Hindawi
Security and Communication Networks
Volume 2021, Article ID 6978772, 20 pages
https://doi.org/10.1155/2021/6978772

Research Article

Secure Image Authentication Scheme Using Double Random-Phase Encoding and Compressive Sensing

Hua Ren,[1] Shaozhang Niu,[1] Haiju Fan,[2] Ming Li,[2] and Zhen Yue[3]

[1]*Beijing Key Lab of Intelligent Telecommunication Software and Multimedia School of Computer, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2]*College of Computer and Information Engineering, Henan Normal University, Xinxiang, Henan 453007, China*
[3]*Modern Educational Technology Center, Henan Normal University, Xinxiang, Henan 453007, China*

Correspondence should be addressed to Shaozhang Niu; szniu@bupt.edu.cn

Received 20 April 2021; Revised 30 July 2021; Accepted 8 September 2021; Published 27 September 2021

Academic Editor: Bruno Carpentieri

Double random-phase encoding- (DRPE-) based compressive sensing (CS) systems support image authentication for noisy images. When extending such systems to resource-constrained applications, how to ensure the authentication strength for noisy images becomes challenging. To tackle the issue, an efficient and secure image authentication scheme is presented. The phase information of the plain image is generated using DRPE and quantized into a binary image as the authentication information. Meanwhile, a sparser error matrix generated by the same plain image and vector quantization (VQ) image works as the input of CS. The authentication information and VQ indexes are self-hidden into the quantized measurements to construct the combined image. Then, it is permutated and diffused with the chaotic sequences generated from a modified Henon map. After decryption at the receiver side, the verifier can implement the blind authentication between the noisy decoded image and the reconstructed image. Supported by the detailed numerical simulations and theoretical analyses, the DRPE-CSVQ exhibits more powerful compression and authentication capability than its counterpart.

1. Introduction

As the primary form of information carrier and exchange, digital images experience fast-growing storage and transmission in communication media today, irrespective of whether mobiles or individual electronic devices are available [1]. When different kinds of digital images are managed and transmitted via open channels, illegal users may tamper, redistribute, and even destroy them, which will bring tremendous losses to legitimate terminal users [2]. It is a nontrivial task to ensure the security of images that contains user privacy or essential information. One viable solution is to encrypt digital images into unrecognizable or noise-like patterns [3, 4]. Image encryption schemes, especially chaotic-based ones, have been widely investigated as a means of privacy protection [5]. However, most chaotic encryption designs are not secure enough against unauthorized operations [6, 7]. Besides, some chaotic encryption schemes [3, 5] encrypt plaintext into the ciphertext of the same size, which is not conductive to resource-constrained applications.

As two kinds of classic lossy compression technologies, vector quantization (VQ) and compressive sensing (CS) have already exerted their strengths in their respective fields [8–15]. VQ, a block-size compression coding method, has a tremendous high compression ratio by transforming block vector into codeword index. Some researchers used the compression property of VQ technology to restore the tampered contents [8–10]. In the recoverable scheme [10], the main content in one carrier region is compressed into an index by the VQ encoder and then embedded into the other carrier regions. After detecting malicious manipulations, the index extracted from the reserved regions can restore the main content of the tampered area with the public codebook. The restoration precision strictly relates to the codebook. If the plain content does not match the codebook closely enough, the restored content will have noticeable block

artifacts [11]. CS is another technique to fulfill the same purpose using a different solution [12, 13, 15]. It has been proven that CS-based cryptosystems are computationally infeasible under brute-force attack and exhaustive searching [13]. However, the security is built on the measurement matrix as the key, which worsens key distribution and transmission [14]. Yu et al. [15] theoretically proved that the measurement matrix generated by chaotic map satisfies restricted isometry property (RIP), which provided an alternative construction of the CS measurement matrix. In addition, since the sparseness of the signal was utilized to reconstruct the original signal from the measurements, directly assigning raw images as inputs of CS may lead to a worse restoration and may not achieve the ideal compression effect due to the lower sparsity of raw images [16, 17].

Double random-phase encoding (DRPE) technology, initially developed by Refregier et al. [18], has the distinct advantages of processing 2D complex data with parallelism and high speed. Many references have integrated DRPE with other conventional signal processing techniques [19–23], such as watermarking, encryption, and authentication by Fourier domain expansion to Fresnel domain. In [23–25], DRPE was mixed with photon-counting imaging to acquire sparse complex information and secure image authentication based on a statistical nonlinear correlation approach. Since phase information obtained by DRPE and photon-counting imaging is sparse and requires less space to store, it has been favored by other studies [22, 26–29]. To reduce storage and provide higher security, the schemes [22, 26] only reserved partial phase information for the authentication. Likewise, references [24, 26] used sparse complex information resulting from 2D elemental images for final authentication. In [23], Cho et al. proposed combining DRPE and 3D integer imaging techniques for 3D image authentication. In [28], Yi et al. noticed that most preliminary DRPE-based image authentication designs implicitly assumed that the receiver successfully received the encrypted images and that there were no attacks during transmission. Thus, most of these would fail to authenticate even when the transmitted images had been disturbed by noises, a common occurrence in reality during Internet transmission.

The schemes [29–32] combined DRPE and CS (DRPE-CS) to cope with the security concerns of current cryptosystems. In [30], Zhang et al. developed a joint orthogonal encoding and CS method to implement DRPE-based multiple-image encryption. The block reconstruction process reestablished every single image perfectly. In [31], Huo et al. proposed a similar multiple-image encryption scheme to sample each plain data and integrate the sampled data into a synthesized ciphertext by the orthogonal encoding process. The key storage is efficient and straightforward since the pseudorandom sequences generated by chaotic systems are employed to construct the CS measurement matrix and the two random phases of DRPE. Besides, through applying dimensionality reduction and random projection to CS sampling, Lu et al. developed a DRPE-CS image encryption scheme in [32], which achieved lower data volume for encryption and higher security for information protection. To upgrade the security level and realize blind authentication, Zhou et al. presented a novel and secure DRPE-BCS method [29]. However, the reconstructed image precision was not ideal. Firstly, a lower sampling ratio would cause a poor-quality reconstructed image because of the raw image as the CS input. Secondly, performing different cropping regions on the cipher images would cause severe distortion on the reconstructed image since no remedy is provided when attacked. Given these considerations, ensuring the quality of the reconstructed image at lower sampling rates and loss reduction after being attacked such that more robust authentication strength can be available becomes a challenge.

To have more robust authentication between the noisy decoded image and the reconstructed image, we detail a secure image authentication scheme by integrating DRPE and VQ with CS. The plain image is encoded into authentication information by DRPE and quantized into the VQ image by the VQ encoder/decoder. The sparse error matrix generated by the same plain image and VQ image is as the CS input. The reconstructed error matrix by CS only fulfills information compensation to the VQ reconstructed image. Consequently, the final reconstructed image quality does not have high requirements for the codebook, and it has no strict restriction for CS compression. The combined image consists of the VQ indexes, the authentication bits, and the quantized measurements, followed by the permutation and diffusion to improve security. Experiments have confirmed that selecting an error matrix for CS compression counteracts the interaction between reconstructed quality and compression ratio. Therefore, the main contributions of this paper are as follows: (1) CS and VQ are combined to achieve sampling at the fast and efficient characteristics. (2) A self-embedding method with authentication capability is implemented, which outperforms conventional DRPE-CS methods. (3) The restoration precision of the reconstructed image at a lower sampling ratio surpasses that of conventional CS where the nature image is as CS input. (4) After being attacked, if replacing the damaged indexes with the undamaged neighbor indexes, the restoration quality of the final reconstructed image will be much better than that of no operation; thus, the DRPE-CSVQ vastly reduces the costs and losses after malicious attacks. Finally, we want to emphasize that (3) and (4) play vital roles in the final authentication effect.

The rest of the paper is organized as follows. In Section 2, related technologies are introduced. In Section 3, the compression, encryption, and authentication method is discussed in detail. Detailed experiment results and performance analyses are given in Section 4. The conclusion is provided in Section 5.

2. Related Technologies

2.1. Double Random-Phase Encoding. DRPE involves the operations of two random-phase marks, respectively, in the input and the Fourier transform planes, which is shown in Figure 1. For an input image $\mathbf{I}_0 = \{I_0(x, y)\}_{x=1,y=1}^{M,N}$, it is encoded into an image $\mathbf{E} = \{E(\xi, \eta)\}_{x=1,y=1}^{M,N}$ of the same size that satisfies stationary white noise using two random-phase masks $\mathbf{m_1} = \{m_1(x, y)\}_{x=1,y=1}^{M,N}$ and $\mathbf{m_2} = \{m_2(\mu, \nu)\}_{x=1,y=1}^{M,N}$,

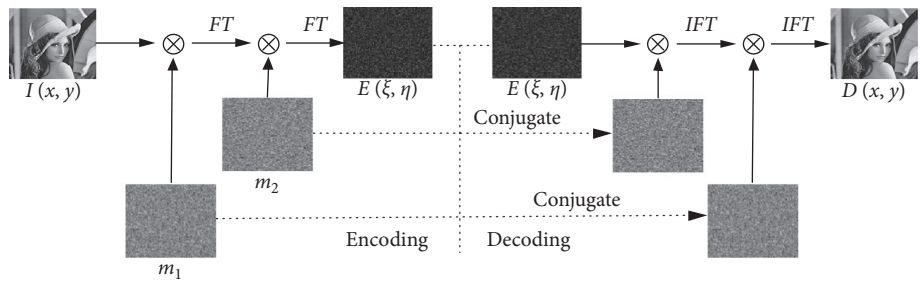


Figure 1: The simplified process of DRPE technology.

where $n(x, y)$ and $b(\mu, \nu)$ are distributed in the range $[0, 1]$ with uniform probability, (x, y) and (μ, ν) denote the coordinates of the input image plane and the second mask plane, respectively, j represents the imaginary unit, $m_1(x, y) = e^{(j2\pi n(x,y))}$, and $m_2(\mu, \nu) = e^{(j2\pi b(\mu,\nu))}$. The encoding process can be expressed as [28]

$$E(\xi, \eta) = FT\left(FT\left(I_0(x, y) \cdot e^{(j2\pi n(x,y))}\right) \cdot e^{(j2\pi b(\mu,\nu))}\right), \quad (1)$$

where (ξ, η) represents the coordinate in CCD plane, $FT(\cdot)$ is the Fourier transform, and $E(\xi, \eta)$ is a complex image that contains an amplitude image and a phase image.

Similarly, DRPE decoding is the reverse process of encoding.

$$D(x, y) = IFT\left(IFT(E(\xi, \eta)) \cdot e^{(j2\pi b(\mu,\nu))}\right) \cdot e^{(j2\pi n(x,y))}, \quad (2)$$

where $D = \{D(x, y)\}_{x=1,y=1}^{M,N}$ is the decoded image and $IFT(\cdot)$ is the inverse Fourier transform.

2.2. Compressive Sensing. CS relies on properties of incoherence, signal sparsity, and compressibility. Suppose $\mathbf{x}$ is a 1D signal of length N, and then the signal can be represented in a dictionary $\Psi = [\Psi_1, \Psi_2, \ldots \Psi_N]$ as follows:

$$\mathbf{x} = \sum_{i=1}^{N} s_i \Psi_i, \quad (3)$$

where s_i is the coefficients of the signal $\mathbf{x}$. The equivalent form of $\mathbf{x}$ is

$$\mathbf{x} = \Psi \mathbf{s}, \quad (4)$$

where Ψ is a $N \times N$ matrix with $\{\Psi_i\}_{i=1}^{N}$ as columns. The core is to find a dictionary so that the coefficient vector $\mathbf{s}$ is sparse; namely, only $K \ll N$ coefficients are nonzero.

After sparsity to the signal, a condensed representation with $M < N$ linear measurements between $\mathbf{x}$ and a collection of functions $\{\Phi_m\}_{m=1}^{M}$ can be written as $\mathbf{y}_m = \langle x, \Phi_m \rangle$. Stacking $\mathbf{y}_m$ into $M \times 1$ vector and Φ_m^T as rows into a matrix Φ of size $M \times N$, we can obtain

$$\mathbf{y} = \Phi x = \Phi \Psi s, \quad (5)$$

where $\mathbf{y}$ and Φ are the measurements and the measurement matrix, respectively. Since the transformation from $\mathbf{x}$ to $\mathbf{y}$ is a dimensionality reduction process, it is difficult to reconstruct the original signal faithfully with CS. Fortunately, it has been proven that, only using $M \geq O(K \log(N/K))$ random measurements, $\mathbf{x}$ can be recovered approximately as long as $\Phi\Psi$ satisfies the restricted isometry property (RIP) [33]. Thus, by solving the ℓ_1-norm optimization problem, we can reconstruct $\mathbf{x}$ from the measurements $\mathbf{y}$ [34].

$$\widehat{\mathbf{s}} = \arg, \min \|\mathbf{s}'\|_1, \text{s.t. } \Phi\Psi\mathbf{s}' = \mathbf{y}. \quad (6)$$

There exist some widely used algorithms to deal with the optimization problem: total variation, orthogonal matching pursuit (OMP), and iterative threshold, and so on. In this paper, a MATLAB-based modeling system for convex optimization (CVX) is used to reconstruct the original signal $\mathbf{x}$.

2.3. Vector Quantization. As a lossy block-size data compression way, VQ was first proposed by Linde et al. in 1980 [35]. The compression coding mainly consists of three components: codebook generation, VQ encoder, and VQ decoder. The codebook $\mathbf{CB} = \{\mathbf{Y}_i\}_{i=1}^{N}$ that contains N k-dimensional codewords $\mathbf{Y}_i = \{y_{i,j}\}_{j=1}^{k}$ should be trained and preshared beforehand. The original image is divided into nonoverlapping sub-blocks $\mathbf{V} = \{\mathbf{v}_j\}_{j=1}^{j=k}$. For each sub-block, the nearest codeword $\mathbf{Y}_i$ is found based on a minimum Euclidean distance by sequentially comparing $\mathbf{V}$ to the codewords $\mathbf{Y}_i$ of the codebook $\mathbf{CB}$. The Euclidean between $\mathbf{V}$ and $\mathbf{Y}_i$ is

$$D(\mathbf{V}, \mathbf{Y}_i) = \sum_{j=1}^{k} \left(v_j - y_{i,j}\right)^2, \quad (7)$$

where $y_{i,j}$ is the j-th component of the codeword $\mathbf{Y}_i$ and v_j is the j-th component of the image sub-block $\mathbf{V}$. When the nearest codeword $\mathbf{Y}_i$ is found, the corresponding index i is used to encode vector $\mathbf{V}$. After all sub-blocks of $\mathbf{V}$ are encoded, the original image can be represented by indices of these nearest codewords.

It is easy to reconstruct the original image from the VQ indexes based on the preshared codebook $\mathbf{CB}$ when VQ decoding is required. The decoding must conduct on each index to retrieve each sub-block of the original image.

3. The Proposed Encryption and Authentication Scheme

Our DRPE-CSVQ can achieve encryption and authentication simultaneously and efficiently. Figure 2 presents the flowchart of the encryption and hiding algorithm, from which one can find the four stages from the plain image to the final encrypted hidden image: DRPE, VQ, CS, and permutation-diffusion. The VQ encoder encodes the plain image into VQ indexes and the error matrix, and the DRPE transformation operates the same plain image into the binary image as authentication information. The obtained error matrix is permuted and compressed by CS to get the measurements. The combined image is constructed that includes the index vector, the quantized measurements, and the authentication information, followed by the encryption to generate the final encrypted hidden image. The following subsections will describe more details about the four stages.

3.1. Error Matrix Generation. Initially, the input plain image $\mathbf{I}_0 = \{I_0(x,y)\}_{x=1,y=1}^{M,N}$ of M rows and N columns is partitioned into small sub-blocks $\mathbf{SB} = \{\mathbf{sb}_i\}_{i=1}^{M\times N/l/l}$ of length $M \times N/l/l$. The element number l^2 in each sub-block equates to the dimension of a codeword. Then, we search for the closest matching codeword for each sub-block and allocate the corresponding index to the sub-block. All indexes constitute an index vector $\mathbf{z} = \{z_p\}_{p=1}^{M\times N/l/l}$ according to

$$z_p = \arg\min_j D(\mathbf{sb}_p, y_j). \tag{8}$$

To comply with the subsequent operations, we reshape the resultant vector into 2D matrix $\mathbf{z} = \{z(x,y)\}_{x=1,y=1}^{M,N/l/l}$. After all the encoded indexes are done VQ decoder, a reconstructed image $\mathbf{I}_{\text{vq}}$ that is much close to the input plain image $\mathbf{I}_0$ can be easily generated. The error $\mathbf{E}_1$ between the reconstructed image and the input plain is

$$\mathbf{E}_1 = \mathbf{I}_0 - \mathbf{I}_{vq}. \tag{9}$$

The reconstructed sub-block by VQ index might not be the same as the input sub-block as the preshared codebook **CB** impacts the reconstruction effect. A larger codebook has a higher chance of seeking the codeword that is precisely the best matching to the input sub-block but meanwhile means more time consumption for codebook training and vice versa. Moreover, there usually exist block artifacts in the reconstructed image $\mathbf{I}_{\text{vq}}$. To lessen the intrinsic dependency for the codebook, we fully leverage CS superiority to compress the error matrix.

3.2. Authentication Information Generation. The same plain image $\mathbf{I}_0 = \{I_0(x,y)\}_{x=1,y=1}^{M,N}$ of M rows and N columns is encoded by the DRPE transformation to generate a complex image composed of a phase image and an amplitude image. The amplitude image is discarded and only the phase image $\mathbf{P}_0 = \{P_0(x,y)\}_{x=1,y=1}^{M,N}$ is reserved as the output. The output phase image $\mathbf{P}_0 = \{P_0(x,y)\}_{x=1,y=1}^{M,N}$ is then quantized as a binary image $\mathbf{B} = \{B(x,y)\}_{x=1,y=1}^{M,N}$.

$$B(x,y) = \begin{cases} 1, & P_0(x,y) > 0, \\ 0, & \text{others}. \end{cases} \tag{10}$$

Then, every 8 bits of the binary image $\mathbf{B} = \{B(x,y)\}_{x=1,y=1}^{M,N}$ are combined into one pixel of the authentication information $\mathbf{Bp} = \{Bp(x,y)\}_{x=1,y=1}^{M,N/8}$.

3.3. Error Matrix Compression. Due to local regularities and global symmetries of nature images, different regions of the error matrix $\mathbf{E}_1$ have massive diversity in sparsities. To better use the same measurement matrix $\Phi \in \mathbb{R}^{M\times N}$ to compress all sub-blocks of the error matrix $\mathbf{E}_1$, the element distribution of the error matrix $\mathbf{E}_1$ must be uniform enough. Thus, we scramble the error matrix $\mathbf{E}_1$ with a pseudorandom sequence generated by the following modified Henon map function [36]:

$$\begin{cases} x_{k+1} = 1 - \alpha\cos(x_k) - \beta y_k, \\ y_{k+1} = -x_k, \end{cases} \tag{11}$$

where x_0 and y_0 are the initial values and α and β are the control parameters. The system is in a chaotic state when $\alpha = 3.85$ and $\beta = 0.3$. The initial parameter set $(x_0^{p_1}, y_0^{p_1}, \alpha^{p_1}, \beta^{p_1})$ as the permutation key iterates equation (11) for $M \times N$ times to generate the pseudorandom sequence $\mathbf{a} = \{a_t\}_{t=1}^{M\times C}$. Let the 1D vector of the error $\mathbf{E}_1$ be$\mathbf{e}_1 = \{e_1(t)\}_{t=1}^{M\times N}$, and the scrambled error vector $\mathbf{e}_2 = \{e_2(t)\}_{t=1}^{M\times N}$ is

$$e_2(t) = e_1(\overline{a}_t), \tag{12}$$

where $\overline{a}_t$ represents the element of the sorted-indexed vector $\overline{\mathbf{a}} = \{\overline{a}_t\}_{t=1}^{M\times C}$ generated by sorting the pseudorandom sequence $\mathbf{a} = \{a_t\}_{t=1}^{M\times C}$ in ascending order. And we can obtain the 2D permuted error matrix $\mathbf{E}_2 = \{E_2(x,y)\}_{x=1,y=1}^{M,N}$ by reshaping the vector $\mathbf{e}_2 = \{e_2(t)\}_{t=1}^{M\times N}$ into M rows and N columns.

After getting the much uniform error $\mathbf{E}_2$, we describe how to compress it with the same measurement matrix Φ. The sparse error $\mathbf{E}_2$ is split into nonoverlapping sub-blocks of size $l' \times l'$, and the elements of all sub-blocks are separately stretched into vector sets $\Lambda = \{\Lambda_t\}_{t=1}^{M\times N/l'/l'}$. If the number of nonzero values of each block is saved in $\text{NZ} = \{NZ_t\}_{t=1}^{M\times N/l_k}$, we can use a measurement matrix of size $M_k \times l_k$ $(l_k > M_k > NZ_t \text{ and } l_k = l' \times l')$ to compress each vector in Λ as follows:

$$\mathbf{y}_t = \Phi\mathbf{\Lambda}_t. \tag{13}$$

Since the newly generated low-dimensional measurements $\mathbf{y}_t$ are double-precision numeric type a uniform quantization is leveraged to map the values to the range $[0, 255]$,

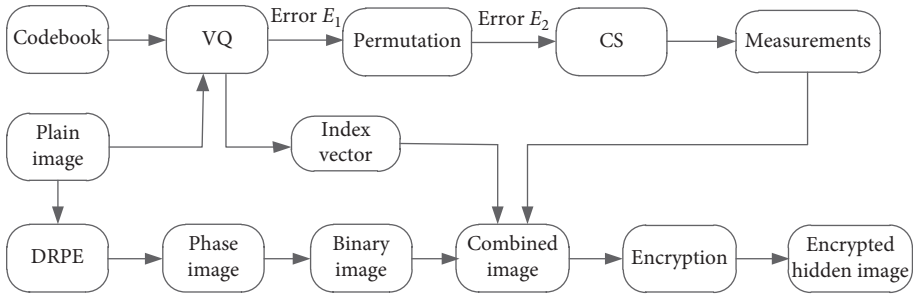


Figure 2: Flowchart of the encryption and hiding algorithm.

$$\mathbf{y}_t' = \text{floor}\left[\frac{255 \cdot \left(\mathbf{y}_t - \mathbf{y}_t^{\min}\right)}{\mathbf{y}_t^{\max} - \mathbf{y}_t^{\min}}\right], \tag{14}$$

where $\mathbf{y}_t^{\min}$ and $\mathbf{y}_t^{\max}$ are the minimum and maximum values in $\mathbf{y}_t$ and floor $(\cdot)$ is the rounding down operation. After all of the sub-blocks in $\mathbf{E}_2$ are compressed with the same measurement matrix, the resulting values constitute a measurement set $\mathbf{Y}_t' = \{\mathbf{y}_t'\}_{t=1}^{M\times N/ll'}$. Resizing it into a 2D matrix, we can get the measurements $\mathbf{Y}' = \{\mathbf{y}'(x,y)\}_{x=1,y=1}^{M\times N/l'/l'}$.

3.4. Self-Embedding and Encryption. In the VQ process, we use a codebook with 256 codewords of length $l \times l = 16$; thus, we can acquire the index vector of size $N_{vq} = \alpha_{vq} \times M \times N$ from the plain image, where $\alpha_{vq} = 1/16$. In the DRPE process, every 8 bits of the binary image are combined into one pixel of authentication information; thus, we can generate the authentication information of size $N_{\text{drpe}} = \alpha_{\text{drpe}} \times M \times N$ from the binary image, where $\alpha_{\text{drpe}} = 1/8$. In the CS process, let $l_k = l' \times l' = 16 \times 16$ and the sampling ratio be α_{cs}, the number of the measurements of each sub-block is then $M_k = \alpha_{cs} \times l_k$, and the number of the whole error matrices is $N_{cs} = M_k \times M \times N/l_k = \alpha_{cs} \times M \times N$. Thus, the total number of VQ indexes, authentication information, and measurements is $\mathrm{N}_{\text{total}} = M \times N \times (\alpha_{vq} + \alpha_{\text{drpe}} + \alpha_{cs})$. Since α_{vq} and α_{drpe} are two constants, the number $\mathrm{N}_{\text{total}}$ of all the data will be consistent with the size of the plain image when the sampling ratio is $\alpha_{cs} = 13/16$. Therefore, after obtaining the index matrix $\mathbf{z} = \{z(x,y)\}_{x=1,y=1}^{M,N/l/l}$ by Section 3.1, the authentication information $\mathbf{Bp} = \{Bp(x,y)\}_{x=1,y=1}^{M,N/8}$ by Section 3.2, and the measurement values $\mathbf{Y}' = \{\mathbf{y}'(x,y)\}_{x=1,y=1}^{M,N/l'/l'}$ by Section 3.3, a combined image $\mathbf{E}_{\mathbf{v}} = \{e_v(x,y)\}_{x=1,y=1}^{M,N}$ of the same size as the plain image can be obtained by appending them orderly:

$$\mathbf{E}_{\mathbf{v}} = [\,\mathbf{z},\ \mathbf{Y}',\ \mathbf{BP}\,]. \tag{15}$$

In the following, we will dedicate to the encryption based on a permutation and diffusion architecture. Using the other two sets of parameters $(x_0^{p_2}, y_0^{p_2}, \alpha^{p_2}, \beta^{p_2})$ and $(x_0^d, y_0^d, \alpha^d, \beta^d)$ to iterate equation (11) $M \times N$ times, two pseudorandom sequences $\mathbf{b} = \{b_t\}_{t=1}^{M\times N}$ and $\mathbf{c} = \{c_t\}_{t=1}^{M\times N}$ are generated, where $(x_0^{p_2}, y_0^{p_2}, \alpha^{p_2}, \beta^{p_2})$ is as the permutation key and $(x_0^d, y_0^d, \alpha^d, \beta^d)$ as the diffusion key. After sorting, we can get their sort-indexed vectors $\overline{\mathbf{b}} = \{\overline{b}_t\}_{t=1}^{M\times N}$ and $\overline{\mathbf{c}} = \{\overline{c}_t\}_{t=1}^{M\times N}$. Reshaping the combined image $\mathbf{E}_{\mathbf{v}}$ into a 1D vector $\mathbf{e}_{\mathbf{v}} = \{e_v(t)\}_{t=1}^{M\times N}$, we can perform permutation with $\overline{\mathbf{b}} = \{\overline{b}_t\}_{t=1}^{M\times N}$.

$$e_p(t) = e_v\left(\overline{b}_t\right). \tag{16}$$

To facilitate subsequent diffusion, we convert each element of the sort-indexed vector $\overline{\mathbf{c}} = \{\overline{c}_t\}_{t=1}^{M\times N}$ into an integer range $[0, 255]$.

$$\overline{\mathbf{c}} = \text{mod}\left(\text{floor}\left(\overline{\mathbf{c}} \times 10^{14}\right), 256\right). \tag{17}$$

The bitwise exclusive or diffusion is conducted according to equation (18) [37]:

$$e_d(t) = \left(e_p(t) + \overline{c}_t\right) \oplus \overline{c} \oplus e_d(t-1). \tag{18}$$

After rearranging all the elements of the diffused vector $\mathbf{e}_d = \{e_d(t)\}_{t=1}^{M\times N}$ into a 2D matrix, the final encrypted and hidden image $\mathbf{E}_d = \{e_d(x,y)\}_{x=1,y=1}^{M,N}$ is yielded.

3.5. Decryption and Authentication. The decryption and authentication are shown in Figure 3. The received image $\dot{\mathbf{E}}_d = \{\dot{e}_d(x,y)\}_{x=1,y=1}^{M,N}$ is restored into a combined image $\dot{\mathbf{E}}_{\mathbf{v}} = \{\dot{e}_v(x,y)\}_{x=1,y=1}^{M,N}$ by the inverse permutation and inverse diffusion with corresponding keys. If the predesignated image size is 256×256, we can extract the index matrix $\dot{\mathbf{z}} = \{\dot{z}(x,y)\}_{x=1,y=1}^{M,N/l/l}$ from the leftmost 16 columns of the combined image $\dot{\mathbf{E}}_{\mathbf{v}}$ and reconstruct the image $\dot{\mathbf{I}}_{\text{vq}}$ with the aid of the preshared codebook $\mathbf{CB}$. In addition, we can extract the authentication information $\dot{\mathbf{Bp}} = \left\{\dot{Bp}(x,y)\right\}_{x=1,y=1}^{M,N/8}$ from the rightmost 32 columns of the combined image $\dot{\mathbf{E}}_{\mathbf{v}}$ and the measurements $\dot{\mathbf{Y}}' = \{\dot{\mathbf{y}}'(x,y)\}_{x=1,y=1}^{M,N/l'/l'}$ from the rest part of the image. To reconstruct the error matrix $\dot{\mathbf{E}}_2 = \left\{\dot{E}_2(x,y)\right\}_{x=1,y=1}^{M,N}$ from the extracted measurements, we divide the measurements into small nonoverlapping sub-blocks $\dot{\mathbf{Y}}' = \{\mathbf{y}_t'\}_{t=1}^{M\times N/l'\times l'}$ and then inversely quantize each sub-block by

$$\dot{\mathbf{y}}_t = \frac{\dot{\mathbf{y}}_t' \times \left(\mathbf{y}_t^{\max} - \mathbf{y}_t^{\min}\right)}{255} + \mathbf{y}_t^{\min}. \tag{19}$$

Then, we solve the ℓ_1-norm optimization:

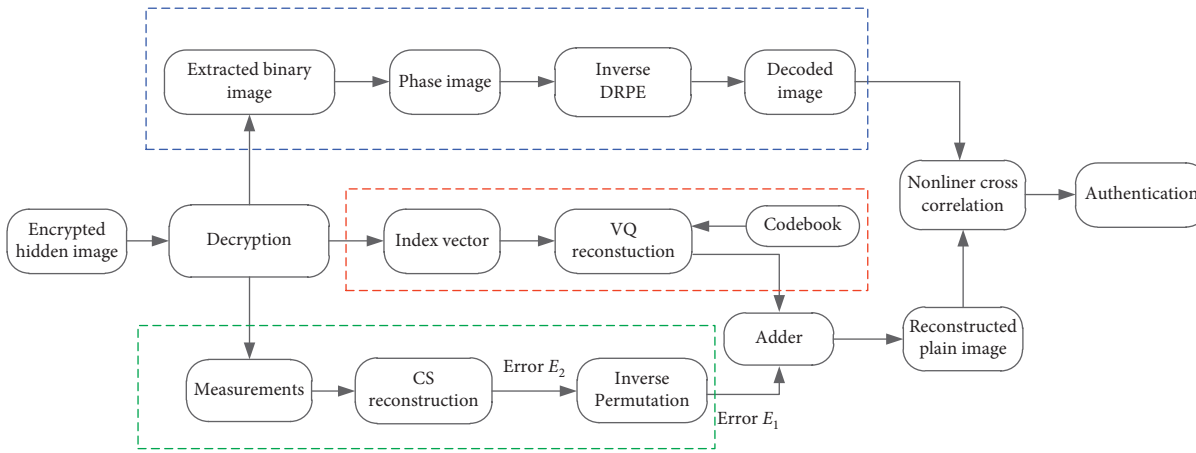


Figure 3: Flowchart of the decryption and authentication algorithm.

$$\widehat{\mathbf{s}}_t = \arg\min \left\|\dot{\mathbf{s}}_t\right\|_1, \text{s.t. } \Phi\Psi\dot{\mathbf{s}}_t = \dot{\mathbf{y}}_t, \tag{20}$$

where Ψ is a dictionary of size $l_k \times l_k$ and $\dot{\mathbf{s}}_t$ is the spare coefficient. Based on the newly generated coefficients $\widehat{\mathbf{s}}_t$, we can reconstruct the elements of the sub-block $\dot{\Lambda}_t$ from the measurements $\dot{\mathbf{y}}_t$.

$$\dot{\mathbf{\Lambda}}_t = \Psi\widehat{\mathbf{s}}_t. \tag{21}$$

Following the elements of all sub-blocks $\dot{\Lambda} = \left\{\dot{\Lambda}_t\right\}_{t=1}^{M\times N/l'/l'}$ which are generated, we reshape them into a matrix $\dot{\mathbf{E}}_2 = \left\{\dot{E}_2(x,y)\right\}_{x=1,y=1}^{M,N}$ and perform an inverse permutation on the matrix to generate the reconstructed error $\dot{\mathbf{E}}_1 = \left\{\dot{E}_1(x,y)\right\}_{x=1,y=1}^{M,N}$. The final reconstructed image $\mathbf{I}_{re} = \left\{\mathbf{I}_{re}(x,y)\right\}_{x=1,y=1}^{M,N}$ is

$$\mathbf{I}_{re} = \mathbf{I}_{vq} + \dot{\mathbf{E}}_1. \tag{22}$$

In addition, the authentication information, namely, the extracted $\mathbf{Bp}$, is transformed into a binary image and is quantized inversely into a phase image $\dot{\mathbf{P}}_0 = \left\{\dot{\mathbf{P}}_0(x,y)\right\}_{x=1,y=1}^{M,N}$.

$$\dot{\mathbf{P}}_0(x,y) = \begin{cases} -\pi, & \dot{B}p(x,y) = 0, \\ \pi, & \dot{B}p(x,y) = 1. \end{cases} \tag{23}$$

The obtained phase image $\dot{\mathbf{P}}_0$ is sparse, and it can be viewed as an input image and decrypted using the inverse DRPE to generate the decoded image $\dot{\mathbf{I}}_0 = \left\{\dot{\mathbf{I}}_0(x,y)\right\}_{x=1,y=1}^{M,N}$. The decoded image $\dot{\mathbf{I}}_0$ is not visually recognized, but we can authenticate it with an advanced statistical nonlinear cross-correlation. The nonlinear cross-correlation transformation coefficient $cc = \{cc(x,y)\}$ between the decoded image $\dot{\mathbf{I}}_0$ and the target image $\mathbf{I}_t = \left\{\mathbf{I}_t(x,y)\right\}_{x=1,y=1}^{M,N}$ is calculated by

$$cc(x,y) = FT^{-1}\left(\left|\mathbf{I}_t(\mu,\eta)\dot{\mathbf{I}}_0(\xi,\upsilon)\right|^k e^{\left(\varphi_{\mathbf{I}_t}(\mu,\eta)-\varphi_{\dot{\mathbf{I}}_0}(\xi,\upsilon)\right)}\right), \tag{24}$$

where $\mathbf{I}_t(\mu,\eta)$ and $\dot{\mathbf{I}}_0(\xi,\upsilon)$ are the 2D Fourier transforms of the target image $\mathbf{I}_t$ and the decoded image $\dot{\mathbf{I}}_0$, $\varphi_{I_t}(\mu,\eta)$ and $\varphi_{\dot{\mathbf{I}}_0}(\xi,\upsilon)$ are the phase signals of $I_t(\mu,\eta)$ and $\dot{\mathbf{I}}_0(\xi,\upsilon)$, FT^{-1} is the inverse Fourier transform, and k denotes the strength of the applied nonlinearity. The value of k is often set to 0.3 [28]. To quantitatively measure the correlation between the decoded image $\dot{\mathbf{I}}_0$ and the target image $\mathbf{I}_t$, peak-to-correlation energy (PCE) is calculated with

$$\text{PCE} = \frac{\max\left(|cc(x,y)|^2\right)}{\sum_{x=1}^{M}\sum_{y=1}^{N}|cc(x,y)|^2}, \tag{25}$$

where $\max(\cdot)$ is a maximum function. A higher PCE value indicates a stronger correlation between the decoded image $\dot{\mathbf{I}}_0$ and the target image $\mathbf{I}_t$.

3.6. Discussion. Based on the above procedures, the proposed method can achieve optical authentication for the noise-like and unrecognizable images in resource-constrained environments, and this will be detailedly analyzed in the next Section 4.2.1. The binary image generated by the DRPE technology serves as the authentication information, and the time complexity of this process is low due to the parallel processing trait of optical DRPE. In addition, compensating the reconstructed error information on the VQ image can obtain a better final reconstructed image quality, making the decrypted noise-like authentication information and the final reconstructed image authenticated with a higher probability.

On the other hand, the purpose of generating encrypted images containing authentication bits is to protect users' copyright information in insecure cloud-based environments. For example, to use the resources in the cloud data centers, the users needed to update the multimedia data onto the cloud servers in advance. Upon updating to cloud servers, the user can retrieve the data when needed from any location, whereas transmitting the data to cloud servers managed by third-party servers may lead to security and privacy issues. It is vital to settle the security concerns involved in cloud computing. Fortunately, the security of stored content can be premanaged by application of the

conventional encryption designs. However, if unwanted processing occurs in an insecure cloud, ensuring users' copyright is a real challenge. Thus, it is necessary to embed authentication information into the encrypted domain.

4. Experimental Results and Performance Analyses

4.1. Experiment Results. We exploit multiple plain images from the USC-SIPI image database [38] to verify the effectiveness of the proposed method. All experiments are conducted by MATLAB R2012b software on a 64-bit Windows 7 PC with 16.0 GB random-access memory (RAM) and Inter(R) Core(TM) i7-4770 CPU @ 3.40 GHz. The standard test image "Camera" of size 256×256 is used to test the effectiveness of the proposed method. Figure 4 shows the detailed implementations on encryption and hiding, and Figure 5 shows the implementations on decryption and authentication. In our experiments, if the sampling ratio α_{cs} is smaller than 13/16, the final encrypted and hidden image will be compressed; otherwise, it will not be compressed. In Figures 4 and 5, the sampling ratio is fixed as $\alpha_{cs} = 13/16$.

The input image, the phase image obtained by DRPE, the binary image generated by the quantization, the VQ image reconstructed by the preshared codebook, and the error matrix between the plain image and the reconstructed VQ image are shown in Figures 4(a)–4(e); and the permuted error matrix, the measurements by CS, the combined image, the permuted image, and the final encrypted and hidden image diffused are shown in Figures 4(f)–4(j). It follows from Figure 4(e) that smaller values or 0 values are full of the whole error matrix; thus, the error matrix is much sparse than the input image. In addition, the permutation process has made the distribution of nonzero values of the error matrix more uniform in Figure 4(f); thus, using the same measurement matrix to compress all sub-blocks of the error matrix will have little or no impact on the error reconstruction. And, one can find intuitively from Figure 4(h) that the VQ index matrix, the measurements, and the authentication information have been aligned orderly in the combined image. At last, the incomprehensible and noise-like image in Figure 4(j) indicates no information leakage compared to the original input.

Figure 5 shows the detailed implementations of decryption and authentication. We know that the VQ image reconstructed from the extracted VQ indexes has noticeable block artifacts in Figure 5(d), while no such issue appears in Figure 5(f). Moreover, the PSNR value between the VQ image in Figure 5(d) and the input image in Figure 4(a) is 24.8878 dB, but the value reaches 40.2863 dB for the final reconstructed image in Figure 5(f) and the input image in Figure 4(a). Thus, the reconstructed error in Figure 5(e) fulfills better information compensation to the VQ image, facilitating subsequent authentication based on a nonlinear cross-correlation coefficient strategy. The authentication information extracted from the rightmost 32 columns of Figure 5(c) is converted into Figure 5(g) and then inversely quantized to the phase image in Figure 5(h). The noisy decoded image in Figure 5(i) are difficult to recognize with naked eyes virtually but have been successfully authenticated in Figure 5(j) based on a nonlinear cross-correlation between it and the reconstructed image in Figure 5(f), the authentication of which is a blind process since it is needless for the participation of the plain image in Figure 4(a).

4.2. Performance Analyses

4.2.1. Compressibility. The compression ratio of our DRPE-CSVQ is defined as the ratio of the final encrypted hidden image to the plain image:

$$\alpha_{cr} = \frac{\left(N_{vq} + N_{\text{drpe}} + N_{cs}\right)}{(M \times N)} = \alpha_{vq} + \alpha_{\text{drpe}} + \alpha_{cs}, \tag{26}$$

where N_{vq}, N_{drpe}, and N_{cs} are the sizes, respectively, from the index matrix, the authentication information, and the measurements, α_{cs} and α_{cr} represent the sampling ratio and the compression ratio, $\alpha_{\text{drpe}} = 1/8$, and $\alpha_{vq} = 1/16$. If the sampling ratio α_{cs} is smaller than 13/16, our DRPE-CSVQ can implement three functions of compression, encryption, and authentication simultaneously. Figure 6 shows the detailed implementations at compression ratio $\alpha_{cs} = 5/8$ with multiple test images "Camera," "Lena," and "Baboon" of sizes 256×256 as inputs. At first, the inputs "Camera," "Lena," and "Baboon" are encoded using the encryption and hiding algorithm to generate the corresponding compressed and encrypted images shown in Figures 6(a1)–6(a3). Then these are decoded using the decryption and authentication algorithm to obtain the reconstructed images in Figures 6(e1)–6(e3) and the decoded images in Figures 6(f1)–6(f3), thus achieving the authentications in Figures 6(g1)–6(g3). The reconstruction quality is evaluated with peak signal-to-noise ratio (PSNR) value, and the authentication result is quantitatively testified by PCE value. The PSNR results of VQ images generated by extracted VQ indexes (in Figures 6(c1)–6(c3)) are 24.7856 dB, 26.0553 dB, and 24.8610 dB while the PSNRs of final reconstruction images (in Figures 6(e1)–6(e3)) reach 29.9680 dB, 29.5055 dB, and 26.3824 dB, respectively. The PSNRs of our DRPE-CSVQ reconstruction are all much larger than the PSNRs of VQ reconstruction for the same image, so the reconstructed error matrices (in Figures 6(d1)–6(d3)) have freed up codebook dependency for VQ reconstruction. Besides, the correlation planes between the final reconstruction images (in Figures 6(e1)–6(e3)) and the decoded images (in Figures 6(f1)–6(f3)) have exhibited high peaks at the centers and possess the PCE values of 0.0064, 0.0030, and 0.0033, respectively, which indicate that the proposed method successfully authenticates all images at compression ratio $\alpha_{cr} = 5/8$.

Besides, Figure 7 shows the correlation planes at different compression ratios. Figures 7(a)–7(d) show the correlation planes at compression ratios $\alpha_{cs} = 13/16$, $\alpha_{cs} = 5/8$, $\alpha_{cs} = 7/16$, and $\alpha_{cs} = 1/4$, respectively. From Figure 7, we can easily find the high peak from the center of each correlation plane; thus, the reconstruction image has a strong correlation with the authentication information. To make a more quantitative analysis of the authentication result, we calculate the PCE values of all the correlation planes, the values of which are 0.0067, 0.0064, 0.0055, and

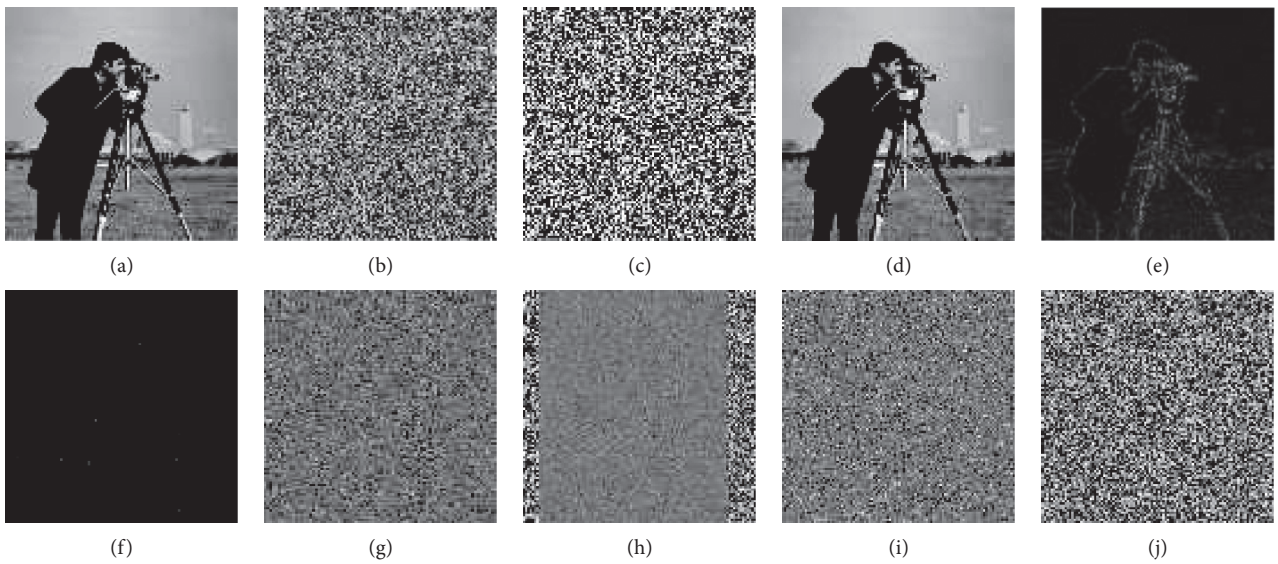


Figure 4: Detailed experimental results for the encryption and hiding. (a) Input image; (b) phase image by DRPE; (c) binary image by quantization; (d) VQ image reconstructed by preshared codebook; (e) error matrix between (a) and (d); (f) permuted error matrix with $(x_0^{p_1}, y_0^{p_1}, \alpha^{p_1}, \beta^{p_1})$; (g) measurements by CS; (h) combined image; (i) permuted image with $(x_0^{p_2}, y_0^{p_2}, \alpha^{p_2}, \beta^{p_2})$; (j) the final encrypted and hidden image with $(x_0^d, y_0^d, \alpha^d, \beta^d)$.

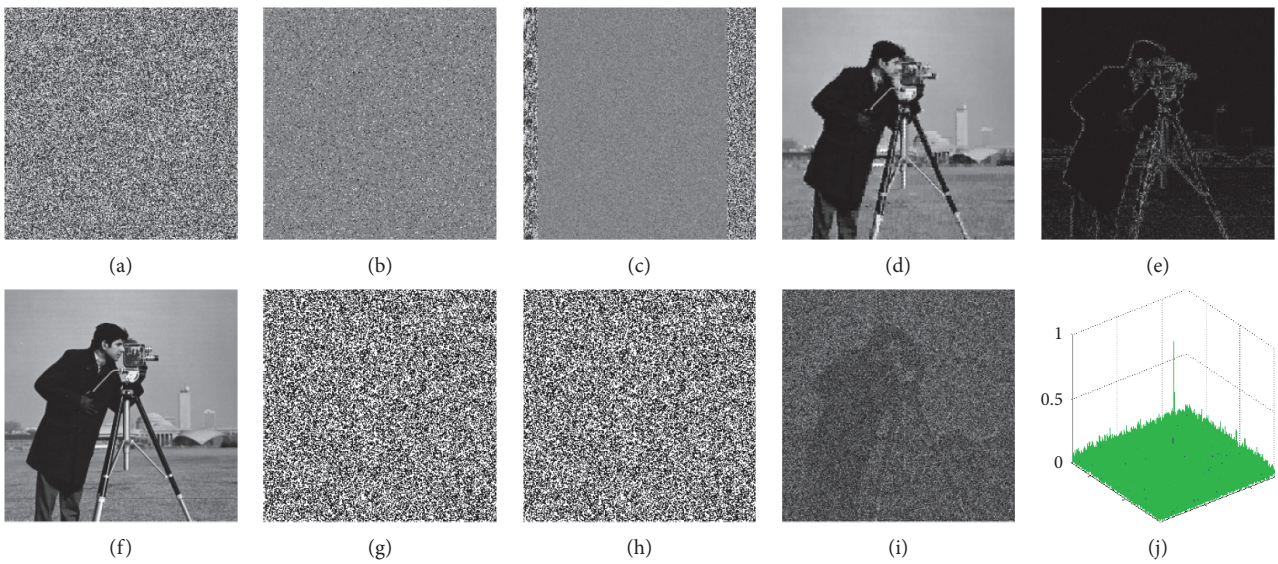


Figure 5: Detailed experimental results for the decryption and authentication. (a) Received image; (b) only-permuted image by inverse-diffusion; (c) combined image by inverse permutation; (d) VQ image with preshared codebook (PSNR = 24.8878); (e) error matrix by CS reconstruction and inverse permutation; (f) reconstructed image with (d) and (e) (PSNR = 40.2863); (g) converted binary image by extracted authentication from (c); (h) extracted phase image by inverse quantization (g); (i) decoded image by inverse DRPE; (j) authentication with (f) and (i) (k = 0.3, PCE = 0.0077).

0.0048, respectively, thus again testifying the authentication ability of our DRPE-CSVQ. Meanwhile, we also execute simulations of multiple plain images and compute the average of PSNRs (APSNRs) to test the reconstructed quality of our DRPE-CSVQ at different compression ratios. Table 1 lists the comparison results among the proposed method and the methods in BLP-CS [39], BCS-In [40], and DRPE-BCS [29]. Table 2 presents all parameter settings of these comparisons. We can find from Table 1 that our DRPE-BCS is greater than the other three approaches at least 1 dB at compression ratio 30%, and at least 2 dB when compression ratio equals 20%. Thus, our DRPE-CSVQ provides a more powerful compression property while keeping image quality.

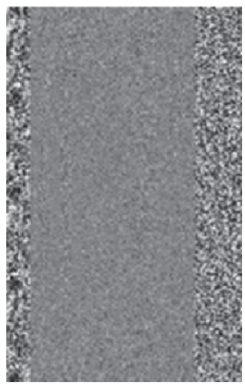
Since we dedicate to the two concerns above [29], we give detailed numerical comparisons. Figure 8 presents comparison

(a1)

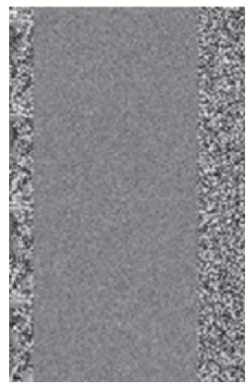
(a2)

(a3)

(a)



(b1)



(b2)

(b3)

(b)

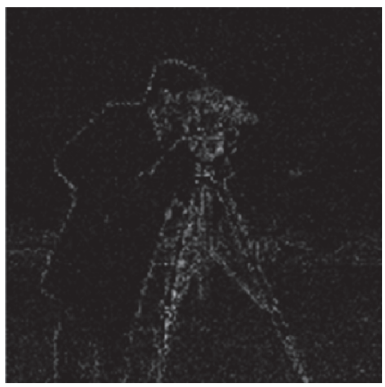
(c1)

(c2)

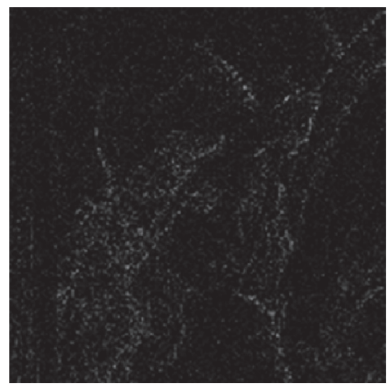
(c3)

(c)

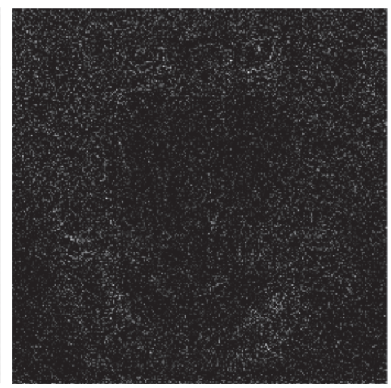
Figure 6: Continued.



(d1)



(d2)



(d3)

(d)

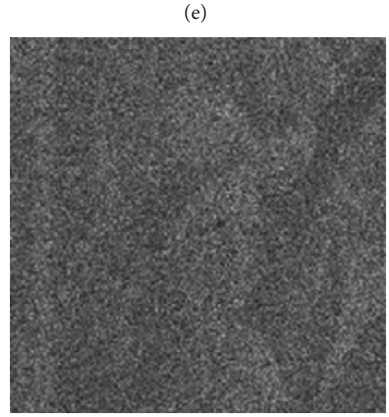
(e1)

(e2)

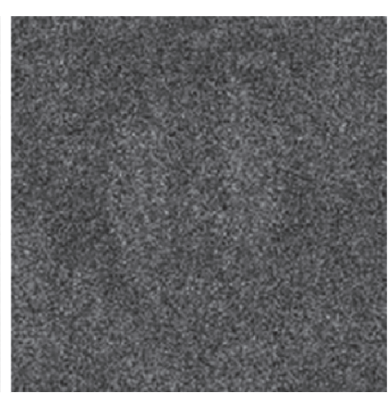
(e3)

(e)

(f1)



(f2)



(f3)

(f)

Figure 6: Continued.

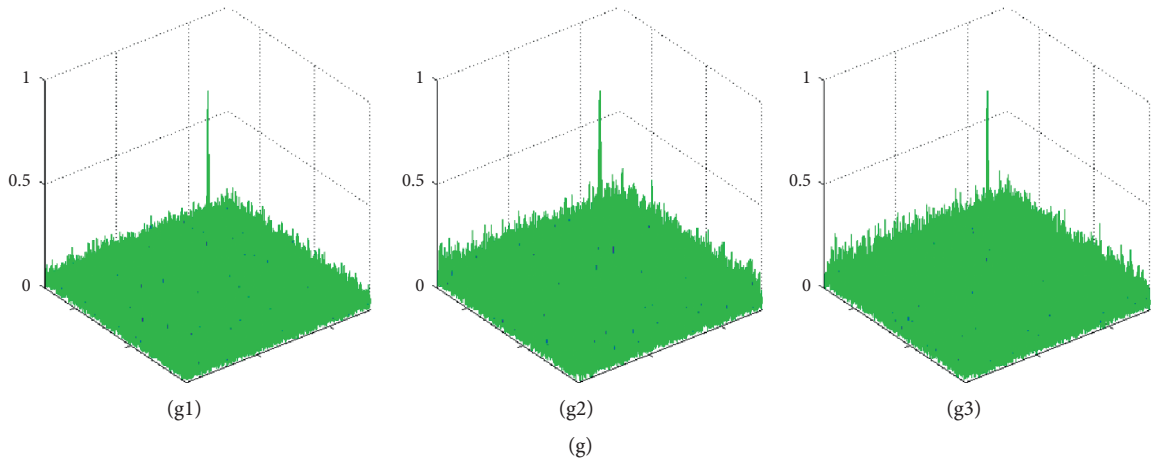


Figure 6: Compression and encryption with authentication ability when compression ratio is 5/8. (a, b, c, d, e, f, g-1, 2, 3) Standard images "Camera," "Lena," and "Baboon" of sizes 256 × 256 used for testing; (a-1, 2, 3) final encrypted and hidden image (i.e., the received image); (b-1, 2, 3) combined image by inverse permutation and inverse diffusion; (c-1, 2, 3) VQ image reconstructed by preshared codebook; (d-1, 2, 3) error matrix by CS and inverse permutation; (e-1, 2, 3) reconstructed image with (c-1, 2, 3) and (d-1, 2, 3); (f-1, 2, 3) decoded image by inverse DRPE; (g-1, 2, 3) authentication with (e-1, 2, 3) and (f-1, 2, 3).

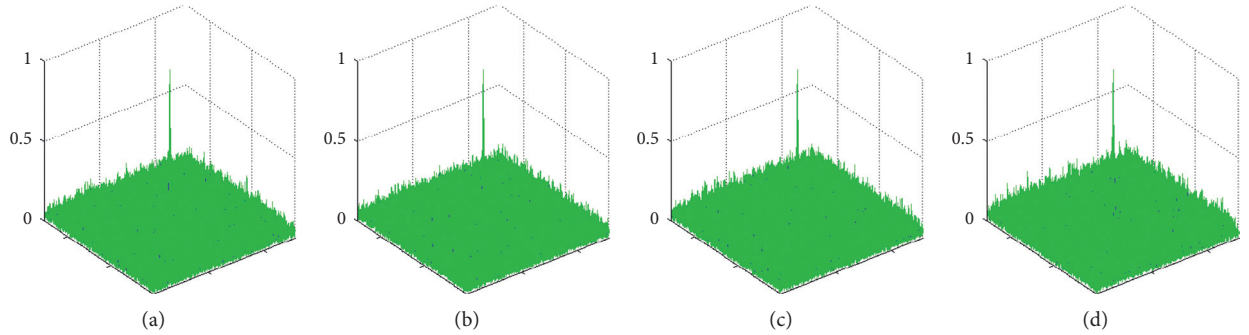


Figure 7: Correlation planes at different compression ratios. (a) Correlation planes with compression ratio α_{cs} = 13/16; (b) correlation planes with compression ratio α_{cs} = 5/8; (c)correlation planes with compression ratio α_{cs} = 7/16; (d) correlation planes with compression ratio α_{cs} = 1/4.

Table 1: Comparisons on APSNRs of reconstructed images at different sampling rates.

Image	Algorithm	20%	30%	50%	70%
Camera	BLP-CS [39]	21.2134	24.8215	28.6241	32.9325
	BCS-In [40]	18.0314	21.5327	27.4108	32.8574
	BCS-DRPE [29]	17.0794	22.3241	26.9541	32.4573
	VQCS-DRPE	**25.4512**	**25.9545**	**28.3244**	32.1575
Lena	BLP-CS [39]	23.6405	27.5214	31.4421	35.7324
	BCS-In [40]	19.5241	23.3256	27.3125	32.1542
	BCS-DRPE [29]	23.9345	27.4571	32.7794	37.9847
	VQCS-DRPE	**27.7841**	**29.3245**	**32.9394**	37.4765
Baboon	BLP-CS [39]	18.8341	20.2345	22.6243	25.8341
	BCS-In [40]	14.7214	17.6211	21.3098	25.2132
	BCS-DRPE [29]	20.3842	21.9848	24.0153	27.3547
	VQCS-DRPE	**25.9657**	**25.1214**	**26.3254**	**27.3655**
Peppers	BLP-CS [39]	23.9135	27.2187	30.9455	34.7241
	BCS-In [40]	18.4241	22.6324	27.9357	32.5048
	BCS-DRPE [29]	21.0541	26.3545	31.8258	37.1323
	VQCS-DRPE	**25.9616**	**27.3547**	31.4575	36.7724

Bold values show that the results of our method are superior to the compared results.

results, where the standard image "Camera" is still the input image. Figure 8(a) shows the PSNR value of the reconstructed image, and Figure 8(b) shows the corresponding PCE value of the authentication result. One can see that our method is wholly better than [29] when the compression ratio is smaller than 0.5 and comparable to [29] when the compression ratio is larger than 0.5. Both PSNR and PCE values in our method decline slowly and entirely outperform the values in [29] while the compression ratio is less than 0.5. The two processes in [29] have a quick decline because the input image "Camera" in [29] was as direct input of CS that makes the reconstructed image accordingly decline with the reduction of the compression ratio. As a contrast, we select a sparser error matrix as CS input. The reconstructed error matrix by CS exclusively achieves information compensation to the VQ reconstructed image; thus, the reconstruction quality of our method was not substantially affected by the descent of compression ratios. In short, our approach can well ensure the restoration precision of the reconstructed image, thereby equipped with more robust authentication capability.

Table 2: Parameter settings of these comparisons.

Algorithm	Size of input image	Input of CS	Sparsity basis?	Block size	$\alpha_{cr} = \alpha_{cs}$?
BLP-CS [39]	256 ∗ 256	Plaintext	FrFT	16 ∗ 16	Yes
BCS-In [40]	256 ∗ 256	Plaintext	LT	16 ∗ 16	Yes
BCS-DRPE [29]	256 ∗ 256	Plaintext	DWT	16 ∗ 16	$\alpha_{cr} = \alpha_{cs} + 1/8$
VQCS-DRPE	256 ∗ 256	Error	No	4 ∗ 4/VQ, 16 ∗ 16/CS	$\alpha_{cr} = \alpha_{cs} + 3/16$

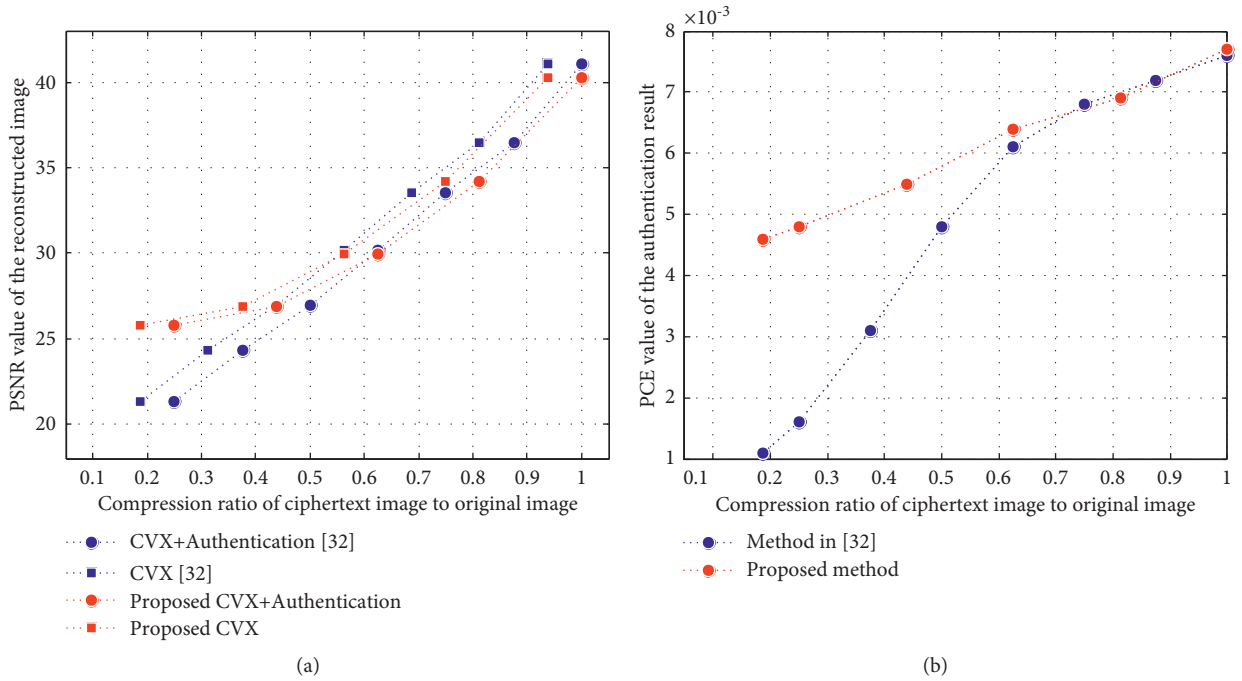


Figure 8: Comparisons on PSNR values and PCE values for [29] and the proposed method under different compression ratios. (a) PSNR values vary with different compression ratios. (b) PCE values vary with different compression ratios.

4.2.2. Histogram Analysis. Figure 9 shows the histograms of the plain image and the encrypted images at compression ratios of $\alpha_{cr} = 1$, $\alpha_{cr} = 13/16$, $\alpha_{cr} = 5/8$, $\alpha_{cr} = 7/16$, and $\alpha_{cr} = 1/4$, respectively. It is clear that as compression ratios decrease, the total numbers of pixels in the cipher images shrink accordingly. Still, all histograms of the cipher images are uniformed, and none of the valuable information is leaked to the adversary. Although the purpose of error matrix permutation is to make the signal as evenly distributed as possible to be compressed by the same measurement matrix and obtain a more efficient reconstruction of the signal later, the permutation also makes the measurements by CS have a similar distribution. Besides, the subsequent permutation and diffusion render the pixel intensities of the combined image uniformly distributed in the range of [0,255]. Thus, we can conclude that the proposed scheme tackles the energy leakage issue.

4.2.3. Correlation Analysis. The correlation among adjacent pixels of an image is a vital criterion to assess encryption security. Here, we randomly select 2000 adjacent pixel pairs in horizontal, vertical, and diagonal directions from the plain "Camera" and the corresponding encrypted image to test the correlation results. Figure 10 shows the correlation distributions of "Camera" and the corresponding encrypted image in the three directions. Two adjacent pixels in the input plain "Camera" are highly correlated. In contrast, the correlation between two adjacent pixels in the encryption version is weak enough and almost disrupted to a randomness pattern. The distributions of the vertical and diagonal directions possess similar modalities.

In addition, to quantitatively analyze this, correlation coefficients are calculated:

$$C_{xy} = \frac{L_s \sum_{i=1}^{L_s} (x_i y_i) - \sum_{i=1}^{L_s} x_i \sum_{i=1}^{L_s} y_i}{\sqrt{\left(L_s \sum_{i=1}^{L_s} x_i^2 - \left(\sum_{i=1}^{L_s} x_i\right)^2\right)\left(L_s \sum_{i=1}^{L_s} y_i^2 - \left(\sum_{i=1}^{L_s} y_i\right)^2\right)}}, \tag{27}$$

where x_i and y_i are the values of two adjacent pixels and L_s is the total number of selected pixel pairs. Table 3 lists the correlation coefficients of plain images and those of the corresponding encrypted versions. The results show that the coefficients for the encrypted images are all sufficiently low, indicating that the proposed method is equipped with a better encryption effect. In Table 4, we compare ours with other encryption schemes [41–43]. We can see that our method outperforms them in three directions. The chaotic operation in our system engages VQ indexes, error

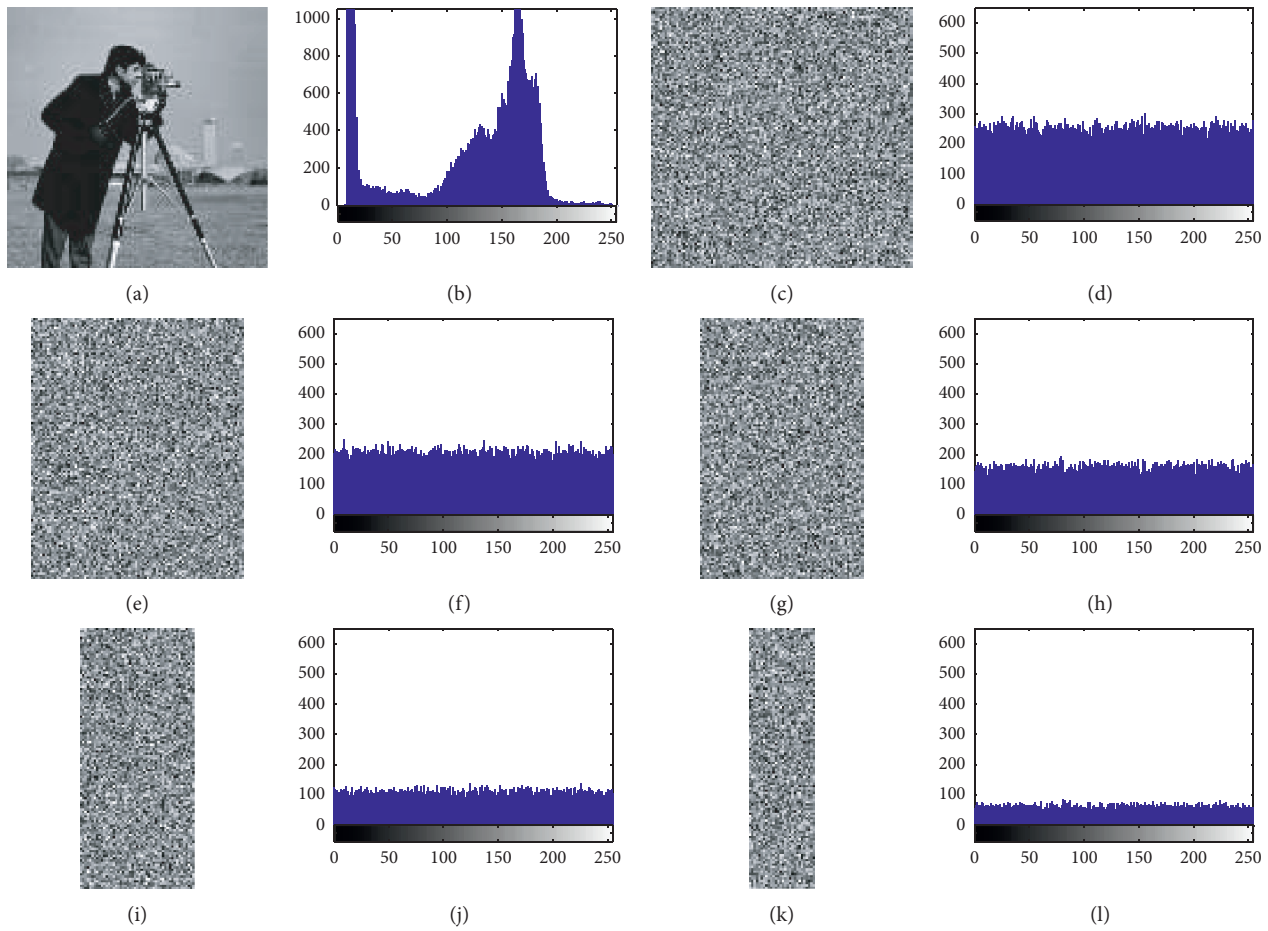


Figure 9: Histograms for the plain "Camera" image and the corresponding encrypted images under different compression ratios. (a) Plain "Camera" image; (b) histogram of (a); (c) encrypted image of the same size as (a); (d) histogram of (c); (e) encrypted image under $\alpha_{cr} = 13/16$; (f) histogram of (e); (g) encrypted image under $\alpha_{cr} = 5/8$; (h) histogram of (g); (i) encrypted image under $\alpha_{cr} = 7/16$; (j) histogram of (i); (k) encrypted image under $\alpha_{cr} = 1/4$; (l) histogram of (k).

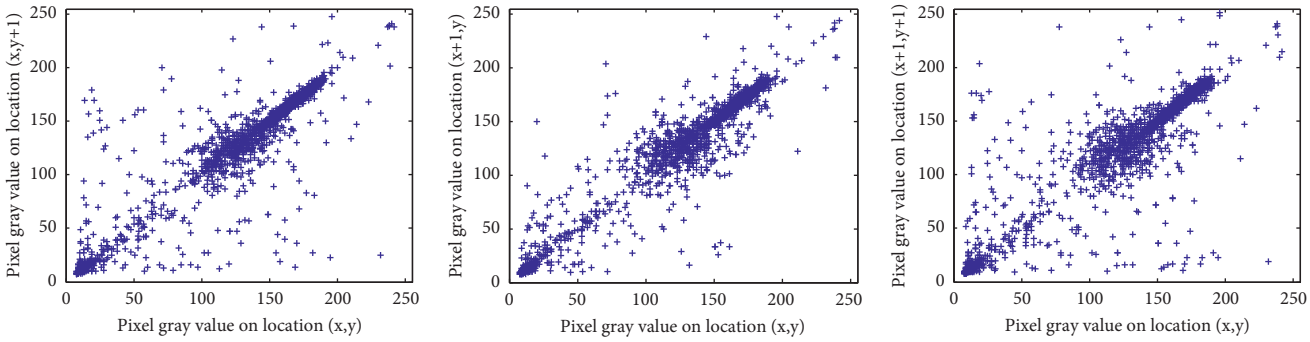
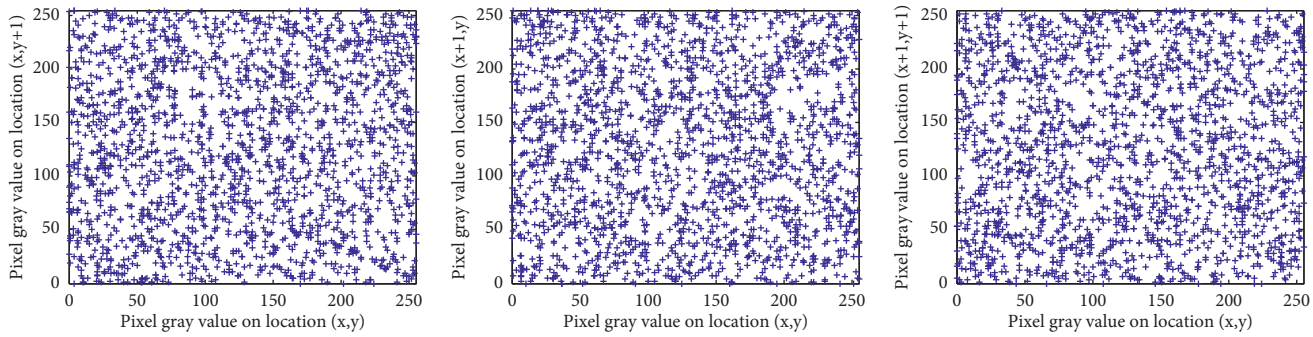


Figure 10: Continued.



(d) (e) (f)

Figure 10: Correlations of the plain "Camera" image of 256 × 256 and the corresponding encrypted image of the same size in different directions. (a–c) Horizontal, vertical, and diagonal correlations of the plain "Camera" image; (d–f) horizontal, vertical, and diagonal correlations of the final encrypted image.

Table 3: Correlation coefficients between adjacent pixels.

Image	Original image			Encrypted image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Camera	0.9334	0.9592	0.9086	0.0032	−0.0007	0.0005
Lena	0.9458	0.9720	0.9211	−0.0025	0.0058	−0.0075
Baboon	0.8733	0.8273	0.7854	0.0054	0.0038	0.0000
Peppers	0.9610	0.9670	0.9296	0.0057	−0.0020	0.0028

Table 4: Comparisons on mean correlation coefficients for various methods.

Direction	Mean correlation coefficients			
	Ref. [41]	Ref. [42]	Ref. [43]	Ours
Horizontal	0.0124	0.0127	0.0132	0.0032
Vertical	0.0070	0.0117	0.0078	0.0025
Diagonal	0.0050	0.0235	0.0182	0.0031

measurements, and authentication information, whereas the operation in other systems engages raw images. These combined VQ indexes, error measurements, and authentication information have a much lower correlation than pixels in nature images. Therefore, our method has stronger robustness to resist correlation-based statistical attacks.

4.2.4. Information Analysis. Information entropy is used to measure the uncertainty and randomness associated with a random variable. The entropy value of a random variable is defined as

$$H(x) = -\sum_{i=1}^{N} p(x_i)\log_2 p(x_i), \tag{28}$$

where $p(x_i)$ is the probability of appearance of x_i. The bigger the information entropy of the cipher image is, the more secure the cryptosystem is. Table 5 lists the entropies of the plain images and the corresponding encrypted versions. One can see that the proposed method is better than the works [42, 43], and the entropies change within a very narrow range, which means that the information leakage of the proposed method is negligible. Thus, our approach can well resist entropy-based statistical analysis.

4.2.5. Differential Attack Analysis. To test the sensitivity to plain image, we randomly select one pixel from each plain image and modify the last bit of the pixel at the same location to obtain the corresponding modified plain image. The original and modified plain images are encrypted with the same keys, and we get two encrypted images. The two encrypted images are evaluated quantitatively by the number of pixels change rate (NPCR) and unified average changing intensity (UACI):

$$\begin{aligned} \text{NPCR} &= \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times 100\%, \\ \text{UACI} &= \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{\left|C_1(i,j) - C_2(i,j)\right|}{255} \times 100\%, \end{aligned} \tag{29}$$

where C_1 and C_2 are two encrypted images obtained by a slight change in the chosen plaintext image and $D(i,j)$ is defined as

Table 5: Information entropies for various methods.

Image	Information entropies				
	Plaintext	Ref. [41]	Ref. [42]	Ref. [43]	Ours
Camera	7.0097	7.9966	7.9955	7.9964	7.9984
Lena	7.2045	7.9951	7.9965	7.9984	7.9983
Baboon	7.0091	7.9947	7.9963	7.9954	7.9982
Peppers	7.5813	7.9965	7.9958	7.9982	7.9984

Table 6: NPCR and UACI values for various methods.

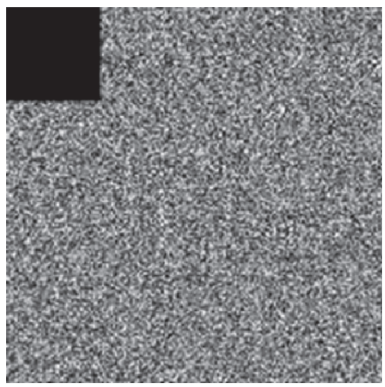
Image	(NPCR (%); UACI (%))			
	Ref. [41]	Ref. [42]	Ref. [43]	Ours
Camera	(99.63, 33.71)	(99.57, 33.37)	(99.61, 33.69)	(99.60, 33.48)
Lena	(99.61, 33.56)	(99.55, 33.34)	(99.61, 33.63)	(99.61, 33.49)
Baboon	(99.60, 33.52)	(99.54, 33.32)	(99.60, 33.61)	(99.60, 33.51)
Peppers	(99.61, 33.63)	(99.58, 33.35)	(99.62, 33.74)	(99.61, 33.50)

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j), \\ 1, & C_1(i,j) \neq C_2(i,j). \end{cases} \tag{30}$$

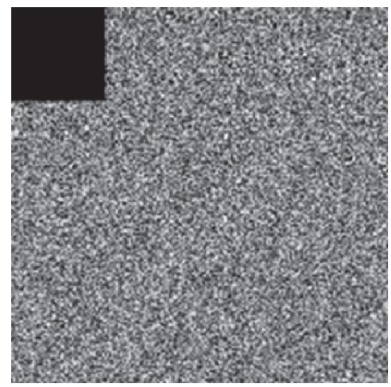
The results are tabulated in Table 6 and compared with the works [41–43]. As seen, our method outperforms the works [41–43] either in NPCR or in UACI. Unlike the results in [41–43], one-pixel variation in two plain images will make at least one pixel changed markedly in the corresponding two encrypted images. In our method, if making the slightest bit of a randomly chosen pixel changed, the two encrypted images may be the same because a tiny change perhaps does not impact the index vector or change authentication information and measurements. It may change one index or 8-bit depth authentication information or error measurements if replacing a chosen pixel by a random value. These changed pixels may influence almost all the pixels of the encrypted image through the subsequent diffusion phase. Thus, our method has a better ability to resist differential attacks.

4.2.6. Cropping Attack Analysis. If the sampling ratio is $\alpha_{cr} = 13/16$, the encrypted image has the same size as the input plain image. The indispensable VQ indexes hold solely 6.25% pixels of the whole encrypted image, and the authentication information and the error information occupy 12.5% and 81.25%, respectively. The VQ indexes share a much smaller number of pixels than the error data while saving the most information of the input plain image. When the encrypted image is subjected to attacks, the probability of the damaged index data will be much smaller than that of error data, and even after being damaged, the damaged indexes can be replaced with the undamaged neighbor indexes. Theoretically, the DRPE-CSVQ can ensure the image restoration quality to a certain degree. Figure 11 also gives the experiment results of the proposed method under cropping attack with the cropping size 64×64. The first column to the third column presents detailed image reconstructions and authentications with multiple standard images "Camera," "Lena," and "Baboon." We can see from the second row that there are full of different types of noises, indicating that the error matrix and the VQ indexes are both destroyed. These destroyed sub-blocks correspond to those VQ indexes damaged in the encrypted image. The PSNR results of the reconstructed images with error compensation are 15.9090 dB, 15.9326 dB, and 15.7447, respectively, which are far from satisfactory to authenticate. If ignoring the error matrix, we can obtain the images in the third row with PSNR values of 19.8572 dB, 21.1723 dB, and 20.9273 dB, respectively, which have better visual perception than those in the second row. But there are still some discrete sub-blocks in the images in the third column, which are indications of the destroyed indexes. An alternative solution is to replace the damaged indexes with their neighbor indexes, and the fourth row shows the final reconstructed images. The PSNR values of the fourth row are 24.4895 dB, 26.5853 dB, and 24.2341 dB, respectively, which are enough to accomplish subsequent authentication. The fifth row shows the decoded images after the inverse DRPE transform, and the last row shows the authentication results between decoded images and final reconstructed images. The PCE values of the authentication results reach 0.0032, 0.0021, and 0.0017, respectively, indicating that our DRPE-CSVQ implements successful authentication after cropping attack.

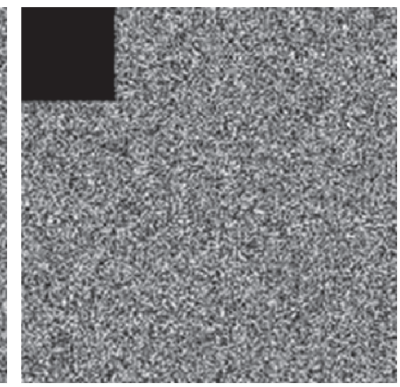
As mentioned earlier, we also implement the work [29] with the same input images under cropping size 64×64. After simulations by the same software, we can obtain the final reconstructed images with respective PSNR values of 7.0614 dB, 10.3057 dB, and 11.5010 dB in Figures 12(b1)–12(b3), which are much worse than those in our method. In addition, one cannot find the apparent high peak from the center of each correlation plane, indicating that the distortions on these reconstructed images have severely influenced the authentication effect. What is more, the PCE values of the authentication results are only 0.000885, 0.000415, and 0.000450, respectively; thus, we can conclude that the method [29] fails to authenticate after being attacked with the cropping size 64×64.



(a1)



(a2)

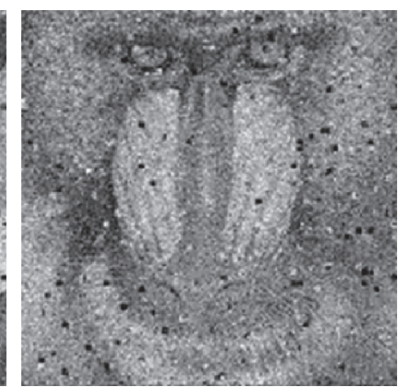


(a3)

(a)

(b1)

(b2)

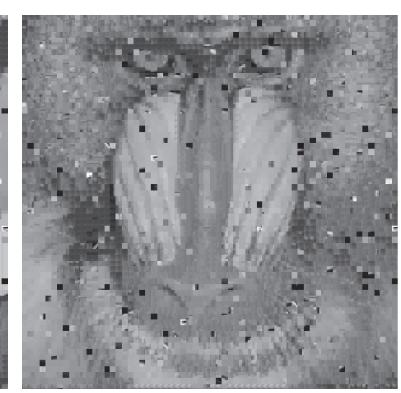


(b3)

(b)

(c1)

(c2)



(c3)

(c)

Figure 11: Continued.

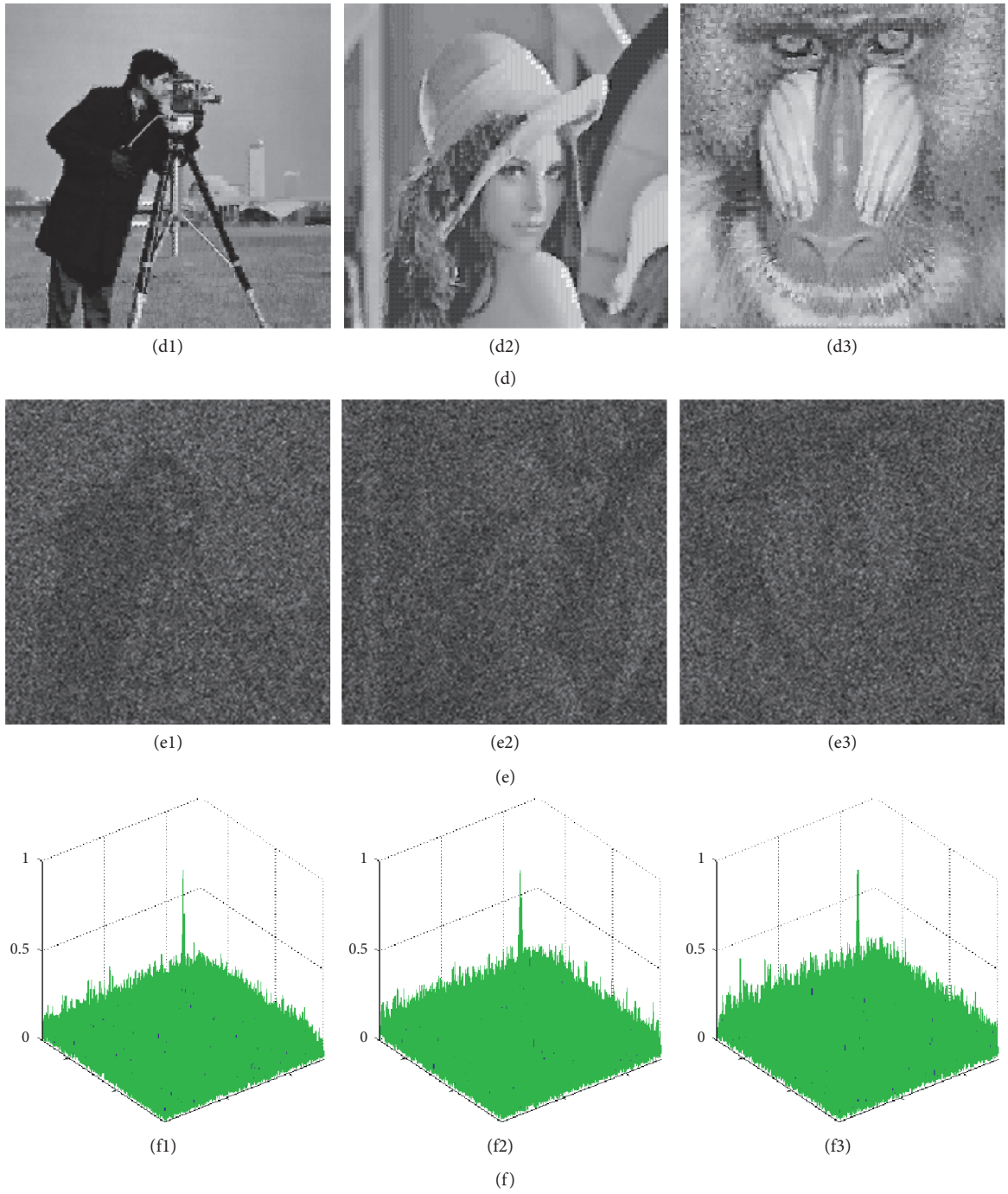


Figure 11: Authentication results of our DRPE-CSVQ under cropping attack with the cropping size 64 × 64. (a, b, c, d, e, f-1, 2, 3) Standard images "Camera," "Lena," and "Baboon" used for testing; (a-1, 2, 3) the encrypted images suffering from the cropping size 64 × 64; (b-1, 2, 3) the reconstructed images with error compensation; (c-1, 2, 3) the reconstructed images without error compensation; (d-1, 2, 3) the reconstructed images corresponding to the images (c-1, 2, 3); (e-1, 2, 3) the decoded images by inverse DRPE; (f-1, 2, 3) the authentication results between the images (d-1, 2, 3) and the images (e-1, 2, 3).

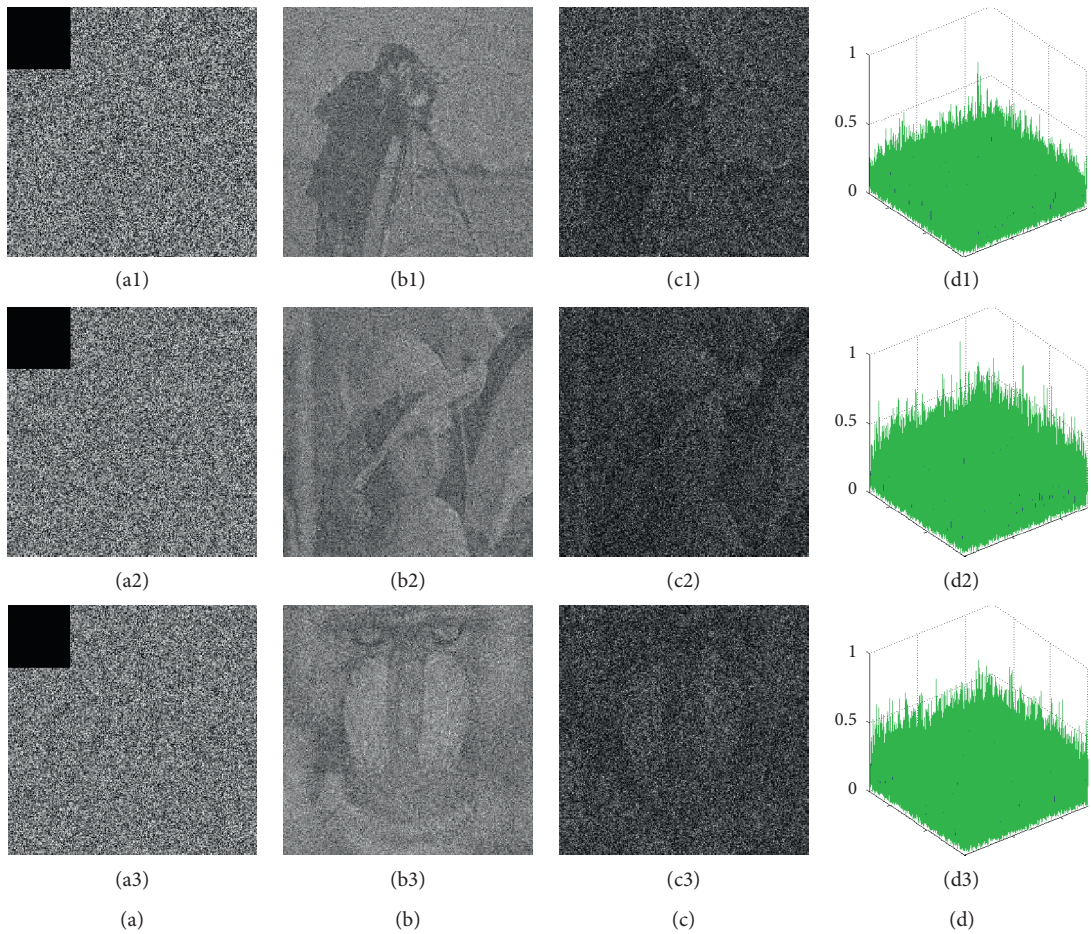


Figure 12: Authentication results of DRPE-BCS [29] under cropping size 64 × 64. (a, b, c, d-1, 2, 3) Standard images "Camera," "Lena," and "Baboon" used for testing; (a-1, 2, 3) the encrypted images suffering from cropping size 64 × 64; (b-1, 2, 3) the reconstructed images; (c-1, 2, 3) the decoded images by inverse DRPE; (f-1, 2, 3) the authentication results between the images (b-1, 2, 3) and the images (b-1, 2, 3).

5. Conclusion

This paper has presented a secure and efficient image authentication scheme based on DRPE-CSVQ. It is the first time we generalize the DRPE technology to compressive sensing and vector quantization application scenarios. The phase information of the plain image is obtained using DRPE and quantized to generate the authentication information. Simultaneously, the same plain image is compressed by VQ, and then an error matrix is generated. Since VQ can preserve enough details of an image, the error matrix would be very sparse. To balance the sparse degree of all sub-blocks of the error matrix such that the sub-blocks can be sensed with the same sensing matrix, we conduct a permutation on the error matrix and follow the block-based CS compression on the error matrix. The combined image that comprises the VQ indexes, the quantized measurements, and the authentication information is permutated and diffused to ensure security. Supported by the detailed numerical simulations and theoretical analyses, the DRPE-CSVQ fits into the practical realm better than its counterpart.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (nos. 61602158 and 61370195), the Science and Technology Research Project of Henan Province (no. 212102210413), and the Joint Funds of the National Natural Science Foundation of China (no. U1536121).

References

[1] X. Yan, B. Cui, Y. Xu, P. Shi, and Z. Wang, "A method of information protection for collaborative deep learning under GAN model attack," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 18, no. 3, pp. 871–881, 2021.

[2] M. Li, H. Ren, E. Zhang, W. Wang, L. Sun, and D. Xiao, "A VQ-based joint fingerprinting and decryption scheme for secure and efficient image distribution," *Security and Communication Networks*, vol. 2018, Article ID 4313769, 11 pages, 2018.

[3] M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Processing*, vol. 171, Article ID 107484, 2020.

[4] W. Y. Wen, Y. K. Hong, Y. M. Fang, M. Li, and M. Li, "A visually secure image encryption scheme based on semi-tensor product compressed sensing," *Signal Processing*, vol. 173, Article ID 107580, 2020.

[5] M. Khan and T. Shah, "An efficient chaotic image encryption scheme," *Neural Computing and Applications*, vol. 26, no. 5, pp. 1137–1148, 2015.

[6] G. Ye, C. Pan, X. Huang, and Q. Mei, "An efficient pixel-level chaotic image encryption algorithm," *Nonlinear Dynamics*, vol. 94, no. 1, pp. 745–756, 2018.

[7] S. L. Sun, "A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling," *IEEE Photonics Journal*, vol. 10, no. 2, Article ID 7201714, 2018.

[8] Z. X. F. Guorui and G. R. Feng, "Inpainting assisted self recovery with decreased embedding data," *IEEE Signal Processing Letters*, vol. 17, no. 11, pp. 929–932, 2010.

[9] C. Qin, C. C. Chang, and P. Y. Chen, "Self-embedding fragile watermarking with restoration capability based on adaptive bit allocation mechanism," *Signal Processing*, vol. 92, no. 4, pp. 1137–1150, 2012.

[10] M. Li, D. Xiao, H. Liu, and S. Bai, "A recoverable chaos-based fragile watermarking with high PSNR preservation," *Security and Communication Networks*, vol. 9, no. 14, pp. 2371–2386, 2016.

[11] Y. Bing and B. Sen, "Design of image confusion-diffusion cryptosystem based on vector quantization and cross chaotic map,," in *Proceedings of the 2nd International Conference on Image, Vision Computing*, pp. 639–644, Chengdu, China, June 2017.

[12] D. L. Donoho, "Compressed sensing," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.

[13] A. Orsdemir, H. O. Altun, G. Sharma, and M. F. Bocko, "On the security and robustness of encryption via compressed sensing," in *Proceedings of the IEEE Military Communications Conference*, pp. 1040–1046, San Diego, CA, USA, November 2008.

[14] P. J. A. Escamilla, M. R. Salinas, E. A. Aguirre, and R. A. Bermejo, "Image compressive sensing cryptographic analysis," in *Proceedings of the International Conference on Electronics Communications and Computers*, pp. 24–26, IEEE, Cholula, Mexico, February 2016.

[15] L. Y. Lei, J. P. Barbot, G. S. Hong, and H. Sun, "Compressive sensing with chaotic sequence," *IEEE Signal Processing Letters*, vol. 17, no. 8, pp. 731–734, 2010.

[16] H. Fan, M. Li, and W. Mao, "VQ-based compressive sensing with high compression quality," *Electronics Letters*, vol. 53, no. 17, pp. 1196–1198, 2017.

[17] H. Fan, K. Zhou, E. Zhang, W. Wen, and M. Li, "Subdata image encryption scheme based on compressive sensing and vector quantization," *Neural Computing and Applications*, vol. 32, no. 16, Article ID 12771, 2020.

[18] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, vol. 20, no. 7, pp. 767–769, 1995.

[19] Y. Sheng, X. H. Yan, L. T. Ming, Y. J. Xin, and X. J. Sun, "An improved method to enhance the security of double random-phase encoding in the Fresnel domain," *Optics and Laser Technology*, vol. 44, no. 1, pp. 51–56, 2012.

[20] J. Chen, Z. L. Zhu, C. Fu, L. B. Zhang, and Y. Zhang, "Information authentication using sparse representation of double random phase encoding in fractional Fourier transform domain," *Optik*, vol. 136, pp. 1–7, 2017.

[21] A. Belazi, A. A. A. E. Latif, A. V. Diaconu, R. Rhouma, and S. Belghith, "Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms," *Optics and Lasers in Engineering*, vol. 88, pp. 37–50, 2017.

[22] J. Zheng and X. Li, "Image authentication using only partial phase information from a double-random-phase-encrypted image in the fresnel domain," *Journal of the Optical Society of Korea*, vol. 19, no. 3, pp. 241–247, 2015.

[23] M. Cho and B. Javidi, "Three-dimensional photon counting double-random-phase encryption," *Optics Letters*, vol. 38, no. 17, pp. 3198–3201, 2013.

[24] E. C. Pérez, H. C. Abril, M. S. Millán, and B. Javidi, "Photon-counting double-random-phase encoding for secure image verification and retrieval," *Journal of Optics*, vol. 14, no. 9, Article ID 094001, 2012.

[25] I. Moon, F. Yi, M. Han, and J. Lee, "Efficient asymmetric image authentication schemes based on photon counting-double random phase encoding and RSA algorithms," *Applied Optics*, vol. 55, no. 16, pp. 4328–4335, 2016.

[26] W. Chen and X. D. Chen, "Double random phase encoding using phase reservation and compression," *Journal of Optics*, vol. 16, no. 2, pp. 218–241, 2014.

[27] F. Yi, Y. Jeoung, and I. Moon, "Three-dimensional image authentication scheme using sparse phase information in double random phase encoded integral imaging," *Applied Optics*, vol. 56, no. 15, pp. 4381–4387, 2017.

[28] F. Yi, Y. Kim, and I. Moon, "Secure Image-authentication Schemes with Hidden Double Random-phase Encoding," *IEEE Access*, vol. 6, Article ID 70113, 2018.

[29] K. Zhou, J. Fan, H. Fan, and M. Li, "Secure image encryption scheme using double random-phase encoding and compressed sensing," *Optics and Laser Technology*, vol. 121, Article ID 105769, 2020.

[30] L. Zhang, Y. Zhou, D. Huo, J. Li, and X. Zhou, "Multiple-image encryption based on double random phase encoding and compressive sensing by using a measurement array preprocessed with orthogonal-basis matrices," *Optics and Laser Technology*, vol. 105, pp. 162–170, 2018.

[31] D. Huo, X. Zhou, L. Zhang, Y. Zhou, H. Li, and S. Yi, "Multiple-image encryption scheme via compressive sensing and orthogonal encoding based on double random phase encoding," *Journal of Modern Optics*, vol. 65, no. 18, pp. 2093–2102, 2018.

[32] P. Lu, Z. Xu, X. Lu, and X. Liu, "Digital image information encryption based on compressive sensing and double random-phase encoding technique," *Optik*, vol. 124, no. 16, pp. 2514–2518, 2013.

[33] E. J. Candes and T. Tao, "Decoding by linear programming," *IEEE Transactions on Information Theory*, vol. 51, no. 12, pp. 4203–4215, 2005.

[34] E. J. Candes and T. Tao, "Near-optimal signal recovery from random projections: universal encoding strategies?" *IEEE Transactions on Information Theory*, vol. 52, no. 12, pp. 5406–5425, 2006.

[35] Y. Linde, A. Buzo, and R. Gray, "An algorithm for vector quantizer design," *IEEE Transactions on Communications*, vol. 28, no. 1, pp. 84–95, 1980.

[36] S. J. Sheela, K. V. Suresh, and D. Tandur, "Image encryption based on modified Henon map using hybrid chaotic shift transform," *Multimedia Tools and Applications*, vol. 77, no. 19, Article ID 25223, 2018.

[37] Z. Parvin, H. Seyedarabi, and M. Shamsi, "A new secure and sensitive image encryption scheme based on new substitution with chaotic function," *Multimedia Tools and Applications*, vol. 75, no. 17, Article ID 10631, 2016.

[38] USC-SIPI Image Database, University of South California, Signal and Image Processing Institute, 2018, https://sipi.usc.edu/database.

[39] L. Y. Zhang, K. W. Wong, Y. Zhang, and J. Zhou, "Bi-level protected compressive sampling," *IEEE Transactions on Multimedia*, vol. 18, no. 9, pp. 1720–1732, 2016.

[40] L. Gan, "Block compressed sensing of natural images," in *Proceedings of the International Conference on Digital Signal Processing*, July 2007.

[41] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Processing*, vol. 92, no. 4, pp. 1101–1108, 2012.

[42] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Optics and Lasers in Engineering*, vol. 66, pp. 10–18, 2015.

[43] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D sine logistic modulation map for image encryption," *Information Sciences*, vol. 297, pp. 80–94, 2015.