f5d463245eb897ab4c246f318070c945 e89388c54b6f919a6800bb8bcded7fccb5f606fd41672b0fe3 67ad248db5d2bc2e8a0be4b1bdbf4dc4c1}$$

$$p = \text{0xffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffd8b}$$

$$G = \begin{pmatrix} \text{0xfea5fc3133202229bfa892104086b8e0fc4c07860} \\ \text{5c76905cd0855fe36327648b5f9b7e2e86b177c61e} \\ \text{77f891798a38e46bd4ae56f4662ce45fb22d16ae4fa} \\ \text{d6,} \\ \text{0xbb425c21989cba9c288fd9022968fe4f54c85a33} \\ \text{535332c328ec804c83c51aac855bd62730e1b6381} \\ \text{e2caf63430662ce5e60746c6195b7adc7118fb6b40} \\ \text{75782} \end{pmatrix}$$

Step 8: Expand the matrix Z into a one-dimensional array ZZ of hexadecimal, and do encryption for it by segment. The length of hexadecimal number is 126 bits for $p/1000-1$. In order to satisfy$0 \leqslant m < p/1000-1$, and reduce the number of encryption, the size of the plain message is set to be 125-bit hexadecimal number, that is, the array $ZZ$is divided into 125-bit hexadecimal numbers and then encrypted. If it is not equal to 125 bits, then do encryption directly for it.

Notes: The cipher pixel after being encoded from the plain pixel is a point on the elliptic curve, but its ordinate can be calculated from the abscissa, so just save the abscissa. The maximum length converted from abscissa to hexadecimal number is 128 bits. Because the length of $p$is 128 bits in hexadecimal number, the result of the modular operation under p will not exceed the length of p. However, the length of the abscissa is sometimes less than 128 bits, so we should add some zeros to the left of the abscissa that is less than 128 bits until the length is 128 bits. The abscissa of all the encrypted points is concatenated to form a cipher pixel. According to the elliptic curve encryption algorithm, the sender needs to transfer two numbers, i.e., $C1$ and $C2$. To reduce the amount of data transmitted, the random number r is set unchanged, therefore, $C2$ will be kept unchanged. Thus, only one time of it need be transmitted.

Step 9: After doing elliptic curve encryption, the row number of the cipher image is slightly larger. In order to decrypt the cipher image more convenient, its column number is kept the same as that of the plain image, and the row number is increased appropriately. Random numbers can be filled at the end of row when the data is not enough. To distinguish between the length of the filled random numbers and the length of the cipher pixel segment, the filled random number combination may not be the abscissa of a point on the elliptic curve. If it is, regenerate again the random numbers. When doing decryption, the cipher image is taken out for inverse operation at intervals of length p.

Step 10: The maximum and the minimum of the matrix Q are needed when doing Quantitation, and so we need both of them in decryption process. In addition, the three initial values are also required for decryption. So, do encryption for these values, and splice together with $C2$. Then they are sent to the receiver [20]. Finally, the transmission mechanism based on public key cryptography can be finished.

3.2. Decryption process

The decryption process is the inverse of the encryption process. Firstly, the cipher image is decrypted by the elliptic curve decryption method to get the compressed image matrix. Then, the two image coefficients are divided into two matrices and reconstructed separately. Finally, the two original plain images can be recovered by using discrete wavelet transform.

4. Simulation results

4.1. Experiment platform

To show the encryption and decryption performances by our method, a computer with platform of Intel i5-2430 M, CPU 2.40 GHz, memory 10 GB, and 64-bit operating system on Windows 7 is selected to do the tests by software MATLAB R2019A.

4.2. Experiment results

Images Peppers, House, Parrots, Barbara, Girlface, and Woman are randomly selected for tests, in which the size of four former images is256×256, and the remaining is 512×512. The parameters are follows:

r = 3546764,

k = 787722005427174492828311566010300241982199441704363091545958188237062144924 00.

By taking 5 bits after point, the initial values for Fig. 3(a) and 3(b) are:x_0 = 0.34668, $y_0 = 0.91312$, $z_0 = 0.25980$. The initial values for Fig. 3(d) and 3(e) are: $x_0 = 0.22535$, $y_0 = 0.48551$, $z_0 = 0.71086$. The initial values for Fig. 3(g) and 3(h) are: $x_0 = 0.38899$, $y_0 = 0.11107$, $z_0 = 0.50006$. All the tests are shown in Fig. 3.

Therefore, from the above test results, the size of the cipher image after compressing two plain images has not changed much compared with that of plain image. So, the algorithm can save about half of the data transmission. Fig. 4 shows the recovery effect when the cipher image is decrypted. We

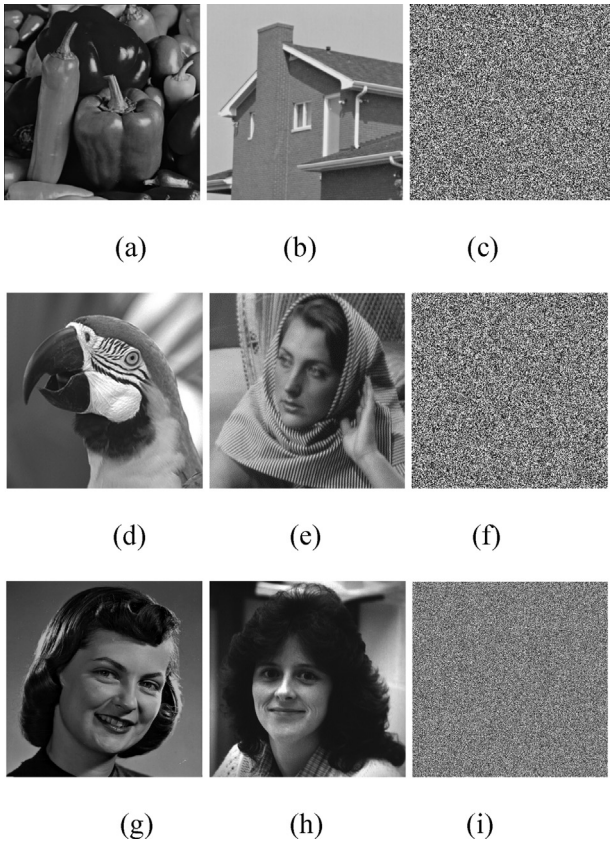

Fig. 3 Tests for encryption: (a) plain image Peppers, (b) plain image House, (c) cipher image (263×256) generated by Peppers and House, (d) plain image Parrots, (e) plain image Barbara, (f) cipher image (263×256) generated by Parrots and Barbara, (g) plain image Girlface,(h) plain image Woman,(i) cipher image (525×512) generated by Girlface and Woman.

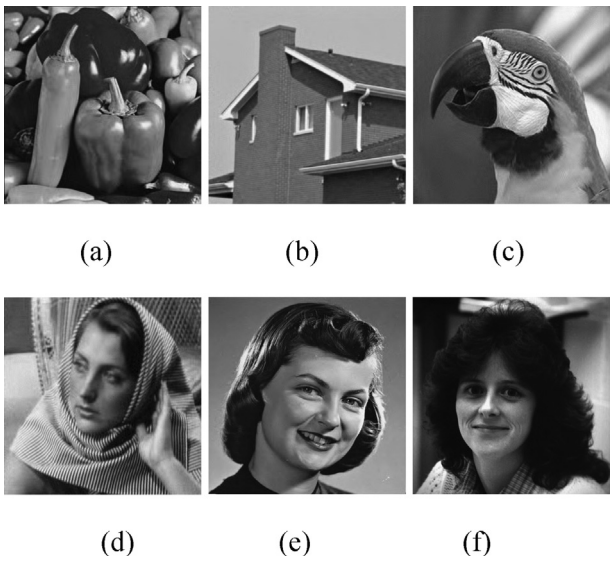

Fig. 4 Decryption: (a) recovered image Peppers, (b) recovered image House, (c) recovered image Parrots, (d) recovered image Barbara, (e) recovered image Girlface, (f) recovered image Woman.

can see that the proposed algorithm can preserve the structure of the plain image well.

4.3. Evaluation of the reconstruction

(1) Peak signal-to-noise ratio

The larger the peak signal-to-noise ratio (PSNR) value is, the smaller the difference is. A PSNR value above 40 dB indicates excellent image quality, a range of 30–40 dB indicates good image quality, a range of 20–30 dB indicates mediocre image quality, and a value below 20 dB indicates poor and unacceptable image quality. Assume that the plain image is P of size $M \times N$and the restored image is C. The PSNR formula for them is as follows:

$$PSNR = 10\log_{10}\left[\frac{255^2}{\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[P(i,j) - C(i,j)]^2}\right] \tag{14}$$

(2) Structural similarity

Structural similarity (SSIM) is a measurement of the brightness, contrast, and structural similarity of an image. The range of SSIM values is [0,1]. The larger the value is, the higher the similarity is. Given two images $P$and Q, the SSIM is calculated as follows:

$$SSIM = \frac{(2\mu_P\mu_Q + c_1)(2\rho_{PQ} + c_2)}{\left(\mu_P^2 + \mu_Q^2 + c_1\right)\left(\rho_P^2 + \rho_Q^2 + c_2\right)}, \tag{15}$$

where $\mu_P$is the mean value for P. μ_Q is the mean value for Q. ρ_P^2 is the variance for P. ρ_Q^2 is the variance for Q. ρ_{PQ} is the covariance for P and Q. $c_1 = (k_1L)^2$and $c_2 = (k_2L)^2$ are constants sused to maintain stability. L is the dynamic range of pixel values. For a gray image, the values are $L = 255$, $k_1 = 0.01$, and $k_2 = 0.03$.

The PSNR and SSIM values of the tested images are shown in Table 1 by using the proposed image encryption algorithm. Thus, it can be seen that the method in this paper has a good effect.

5. Security analyses

5.1. Key space analysis

A key space is a collection of all possible keys used in an encryption algorithm. If the key space of an encryption algorithm is too small, the attacker can use brute-force attack to crack the encryption algorithm. The elliptic curve discrete logarithm problem is an exponential problem. This paper adopts 512-bit elliptic curve parameters. Therefore, it needs a lot of computation to use exhaustive attack to crack the algorithm. One of the most famous attacks on elliptic curve cryptography is Pollard's Rho attack [21], which is a probabilistic solution requiring $\sqrt{n}$steps of computation, in which n is the number of cycles of the elliptic curve equation. For a 512-bit elliptic curve, $\sqrt{n} = 9.4599 \times 10^{79}$steps are needed, which is very difficult to find a probabilistic solution. Therefore, the image encryption algorithm proposed in this paper has enough ability to resist exhaustive attack.

5.2. Histogram analysis

Histograms are commonly used to represent the overall distribution of pixel values in an image. In general, the histogram of a natural meaningful image has obvious statistical characteristics. If the encryption algorithm works well, then the histogram of the cipher image should be evenly distributed. As shown in Fig. 5, it is clear that the histogram of the cipher image is evenly distributed. In other words, if an attacker obtains a cipher image, he or she can not obtain any original information about the plain image.

5.3. Correlation coefficient analysis

In general, the adjacent pixels (horizontal, vertical and diagonal) of a natural plain image have strong correlation. In order to protect the cipher image information more effectively, any new proposed image encryption algorithm must destroy completely the correlation among these pixels. If the correlation coefficient of the adjacent pixels in the cipher image is lower, that is, tends to zero, the better the performance of the algorithm is, and the better the effect of resisting the statistical attack is. The correlation coefficient is calculated as follows:

Table 1 Tests for PSNR and SSIM.

Images	Size	PSNR	SSIM
Peppers	256 × 256	37.5465	0.9478
House	256 × 256	37.6543	0.9356
Parrots	256 × 256	37.3141	0.9376
Barbara	256 × 256	35.2313	0.9456
Girlface	512 × 512	38.4312	0.9476
Woman	512 × 512	42.1324	0.9743

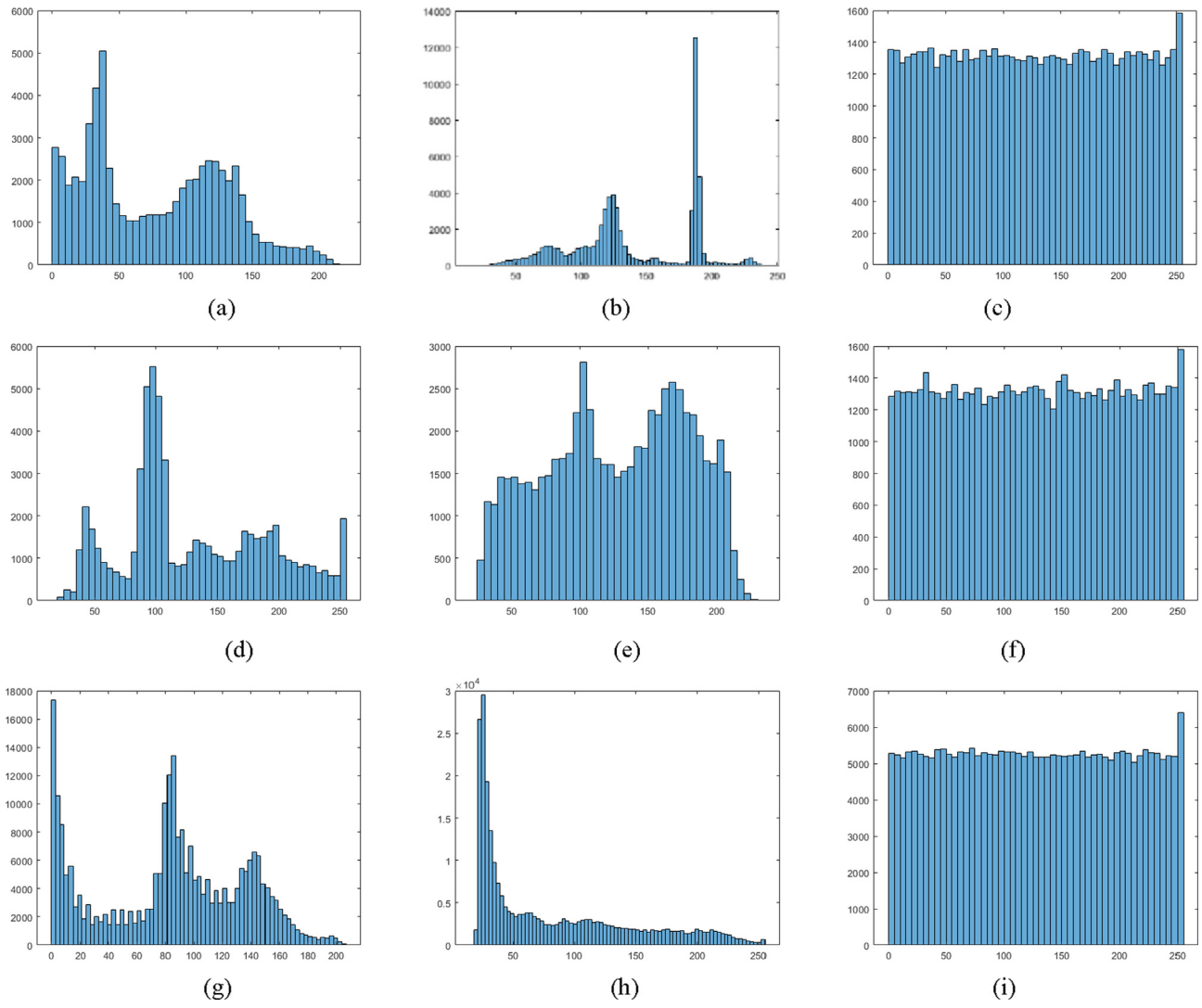

Fig. 5 Histogram tests: (a) plain image Peppers, (b) plain image House, (c) cipher image generated from Peppers and House, (d) plain image Parrots, (e) plain image Barbara, (f) cipher image generated from Parrots and Barbara, (g) plain image Girlface, (h) plain image Woman, (i) cipher image generated from Girlface and Woman.

$$R_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{16}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \tag{17}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i, \tag{18}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2, \tag{19}$$

where R_{xy} is the correlation coefficient, while N is the number of adjacent pixels selected from the image. In this paper, 10,000 pairs of pixels from the horizontal, vertical, and diagonal directions of the plain and the cipher images are selected randomly, with corresponding results shown in Fig. 6. Therefore, the correlation coefficient of the cipher image is much weaker than that of the plain image. Table 2 lists the correlation coefficients in the three directions of the test images. That is, the correlation coefficient of the plain image is close to 1, while that of the cipher image is close to 0. This shows that the proposed encryption algorithm can eliminate the correlation between pixels, making the pixel arrangement of the cipher image more random.

5.4. Sensitivity of plaintext

For an ideal encryption algorithm, if it has strong sensitivity to plaintext, then, the more robust the algorithm is to resist differential attack. Typically measured by pixel rate of change (NPCR) and uniform mean change intensity (UACI) are defined as:

$$NPCR = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j) \times 100\%, \tag{20}$$

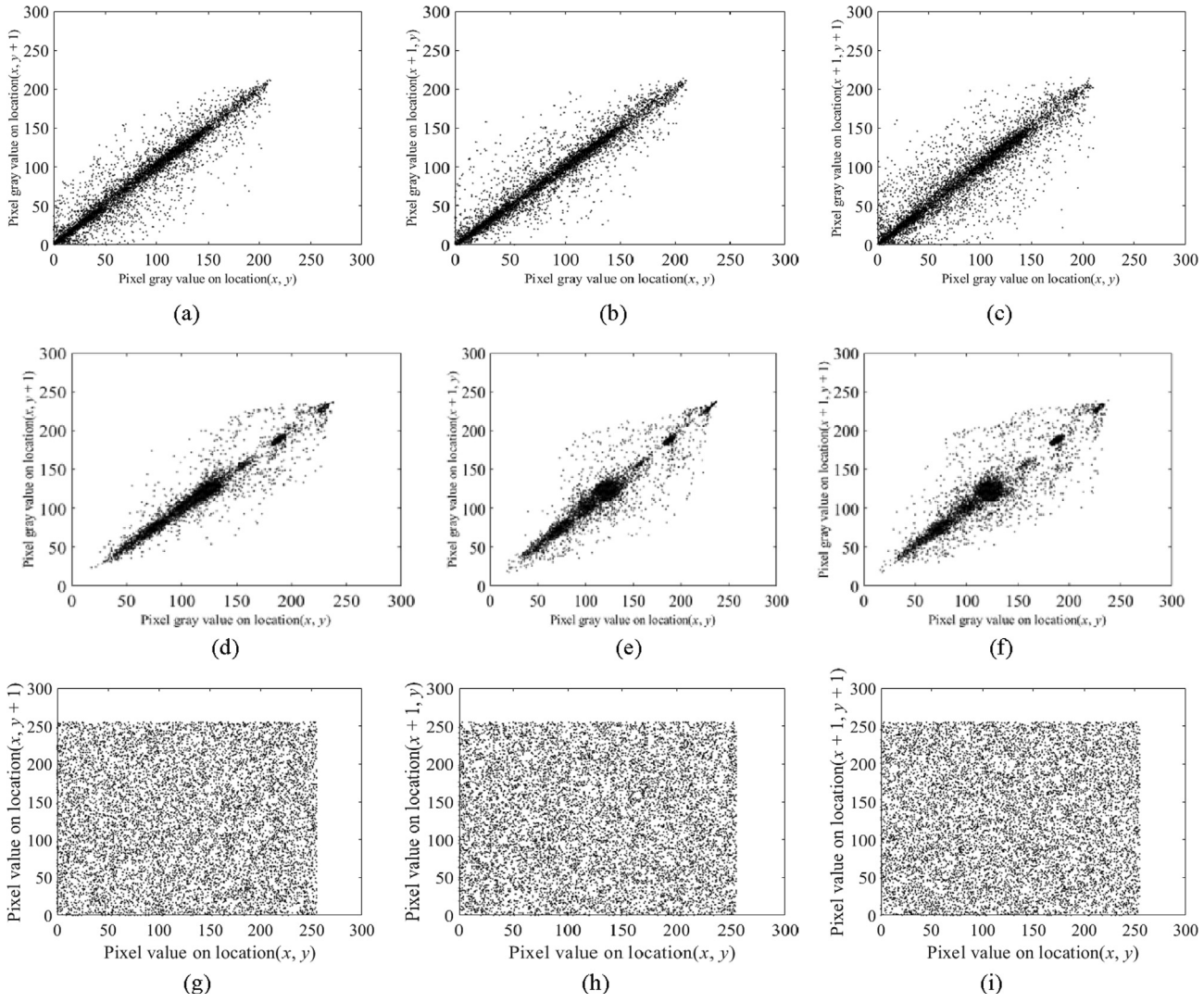

Fig. 6 Tests for correlation to image: Peppers: (a) horizontally, (b) vertically, (c) diagonally; House: (d) horizontally, (e) vertically, (f) diagonally; Cipher image: (g) horizontally, (h) vertically, (i) diagonally.

Table 2 Correlation coefficients for different images.

Images	Horizontally	Vertically	Diagonally
Peppers	0.9719	0.9687	0.9488
House	0.9664	0.9780	0.9484
Cipher image of Peppers and House	0.0040	−0.0044	−0.0012
Parrots	0.9646	0.9717	0.9501
Barbara	0.9693	0.8971	0.8487
Cipher image of Parrots and Barbara	0.0070	−0.0193	0.0031
Girlface	0.9873	0.9846	0.9725
Woman	0.9972	0.9968	0.9947
Cipher image of Girlface and Woman	0.0043	−0.0118	−0.0116

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%, \tag{21}$$

where $C_1(i,j)$ and $C_2(i,j)$ are the pixels for two cipher images C_1 and C_2respectively at the point (i,j). If $C_1(i,j) = C_2(i,j)$, then $D(i,j) = 0$, otherwise, $D(i,j) = 1$. The

Table 3 Plaintext sensitivity tests.

Images	Size	PSNR	UACI
Peppers	256 × 256	99.5424%	33.5112%
House	256 × 256	99.6546%	33.5341%
Parrots	256 × 256	99.5552%	33.5423%
Barbara	256 × 256	99.6768%	33.5312%
Girlface	512 × 512	99.6754%	33.5432%
Woman	512 × 512	99.6354%	33.5141%

Table 4 Tests of information entropy.

Images	Size	Information entropy
Peppers	256 × 256	7.3613
House	256 × 256	6.4971
Cipher image of Peppers and House	263 × 256	7.9976
Parrots	256 × 256	7.4141
Barbara	256 × 256	7.5252
Cipher image of Parrots and Barbara	263 × 256	7.9974
Girlface	512 × 512	7.8018
Woman	512 × 512	7.0879
Cipher image of Girlface and Woman	525 × 512	7.9993

Table 5 Comparisons of PSNR.

Methods	Image size	PSNR
Ref [22]	256 × 256	29.8300
Ref [23]	512 × 512	32.9660
Proposed work	256 × 256	33.2542
Proposed work	512 × 512	37.0534

theoretical values of NPCR and UACI are 99.6094% and 33.4635%, respectively. Table 3 presents the results of NPCR and UACI tests for one-bit difference in the same plain image. One can see that the proposed algorithm has a strong ability to resist the differential attack.

5.5. *Information entropy*

It is well known that the greater the information entropy of an image is, the more uniform and random the distribution of pixels will be. Table 4 shows the results of the information entropy test. From values in Table 4, the information entropy of the cipher image is closer to the theoretical value of 8. So, the algorithm in this paper can show good randomness and high security for images.

5.6. *Comparisons*

This algorithm is proposed based on compressive sensing technology, so the quality of restored image is an important issue to measure the performance. The compression ratio is set to 0.5 in this paper. So, compared with the same compression ratio of encryption algorithm with image Lena of size 256×256 and 512×512, the comparison results of PSNR are shown in Table 5. Thus, the scheme designed in this paper has a good recovery effect.

6. Conclusions

With the rapid increase of image transmission data, the security of image transmission faces many difficulties and challenges, and multi-image encryption is one of good solutions. By encrypting multiple images at the same time, the amount of used key is reduced and the ability of resisting various attacks is increased. In this paper, a new chaotic system ImproBsys was designed, which has hyperchaotic behavior. The plain image is compressed by compressive sensing, and then the compressed image is encrypted by public key elliptic curve encryption algorithm to improve the security level. By using the proposed method, the data volume and transmission volume of multi-image encryption can be effectively reduced, and the majority of the advantages of multi-image encryption can be maintained. Furthermore, the public key elliptic curve cryptography makes the security of the image based on the more rigorous discrete logarithm difficulty. The analysis and test results also showed that the proposed method has high security and recovery effect. At the same time, the method is illustrated with two images, and can be extended to more than one image. Of course, there is a certain impact on the image restoration effect if we encrypt more images considering compression ratio.

In the future work, we will continue to study and improve the encryption scheme of more images, and expect to have better results. Moreover, the technology of the reversible information hiding for image can supply another way to protect the communicated images. The principal principle is to hide a secret image into a carrier image. We suppose to do the encryption first for the plain image, and then insert it into a meaningful carrier image. The attackers cannot perceive directly the existing secrets from a meaningful carrier image so as to improve furthermore the security.

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.

Acknowledgments

The authors would like to thank the anonymous reviewers for their valuable comments and the editor's helpful suggestions. This work was supported in part by the National Natural Science Foundation of China (No.61972103), the Natural Science Foundation of Guangdong Province of China (No.2019A1515011361), and the Key Scientific Research Project of Education Department of Guangdong Province of China (No.2020ZDZX3064).

References

[1] G. Ye, K. Jiao, X. Huang, Quantum logistic image encryption algorithm based on SHA-3 and RSA, Nonlinear Dyn. 104 (3) (2021) 2807–2827.
[2] N.R. Zhou, L.X. Huang, L.H. Gong, Q.W. Zeng, Novel quantum image compression and encryption algorithm based on DQWT and 3D hyper-chaotic Henon map, Quantum Inf. Process., 19(9)(2020) 284.
[3] H.M. Ghadirli, A. Nodehi, R. Enayatifar, An overview of encryption algorithms in color images, Signal Process. 164 (2019) 163–185.
[4] A. Kamal, E. Hagras, H.A. El-Kamchochi, Dynamic fractional chaotic biometric isomorphic elliptic curve for partial image encryption, Comput. Sci. Inf. Syst. 18 (3) (2021) 1057–1076.

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

[6] K.M. Hosny, S.T. Kamal, M.M. Darwish, G.A. Papakostas, New image encryption algorithm using hyperchaotic system and fibonacci Q-matrix, Electronics 10 (9) (2021) 1066.

[7] E.J. Candes, M.B. Wakin, An introduction to compressive sampling, IEEE Signal Process. Mag. 25 (2) (2008) 21–30.

[8] A.H. Brahim, A.A. Pacha, N.H. Said, Image encryption based on compressive sensing and chaos systems, Opt. Laser Technol. 132 (2020) 106489.

[9] W. Xiao-Qing, Z. Hao, S. Yu-Jie, W. Xing-Yuan, A plaintext-related image encryption algorithm based on compressive sensing and a novel hyperchaotic system, Int. J. Bifurcat. Chaos 31 (02) (2021) 2150021, https://doi.org/10.1142/S0218127421500218.

[10] Y. Li, B. Song, R. Cao, Y. Zhang, H. Qin, Image encryption based on compressive sensing and scrambled index for secure multimedia transmission, ACM Trans. Multimedia Comput. Commun. Appl. 12 (4s) (2016) 1–22.

[11] J. Chen, S. Sun, N. Bao, Z. Zhu, L.-B. Zhang, Improved reconstruction for CS based ECG acquisition in internet of medical things, IEEE Sens. J. 21 (22) (2021) 25222–25233, https://doi.org/10.1109/JSEN.2021.3055635.

[12] J. Chen, S. Sun, L.-b. Zhang, B. Yang, W. Wang, Compressed sensing framework for heart sound acquisition in internet of medical things, IEEE Trans. Industr. Inform. 18 (3) (2022) 2000–2009, https://doi.org/10.1109/TII.2021.3088465.

[13] Y.G. Yang, B.P. Wang, Y.L. Yang, Y.H. Zhou, W.M. Shi, X. Liao, Visually meaningful image encryption based on universal embedding model, Inf. Sci. 562 (2021) 304–324.

[14] G.D. Ye, C. Pan, Y.X. Dong, Y. Shi, X.L. Huang, Image encryption and hiding algorithm based on compressive sensing and random numbers insertion, Signal Process. 172 (2020) 107563.

[15] Q.Y. Zhang, J.T. Han, Y.T. Ye, Multi-image encryption algorithm based on image hash, bit-plane decomposition and dynamic DNA coding, IET Image Process. 15 (4) (2021) 885–896.

[16] G. Ye, C. Pan, Y. Dong, K. Jiao, X. Huang, A novel multi-image visually meaningful encryption algorithm based on compressive sensing and Schur decomposition, Trans. Emerg. Telecommun. Technol. 32 (2) (2021), https://doi.org/10.1002/ett.v32.210.1002/ett.4071.

[17] K.A.K. Patro, B. Acharya, An efficient dual-layer cross-coupled chaotic map security-based multi-image encryption system, Nonlinear Dyn. 104 (2021) 2759–2805.

[18] J.C. Sprott, Some simple chaotic flows, Phys. Rev. E 50 (2) (1994) R647–R650.

[19] N. Koblitz, Elliptic curve cryptosystems, Math. Comput. 48 (177) (1987) 203–209.

[20] M.S. Khoirom, D.S. Laiphrakpam, T. Tuithung, Audio encryption using ameliorated ElGamal public key encryption over finite field, Wirel. Pers. Commun. 117 (2) (2021) 809–823.

[21] J.M. Pollard, Monte Carlo methods for index computation (mod p), Math. Comput. 32 (143) (1978) 918–924.

[22] X.L. Chai, H.Y. Wu, Z.H. Gan, Y.S. Zhang, Y.R. Chen, K.M. Nixon, An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding, Opt. Lasers Eng. 124 (2020) 105837.

[23] Z. Gan, X. Chai, J. Zhang, Y. Zhang, Y. Chen, An effective image compression-encryption scheme based on compressive sensing (CS) and game of life (GOL), Neural. Comput. Appl. 32 (17) (2020) 14113–14141.