






Computer Generated Hologram-Based Image Cryptosystem with Multiple Chaotic Systems

Chuying Yu  and Jianzhong Li  

Hanshan Normal University, Chaozhou 521041, China
henry_stu@163.com

Abstract. Based on computer generated hologram (CGH) and multiple chaotic systems, a novel image encryption scheme is presented, in which shuffling the positions and changing the values of image pixels are combined to confuse the relationship between the ciphertext and the original image. In the encryption process, the complex distribution is permuted by use of the designed scrambling algorithm which is based on Chen's chaotic system and logistic maps firstly. Subsequently, the Burch's coding method is used to fabricate the CGH as the encrypted image. Finally, the pixel values of the encrypted CGH are changed by sine map to withstand statistical analysis attacks. Simulation results demonstrate that the proposed method has high security level and certain robustness against statistical analysis attacks, data loss and noise disturbance.

Keywords: Computer generated hologram · Chaos · Security and encryption

1 Introduction

With the rapid development of computational technology and modern optical technology, digital computer is widely used to simulate, calculate and deal with all kinds of optical processes [1, 2]. In recent years, the optical information processing technique has been applied in information security [1–8] because of its excellent characteristics, such as high-speed parallel processing of information with multiple degrees of freedom. Since the double random phase encryption (DRPE) technique has been developed [3], a number of improved optical image encryption methods have been proposed [1, 2, 4]. However, it is difficult to transmit the encrypted complex data, which is obtained by the traditional optical encryption techniques, through the network. Computer generated hologram (CGH), which is often employed to implement optical encryption schemes [2, 5, 6], is an effective method of the digitization of encrypted data. In comparison with conventional optical holography, CGHs have the advantage of being easily and effectively generated by computer.

In this paper, a novel image encryption scheme with off-axis Fourier transform CGH and multiple chaotic maps is proposed. In this method, shuffling the positions and changing the pixel values are performed simultaneously. In the encryption process, the complex distribution is permuted by use of the designed scrambling algorithm which is based on Chen's chaotic system and logistic maps first. Then the Burch's coding method is used to fabricate the CGH as the ciphertext. To resist statistical analysis

attacks, the pixel values of the obtained CGH are changed by sine map. The simulations demonstrate the validity and performance of the proposed method.

2 Related Background

2.1 Fourier Transform Computer Generated Hologram Based on Burch's Method

Let $O(x, y) = A(x, y)\exp[j\varphi(x, y)]$ and $R(x, y) = A_r\exp[j2\pi\rho\varphi_r(x, y)]$ be the object wave and the parallel reference wave, respectively. And let $|A(x, y)|_{\max} = 1$ and $A_r = 1$, then the transmittance of the off-axis Fourier transform CGH based on Burch's coding method can be expressed as follows [8]:

$$\begin{aligned} h(x, y) &= |O(x, y) + R(x, y)|^2 \\ &= |A(x, y)|^2 + A_r^2 + 2A_r A(x, y) \cos[2\pi\rho\varphi_r(x, y) - \varphi(x, y)] \\ &= 0.5\{1 + A(x, y) \cos[2\pi\rho\varphi_r(x, y) - \varphi(x, y)]\}. \end{aligned} \quad (1)$$

where ρ is the carrier frequency. With the conjugate reference wave, the hologram can be reconstructed by inverse discrete Fourier transform. For further details the reader is referred to [8].

2.2 Chen's Chaotic System

The three-dimensional Chen's chaotic system is described as following [9]

$$\begin{aligned} \dot{x} &= a(y - x), \\ \dot{y} &= (c - a)x - xz + cy, \\ \dot{z} &= xy - bz, \end{aligned} \quad (2)$$

where a , b and c are parameters. The system has chaotic behavior when $a = 35$, $b = 3$, $c \in [20, 28.4]$.

2.3 Logistic Map

The logistic map, which is a 1D nonlinear chaos function, is expressed as [7]

$$x_{n+1} = \mu x_n(1 - x_n), \quad (3)$$

where μ is the logistic map parameter, and $\mu \in [0, 4]$, $x_n \in (0, 1)$. When $3.5699456 < \mu \leq 4$, the dynamical system is in chaotic state.

2.4 Sine Map

The sine map is also a 1D chaos function and defined as [10].

$$x_{n+1} = [\gamma \sin(\pi x_n)]/4, \quad (4)$$

where γ is sine map parameter. when $0 < \gamma \leq 4$, sine mapping works in a chaotic state.

3 The Chaos-Based Image Scrambling Method

In the proposed scrambling technique, the chaotic sequences generated by Chen's system and logistic map are used to permute the plaintext image. Suppose the size of the input data $I(x, y)$ is $M \times N$, the scrambling method is described as follows

- (1) Initialize $XC(1)$, $YC(1)$ and $ZC(1)$ randomly and choose an arbitrary natural number L first, then iteratively generate the chaotic sequences $XC(i)$, $YC(i)$ and $ZC(i)$ whose lengths are all L by using Eq. (2). Here, $i = 1, 2, \dots, L$.
- (2) Generate three integers $p1$, $p2$ and $p3$ which are between 1 and L randomly first. In other words, $1 \leq p1 \leq L$, $1 \leq p2 \leq L$ and $1 \leq p3 \leq L$. Then calculate the initial value $XL(1)$ of logistic map according to the following Eqs. (5) and (6)

$$X(1) = [XC(p1) + YC(p2) + ZC(p3)]/3, \quad (5)$$

where $XC(p1)$, $YC(p2)$ and $ZC(p3)$ are the $p1^{\text{th}}$ element in XC , the $p2^{\text{th}}$ element in YC and the $p3^{\text{th}}$ element in ZC , respectively.

$$XL(1) = 10^5 \times \text{abs}(X(1)) - \text{fix}(10^5 \times \text{abs}(X(1))), \quad (6)$$

where $\text{fix}(x)$ is the operation that rounds the elements of x toward zero.

- (3) Using $XL(1)$ and Eq. (3), generate the chaotic sequences $XL(i)$ whose length is $MN + T$ iteratively. Here, $i = 1, 2, \dots, MN+T$, T is an arbitrary natural number.
- (4) Truncate NM elements of $XL(i)$ from the $p4^{\text{th}}$ element to obtain a chaotic sequence $S = \{XL(i), i = p4, p4 + 1, \dots, p4 + MN - 1\}$. Here, $p4$ is a random integer which is between 1 and T .
- (5) Sort the sequences S in ascending order to obtain a new sequence SN and its corresponding permutation indices ISN . There are MN elements in ISN . The relations between S and SN is $SN = S(ISN)$. For example, the m^{th} element in SN corresponds to the $ISN(m)^{\text{th}}$ element in S .
- (6) With the zigzag algorithm [11], map $I(x, y)$ into an 1D array $I1$. The length of $I1$ is MN .
- (7) Then the permutation indices ISN is employed to permute $I1$ and the scrambled vector $I2$ can be achieved as follows

$$I2 = I1(ISN). \quad (7)$$

- (8) Finally, apply the inverse zigzag scan process [11] to $I2$, the permuted image SI can be obtained.

The inverse image scrambling process is similar to the image scrambling process. In inverse scrambling process, obtain the permutation indices ISN as described in steps (1)–(5) with the same initial values and control parameters of the chaotic functions first. Then the scrambled image SI is mapped into an 1D vector $SI1$ by use of the zigzag algorithm. Subsequently, permute $SI1$ back to their original position according to the following equation

$$SI2(ISN) = SI1. \quad (8)$$

After applying the inverse zigzag algorithm to $SI2$, the decrypted image can be retrieved.

4 The Encrypted Computer Generated Hologram

The presented algorithm is divided into three parts. First the complex distribution is permuted by the proposed scrambling scheme. Then the CGH is generated by employed Burch's method. Lastly, sine map is applied to change the pixel values of the shuffled-CGH. Supposing $f(x_0, y_0)$ denotes the input image with size $M \times N$, the proposed method is described as follows.

- (1) To reduce the dynamic range of the hologram, $f(x_0, y_0)$ should be multiplied by a random phase, which can be expressed as

$$f_1(x_0, y_0) = f(x_0, y_0)\exp[j2\pi\phi(x_0, y_0)], \quad (9)$$

where $\phi(x_0, y_0)$ is a random function distributed uniformly in the interval $[0, 1]$.

- (2) By use of the Fourier transform, the object wave $O(x, y)$ can be obtained.

$$O(x, y) = DFT[f_1(x_0, y_0)] = A(x, y)\exp[j\varphi(x, y)], \quad (10)$$

where $DFT()$ represents discrete Fourier transform operator.

- (3) Permute the object wave $O(x, y)$ and the reference wave $R(x, y)$ to obtain $O_p(x, y)$ and $R_p(x, y)$ by the proposed chaos-based scrambling method shown in sub-Sect. 2.3 with the parameters $XC(1)$, $YC(1)$, $ZC(1)$, c , μ , $p1$, $p2$, $p3$, and $p4$.
- (4) With $O_p(x, y)$ and $R_p(x, y)$, the shuffled hologram transmittance $h(x, y)$ can be achieved by using Eq. (1). When $h(x, y)$ is 8-bit (256 levels) quantized, the gray-level computer generated hologram HG can be obtained.
- (5) To resist statistical analysis attacks, sine map is adopted to change the pixel values of the shuffled hologram $h(x, y)$. Initialize $XS(1)$ randomly and choose an arbitrary natural number v first, then iteratively generate the chaotic sequences $XS(i)$ whose length is $MN+V$ by use of Eq. (4). Here, $i = 1, 2, \dots, MN+V$. Then truncate NM elements of $XS(i)$ from the $s1^{\text{th}}$ element to get a chaotic sequence $XS1 = \{X(i), i = s1, s1 + 1, \dots, s1 + MN - 1\}$.
- (6) Compute the chaotic sequence $XS1$ using the following equation

$$XS2 = \text{mod}(\text{round}((\text{abs}(XS1) - \text{floor}(\text{abs}(XS1)))10^{14}, 256), \quad (11)$$

where $\text{round}(x)$ rounds the elements of x to the nearest integers, $\text{floor}(x)$ rounds the element of x to the nearest integers less than or equal to x , $\text{abs}(x)$ returns the absolute value of x , and $\text{mod}(x, y)$ returns the remainder after division, respectively. Then apply the inverse zigzag scan process to the 1D vector $XS2$ to obtain the two-dimensional integer matrix $XS3$.

- (7) Finally, change the pixel values of the permuted CGH to achieve the encrypted CGH according to the following Eq. (12)

$$HGP = HG \oplus XS3, \quad (12)$$

where the symbol \oplus represents the exclusive OR operation bit-by-bit.

The parameters $XC(1)$, $YC(1)$, $ZC(1)$, $XS(1)$, c , μ , γ , $p1$, $p2$, $p3$, $p4$ and $s1$ are used as private keys and form a large key space in the encryption and decryption processes. The decryption process is described as follows:

- (1) Use the same parameters $XS(1)$, γ and $s1$ to obtain $XS3$ as described in steps (5)–(6) first.
 (2) Perform the exclusive OR operation between HGP and $XS3$ to obtain the permuted hologram HG using Eq. (13)

$$HG = HGP \oplus XS3, \quad (13)$$

- (3) With the parameters $XC(1)$, $YC(1)$, $ZC(1)$, c , μ , $p1$, $p2$, $p3$ and $p4$, HG is permuted by the proposed inverse scrambling process mentioned in Subsect. 2.3 to obtain $HG1$.
 (4) With the conjugate reference wave, the reconstruction RG of the CGH can be obtained by using inverse DFT. Thus, the decrypted image is achieved.

5 Simulation Results

The presented method is carried out to verify the feasibility of the cryptosystem with the image ‘‘Lena’’ shown in Fig. 1(a), which size is 256×256 . The experiments were performed using MATLAB. Since the CGH is under-sampled, the input image is expanded to 560×560 pixels to deal with the under-sampling problem and obtain spatial separation of the reconstructed terms, as shown in Fig. 1(b). The parameters of the cryptosystem are $XC(1) = -10.058$, $YC(1) = 0.368$, $ZC(1) = 37.368$, $c = 28$, $\mu = 3.8$, $\gamma = 3.92$, $L = 10^5$, $T = 10^5$, $V = 10^5$, $p1 = 35762$, $p2 = 29637$, $p3 = 88365$, $p4 = 15759$ and $s1 = 51123$, respectively. To measure the quality of the decrypted image, the peak signal-to-noise ratio (PSNR) [12] was used to calculate the similarity between the original plaintext image and the decrypted image. If the PSNR value is larger than 40 dB, the decrypted image almost has no difference from the original one in visual quality.

5.1 Performance of the Encryption System

Using the proposed encryption scheme, the plaintext image is encrypted, and the ciphertext shown in Fig. 1(c) is acquired. To evaluate the performance of the proposed scheme, the ciphertext is decrypted using both correct and incorrect keys. Figures 1(d)–(e) exhibit the well reconstructed image and decrypted image with the correct keys respectively. As shown in Fig. 1(e), the PSNR of the decrypted image is above over 45 dB when all the keys are correct.

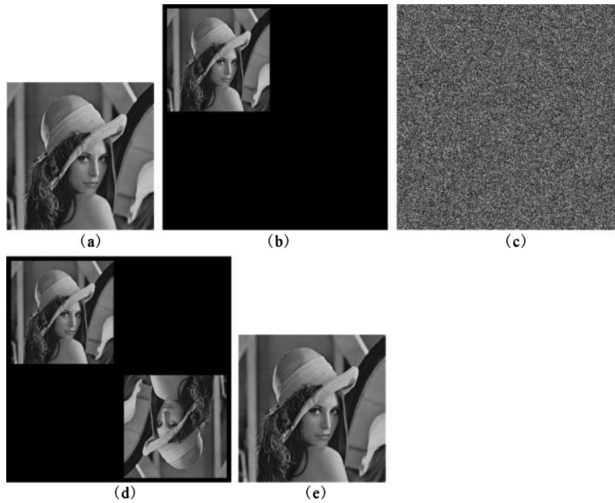


Fig. 1. Results of the proposed image encryption: (a) the plaintext image ‘Lena’ (256 × 256); (b) the expansion image (560 × 560); (c) the ciphertext (560 × 560); (d) the reconstruction of (c) (560 × 560); (e) the decrypted image with correct keys (256 × 256) (PSNR = 45.05).

Now we explore the sensitivity of recovered image to slight change of the cipher keys. The decrypted images with the wrong decryption keys $XC(1) = XC(1) + 10^{-15}$, $YC(1) = YC(1) + 10^{-14}$, $ZC(1) = ZC(1) + 10^{-14}$, $XS(1) = XS(1) + 10^{-14}$, $c = c + 10^{-14}$, $\mu = \mu + 10^{-14}$, $\gamma = \gamma + 10^{-15}$, $p1 = p1 + 1$, $p2 = p2 - 1$, $p3 = p3 + 1$, $p4 = p4 + 1$ and $S1 = S1 + 1$ are illustrated in Fig. 2(a)–(l), respectively. It can be observed from Fig. 2(a)–(g) that any valid information cannot be obtained from the decrypted images when the absolute values of the deviations of $XC(1)$ and γ are up to 10^{-15} and those of $YC(1)$, $ZC(1)$, $XS(1)$, c and μ are up to 10^{-14} , respectively. Additionally, as can be seen from Fig. 2(h)–(l), all the decrypted images are unrecognizable if the parameters $p1$, $p2$, $p3$, $p4$ and $S1$ are less 1 or more 1 than the correct value. All the PSNR values of the decrypted images in Fig. 2 are less than 10 dB. Please note that the other keys remain correct while a key is changed in the mentioned above experiments. Because the key space of the cryptosystem consists of the parameters $XC(1)$, $YC(1)$, $ZC(1)$, $XS(1)$, c , μ , γ , $p1$, $p2$, $p3$, $p4$ and $s1$, the entire key space of the encryption scheme is $10^{15} \times 10^{14} \times 10^{14} \times 10^{14} \times 10^{14} \times 10^{14} \times 10^{15} \times 10^5 \times 10^5 \times 10^5 \times 10^5 \times 10^5 = 10^{125} \approx 2^{415}$.

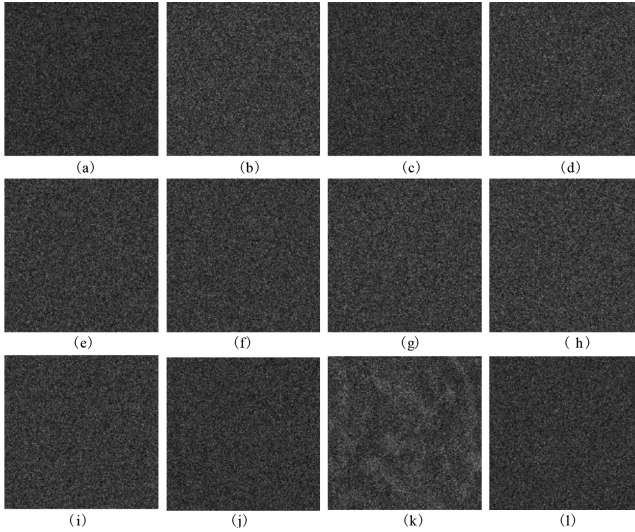


Fig. 2. The decrypted images with incorrect keys: (a) the decrypted images with $XC(1) = XC(1) + 10^{-15}$ (PSNR = 8.57); (b) the decrypted images with $YC(1) = YC(1) + 10^{-14}$ (PSNR = 9.15); (c) the decrypted images with $ZC(1) = ZC(1) + 10^{-14}$ (PSNR = 8.73); (d) the decrypted images with $XS(1) = XS(1) + 10^{-14}$ (PSNR = 8.82); (e) the decrypted images with $c = c + 10^{-14}$ (PSNR = 8.98); (f) the decrypted images with $\mu = \mu + 10^{-14}$ (PSNR = 9.01); (g) the decrypted images with $\gamma = \gamma + 10^{-15}$ (PSNR = 9.13); (h) the decrypted images with $p1 = p1 + 1$ (PSNR = 9.18); (i) the decrypted images with $p2 = p2 - 1$ (PSNR = 8.97); (j) the decrypted images with $p3 = p3 + 1$ (PSNR = 8.72); (k) the decrypted images with $p4 = p4 + 1$ (PSNR = 9.46); (l) the decrypted images with $S1 = S1 + 1$ (PSNR = 8.75).

5.2 Robustness of the Proposed Scheme Against Attacks

Except for having a large key space, a desirable encryption technique should also well withstand various attacks such as statistical attack and occlusion attack.

Several types of statistical analysis including histogram analysis, entropy analysis, and correlation analysis are performed in the experiments. Figure 3(a) and (b) show histograms of the original image and the encrypted image, respectively. As shown in Fig. 3(b), the experiment result is nearly uniform. So, the histograms of ciphertext cannot provide any useful information for the attacker to carry out this kind of statistical analysis attack.

The entropy is the most outstanding feature of the randomness [13]. The information entropy of an image f can be computed according to the following Eq. (14).

$$H(f) = \sum_{i=1}^{255} P(f_i) \log_2 \frac{1}{P(f_i)}, \tag{14}$$

where $P(f_i)$ represents the probability of symbol f_i . For a purely random source emitting 2^N symbols, the entropy is $H(f) = N$. For example, the theoretical entropy of the image with 256 gray levels is 8.

Using Eq. (14), the entropy of the original image and ciphered image can be calculated. They are 7.4363 and 7.9994, respectively. The entropy of the encrypted image is very close to the theoretical value of 8. It means that the proposed encryption method is secure upon entropy attack.

Because each pixel is highly correlated with its adjacent pixels either in horizontal, vertical or diagonal direction in an image, the cryptanalysis can be carried out by employing this characteristic. The 3000 pairs of adjacent pixels in vertical, horizontal and diagonal directions are randomly selected from the plain images and the ciphertext to probe the correlations of the adjacent pixels by calculating their corresponding correlation coefficient r_{xy} [13]. The bigger absolute value of r_{xy} is, the stronger correlation is. The correlation coefficients of the plain image and the ciphertext are shown in Table 1 and the distributions are shown in Figs. 4 and 5. From Table 1 and Fig. 5, it is evident that a random relation exists in the ciphered image. Not only correlation coefficient but also the figures illustrate that neighboring pixels of the ciphered image have no correlation. The encryption method improves the image's security.

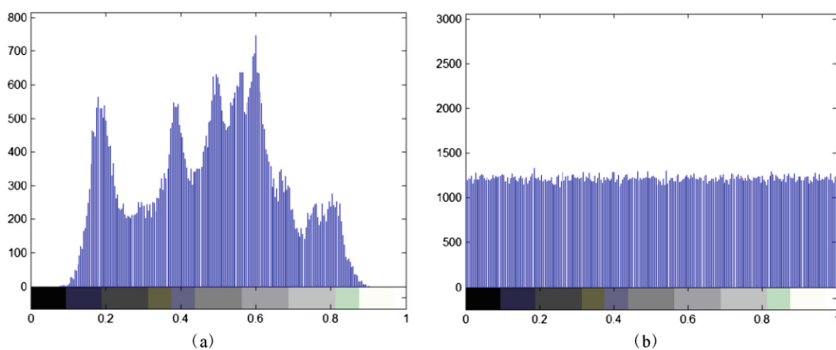


Fig. 3. (a) Histogram of plain image ‘Lena’, (b) histogram of ciphered image.

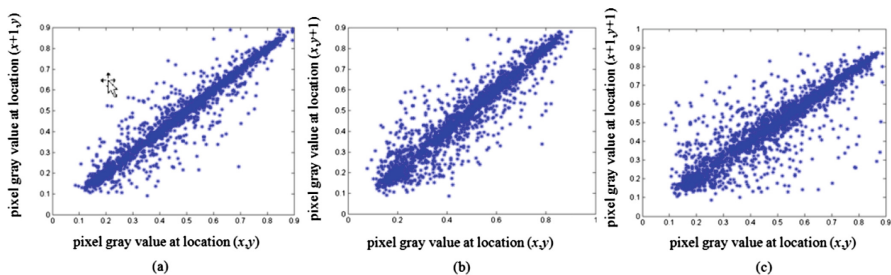


Fig. 4. Correlation between two adjacent pixels in ‘Lena’: (a) horizontal correlation; (b) vertical correlation; (c) diagonal correlation.

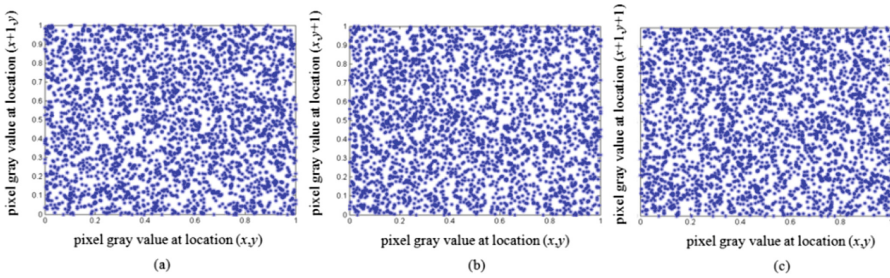


Fig. 5. Correlation between two adjacent pixels in the encrypted image: (a) horizontal correlation; (b) vertical correlation; (c) diagonal correlation.

Table 1. Results of correlation coefficients.

Direction	Lena	Encrypted image
Horizontal	0.9680	-0.0079
Vertical	0.9424	0.0024
Diagonal	0.9175	0.0272

In the noise attack experiments, the ciphertext is added with the Gaussian random noise with mean value 0 and standard deviation 15. Figure 6(a) is the encrypted image distorted by Gaussian noise with mean value 0 and standard deviation 15. The reconstruction is displayed in Fig. 6(b). The recovered image which PSNR is 11.03 dB is shown in Fig. 6(c). Though the decrypted image depicted in Fig. 6(c) is interfered seriously and the corresponding PSNR is small, it can still be recognized among the noise.

During data transmission, information loss also often occurs. The robustness of the proposed method against occlusion attack which is regarded as data loss is tested. Figure 7(a) shows the ciphertext occluded by 10%. Figures 7(b)–(c) exhibit the corresponding reconstructed image and decrypted image obtained by use of all correct keys. Though the PSNR of the decrypted image is less than 13 dB, it can still be distinguished.

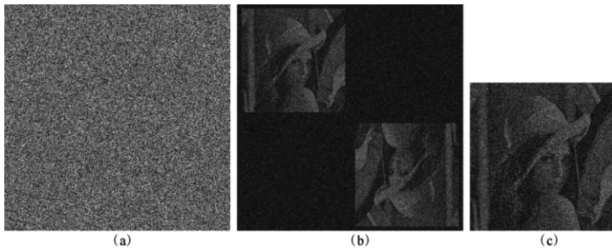


Fig. 6. Robustness against noise. (a) the encrypted image undergone noise attack; (b) the reconstruction of (a) with all correct keys; (c) the decrypted image (PSNR = 11.03).

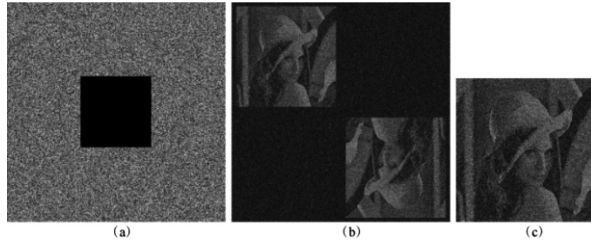


Fig. 7. Robustness against occlusion. (a) the encrypted image with 10% occlusion; (b) the reconstruction of (a) with all correct keys; (c) the decrypted “Lena” (PSNR = 12.52)

6 Conclusion

In this paper, based on CGH technique and chaotic theory, a new image encryption method is proposed. Permuting the positions and changing the values of image pixels are combined simultaneously to enhance the security of our scheme. The proposed approach has the following merits: (1) the method is highly sensitive to the secret keys and it has a large enough key space to resist all kinds of brute-force attacks; (2) the encrypted image has a good statistical property; (3) the encrypted holograms which are generated by computer are real-value data, so they are convenient for storage and transmission.

Acknowledgment. This work is partly supported by the Natural Science Foundation of Guangdong Province (No.2018A0303070009, No. 2014A030310038), the Educational and Commission of Guangdong Province (No. 2015KTSCX089).

References

1. Liu, Z.J., Xu, L., Lin, C., et al.: Image encryption scheme by using iterative random phase encoding in gyrator transform domains. *Opt. Lasers Eng.* **49**(4), 542–546 (2011)
2. Xi, S., Wang, X., Song, L., et al.: Experimental study on optical image encryption with asymmetric double random phase and computer-generated hologram. *Opt. Express* **25**, 8212–8222 (2017)
3. Refregier, P., Javidi, B.: Optical image encryption based on input plane and fourier plane random encoding. *Opt. Lett.* **20**, 767–769 (1995)
4. Nischal, N.K., Joseph, J., Singh, K.: Securing information using fractional fourier transform in digital holography. *Opt. Commun.* **235**, 253–259 (2004)
5. Pan, W., Wun, W.W., Zhang, X.L.: Encryption algorithm of virtual optical based on computer-generated hologram and double random phase. *Chin. J. Lasers* **36**(s2), 312–317 (2009)
6. Wang, Y.Y., Wang, Y.R., Wang, Y., et al.: Optical image encryption based on binary fourier transform computer-generated hologram and pixel scrambling technology. *Opt. Lasers Eng.* **45**(7), 761–765 (2007)
7. Singh, N., Sinha, A.: Optical image encryption using Hartley transform and logistic map. *Opt. Commun.* **282**, 1104–1109 (2009)

8. Tricoles, G.: Computer generated holograms: an historical review. *Appl. Opt.* **26**, 4351–4357 (1987)
9. Guan, Z.H., Huang, F.J., Guan, W.J., et al.: Chaos-based image encryption algorithm. *Phys. Lett. A* **346**(1), 153–157 (2005)
10. Belazi, A., Ellatif, A.A.: A simple yet efficient S-box method based on chaotic sine map. *Optik* **130**, 1438–1444 (2017)
11. Smila, M., Sankar, S.: Novel algorithms for finding an optimal scanning path for JPEG image compression. *IJETCSE* **8**, 230–236 (2014)
12. Shen, J.J., Ren, J.M.: A robust associative watermarking technique based on vector quantization. *Digital Signal Process.* **20**, 1408–1423 (2010)
13. Akhshani, A., Behnia, S., Akhavan, A., et al.: A novel scheme for image encryption based on 2D piecewise chaotic maps. *Opt. Commun.* **283**(17), 3259–3266 (2010)