Fully phase color image encryption based on joint fractional Fourier transform correlator and phase retrieval algorithm

Ding Lu (鲁 丁) and Weimin Jin (金伟民)*

Institute of Information Optics, Zhejiang Normal University, Jinhua 321004, China

**Corresponding author: jhjinwm@163.com*

Received September 7, 2010; accepted October 28, 2010; posted online January 28, 2011

A novel fully phase color image encryption/decryption scheme based on joint fractional Fourier transform correlator (JFRTC) and phase retrieval algorithm (PRA) is proposed. The security of the system is enhanced by the fractional order as a new added key. This method takes full advantage of the parallel processing features of the optical system and could optically realize single-channel color image encryption. The system and operation procedures are simplified. The simulation results of a color image indicate that the new method provides efficient solutions with a strong sense of security.

OCIS codes: 100.5070, 070.2575, 070.4550, 100.4550.

doi: 10.3788/COL201109.021002.

Information encrypting and anti-counterfeiting techniques have become an important role for information security. Optical and optoelectronic signal processing has distinct advantages due to its inherent parallelism, high speed, and low cost, especially. Optical encryption based on double random-phase (DRP) encoding[1] has received extensive attention. In recent years, several modified optical image encryption methods[2−7] have been proposed in order to improve the security of DRP encryption. Encryption methods based on phase retrieval algorithm (PRA)[5−7] have been greatly developed because of PRA has great flexibility and high security. For color image encryption, several three-channel techniques using tricolor lasers[8−10] have been proposed. However, all these methods need more complicated systems with high cost and more procedures. Yang *et al.* developed a single-channel color image encryption method based on tricolor grating[11]. Recently, Chang *et al.* proposed an asymmetric gray image encryption method based on PRA and joint Fourier transform correlator (JFTC)[12]. The main limitation of this method is that the phase distribution in the Fourier spectrum plane dominates the decryption progress, whereas that in the input plane does not, causing the security of the system to be degraded. Most recently, a modified method was proposed by the same group[13]. Although the phase distribution of the input plane could also play an important role in the security, the parameters in the power-law and log-sigmoid functions are restricted in the modified method.

Previously, we have proposed a color image recognition technique based on joint fractional Fourier transform correlator (JFRTC)[14]. In this letter, a single-channel color image encryption method based on PRA and JFRTC is proposed. In this method, the joint fractional spectrum is transformed into pure phase information through a simpler nonlinear transformation than that in Ref. [13]. The security of the system could be ensured for the phase distribution in the input and fractional Fourier spectrum planes, playing the same important role in the decryption progress. The fractional order, as a new key, greatly improves the security. This method could simplify the system and reduce costs compared with the traditional three-channel color image encryption technique.

The target color image is expressed as $g(x,y) = g_{\rm r}(x,y+a) + g_{\rm g}(x,y) + g_{\rm b}(x,y-a)$, where $g_{\rm r}$, $g_{\rm g}$, and $g_{\rm b}$ correspond to the red, green, and blue (RGB) color components, respectively. In the encryption process, the phase mask $f(x,y) = f_1(x,y) + f_2(x,y)$, which is located in the input plane, is randomly generated at first. $f_1(x,y)$ and $f_2(x,y)$ are respectively defined as

$$f_1(x,y) = \exp\{{\rm i}[\varphi_{\rm r}(x-a,y+b) + \varphi_{\rm g}(x-a,y) + \varphi_{\rm b}(x-a,y-b)]\}, \quad (1)$$

$$f_2(x,y) = \exp\{{\rm i}[\varphi_{\rm r}(x+a,y+b) + \varphi_{\rm g}(x+a,y) + \varphi_{\rm b}(x+a,y-b)]\}, \quad (2)$$

where $f(x,y)$ is the phase key in the input plane; $\varphi_{\rm r}$, $\varphi_{\rm g}$, and $\varphi_{\rm b}$ are the phases corresponding to RGB, respectively. To obtain the phase key $\exp[{\rm i}H_3(\mu,\nu)]$ located in the fractional Fourier spectrum plane based on a predefined target image, the projection onto constraint sets (POCS) algorithm is employed.

The block diagram of the application of the POCS algorithm on the proposed setup is shown in Fig. 1. The received joint fractional power spectrum (JFPS) is

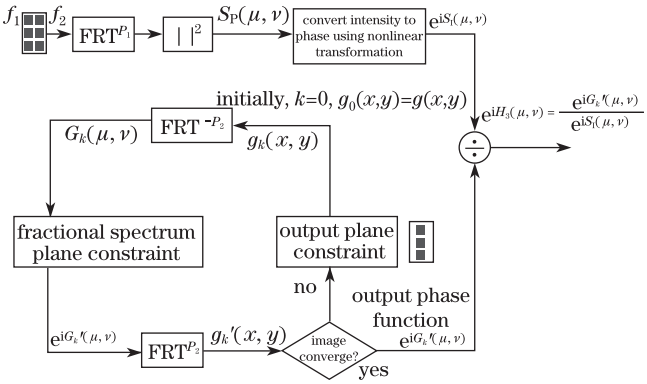

Fig. 1. Block diagram of the proposed setup. FRT^{P_1} represents fractional Fourier transform with fractional order P_1.

normalized to 255, and then the JFPS is nonlinearly transformed to phase information as

$$S_{\mathrm{I}}(\mu,\nu)=\begin{cases} S_{\mathrm{P}}(\mu,\nu) & \text{if} S_{\mathrm{P}}(\mu,\nu)\le 2\pi \\ S_{\mathrm{P}}(\mu,\nu)\pm 2k\pi & \text{if} S_{\mathrm{P}}(\mu,\nu)>2\pi \end{cases}. \quad (3)$$

During the iteration process, the convergence criterion of the reconstructed images with size $m \times n$ (pixel) is represented by the mean squared error (MSE), which is defined as

$$\mathrm{MSE}=\frac{1}{m\times n}\sum_{x=1}^{m}\sum_{y=1}^{n}[|g(x,y)|^2-|g_{\mathrm{k}}(x,y)|^2]^2. \quad (4)$$

The phase distribution $f(x,y)$ located in the input plane and the phase distribution $\exp[\mathrm{i}H_3(\mu,\nu)]$ acquired in the last iteration represent the two phase keys.

The color image decryption process proposed in this letter can be implemented through an optical system with monochromatic plane wave illumination, as shown in Fig. 2. In the decryption process, once a coherent plane wave is incident to the $f(x,y)$ located in the input plane, the JFPS is detected by a square-law detector such as charge-coupled device (CCD), and the JFPS is nonlinearly transformed to phase distribution. The transformed phase is then multiplied by a matched phase key, $\exp[\mathrm{i}H_3(\mu,\nu)]$. The results are then displayed in the phase-only spatial light modulator (SLM). Three retrieved space separated RGB components are obtained in the output plane. A decrypted color image can be obtained after the three RGB components are extracted and have undergone layer superposition.

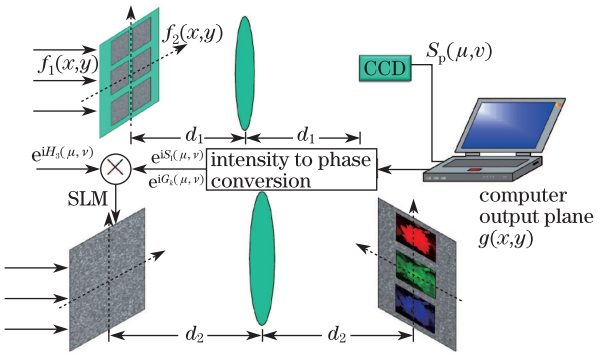

Fig. 2. Optical setup of the fully phase JFRTC setup for color image decryption.

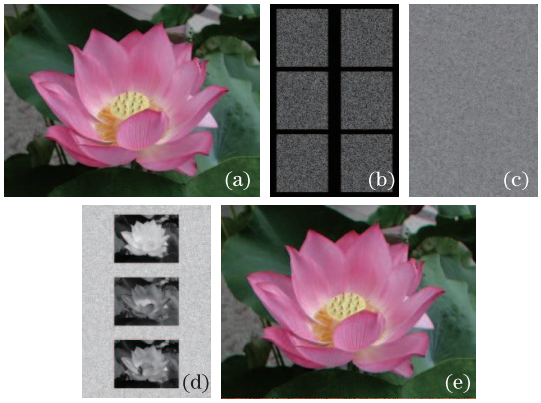

Fig. 3. (a) Target color image; (b) phase distribution of the input plane; (c) phase key stored in the computer; (d) decrypted RGB component image; (e) decrypted color image after synthesis.

Only one phase-only SLM is required in the decryption process. The system is simple and requires low cost; its security and reliability are assured. In addition, this method could avoid the phase distortion introduced by the gap that inevitably exists between two SLMs when they are placed side by side. The reconstructed image will obviously degrade when there are phase distortions.

The simulation results are presented to demonstrate the performance of the system. The input RGB image chosen for encryption is a lotus flower with a size of 340 $\times$ 256 $\times$ 3 (pixel), as shown in Fig. 3(a). The fractional orders P_1 and P_2 chosen for the encryption process are 0.78 and 1.34, respectively. The phase in the input plane are uniformly distributed in the interval $[0, 2\pi]$ and statistically independent. The phase distributions of the two phase masks after 100 iterations are shown in Figs. 3(b) and (c), respectively. As can be seen, the target color image has been encoded into the two phase masks, representing the encrypted results.

In the decryption process, a correct spatially separated RGB component image can be constructed when the two phase masks are matched, as shown in Fig. 3(d). The corresponding regions of the RGB components are extracted and synthesized. A decrypted color image is obtained, as shown in Fig. 3(e). The recovered color image clearly has high quality.

The JFPS of the input random phase and the converted phase are shown in Figs. 4(a) and (c), respectively; meanwhile, their corresponding histograms are shown in Figs. 4(b) and (d), respectively. The histogram of the phase information shown in Fig. 4(d) is clearly more uniform than that in Fig. 4(b). Thus the disadvantage of the dominating effect arising from the phase distribution at the JFPS plane[12] was eliminated effectively in Ref. [13]. When the phase distribution at the input plane is incorrect, the correct decrypted image cannot be reconstructed.

From the MSE evolution curve of the RGB components

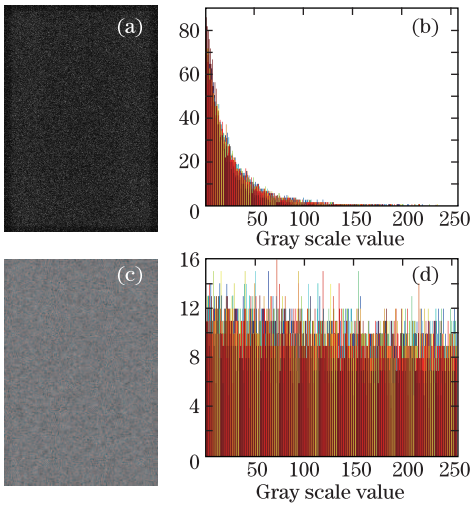

Fig. 4. (a) JFPS at the fractional Fourier plane; (b) histogram of the original JFPS; (c) distribution after converting intensity to phase; (d) histogram of $S_1(\mu\nu)$.

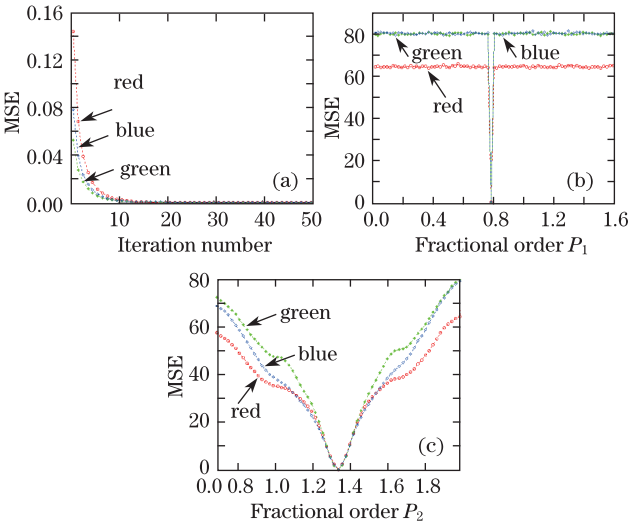

Fig. 5. MSE results of the RGB components versus (a) the number of iteration, (b) fractional order P_1, and (c) fractional order P_2.

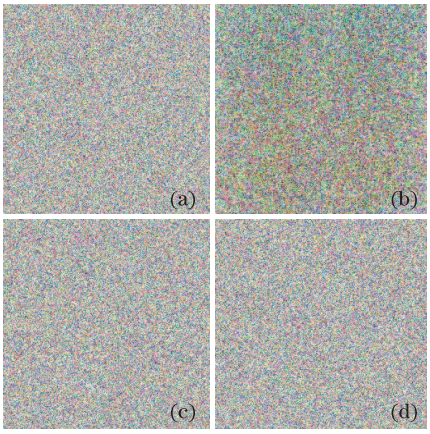

Fig. 6. Decrypted color image with (a) incorrect fractional order $P_1(P_1 = 0.7, P_2 = 1.34)$; (b) incorrect input plane phase distribution; (c) incorrect fractional order $P_2(P_1 = 0.78, P_2 = 1.2)$; (d) incorrect fractional spectrum plane phase distribution.

with different iteration numbers, as shown in Fig. 5(a), the convergence of MSE is initially very fast and then eventually slowed down after about five loops. The MSE results of the RGB components versus the change of the fractional orders P_1 and P_2 are given in Figs. 5(b) and (c), respectively. Figure 6 shows the decrypted color image when only one key is incorrect, clearly showing that the security of the system is very high. The recovered color image is distributed like white noise when the fractional order is deviated or the phase distribution is incorrect.

In conclusion, we propose a fully phase optical security system based on JFRTC and PRA, which can perform color image encryption. This method does not require the fabrication of conjugate phase mask in the decryption process and could be implemented through photoelectric system. Simulation results show that the algorithm is simple and converges fast. Without the correct keys such as phase distribution at the input and output planes and the fractional orders, illegal users can hardly recover the decrypted image through blind deconvolution operations. On the other hand, pure phase distribution can be realized by adopting diffractive optical element, which has many advantages such as high diffractive efficiency, small dimension, large design flexibility, and ease to integrate. With the development of micro-fabrication technique, micro and compact integrated optical encryption system can be realized in the future.

This work was supported by the Zhejiang Provincial Natural Science Foundation of China under Grant No. Y1080944.

References

1. P. Refregier and B. Javidi, Opt. Lett. **20,** 767 (1995).
2. G. Unnikrishnan and K. Singh, Opt. Eng. **39,** 2853 (2000).
3. N. Zhou, T. Dong, and J. Wu, Opt. Commun. **283,** 3037 (2010).
4. J. Ma, Z. Liu, Z. Guo, and S. Liu, Chin. Opt. Lett. **8,** 290 (2010).
5. J. Hahn, H. Kim, and B. Lee, Opt. Express **14,** 11103 (2006).
6. Y. Shi and J. Zhang, Acta Opt. Sin. (in Chinese) **29,** 2705 (2009).
7. H.-E. Hwang, H. T. Chang, and W.-N. Lie, Opt. Express **17,** 13700 (2009).
8. J. Zhao, H. Lu, and Q. Fan, Proc. SPIE **6279,** 62793B (2007).
9. M. Joshi, C. Shakher, and K. Singh, Opt. Commun. **279,** 35 (2007).
10. L. Chen and D. Zhao, Opt. Express **14,** 8552 (2006).
11. X. P. Yang, L. J. Gao, X. L. Wang, H. C. Zhai, and M. W. Wang, Acta Phys. Sin. (in Chinese) **58,** 1662 (2009).
12. H. T. Chang and C. T. Chen, Opt. Commun. **239,** 43 (2004).
13. H. T. Chang and C.-C. Chen, Opt. Express **14,** 1458 (2006).
14. W. Jin and Y. Zhang, Chin. Opt. Lett. **5,** 628 (2007).