Optical information authentication of triple-image encryption

Emad A. Mohammed

Laser Applications & Optical Materials Group, Department of Physics, College of Science, University of Basrah, Iraq
emadn73@yahoo.com

Abstract:

In this work, a novel optical triple-image encryption and authentication method based on joint transform correlator and a classical 4*f*-correlator is proposed. By using this method, three images can be encrypted together into one image at the same time. The encrypted image achieved the requirements of simultaneous recognition, invisible content and high secure authentication. Simulation results were presented to verify the validity of the proposed method. Nonlinear operation is also presented to enhance the authentication process of the encrypted data. In addition, the performance of the system demonstrates that the proposed method is feasible and effective to encrypt three images.

http://dx.doi.org/10.31257/2018/JKP/100108

Key words: Optical security and encryption; information authentication; Multiple-image; optical recognition; nonlinear correlation; Fourier optics.

المصادقة البصرية للمعلومات لثلاثة صور مشفره

عماد عبد الزهره محمد

قسم الفيزياء – كلية العلوم – جامعة البصره

الخلاصة:

لقد تم في هذا البحث أقتراح طريقة جديدة لتشفيرومصادقة ثلاثة صور بصريا بالاعتمادعلى وصلة التحويل المتشابكه *JTC* وعلاقة *4f* الكلاسيكية. في هذه الطريقة، تم تشفير ثلاث صور معا في صورة واحدة وفي نفس الوقت. لقد حققت الصور المشفره متطلبات التمييز الآني والمحتوى اللامرئي والمصادقة عالية الأمان. لقد أثبتت نتائج المحاكاة صحة الطريقة المقترحة. وتم استخدام التشابك اللاخطي لتحسين عملية المصادقة البصريه. إن أداء النظام أظهر أمكانية وفعالية الأسلوب المقترح لتشفير ومصادقة ثلاثة صور آنيا.

الكلمات المفتاحيه: التشفير والامن البصري، توثيق المعلومات، الصورالمتعدده، التمييز البصري، التشابك اللاخطي، البصريات الفوريريه.

1. Introduction

Optical information processing techniques are presented for data security applications in communication systems and computer technology extensively in the recent years. Due to high speed of parallel processing and multidimensional capabilities, several optical encryption methods have been proposed [1-3]. A considerable work in this filed is the double random phase encoding (DRPE) technique proposed by Refregier and Javidi [4]. The experimental application of the DRPE has been firstly

fulfilled in a *4f*-processor [5]. Other expansions have been developed in the Fresnel [6], Fractional Fourier [7] and gyrator (GT) domains [8]. In addition, the DRPE has been found vulnerable to some attacks, therefore many improvements have been developed to overcome this difficulties [9-13]. However, this technique is used to encrypt one input image by two random phase masks. In the last years, optical encryption systems are developed into multiple-image encryption (MIE) owing to economic memory occupation and efficient transmission [14-16]. These developments permit to encrypt multiple images in one encrypted image [8, 17] and also store in optical memory [18].

Recently, multiple image encryption (MIE) with quantum imaging or photon-counting has been presented in a single encrypted image [19]. This technique performs security authentication of the data with far fewer photons than conventional techniques. Because the quantum imaging technology does not exit, this technique is still limited and not widespread. In order to overcome this drawback, the MIE with sparse representation are integrated for information authentication which permitted to increase the security of the method and reduced data transmission to achieve the requirements of protection, storage [20].

In this paper, a novel an information verification based on optical triple-image encryption is proposed. The three input images will be firstly encrypted to obtain one encrypted image with similar spatial resolution as the primary images. In the second step, the resultant encrypted for complex-valued distribution is kept for information authentication process. Simultaneous authentication process is presented for triple-image encryption.

In what follows, the method of triple image encryption and authentication processes is described in Section 2. Section 3 describes two numerical simulations, the first one encrypts three images, and the other one verifies the encrypted data. The conclusions are outlined in Section 4.

2. Triple-image encryption and authentication

The principle of triple-image encryption and authentication processes is discussed here. The block diagram of the encryption and authentication method is shown in Fig. 1. The proposed method encrypts three primary images with one random phase mask (RPM) by combined nonlinear joint transform correlator (JTC) and a classical 4*f*-correlator.

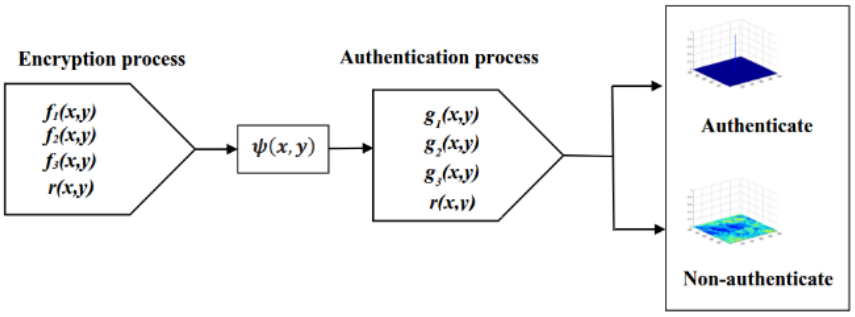


Figure 1: Block diagram of the optical triple image encryption and authentication.

The three input images $O_1(x,y)$, $O_2(x,y)$ and $O_3(x,y)$ are first normalized with maxima as 1 and then phase encoded. The functions containing these images are given by the equations:

$$f_1(x,y) = exp[i\pi O_1(x,y)] \quad (1a)$$

$$f_2(x,y) = exp[i\pi O_2(x,y)] \quad (1b)$$

$$f_3(x,y) = exp[i\pi O_3(x,y)] \quad (1c)$$

where symbol (x, y) is employed to denote the spatial coordinates and $f_1(x,y)$, $f_2(x,y)$ and $f_3(x,y)$ are phase encoded functions.

Suppose $r(x,y)$ is independent random white sequences used to encrypt the information of the images,

$$r(x,y) = exp[i2\pi\rho(x,y)] \quad (2)$$

where $\rho(x,y)$ is normalized positive function distributed in the range [0,1]. Then, the encrypted function $\psi(x,y)$ including the triple images and phase mask will be depicted by the expression:

$$\psi(x,y) = F^{-1}[\, F\{f_1(x,y).f_2(x,y) * f_3(x,y)\} * r(x,y)] \quad (3)$$

where the notation $*$ denotes the convolution operation, F and F^{-1} are the Fourier transform and inverse Fourier transform, respectively.

In the authentication step, let $g_1(x,y)$, $g_2(x,y)$ and $g_3(x,y)$ are the input images and to be compared with the set of reference images $f_1(x,y)$, $f_2(x,y)$ and $f_3(x,y)$, respectively, and let $r(x,y)$ is known by this processor.

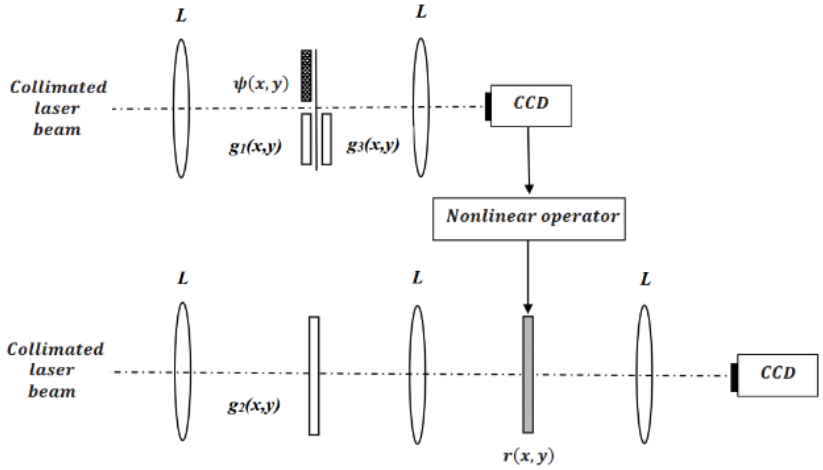


Figure 2: Schematic optical setup for the authentication process. L is lens; CCD: charge coupled device.

To implement the verification authentication, a three-step optoelectronic hybrid setup was carried out, as shown in Fig. 2. In the first, a JTC technique is applied to the encrypted distribution $\psi(x,y)$ which is sited side by side with the first input image $g_1(x,y)$. The second input image $g_2(x,y)$ is putted against the screen, where the $g_1(x,y)$ is placed. Then, the joint power spectrum $I(u,v)$ is recorded by CCD camera in the Fourier plane which can be given by:

$$I(u,v) = |FT\,[\,\psi(x,y) + g_1(x,y)]|^2 \quad (4)$$

where symbol (u,v) is the frequency coordinates. secondly, the joint power spectrum $I(u,v)$ can be digitally modified by a variety of nonlinear technique to adjust the discrimination capability. Therefore, Eq. (4) is converted to

$$NL^{\omega}\{I(u,v)\} = I(u,v)|I(u,v)|^{\omega-1} \quad (5)$$

where the parameter ω describes the strength of the applied nonlinearity, and it can vary from the linear case ($\omega=1$) to the phase extraction case ($\omega=0$). Lastly, the third input image $g_3(x,y)$ was placed in the input plane and the phase mask $r(x,y)$ was placed in the Fourier plane of the 4*f*-classical correlator. Afterward, the resultant nonlinearity of the second step is displayed on the Fourier plane of the 4*f*-system. Thus, the output correlation intensity in the recording plane is recorded

by a CCD camera and can be described by[20]

$$G_3(u,v)\ [\,NL^{\omega}\{I(u,v)\}\,]\,r(u,v) \qquad (6)$$

where a function in capital letter indicates the Fourier transform of the function in small letter. Equation (6) will carry the correlation signals which lead to spatially separated distributions in the output plane. The developments of Eq. (6) will lead to the term of interest for optical processor corresponds to the cross-correlation of the autocorrelation (AC) signals as follows [20]:

$$|AC_{POF}[f_2(x,y)] \otimes AC^{*}_{PPC}[f_1(x,y)f_3(x,y)] \otimes AC^{*}_{CMF}[R(x,y)]|^2 \qquad (7)$$

The symbol $\otimes$ is the cross correlation, sub-indices CMF (classical matched filter), POF (phase-only filter), and PPC (pure phase correlation) represent the kind of filter contributed in the autocorrelation signal [21]. when the input images and the corresponding reference images are correct [$g_1(x,y) = f_1(x,y)$, $g_2(x,y) = f_2(x,y)$ and $g_3(x,y) = f_3(x,y)$] and $\omega=0$, one remarkable peak can be generated in the output plane and a positive validation is satisfied. Also, if the input images compare with reference images are incorrect [$g_1(x,y) \neq f_1(x,y)$, $g_2(x,y) \neq f_2(x,y)$ and $g_3(x,y) \neq f_3(x,y)$], a negative validation occurs and the output is broader and less intensity than the AC peak.

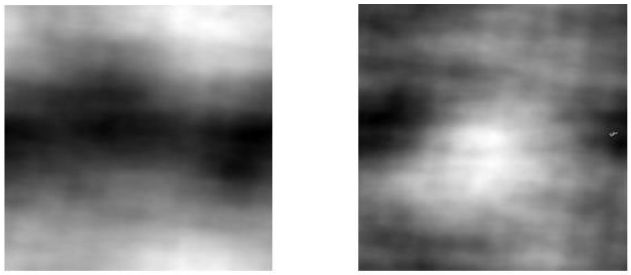
3. Results and discussion

In the encryption process, three grayscale input images are adopted as illustrated in Fig. 3(a), (b), (c) to demonstrate the effectiveness of the proposed method. All images have dimensions of 512 x 512 pixels. The random phase mask was generated in the computer on the platform of MATLAB 8.6.

a b c

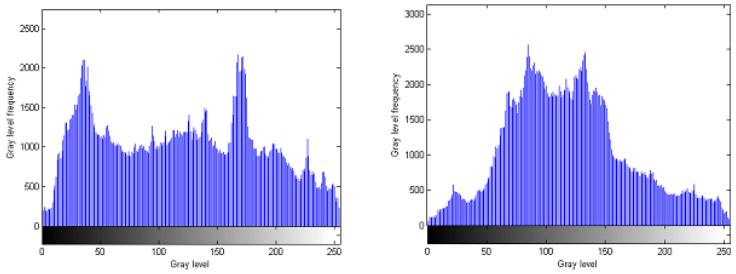
Figure 3: The original images (a), (b) and (c) to be encrypted.

By using Eq. (3), the encrypted image is generated by the three images and phase key. It is clear that the three images are encrypted into one image with white noise amplitude distribution. Fig. 4 shows the amplitude $|\psi(x,y)|$ and phase $\varphi_{\psi}(x,y)$ information of the encrypted image. The histogram of the magnitude and phase encrypted distribution function $\psi(x,y)$ is shown in Fig. 5. The final encrypted distribution $\psi(x,y)$ is used to validate the information of the triple images data.



a b

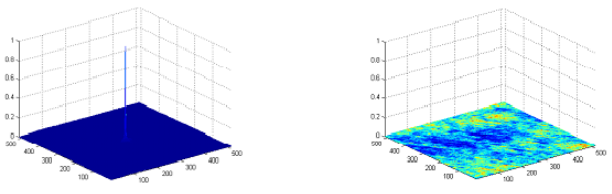
Figure 4: (a) magnitude distribution of the encrypted function (b) phase distribution of the encrypted function.



a b

Figure 5: The histogram of the encrypted distribution $\psi(x,y)$ for (a) magnitude $|\psi(x,y)|$ and (b) phase $\varphi_{\psi}(x,y)$.

In order to validate the proposed method, the output intensity distribution of the encrypted data with phase extraction nonlinearity ($\omega=0$) is computed by Eq. (7). The key phase code $r(x,y)$ is correctly provided from the system database. Fig.6(a) shows the output intensity distribution when input images is matched with correct images [$g_1(x,y) = f_1(x,y)$, $g_2(x,y) = f_2(x,y)$ and $g_3(x,y) = f_3(x,y)$] which confirms that the positive validation. From this figure, a high and sharp autocorrelation peak was observed. Consequently, the system is confirmed the simultaneous verification with free of noise and distortions. Fig. 6(b) depicts the output intensity distribution when the false images as shown in Fig. 7 are used. In this case, only a noisy background was obtained without any remarkable correlation peak [$g_1(x,y) \neq f_1(x,y)$, $g_2(x,y) \neq f_2(x,y)$ and $g_3(x,y) \neq f_3(x,y)$]. Thus, the output intensity distribution had cross correlation signal and confirmed the negative validation. From Fig. 6, it is to be noted that the proposed system has verified the authorized images and reject the unauthorized images.



a b

Figure 6: Authentication of encrypted function; (a) positive validation and (b) negative validation.

Figure 7: The input images (a), (b) and (c) to be compared with the primary reference images of Fig.3(a,b,c).

Any mismatching between the set of input images [$g_1(x,y)$, $g_2(x,y)$ and $g_3(x,y)$] and the set of reference primary images [$f_1(x,y)$, $f_2(x,y)$ and $f_3(x,y)$], leads to a decrease of the output intensity distribution as in Table 1. The obtained results from this table also are confirmed the negative validation when false key phase code is used.

Table 1. Validation processes for optical triple image authentication. Output intensity of correlation value for ω=0.

g_1	g_2	g_3	r	*Correlation value*	*Authorized*
True	*True*	*True*	*True*	*1.0*	*Yes*
False	*True*	*True*	*True*	*0.013*	*No*
True	*False*	*True*	*True*	*0.322*	*No*
True	*True*	*False*	*True*	*0.023*	*No*
True	*True*	*True*	*False*	*0.117*	*No*
False	*False*	*True*	*True*	*0.014*	*No*
True	*False*	*False*	*True*	*0.019*	*No*
True	*True*	*False*	*False*	*0.020*	*No*
True	*False*	*True*	*False*	*0.018*	*No*
False	*True*	*False*	*True*	*0.013*	*No*
False	*True*	*True*	*False*	*0.013*	*No*
True	*False*	*False*	*False*	*0.017*	*No*
False	*True*	*False*	*False*	*0.013*	*No*
False	*False*	*True*	*False*	*0.012*	*No*
False	*False*	*False*	*True*	*0.013*	*No*
False	*False*	*False*	*False*	*0.013*	*No*

To demonstrate the effect of the parameter ω, the output intensity distribution was computed at different nonlinearities as illustrated in Figs. 8. Figs. 8(a)-(e) show the positive validation while Figures 8(f)-(j) show the negative validation at ω=0.1, 0.3, 0.5, 0.7 and 0.9, respectively. The results indicated that the nonlinear parameter effected in the performance of the correlation system. Therefore, the ω<0.5 can be achieve a good result for optical security system.

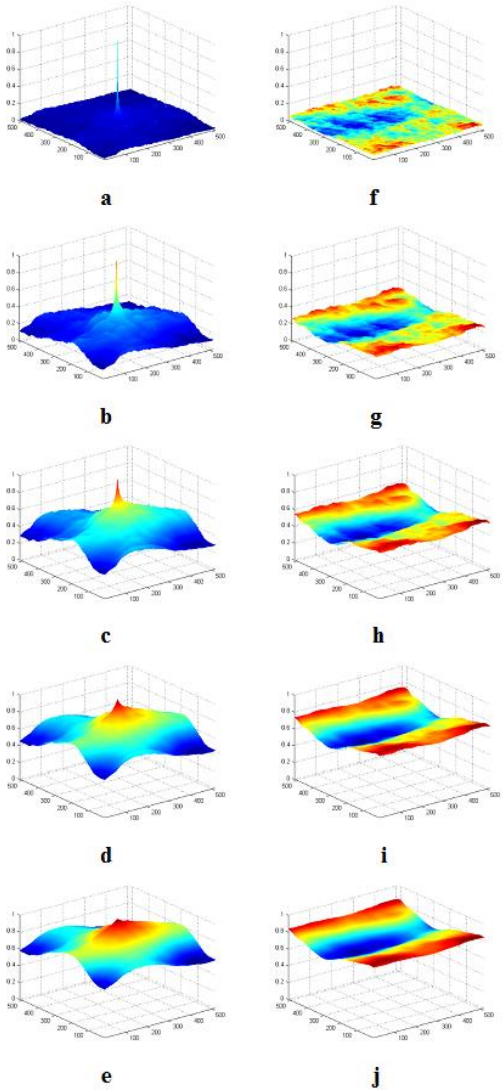


Figure 8: The effectiveness of the nonlinear operator; (a)-(e) positive validation for ω=0.1, 0.3, 0.5, 0.7 and 0.9, respectively, and (f)-(j) negative validation for ω=0.1, 0.3, 0.5, 0.7 and 0.9, respectively.

4. Conclusion

An optical triple-image encryption and authentication method by using JTC and 4*f*-system was proposed. This method can encrypt three grayscale images into one image at the same time. The resulting encrypted function can be verified by introducing the nonlinear operation in the Fourier plane for authentication stage. The simulation results have been performed to verify its validity. The results demonstrate that the nonlinear parameter is effective in the performance of the correlation system. Therefore, the value of the nonlinear parameter (ω) should be less than 0.5 to achieve the best system performance. Finally, it is concluded that the results demonstrated the feasibility and effectively of the three image encryption and authentication method.

References

[1] W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," *Adv. Opt. Photon,* vol. 6, pp. 120-154, 2014.

[2] S. Liu, C. Guo, and J. T. Sheridan, "A review of optical image encryption techniques," *Opt. & Las. Tech.* , vol. 57, pp. 327-342, 2014.

[3] B. Javidi, "Roadmap on optical security," *J. Opt.,* vol. 18, pp. 83001-83039, 2016.

[4] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.,* vol. 20, pp. 767-769, 1995.

[5] J. W. Goodman, *Introduction to Fourier Optics*, 3rd ed.: McGraw-Hill, 2004.

[6] G. Situ, G. Pedrini, and W. Osten, "Strategy for cryptanalysis of optical encryption in the Fresnel domain," *Appl. Opt.,* vol. 49, pp. 457-462, 2010.

[7] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Opt. Lett.,* vol. 25, pp. 887-889, 2000.

[8] Z. Liu, H. Chen, T. Liu, P. Li, J. Dai, X. Sun, *et al.*, "Double-image encryption based on the affine transform and the gyrator transform," *J. Opt.,* vol. 12, p. 035407, 2010.

[9] A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," *Opt. Lett.,* vol. 30, pp. 1644-1646, 2005.

[10] U. Gopinathan, D. S. Monaghan, T. J. Naughton, and J. T. Sheridan, "A known-plaintext heuristic attack on the Fourier plane encryption algorithm," *Opt. Express,* vol. 14, pp. 3181-3186, 2006.

[11] P. Kumar, J. Joseph, and K. Singh, "Known-plaintext attack-free double random phase-amplitude optical encryption: vulnerability to impulse function attack," *J. Opt.,* vol. 14, p. 045401, 2012.

[12] X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," *Opt. Lett.,* vol. 31, pp. 1044-1046, 2006.

[13] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," *Opt. Express,* vol. 15, pp. 10253-10265, 2007.

[14] M. S. Millán, E. Pérez-Cabré, and B. Javidi, "Multifactor authentication reinforces optical security," *Opt. Lett.* , vol. 31, pp. 721-723, 2006.

[15] A. Alfalou and A. Mansour, "A new double random phase encryption scheme to multiplex and simultaneous encode multiple images," *Appl. Opt.,* vol. 48, pp. 5933-5947, 2009.

[16] R. Tao, Y. Xin, and Y. Wang, "Double image encryption based on random phase encoding in the

fractional Fourier domain," *Opt. Express*, vol. 15, pp. 16067-16079, 2007.

[17] Z. Liu and S. Liu, "Double image encryption based on iterative fractional Fourier transform," *Opt. Commun.*, vol. 275, pp. 324-329, 2007.

[18] O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," *Opt. Lett.*, vol. 24, pp. 762-764, 1999.

[19] E. Pérez-Cabré, E. A. Mohammed, M. S. Millán, and H. L. Saadon, "Photon-counting multifactor optical encryption and authentication," *J. Opt.*, vol. 17, p. 025706, 2015.

[20] E. A. Mohammed and H. L. Saadon, "Optical double-image encryption and authentication by sparse representation," *Appl. Opt.*, vol. 55, pp. 9939-9944, 2016.

[21] B. V. K. V. Kumar and L. Hassebrook, "Performance measures for correlation filters," *Appl. Opt.*, vol. 29, pp. 2997-3006, 1990.