sensors

Article

A Multi-Image Encryption Based on Sinusoidal Coding Frequency Multiplexing and Deep Learning

Qi Li, Xiangfeng Meng *, Yongkai Yin and Huazheng Wu

School of Information Science and Engineering and Shandong Provincial Key Laboratory of Laser Technology and Application, Shandong University, Qingdao 266237, China; 202032785@mail.sdu.edu.cn (Q.L.); yinyongkai@sdu.edu.cn (Y.Y.); 201812554@mail.sdu.edu.cn (H.W.)

* Correspondence: xfmeng@sdu.edu.cn

Abstract: Multi-image encryption technology is a vital branch of optical encryption technology. The traditional encryption method can only encrypt a small number of images, which greatly restricts its application in practice. In this paper, a new multi-image encryption method based on sinusoidal stripe coding frequency multiplexing and deep learning is proposed to realize the encryption of a greater number of images. In the process of encryption, several images are grouped, and each image in each group is first encoded with a random matrix and then modulated with a specific sinusoidal stripe; therefore, the dominant frequency of each group of images can be separated in the Fourier frequency domain. Each group is superimposed and scrambled to generate the final ciphertext. In the process of decryption, deep learning is used to improve the quality of decrypted image and the decryption speed. Specifically, the obtained ciphertext can be sent into the trained neural network and then the plaintext image can be reconstructed directly. Experimental analysis shows that when 32 images are encrypted, the CC of the decrypted result can reach more than 0.99. The efficiency of the proposed encryption method is proved in terms of histogram analysis, adjacent pixels correlation analysis, anti-noise attack analysis and resistance to occlusion attacks analysis. The encryption method has the advantages of large amount of information, good robustness and fast decryption speed.

Keywords: optical information security; deep learning; sinusoidal coding; frequency multiplexing

check for updates

Citation: Li, Q.; Meng, X.; Yin, Y.; Wu, H. A Multi-Image Encryption Based on Sinusoidal Coding Frequency Multiplexing and Deep Learning. *Sensors* **2021**, *21*, 6178. https://doi.org/ 10.3390/s21186178

Academic Editor: Evangelia I. Zacharaki

Received: 20 August 2021
Accepted: 13 September 2021
Published: 15 September 2021

1. Introduction

As the development of the Internet, networks and information systems are playing an increasingly important role in people's life, work and study. However, as people's expectations for informatization have deepened, a subject that cannot be ignored has been placed in front of people, that is, the security of information. The resolution of these security issues depends on the progress and development of information security technology. Therefore, the research on information security technology plays a vital role, which not only has academic value but also plays an important role in promoting the development of the entire human society. Data encryption technology based on optical theory and method is a new generation of information security theory and technology that has begun to develop internationally in recent years. Compared with traditional information security technology, optical information security technology has the following advantages: firstly, optical cryptography system has parallelism [1]. Secondly, optical cryptography systems usually have large key space. Thirdly, optical cryptography system has the characteristics of multi-dimension [2]. Some inherent parameters of the system, such as amplitude, phase, wavelength and optical element parameters, can be used as the key parameters of the optical cryptosystem to achieve multi-dimensional encryption. Therefore, optical information security technology has the characteristics of large capacity, fast storage speed, multi-dimensional parallel processing and so on and has unique advantages in data transmission and protection. Today, with the growing development of optical information technology, optical image encryption technology has made great progress.

In 1995, Refregier et al. [3] proposed an optical image encryption scheme based on double random phase encoding for the first time, which means it uses two uncorrelated random phase templates and Fourier transform to realize optical image encryption. In essence, this scheme is based on optical transformation to disturb the information of plaintext images and generate ciphertext images, such as fractional Fourier transform [4], fractional wavelet transform [5], fractional Merlin transform [6], interference [7], single-pixel imaging [8,9], etc. Optical image encryption belongs to parallel encryption with high speed and high efficiency, but its encryption performance is limited by the technology and precision of various optical devices in the optical path [10].

In addition, many previous studies [11–15] only consider the encryption of a single image, which greatly reduced the efficiency of the encryption system. As another important branch of optical encryption technology, multi-image encryption technology has attracted an increasing number of attention since it not only improves the encryption ability but also reduces the amount of ciphertext data. In recent years, multiple image encryption methods have been proposed based on wavelength multiplexing [16], multiplexing position [17], phase mask only (PMO) multiplexing [18], lateral transfer [19], optical data compression [20] and so on. Lee and Cho [21] proposed a double random phase encryption method for multi-image transmission based on orthogonal coding. Li et al. [22] proposed a multi-image encryption method based on compressed ghost imaging. Wu et al. [23] proposed a multi-image encryption scheme based on different diffraction distances to calculate ghost images. Zhang et al. [24] proposed a multi-image encryption scheme based on the concept of compressed ghost imaging and the sampling principle of Fourier transform. Yang [25] et al. proposed a multi-image encryption scheme based on compression coding aperture imaging. However, with the advent of the era of big data, a growing number of data need to be transmitted, and the above encryption methods can only encrypt a small number of images. At the same time, during decryption, it takes a lot more time than using the traditional multi-image encryption method, which greatly limits its application in practice. This inspired us to adopt a more efficient method to encrypt more images.

The energy of a natural image in the Fourier frequency domain is concentrated in the low-frequency component [26,27], and such multiplexing of the frequency information would be of few resolution loss. Codes with Fourier coefficients following impulse-shaped distribution can conduct effective frequency multiplexing [28]. Typical Fourier encoding is sinusoidal modulation, which shifts the Fourier spectrum of the original image to a specific region determined by the modulation frequency.

Inspired by the above theory, this paper introduces the sinusoidal stripe coding on the basis of random matrix. Specifically, the plaintext images are grouped before encryption, and each group of images is first subjected to random matrix coding and then sinusoidal stripe coding during encryption. The specially designed sinusoidal stripe moves the frequency components of each group of images in the Fourier frequency domain with different offsets. In this way, the number of encrypted images is far more than that of the traditional encryption method. In order to improve the quality of decrypted image and the speed of decryption, deep learning (DL) is used to reconstruct the plaintext during decryption, which is a powerful tool in many areas [29–34]. A predominant characteristic of DL is that it enables neural networks to automatically analyze the relationship between data and data. Therefore, we can use this characteristic of the neural network to study the corresponding relationship between the plaintext and the ciphertext in optical image encryption, that is to say, we can successfully realize the ciphertext decryption by analyzing the relationship between them.

The main contributions of the proposed encryption methods can be summarized as follows:

1. A multi-image encryption method based on sinusoidal coding frequency multiplexing and deep learning is proposed.

2. The proposed encryption method can realize the encryption of a greater number of images, which makes it more widely used.
3. In the process of decryption, deep learning is used to improve the quality of the decrypted image and the decryption speed.

The rest of this paper is organized as follows. The second part is to analyze the theories, which will include the introduction of sinusoidal stripes and the adoption of deep neural networks. The third part will explore the process of encryption and decryption in detail. Furthermore, the security and robustness will be analyzed in the fourth part. The final part is a conclusion.

2. The Theoretical Analysis

2.1. The Encryption Process

A multiplexed coding scheme will be proposed to encrypt images, and the encryption process is shown in Figure 1.

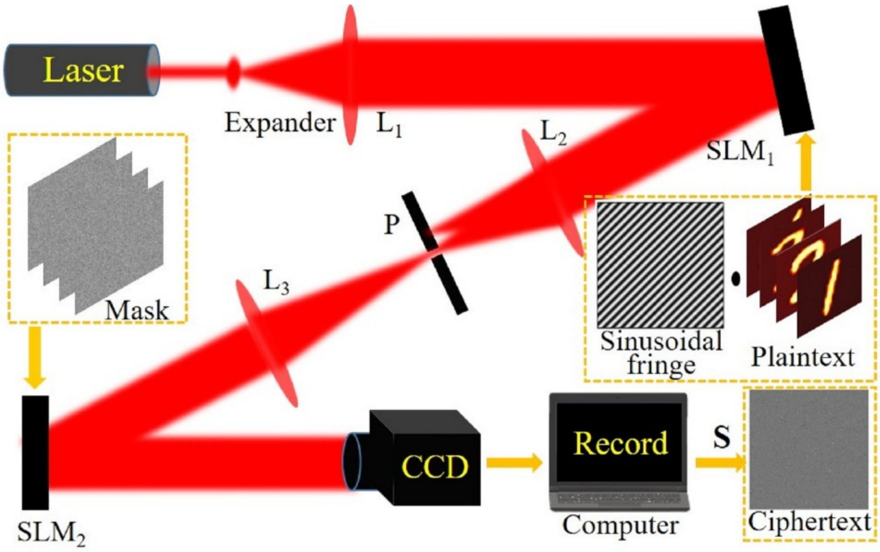


Figure 1. Schematic diagram of multi-image encryption and coding scheme.

Assuming that there are many $n \times m$ plaintext images, the encryption process is described as follows:

1. All the $n \times m$ plaintext images are divided into n groups; the plaintext images in each group and the sinusoidal code corresponding to each group of the plaintext images are successively sent to a spatial light modulator (SLM1) for display.
2. The L2 and L3 lenses form the 4F system, and the hole P is located on the spectral plane of the 4F system, which is used to extract the zero-order frequency after SLM1 and reduce the influence of errors caused by other orders. The random matrix corresponding to each plaintext image is uploaded to SLM2 for coding.
3. The superimposed light intensity recorded by the CCD is the time integral of the light field reaching the target surface within a certain period of time. Therefore, we make the exposure time of the CCD equal to the sum of the encoding time of all images in the SLM. In addition, their starting time should be synchronized, and the encoding time of each image should also be the same, which can be expressed as follows:

$$I(\overrightarrow{p}) = \sum_{j=1}^{n}\sum_{i=1}^{m} s_j(\overrightarrow{p}) r_i(\overrightarrow{p}) I_{ij}(\overrightarrow{p}) \tag{1}$$

Here $I(\vec{p})$ represents the ciphertext, $s_j(\vec{p})$ represents the j-th specially designed sinusoidal stripe, $r_i(\vec{p})$ represents the i-th random matrix, $I_{ij}(\vec{p})$ represents the plaintext image, and $\sum(\cdot)$ represents the sum of the elements.

1. According to the number of pixels with superimposed light intensity, an integer random sequence without repeating elements is generated. Secondly, replace the light intensity value on each pixel of the superimposed light intensity according to the value of the random sequence, so as to realize the scrambling operation. Scramble (S) [25] $I(\vec{p})$ to get the final ciphertext.

2.2. The Decryption Process

2.2.1. Downsampling in Fourier Frequency Domain

If we convert the obtained ciphertext image to the Fourier domain after scrambling recovery, its spectrum can be expressed as:

$$\widetilde{I}(\vec{p}) = \sum_{j=1}^{n}\sum_{i=1}^{m}\left[a\delta(\vec{\omega}) + \frac{b}{2}(\vec{\omega}+\vec{\omega}_j)e^{-\phi} + \frac{b}{2}(\vec{\omega}-\vec{\omega}_j)e^{\phi}\right] * \mathbb{F}\left[r_i(\vec{p})I_{ij}(\vec{p})\right] \tag{2}$$

where $\mathbb{F}[\bullet]$ represents the Fourier transform, $\vec{\omega}$ and ϕ represent the frequency and phase of the sinusoidal stripe, respectively. As shown in Figure 2, here we take m = 4 and n = 8 as an example. Each group is coded using four random matrices, followed by eight sinusoidal codes that move the frequency components of each group by different offsets; therefore, their dominant frequencies are staggered in Fourier domain. For each group, the shifted frequencies have two symmetrically conjugated positions (denoted by solid and dashed circular of the same color).

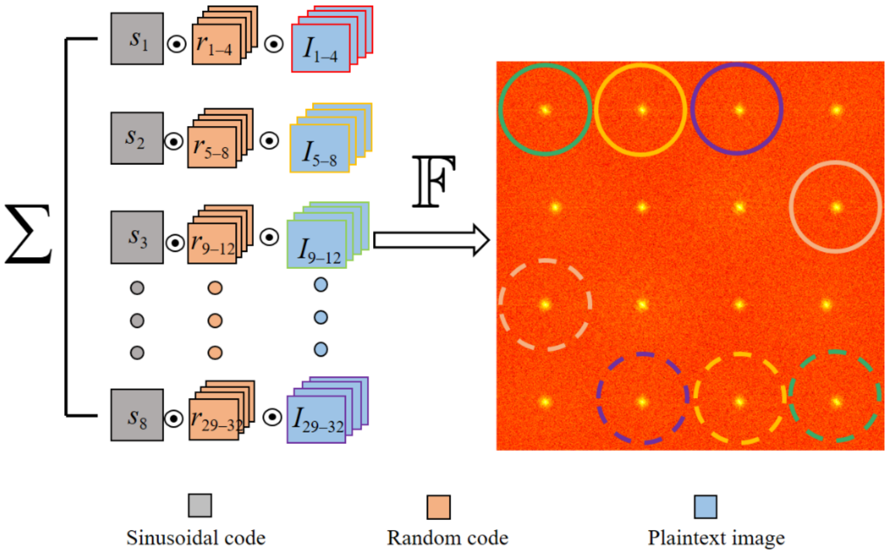


Figure 2. The coding scheme and the Fourier spectrum.

Since most energy of the plaintext images and the random matrix concentrates at low frequencies, $\sum_{i=1}^{m} r_i(\vec{p})I_{ij}(\vec{p})$ can be extracted via the operation ε as follows:

$$I_j(\vec{p}) = \sum_{i=1}^{m} r_i(\vec{p})I_{ij}(\vec{p}) = \frac{2}{b}\left|\mathbb{F}^{-1}\left[\varepsilon\left[\widetilde{I}(\vec{p})\right]\right]\right| \tag{3}$$

Here the operation ε includes two steps: first extracting the Fourier modulus from $\widetilde{I}(\vec{p})$, and then padding its surroundings with zeros to keep the original pixel resolution.

Then, I_j is taken as the input to the network, and the output is m plaintext images. The detailed process of deep neural network decryption will be described in the next section. So far, we can extract and decrypt m plaintext images from each group of I_j.

2.2.2. The Network Structure

Deep learning (DL) is a powerful tool in many areas. In the aspect of network structure, this paper adopts the classic U-Net [35] network structure, which is applied to plaintext reconstruction after modifying the output layer and loss function of U-Net. The input of the network is a single-channel two-dimensional image, and the final output is an m-channel two-dimensional image after passing through five down-sampling convolutional layers and five up-sampling deconvolution layers. Each channel represents a plaintext image. Its network structure and specific parameters of each layer are shown in Figure 3.

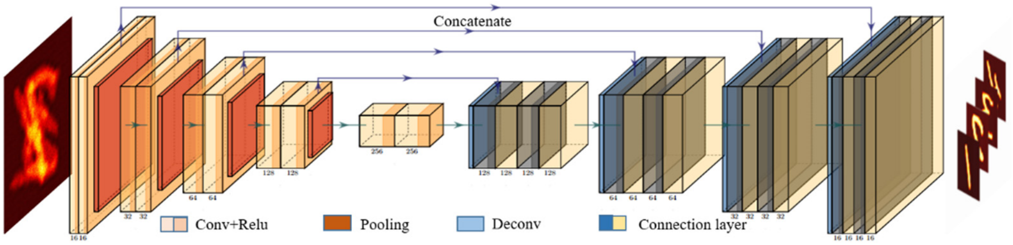


Figure 3. U-Net architecture.

In the process of neural network training, the datasets play an important role. A high quality dataset can often improve the quality of model training, speed up the progress of training and improve the final output results. Considering the particularity of the image encryption method proposed in this paper, we choose the self-made dataset, in which the data pair consists of m plaintext images and ciphertext. In this paper, 15,000 images are selected from MNIST handwritten dataset as the plaintext images, and then encrypted according to the encryption method mentioned above, so as to obtain the ciphertext-plaintext data pairs.

In order to better restore the plaintext images, mean-square error (MSE) is utilized and defined as follows:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M \times N} (x_i - y_i)^2 \tag{4}$$

where M and N represent the width and height of the image respectively, and x_i and y_i represent the output value of the last layer of the network and the truth value of the original image respectively. Since the last layer of the modified U-Net network is M-channel, the loss function is:

$$Loss_1 = \frac{1}{M \times N} \sum_{i=1}^{m} \sum_{j=1}^{M \times N} (x_{ij} - y_{ij})^2 \tag{5}$$

We further optimize the loss function and the benefit of this is to improve the training ability of the network. Specifically, the m plaintext images output from the network are encrypted again according to the proposed encryption method, and then the MSE is calculated with the real ciphertext, which can be expressed as:

$$Loss_2 = MSE(I(\vec{p}), I'(\vec{p})) = \frac{1}{M \times N} \sum_{i=1}^{M \times N} (I_i(\vec{p}) - I_i{}'(\vec{p}))^2 \tag{6}$$

where $I(\overrightarrow{p})$ represents the real ciphertext, and $I'(\overrightarrow{p})$ represents the reconstruction ciphertext that is re-encrypted using the plaintext image output from the network. Therefore, the total loss function is:

$$Loss = Loss_1 + Losss_2 = \frac{1}{M \times N}\sum_{i=1}^{m}\sum_{j=1}^{M\times N}(x_{ij} - y_{ij})^2 + \frac{1}{M \times N}\sum_{i=1}^{M\times N}(I_i(\overrightarrow{p}) - I_i{}'(\overrightarrow{p}))^2 \quad (7)$$

In the training process, the learning rate is set to 0.001 and the Adam optimizer [36] is used to optimize and update the parameters of the network. The number of training epoch is 50. All programs run in Python 3.7 with NVIDIA GeForce GTX 3060 GPU for acceleration.

3. Experiment Results

In order to prove the feasibility of our method in encryption and the superiority of decryption, we conduct numerical simulation experiments to verify it. In the process of encryption, 32 images are selected from MNIST handwritten digital dataset and divided into eight groups, with four images in each group, and the resolution is 256 × 256. Figure 4 shows the encryption process for multiple images.

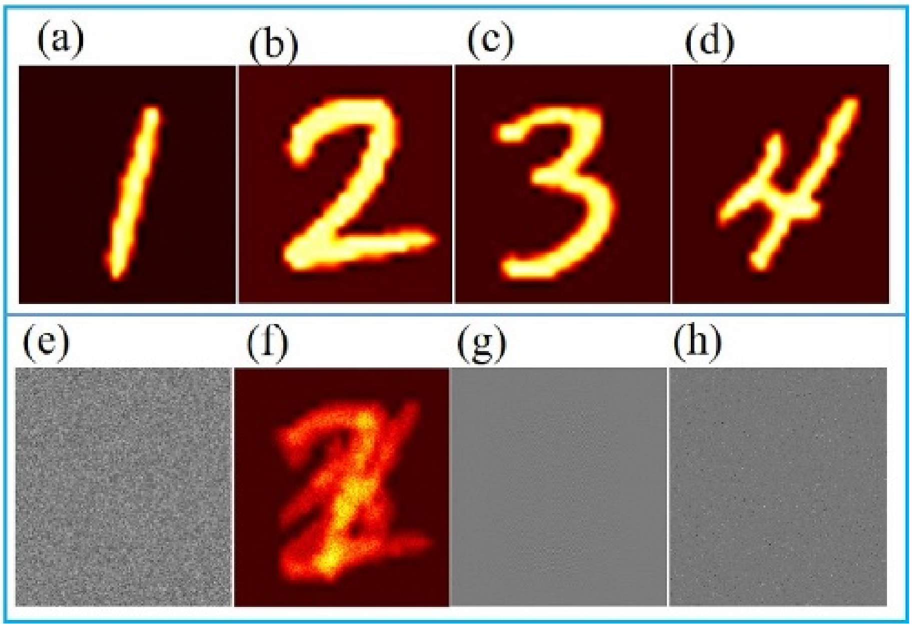


Figure 4. (**a**–**d**) Four plaintext images in the first group. (**e**) One of the random matrices. (**f**) The group ciphertext. (**g**) After superposition ciphertext. (**h**) After scrambling ciphertext.

The first line (a–d) in Figure 4 shows the plaintext images in the first group, Figure 4e represents one of the corresponding four random matrices, and Figure 4f–h represent the images encoded by random codes and sinusoidal stripes of the first group, the 8 groups of superimposed ciphertext image and the scrambled ciphertext images respectively. It can be found intuitively that it is almost impossible to detect any information of the original image from the ciphertext.

As shown in Figure 5, the detailed decryption process is described as follows:

1. The pixel location of the ciphertext is rearranged by the correct index keys to get the superimposed images;
2. Fourier transform is applied to the superimposed ciphertext image and appropriate down-sampling is carried out according to the specific spectrum distribution of each group;
3. Its surroundings are padded with zeros to keep the original pixel resolution;

4. Inverse Fourier transform is carried out and it is fed into the trained U-Net network.

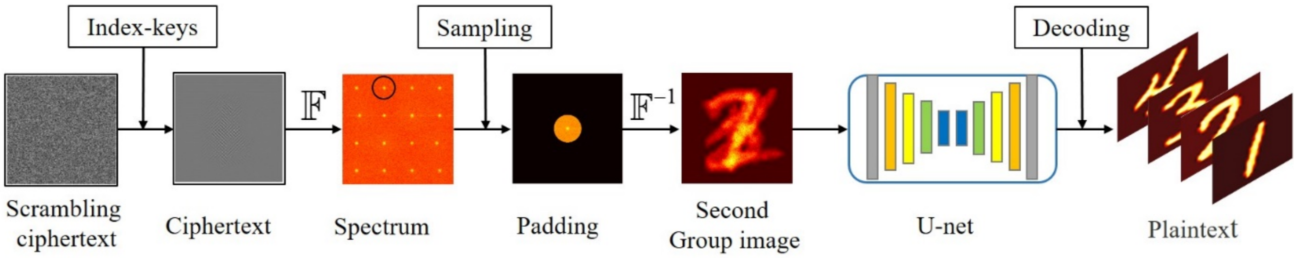
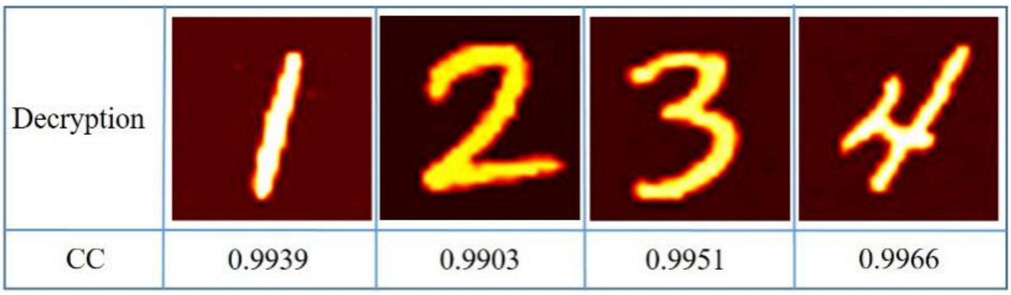


Figure 5. The decryption process.

The correlation coefficient (CC) is used to calculate the similarity between the original plaintext image and the decrypted image, which is defined as follows:

$$CC = \frac{E\{[I_t - E(I_t)] - [I - E(I)]\}}{\sigma_{I_t}\sigma_I} \tag{8}$$

where $E\{\cdot\}$ denotes the expected value operator, and σ is the standard deviation of the corresponding image. I_t and I are the original plaintext images and decrypted images, respectively. The closer CC value is to 1.0, the better the quality of the reconstructed images. The decryption results are shown in Figure 6, with CC of 0.9939, 0.9903, 0.9951, and 0.9966, respectively.



Decryption				
CC	0.9939	0.9903	0.9951	0.9966

Figure 6. The first set of decryption results.

Obviously, these final decrypted images with high quality are very similar to the corresponding plaintext images. At the same time, as the deep neural network is used to decrypt, the decryption time is very fast. Using Intel(R) Core(TM) i7-9700K CPU without using GPU acceleration, the entire decryption process can be completed in only 3.15 s. The decryption results for all groups are shown in Figure 7.

In addition, we use some plaintext images that do not belong to the training set for reconstruction to test the generalization of the encryption model proposed in this paper. For convenience, Handwritten English alphabets are used for testing and the reconstructed plaintext images are shown in Figure 8.

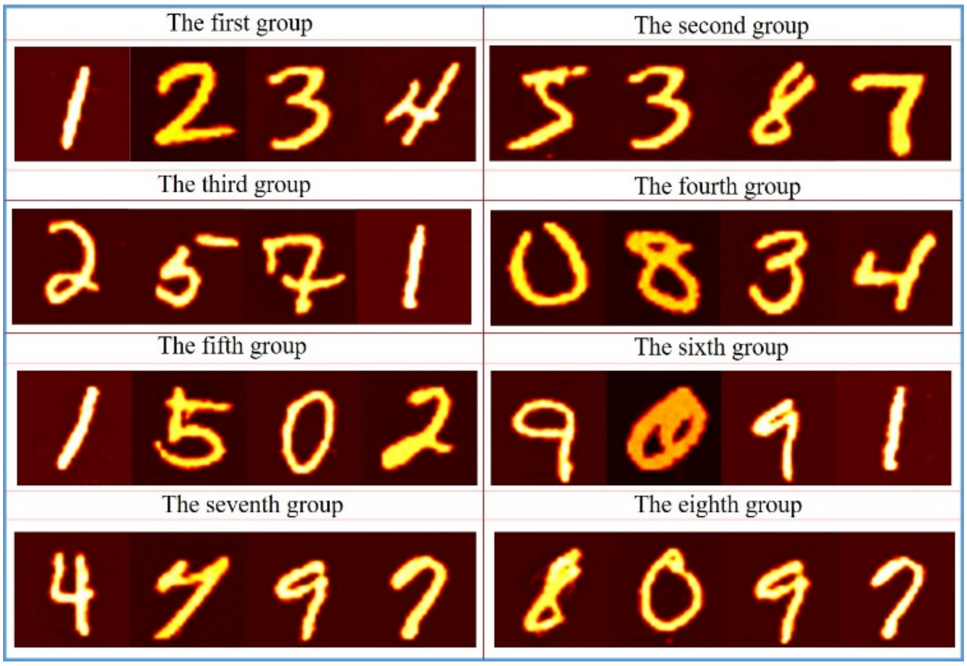


Figure 7. Decryption results for all groups.

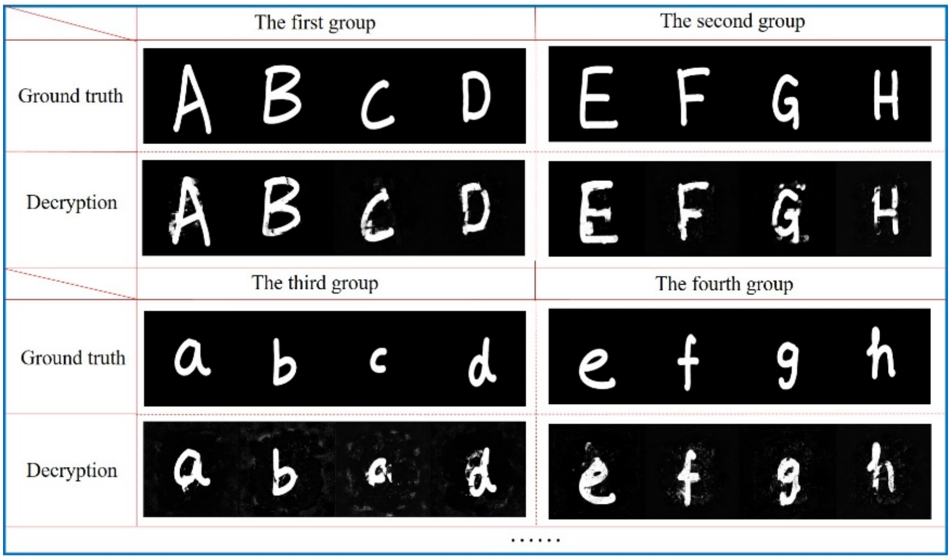


Figure 8. Testing results for handwritten English alphabet.

Although the network has been trained with MNIST handwritten datasets, it can perform high-quality reconstruction of handwritten English alphabet, which indicates that the U-Net networks can learn the correspondence between ciphertext images and original plaintext images very well.

In order to further verify the feasibility of the encryption method, we use FEI FACE Database [37] for training, in which the images are gray images with more complex content and richer details. In the process of encryption, four face images are used and divided into two groups, according to the encryption steps mentioned above. By reducing the number of encrypted images, each group of images can obtain a large sampling rate in the Fourier frequency domain to ensure high quality plaintext reconstruction. The decryption result is shown in Figure 9.

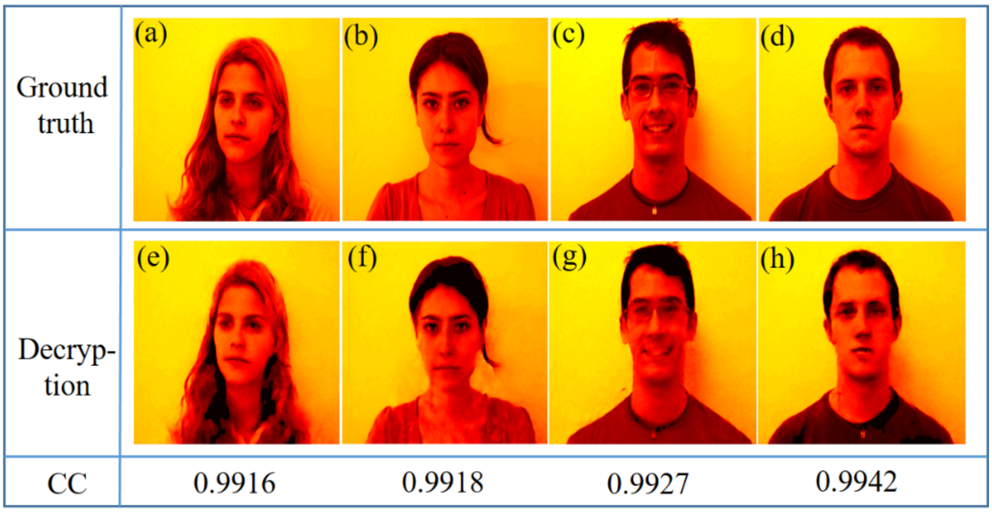


Figure 9. FEI face decryption results. (**a**–**d**) Groudtruth; (**e**–**h**) Decryption.

4. Algorithm Analysis

We know that the ciphertext and the key will inevitably be attacked or changed in the process of transmission, such as data missing, affected by the noise and so on. A good information security system can not only guarantee the confidentiality of information but also ensure the integrity of information decryption, so the information encryption system proposed by researchers is required to have good security and robustness.

4.1. Key Security Analysis

The proposed encryption method has great security, even if the attacker knows what kind of network structure to use and the corresponding encryption method, and tries to attack the encryption system through training, but the use of random matrix in the encryption process is unknown, based on the wrong random matrix training network leading to decryption failure. The top row of Figure 10 shows the decryption results under the correct random matrix, and the bottom row shows four images that failed to decrypt based on incorrect random matrix training.

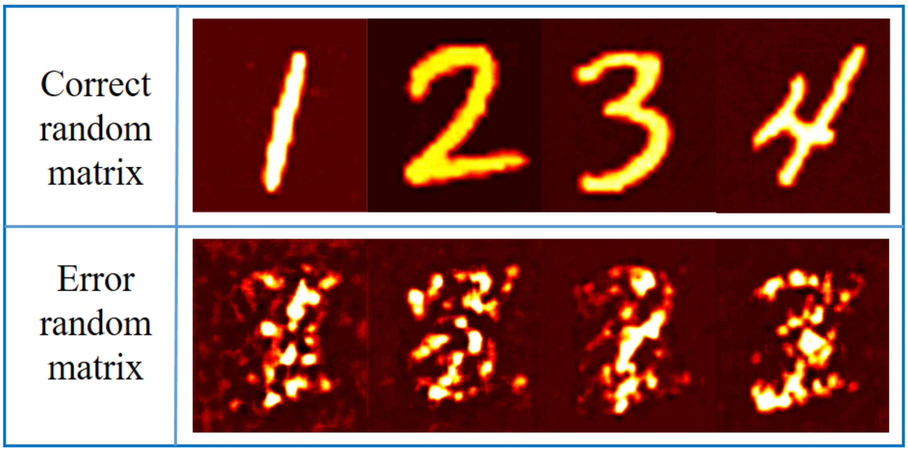


Figure 10. Decryption results under different random matrices.

It can be seen that if the wrong random matrix is used for training, no useful information can be seen from the decryption results. This fully shows that the proposed encryption algorithm has good security.

4.2. Anti-Noise Attack Analysis

It is also necessary to evaluate the robustness of the encryption algorithm when the ciphertext is attacked by noise. In order to verify that the encryption method has good anti-noise ability, speckle noise and Gaussian noise are added in the process of network training to improve the robustness. The mean values of speckle noise and Gaussian noise added in the training process are all 0, and the variance is randomly selected in (0.05, 0.06, 0.07, 0.08, 0.1). At the same time, four different types of noise attacks are added into the ciphertext: Gaussian noise, speckle noise, raylrnd noise and salt and pepper noise. CC change curve of decrypted image under noise attack is shown in Figure 11.

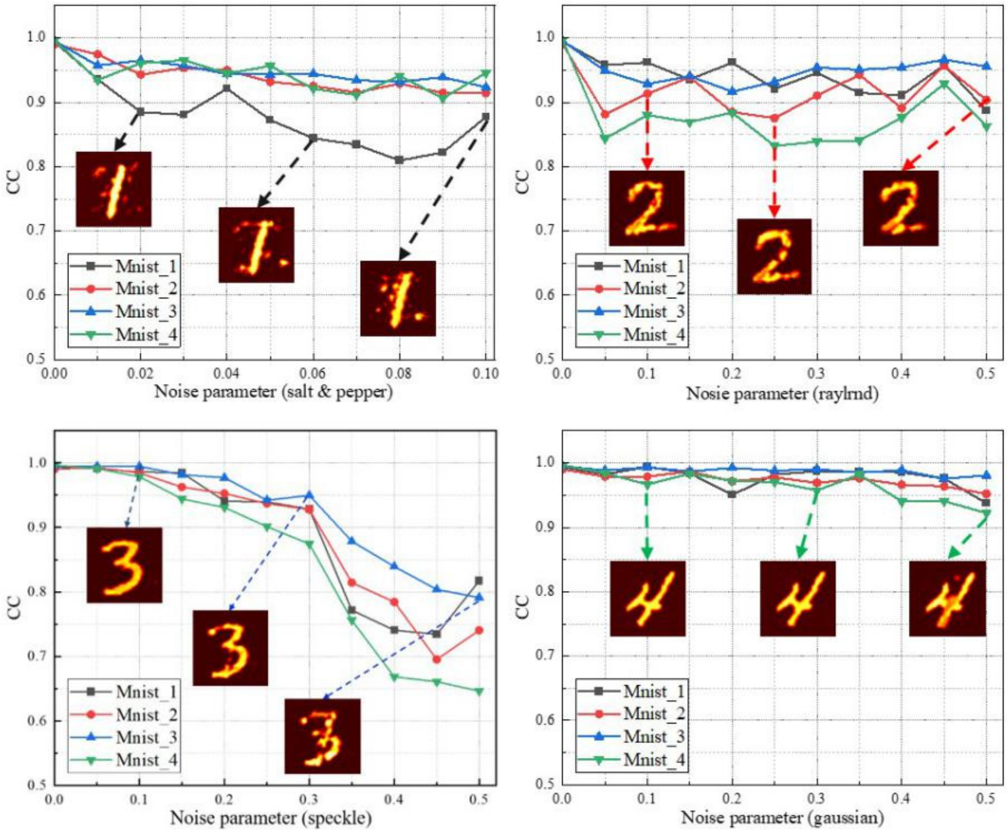


Figure 11. The CC curve of the decryption results after adding different noise attacks to the ciphertext.

For Gaussian noise and speckle noise, the abscissa represents the variance parameter. It can be seen from Figure 11 that the proposed encryption model has a very good ability to resist Gaussian noise. Even when the variance is 0.5, CC is still higher than 0.9. At the same time, when the network is attacked by other kinds of noise, although the decryption quality decreases with the increase of noise, the image can still be decrypted clearly.

4.3. Resistance to Occlusion Attacks

Next, we analyze the influence of the occlusion attack on the decryption results. Three different occlusion styles and their corresponding decrypted images are shown in Figure 12. The corresponding plaintext images are shown on the right side of Figure 12, from which the primary information of the original plaintext images can be recognized visually.

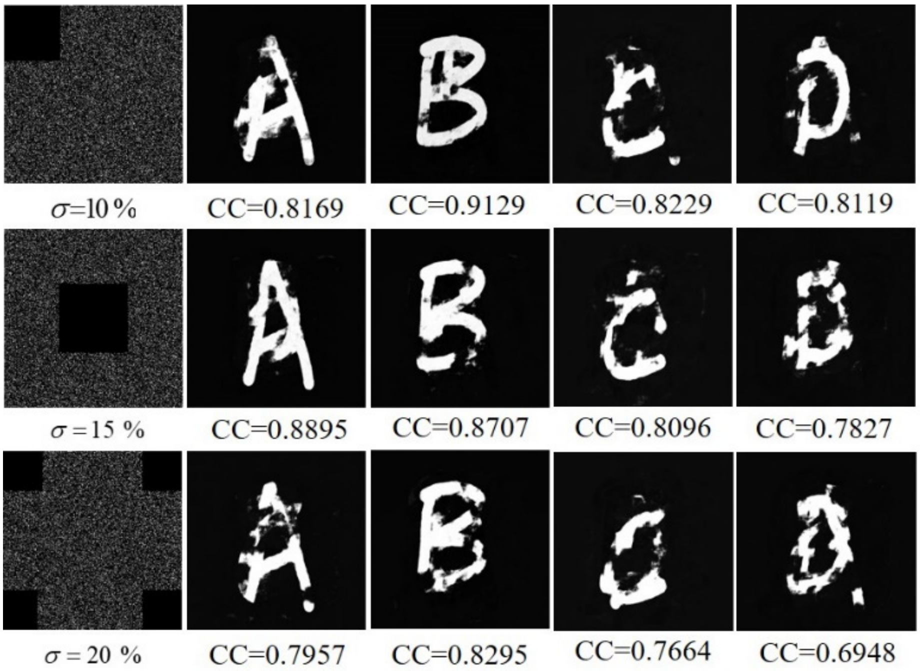


Figure 12. Decryption results after different degrees of occlusion attacks on ciphertext.

4.4. Correlation Analysis

The correlation of adjacent pixels reflects the correlation degree of pixel values at adjacent positions of the image. A secure encryption algorithm should reduce the degree of correlation between pixel values in adjacent positions of the image. The correlation of the image should include horizontal correlation, vertical correlation and diagonal correlation. The formula for calculating correlation coefficient is as follows:

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)D(y)}} \tag{9}$$

$$E(x) = \frac{1}{N} \times \sum_{i=1}^{N} x_i, D(x) = \frac{1}{N} \times \sum_{i=1}^{N} (x_i - E(x))^2 \tag{10}$$

$$\mathrm{cov}(x, y) = \frac{1}{N} \times \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \tag{11}$$

As shown Table 1, the correlation coefficients between adjacent pixels of plaintext images are all greater than 0.9, indicating a high correlation. In the ciphertext image, the average correlation coefficient of adjacent pixels in three directions is closer to 0. This means that the pixel distribution of the ciphertext image is very chaotic and there is no statistical correlation.

Table 1. Correlation coefficient between adjacent pixels of plaintext image and ciphertext image in each of three directions.

Test Image	Horizontal	Vertical	Diagonal
Img1	0.9831	0.9749	0.9779
Img2	0.9689	0.9594	0.9638
Img3	0.9337	0.9220	0.9321
Img4	0.9605	0.9487	0.9548
Ciphertext	−0.0115	−0.0063	0.0038

At the same time, in order to show the correlation between adjacent pixels of the image intuitively, one of the four plaintext images is selected and the correlation analysis diagram of three directions is drawn. The correlation analysis results are shown in Figure 13.

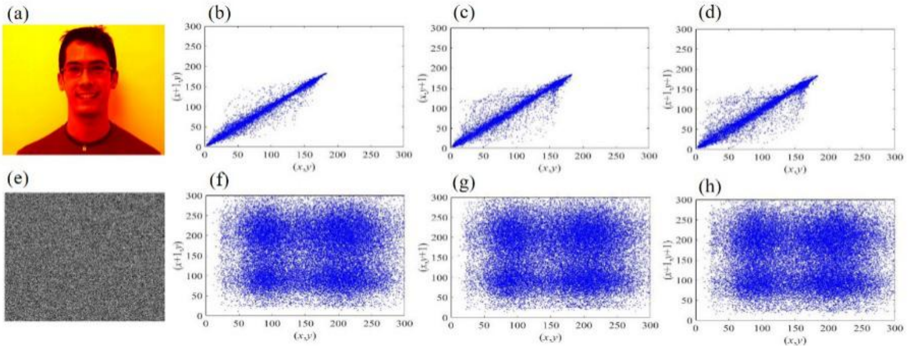


Figure 13. (**a**) One of the plaintext images. Correlation distributions of the plaintext image in horizontal (**b**), vertical (**c**) and diagonal (**d**), respectively. (**e**) Ciphertext image. Correlation distributions of the ciphertext image in horizontal (**f**), vertical (**g**) and diagonal (**h**), respectively.

The experimental results show that the adjacent pixels of the ciphertext image have low correlation in horizontal, vertical and diagonal directions, which reduces the statistical characteristics of pixel correlation, thus proving that the proposed method for image encryption can resist the statistical attack based on pixel correlation.

4.5. Histogram Analysis

In the case of image feature leakage, it is vital that the encryption scheme can resist statistical analysis. The histogram of the image shows the distribution of pixel values in the image, so the histogram is a key indicator reflecting the robustness of the image encryption scheme [38]. The histograms of four plaintext images, ciphertext images, and decrypted images are shown in Figure 14. The experimental results show that the distribution of pixel values in the ciphertext image is significantly different from that of the plaintext image. It can be seen from the histograms of the four plaintext images that the encryption model has successfully changed the distribution of pixel values, removed the statistical characteristics of pixel values, and can effectively resist attacks based on statistical analysis.

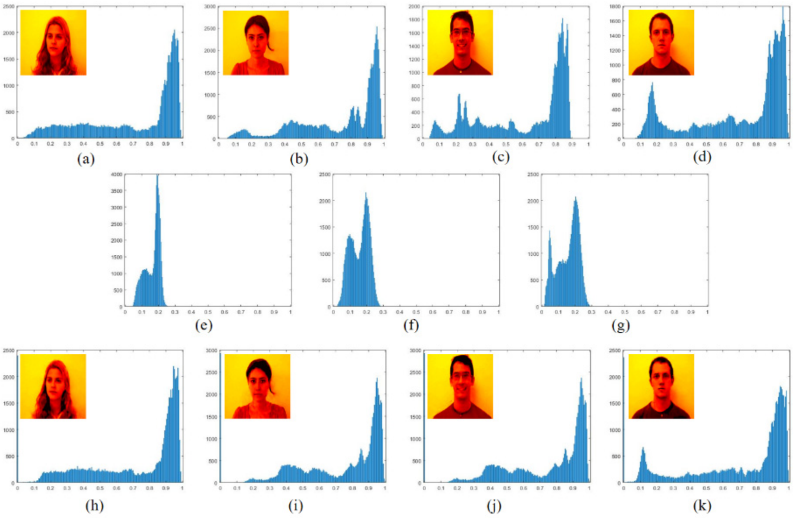


Figure 14. (**a**–**d**) Histograms of 4 plaintext images. (**e**) Superimposed light intensity histogram after encoding the first two images. (**f**) Superimposed light intensity histogram after encoding of the last two images. (**g**) Histogram of the final ciphertext image. (**h**–**k**) Histograms of the decrypted image.

4.6. Analysis of the Number of Encrypted Images

The number of encrypted images in multiple image encryption will directly affect the application of the algorithm in practice. Next, we analyze the relationship between the number of encrypted images and the quality of decrypted images. As shown in Figure 15, taking four images per group, as the number of encrypted images increases, the decryption result decreases. However, when the number of encrypted images is 64, the content of the image can still be clearly distinguished, which cannot be achieved by the traditional multi-image encryption algorithm [21–25]. Due to the limitation of image size, the sampling ratio in the frequency domain is too small to achieve better decryption when the number of encrypted images is 128.

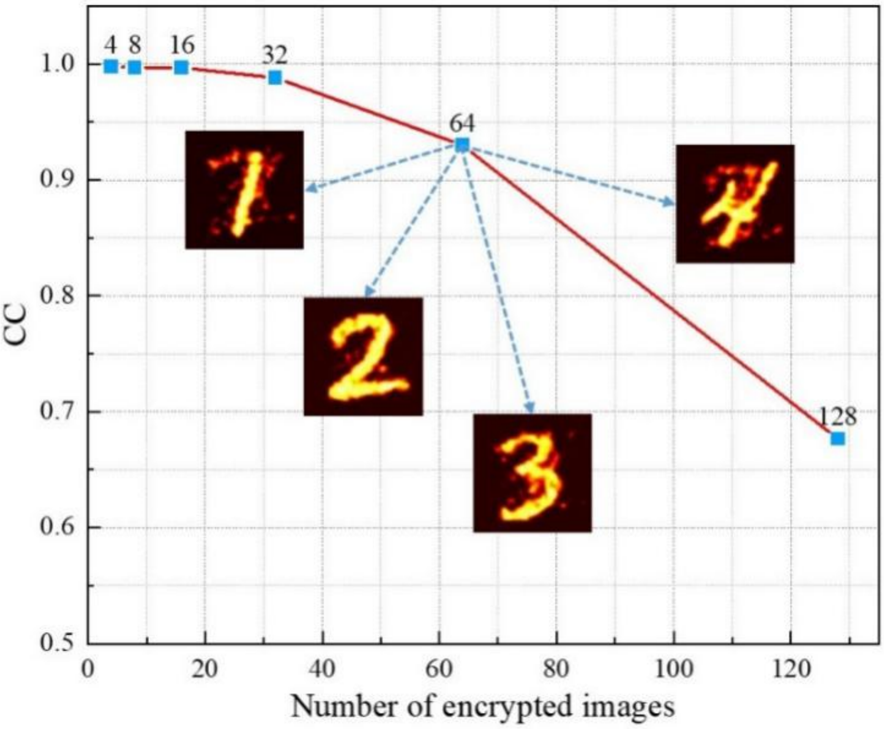


Figure 15. The relationship between the number of encrypted images and the quality of decrypted images.

5. Conclusions

In this paper, we propose a multi-image encryption method based on deep learning and sinusoidal stripe coding frequency multiplexing. The CCD camera can detect the superposed image after grouping, random matrix coding and sinusoidal stripe modulation operation. Then the deep neural network is trained to learn the correspondence between the plaintext and the ciphertext. After the training, the ciphertext image is transmitted to the trained network for decryption after scrambling recovery, Fourier transform, downsampling and inverse Fourier transform. Compared with the previous multi-image encryption methods, the proposed encryption method has more encrypted images and faster decryption speed, which makes it more widely used. Moreover, theoretical analysis, numerical simulation experiment results and robustness test all verify the feasibility and safety of the proposed method. In future work, we will further optimize the encryption method and deep neural network structure to enable it to encrypt more general grayscale images. Furthermore, the Bayer matrix can be used to preprocess color images into grayscale images, which is expected to restore the original color of the decrypted image after the introduction of De-Mosaic algorithm, thereby realizing color image encryption.

Author Contributions: Conceptualization, Q.L. and H.W.; methodology, X.M.; software, Q.L.; validation, H.W., X.M. and Y.Y.; formal analysis, X.M.; investigation, H.W.; resources, X.M.; data curation, Q.L.; writing—original draft preparation, Q.L.; writing—review and editing, X.M.; visualization, Q.L.; supervision, H.W.; project administration, Y.Y.; funding acquisition, X.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Natural Science Foundation of China (NSFC) (Grant Nos. 61775121, 11574311), the Key R&D Program of Shandong Province (Grant No. 2018GGX101002) and the Natural Science Foundation of Shandong Province (Grant No. ZR2019QF006).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Publicly available datasets were analyzed in this study. This data can be found here: https://github.com/liqi-sdu/Test (accessed on 14 September 2021).

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

References

1. Alfalou, A.; Brosseau, C. Optical image compression and encryption methods. *Adv. Opt. Photon.* **2009**, *1*, 589–636. [CrossRef]
2. Liu, S.; Guo, C.; Sheridan, J.T. A review of optical image encryption techniques. *Opt. Las. Technol.* **2014**, *57*, 327–342. [CrossRef]
3. Refregier, P.; Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **1995**, *20*, 767–769. [CrossRef] [PubMed]
4. Ben Farah, M.A.; Guesmi, R.; Kachouri, A.; Samet, M. A novel chaos based optical image encryption using fractional fourier transform and DNA sequence operation. *Opt. Las. Tech.* **2020**, *121*, 105777. [CrossRef]
5. Kong, D.; Shen, X. Multiple-image encryption based on optical wavelet transform and multichannel fractional Fourier transform. *Opt. Las. Technol.* **2014**, *57*, 343–349. [CrossRef]
6. Wang, M.; Pousset, Y.; Carré, P.; Perrine, C.; Zhou, N.R.; Wu, J. Optical image encryption scheme based on apertured fractional Mellin transform. *Opt. Las. Technol.* **2020**, *124*, 106001. [CrossRef]
7. Luan, G.; Li, A.; Chen, Z.; Huang, C. Asymmetric Optical Image Encryption with Silhouette Removal Using Interference and Equal Modulus Decomposition. *IEEE Photon. J.* **2020**, *12*, 1–8. [CrossRef]
8. Clemente, P.; Durán, V.; Torres-Company, V.; Tajahuerce, E.; Lancis, J. Optical encryption based on computational ghost imaging. *Opt. Lett.* **2009**, *35*, 2391–2393. [CrossRef]
9. Jiao, S.; Feng, J.; Gao, Y.; Lei, T.; Yuan, X. Visual cryptography in single-pixel imaging. *Opt. Express.* **2020**, *28*, 7301–7313. [CrossRef]
10. Chen, W.; Javidi, B.; Chen, X. Advances in optical security systems. *Adv. Opt. Photon.* **2014**, *6*, 120–155. [CrossRef]
11. Xie, Y.; Li, J.; Kong, Z.; Zhang, Y.; Liao, X.; Liu, Y. Exploiting Optics Chaos for Image Encryption-Then-Transmission. *J. Lightwave Technol.* **2016**, *34*, 5101–5109. [CrossRef]
12. Su, Y.; Tang, C.; Li, B.; Chen, X.; Xu, W.; Cai, Y. Single-lens Fourier-transform-based optical color image encryption using dual two-dimensional chaotic maps and the Fresnel transform. *Appl. Opt.* **2017**, *56*, 498–505. [CrossRef] [PubMed]
13. Deng, X.; Zhao, D. Single-channel color image encryption using a modified Gerchberg–Saxton algorithm and mutual encoding in the Fresnel domain. *Appl. Opt.* **2011**, *50*, 6019–6025. [CrossRef]
14. Zhang, L.; Pan, Z.; Zhou, G. Study on the key technology of optical encryption based on adaptive compressive ghost imaging for a large-sized object. *J. Opt. Soc. Korea* **2017**, *84*, 471–476. [CrossRef]
15. Qin, Y.; Wang, Z.; Gong, Q. Diffractive-imaging-based optical image encryption with simplified decryption from single diffraction pattern. *Appl. Opt.* **2014**, *53*, 4094–4099. [CrossRef] [PubMed]
16. Situ, G.; Zhang, J. Multiple-image encryption by wavelength multiplexing. *Opt. Lett.* **2005**, *30*, 1306–1309. [CrossRef]
17. Situ, G.; Zhang, J. Position multiplexing for multiple-image encryption. *J. Opt. A* **2006**, *8*, 391–397. [CrossRef]
18. Wang, Q.; Guo, Q.; Lei, L.; Zhou, J. Multiple-image encryption based on interference principle and phase only mask multiplexing in Fresnel transform domain. *Appl. Opt.* **2013**, *52*, 6849–6857. [CrossRef]
19. Barrera, J.F.; Henao, R.; Tebaldi, M.; Torroba, R.; Bolognini, N. Multiplexing encryption–decryption via lateral shifting of a random phase mask. *Opt. Commun.* **2006**, *259*, 532–536. [CrossRef]
20. Alfalou, A.; Brosseau, C. Exploiting root-mean-square time-frequency structure for multiple-image optical compression and encryption. *Opt. Lett.* **2010**, *35*, 1914–1916. [CrossRef]
21. Lee, I.H.; Cho, M. Double random phase encryption using orthogonal encoding for multipleimage transmission. *J. Opt. Soc. Korea* **2014**, *18*, 201–206. [CrossRef]
22. Li, X.; Meng, X.; Yang, X.; Yin, Y.; Wang, Y.; Peng, X.; He, W.; Dong, G.; Chen, H. Multiple-image encryption based on compressive ghost imaging and coordinate sampling. *IEEE Photon. J.* **2017**, *8*, 1–11. [CrossRef]
23. Wu, J.; Xie, Z.; Liu, Z.; Liu, W.; Zhang, Y.; Liu, S. Multiple-image encryption based on computational ghost imaging. *Opt. Commun.* **2016**, *359*, 38–43. [CrossRef]

24. Zhang, L.; Yuan, X.; Zhang, D.; Chen, J. Research on Multiple-image Encryption Scheme Based on Fourier Transform and Ghost Imaging Algorithm. *Curr. Opt. Photon.* **2018**, *2*, 315–323.
25. Yang, X.; Wu, H.; Yin, Y.; Meng, X.; Peng, X. Multiple-image encryption base on compressed coded aperture imaging. *Opt. Lasers Eng.* **2020**, *127*, 105976. [CrossRef]
26. Bian, L.; Suo, J.; Hu, X.; Chen, F.; Dai, Q. Efficient single pixel imaging in Fourier space. *J. Opt.* **2016**, *18*, 085704. [CrossRef]
27. Chakrabarti, A.; Zickler, T. Statistics of real-world hyperspectral images. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Colorado, CO, USA, 20–25 June 2011; pp. 193–200.
28. Deng, C.; Zhang, Y.; Mao, Y.; Fan, J.; Suo, J.; Zhang, Z.; Dai, Q. Sinusoidal Sampling Enhanced Compressive Camera for High Speed Imaging. *IEEE Trans. Pattern Anal.* **2019**, *43*, 1380–1393. [CrossRef] [PubMed]
29. Cai, B.; Xu, X.; Jia, K.; Qing, C.; Tao, D. DehazeNet: An End-to-End System for Single Image Haze Removal. *IEEE Trans. Image Process* **2016**, *25*, 5187–5198. [CrossRef]
30. Long, J.; Shelhamer, E.; Darrell, T. Fully Convolutional Networks for Semantic Segmentation. *IEEE Trans. Patter. Recog. Mach. Intellig.* **2017**, *39*, 640–651.
31. Kulkarni, K.; Lohit, S.; Turaga, P.; Kerviche, R.; Ashok, A. ReconNet: Non-Iterative Reconstruction of Images from Compressively Sensed Measurements. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Las Vegas, NV, USA, 27–30 June 2016; pp. 449–458.
32. Lyu, M.; Wang, W.; Wang, H.; Wang, H.; Li, G.; Chen, N.; Situ, G. Deep-learning-based ghost imaging. *Sci. Rep.* **2017**, *7*, 17865. [CrossRef]
33. Sinha, A.; Lee, J.; Li, S.; Barbastathis, G. Lensless computational imaging through deep learning. *Optica* **2017**, *4*, 1117–1125. [CrossRef]
34. Hai, H.; Pan, S.; Lia, M.; Lu, D.; He, W.; Peng, X. Cryptanalysis of random-phase-encoding based optical cryptosystem via deep learning. *Opt. Express* **2019**, *27*, 21204–21213. [CrossRef] [PubMed]
35. Ronneberger, O.; Fischer, P.; Brox, T. U-net: Convolutional networks for biomedical image segmentation. In Proceedings of the International Conference on Medical Image Computing and Computer-Assisted Intervention, Munich, Germany, 5–9 October 2015; pp. 234–241.
36. Kingma, D.P.; Ba, J. Adam: A Method for Stochastic Optimization. In Proceedings of the International Conference on Learning Representations (ICLR), San Diego, CA, USA, 7–9 May 2015.
37. FEI Face Database, Image Processing Laboratory, Department of Electrical Engineering, Centro Universitario da FEI, São Bernardo do Campo, São Paulo, Brazil. Available online: https://fei.edu.br/~{}cet/facedatabase.html (accessed on 18 August 2021).
38. Msood, F.; Driss, M.; Boulila, W.; Ahmad, J.; Rehman, S.U.; Jan, S.U.; Qayyum, A.; Buchanan, W.J. A Lightweight Chaos-Based Medical Image Encryption Scheme Using Random Shuffling and XOR Operations. *Wirel. Pers. Commun.* **2021**. [CrossRef]