Double-image encryption based on joint transform correlation and phase-shifting interferometry

Lina Shen (沈丽娜), Jun Li (李 军), and Hongsen Chang (常鸿森)

School of Physics and Telecommunication Engineering, South China Normal University, Guangzhou 510006

Received February 2, 2007

An image encryption method combining the joint transform correlator (JTC) architecture with phase-shifting interferometry to realize double random-phase encoding is proposed. The encrypted field and the decrypting key are registered as holograms by phase-shifting interferometry. This method can encrypt two images simultaneously to improve the encryption efficiency of the methods based on JTC architecture, and eliminate the system alignment constraint of the methods based on Mach-Zehnder interferometer (MZI) architecture. Its feasibility and validity are verified by computer simulations. Moreover, image encryption and decryption can be achieved at high speed optically or digitally. The encrypted data are suitable for Internet transmission.

OCIS codes: 100.2000, 100.4550, 090.2880, 100.3010.

Information security has been given more and more attention with the rapid development of computer technology and Internet. For the security of image data, many image encryption methods have been proposed successively, for example, the random-phase encoding, digital holography, fractional Fourier transformation, polarization encoding, virtual optics, phase-only encryption, and double-image encryption[1−9]. Among them, those methods involving phase-shifting interferometry (PSI) are mostly based on Mach-Zehnder interferometer (MZI) architecture, and generally require accurate alignment due to the use of optical phase retarders and phase masks. Even one pixel error in the alignment would result in failed reconstruction[8−12]. The encryption method proposed by La Mela *et al.*[13] can overcome the alignment drawbacks perfectly, but its efficiency is comparatively low, at least six interferograms must be recorded and delivered to retrieve the original object field. In this paper, a new image encryption method is proposed, which combines the joint transform correlator (JTC) architecture and PSI to realize double random-phase encoding. The encrypted field and the decrypting key are obtained by three-step PSI and registered as holograms by charge coupled device (CCD) camera, which are suitable for the Internet transmission. This method can greatly improve the encryption efficiency of the methods based on JTC architecture by use of encrypting two images simultaneously, and eliminate the system alignment constraint which exists in the popular encryption systems based on MZI. Moreover, image encryption and decryption can be achieved at high speed either optically or digitally.

The encryption system is illustrated in Fig. 1, where a linearly polarized laser beam is expanded and collimated, and then illuminates an amplitude-modulated spatial light modulator (AMSLM) contacted closely with a phase-modulated spatial light modulator (PMSLM). Under the control of computer, the AMSLM displays one input image $f(x_0, y_0)$ on its right half, and the constant one on its left half. Simultaneously, the PMSLM displays the sum of another input image $g(x_0, y_0)$ and a random phase mask (RPM) $n_1(x_0, y_0)$ on its right half, and another RPM $n_2(x_0, y_0)$ on its left half. So the right half and the left half waves passing through SLMs respectively correspond to the object wave and the reference wave in the PSI. A CCD camera is used to record the interferograms which contain the encrypted object information in the output plane.

Suppose that the input images $f(x_0, y_0)$ and $g(x_0, y_0)$ have been normalized into the ranges of $[0, 1]$ and $[0, \frac{1}{2}]$ respectively, the RPMs $n_1(x_0, y_0)$ and $n_2(x_0, y_0)$ are two independent white noises uniformly distributed in $[0, 1]$. The distance between the centers of object scene and reference scene is $2c$, the wavelength of the input plane wave is λ, and the diffraction distance is d. In combination with the adequate state of light polarization, the PMSLM can reach a phase modulation 2π. The object wave and the reference wave on the behind side of PMSLM can be described respectively as

$$o(x_0 - c, y_0) = f(x_0 - c, y_0) \times \exp[i2\pi g(x_0 - c, y_0)] \times \exp[i2\pi n_1(x_0 - c, y_0)], \quad (1)$$

$$r(x_0 + c, y_0) = \exp[i2\pi n_2(x_0 + c, y_0)], \quad (2)$$

where $o(x_0 - c, y_0)$ represents the object wave, and $r(x_0 - c, y_0)$ is the reference wave in the input plane.

After being Fresnel diffracted, the two complex waves in the output plane become

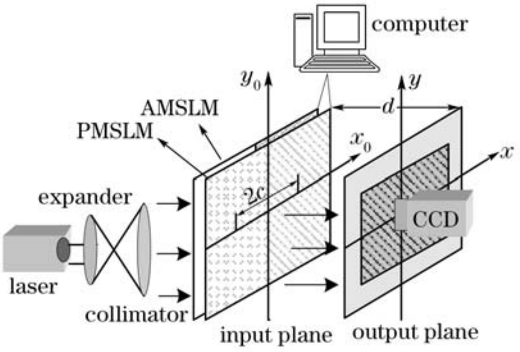

Fig. 1. Scheme of the image encryption system.

$$O(x,y) = FR_d[o(x_0 - c, y_0)] = A_0 \exp[i\phi_0(x,y)], \quad (3)$$

$$R(x,y) = FR_d[r(x_0 + c, y_0)] = A_r \exp[i\phi_r(x,y)], \quad (4)$$

where FR_d stands for the Fresnel transform of distance d, $O(x,y)$ and $R(x,y)$ respectively stand for the diffracted fields of object wave $o(x_0 - c, y_0)$ and reference wave $r(x_0 - c, y_0)$ in the output plane.

Using standard three-step PSI in JTC[14] with phase shifting angles of 0, $\pi/2$, and π, we can get three interferograms whose intensity distributions are

$$I_n(x,y) = A_\mathrm{o}^2 + A_\mathrm{r}^2 + 2A_\mathrm{o}A_\mathrm{r} \times \cos[\phi_\mathrm{o}(x,y) - \phi_\mathrm{r}(x,y) - 2cx + n\frac{\pi}{2}], \quad n = 1,2,3. \quad (5)$$

So the encrypted object wave $O_\mathrm{e}(x,y)$ in the output plane can be retrieved by the expression

$$O_\mathrm{e}(x,y) = A_\mathrm{o}A_\mathrm{r}\exp[i(\phi_\mathrm{o} - \phi_\mathrm{r} - 2cx)] = \frac{1}{4}[I_1 - I_3 + i(2I_2 - I_1 - I_3)]. \quad (6)$$

In order to decrypt $O_\mathrm{e}(x,y)$, we must obtain the principal key $R'(x,y)$ which is got from the diffracted field $R(x,y)$ with a phase deviation. So we carry out the three-step PSI process again, but now the RPM $n_2(x_0,y_0)$ is displayed on the left half of the PMSLM, zero on its right half, and the constant one is displayed on the AMSLM. Then the field diffracted by object wave, in the output plane, becomes a plane wave represented as $C(x,y) = \exp(i \cdot \phi_\mathrm{c})$, where ϕ_c is a constant. And the field diffracted by reference wave remains $R(x,y)$. Suppose that the new obtained interferograms are I_1', I_2', and I_3'. Once these interferograms are transmitted via Internet, the receiver can first calculate the principal key $R'(x,y)$ by

$$R'(x,y) = A_\mathrm{r}\exp[i(\phi_\mathrm{c} - \phi_\mathrm{r} - 2cx)] = \frac{1}{4}[I_1' - I_3' + i(2I_2' - I_1' - I_3')], \quad (7)$$

and further obtain $O'(x,y)$, which represents the product of the object wave $O(x,y)$ and a constant phase term, by

$$O'(x,y) = O_\mathrm{e}(x,y)/R'(x,y) = A_\mathrm{o}\exp[i(\phi_\mathrm{o}(x,y) - \phi_\mathrm{c})]. \quad (8)$$

Then the original object wave $o(x_0 - c, y_0)$ can be reconstructed from

$$o(x_0 - c, y_0) = IFR_d\left[O'(x,y)\right], \quad (9)$$

where IFR_d stands for the inverse Fresnel transform of distance d. Finally, after multiplying $o(x_0 - c, y_0)$ by $\exp[-i2\pi n_1(x_0 - c, y_0)]$, we can obtain the input image $f(x_0,y_0)$ by taking the amplitude of the result. Extracting the phase of the result and dividing it by π, we can obtain the other input image $g(x_0,y_0)$.

So, with λ, d and $n_1(x_0,y_0)$ having been known, we can achieve the encryption and decryption of double-image as long as we get the interferograms I_1, I_2, I_3, I_1', I_2', and I_3'. In addition, λ, d and $n_1(x_0,y_0)$ as supplementary keys make the security higher.

We made a series of computer simulations to verify the feasibility and validity of the proposed method. The parameters used in these simulations are $\lambda = 632.8$ nm, $d = 0.5$ m. All the frames are digitized to 256 gray levels with the size of 256 × 256 pixels.

The two input images modulated by AMSLM and PMSLM respectively are shown in Fig. 2. Two interferograms I_1 and I_1' recorded by CCD camera are shown in Fig. 3; others just look similar to those. The retrieved images obtained when correct keys are used are shown in Fig. 4, while the results obtained when incorrect keys are used are shown in Figs. 5 and 6.

Obviously, we can retrieve the input images perfectly with the correct keys, but cannot get any hint of them once any key is incorrect. The image $g(x_0,y_0)$ is more sensitive to the variation of λ and d than the image $f(x_0,y_0)$, and $n_1(x_0,y_0)$ only affects the reconstruction of image $g(x_0,y_0)$.

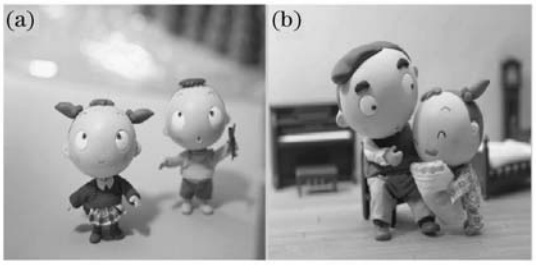

Fig. 2. Two input images to be encrypted. (a) The image modulated by AMSLM; (b) the image modulated by PMSLM.

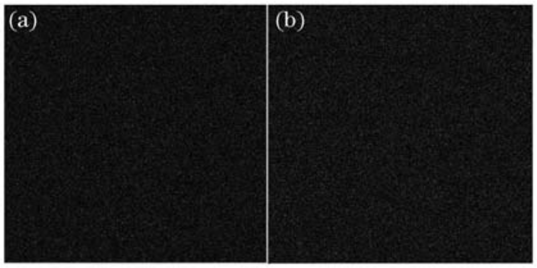

Fig. 3. Interferograms recorded by CCD and transmitted to the receiver. (a) One of the three interferograms in encryption process; (b) one of the three interferograms in making the principal key process.

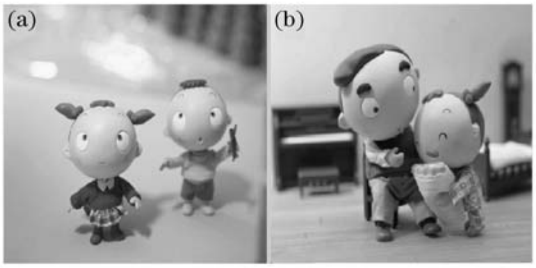

Fig. 4. Retrieved images of the input in Fig. 2 with correct keys.

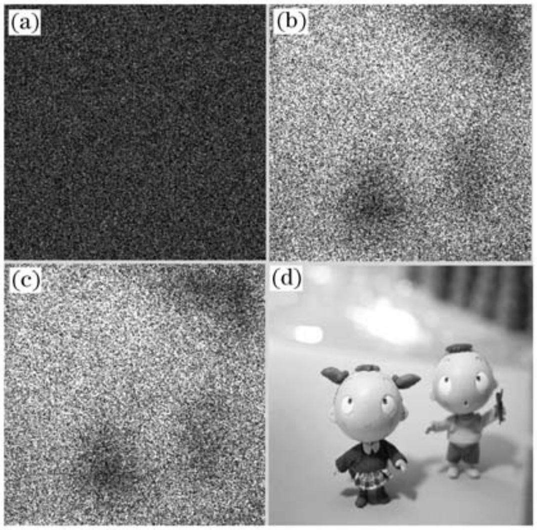

Fig. 5. Retrieved images of the input in Fig. 2(a) with incorrect keys. (a) The principal key is not used; (b) there is a relative error of 0.80% in λ; (c) there is a relative error of 0.80% in d; (d) $n_1(x_0, y_0)$ is not eliminated.

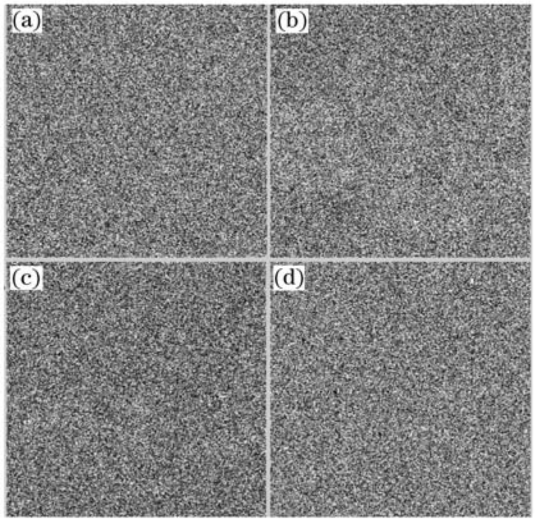

Fig. 6. Retrieved images of the input in Fig. 2(b) with incorrect keys. (a) The principal key is not used; (b) there is a relative error of 0.08% in λ; (c) there is a relative error of 0.08% in d; (d) $n_1(x_0, y_0)$ is not eliminated.

In conclusion, we have proposed an image encryption method based on the principles of JTC and PSI. It can encrypt two images simultaneously, accordingly improve the encryption efficiency of the system greatly. Its simple JTC architecture overcomes the alignment drawbacks existing in the systems based on MZI architecture. Moreover, the complete process can be achieved at high speed optically or digitally, and the series of interferograms involving the information of the encrypted images and the principal key are very suitable for transmission via Internet.

J. Li is the author to whom the correspondence should be addressed, his e-mail address is lijunc@126.com.

References

1. S. Kishk and B. Javidi, Appl. Opt. **41,** 5462 (2002).
2. N. Takai and Y. Mifune, Appl. Opt. **41,** 865 (2002).
3. B. Hennelly and J. T. Sheridan, Opt. Lett. **28,** 269 (2003).
4. B. Javidi and T. Nomura, Opt. Eng. **39,** 2439 (2000).
5. L. Yu, X. Peng, and L. Cai, Opt. Commun. **203,** 67 (2002).
6. B. Yu and X. Peng, Acta Opt. Sin. (in Chinese) **25,** 881 (2005).
7. Y.-Y. Wang, Y.-R. Wang, and Y.-B. Yang, Chin. J. Lasers (in Chinese) **33,** 1360 (2006).
8. M.-Z. He, L.-Z. Cai, Q. Liu, and X.-L. Yang, Appl. Opt. **44,** 2600 (2005).
9. X. F. Meng, L. Z. Cai, M. Z. He, G. Y. Dong, and X. X. Shen, J. Opt. A **7,** 624 (2005).
10. S. K. Gil, S. H. Jeon, N. Kim, and J. R. Jeong, Proc. SPIE **6136,** 613615 (2006).
11. E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi, Appl. Opt. **39,** 2313 (2000).
12. A. E. Shortt, T. J. Naughton, and B. Javidi, Proc. SPIE **5908,** 590811 (2005).
13. C. La Mela and C. Iemmi, Opt. Lett. **31,** 2562 (2006).
14. G. Lu, Z. Zhang, S. Wu, and F. T. S. Yu, Appl. Opt. **36,** 470 (1997).