Asymmetric Optical Cryptosystem in the Fractional Fourier Domain Using Photon Counting Imaging

Rafid A. Jassim[1,2,*], Emad A. Mohammed[2]

1. Laser Applications Research Group (LARG), Department of Physics, College of Science, University of Basrah, Basra, Iraq

2. College of Higher Studies, University of Basrah, Basra, Iraq.

*Corresponding author E-mail: rafid.jasim.sci@uobasrah.edu.iq

Doi:10.29072/basjs.202202178

ARTICLE INFO **ABSTRACT**

Keywords:

Optical information security, Double Random Phase Encryption, optical encryption and authentication, Fractional Fourier transform, Photon counting.

By extending the space of the keys, the double random phase encryption approach based on the Fractional Fourier domain improves optical security systems. A novel method for optical security is proposed in this paper. The method is based on combining photon counting (PC) imaging with double random phase encryption (DRPE) in the Fractional Fourier (FrFT) domain. Photon counting is used to generate sparse data from the encrypted amplitude function. Not only does integration improve the security system's resistance to intruder attacks, but it also minimizes information data for better meeting storage and transmission needs. The optical Asymmetric cryptosystem has been offered since the proposed method's encryption step differs from the decryption stage due to the use of photon counting imaging. Only the encrypted image's sparse data will be maintained during the decryption procedure. Wherever the generated image is unrecognizable and is not a replica of the original image As a result, to validate the sparse information, a non-linear optical correlation approach is demonstrated. The discrimination ratio measure is evaluated for different values of the number of photons (Np) and the nonlinear parameter to test the system's verification procedure (k). The simulation results show that the proposed solution is effective and practicable, and that it can increase the level of protection for optical security systems.

Received 24 July 2022; Received in revised form 19 Aug 2022; Accepted 26 Aug 2022, Published 31 Aug 2022

1. Introduction.

Many researchers were attracted by optical techniques, especially after the publication of the first method in this field, which is called double- random phase encoding[1]. Optical encryption techniques use many transformations such as classical Fourier transform (FT), fractional Fourier transform (FrFT)[2], Fresnel transform (FST) [3], gyrator transform (GT)[4], and Wavelets transform [5]. In order to control the information meaning of image in a nonlinear and indiscriminate style, photon counting technique is applied [6, 7]. The Photon Counting is combined with optical security system to safe image encryption and authentication[8]. To boosts the security of the encryption and verification versus attacks, the photon counting is applied to the amplitude encrypted data. [9]. Furthermore, PC technique can be influenced by the original or encoded image and if its effected by the original data, a photon-limited image with only a few pixels is secured. The confidential information of the original image is hiding from visual observation (information hiding) by applying PC. Otherwise, a sparse encoded distribution is produced if PC effected to the encoded image, and lead to information compression by reduce the transmitted/stored information. In this paper the combination of DRPE in the Fractional Fourier domain is presented. Firstly, the input data will be encrypted with DRPE in FrFT domain. Then, the sparse data will be generated randomly from the cipher data by using photon counting technique. In the decryption stage, the decipher data is completely unrecognizable. Thus, the decrypted data will be intended for verification but not direct visualization. The proposed scheme is demonstrated that it is feasible and more robust that the tradition DRPE-FrFT.

The paper is organized as follows: In section 2 the encryption and decryption processes in the Fractional Fourier domain is presented. In section 3 numerical results of image encryption and verification with photon counting are given. In section 4 the evaluation of discrimination ratio is presented to verify the capability of the proposed method. Finally, the conclusion is given in section 5.

2. Theoretical analysis

2.1 DRPE in the Fractional Fourier transform (FrFT)

In the first, let us recall the definition of Fractional Fourier transform in one dimensional coordinates for simplicity[10]. The FrFT is mathematically defined as a linear canonical integral transform. The FrFT parameters *a*, *b*, and α of one dimensional function *f(x)* can be written in the following form[2]:

$$\mathrm{g}(u) = K \int f(x)\, R_1 \times exp\left(i\pi \frac{a^2x^2 + b^2u^2}{tan\,\alpha} - i2\pi \frac{abux}{sin\,\alpha}\right) dx \qquad (1)$$

where the R_1 is random phase code and represented by R_1 = $exp\,[i\phi_1(u)]$, $\phi_1(u)$ is a random white sequence uniformly distributed in the interval [0,2π], and g(u) is distribution encoded by R_1. The quantities *a*, *b*, and *α* represent three complex parameters of FrFT and *K* denote a complex constant. Action FrFT spanning a function is equivalent to expanding the function *a* times, FrFT execution of the command *a*, contracting the resulting distribution *b* times. The distances d_1 and d_2 and focal length f_1 of the lens are related to the parameters *a*, *b*, and *α* by the relations [2]:

$$a^2 = \frac{1}{\lambda}\frac{\sqrt{f_1 - d_2}}{\sqrt{f_1 - d_1}}\frac{1}{\left[{f_1}^2 - (f_1 - d_1)(f_1 - d_2)\right]^{1/2}} \qquad (2)$$

$$\alpha = \mathrm{arc\,cos}\left[\frac{\sqrt{\mathrm{f}_1 - \mathrm{d}_1}\sqrt{\mathrm{f}_1 - \mathrm{d}_2}}{\mathrm{f}_1}\right] \qquad (3)$$

$$b^2 = \frac{1}{\lambda}\frac{\sqrt{f_1 - d_1}}{\sqrt{f_1 - d_2}}\frac{1}{\left[{f_1}^2 - (f_1 - d_1)(f_1 - d_2)\right]^{1/2}} \qquad (4)$$

where λ is wave length for light source. The encrypted data for DRPE in the FrFT domain can be written as[2]:

$$\psi(\mathrm{x}) = \mathrm{F}^{\,\beta}\{\mathrm{F}^{\,\alpha}\{[\mathrm{f(x)}\times \mathrm{R}_1(\mathrm{x})] \times \mathrm{R}_2(\mathrm{u})\}\} \qquad (5)$$

where F is Fourier transform, β is the Fractional order in the output plane and, $R_{1,2}$ are the random phase codes represented by $R_2 = \exp[i\varphi_2(u)]$, in Fractional domain. $\varphi_2(\,)$ are the random white sequence uniformly distribution in the interval (0,2π) and are statistically independent.

When (α = 0) or (β = 0) it corresponds to the Identity transform and when (α = π/2) or (β = π/2) the Fractional transformation will be converted to the traditional Fourier transform, but when (α = π) or (β = π), we will get the inverse transformation and the inverse Fourier transform can be obtained If (α =-π/2) or (β = -π/2). Here, α and β are considered for the retrieval of original information in addition to the use of RPMs. For decryption, the encryption process is reversed to obtain the original information.

2.2. Photon Counting Imaging (PC)

The number of incident photons can be expected on an image captured by PC technique. Therefore, the low-photon image will have less information than the original image[11]. In general, the Poisson distribution can be show the probability of enumeration l_j photons at pixel j[11].

$$\mathrm{P}(l_j, \lambda_j) = \frac{[\lambda_j]^{l_j} e^{-\lambda_j}}{l_j\,!} \text{ , for } \lambda_j > 0 \text{ , } l_j \in \{0,1,2, \dots\} \qquad (6)$$

where the Poisson parameter λ_j is given by $\lambda_j = N_p\ g(x_j)$, with $g(x_j)$ being of the normalized irradiance at pixel x_j like that $\sum_{j=1}^{m} g(x_j) = 1$ and m equivalent to the total number of pixels in the image. The input image has a real value while the encoded image has a complex values and the PC can be applied on both. By applying the equation (6) on normalized real image $[g(x) = f(x) \,/\, \sum_{j=1}^{m} f(x_j)]$, we get the photon-limited image $f_{ph}(x)$, where $f(x)$ is a real value image. While a photon-limited amplitude information $|E(x)|$, is generated from the normalized amplitude image $g(x) = |E(x)| \,/\, \sum_{j=1}^{m} |E(x_j)|$ by applying the equation (6) on a complex-valued encoded image *(E(x))*. It is required that the pixels receive at least one photon count.

2.3 Integration of the PC with the DRPE in the FrFT

The proposed method in this work is based on the process of integrating DRPE in the Fractional Fourier domain with Photon Counting Imaging (PC); the main purpose of this integration is information verification, not retrieval as is done in traditional optical encryption using DRPE. There is also another purpose of this integration, which is to reduce the size of the information to be stored or transmitted. In this paper, numerical results are employed to test the capability and security of the proposed method. All the images and RPMs (keys) have 512*512 pixels. The scheme has been tested by executing the scheme on personal computer with configuration Intel(R) Core (TM) i5-7200 CPU @ 2.5 GHz-2.71 GHz, 8GB RAM running Windows 10 on MATLAB (R2017b).

3. Results and discussions

3.1 Encryption Process

The encryption process in this work is carried out using the DRPE method in the fractional Fourier domain and using the coefficients (α =0.75) and (β =0.9), which append an additional degree of the security to the proposed system by moving the lenses used in the traditional *4f* system with specific dimensions**.** The binary image has been studied in the figure 1(a) also shows the random phase masks (RPM1 and RPM2), which are used as keys. After applying the equation (5), we get the encrypted image, as shown in figure 1(d), which are randomly distributed functions with complex values. The decrypted is retrieved with the corrects keys (RPMs), fractional parameter, and wave length as shown in Fig.1(d). To study the performance of DRPE-FrFT method, the quality parameters are computed and compared with the traditional DRPE parameters in Fourier domain. Table (1) illustrates the results of the test for the quality parameter (MSE, RMSE, PSNR and Entropy). From the table, we can see the convergence of the results between the classical DRPE in FT domain and the DRPE in FrFT domain.

Table 1: Values of the image quality encryption parameters in the Fourier and Fractional Fourier domains

	FT	FrFT
MSE	8.7141e-32	2.39619e-31
RMSE	5.1336e-16	3.9513e-16
PSNR	364.18	361.02
Entropy for PT	0.3079	0.3079
Entropy for Enc.	6.7623	7.6887

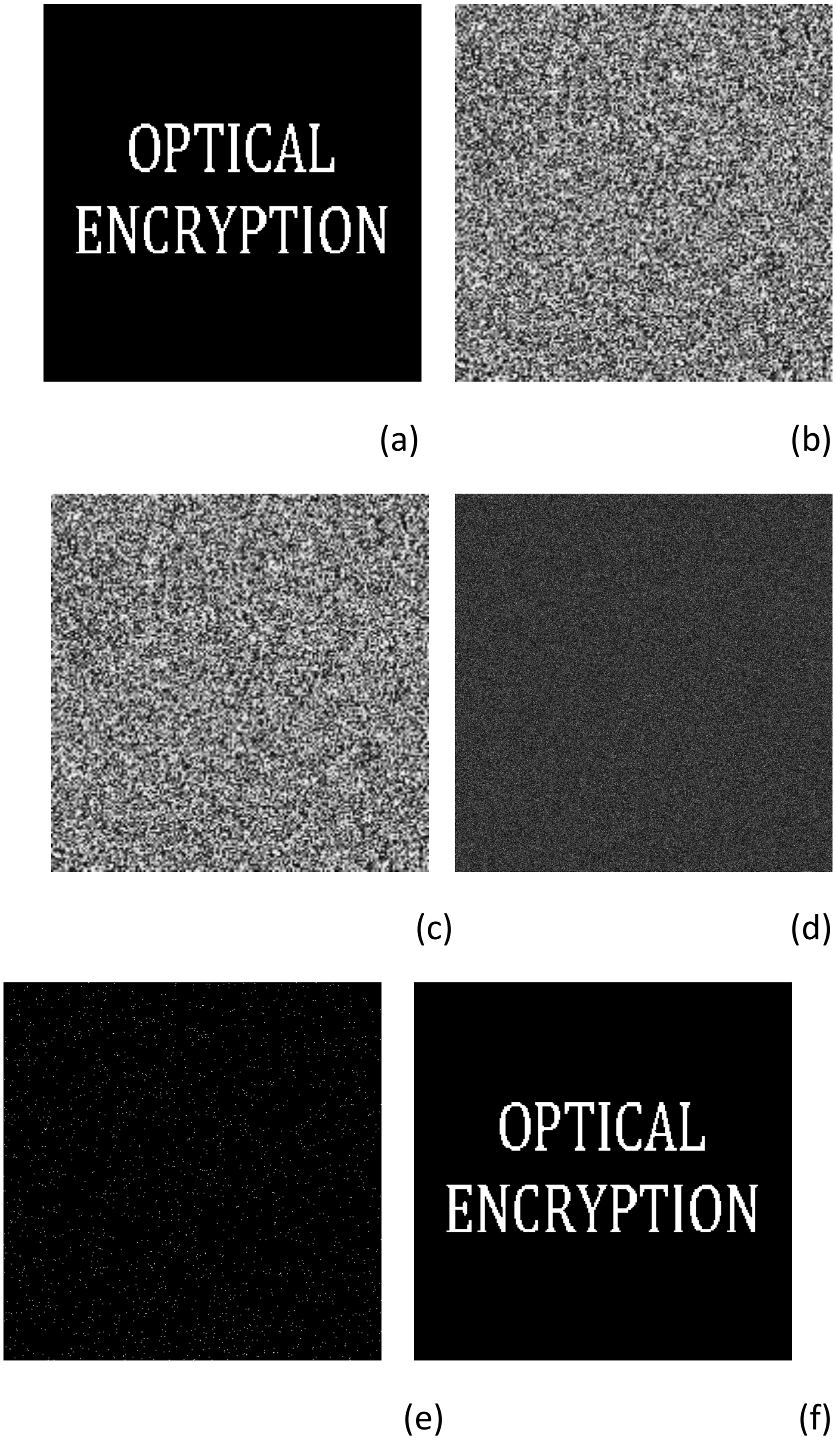

Fig.1: Binary image encryption process: (a) The original binary image. (b) and (c) the phase masks used (keys) (d) The amplitude encrypted image |ψ(x)| (e) The phase encrypted image $\varphi_{\psi}(x)$ (e) The decrypted image

To evaluate the Fractional parameters (α,β) of DRPE-FrFT, we demonstrate the effect of these parameter by computing the root mean squared error (RMSE) between the decrypted image and original image [12-14].The results are given in Fig.2, which depicts that the RMSE values are very small for all values of α and β, expect zero had large values. It may be seen that the RMSE is higher just when the α and β equal to zero, Thus, we can use different values of it. α =0.75 and β =0.9 are considered in this work to satisfy our results with the rest which are published in this field.

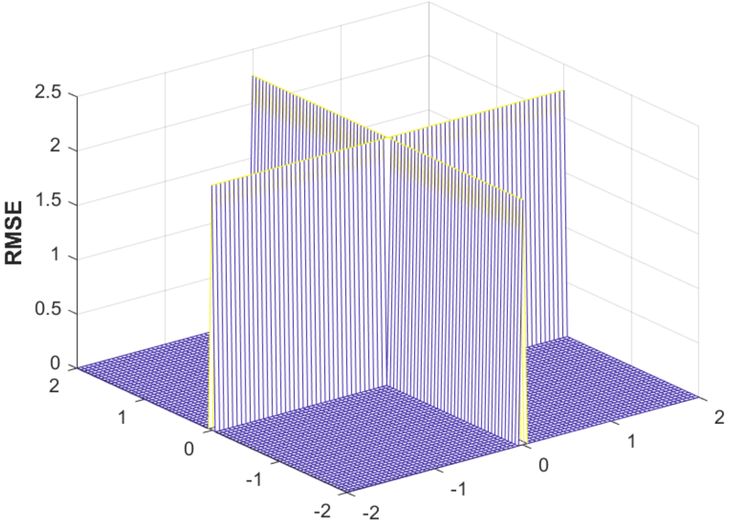

Fig. 2: RMSE values corresponding to the values of α and β

In order to obtain a photon limited encrypted image $\psi_{ph}(x)$,we applied PC technique with a number of photon counts Np over the amplitude value of the encrypted image ($|\psi(x)|$) by using the equations in section 2.2. To validate the encrypted information of the images, the images with the selected photons is decrypted using the equation (5). It is noted from the recovered image that it is still noisy, and its information cannot be identified by direct view; therefore, another degree of security has been added to the system to be more secure against illegal attackers. The (PC) technology has also contributed to reducing the information that is intended to be transmitted or stored in the future. After the decryption process, the recovered image cannot be verified by the truth of its information except through the use of one of the verification methods. An example of this, Is the method of the nonlinear correlation filter, and accordingly, the k^{th} filter will be used in our work because its simplicity and ease of application in practice.

The nonlinear correlation is obtained by using the equation[15]:

$$c(x) = F^{-1}\{\left|F_{ph}(u)F(u)\right|^{k} \exp[\mathrm{i}\phi_{ph}(u) - \phi(u))]\} \qquad (7)$$

Where F^{-1} is inverse Fourier transform, $F_{ph}(u)$ Fourier transform for decrypted image after applying PC, $F(u)$ Fourier transform for input image, the k^{th} parameter k ∈[0,1] represents the strength of the applied nonlinearity, $\phi_{ph}(u)$ is Fourier transform for phase decrypted image, $\phi(u)$ is Fourier transform for phase input image. In this process, the decrypted image is compared with the original image to verify the encrypted information. Figure 3(a) shows the retrieved image which is compared with the original binary image (Fig. 3(b)) and fake binary image (Fig.3(d)). when the images are identical, the output of the correlation process was high and sharp as in Fig.3(c), and this represents the positive verification process despite the significant reduction in information as a result of using photon counting technique. And, when the images are not identical, as in Fig.3(d), where the recovered image was compared with a fake image, the results showed a noisy back ground in the correlation peak, and it represents the negative verification process as shown in Fig.3(e).

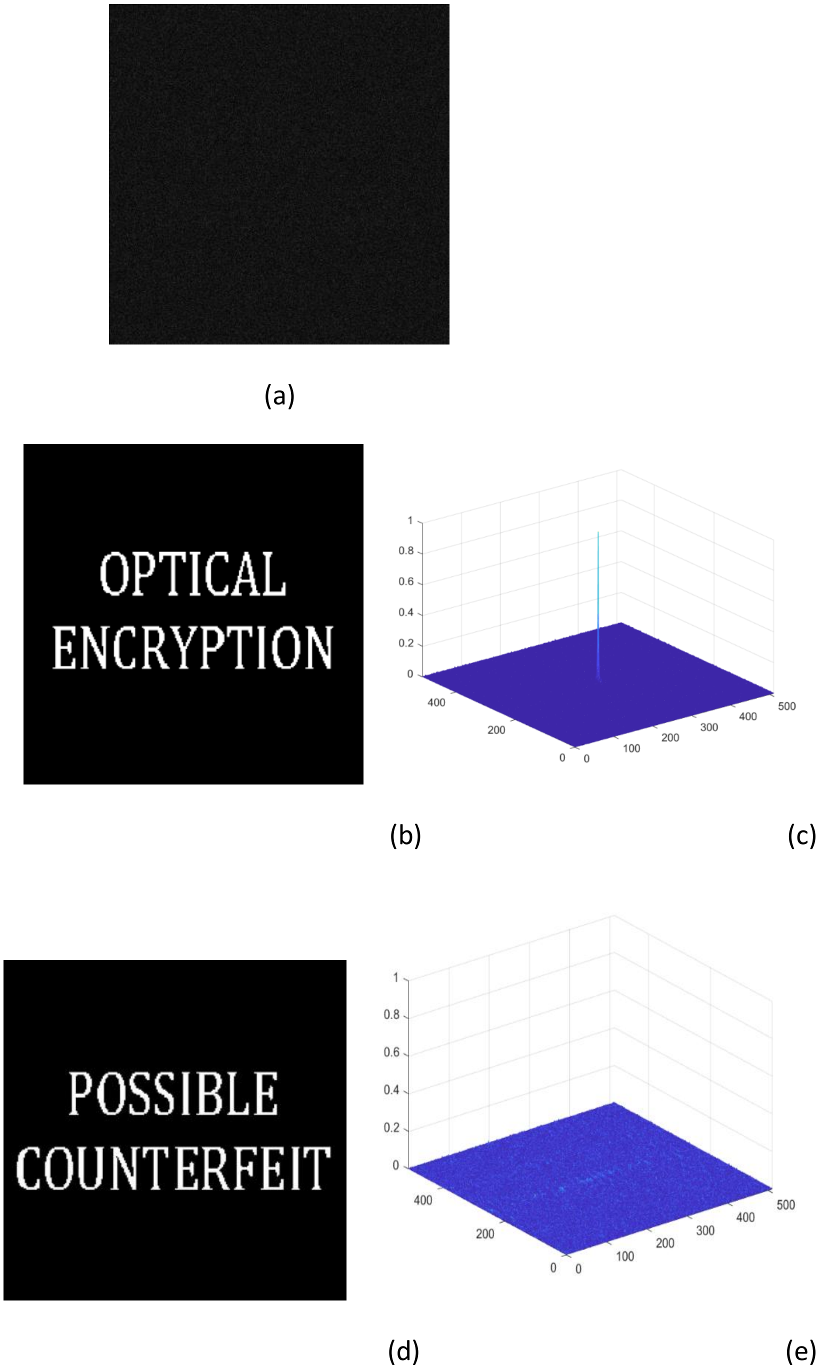

Figure 3: (a) The decrypted image. (b) The original image. (c) The correlation distribution of the binary image when the recovered image compared with the original image. (d) The fake image. (e) Correlation distribution when the retrieved image compared with fake image.

4. Performance of the Verification System

To create the most suitable nonlinearity and the most suitable number of photons that give the best performance of the proposed DRPE-FrFT-PC system, one metric is going to be used: the discrimination ratio. To evaluate the performance of pattern recognition systems based on optical correlation, it used DR measurements. Where the ratio between the maximum peak value of the cross-correlation, CC, and the maximum peak value of the autocorrelation is defined as DR parameter[16]:

$$\mathrm{DR} = \left|1 - \frac{\mathrm{CC}}{AC}\right| \tag{8}$$

The information about the ability of a recognition system to distinguish small differences between objects provides by DR parameter. The performance of the proposed method in terms of DR has been analyzed from the results obtained for a set of 20 numerical experiments. Then, the mean and standard deviation of the DR coefficients are calculated, in order to avoid the impact of random processes in the Poisson distribution. Fig.4 shows the DR values computed for a set of numerical simulations against the number of photons *Np* and for different values of the nonlinear correlation factor *k*. The standard deviations of the numerical simulations allow inaccuracies to be estimated. The value of DR = 0.5 is adopted as a critical value for evaluating this parameter. The DR had been studied for k values less than 0.5 because the values higher than that do not give positive results. From Fig.4, we notice that the DR values are good when *Np*=3000 and *k*=0.4. Accordingly, it can be concluded that 1% of the encrypted data is sufficient to obtain effective verification. This means that the use of photon counting imaging technology and its combination with random phase encryption in the Fourier partial domain, led to a significant reduction in the information to be transmitted or stored, and this is one of the most important goals of optical encryption**.**

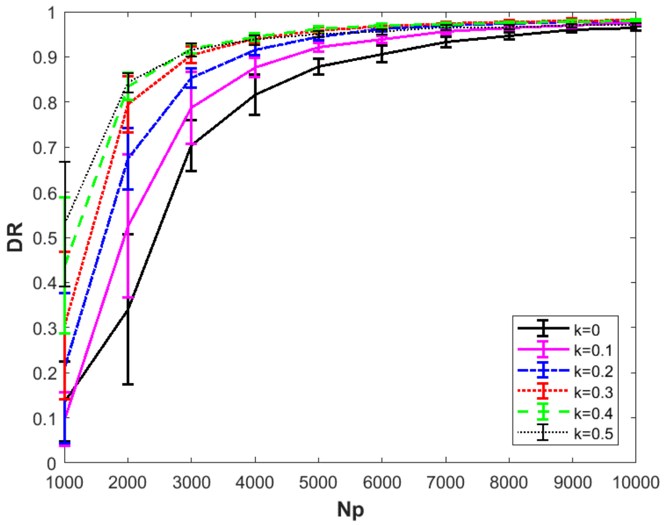

Figure 4: DR values corresponding to the number of photons (Np) and different values of nonlinearity coefficient (k) in the DRPE-FrFT-PC

5. Conclusions

The optical double-phase random encrypted method (DRPE) is one of the most important optical encryption methods, but it is implemented in many transformative fields which is suffer from weakness due to the linearity of this method. In this work, a new optical encryption method is proposed based on the combination of DRPE in the FrFT with PC imaging technique, in order to increase the safety of this method to break the linearity found in the traditional method.

The following are the most important conclusions obtained during this work:

1. It is possible to integrate the DRPE in the FrFT domain with the photon counting technique. The results showed the high effectiveness of this integration.
2. The process of merging the double-phase random encryption method in FrFT domain with the photon counting technique increases the area of encryption keys and thus enhances the security of the optical encrypted data by six additional keys (*λ, α, a, b, k, Np*) in addition to the presence of the original keys which are the random phase masks $RPM_1$and RPM_2

3. The proposed method is considered as a one of the optical asymmetric cryptosystems (OAC) systems, where the encryption process is not identical to the decryption process by achieving the principle of asymmetry and by applying the photon counting technique.
4. The number of photon equal to 3000 and the nonlinear parameter k=0.4, presented good results for performance parameter DR.

References

[1] P. Refregier, B. Javidi, Optical image encryption based on input plane and Fourier plane random encoding, Opt. Lett., 20 (1995) 767-769. https://doi.org/10.1364/OL.20.000767

[2] G. Unnikrishnan, J. Joseph, K. Singh, Optical encryption by double-random phase encoding in the fractional Fourier domain, Opt. Lett., 25 (2000) 887-889.

https://doi.org/10.1364/OL.25.000887

[3] G.S.a.J. Zhang, Double random-phase encoding in the Fresnel domain, Opt. Lett., vol. 29 (2004)1584-1586. https://doi.org/10.1364/OL.29.001584

[4] H. Singh, Security-enrichment of an asymmetric optical image encryption-based devil's vortex Fresnel lens phase mask and lower upper decomposition with partial pivoting in gyrator transform domain, Opt. Quantum Electron., 53 (2021) 1-23. https://link.springer.com/article/10.1007/s11082-021-02854-7

[5] S. Liu, C. Guo, J.T. Sheridan, A review of optical image encryption techniques, Opt. Laser Technol. 57 (2014) 327-342.https://doi.org/10.1016/j.optlastec.2013.05.023

[6] S.K. Rajput, D. Kumar, N.K. Nishchal, Photon counting imaging and phase mask multiplexing for multiple images authentication and digital hologram security, Appl. Opt., 54 (2015) 1657-1666.https://doi.org/10.1364/AO.54.001657

[7] S.K. Rajput, N.K. Nishchal, Optical asymmetric cryptosystem based on photon counting and phase-truncated Fresnel transforms, J. Mod. Opt., 64 (2017) 878-886.https://doi.org/10.1080/09500340.2016.1265677

[8] E.A. Mohammed, H.L. Saadon, Optical double-image encryption and authentication by sparse representation, Appl Opt., 55 (2016) 9939-9944.

https://doi.org/10.1364/AO.55.009939

[9] Y. Frauel, A. Castro, T.J. Naughton, B. Javidi, Resistance of the double random phase encryption against various attacks, Opt. Express, 15 (2007) 10253-10265.https://doi.org/10.1364/OE.15.010253

[10] O.S. Faragallah, H.S. El-sayed, A. Afifi, W. El-Shafai, Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform, Opt. Lasers Eng., 137 (2021) 106333.https://doi.org/10.1016/j.optlaseng.2020.106333

[11] A. Hazer, R. Yıldırım, A review of single and multiple optical image encryption techniques, J. Opt., (2021).https://doi.org/10.1088/2040-8986/ac2463

[12] E. A. Mohammed, Optical information authentication of triple-image encryption, kufa J. Phys., 10 (2018) 60-67. http://dx.doi.org/10.31257/2018/JKP/100108

[13] E.A. Mohammed, H.L. Saadon, Simultaneous verification of optical triple-image encryption using sparse strategy, J. Phys.: Conference Series, 1234 (2019) 012037.https://doi.org/10.1088/1742-6596/1234/1/012037

[14] E.A. Mohammed, H.L. Saadon, Sparse phase information for secure optical double-image encryption and authentication, Opt. Laser Technol., 118 (2019) 13-19.https://doi.org/10.1016/j.optlastec.2019.04.035

[15] B. Javidi, Nonlinear joint power spectrum based optical correlation, Appl. Opt., 28 (1989) 2358-2367.https://doi.org/10.1364/AO.28.002358

[16] S.K. Rajput, D. Kumar, N.K. Nishchal, Photon counting imaging and polarized light encoding for secure image verification and hologam watermarking, J. Opt., 16 (2014) 125406.https://doi.org/10.1088/2040-8978/16/12/125406

منظومة التشفير البصري الغير متماثل في نطاق فورير الجزئي بأستخدام تقنية تصوير العد الفوتوني

المستخلص

إنّ طريقة التشفير بالطور العشوائي المزدوج المعتمدة على نطاق فورير الجزئي تعمل على تعزيز آمن المنظومات البصرية عن طريق زيادة مساحة المفاتيح. في هذا العمل، تم اقتراح طريقة جديدة للأمن البصري تعتمد على الدمج بين تقنية تصوير العد الفوتوني (PC) وطريقة التشفير بالطور العشوائي المزدوج (DRPE) في نطاق فورير الجزئي (FrFT). لقد تم انشاء بيانات متناثرة من خلال تطبيق تقنية العد الفوتوني على سعة الدالة المشفرة. إنّ هذا الدمج لا يزيد متانة آمن النظام ضد هجمات المتطفلين فقط، وانما يعمل على تقليص حجم بيانات المعلومات المراد تخزينها ونقلها بشكل أفضل أيضاً. لقد تم تقديم نظام تشفير بصري غير متماثل في الطريقة التي تم اقتراحها لكون عملية التشفير لا تشابه عملية فك التشفير بسبب تطبيق تقنية العد الفوتوني. لقد تم اعتماد البيانات المتناثرة للصورة المشفرة خلال عملية فك التشفير. بالاضافة الى ذلك، فإنّ الصورة الناتجة تكون غير واضحة المعالم ولايمكن تمييزها وليست نسخة من الصورة الاصلية. وعليه تم استخدام طريقة الترابط البصري غير الخطي للتحقق من مصداقية المعلومات المتناثرة. ولإختبار قابلية التحقق للمنظومة، تم حساب نسبة التمايز (DR) ولقيم مختلفة من عدد الفوتونات (Np) ومعامل اللاخطية (k). لقد برهنت نتائج المحاكاة أنّ الطريقة المقترحة فعالة ومناسبة، وبإمكانها توفير حماية اضافية لأنظمة الآمن البصري.