

Full length article

Secure image encryption scheme using double random-phase encoding and compressed sensing

Kanglei Zhou^{a,b}, Jingjing Fan^c, Haiju Fan^{a,b}, Ming Li^{a,b,*}^a College of Computer and Information Engineering, Henan Normal University, Xixiang 453007, China^b Big Data Engineering Laboratory for Teaching Resources & assessment of Education Quality, Henan Province, China^c Department of Mathematics, University of Hong Kong, 999077, Hong Kong, China

HIGHLIGHTS

- DPCS is combined with CS to achieve secure image encryption.
- The cipher image can be authenticated blindly.
- Signal processing at the speed of light when sampling.

ARTICLE INFO

Keywords:

Encryption
Authentication
Double random-phase encoding
Compressed sensing

ABSTRACT

A secure optical digital image encryption scheme with authentication capability is proposed using double random-phase encoding (DRPE) and compressed sensing (CS). Phase information of the plaintext image is obtained using DRPE and quantized to generate authentication information. Simultaneously, the plaintext image is compressed by CS and its measurements are quantized using the sigmoid map. Then the ciphertext image is obtained by permutation and diffusion after authentication information is embedded in quantified measurements. At receiving end, the authentication information is first extracted by inverse permutation and diffusion, and then the authentication image is obtained by inverse DRPE. Finally, the ciphertext image can be blindly authenticated using a nonlinear cross-correlation method with authentication image and reconstructed image. Experimental results demonstrate the effectiveness of our proposed scheme.

1. Introduction

With the ultra-fast development of information technology and the increasing amount of information interaction, the integrity, confidentiality, security and other issues of information are increasingly prominent [1–3]. Information security and protection technology research cannot be ignored and play an important role in many fields such as military, medical, and cloud-computing [4–6]. To ensure the security of information, some ways must be taken to protect it, and the most effective way to hide information is encryption. Digital images are frequently used in daily life because they can vividly and intuitively present information, which carry so much data that the traditional information encryption method cannot meet the processing speed [7–9]. However, the image information security system based on optical has attracted extensive attention of scholars because of its unique characteristics such as multiple-dimensional, parallel processing of data and low cost. Recently, many optical image encryption and authentication

algorithms [10–22] have been proposed and studied. In our study, we focused on the image encryption scheme with authentication capability based on optical information hiding techniques. Information hiding as a novel steganography technique is very different from traditional encryption scheme, which not only hides the content of secret information, but also the existence [23].

Double random-phase encoding (DRPE) as an optical encoding method was first developed by Refregier et al. [24], which has been widely applied in image encryption and authentication. After the input image is encoded using two relatively independent random phases, the encoded image has better security and robustness due to its white noise characteristic. Furthermore, DRPE technique is successfully integrated with other classic optical information processing technologies such as optical image encryption schemes and authentication algorithms by Fourier transform domain expansion to Fresnel transform domain, wavelet transform domain, Gyrator transform domain and other transform domains [15,19,25–30]. At the same time, iterative phase

* Corresponding author.

E-mail address: liming@htu.edu.cn (M. Li).<https://doi.org/10.1016/j.optlastec.2019.105769>

Received 23 May 2019; Received in revised form 21 July 2019; Accepted 16 August 2019

Available online 24 August 2019

0030-3992/ © 2019 Elsevier Ltd. All rights reserved.

recovery algorithm, phase truncation and other new encryption techniques derived from DRPE are also universally promoted and applied in practice. In [10–12], DRPE technology is combined with photon counting imaging technology using sparse complex information in order to achieve the secure image authentication based a statistical nonlinear correlation approach. Due to the phase information generated by DRPE for image authentication requires small storage space, it is favored by some researchers [15,27–29]. In [29], to reduce the cost of data storage and enhance the image compression and data transmission, only part of phase information is retained, while all amplitude information is discarded. In [16–18], some optical encryption schemes combined DRPE with compressed sensing (CS) are proposed. In [16], the plaintext image is encrypted twice into the ciphertext image through CS and DRPE, respectively, which dramatically reduces its key space.

Indeed, CS is successfully utilized in image encryption because it can reduce the storage space to a great extent and reconstruct the original information from a small number of measurements [31]. If the original signal is sparse in a transform domain, an observation matrix can be used to project the transformed high-dimension signal onto the low-dimension [32–34]. Moreover, CS is difficult to be attacked due to the problems such as large amount of calculation, low efficiency and uncontrollable process, which is still of research significance for image encryption. Recently, many secure image encryption schemes based on CS are proposed [16–18,35,36]. In [35], Chai et al. proposed an encryption scheme based on CS whose measurement matrix is generated by the chaotic system. In [36], Fan et al. combined CS and vector quantization to achieve high compression rate and accurate restoration. Although traditional CS encryption cannot provide the capability of authentication, CS can make room for authentication information. Therefore, we design a novel secure image encryption scheme based on CS and DRPE, in which DRPE is be used to achieve the authentication capability.

In our image encryption scheme, the input image is first encoded into authentication information by DRPE and simultaneously compressed by CS. Then, the measurements are embedded in the authentication information after being quantified. Finally, the fusion image is permuted and diffused into the cipher image. In the receiving end, the receiver can authenticate the reconstructed image according to the extracted authentication information by an advanced statistical nonlinear cross-correlation method. However, the ciphertext image may be disturbed or maliciously tampered during the transmission. The experimental results show that the proposed encryption scheme can successfully authenticate whether the transmitted images are available. Therefore, the main contributions of this paper are as follows: (1) DRPE and CS realize signal processing at the speed of light when sampling, so our proposed encryption system constitutes a large optical transformation system with fast and efficient characteristics. (2) By sampling, a self-embedding image signal with authentication capability can be obtained directly, which is superior to conventional image authentication and CS.

The remaining of this paper is presented as follows. Section 2 presents a simple review of DRPE technique and CS theory. Section 3 describes our proposed encryption scheme. Section 4 shows the experimental results. Section 5 analyzes the security of our proposed encryption scheme. Section 6 concludes this paper.

2. Theoretical review

2.1. DRPE technique

DRPE has been widely studied for its parallel processing and easy configuration. For the input image $\mathbf{I} = \{I(x, y)\}_{x=1, y=1}^{M, N}$ of size $M \times N$, it is first encoded into an image $\mathbf{E} = \{E(\xi, \eta)\}_{\xi=1, \eta=1}^{M, N}$ that satisfies with stationary white noise using two random phase masks

$\mathbf{M}_1 = \{M_1(x, y)\}_{x=1, y=1}^{M, N}$ and $\mathbf{M}_2 = \{M_2(\mu, \nu)\}_{\mu=1, \nu=1}^{M, N}$, where $M_1(x, y) = e^{i2\pi n(x, y)}$ and $M_2(\mu, \nu) = e^{i2\pi b(\mu, \nu)}$. Here, (x, y) and (μ, ν) denote the coordinates of the input image plane and the second mask plane respectively, $n(x, y)$ and $b(\mu, \nu)$ are randomly distributed in the range $[0, 1]$, and i represents the imaginary unit. In this paper, two phase masks \mathbf{M}_1 and \mathbf{M}_2 are located in the input image plane and the Fourier domain, respectively. The DRPE processing can be described as

$$E(\xi, \eta) = \text{IFT}(\text{FT}(\mathbf{I}(x, y) \cdot e^{i2\pi n(x, y)}) \cdot e^{i2\pi b(\mu, \nu)}), \quad (1)$$

where (ξ, η) represents the coordinate of CCD plane, $E(\xi, \eta)$ is complex-valued data in the CCD plane, and $\text{FT}(\cdot)$ and $\text{IFT}(\cdot)$ indicate the Fourier transform and inverse Fourier transform, respectively.

Similarly, the decoding process is the reverse of DRPE, which can be mathematically described as follows.

$$D(x, y) = |\text{IFT}(\text{FT}(E(x, y) \cdot e^{-i2\pi b(\mu, \nu)})|), \quad (2)$$

where $\mathbf{D} = \{D(x, y)\}_{x=1, y=1}^{M, N}$ is the decoded image and $|\cdot|$ denotes the modulus operation. Since the first phase mask \mathbf{M}_1 is removed by the modulus operation in Eq. (2), it can be omitted during the image decoding.

2.2. CS theory

As a revolutionary data acquisition technique, CS is originally developed by exploiting signal sparsity or compressibility.

Suppose $\mathbf{x} \in \mathbb{R}^N$ is a 1D discrete signal and can be represented by only K coefficients under some linear transform $\mathbf{x} = \Psi \mathbf{s}$, where Ψ is an orthonormal basis and \mathbf{s} is the sparse coefficient vector with only $K \ll N$ nonzero entries. Then CS signal measurements can be condensed as follows.

$$\mathbf{y} = \Phi \mathbf{x} = \Phi \Psi \mathbf{s} = \mathbf{T} \mathbf{s}, \quad (3)$$

where $\mathbf{y} \in \mathbb{R}^M$ ($M < N$) is the measurement vector, $\Phi \in \mathbb{R}^{M \times N}$ denotes the measurement matrix, $\mathbf{T} \in \mathbb{R}^{M \times N}$ represents the sensing matrix. Similarly, 2D or HD signals can be reduced to the 1D format by superimposing column vectors. Furthermore, if the measurement matrix generated by a chaotic map is used for the secret key, CS can be also regarded as a sort of encryption method.

Since the transformation from the original signal \mathbf{x} to the measurements \mathbf{y} is a dimensional reduction process, it is difficult to reconstruct the original signal \mathbf{x} faithfully with CS. However, \mathbf{x} can be recovered precisely using only $M \geq O(K \cdot \log(N/K))$ measurements with preponderant probability as long as Φ satisfies the Restricted Isometry Property (RIP). To recover the original signal \mathbf{x} from the measurements \mathbf{y} , it has been proved by solving the following ℓ_1 -norm minimization problem:

$$\min \|\mathbf{s}\|_1 \quad \text{s.t. } \mathbf{y} = \mathbf{T} \mathbf{s}. \quad (4)$$

In this paper, the discrete wavelet transform (DWT) is used as the sparse transform, the measurement matrix Φ is generated by [37], and the orthogonal matching pursuit algorithm (OMP) and MATLAB-based modeling system for convex optimization (CVX) are used to reconstruct original signal \mathbf{x} , respectively.

3. Proposed image encryption and decryption scheme

3.1. Encryption process

The proposed cryptosystem integrating CS with DRPE can achieve encryption and authentication synchronously. The flowchart of our proposed encryption scheme is depicted in Fig. 1, which clearly shows that the encryption process from plaintext image to ciphertext image goes through four stages: DRPE phase, CS phase, permutation phase and diffusion phase, respectively. First, the plaintext image is encoded and quantified to obtain the authentication information through DRPE transformation, and then, the same plaintext image is compressed and

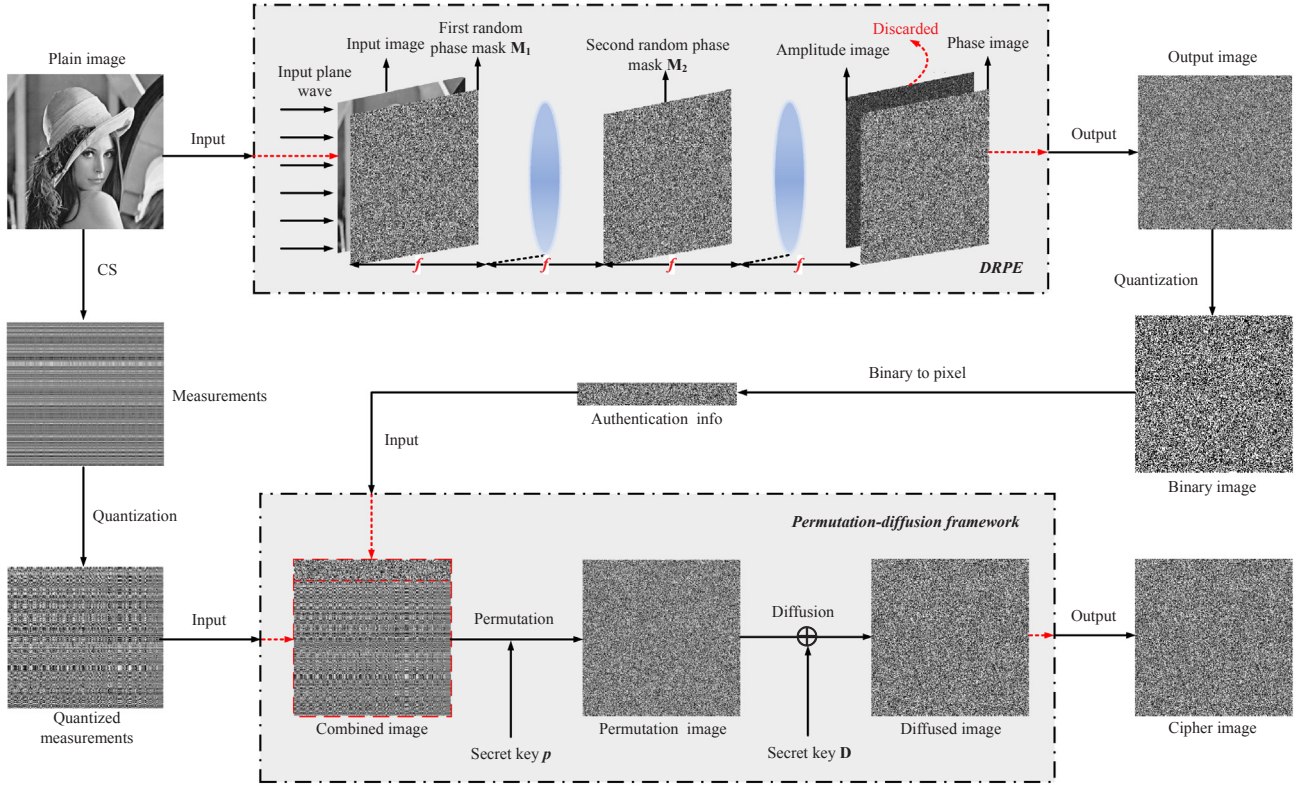


Fig. 1. Procedure for our proposed image encryption scheme.

quantified to obtain the corresponding measurements through CS. Next, the authentication information and the measurements are permuted together to obtain the permutation image. Finally, the permutation image is diffused into the ciphertext image by the XOR operation.

3.1.1. DRPE phase

The plain image $\mathbf{I} = \{I(x, y)\}_{x=1, y=1}^{M, N}$ of size $M \times N$ as input for generating authentication information is first encoded using the DRPE technique, and a complex image composed of phase and amplitude information is obtained. All amplitude information is discarded and only the phase signal is reserved as output. The output phase image $\mathbf{PH} = \{PH(x, y)\}_{x=1, y=1}^{M, N}$ is then quantized as a binary image $\mathbf{B} = \{B(x, y)\}_{x=1, y=1}^{M, N}$.

$$B(x, y) = \begin{cases} 1, & PH(x, y) > 0 \\ 0, & PH(x, y) \leq 0 \end{cases} \quad (5)$$

Then, every 8 bits of the binary image are combined into one pixel of authentication information.

3.1.2. CS phase

The same plain image $\mathbf{I} = \{I(x, y)\}_{x=1, y=1}^{M, N}$ is encrypted and compressed by CS. Since the range of the measurement information is relatively large, it needs to be quantized by using the following sigmoid map:

$$\mathbf{z} = \text{round}(a_1 \cdot (1 + e^{-a_2(y-a_3)})^{-1}), \quad (6)$$

where $\text{round}(\cdot)$ denotes rounding the elements to the nearest integer. In this paper, $a_1 = 255$, $a_2 = y_{\max} - y_{\min}$, $a_3 = (y_{\max} + y_{\min})/2$, where y_{\max} and y_{\min} are the maximum and minimum of the measurements \mathbf{y} , respectively. According to Eq. (6), the value range of measurements after quantization is an integer between 0 and 255.

3.1.3. Permutation phase

The authentication information and quantized measurements are

first combined into a complete image $\mathbf{R} = \{R(x, y)\}_{x=1, y=1}^{M, N}$. Chaotic sequences generated by 2D Henon map are used to permute the combined image. Henon map is a typical invertible 2D map, which can be mathematically expressed as

$$\begin{cases} x_{n+1} = 1 - \alpha x_n^2 + y_n \\ y_{n+1} = \beta x_n \end{cases} \quad (7)$$

where initial values used for encryption are x_0 and y_0 . And when the system parameters α and β are set to 1.4 and 0.3 respectively, Henon map shows the chaotic characteristics.

In this paper, we can modify the controlling parameters appropriately to obtain other chaotic attractors. And the permutation matrix can be obtained by sorting the chaotic sequence generated from Henon map. For the plain image of size $M \times N$, the chaotic sequence of length $M \times N$ is generated by the key set $(x_0, y_0, \alpha, \beta)$. Then chaotic sequence is sorted in descending order, and its original location index is obtained as the permutation vector $\mathbf{p} = \{p_x\}_{x=1}^{M \times N}$. Finally, the combined image \mathbf{R} is permuted into the permutation image $\mathbf{P} = \{P(x, y)\}_{x=1, y=1}^{M, N}$.

$$P(s, t) = R(x, y), \quad (8)$$

where each pixel in the combined image \mathbf{R} is mapped to one exact pixel in the ciphertext image \mathbf{C} by the permutation vector \mathbf{p} , and the pairs (x, y) and (s, t) satisfy:

$$\begin{cases} s = \lfloor (p_{(x-1) \cdot M + y} - 1) \cdot M^{-1} \rfloor + 1 \\ t = p_{(x-1) \cdot M + y} - (s - 1) \cdot M \end{cases}, \quad (9)$$

where $\lfloor \cdot \rfloor$ denotes rounding the elements to the nearest integers towards minus infinity.

3.1.4. Diffusion phase

The diffusion process reflects the influence of the changes of pixels in plaintext on the pixels in ciphertext, thus hiding the statistical structure of plaintext. In order to make our proposed encryption scheme

more secure, chaotic matrix $\mathbf{D}' = \{D'(x, y)\}_{x=1, y=1}^{M, N}$ is first generated from Henon map controlled by another key set $(x'_0, y'_0, \alpha', \beta')$. And then the chaotic matrix \mathbf{D}' is transformed into the diffusion matrix $\mathbf{D} = \{D(x, y)\}_{x=1, y=1}^{M, N}$ by Eq. (10) whose bits are consistent with the image format in order to change some of the pixel values.

$$D(x, y) = \text{round}(\text{mod}(D'(x, y) \times 10^8, 256)), \quad (10)$$

where $\text{mod}(\cdot)$ denotes modulus after division.

Then the ciphertext image $\mathbf{C} = \{C(x, y)\}_{x=1, y=1}^{M, N}$ is obtained by the XOR operation of the permutation image \mathbf{P} and the diffusion matrix \mathbf{D} .

$$C(x, y) = \begin{cases} D(x, y) \oplus P(x, y), & x = 1 \text{ and } y = 1 \\ D(x, y) \oplus P(x, y) \oplus P(x, y - 1), & x = 1 \text{ and } 1 < y \leq N \\ D(x, y) \oplus P(x, y) \oplus P(x - 1, y), & 1 < x \leq M \text{ and } y = 1, \\ D(x, y) \oplus P(x, y) \oplus P(x, y - 1) \oplus P(x - 1, y), & 1 < x \leq M \text{ and } 1 < y \leq N \end{cases} \quad (11)$$

where \oplus denotes the bitwise XOR operation of arguments.

3.2. Decryption process

During the decryption process, there are also four steps for the receiver to authenticate and decrypt the ciphertext image according to the inverse operation of the encryption process. (1) The ciphertext image \mathbf{C} is restored to the permutation image \mathbf{P} by the XOR operation with the diffusion matrix \mathbf{D} . (2) The recovered combined image $\bar{\mathbf{R}}$ can be obtained by the inverse permutation operation. (3) The authentication information in the combined image is extracted and recovered to the binary image $\bar{\mathbf{B}}$. Then the binary image $\bar{\mathbf{B}}$ is converted to a phase image $\bar{\mathbf{P}}\mathbf{H}$ by assigning a value of $-\pi$ to zero and a value of π to 1. The phase image $\bar{\mathbf{P}}\mathbf{H}$ is further processed by the inverse DRPE to obtain the authentication image $\mathbf{A} = \{A(x, y)\}_{x=1, y=1}^{M, N}$. (4) The remaining of the combined image is reconstructed to the plain image $\bar{\mathbf{I}}$ by OMP algorithm, and an advanced statistical nonlinear cross correlation method is used to authenticate the reconstructed image according to the authentication image. Nonlinear cross-correlation transformation coefficient $\mathbf{CO} = \{CO(x, y)\}_{x=1, y=1}^{M, N}$ between reconstructed image $\bar{\mathbf{I}}$ and authentication image \mathbf{A} can be defined as

$$CO(x, y) = \text{IFT}(\bar{I}(\mu, \eta) \cdot A(\xi, \nu))^k \cdot e^{\varphi_I(\mu, \eta) - \varphi_A(\xi, \nu)}, \quad (12)$$

where $\bar{I}(\mu, \eta)$ and $D(\xi, \nu)$ are the 2D Fourier transforms of the reconstructed image $\bar{I}(x, y)$ and authentication image $A(x, y)$; $\varphi_I(\mu, \eta)$ and $\varphi_A(\xi, \nu)$ are the phase images of $\bar{I}(\mu, \eta)$ and $A(\xi, \nu)$, the parameter k is usually set to 0.3.

4. Experimental results

We used MATLAB R2016b software to conduct the simulation experiments on a 64-bit Windows 10 PC with 8 GB random-access memory (RAM) and 2.70 GHz Intel Core i7-7500U CPU. An image 'Lena' of size 256×256 is shown in Fig. 2(a) to verify our proposed encryption scheme. If the sampling rate r is smaller than 0.875, the ciphertext image containing the authentication information is compressed; otherwise, the ciphertext image will not be compressed. In Fig. 2 the sampling rate is defined by $r = 0.875$. The cipher image, reconstructed image, authentication image, differential image between the plain image and reconstructed image and the nonlinear cross-correlation transformation plane between the reconstructed image and authentication image are shown in Fig. 2(b), (c), (d), (e) and (f), respectively.

To evaluate the reconstructed image quality quantitatively, the peak signal to noise ratio (PSNR) is introduced as follows:

$$\text{PSNR} = \frac{255^2}{\frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N [\bar{I}(i, j) - I(i, j)]^2}, \quad (13)$$

where $I(i, j)$ and $\bar{I}(i, j)$ are the pixel values of the plaintext image \mathbf{I} and the reconstructed image $\bar{\mathbf{I}}$, respectively. As can be seen from Fig. 2, the visual quality of the reconstructed image $\bar{\mathbf{I}}$ is well, and the corresponding PSNR value between Fig. 2(a) and (b) is 39.8233 dB.

The peak-to-correlation energy (PCE) can be used to measure the correlation between reconstructed image $\bar{\mathbf{I}}$ and authentication image \mathbf{D} , which can be defined as:

$$\text{PCE} = \frac{\max(CO(x, y)^2)}{\sum_{x=1}^M \sum_{j=1}^N CO(x, y)^2}, \quad (14)$$

where M and N are the image size along the horizontal and vertical axes, respectively. The higher the PCE value, the stronger the correlation between reconstructed image $\bar{\mathbf{I}}$ and authentication image \mathbf{D} . It is clear from Fig. 2(d) that Fig. 2(b) and (c) have a strong correlation due to the high peak in the center of the correlation plane between the authentication image and the reconstructed image. And the PCE value in Fig. 2(d) is 0.0060.

To obtain the measurements without increasing the storage space, CS is adopted to make room for the authentication information. Therefore, our proposed encryption scheme sacrifices the compression rate for authentication capability. Fig. 3(a) and (b) show the PSNR values and PCE values under different compression effects. In this paper, the compression ratio of the image is defined as the ratio of the ciphertext image to the plaintext image. Without considering the authentication information, the image compression rate is the sampling rate. As can be seen from Fig. 3(a), the PSNR value of images reconstructed by CVX is 2.21 dB higher than that of the OMP algorithm on average. The average distance between the blue lines is 3.11 dB, and the average distance between the red broken lines is 2.89 dB, indicating that the use of CVX to reconstruct the image after increasing the authentication information has a greater impact on the PSNR value of the reconstructed image than the use of the OMP algorithm. In addition, the time cost of image reconstruction using CVX is higher than that of the OMP algorithm. Therefore, the OMP algorithm is preferred to reconstruct the original plaintext image, and the sampling rate should be above 0.7 to ensure the visual quality of the reconstructed image. In Fig. 3(b), the PCE value increases gradually with the increase of compression rate. When the compression rate is greater than 0.5, the PCE value changes relatively slowly, which indicates that the PCE value is less influenced by the compression rate. When the compression rate is less than 0.5, it is just the opposite.

Fig. 4 shows the correlation planes under different compression rates. Fig. 4(a), (b) and (c) are correlation planes when the compression rate is 0.125, 0.25 and 0.50, respectively. The obvious peak value in the center of Fig. 4 indicates that the reconstructed image has a strong correlation with the authentication information. Although the quality of reconstructed image affects vision when the compression rate is less than 0.5, its PCE value is higher, which can ensure that the proposed system can successfully verify the true image. Therefore, the authentication capability of the system is robust to the compression rate.

5. Security analysis

Because of the inherent properties of digital images, many statistical analysis methods and other security criterions can be used for preliminary analysis of cryptosystem security [38]. We evaluated the performance of the proposed encryption scheme to resist several attacks in terms of histogram analysis, adjacent pixels correlation, information entropy, noise attack, cropping attack, key space analysis and key sensitivity analysis, respectively.

5.1. Histogram analysis

Since the image histogram displays the frequency distribution of pixels for each tonal value and can provide statistic information of the

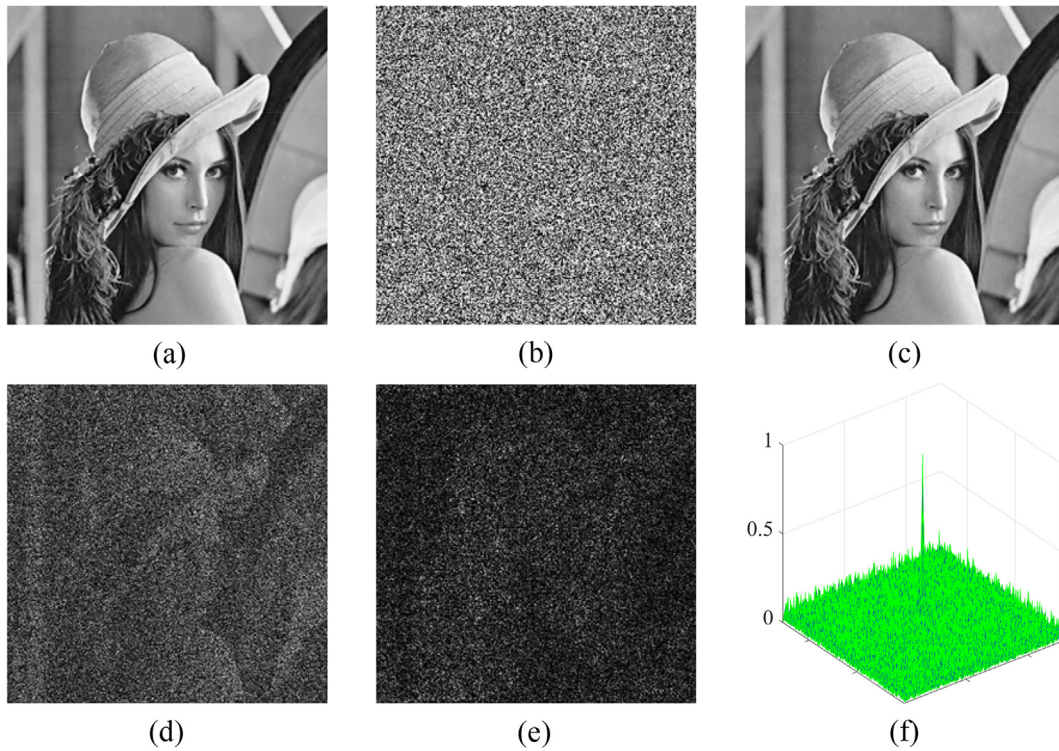


Fig. 2. Reconstructed results based on DRPE and CS. (a) Plaintext image. (b) Ciphertext image. (c) Reconstructed image. (d) Authentication image. (e) Differential image between (a) and (c) (f) Correlation plane between (b) and (c).

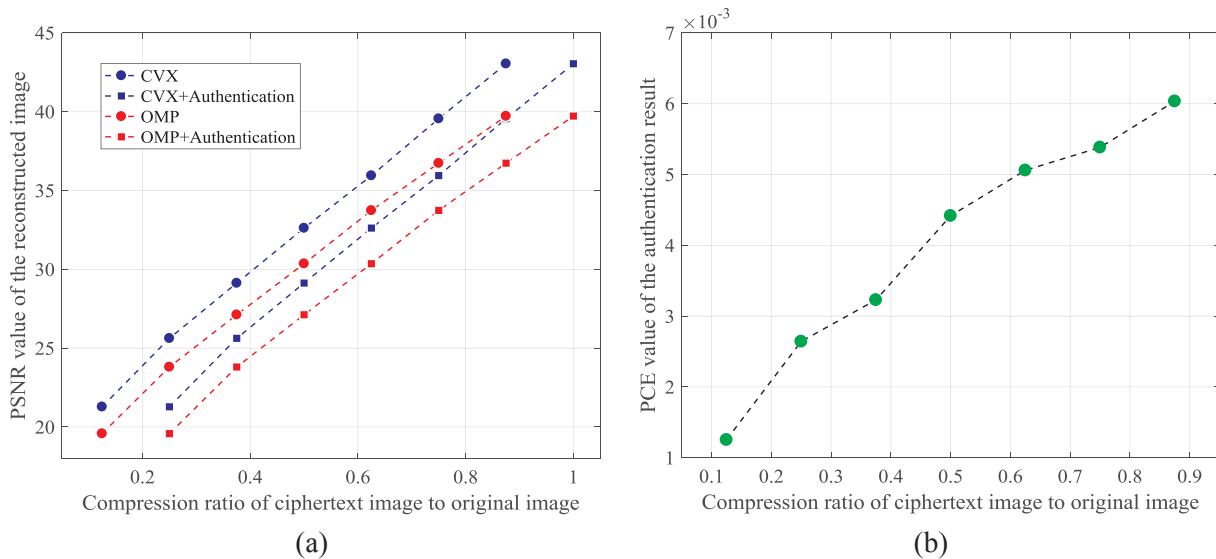


Fig. 3. PSNR values and PCE values at different compression efficiencies. (a) PSNR values vary with different compression efficiencies. (b) PCE values vary with different compression efficiencies.

images, the analysis of uniform histogram of ciphertext image can quantitatively determine that the original encryption system is more reliable to statistical attacks. Fig. 5 shows gray histograms of 'Lena' during encryption and decryption process. Fig. 5(a), (b) and (c) are gray histograms of original plaintext image, cipher image and reconstructed image, respectively. It can be seen from Fig. 5(a) and (b) that the distribution of ciphertext image pixels is relatively uniform, while the distribution of original plaintext image pixels is very similar to that of ciphertext image pixels. Therefore, the proposed encryption scheme has strong resistance to statistical and differential attacks. And it can be observed from Fig. 5(a) and (c) that the pixel distribution of reconstructed image is almost identical with that of the original plaintext

image, which qualitatively indicates the superiority of the reconstruction algorithm.

5.2. Correlation coefficient analysis

Image data is vulnerable to attack because of its high data redundancy and strong correlation between adjacent pixels. Correlation coefficient analysis of plaintext image and ciphertext image is widely used for qualitative evaluation of encryption schemes. The correlation coefficient can be defined as:

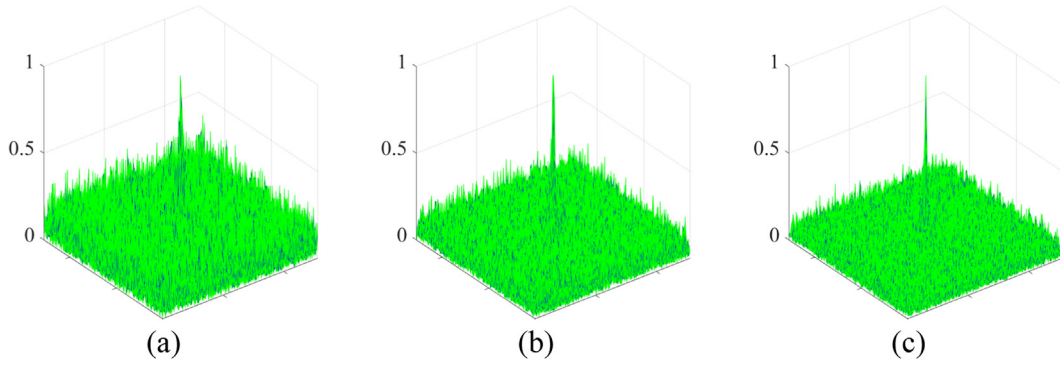


Fig. 4. Correlation planes at different compression ratios. (a) Correlation plane with a compression ratio of 0.125. (b) Correlation plane with a compression ratio of 0.25. (c) Correlation plane with a compression ratio of 0.5.

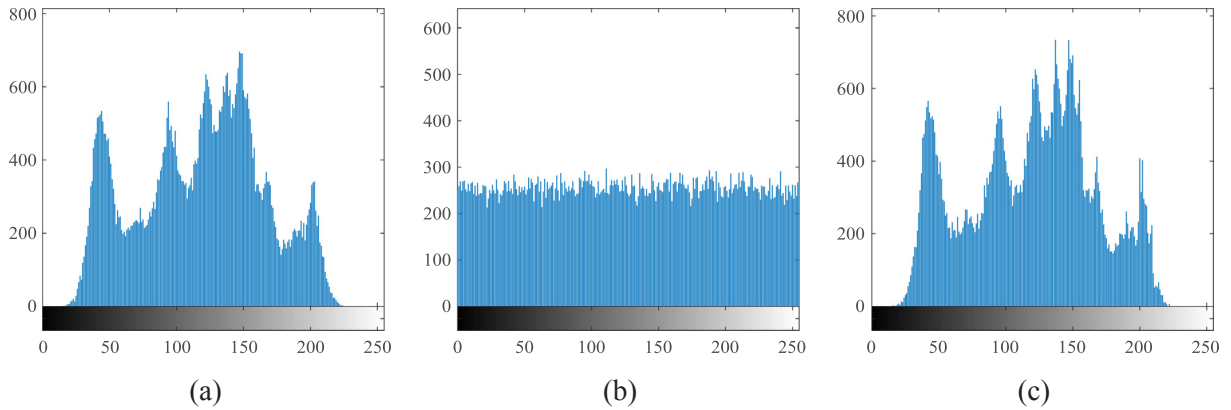


Fig. 5. Gray histograms of 'Lena' during encryption and decryption. (a) Gray histogram of the original plaintext image. (b) Gray histogram of the cipher image. (c) Gray histogram of the reconstructed image.

$$CC = \frac{Cov(v_{ij}, v_{xy})}{\sqrt{D(v_{ij}) \cdot D(v_{xy})}}, \quad (15)$$

$$Cov(v_{ij}, v_{xy}) = \frac{1}{MN} \sum_{i,x=1}^M \sum_{j,y=1}^N ([v_{ij} - E(\mathbf{v})] \cdot [v_{xy} - E(\mathbf{v})]), \quad (16)$$

where v_{ij} and v_{xy} are values of two adjacent pixels in the position (i, j) and (x, y) of the image respectively, $E(\cdot)$ denotes the mean value of the image pixels, and $D(\cdot)$ represents the variance of the values.

In this paper, we randomly select 2000 pairs of adjacent pixels from the plaintext image and ciphertext image of 'Lena', and analyze the correlations from three directions: horizontal, vertical and diagonal, respectively. Fig. 6 shows the correlation diagrams among adjacent pixels of 'Lena' before and after encryption. Fig. 6(a1), (b1) and (c1) are correlation diagrams of the plaintext image at horizontal, vertical and diagonal directions, respectively. And Fig. 6(a2), (b2) and (c2) are correlation diagrams of the ciphertext image at horizontal, vertical and diagonal directions, respectively. Because of the high redundancy of plane information in plain images, there is a strong correlation between adjacent pixels in the plaintext images as shown in the first row of Fig. 6. However, the correlation between adjacent pixels is weak in the ciphertext images as shown in the second row of Fig. 6.

Moreover, the correlation coefficients according to each direction of different images are shown in Table 1. From Table 1, the correlation coefficient of the plaintext image tends to be 1, while that of the ciphertext image tends to be 0, which indicates that there is almost no correlation between plaintext image and ciphertext image and the proposed encryption scheme has good confusion performance.

5.3. Information entropy analysis

The information entropy of the image is a statistical form of features, which reflects the randomness of information in the image. The information entropy of the grayscale image $\mathbf{I} = \{I(x, y)\}_{x=1, y=1}^{M, N}$ can be explicitly defined as:

$$H(\mathbf{I}) = - \sum_{i=0}^{2^b-1} P(\mathbf{I} | I(x, y) = i) \log_2 P(\mathbf{I} | I(x, y) = i), \quad (17)$$

where b represents bits per pixel and $P(\cdot)$ denotes the probability of occurrence of the element. For 8 bits of each pixel data, there are $2^b = 256$ possible gray-level values with equal probability and the ideal value of entropy should be 8.

The information entropy of different cipher images is given in Table 2. It can be observed from Table 2 that the information entropy of each cipher image is much close to the ideal value 8, which implies that the leakage of information can be negligible during encryption process and the proposed scheme is robust against entropy attack.

5.4. Differential attack analysis

The attacker usually make some slight changes to the plaintext image and then compare the corresponding ciphertext image to get the clues of the key. Therefore, the minor modification of plaintext images will produce great changes in ciphertext images, which will effectively resist differential attacks. And the higher the sensitivity to plaintext, the stronger the ability of the algorithm to resist differential attacks. Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) can be used to measure the sensitivity of encryption algorithm to plaintext, which can be defined as follows:

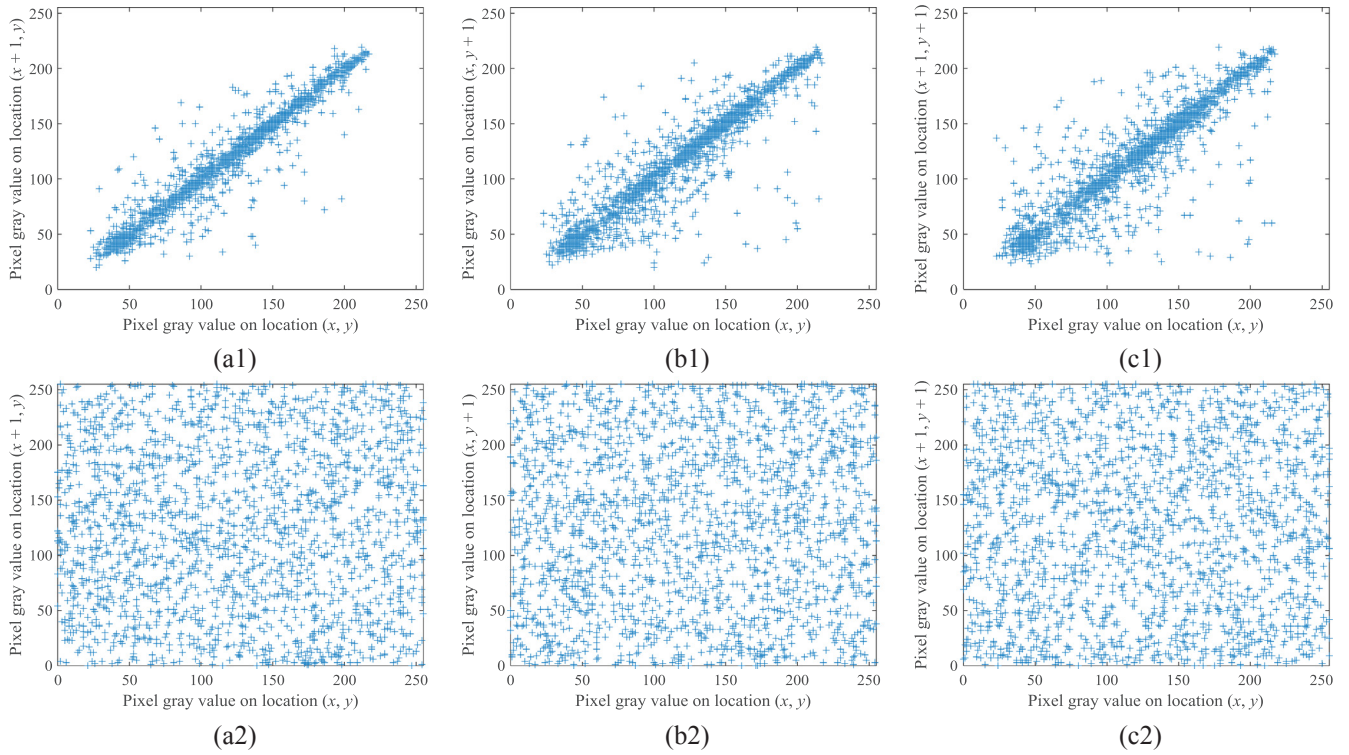







Fig. 6. Correlation analysis of 'Lena' before and after encryption in different directions. (a1), (a2) Horizontal correlation of plaintext and ciphertext images. (b1), (b2) Vertical correlation of plaintext and ciphertext images. (c1), (c2) Diagonal correlation of plaintext and ciphertext images.

Table 1
Correlation coefficient of different images.

Image	Plaintext image			Ciphertext image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
	0.9681	0.9390	0.9135	0.0075	-0.0015	-0.0044
	0.9736	0.9656	0.9417	0.0025	0.0011	0.0033
	0.9451	0.9268	0.8833	0.0014	0.0012	-0.0004
	0.9903	0.9840	0.9825	-0.0041	-0.0016	-0.0033
	0.8261	0.8737	0.7843	-0.0034	-0.0098	0.0035

$$UACI = \frac{1}{MN} \sum_{x=1}^M \sum_{y=1}^N \frac{C_1(x, y) - C_2(x, y)}{2^b - 1} \times 100\%, \quad (20)$$

where $C_1 = \{C_1(x, y)\}_{x=1, y=1}^{M, N}$ and $C_2 = \{C_2(x, y)\}_{x=1, y=1}^{M, N}$ two ciphertext images of slightly different plaintext images. For 8 bits of each pixel data, the expected scores of NPCR and UACI are 99.6094% and 33.4635% [39].

We have tested the ability of the proposed encryption scheme to resist differential attacks by modifying the last bit of a randomly selected pixel of the same plaintext image respectively. The NPCR and UACI values of different ciphertext images are shown in Table 3. It can be seen from Table 3 that the values of NPCR and UACI are very close to the ideal values, which means that the proposed encryption scheme can effectively propagate the small difference of the plaintext image to the whole ciphertext and has good performance against differential attacks.

5.5. Noise attack analysis

However, the cipher image may be distorted and attacked during Internet transmission. Therefore, we used pepper and salt noise of different intensity to disturb the cipher image to simulate the noise attack. Fig. 7 shows the authentication results for the noise attack. In Fig. 7, the first row to the last is the authentication results when the noise intensity is 0.0001, 0.001, 0.01 and 0.1, respectively; the first column to the last is ciphertext images, reconstructed images by the OMP algorithm,






$$L(x, y) = \begin{cases} 0, & C_1(x, y) = C_2(x, y) \\ 1, & C_1(x, y) \neq C_2(x, y) \end{cases} \quad (18)$$

$$NPCR = \frac{1}{MN} \sum_{x=1}^M \sum_{y=1}^N L(x, y) \times 100\%, \quad (19)$$

Table 2
Entropy values of different images.

Image					
Entropy (Plain)	7.4204	7.5700	7.1587	7.4560	7.2289
Entropy (Cipher)	7.9973	7.9972	7.9973	7.9966	7.9972

Table 3
NPCR and UACI of different images.

Image					
NPCR (%)	99.6368	99.4125	99.8746	99.4064	99.5162
UACI (%)	33.5787	33.6411	33.4079	33.7329	33.3363

authentication images and correlation planes between the corresponding reconstructed image and authentication image, respectively. The PSNR values of the reconstruction results in Fig. 7(b1), (b2), (b3) and (b4) are 33.7034 dB, 24.2231 dB, 14.7652 dB and 5.1379 dB, respectively, which indicates that the reconstructed image is sensitive to

noise, and the quality of the reconstructed image decreases obviously with the increase of noise intensity. When the noise intensity is 0.01, the reconstructed image in Fig. 7(b3) is almost difficult to be recognized. However, the obvious peak value in Fig. 7(d3) proves that the reconstructed image still has a strong correlation with the

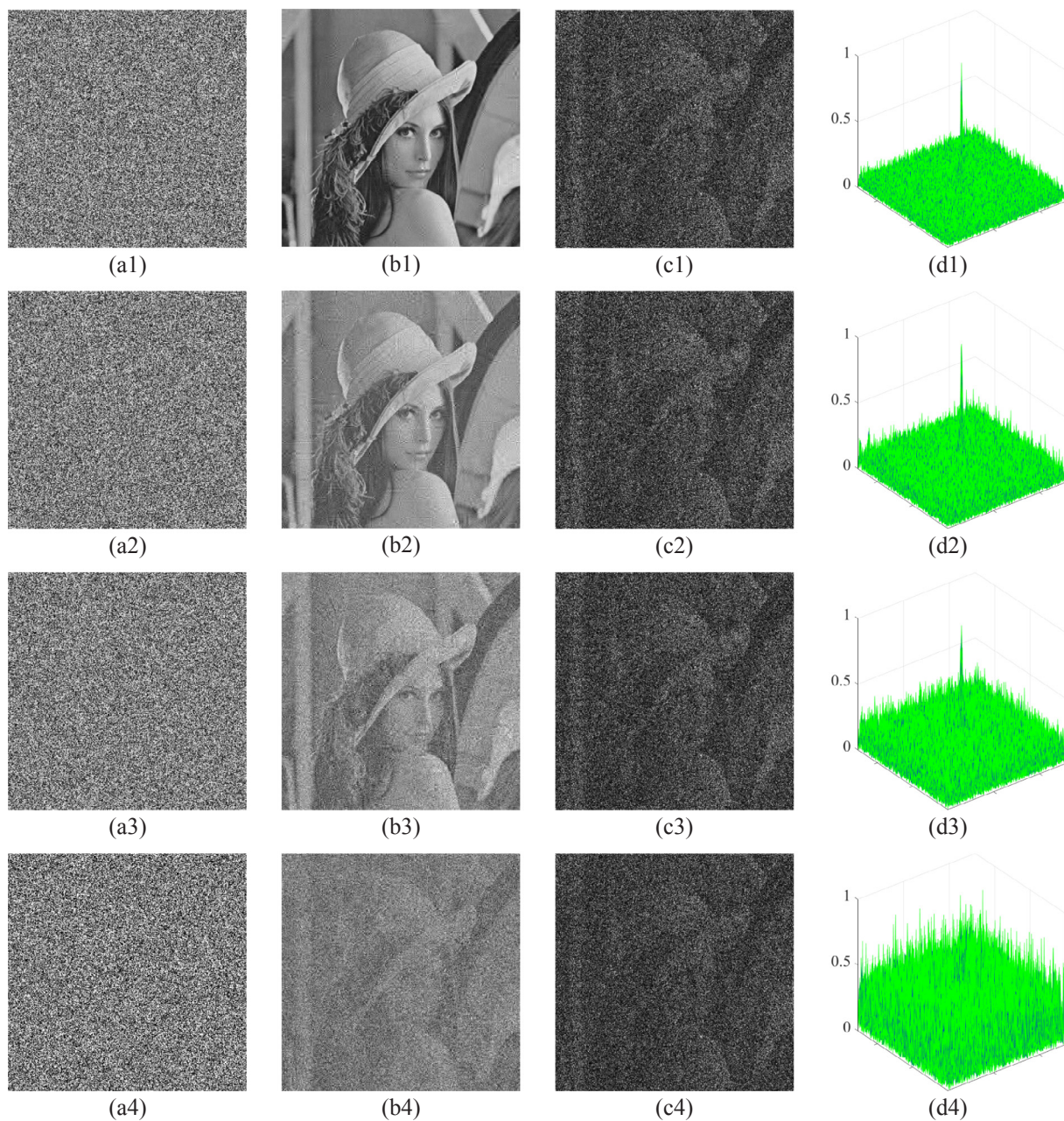


Fig. 7. Authentication results for noise attack. (a1), (a2), (a3), (a4) Cipher images with different noise intensity (0.0001, 0.001, 0.01 and 0.1, respectively) (b1), (b2), (b3), (b4) Reconstructed images correspond to (a1), (a2), (a3) and (a4), respectively. (c1), (c2), (c3), (c4) Authentication images correspond to (b1), (b2), (b3) and (b4), respectively. (d1), (d2), (d3), (d4) Correlation planes between (b1) and (c1), (b2) and (c2), (b3) and (c3), and (b4) and (c4), respectively.

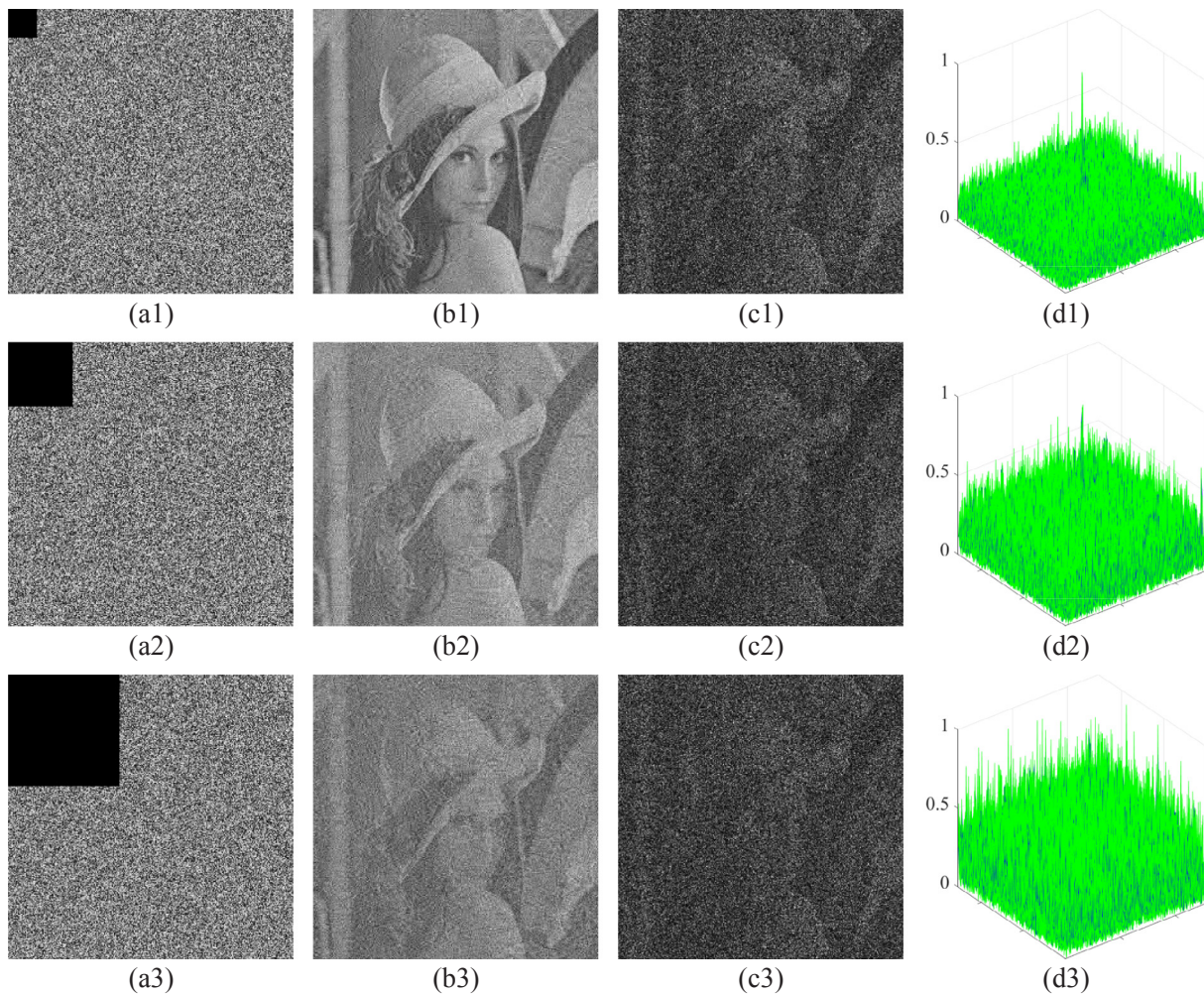


Fig. 8. Authentication results for cropped images. (a1), (a2), (a3) Cropped images with different cropping rates (5%, 10% and 15%, respectively). (b1), (b2), (b3) Reconstructed images correspond to (a1), (a2) and (a3), respectively. (c1), (c2), (c3) Authentication images correspond to (b1), (b2) and (b3), respectively. (d1), (d2), (d3) Correlation planes between (b1) and (c1), (b2) and (c2), and (b3) and (c3), respectively.

authentication information. Until the noise intensity reaches 0.1, the PCE value is less than 0.0001 and there is no peak value in the center of Fig. 7(d4), so the system cannot verify the true image successfully. Therefore, the authentication capability of our proposed scheme is robust to noise when the noise intensity is less than 0.01 and the quality of reconstructed image is high when the noise intensity is less than 0.0001. The results show that the proposed encryption scheme can check the availability of transmitted images.

5.6. Cropping attack analysis

Cropping attack is another common attack in ciphertext image. Here, we test the algorithm's resistance to cropping attack by setting a certain proportion of pixel values in the ciphertext image to 0, and the corresponding results for 'Lena' are shown in Fig. 8. The first to last row in Fig. 8 shows the authentication results after the pixel information in the ciphertext image is cropped by 5%, 10% and 15%, respectively. And the first to last column in Fig. 8 shows ciphertext images, reconstructed images, authentication images and correlation planes, respectively. The PSNR values of the reconstructed images in Fig. 8(b1), (b2) and (b3) are 14.0044 dB, 11.6370 dB and 10.3960 dB, respectively, which shows that the reconstructed image is sensitive to cropping attack, and the larger the cropping ratio is, the greater the impact on the quality of reconstructed image will be. Therefore, as the cropping ratio of ciphertext image increases, the quality of reconstructed image decreases

gradually. No obvious peak value at the center in Fig. 8(d3) indicates that the true class image cannot be verified when the cropping rate is greater than 15%. While the obvious peak value in the center of Fig. 8(d1) and (d2), which shows that the system can successfully verify the true class image when the cropping rate is less than 15%. And it also shows that the authentication capability of the system is robust to the cropping attack. Therefore, the proposed encryption scheme is robust to cropping attacks in image authentication and easy to perceive in image reconstruction. And it is also helpful to checking the availability of the transmitted images.

5.7. Key space analysis

For an image cryptosystem, the attacker can recover any ciphertext image by violent attacks or searching all possible keys in the key space until the exact key is found. Therefore, the feasibility of violent attacks mainly depends on the size of key space in the encryption system. Alvarez et al. in [40] proposed that the effective key space of an image encryption system should be larger than 2^{100} to prevent the attacker from eavesdropping through violent attacks.

The proposed encryption scheme uses a set of keys which include the initial parameters and system parameters used in two random phase masks, the measurement matrix, the permutation matrix and diffusion matrix generator. For example, all the values of $(x_0, y_0, \alpha, \beta)$ for Henon map are real numbers between 0 and 2. Since there is an infinite

number of real numbers between 0 and 2, the key space for these keys is so large that it is almost impossible to guess. According to Chen et al. in [39], the total number of the possible combinations for the 64-bit double-precision number is about $2^{199} > 2^{100}$. Therefore, the proposed encryption scheme is sufficiently powerful against violent attacks.

5.8. Key sensitivity analysis

Assessing the key sensitivity of a cryptosystem is that when using slightly different keys to encrypt the same plaintext image, it generates entirely different ciphertext image or when using slightly different keys to decrypt the same ciphertext image, it cannot correctly decrypt the plaintext image. For the proposed encryption scheme, the permutation matrix and the diffusion matrix are generated by Henon map and controlled by the key set $(x_0, y_0, \alpha, \beta)$. We first randomly generate one default key $Key_0 = \{x_0, y_0, \alpha, \beta\}$, and then add 10^{-10} error to the default keys to generate four different keys $Key_1 = \{x_0 + 10^{-10}, y_0, \alpha, \beta\}$, $Key_2 = \{x_0, y_0 + 10^{-10}, \alpha, \beta\}$, $Key_3 = \{x_0, y_0, \alpha + 10^{-10}, \beta\}$ and $Key_4 = \{x_0, y_0, \alpha, \beta + 10^{-10}\}$, respectively.

To evaluate the key sensitivity of the proposed encryption scheme during the encryption process, the image 'Lena' as shown in Fig. 2(a) is encrypted with the default keys Key_0 to obtain the default ciphertext image as shown in Fig. 2(b), and then the same images 'Lena' are encrypted independently with four different key sets Key_1, Key_2, Key_3 and Key_4 respectively. Fig. 9 shows the corresponding ciphertext images and differential images. The first row in Fig. 9 is the ciphertext images and the second row is the corresponding differential images between Fig. 2(b) and the corresponding ciphertext images in the first row in Fig. 9. It can be seen from Fig. 9 that there is no obvious correlation among these ciphertext images and there is no correlation between differential images.

In order to measure the difference between the default ciphertext image as shown in Fig. 2(b) and the ciphertext images in Fig. 9, Mean Squared Error (MSE) is introduced as follows:

$$MSE = \frac{1}{MN} \sum_{x=1}^M \sum_{y=1}^N [C_1(x, y) - C_2(x, y)]^2, \quad (21)$$

where $C_1 = \{C_1(x, y)\}_{x=1, y=1}^{M, N}$ and $C_2 = \{C_2(x, y)\}_{x=1, y=1}^{M, N}$ two ciphertext images with slightly different keys. Furthermore, the MSE values

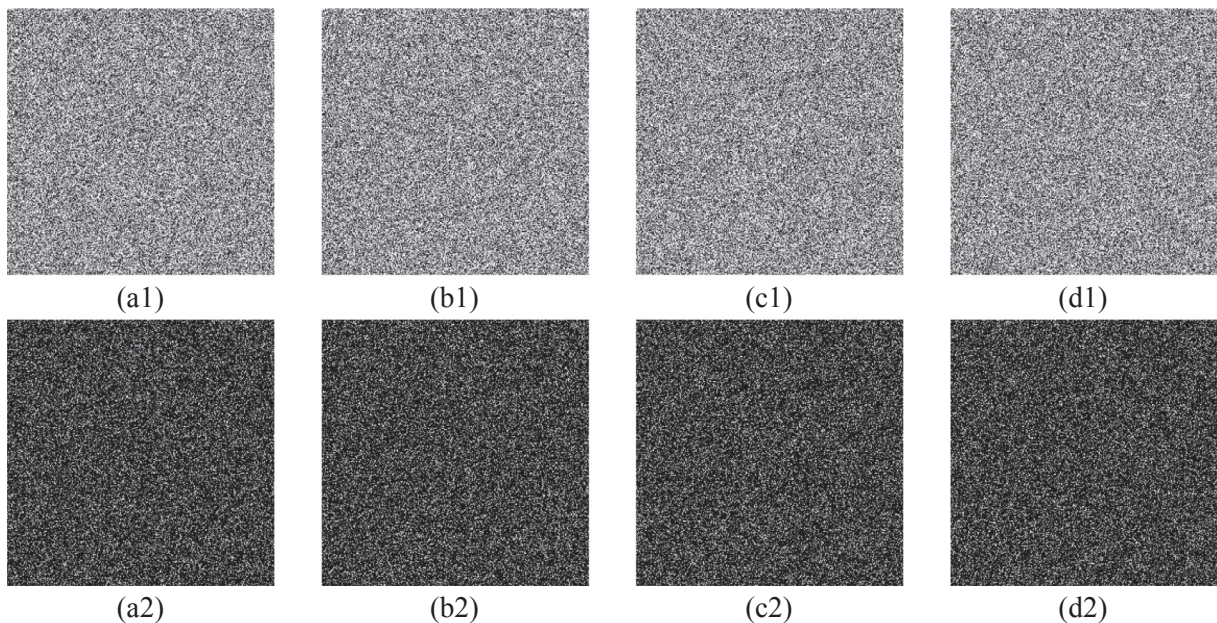


Fig. 9. Key sensitivity analysis of encryption process. (a1), (b1), (c1), (d1) Ciphertext images with Key_1, Key_2, Key_3 and Key_4 , respectively. (a2), (b2), (c2), (d2) Differential images between Fig. 2(b) and (a1), (b) and (b1), (b) and (c1), and (b) and (d1), respectively.

Table 4

Differences between cipher images with different keys.

Image	Fig. 9(b1)	Fig. 9(c1)	Fig. 9(d1)	Fig. 9(d1)
Key	Key_1	Key_2	Key_3	Key_4
MSE ($\times 10^5$)	1.0849	1.0937	1.0952	1.0816

between Fig. 2(b) and the corresponding ciphertext images is shown in Table 4. It can be seen from Table 4 that the MSE values of ciphertext images with slightly different encryption keys will vary greatly, which reflects the sensitivity of the proposed encryption scheme to the key.

To evaluate the key sensitivity of the proposed encryption scheme during the decryption process. We use these four different keys to decrypt the default ciphertext image. The key sensitivity analysis results as shown in Fig. 10 are conducted on all these four keys. The first column to the last in Fig. 10 is the authentication results of Key_1, Key_2, Key_3 and Key_4 , respectively. And the first row to the last in Fig. 10 is reconstructed images, authentication images and correlation planes between reconstructed images and authentication images. The PSNR values of the reconstructed image in Fig. 10(a1), (b1), (c1) and (d1) are 4.3068 dB, 4.1985 dB, 4.2193 dB and 4.2639 dB, respectively. It also can be seen that when the key is wrong, these reconstructed images in Fig. 10(a1), (b1), (c1) and (d1) are hard to distinguish visually. In Fig. 10(a1–d3), there is no obvious peak value in the center of correlation planes, indicating that only when all the keys are completely correct can the cryptosystem successfully authenticate whether the ciphertext image is available. Therefore, the experimental results show that the proposed encryption scheme is robust to violent attacks and the authentication capability is fragile.

6. Conclusion

This paper has proposed an image encryption method with robust and blind authentication capability combining DRPE and CS. Experimental results show that when the pixel of the ciphertext image is tampered with less than 5% during transmission, the proposed encryption scheme can authenticate the availability of transmitted images. The proposed encryption scheme has the following merits: (1) All the steps of image encryption, compression, authentication

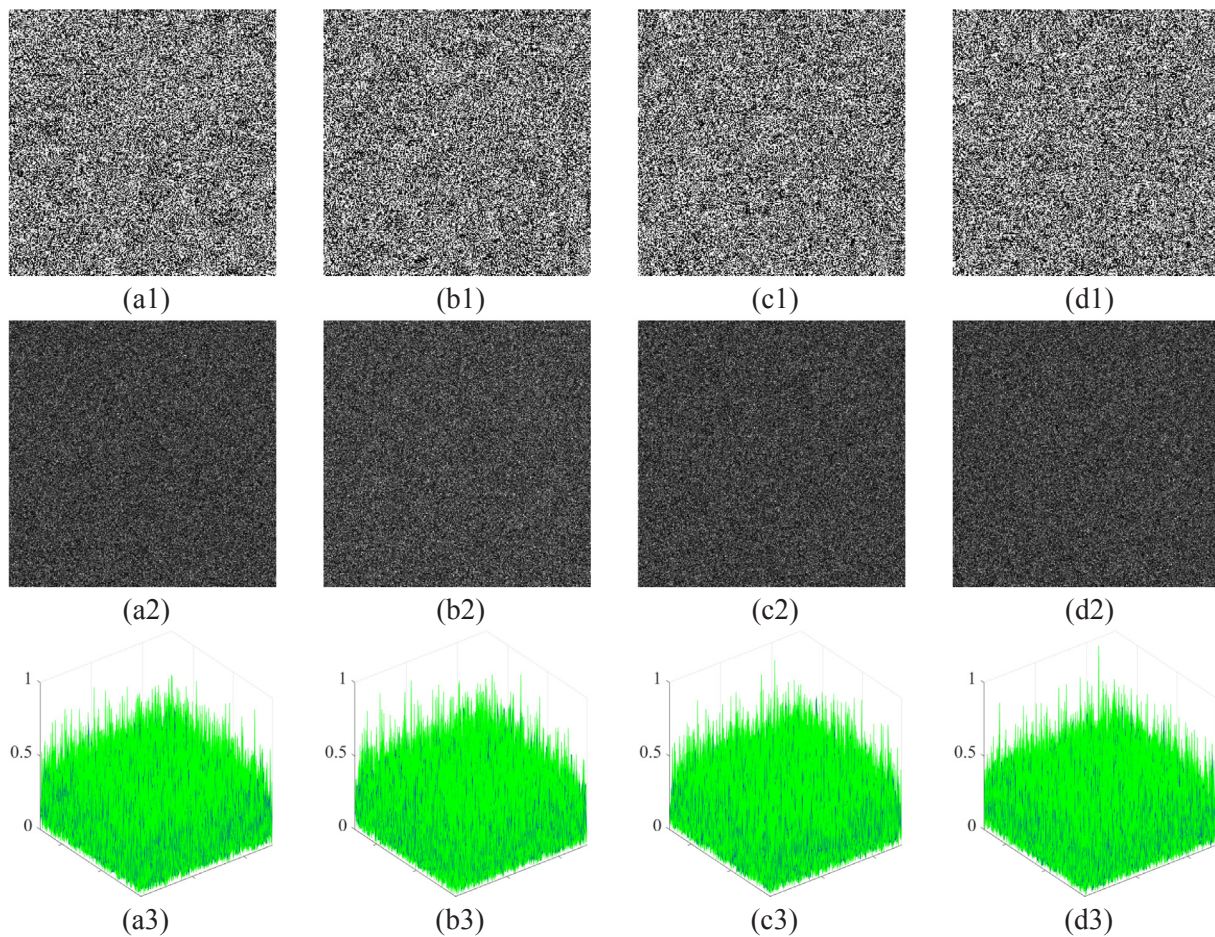


Fig. 10. Authentication results using wrong keys. (a1), (b1), (c1), (d1) Reconstructed images with Key_1 , Key_2 , Key_3 and Key_4 , respectively. (a2), (b2), (c2), (d2) Authentication images correspond to (a1), (b1), (c1), (d1) and (e1), respectively. (a3), (b3), (c3), (d3) Correlation planes between (a1) and (a2), (b1) and (b2), (c1) and (c2), and (b1) and (c2), respectively.

information generation and embedding can be performed simultaneously by an integrated optical system during image sampling. The entire cryptosystem requires only optical transformation, which is processed at the speed of light and is therefore not limited by computer hardware performance. (2) Compared with traditional image encryption schemes and CS, our proposed encryption scheme has the authentication capability simultaneously. A self-embedding ciphertext image with authentication capability can be directly obtained through sampling. (3) Compared with traditional watermarking methods with authentication capability, no additional information hiding operations are required. Therefore, the proposed encryption scheme is superior to both the traditional CS and the traditional information hiding method.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant no. 61602158) and the PhD Scientific Research Foundation of Henan Normal University (Grant no. 5101119170143).

References

- [1] Zhaoqing Pan, He Qin, Xiaokai Yi, et al., Low complexity versatile video coding for traffic surveillance system, *Int. J. Sens. Netw.* 30 (2) (2019) 116–125.
- [2] Zhaoqing Pan, Weijie Yu, Xiaokai Yi, et al., Recent progress on generative adversarial networks (GANs): a survey, *IEEE Access* 7 (2019) 36322–36333.
- [3] Zhaoqing Pan, Ching-Nung Yang, Victor S. Sheng, et al., Machine learning for wireless multimedia data security, *Secur. Commun. Netw.* 2019 (2019) 1–2.
- [4] William J. Gordon, Adam Fairhall, Adam Landman, Threats to information security: public health implications, *N. Engl. J. Med.* 377 (8) (2017) 707–709.
- [5] Zhihua Xia, Xinhui Wang, Xingming Sun, et al., A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data, *IEEE Trans. Parallel Distrib. Syst.* 27 (2) (2016) 340–352.
- [6] Wei Zhang, Yaping Lin, Sheng Xiao, et al., Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing, *IEEE Trans. Comput.* 65 (5) (2016) 1566–1577.
- [7] Ming Li, Dandan Lu, Wenyong Wen, et al., Cryptanalyzing a color image encryption scheme based on hybrid hyper-chaotic system and cellular automata, *IEEE Access* 6 (2018) 47102–47111.
- [8] Ming Li, Haiju Fan, Yong Xiang, et al., Cryptanalysis and improvement of a chaotic image encryption by first-order time-delay system, *IEEE Multimedia* 25 (3) (2018) 92–101.
- [9] Ming Li, Lu Dandan, Yong Xiang, et al., Cryptanalysis and improvement in a chaotic image cipher using two-round permutation and diffusion, *Nonlinear Dyn.* 96 (1) (2019) 31–47.
- [10] Sudheesh K. Rajput, Dharendra Kumar, Naveen K. Nishchal, Photon counting imaging and polarized light encoding for secure image verification and hologram watermarking, *J. Opt.* 16 (12) (2014) 125406.
- [11] Jieun Lee, Nishat Sultana, Faliu Yi, et al., Avalanche and bit independence properties of photon-counting double random phase encoding in gyrator domain, *Curr. Opt. Photon.* 2 (4) (2018) 368–377.
- [12] Inkyu Moon, Faliu Yi, Mingu Han, et al., Efficient asymmetric image authentication schemes based on photon counting-double random phase encoding and RSA algorithms, *Appl. Opt.* 55 (16) (2016) 4328–4335.
- [13] Dongming Huo, Ding-fu Zhou, Sheng Yuan, et al., Image encryption using exclusive-OR with DNA complementary rules and double random phase encoding, *Phys. Lett. A.* 383 (9) (2019) 915–922.
- [14] Faliu Yi, Youhyun Kim, Inkyu Moon, Secure image-authentication schemes with hidden double random-phase encoding, *IEEE Access* 6 (2018) 70113–70121.
- [15] Junxin Chen, Zhi-Liang Zhu, Fu Chong, et al., Information authentication using sparse representation of double random phase encoding in fractional Fourier transform domain, *Optik* 136 (2017) 1–7.
- [16] Luozhi Zhang, Yuanyuan Zhou, Dongming Huo, et al., Multiple-image encryption based on double random phase encoding and compressive sensing by using a measurement array preprocessed with orthogonal-basis matrices, *Opt. Laser*

- Technol. 105 (2018) 162–170.
- [17] Dongming Huo, Xin Zhou, Luozhi Zhang, et al., Multiple-image encryption scheme via compressive sensing and orthogonal encoding based on double random phase encoding, *J. Mod. Opt.* 65 (18) (2018) 2093–2102.
- [18] Pei Lu, Xu Zhiyong, Lu Xi, et al., Digital image information encryption based on Compressive Sensing and double random-phase encoding technique, *Optik* 124 (16) (2013) 2514–2518.
- [19] Akram Belazi, Ahmed A. Abd, Adrian-Viorel Diaconu El-Latif, et al., Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms, *Opt. Lasers Eng.* 88 (2017) 37–50.
- [20] H. Wang, D. Xiao, M. Li, et al., A visually secure image encryption scheme based on parallel compressive sensing, *Signal Process.* 155 (2019) 218–232.
- [21] Yanjie Song, Zhiliang Zhu, Wei Zhang, et al., Joint image compression-encryption scheme using entropy coding and compressive sensing, *Nonlinear Dyn.* 95 (3) (2019) 2235–3226.
- [22] Junxin Chen, Nan Bao, Zhi-liang Zhu, Optical information authentication via compressed sensing and double random phase encoding, *J. Opt.* 19 (10) (2017) 105702.
- [23] Ming Li, Haiju Fan, Hua Ren, et al., Meaningful Image encryption based on reversible data hiding in compressive sensing domain, *Secur. Commun. Netw.* 2018 (2018) 1–12.
- [24] Philippe Refregier, Bahram Javidi, Optical image encryption based on input plane and Fourier plane random encoding, *Opt. Lett.* 20 (7) (1995) 767–769.
- [25] G.H. Situ, J.J. Zhang, Double random-phase encoding in the Fresnel domain, *Opt. Lett.* 29 (14) (2014) 1584–1586.
- [26] G. Unnikrishnan, J. Joseph, K. Singh, Optical encryption by double-random phase encoding in the fractional Fourier domain, *Opt. Lett.* 25 (12) (2000) 887–889.
- [27] Jiecai Zheng, Xueqing Li, Image authentication using only partial phase information from a double-random-phase-encrypted image in the Fresnel domain, *J. Opt. Soc. Korea* 19 (3) (2015) 241–247.
- [28] Wen Chen, Xudong Chen, Double random phase encoding using phase reservation and compression, *J. Opt.* 16 (2) (2014) 025402.
- [29] Faliu Yi, Yousun Jeoung, Inkyu Moon, Three-dimensional image authentication scheme using sparse phase information in double random phase encoded integral imaging, *Appl. Opt.* 56 (15) (2017) 4381–4387.
- [30] Zhengjun Liu, Qing Guo, Lie Xu, et al., Double image encryption by using iterative random binary encoding in gyration domains, *Opt. Exp.* 18 (11) (2010) 12033–12043.
- [31] D.L. Donoho, Compressed sensing, *IEEE Trans. Inf. Theory* 52 (4) (2016) 1289–1306.
- [32] Zheng Zhang, Yong Xu, Jian Yang, et al., A survey of sparse representation: algorithms and applications, *IEEE Access* 3 (2015) 490–530.
- [33] Zheng Zhang, Li Liu, Fumin Shen, et al., Binary multi-view clustering, *IEEE Trans. Pattern Anal. Mach. Intell.* 41 (7) (2019) 1774–1782.
- [34] Zheng Zhang, Ling Shao, Xu Yong, et al., Marginal representation learning with graph structure self-adaptation, *IEEE Trans. Neural Netw. Learn. Syst.* 29 (10) (2018) 4645–4659.
- [35] Xiuli Chai, Xiaoyu Zheng, Zhihua Gan, et al., An image encryption algorithm based on chaotic system and compressive sensing, *Signal Process.* 148 (2018) 124–144.
- [36] Haiju Fan, Ming Li, Wentao Mao, VQ-based compressive sensing with high compression quality, *Electron. Lett.* 53 (17) (2017) 1196–1198.
- [37] S. George, D. Pattathil, A novel approach for secure compressive sensing of images using multiple chaotic maps, *J. Opt.* 43 (1) (2014) 1–17.
- [38] Leo Yu Zhang, Yuansheng Liu, Fabio Pareschi, et al., On the security of a class of diffusion mechanisms for image encryption, *IEEE Trans. Cybernet.* 48 (4) (2018) 1163–1175.
- [39] Chen Junxin, Zhu Zhi-liang, et al., Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption, *Signal Process.* 142 (2018) 340–353.
- [40] Gonzalo Alvarez, Shujun Li, Some basic cryptographic requirements for chaos-based cryptosystems, *Int. J. Bifurcat. Chaos* 16 (8) (2006) 2129–2151.