mathematics

MDPI

*Article*

# Double Image Encryption Scheme Based on Compressive Sensing and Double Random Phase Encoding

**Rui Zhang and Di Xiao ***

College of Computer Science, Chongqing University, Chongqing 400044, China; mail@zhangrui.org
* Correspondence: dixiao@cqu.edu.cn

**Abstract:** In order to overcome the shortcomings of the standard compressive sensing (CS) encryption framework, a novel fusion application scheme of CS and optical transformation technology is proposed. The proposed scheme, making full use of the feature of CS to achieve compression and encryption simultaneously, compresses and encrypts two images into one image, which not only reduces storage space and transmission bandwidth, but also improves the security performance of encryption. In the proposed scheme, the two original images are first sampled with CS, and then double random phase coding is performed to obtain two small-sized images. Meanwhile, the two original images are directly encrypted with double random phase coding to obtain the authentication information. Next, we combine two small-sized images and authentication information into one image, and finally perform double random phase coding again to obtain the final encrypted image. It should be emphasized that the proposed scheme has the function of image authentication. Experiment results validate the effectiveness and advancement of the proposed fusion application scheme.

**Keywords:** compressive sensing; image cipher; double random phase encoding

**MSC:** 94-08



**Citation:** Zhang, R.; Xiao, D. Double Image Encryption Scheme Based on Compressive Sensing and Double Random Phase Encoding. *Mathematics* **2022**, *10*, 1242. https://doi.org/10.3390/math10081242

Academic Editors: Zhongyun Hua and Yushu Zhang

Received: 13 March 2022
Accepted: 7 April 2022
Published: 10 April 2022



## 1. Introduction

Since compressive sensing (CS) theory was proposed in 2004 [1–3], it has shown broad application prospects in many fields including signal processing, communication system, image coding, and so on. The main principle of CS is that for a sparse or compressible high-dimensional signal, the measurement matrix can be used to project it onto a low-dimensional space, and then the original high-dimensional signal can be reconstructed from a small number of projections by solving the optimization problem. CS can simultaneously realize sampling and compression, so that the original signal can still be reconstructed under the condition of greatly reducing the sampling rate, and the cost is higher computational complexity in the decoding and reconstruction process. This projection of CS is a way of information protection [4].

When applied to information encryption, CS can be regarded as a symmetric cryptographic system, and its characteristics of simultaneously realizing sampling and compression are manifested as simultaneously realizing encryption and compression. The sparse signal, measurement matrix, compressed sampling, measured values, signal reconstruction, and reconstructed signal of CS correspond to the plaintext information, key, encryption operation, ciphertext information, decryption operation, and decrypted plaintext information in the traditional symmetric cryptosystem. The good fit between CS and traditional symmetric cryptographic systems makes it more natural to apply it to information encryption.

However, the standard CS encryption framework has its own shortcomings like other encryption techniques. For example, the measurement matrix used as the key requires a large storage and transmission overhead; the decryption and reconstruction of the signal

is realized by solving an optimization problem, which is more timeconsuming compared with the compression and encryption process [5–7]; the measurement values, as ciphertext, will leak the energy information of the plaintext; the encryption cannot achieve the perfect security defined by Shannon [8]. Obviously, in order to overcome the above shortcomings and improve the security level and encryption performance of encryption, the standard CS encryption framework needs to be improved or introduced other techniques for "repair".

With the rapid development of multimedia information-processing technology, network technology, and cloud computing, image, as a form of multimedia data, is widely used in military, law, economics, medicine, and daily life and other fields, becoming a frequently used information transmission carrier. However, when an image is transmitted through an insecure channel, it is often very susceptible to illegal operations, such as stealing, leaking, and tampering, thereby causing immeasurable losses to the holder of the image. In this way, protecting the privacy of image information has become a very urgent need, which has very important significance and research value.

As more and more researchers pay attention to and participate in the research of image information privacy protection, a large number of image encryption methods and techniques continue to emerge. Among these methods and techniques, image encryption based on CS is believed to be particularly suitable for use in resource-limited scenarios since CS can realize image compression and encryption simultaneously, which has therefore been favored by researchers. As mentioned earlier, the standard CS encryption framework has shortcomings, so the application of CS to image encryption also needs to be improved and "fixed". Improvement and "repair" are often achieved by combining CS with other image encryption techniques such as optical transformation. As we all know, in the field of image encryption, chaotic system [9–19] and optical transformation are the two most extensive and important techniques. Optical transformation techniques have the characteristics of excellent parallelism, ultra-high speed, large capacity, and small size. The fusion of CS and optical transformation techniques not only strengthens security, but also retains the advantages of the standard CS encryption framework to the greatest extent.

The fusion of CS image encryption and other image encryption techniques brings new vitality to image encryption and provides powerful technology guarantee for safer and more efficient applications of images in military, medical, economic, legal, and other industries.

However, in the existing image encryption methods based on CS and optical transformation, the encrypted image often fails to maintain the same size as the original image, which makes it easy for attackers to perceive compressed sensing encryption. In this way, encrypted images are subject to more targeted attacks and cracking threats. For this reason, we propose a scheme of encrypting two images into one image using CS and double random phase encoding (DRPE), which not only makes the encrypted image consistent in size with the original image, but also gives full play to the compression function of CS. In the proposed scheme, the two original images are first sampled with CS, and then DRPE is performed to obtain two small-sized images. Meanwhile, the two original images are directly encrypted with DRPE to obtain the authentication information. Next, we combine two small-sized images and authentication information into one image, and finally perform DRPE again to obtain the final encrypted image. It should be emphasized that the proposed scheme has the function of image authentication.

## 2. Related Works

Optical image encryption is believed to be very efficient. Its working principle is to scramble and encode the inherent information of plaintext images through optical transformation processes, such as interference, diffraction, and imaging, so as to realize image information encryption. As a multi-dimensional information carrier, light has the characteristics of short wavelength and large information capacity. It also has multiple attributes such as amplitude, phase, wavelength, and polarization. All these features make the use of optical transformation technology for image encryption more natural advantages than the use of electronic means. In the process of optical image encryption, various

attributes, such as wavelength, focal length, diffraction distance, and phase, can be used as the multi-dimensional key of the encryption system, which has a large key space and provides security for encryption to a certain extent.

In 1995, Refregier et al. proposed an image encryption scheme with DRPE based on the 4f system [20], which has better security and robustness. Subsequently, the researchers put forward some improvement schemes based on DRPE, such as the DRPE scheme based on Fourier transform [21], the DRPE scheme based on Fresnel diffraction [22], the optical encryption scheme based on interference principle [23], the asymmetric encryption scheme based on phase-truncated Fourier transform [24], the encryption scheme based on joint transform correlator, and the DRPE encryption scheme using digital holography technology [25], which make the field of optical image encryption colorful.

In the fusion application of CS and optical transformation technology, researchers have also proposed some encryption schemes. The authors of [26] proposed an image information encryption method based on CS and DRPE. Considering that natural image tends to be compressible in a transform domain, the characteristics of CS, dimensional reduction, and random projection are utilized to sample or encrypt a digital image first. Then, the measured values with low data volume are re-encrypted by the double random phase encoding technique with smaller random phase masks based on sequences of irrational numbers. Moreover, the double-encrypted information is dispersed and embedded into the host image. At the received side, original image is reconstructed approximately via Orthogonal Matching Pursuit algorithm. This encryption scheme is proved to have the following features: low data volume for encryption and high security of information. The authors of [27] proposed a novel approach in double random phase encryption based on compressive fractional Fourier transform along with the kernel steering regression. The scheme increases the complexity of the image by using fractional Fourier transform and taking fewer measurements from the image data. The encryption process has kernel steering regression algorithm for denoising and CS technique for image compression along with the fractional Fourier transform that makes the image in more complex form. The authors of [28] proposed a new multiple-image encryption scheme that utilizes the CS concept along with a double random phase encoding. The space multiplexing method is employed for integrating multiple-image data. The method, which results in a nonlinear encryption system, is able to overcome the vulnerability of classical DRPE. The authors of [29] designed a new image encoding scheme for simultaneous encryption and compression applications, which was based on random convolution and random sub-sampling. In comparison with the existing joint optical encryption and compression schemes tailored for multiple images, the proposed scheme can process a single image and achieve a robust reconstruction. The scheme with the architecture of double random masks is somewhat similar to DRPE. The authors of [30] utilized the combination of fiber specklegram-based CS and DRPE to propose an image compression–encryption method. The original image is compressed and encrypted by CS and then re-encrypted by DRPE. Since the measurement matrices for CS are constructed from multimode fiber specklegrams, the method shows better performance compared with those based on Gaussian random variables. The authors of [31] proposed an image compression and encryption algorithm based on 2D CS and DRPE. The original image is first compressed from two directions to obtain the measurement value. Then, DRPE is performed on the measurement value to obtain the final cipher image. The theoretical analysis and simulation experiments show that the combination of DRPE and 2D CS can improve the execution efficiency of compression encryption and ensure the security and robustness of encryption. The authors of [32] proposed a CS-based image compression, authentication, and encryption algorithm in cloud. The original image is divided into the low-frequency part and the high-frequency part. The low-frequency part of the image is encrypted with the proposed binary data cyclic encryption algorithm, while the high-frequency part is randomized for compression by the CS and then encrypted by DRPE. Empirical evaluations show that the proposed scheme can resist exhaustive attack, differential attack, and classical attacks.

## 3. The Proposed Scheme

### *3.1. The Framework of Proposed Scheme*

The proposed double image encryption scheme based on CS and DRPE includes two main stages: the encryption stage and the decryption stage. In the encryption stage, the two original images A and B are compressed and sampled (encrypted), respectively, through CS, and then DRPE is performed to obtain two small-sized images, A1 and B1. Meanwhile, the two original images are directly encrypted with DRPE to obtain the authentication information, A2 and B2. Next, the two small-sized images (A1 and B1) are combined with the authentication information of the two images (A2 and B2) into an image C, and we finally perform DRPE on C to obtain the final encrypted image. The decryption process is the reverse process of encryption. Figure 1 shows the overall framework of the encryption process.

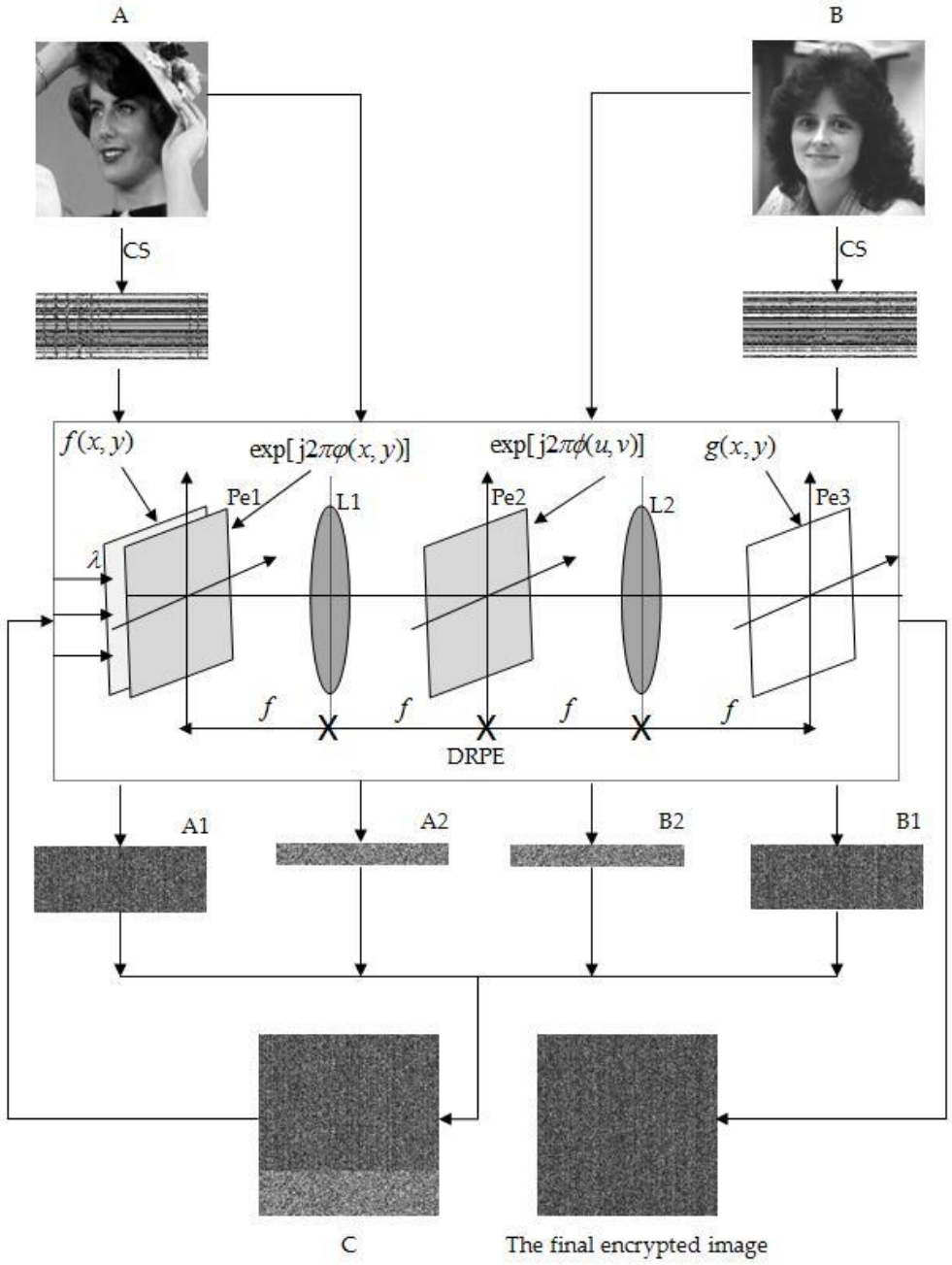


**Figure 1.** The framework of the proposed encryption process.

### *3.2. Compresive Sampling and DRPE Encryption*

The double image encryption scheme based on CS and DRPE can encrypt two images into one image in one encryption process. The whole process uses CS two times and DRPE five times. In this proposed scheme, the purpose of using CS is to compress the original image, and the starting point for compressing and encrypting two images at the same time is not only to improve the efficiency of image transmission when resources are limited, but also to make the attacker imperceptible for reducing threats against CS encryption. The detailed steps of compressive sampling and DRPE encryption are as follows:

Step 1: For original image A and B with size of $N \times N$, perform discrete wavelet transform (DWT), respectively, to obtain the coefficient matrices *CMA* and *CMB*.

$$CMA = \Psi \times \mathrm{A} \times \Psi' \tag{1}$$

$$CMA = \Psi \times \mathrm{B} \times \Psi' \tag{2}$$

where $\Psi$ is an orthogonal wavelet matrix and its transpose is $\Psi'$.

Step 2: Set the sample rate to 3/8. Without loss of generality, use a random Gaussian matrix to generate two measurement matrices $\Phi_A$ and $\Phi_B$ with size of $(3/8N) \times N$.

Step 3: The coefficient matrices *CMA* and *CMB* are sampled with the measurement matrices $\Phi_A$ and $\Phi_B$, respectively, and the measurement value matrices $Y_A$ and $Y_B$ are obtained.

$$Y_A = \Phi_A \times CMA \tag{3}$$

$$Y_B = \Phi_B \times CMB \tag{4}$$

Step 4: According to DRPE proposed by Philippe Refregier and Bahram Javidi in [20], construct two independent random matrices $R_1$ and $R_2$ with size of $(3/8N) \times N$ uniformly distributed on [0, 1], denoted as $s(x, y)$ and $f(u, v)$, respectively. Use the following formulas to generate the space-domain encryption key $RPM_1$ and the frequency-domain encryption key $RPM_2$ for DRPE, denoted as $m(x, y)$ and $M(u, v)$, respectively.

$$m(x, y) = \exp[i2\pi s(x, y)] \tag{5}$$

$$M(u, v) = \exp[i2\pi f(u, v)] \tag{6}$$

where $(x, y)$ are the space domain coordinates and $(u, v)$ are the frequency domain coordinates.

Step 5: Quantify the measurement matrices $Y_A$ and $Y_B$ to the interval [0, 255]. Perform DRPE to $Y_A$ and $Y_B$ to obtain encrypted matrices $E_{A1}$ and $E_{B1}$.

$$\begin{aligned} E_{A1} &= FT^{-1}\{FT\{Y_{Aq}m(x, y)\} \cdot M(u, v)\} \\ &= Y_{Aq}m(x, y) * FT^{-1}\{M(u, v)\} \end{aligned} \tag{7}$$

$$\begin{aligned} E_{B1} &= FT^{-1}\{FT\{Y_{Bq}m(x, y)\} \cdot M(u, v)\} \\ &= Y_{Bq}m(x, y) * FT^{-1}\{M(u, v)\} \end{aligned} \tag{8}$$

where $Y_{Aq}$ and $Y_{Bq}$ are the quantized matrices of measurement value matrices $Y_A$ and $Y_B$, respectively, "$*$" denotes convolution operation, $FT\{\cdot\}$ denotes Fourier transform, and $FT^{-1}\{\cdot\}$ denotes inverse Fourier transform. The obtained encryption matrices $E_{A1}$ and $E_{B1}$ are both generalized stationary random white noise.

Step 6: The same as Step 4. Construct two independent random matrices $R_3$ and $R_4$ with size of $N \times N$ uniformly distributed on [0, 1]. Generate the space-domain encryption key $RPM_3$ and the frequency-domain encryption key $RPM_4$ for DRPE, respectively.

Step 7: The same as Step 5. Perform DRPE directly to original images A and B to obtain encrypted matrices $E_A$ and $E_B$. Compute the phase diagram matrices $PH_A$ and $PH_B$, respectively, by the following formulas:

$$PH_A = angle(E_A) \times 180/\pi \tag{9}$$

$$PH_B = angle(E_B) \times 180/\pi \tag{10}$$

where $angle()$ is a function for calculating the complex phase angle of $E_A$ and $E_B$.

Step 8: Use 0 as the threshold to quantify $PH_A$ and $PH_B$, respectively, obtaining two binary images $I_A$ and $I_B$.

$$I_A(x,y) = \begin{cases} 1, & PH_A(x,y) > 0 \\ 0, & PH_A(x,y) \leq 0 \end{cases} \tag{11}$$

$$I_B(x,y) = \begin{cases} 1, & PH_B(x,y) > 0 \\ 0, & PH_B(x,y) \leq 0 \end{cases} \tag{12}$$

Step 9: Combine every 8 pixels of binary image images $I_A$ and $I_B$ into a gray image pixel with value range of [0, 255] to obtain the authentication information matrices $E_{A2}$ and $E_{B2}$ of original images A and B, respectively. They have the same size, $(1/8N) \times N$.

Step 10: Combine, $E_{A1}$, $E_{B1}$, $E_{A2}$, and $E_{B2}$ generated by the above steps into an image C, the size of which is exactly $N \times N$, which is consistent with the size of the original images A and B.

Step 11: Using the space-domain encryption key $RMP_3$ and the frequency-domain encryption key $RMP_4$ generated by Step 6, DRPE is performed on C again to obtain the final encrypted image $E_C$, with size of $N \times N$. So far, the proposed scheme has successfully encrypted the two original images into one ciphertext image.

### *3.3. Decryption Process*

The decryption process is the reverse process of encryption. The entire decryption process uses two times of CS reconstruction and five times of inverse DRPE. Figure 2 shows the framework of the decryption process.

Step 1: With the help of the frequency-domain encryption key $RMP_4$ generated by the encryption process Step 6, the frequency-domain decryption key $RMP_4^*$ is constructed. The decryption key is the complex conjugate function of the encryption key,$M^*(u,v)$.

$$M^*(u,v) = \exp[-i2\pi f(u,v)] \tag{13}$$

Step 2: Perform inverse DRPE on the ciphertext image $E_C$ to obtain the decrypted image $\widetilde{C}$.

$$\widetilde{C}(x,y) = FT^{-1}\{FT\{E_C(x,y)\} \cdot \exp[-i2\pi f(u,v)]\} \tag{14}$$

Substitute the formula similar with Step 5 in the encryption process into the above formula. The above formula can be further simplified:

$$\begin{aligned} \widetilde{C}(x,y) &= FT^{-1}\{FT\{C(x,y) \cdot \exp[i2\pi s(x,y)]\}\} \\ &= C(x,y) \cdot \exp[i2\pi s(x,y)] \end{aligned} \tag{15}$$

where $C(x,y)$ denotes the original image of $C$. $\exp[i2\pi s(x,y)]$ is the space-domain encryption key $RMP_3$. Since $C(x,y)$ is a positive real value, the phase term will disappear when a light intensity detector such as a CCD is placed on the output surface for detection, and the original image $C(x,y)$ can be obtained.

Step 3: With the help of compressive sampling rate and authentication message processing algorithm during encryption, decompose the decrypted image $\widetilde{C}$ into four parts $\widetilde{A}_1, \widetilde{B}_1, \widetilde{A}_2$, and $\widetilde{B}_2$. The size of $\widetilde{A}_1$ and $\widetilde{B}_1$ is $(3/8N) \times N$, while the size of $\widetilde{A}_2$ and $\widetilde{B}_2$ is $(1/8N) \times N$.

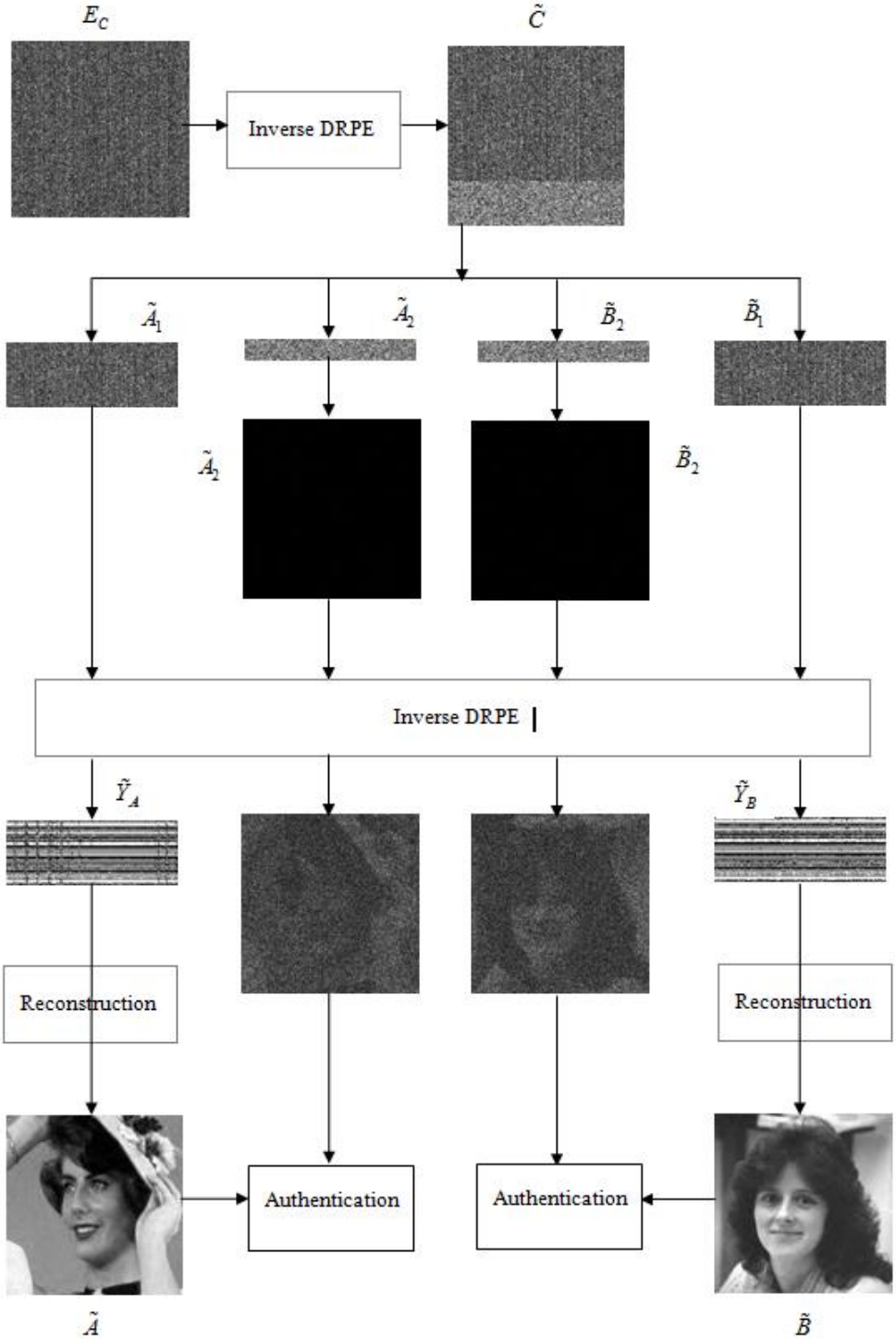


**Figure 2.** The framework of the proposed decryption process.

Step 4: With the help of the space-domain encryption key $RPM_1$ and the frequency-domain encryption key $RPM_2$ generated by Step 4 in the encryption process, use the algorithm shown in decryption process Step 1 to generate the frequency-domain decryption key, and use the algorithm shown in decryption process Step 2 to perform inverse DRPE on $\widetilde{A}_1$ and $\widetilde{B}_1$, respectively, to obtain $\widetilde{Y}_A$ and $\widetilde{Y}_B$.

Step 5: Decompose each pixel of $\widetilde{A}_2$ and $\widetilde{B}_2$ (value range [0, 255]) bit by bit into eight binary values, respectively, and rearrange these binary values into two $N \times N$-sized matrices to obtain two binary images.

Step 6: Perform the following transformations on the binary images $\widetilde{A}_2$ and $\widetilde{B}_2$ to obtain two phase images $P\widetilde{H}_A$ and $P\widetilde{H}_B$.

$$P\widetilde{H}_A = \begin{cases} -\pi, & \widetilde{A}_2(x,y) = 0 \\ \pi, & \widetilde{A}_2(x,y) = 1 \end{cases} \tag{16}$$

$$P\widetilde{H}_B = \begin{cases} -\pi, & \widetilde{B}_2(x,y) = 0 \\ \pi, & \widetilde{B}_2(x,y) = 1 \end{cases} \tag{17}$$

Step 7: The same as Step 1 of the decryption process. The frequency-domain decryption key for DRPE decryption is calculated. Using the algorithm of Step 2 in the decryption process, DRPE decryption is performed on $P\widetilde{H}_A$ and $P\widetilde{H}_B$, and the authentication information $PA_A$ and $PA_B$ for detection and authentication are obtained, respectively.

Step 8: With the help of the orthogonal wavelet matrix $\Psi$ and the measurement matrices $\Phi_A$ and $\Phi_B$ generated by Step 1 and Step 2 in the encryption process, the OMP algorithm is applied for reconstruction, and the reconstructed images $\widetilde{A}$ and $\widetilde{B}$ are obtained.

Step 9: With the help of $PA_A$ and $PA_B$ obtained in Step 7 of the decryption process, authentication is performed on the reconstructed image $\widetilde{A}$ and $\widetilde{B}$. For authentication testing, it is first necessary to calculate the statistical non-linear correlation between the reconstructed image and the authentication information. The mathematical definition is as follows:

$$CO(x,y) = FT^{-1}\left\{ \left| \widetilde{A}(\mu,\eta) \cdot PA_A(\xi,\upsilon) \right|^k \cdot \exp[\varphi_{\widetilde{A}}(\mu,\eta) - \varphi_{PAA}(\xi,\upsilon)] \right\} \tag{18}$$

where $\widetilde{A}(\mu,\eta)$ denotes the reconstructed image $\widetilde{A}$, $PA_A(\xi,\upsilon)$ denotes the 2D Fourier transform form of the authentication information $PA_A$, $\varphi_{\widetilde{A}}(\mu,\eta)$ denotes the phase image of reconstructed image $\widetilde{A}$, and $\varphi_{PAA}(\xi,\upsilon)$ denotes the phase image of authentication information $PA_A$. The parameter $k$ is usually set to 0.3.

Peak to Correlation Energy (PCE) [33] refers to the energy ratio of the correlation peak on the entire correlation surface, which is usually used to measure the correlation between the reconstructed image and the authentication information. Its mathematical definition is as follows:

$$PCE = \frac{\max(CO(x,y)^2)}{\sum_{X=1}^{M}\sum_{y=1}^{N} CO(x,y)^2} \tag{19}$$

where $M$ and $N$ are the size of the image in the horizontal and vertical directions, respectively. The higher the $PCE$ value, the stronger the correlation between the reconstructed image and the authentication information.

## 4. Experiments and Analysis

In order to evaluate the performance of the proposed scheme, this section conducts simulation experiments and analysis. Image Lady, Woman, Milkdrop, and Airplane with size of $256 \times 256$ are chosen as test images. Two-dimensional discrete wavelet transform is applied for sparse representation of the test images. Without loss of generality, the compression rate is set to 3/8 and the Orthogonal Match Pursuit (OMP) algorithm is used to reconstruct the original image.

### *4.1. Encryption and Decryption Effect Evaluation*

Based on the theoretical analysis of the proposed scheme, the encryption effects of this scheme come from the dual effects of CS and DRPE. Figure 3 shows the relevant experimental results. From left to right, the first to third columns correspond to the original images, the encrypted image, and the reconstructed image with the correct secret key.

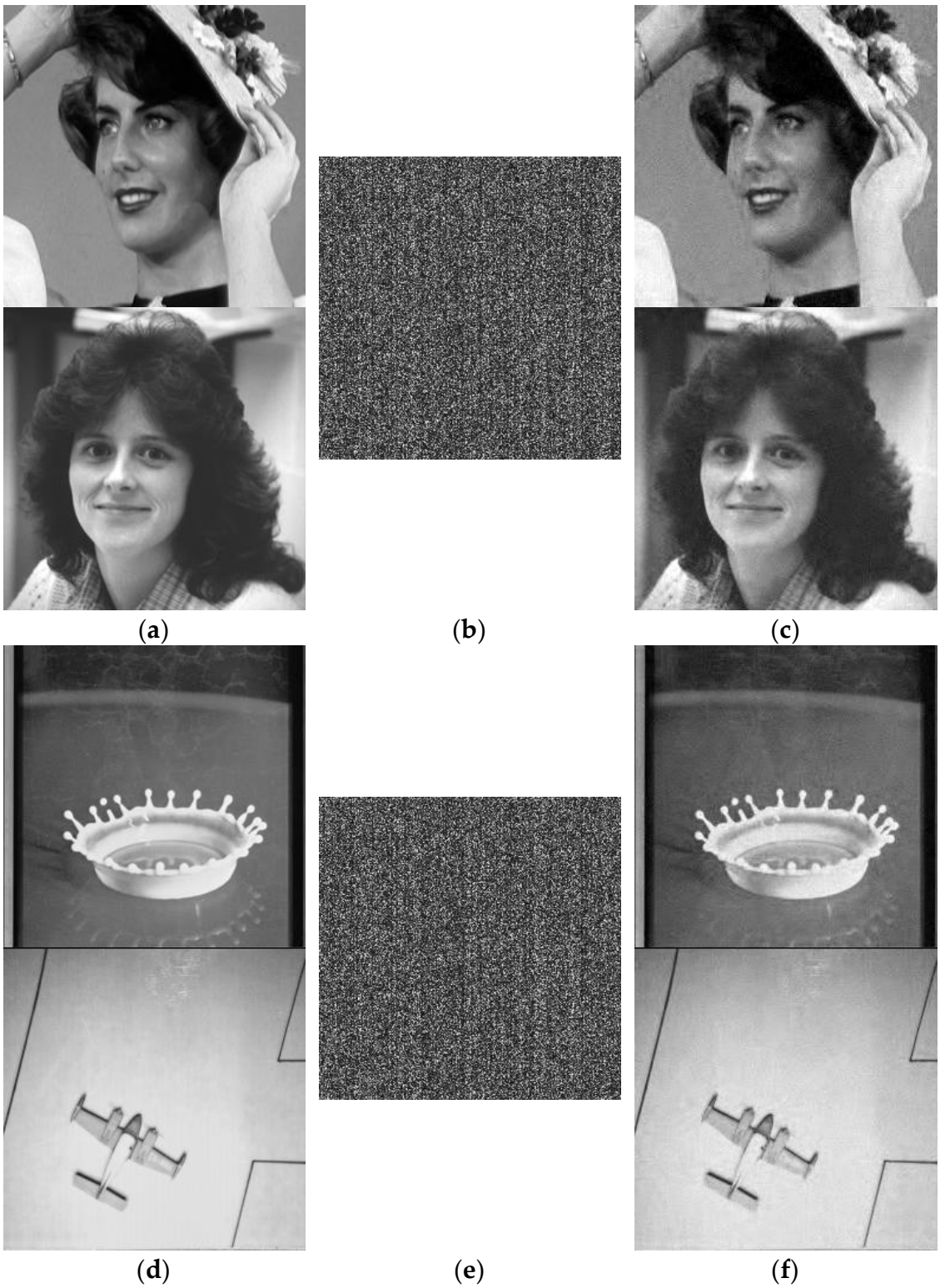

**Figure 3.** *Cont.*

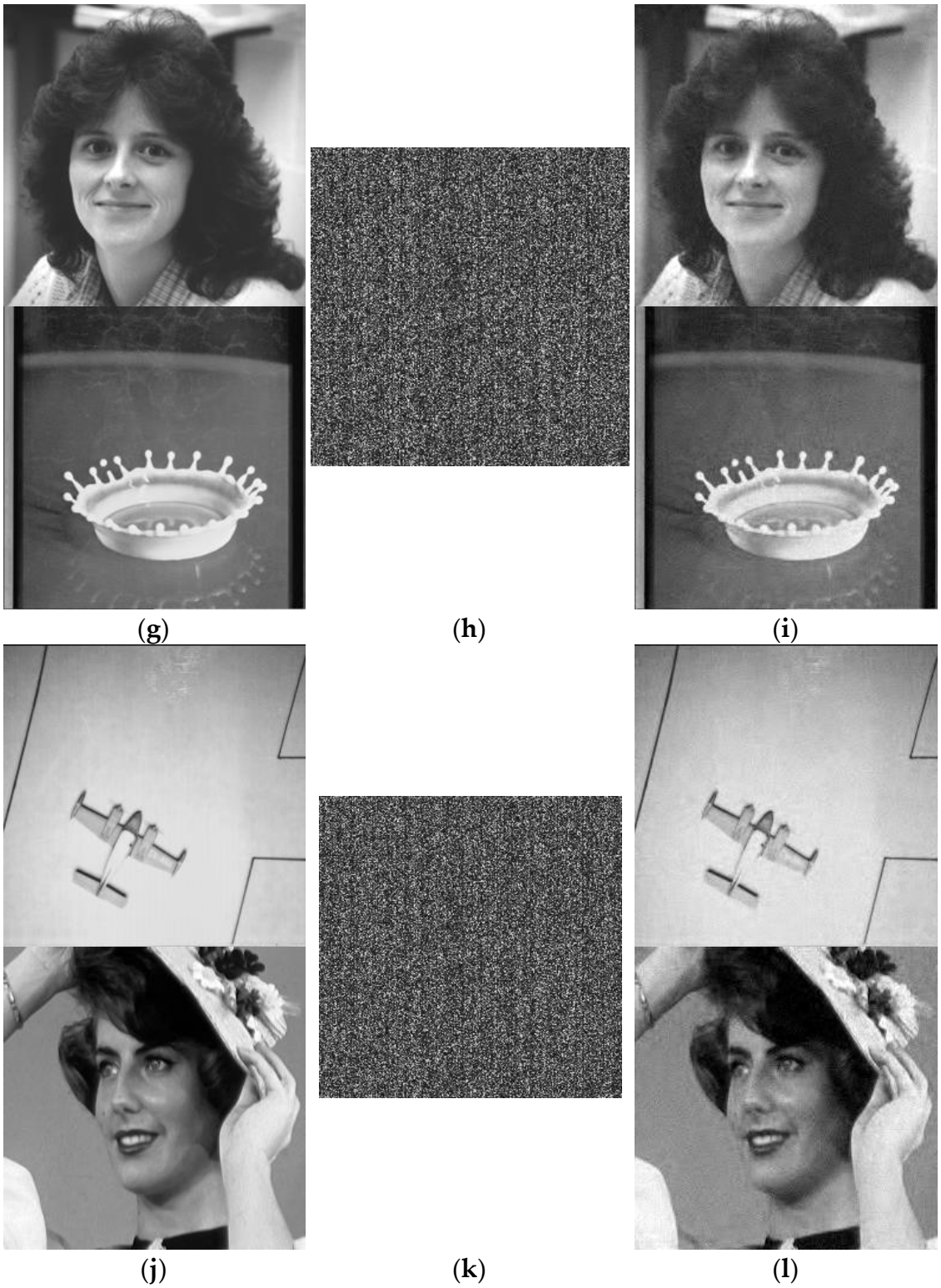

**Figure 3.** Effectiveness evaluation of the proposed scheme. (**a**) Original images Lady and Woman, (**b**) encrypted image, and (**c**) reconstructed images Lady (PSNR: 30.2424 dB) and Woman (PSNR: 32.8682 dB). (**d**) Original images Milkdrop and Airplane, (**e**) encrypted image, and (**f**) reconstructed imagesMilkdrop (PSNR: 32.740 dB) and Airplane (PSNR: 33.6446 dB). (**g**) Original images Woman and Milkdrop, (**h**) encrypted image, and (**i**) reconstructed images Woman (PSNR: 32.9014 dB) and Milkdrop (PSNR: 32.7725 dB). (**j**) Original images Airplane and Lady, (**k**) encrypted image, and (**l**) reconstructed images Airplane (PSNR: 33.6833 dB) and Lady (PSNR: 30.3596 dB).

From the perspective of encryption performance, it is impossible to obtain any valuable information from the encrypted image. Encrypt two original images with a size of $256 \times 256$ into an encrypted image with a size of $256 \times 256$, and the storage space occupied by the encrypted image is only half of the original images. It can be seen that the encryption performance and compression performance of the proposed scheme were verified. Next, we mainly use visual effects and peak signal-to-noise ratio (PSNR), a commonly used evaluation indicator of decrypted image quality, to evaluate the quality of the image decrypted and reconstructed with the correct key. In terms of visual effects, the decrypted and reconstructed image in column 3 is very similar to the original image in column 1, and the main information in the original image can be clearly identified in the decrypted and reconstructed image. From the value of peak signal-to-noise ratio, the PSNR of the decrypted and reconstructed images are both greater than 30 dB. In addition, since the proposed scheme is to encrypt two images into one image, we deliberately set up comparative simulation experiments to investigate whether the two images affect each other's decryption and reconstruction image quality. Through experiments, it can be seen that the quality of the reconstructed image has nothing to do with the partner image when not being attacked. For example, the PSNR of the reconstructed and decrypted image after encrypting image Woman and Lady together is 32.8682 dB, and the PSNR of the reconstructed and decrypted image after encrypting image Woman and Milkdrop together is 32.9014 dB. The difference between the two is only due to the quantization error in both the encryption process and decryption process.

### *4.2. Histogram Analysis*

The image histogram is used to represent the histogram of the brightness distribution in the digital image. It plots the number of pixels of each brightness value in the image. It is an effective indicator for evaluating the distribution of pixel values. The histogram does not change due to image translation, rotation, or scaling.Generally speaking, the histogram of the plaintext image shows obvious statistical law, and the attack against this statistical law is called a statistical analysis attack. The histogram statistical analysis attack means that the attacker cracks the encrypted image by analyzing the law of the histogram of the encrypted image and the original image. An effective image encryption scheme should make the histograms of encrypted images uniformly distributed or make the histograms of all encrypted images have similar distributions, so as to effectively resist attacks based on pixel value statistics. Figure 4 shows the simulation results of the histogram. It is not difficult to see from the figure that the histogram of any image in each group of images is obviously different from the histogram of encrypted image.

In addition, for all encrypted images, their histograms show similar distribution rules, and it is impossible to distinguish the effective features of original images from encrypted images.

In order to measure the similarity of the histograms, we use the Euclidean distance method, that is, to compare their similarity by calculating the Euclidean distance of the histograms of two images. The smaller the value, the more similar the histograms of the two images. Table 1 shows the Euclidean distances between the histograms of each encrypted image in Figure 4. It can be seen from the numerical value that the similarity of the histograms of all ciphertext images is very high.

In summary, it can be concluded that this encryption scheme can effectively resist histogram statistical analysis attacks.

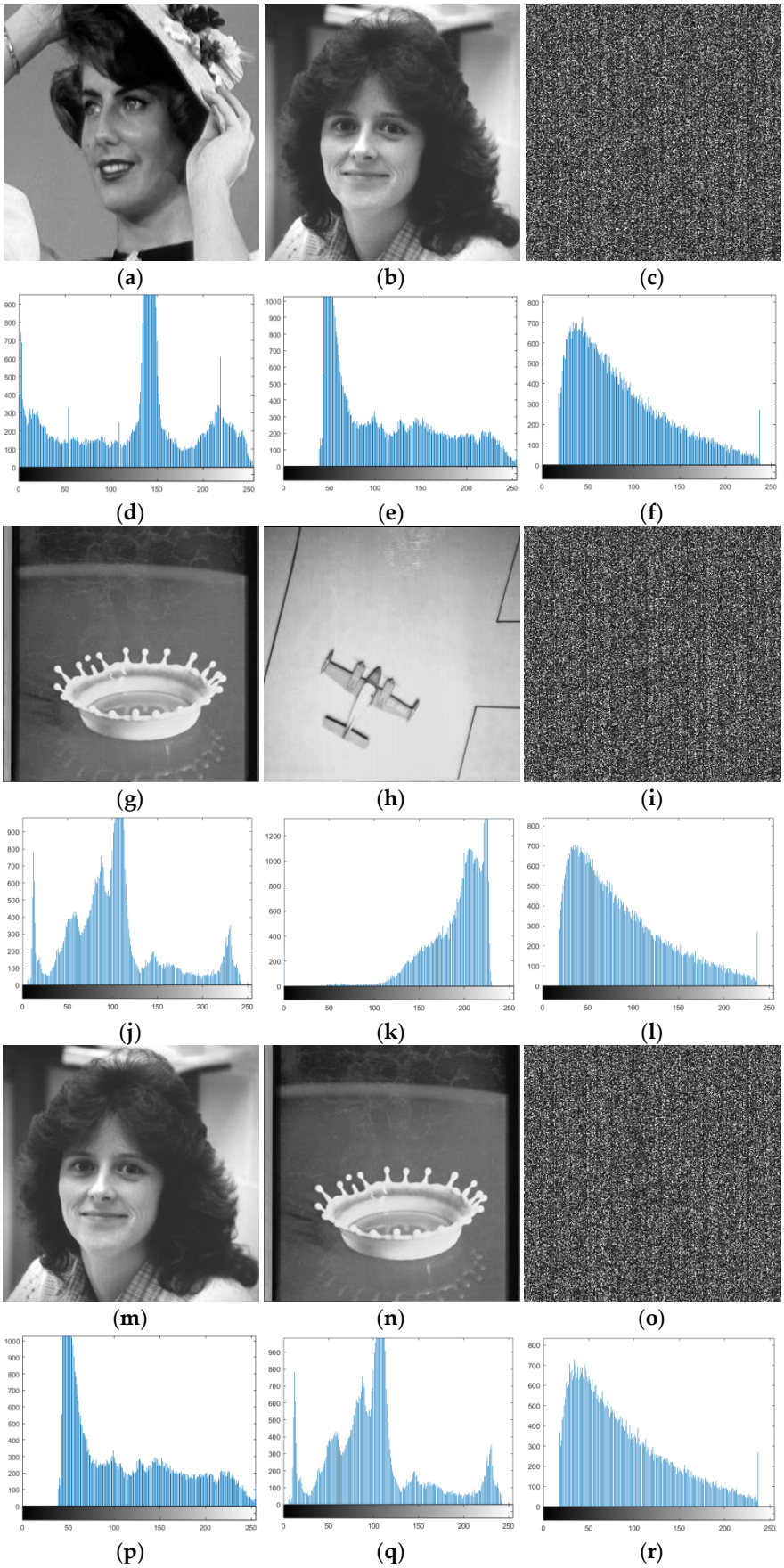


**Figure 4.** *Cont.*

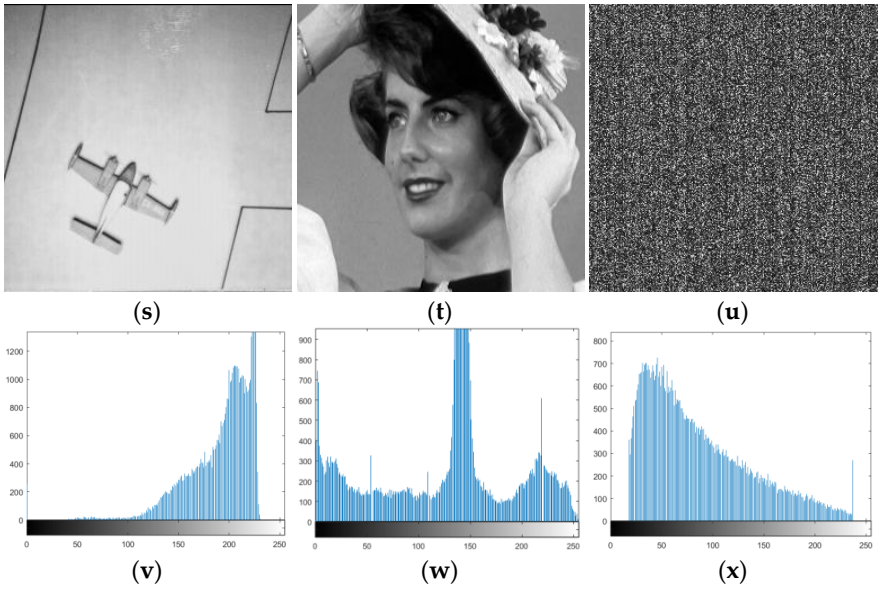

**Figure 4.** Histogram analysis. (**a**) Original image Lady, (**b**) original imageWoman, (**c**) encrypted image 1, (**d**) the histogram of Lady, (**e**) the histogram of Woman, (**f**) and the histogram of encrypted image 1. (**g**) Original image Milkdrop, (**h**) original image Airplane, (**i**) encrypted image 2, (**j**) the histogram of Milkdrop, (**k**) the histogram of Airplane, and (**l**) the histogram of encrypted image 2. (**m**) Original image Woman, (**n**) original image Milkdrop, (**o**) encrypted image 3, (**p**) the histogram of Woman, (**q**) the histogram of Milkdrop, and (**r**) the histogram of encrypted image 3. (**s**) Original image Airplane, (**t**) original image Lady, (**u**) encrypted image 4, (**v**) the histogram of Airplane, (**w**) the histogram of Lady, and (**x**) the histogram of encrypted image 4.

**Table 1.** Comparison of histogram similarity between cipher images in Figure 4.

| Histogram 1 | Histogram 2 | Euclidean Distance |
|---|---|---|
| Encrypted image 1 | Encrypted image 2 | 0.0054 |
| Encrypted image 1 | Encrypted image 3 | 0.0057 |
| Encrypted image 1 | Encrypted image 4 | 0.0056 |
| Encrypted image 2 | Encrypted image 3 | 0.0055 |
| Encrypted image 2 | Encrypted image 4 | 0.0054 |
| Encrypted image 3 | Encrypted image 4 | 0.0059 |

### *4.3. Key Space Analysis*

The key space is an important indicator to measure the security performance of an encryption system. The larger the key space, the more difficult it is to brute force. The size of the key space is determined by the key length. According to [34], when the key space is greater than $2^{100}$, in theory, the cryptosystem can resist brute force attacks. The proposed encryption scheme uses a set of keys, including parameters such as sampling rate, four random phase masks, and a CS measurement matrix. The sampling rate is a double-precision type with a value range of [0, 1]. The random phase mask and the measurement matrix are both matrices. They are used as keys. Obviously, the key space is extremely large, so that the attacker cannot make enough attempts within the effective time. Therefore, it can resist brute force attacks well.

### *4.4. Correlation Analysis*

Another important indicator for evaluating the performance of an image encryption scheme is the correlation between adjacent pixels. Generally speaking, there is a strong correlation between adjacent pixels of a plaintext image, while the correlation between adjacent pixels of a ciphertext image encrypted by an effective encryption scheme is

relatively low. In the adjacent pixel correlation simulation, without loss of generality, we choose image Lady and Woman as plaintext images, and use the encrypted image of the two as the contrast ciphertext image. In order to calculate the correlation coefficient in the horizontal direction, the vertical direction and the diagonal direction, 5000 pairs are randomly selected from the plaintext images and the ciphertext image, respectively. The following formula is the mathematical definition of the correlation coefficient *Cor*, which is used to evaluate the correlation between two adjacent pixels

$$Cor(X) = \frac{\sum_{i=1}^{m} (x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{m} (x_i - E(x))^2 \sum_{i=1}^{m} (y_i - E(y))^2}} \tag{20}$$

where $x_i$ and $y_i$ denote two randomly selected pixels in the test image, m denotesthe number of selected pixel pair, and $E(\cdot)$ refers to the function to calculate the average. Figure 5 and Table 2 show the correlation calculation results of the original image and the encrypted image involved in the proposed scheme in the horizontal, vertical, and diagonal directions. From the figure, we can clearly see that there is a strong correlation between the pixels of the original image, while the correlations between the pixels of the encrypted image are weak.

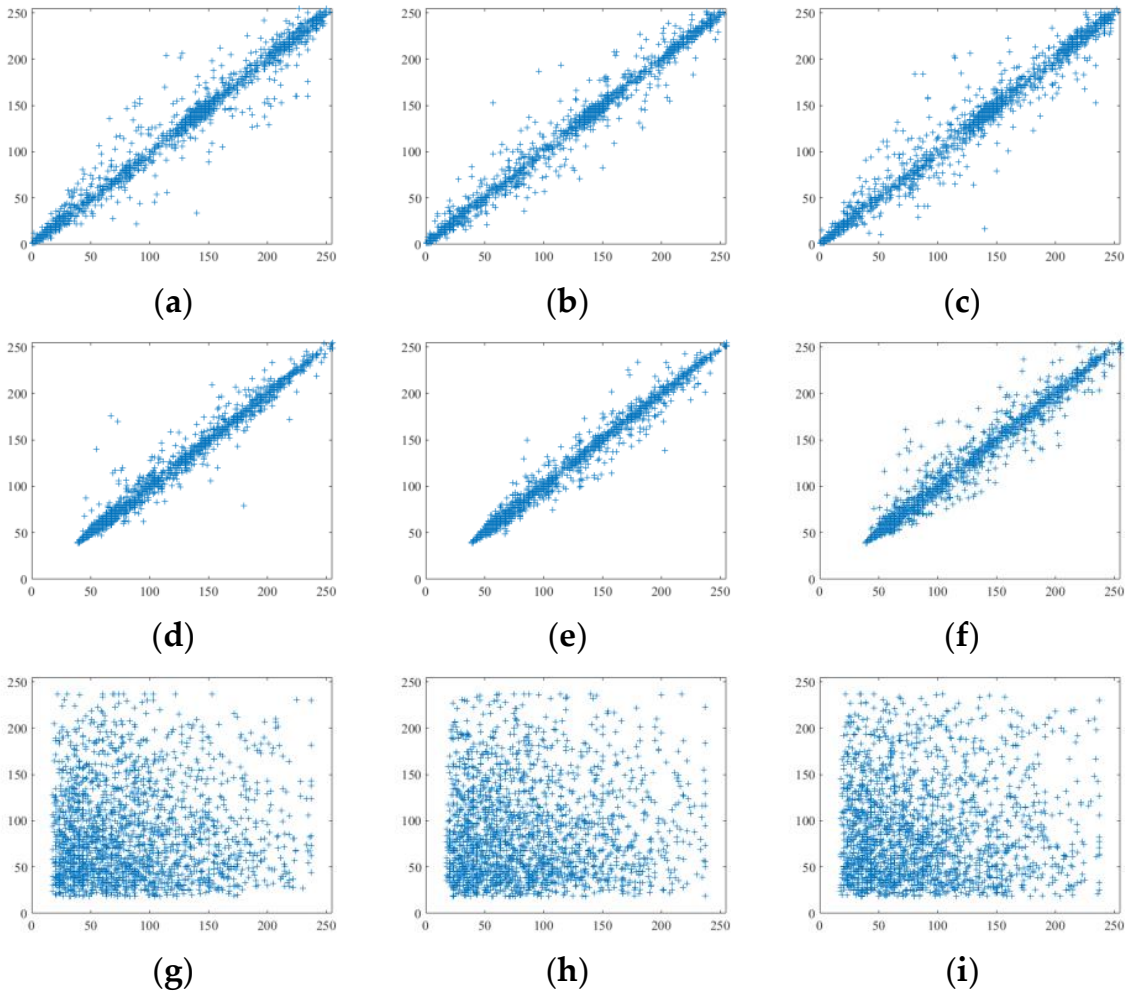


**Figure 5.** Correlation analysis: (**a**–**c**) horizontal direction, vertical direction, and diagonal direction in plain image Lady; (**d**–**f**) horizontal direction, vertical direction, and diagonal direction in plain image Woman; (**g**–**i**) horizontal direction, vertical direction, and diagonal direction in encrypted image.

**Table 2.** Correlation coefficients of two adjacent pixels in the pain and encrypted images.

| Image | Plaintext Image | | | Ciphertext Image | | |
|---|---|---|---|---|---|---|
| | Horizontal Direction | Vertical Direction | Diagonal Direction | Horizontal Direction | Vertical Direction | Diagonal Direction |
| Lady | 0.9840 | 0.9903 | 0.9825 | −0.0004 | 0.0266 | 0.0081 |
| Woman | 0.9914 | 0.9926 | 0.9859 | | | |
| Milkdrop | 0.9723 | 0.9843 | 0.9602 | −0.0026 | 0.0298 | 0.0047 |
| Airplane | 0.9571 | 0.9366 | 0.8927 | | | |
| Woman | 0.9914 | 0.9926 | 0.9859 | −0.0001 | 0.0272 | 0.0043 |
| Milkdrop | 0.9723 | 0.9843 | 0.9602 | | | |
| Airplane | 0.9571 | 0.9366 | 0.8927 | −0.0034 | 0.0259 | 0.0029 |
| Lady | 0.9840 | 0.9903 | 0.9825 | | | |

### *4.5. Authentication Performance Analysis*

The proposed scheme can conduct authentication. Step 9 in decryption process gives the method of authentication, i.e., calculating the peak correlation energy (PCE). Table 3 and Figure 6 show the PCE values of the relevant reconstructed images and the corresponding authentication information. It can be seen from the third column of Figure 6 that there is a peak on the correlation plane between the reconstructed image and the authentication information, which shows that the reconstructed image has a strong correlation with the authentication information.

**Table 3.** The PCE values between the constructed images and their authentication information.

| Group | Image | PCE |
|---|---|---|
| Group 1 | Lady | 0.002625 |
| | Woman | 0.003823 |
| Group 2 | Milkdrop | 0.004608 |
| | Airplane | 0.000711 |
| Group 3 | Woman | 0.002654 |
| | Milkdrop | 0.004656 |
| Group 4 | Airplane | 0.000522 |
| | Lady | 0.003023 |

### *4.6. Robustness Analysis*

In order to test the robustness of the proposed scheme against noise attacks, we test the quality of decrypted reconstructed images under different intensities of noise. In this section, image Lady and Woman with size of $256 \times 256$ are selected as the test images. Salt and pepper noise with an intensity of 0.001%, 0.003%, 0.005%, and 0.007% is respectively added to the ciphertext image encrypted by the above two images, and then we decrypt and reconstruct the encrypted ciphertext. Figure 7 shows the results of the simulation experiment. Similarly, Gaussian noise with intensity 0.0001%, 0.0003%, 0.0005%, and 0.0007% is respectively added to the ciphertext image encrypted by the above two images, and then the encrypted ciphertext is decrypted and reconstructed. Figure 8 gives the results of the simulation experiment. We add speckle noise with an intensity of 0.0001%, 0.0003%, 0.0005%, and 0.0007% to the ciphertext image encrypted by the above two images, respectively, and then decrypt and reconstruct the encrypted ciphertext. Figure 9 shows the result of the simulation experiment. Through the above three anti-noise tests, it can be seen that when the ciphertext image is contaminated by different noises, the decrypted and reconstructed image still maintains a higher PSNR with the original image, which is meaningful.

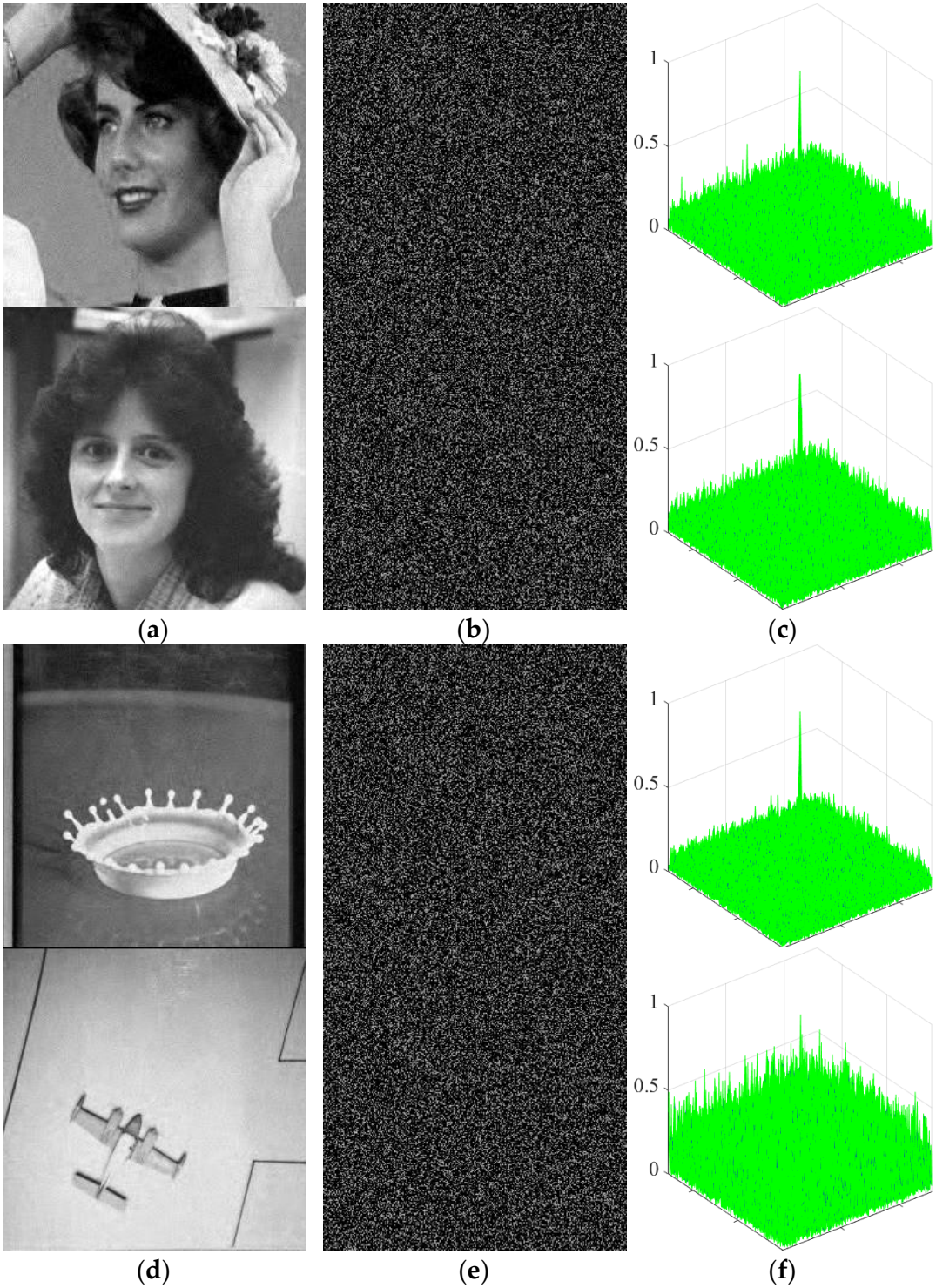


**Figure 6.** *Cont.*

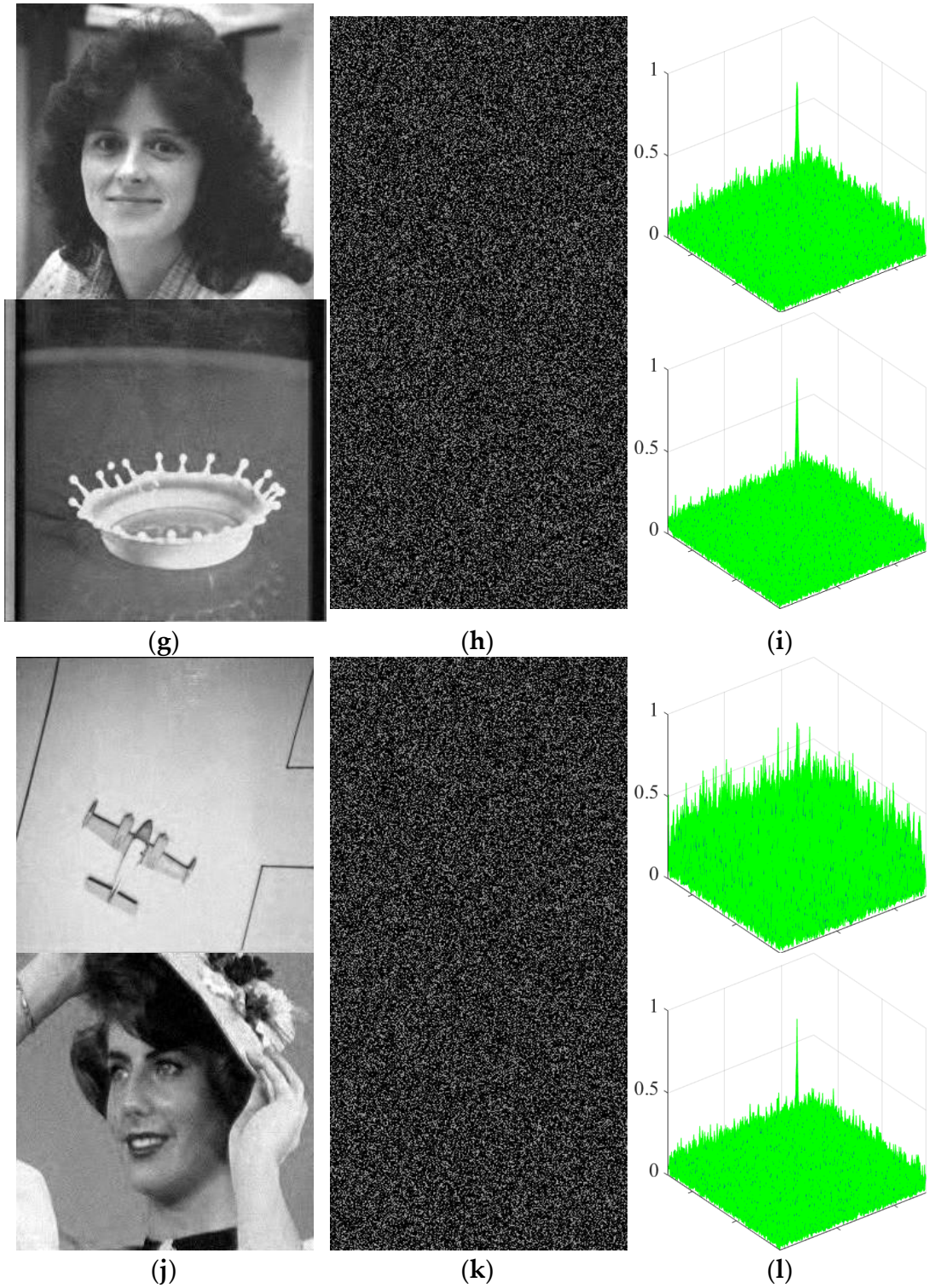


**Figure 6.** Authentication performance analysis. (**a**) The reconstructed images Lady and Woman, (**b**) the authentication information, and (**c**) PCE: Lady (PCE: 0.002625) andWoman (PCE: 0.003823). (**d**) The reconstructed images Milkdrop and Airplane, (**e**) the authentication information, and (**f**) PCE: Milkdrop (PCE: 0.004608) and Airplane (PCE: 0.000711). (**g**) The reconstructed images Woman and Milkdrop, (**h**) the authentication information, and (**i**) PCE: Woman (PCE: 0.002654) and Milkdrop (PCE: 0.004656). (**j**) The reconstructed images Airplane and Lady, (**k**) the authentication information, and (**l**) PCE: Airplane (PCE: 0.000522) and Lady (PCE: 0.003023).

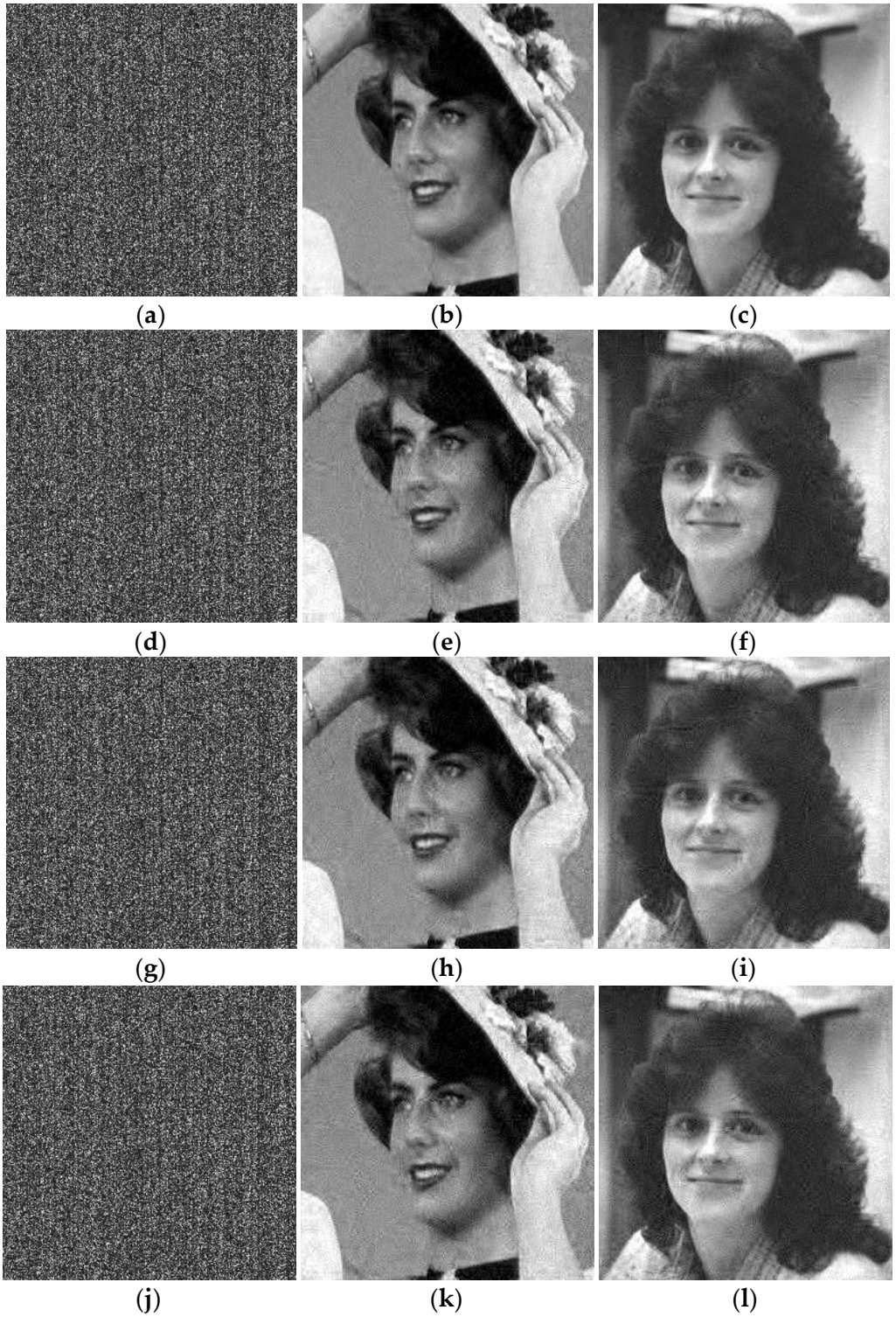


**Figure 7.** Robustness evaluation against salt and pepper noise: the first column is sequentially cipher image with salt and pepper noise intensities of 0.001%, 0.003%, 0.005%, and 0.007%, while the second and third columns denote the decrypted images corresponding to the first column, respectively. (**a**) Salt and pepper noise with intensity of 0.001%, (**b**) PSNR = 30.0951, (**c**) PSNR = 32.6647; (**d**) salt and pepper noise with intensity of 0.003%, (**e**) PSNR = 26.5440, (**f**) PSNR = 28.5623; (**g**) salt and pepper noise with intensity of 0.005%, (**h**) PSNR = 26.2989, (**i**) PSNR = 28.0024; (**j**) salt and pepper noise with intensity of 0.007%, (**k**) PSNR = 25.9692, (**l**) PSNR = 27.9644.

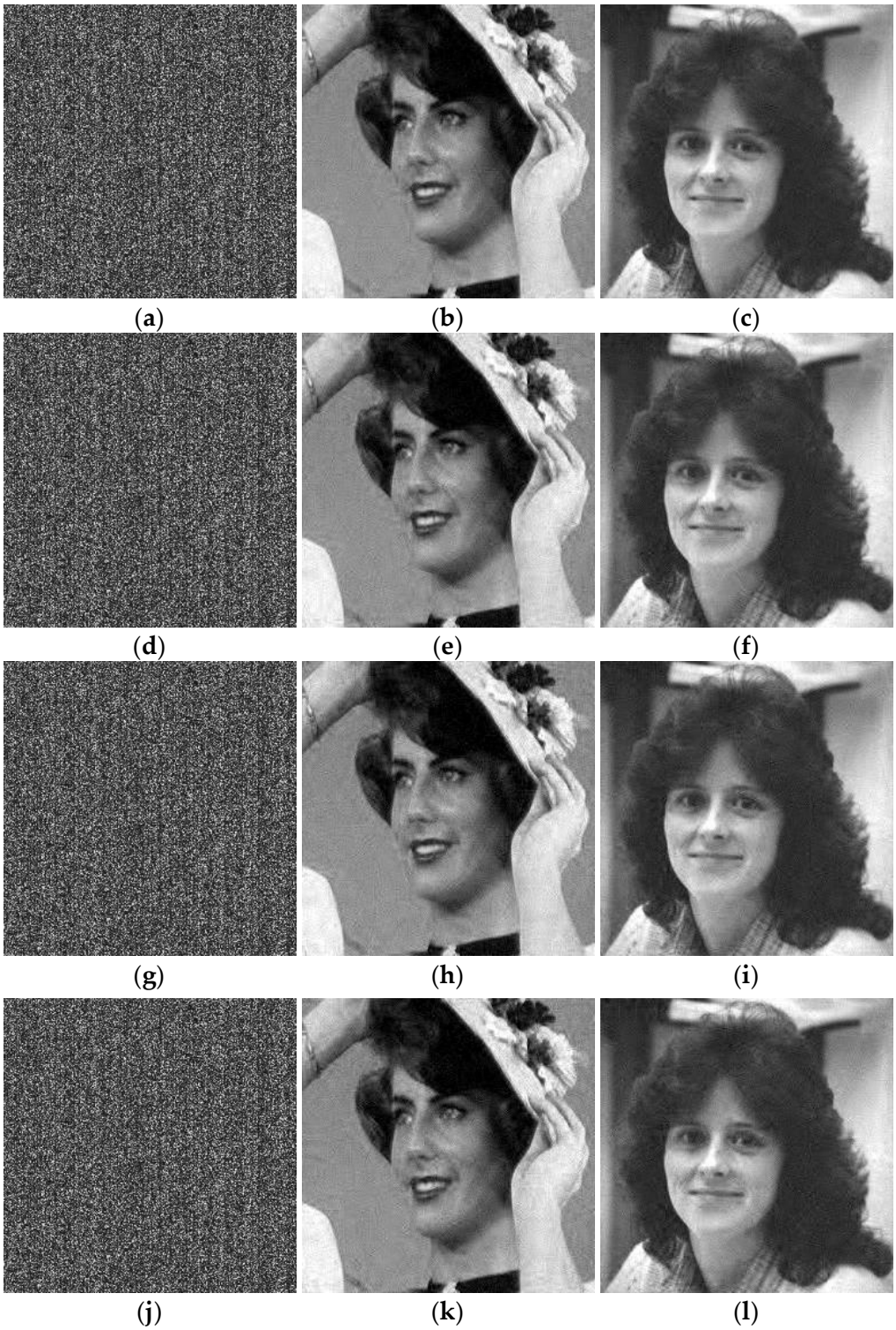


**Figure 8.** Robustness evaluation against Gaussian noise: the first column has asequentially cipher image with Gaussian noise intensities of 0.0001%, 0.0003%, 0.0005%, and 0.0007%, while the second and third columns denote the decrypted images corresponding to the first column, respectively. (**a**) Gaussian noise with intensity of 0.0001%, (**b**) PSNR = 29.8744 dB, (**c**) PSNR = 32.2412 dB; (**d**) Gaussian noise with intensity of 0.0003%, (**e**) PSNR = 29.1993 dB, (**f**) PSNR = 31.4085 dB; (**g**) Gaussian noise with intensity of 0.0005%, (**h**) PSNR = 28.7798 dB, (**i**) PSNR = 31.0102 dB; (**j**) Gaussian noise with intensity of 0.0007%, (**k**) PSNR = 28.5866 dB, (**l**) PSNR = 30.6265 dB.

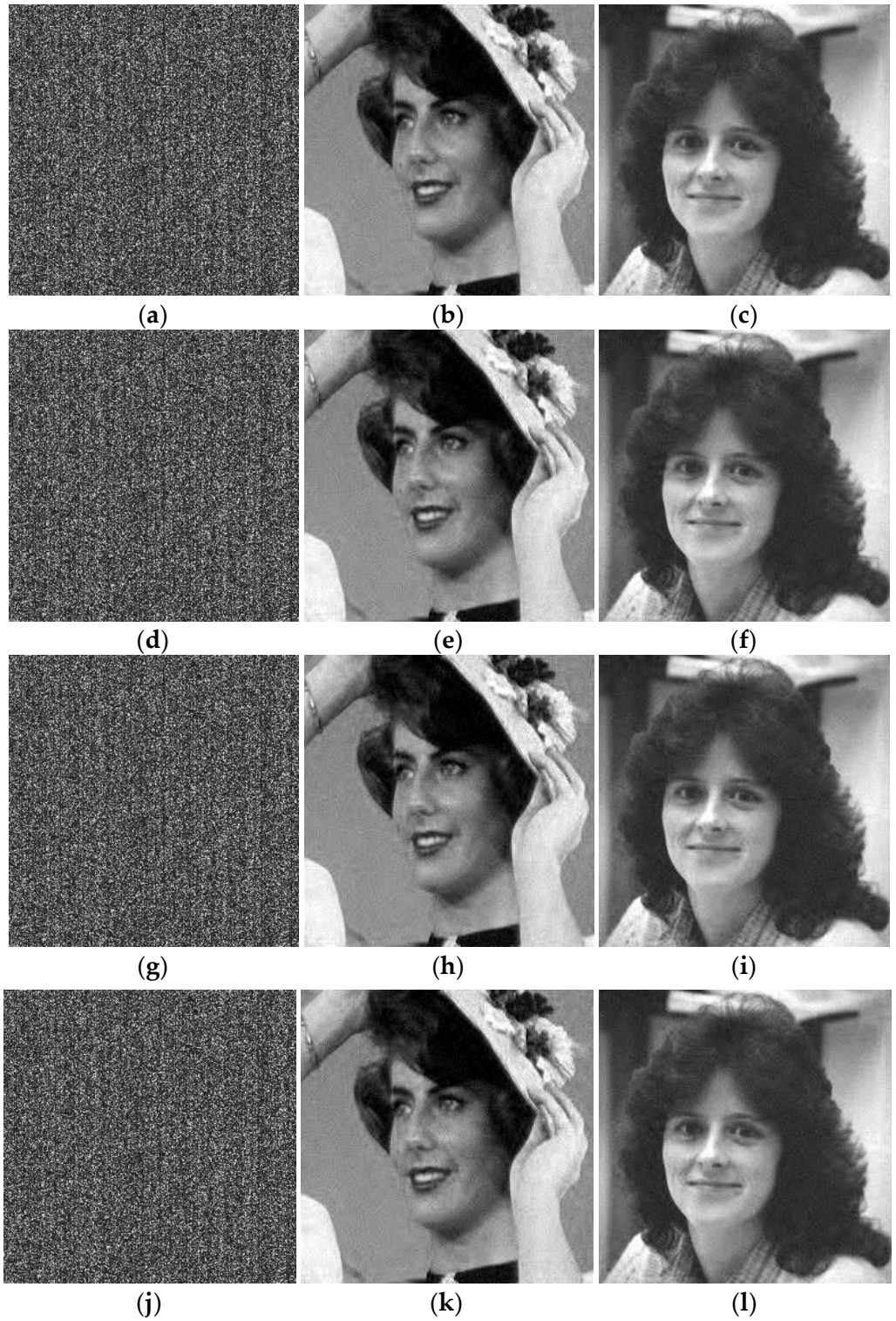


**Figure 9.** Robustness evaluation against speckle noise: the first column has a sequentially cipher image with speckle noise intensities of 0.0001%, 0.0003%, 0.0005%, and 0.0007%, while the second and third columns denote the decrypted images corresponding to the first column, respectively. (**a**) Speckle noise with intensity of 0.0001%, (**b**) PSNR = 30.0951 dB, (**c**) PSNR = 32.6647 dB; (**d**) speckle noise with intensity of 0.0003%, (**e**)PSNR = 30.0451 dB, (**f**) PSNR = 32.5451 dB; (**g**) speckle noise with intensity of 0.0005%, (**h**) PSNR = 29.9122 dB, (**i**) PSNR = 32.3052 dB; (**j**) speckle noise with intensity of 0.0007%, (**k**) PSNR = 29.7490 dB, (**l**) PSNR = 32.1894 dB.

In order to test the robustness of the proposed scheme against shearing attacks, we cut the image blocks with size of in the upper left corner, lower left corner, upper right corner, lower right corner, and central position of the ciphertext image in order to obtain the corresponding shearing-attacked ciphertext images, which are shown in the first column of Figure 10. The second and third columns of Figure 10 show the decrypted and reconstructed images corresponding to the shearing-attacked ciphertext images. The experimental simulation results show that the decrypted and reconstructed images from the shearing-attacked ciphertext images still contain most of the information of the original image, indicating that the proposed scheme can resist the shearing attack to a certain extent.

**Figure 10.** Robustness against shearing attack analysis: The first row to the fifth row in the first column are sequentially the cipher image with shearing attack in the upper left corner, the upper right corner, the bottom left corner, the bottom right corner, and the central directions; the second column and the third column denote the decrypted images corresponding to the first column.

For the perspective of the robustness against differential attack, we give our theoretical analysis here. Differential attack works when the key is reused. In this proposed scheme, the key, including sampling/compression rate, four random phase masks, and a CS measurement matrix, is used only once. We change our key each time of encryption. Therefore, the proposed scheme can resist differential attack.

## 5. Conclusions

This paper puts forward a new secure double image encryption scheme based on CS and DRPE, which not only realizes the compression and encryption of two images into one image, but also realizes image authentication. In the proposed scheme, the two original images are firstly compressed using CS, and then DRPE is performed to obtain two small-sized images. Meanwhile, the two original images are directly subjected to DRPE to obtain the authentication information. Then, we combine two small-size images and authentication information into one image, and finally perform DRPE to obtain the final encrypted image. The proposed scheme makes full use of the advantages of CS to achieve compression and encryption simultaneously, and combines CS with optical transformation technology, which not only reduces storage space and transmission bandwidth, but also improves the security performance of encryption. It has better application value in resource-constrained scenarios.

**Author Contributions:** Conceptualization, R.Z.; validation, D.X.; Writing—original draft, R.Z.; supervision, D.X.; project administration, D.X.; funding acquisition, D.X. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by the National Natural Science Foundation of China (Grant No. 62072063).

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Donoho, D.L. Compressed sensing. *IEEE Trans. Inf. Theory* **2006**, *52*, 1289–1306. [CrossRef]
2. Candes, E.J.; Romberg, J.; Tao, T. Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information. *IEEE Trans. Inf. Theory* **2006**, *52*, 489–509. [CrossRef]
3. Candès, E.J.; Wakin, M.B. An Introduction to Compressive Sampling. *IEEE Signal Process. Mag.* **2008**, *25*, 21–30. [CrossRef]
4. Candes, E.J.; Tao, T. Near-Optimal Signal Recovery from Random Projections: Universal Encoding Strategies? *IEEE Trans. Inf. Theory* **2006**, *52*, 5406–5425. [CrossRef]
5. Tropp, J.A.; Gilbert, A.C. Signal Recovery from Random Measurements Via Orthogonal Matching Pursuit. *IEEE Trans. Inf. Theory* **2007**, *53*, 4655–4666. [CrossRef]
6. Figueiredo, M.; Nowak, R.D.; Wright, S.J. Gradient Projection for Sparse Reconstruction: Application to Compressed Sensing and Other Inverse Problems. *IEEE J. Sel. Top. Signal Process.* **2007**, *1*, 586–597. [CrossRef]
7. Chartrand, R. Exact Reconstruction of Sparse Signals via Nonconvex Minimization. *IEEE Signal Process. Lett.* **2007**, *14*, 707–710. [CrossRef]
8. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
9. Hua, Z.; Zhou, Y. Image encryption using 2D logistic-adjusted-sine map. *Inf. Sci.* **2016**, *339*, 237–253. [CrossRef]
10. Wang, X.; Teng, L.; Qin, X. A novel color image encryption algorithm based on chaos. *Signal Process.* **2012**, *92*, 1101–1108. [CrossRef]
11. Zhang, Y.; Xiao, D. Self-adaptive permutation and combined global diffusion for chaotic color image encryption. *AEU Int. J. Electron. Commun.* **2014**, *68*, 361–368. [CrossRef]
12. Lui, O.-Y.; Wong, K.-W.; Chen, J.; Zhou, J. Chaos-based joint compression and encryption algorithm for generating variable length ciphertext. *Appl. Soft Comput.* **2012**, *12*, 125–132. [CrossRef]
13. Hua, Z.; Zhou, Y.; Pun, C.M.; Chen, C.L.P. 2D Sine Logistic modulation map for image encryption. *Inf. Sci.* **2014**, *297*, 80–94. [CrossRef]
14. Zhang, L.Y.; Hu, X.; Liu, Y.; Wong, K.-W.; Gan, J. A chaotic image encryption scheme owning temp-value feedback. *Commun. Nonlinear Sci. Numer. Simul.* **2014**, *19*, 3653–3659. [CrossRef]

15. Wen, W.; Zhang, Y.; Fang, Z.; Chen, J.-X. Infrared target-based selective encryption by chaotic maps. *Opt. Commun.* **2015**, *341*, 131–139. [CrossRef]
16. Chen, J.-X.; Zhu, Z.-L.; Liu, Z.; Fu, C.; Zhang, L.-B.; Yu, H. A novel double-image encryption scheme based on cross-image pixel scrambling in gyrator domains. *Opt. Express* **2014**, *22*, 7349–7361. [CrossRef]
17. Chen, J.-X.; Zhu, Z.-L.; Fu, C.; Zhang, L.-B.; Zhang, Y. Cryptanalysis and improvement of an optical image encryption scheme using a chaotic Baker map and double random phase encoding. *J. Opt.* **2014**, *16*, 125403. [CrossRef]
18. Chen, J.-X.; Zhu, Z.-L.; Fu, C.; Zhang, L.-B.; Yu, H. Analysis and improvement of a double-image encryption scheme using pixel scrambling technique in gyrator domains. *Opt. Lasers Eng.* **2015**, *66*, 1–9. [CrossRef]
19. Zhang, Y.; Xiao, D.; Wen, W.; Tian, Y. Edge-based lightweight image encryption using chaos-based reversible hidden transform and multiple-order discrete fractional cosine transform. *Opt. Laser Technol.* **2013**, *54*, 1–6. [CrossRef]
20. Refregier, P.; Javidi, B. Optical image encryption using inputplane and Fourier plane random encoding. *Opt. Lett.* **1995**, *20*, 767–769. [CrossRef]
21. Unnikrishnan, G.; Joseph, J.; Singh, K. Optical encryption by double-random phase encoding in the fractional Fourier domain. *Opt. Lett.* **2000**, *25*, 887–889. [CrossRef]
22. Situ, G.; Zhang, J. Double random-phase encoding in the Fresnel domain. *Opt. Lett.* **2004**, *29*, 1584–1586. [CrossRef] [PubMed]
23. Zhang, Y.; Wang, B. Optical image encryption based on interference. *Opt. Lett.* **2008**, *33*, 2443–2445. [CrossRef] [PubMed]
24. Qin, W.; Peng, X. Asymmetric cryptosystem based on phase-truncated Fourier transforms. *Opt. Lett.* **2010**, *35*, 118–120. [CrossRef] [PubMed]
25. Nomura, T.; Javidi, B. Optical encryption using a joint transform correlator architecture. *Opt. Eng.* **2000**, *39*, 2031–2035.
26. Lu, P.; Xu, Z.; Lu, X.; Liu, X. Digital image information encryption based on Compressive Sensing and double random-phase encoding technique. *Optik* **2013**, *124*, 2514–2518. [CrossRef]
27. Rawat, N.; Kumar, R.; Lee, B. Implementing compressive fractional Fourier transformation with iterative kernel steering re-gression in double random phase encoding. *Optik* **2014**, *125*, 5414–5417. [CrossRef]
28. Deepan, B.; Quan, C.; Wang, Y.; Tay, C.J. Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique. *Appl. Opt.* **2014**, *53*, 4539–4547. [CrossRef] [PubMed]
29. Zhang, Y.; Zhang, L.Y. Exploiting random convolution and random subsampling for image encryption and compression. *Electron. Lett.* **2015**, *51*, 1572–1574. [CrossRef]
30. Liu, Y.; Hu, Y.; Li, Y.; Qin, Q.; Li, G.; Tan, Z.; Wang, M.; Yan, F. Image Compression-Encryption Scheme via Fiber Specklegram-Based Compressive Sensing and Double Random Phase Encoding. *IEEE Photon. J.* **2020**, *12*, 7102311. [CrossRef]
31. Liu, J.L.; Zhang, M.; Tong, X.J.; Wang, Z. Image compression-encryption algorithm based on 2D compressive sensing and dou-ble random phase encoding. *J. Phys. Conf. Ser.* **2020**, *1684*, 012123. [CrossRef]
32. Li, H.; Yu, C.; Wang, X. A novel 1D chaotic system for image encryption, authentication and compression in cloud. *Multimed. Tools Appl.* **2020**, *80*, 8721–8758. [CrossRef]
33. Kumar, B.V.K.V.; Hassebrook, L. Performance measures for correlation filters. *Appl. Opt.* **1990**, *29*, 2997–3006. [CrossRef] [PubMed]
34. Alvarez, G.; Li, S. Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. *Int. J. Bifurc. Chaos* **2006**, *16*, 2129–2151. [CrossRef]