Hindawi
Journal of Electrical and Computer Engineering
Volume 2018, Article ID 3987105, 6 pages
https://doi.org/10.1155/2018/3987105

*Research Article*

# An Image Encryption Scheme of Logistic Modulation Using Computer-Generated Hologram and Chaotic Map

**Hui Ren, Jun Wang, and Qiong-Hua Wang**

*School of Electronics and Information Engineering, Sichuan University, Chengdu 610065, China*

Correspondence should be addressed to Jun Wang; jwang@scu.edu.cn

Received 8 October 2017; Accepted 20 March 2018; Published 23 April 2018

Academic Editor: Jit S. Mandeep



We introduce an image encryption method based on computer-generated hologram (CGH) and two-dimensional Sine Logistic modulation map (2D-SLMM). We combine CGH and 2D-SLMM to improve encryption security. During the encryption process, the hologram needs to be logistically modulated by 2D-SLMM. This logistic modulation technique can avoid complex algorithms. Simulation results and security analysis demonstrate that the proposed approach has a high security level, good invisibility of image information in ciphertext, large key space, and strong robustness.

## 1. Introduction

Since Refregier and Javidi proposed a double random-phase encryption technique in 1995 [1], various improved optical image encryption methods have been presented [2–6]. However, data information of optical encryption is difficult to be transmitted through the network. And without the digital processing or conversion, the information must be reconstructed with an optical method. The digitization of encryption information favors the preservation and transmission of information. One of the most effective methods of the digitization of encrypted information is CGH [7–10]. Besides the fact that the virtual object, which does not yet exist in nature, can be recorded, CGH also permits any wavelength to be selected and system parameters to be adjusted arbitrarily, which offers more flexibility. Since this encryption method has only two secret keys of wavelength and diffraction distance, it is necessary to expand the key space of cipher system.

In the field of image encryption, many encryption methods involved chaos theory [11–16]. Chaotic maps have the properties of unpredictability and sensitivity to their parameters and initial values. They can generate different random sequences with different settings of parameters or initial values. Existing chaotic maps can be classified into two categories: one-dimensional (1D) chaotic maps and high-dimensional (HD) chaotic maps. 1D chaotic maps usually contain one variable and a few parameters. However, the structures and chaotic orbits of 1D chaotic maps are rather simple and may be estimated. And parameters or/and initial values of them may be predicted, too. Compared with 1D chaotic maps, HD chaotic maps usually have more complex structures and better chaotic performance. These make their chaotic orbits much difficult to predict [17, 18]. 2D Sine Logistic modulation map (2D-SLMM) which belongs to a kind of HD chaotic map has been proposed [17]. Performance analysis is provided to show that 2D-SLMM has wider chaotic range, better ergodicity, and hyperchaotic properties than the existing chaotic maps. If only 2D-SLMM is used in logistic modulation, the encrypted information cannot be completely hidden. Therefore, it is desired to increase the invisibility of image information in ciphertext.

In order to expand secret key space further and make the encrypted information totally invisible, we proposed an encryption method combining CGH and 2D-SLMM in this paper. Firstly, the mathematical model of CGH is built to get the hologram of original image. Then, the various parameters and initial values of the chaotic system are determined to acquire 2D-SLMM by them. Lastly, 2D-SLMM is modulated by the obtained hologram with a very simple way to get

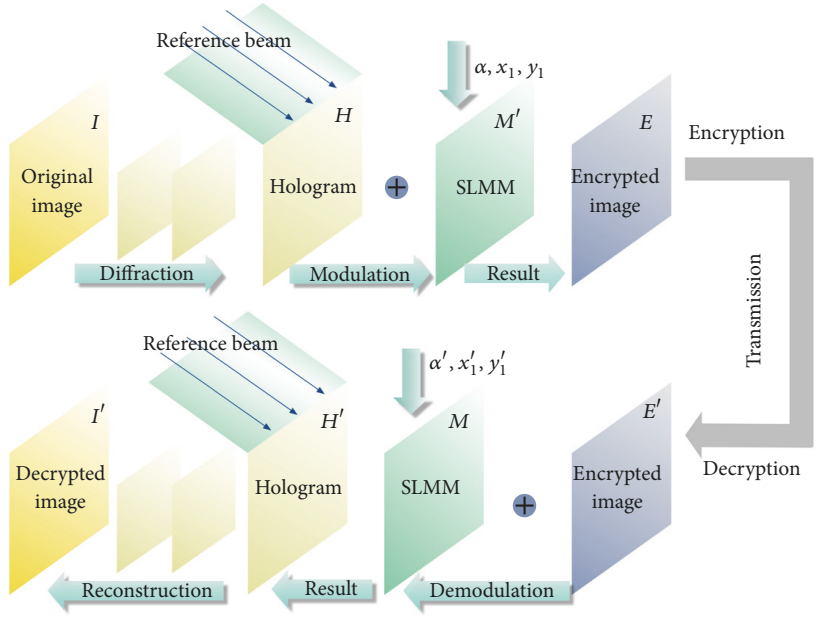


Figure 1: Encryption and decryption process.

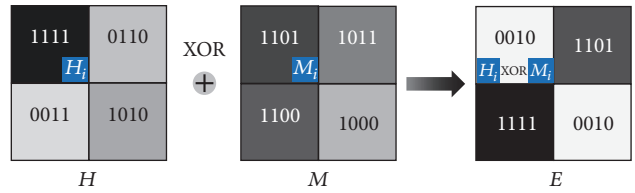


Figure 2: Process of logistic modulation.

the encrypted image. This modulation technique is logistic modulation, which can be implemented in not only software but hardware. Therefore, it is beneficial to greatly expand the application scope of this method. Simulation and security analysis verify the feasibility and security of this method.

## 2. Proposed Encryption Method

The proposed encryption process is shown in Figure 1. At the beginning, we get the hologram marked with $H$. Then, acquire 2D-SLMM marked with $M$ by setting parameters and initial values. In the end, the obtained hologram is modulated logistically by 2D-SLMM to get the encrypted image marked with $E$. It should be emphasized that because the decryption is the inverse progress of encryption, the detailed description of decryption is omitted.

First, we need to obtain the hologram of the original image. The schematic diagram of the generation of a hologram can be referenced in [19], where wave of object and reference beam interference with each other. And the interference pattern as a hologram is to be recorded on the observation plane.

Next, 2D-SLMM is acquired with different settings of parameters and initial values. It is defined by

$$\begin{aligned} x_{i+1} &= \alpha \left(\sin\left(\pi y_i\right) + \beta\right) x_i \left(1 - x_i\right) \\ y_{i+1} &= \alpha \left(\sin\left(\pi x_{i+1}\right) + \beta\right) y_i \left(1 - y_i\right), \end{aligned} \tag{1}$$

where $\alpha$ and $\beta$ are control parameters. $\alpha \in [0, 1]$ and $\beta \in [0, 3]$.

2D-SLMM is derived from two 1D chaotic maps, the Logistic and Sine maps. A combination of the Sine map and parameter $\beta$ is used to modulate the output of the Logistic map to enhance its nonlinearity and randomness. The result is then extended from one-dimension to two-dimension to obtain 2D-SLMM. Two output values of 2D-SLMM $x_{i+1}$ and $y_{i+1}$ intertwine each other. Thus, its orbits and iteration values are difficult to predict. When parameter $\beta$ is close to 3, 2D-SLMM shows good chaotic performance. For simplicity, we set $\beta = 3$ in the rest of this paper [17]. In addition to control parameters, the initial values $x_1$ and $y_1$ can also be used as secret keys, which can expand the key space significantly.

Finally, the obtained hologram $H$ is logistically modulated by 2D-SLMM $M$ to get encrypted image $E$. The process is shown in Figure 2, where $H_i$ and $M_i$ represent number $i$ pixel of $H$ and $M$, respectively. The numbers in the figure are the binary representation of pixel values. It should be emphasized that, to achieve better effect, we can also make

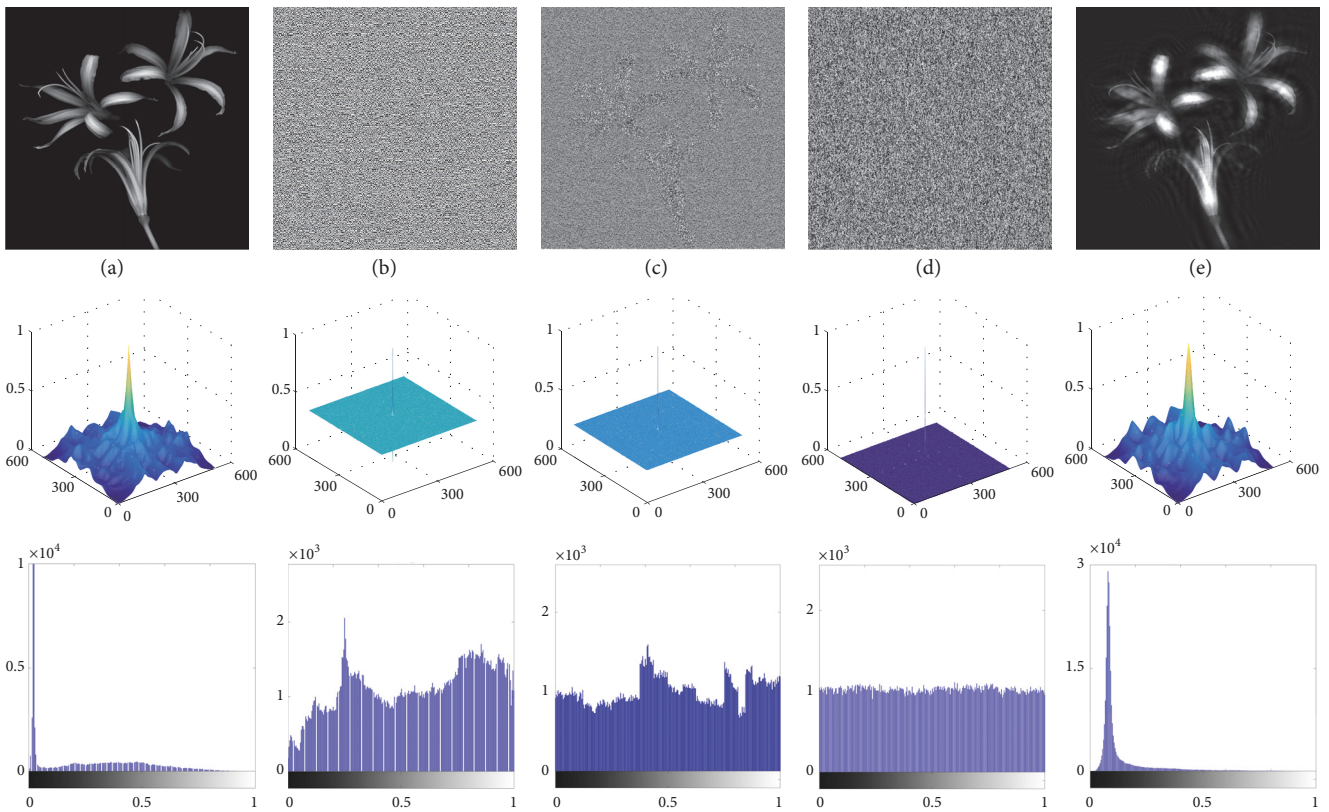


Figure 3: Simulation of proposed method: (a) the original image, (b) 2D-SLMM, (c) 1st round XOR encrypted image, (d) 2nd round XOR encrypted image, and (e) decrypted image. The second row shows their corresponding autocorrelation images and the third row shows their corresponding histograms.

twice logistic modulation and the detailed analysis is depicted in Section 3.

## 3. Simulated Results and Security Analysis

The object to be encrypted is a gray image of "Flowers" with 512 × 512 pixels as shown in Figure 3(a) and 2D-SLMM is shown in Figure 3(b). After the first round of logistic modulation, as can be seen from Figure 3(c), there is still a little bit of effective information. Therefore, we make the second round of modulation to complete the encryption. Then the encrypted image is shown in Figure 3(d). Obviously, all the information is hidden in the noise-like image. Finally, the decrypted image is in Figure 3(e). The rest of images of Figure 3 show their corresponding autocorrelation images and histograms.

The proposed method can apply to many other types of images. There are two sets of comparison experiment, "Camera man" and "Chess," respectively, in Figures 4 and 5. In addition to proposed method as shown in Figure 4(a), there are three other encryption methods as shown in Figures 4(c), 4(d), and 4(e). They are SBE-LBP [20], BPE-XOR [21], and the method of using 2D-SLMM to modulate original image instead of hologram. The rest images of Figure 4 show their corresponding histograms and autocorrelation images. By comparison, we can find that the encryption effect of the proposed method is the best. It needs to be emphasized that we just take only 1st round XOR operation to ensure fairness. The analysis of Figure 5 is the same as that of Figure 4.

*3.1. Robustness Test.* Figure 6 shows experimental results of noise and data loss attacks to the cipher-images. Some attacked on holograms with noise are shown in Figures 6(a)–6(c) and their corresponding decrypted images are shown in Figures 6(g)–6(i). The image quality assessment, structural similarity (SSIM) index, can assess the similarity between two images [22]. So we calculate the SSIM indexes between decrypted images Figures 6(g)–6(i) and original image Figure 3(a). When SIMM index is 1, it means that the two images are exactly the same. Less than 1, it means that the similarity between the two images is weak. By calculation, the SIMM index between Figures 6(g) and 3(a) is 0.44 rather than 1. It is because that there still exists the error of algorithm even without noise interference. Through these SSIM indexes, we can draw a conclusion that this method can resist noise attack when the noise level is not too high.

Then, the situation of data loss in public media transmission is simulated. Some encrypted images of data loss are shown in Figures 6(d)–6(f) and their corresponding decrypted images are shown in Figures 6(j)–6(l). At the same time, the SSIM indexes between decrypted images and original image Figure 3(a) are on the top of the decrypted

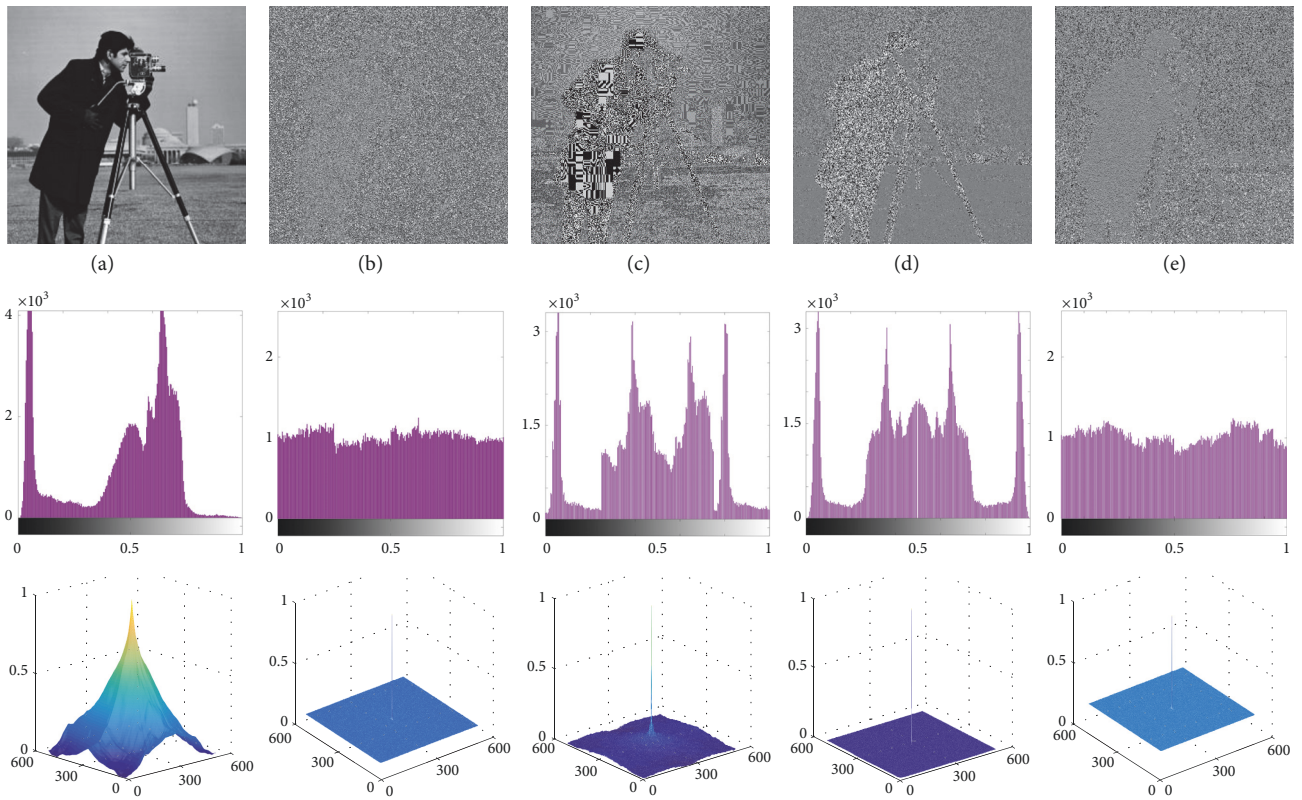


Figure 4: Comparative experiment of "Camera man": (a) original image, (b) 2D-SLMM, (c) SBE-LBP, (d) BPE-XOR, and (e) method of using 2D-SLMM to modulate original image. The second row shows their corresponding histograms and the third row shows their corresponding autocorrelation images.

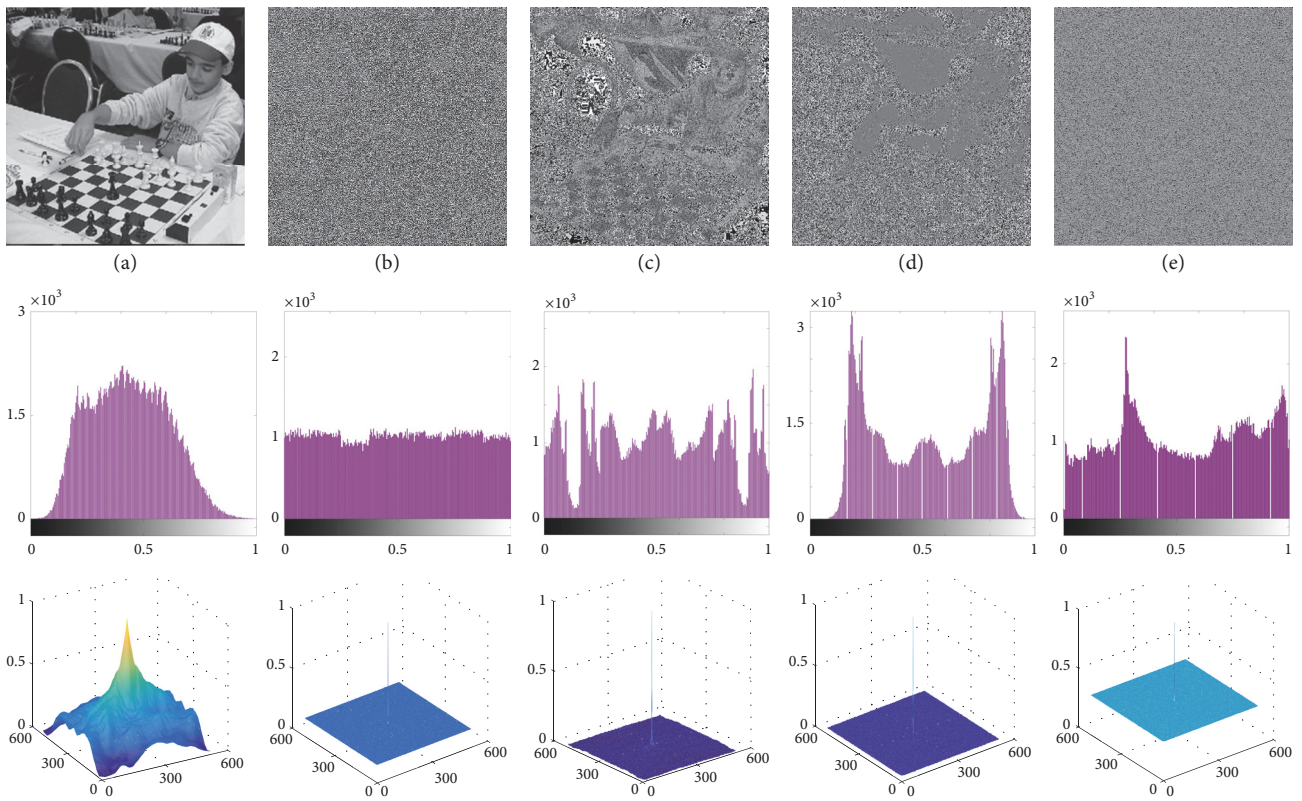


Figure 5: Comparative experiment of "Chess": (a) original image, (b) 2D-SLMM, (c) SBE-LBP, (d) BPE-XOR, and (e) method of using 2D-SLMM to modulate original image. The second row shows their corresponding histograms and the third row shows their corresponding autocorrelation images.

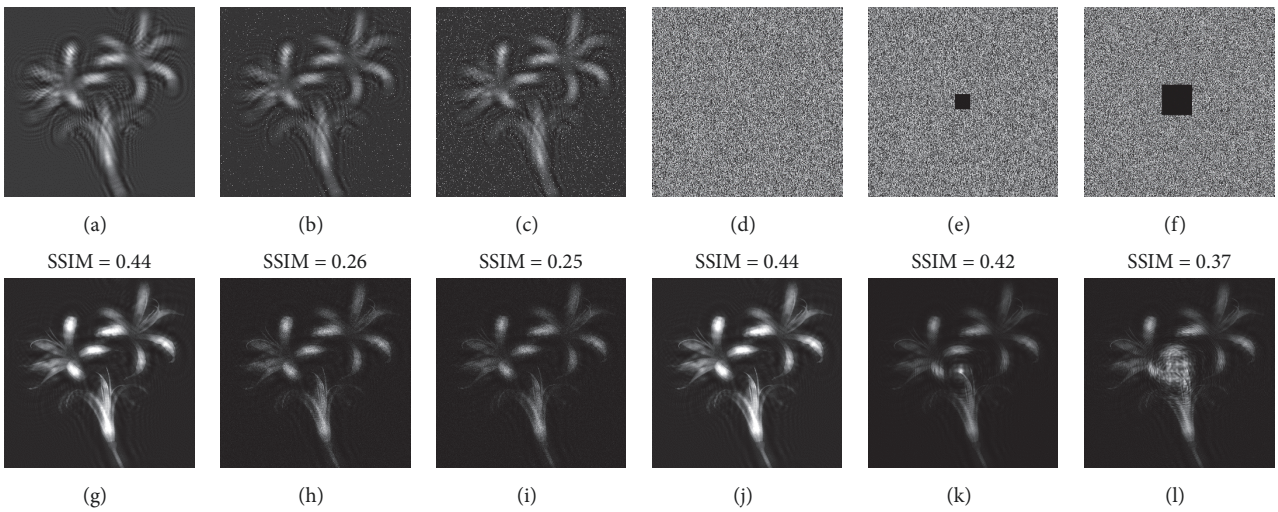


Figure 6: Test of robustness against noise attack and occlusion: (a) hologram without noise, (b) 1% Salt and Pepper noise on hologram, (c) 1.5% Salt and Pepper noise on hologram, (d) encrypted image, (e) 0.6% data loss on (d), and (f) 2.44% data loss on (d). The second row shows their corresponding decrypted images.

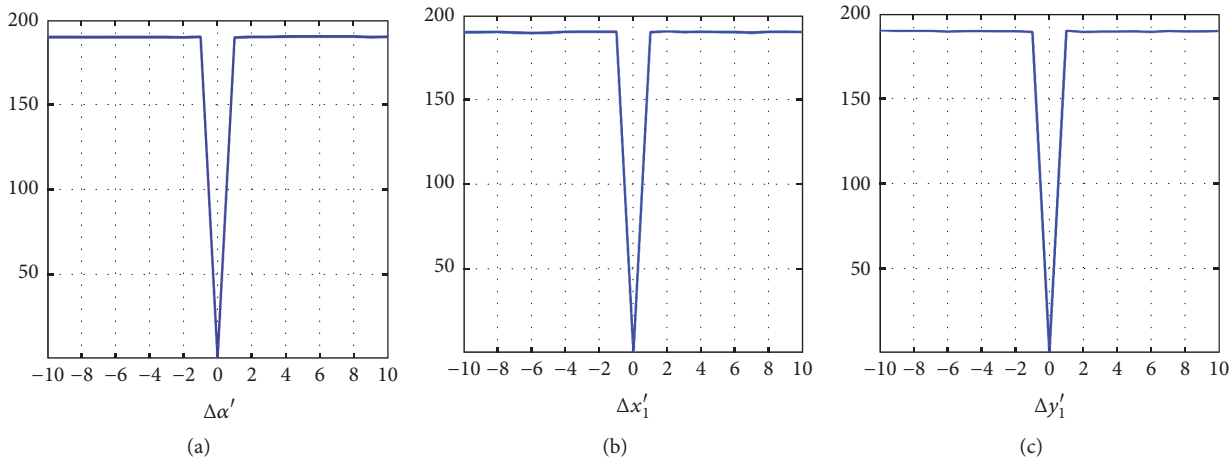


Figure 7: MSE varies with (a) the control parameter $\alpha'$ shift, (b) the initial value $x_1'$ shift, and (c) the initial value $y_1'$ shift.

images. It can be seen from SSIM indexes of Figures 6(j)–6(l) that this method can tolerant a certain degree of data loss.

*3.2. Key Space and Sensitivity Analysis.* The high sensitive to initial conditions is inherent in any chaotic system. To provide an encryption algorithm with high security, the key space should be large enough to make any brute force attack ineffective. When wavelength $\lambda$ and diffraction distance $z$ are given certain values, control parameter $\alpha$ and and initial values $x_1$ and $y_1$ can also be used as encryption keys. The dependence of MSE (Mean Square Error) on the change of decryption keys $\alpha'$, $x_1'$, and $y_1'$ is shown in Figures 7(a), 7(b), and 7(c), respectively. On the $x$-axis, the unit of $\alpha'$, $x_1'$, and $y_1'$ is $9.0 \times 10^{-17}$, $1.0 \times 10^{-16}$, and $1.0 \times 10^{-15}$. Only when the values of $\alpha'$, $x_1'$, and $y_1'$ are the same as $\alpha$, $x_1$, and $y_1$ do the MSE reach a very small value. In the case of small derivations, the MSE increases quickly and there is a failure to recognize the original image visually. The high sensitivity results in great difficulty in duplicating the decryption system.

## 4. Conclusion

We proposed an encryption method based on CGH and 2D-SLMM. It has better encryption performance than the compared methods. The experiments also verify the resistance to multiple attacks: noise, occlusion, and the tiny change of keys. Furthermore, beside keys of $\lambda$ and $z$, the other parameters of $\alpha$, $x_1$, and $y_1$ are used as additional secret keys to provide a larger key space. Therefore, the security of the system has been greatly improved. Hologram can be realized in computer or optical setup. Moreover, the algorithm of logistic modulation is very simple to implement in software, hardware, and all-optical XOR logic gate. Therefore, the proposed encryption method is not only effective but also flexible. In

the future, it could be applied in the field of national defense science and technology or other places requiring a higher level of image security and system flexibility.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## References


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

[2] A. Alfalou and A. Mansour, "Double random phase encryption scheme to multiplex and simultaneous encode multiple images," *Applied Optics*, vol. 48, no. 31, pp. 5933–5947, 2009.

[3] J. Yi and G. Tan, "Optical compression and encryption system combining multiple measurement matrices with fractional Fourier transform," *Applied Optics*, vol. 54, no. 36, pp. 10650–10658, 2015.

[4] X.-W. Li and I.-K. Lee, "Modified computational integral imaging-based double image encryption using fractional Fourier transform," *Optics and Lasers in Engineering*, vol. 66, pp. 112–121, 2015.

[5] X. Li, D. Xiao, and Q.-H. Wang, "Error-free holographic frames encryption with CA pixel-permutation encoding algorithm," *Optics and Lasers in Engineering*, vol. 100, pp. 200–207, 2018.

[6] C. Li, D. Lin, and J. Lu, "Cryptanalyzing an Image-Scrambling Encryption Algorithm of Pixel Bits," *IEEE MultiMedia*, vol. 24, no. 3, pp. 64–71, 2017.

[7] J. Liu, H. Jin, L. Ma, Y. Li, and W. Jin, "Optical color image encryption based on computer generated hologram and chaotic theory," *Optics Communications*, vol. 307, pp. 76–79, 2013.

[8] S.-X. Xi, X. Wang, X. Sun, S. Chang, and L. Lin, "Three random phase encryption technology in the Fresnel diffraction system based on computer-generated hologram," *Optical Engineering*, vol. 53, no. 1, Article ID 011004, 2014.

[9] S. Xi, X. Wang, L. Song et al., "Experimental study on optical image encryption with asymmetric double random phase and computer-generated hologram," *Optics Express*, vol. 25, no. 7, pp. 8212–8222, 2017.

[10] H. Yoshikawa and T. Yamaguchi, "Review of Holographic Printers for Computer-Generated Holograms," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 4, pp. 1584–1589, 2016.

[11] G. Ye and K.-W. Wong, "An efficient chaotic image encryption algorithm based on a generalized Arnold map," *Nonlinear Dynamics*, vol. 69, no. 4, pp. 2079–2087, 2012.

[12] Y. Zhou, L. Bao, and C. L. P. Chen, "Image encryption using a new parametric switching chaotic system," *Signal Processing*, vol. 93, no. 11, pp. 3039–3052, 2013.

[13] A. Kanso, H. Yahyaoui, and M. Almulla, "Keyed hash function based on a chaotic map," *Information Sciences*, vol. 186, pp. 249–264, 2012.

[14] X. Wang, W. Zhang, W. Guo, and J. Zhang, "Secure chaotic system with application to chaotic ciphers," *Information Sciences*, vol. 221, pp. 555–570, 2013.

[15] Y.-Q. Zhang and X.-Y. Wang, "A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice," *Information Sciences*, vol. 273, pp. 329–351, 2014.

[16] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172–182, 2014.

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

[18] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," *Information Sciences*, vol. 339, pp. 237–253, 2016.

[19] X. Su, *Optical Information*, Science Press, Beijing, China, 2nd edition, 2010.

[20] Y. Zhou, K. Panetta, S. Agaian, and C. L. P. Chen, "Image encryption using P-Fibonacci transform and decomposition," *Optics Communications*, vol. 285, no. 5, pp. 594–608, 2012.

[21] J. A. C. Gallas, "Structure of the parameter space of the Hénon map," *Physical Review Letters*, vol. 70, no. 18, pp. 2714–2717, 1993.

[22] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, 2004.