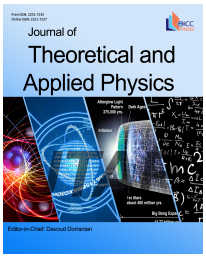

Volume 19, Issue 1, 192508 (1-10)

Journal of Theoretical and Applied Physics (JTAP)

https://doi.org/10.57647/j.jtap.2025.1901.08

Secure optical image encryption and authentication based on phase information and Collins diffraction transform

Israa Mohammed Qasim[1,*], Emad Abdulzahra Mohammed[2]

[1]*General Directorate of Education in Basrah, Ministry of Education, Iraq.*
[2]*Department of Physics, College of Science, University of Basrah, Iraq.*

[*]**Corresponding authors:** israaqasim92@gmail.com

Original Research

Received:
20 November 2024
Revised:
30 December 2024
Accepted:
3 January 2025
Published online:
10 February 2025

Abstract:

In this work, an optical asymmetric scheme for image encryption and authentication is proposed. Our proposal uses an information authentication process for phase encrypted data in the Collins diffraction domain. A partial phase component of the optical image encrypted is used in the decryption stage to validate the grayscale encrypted data. Meanwhile, the use of phase component will be facilitating the design and implementation of optical encryption schemes. The limited phase data makes the scheme more secure owing to difficult reorganization of the confidential information. In addition to security increases, a reduction of encrypted data is achieved by selecting some parts of the phase component of the encrypted data for the decryption process. Therefore, this development strategy efficiently facilitates optical information transfer and storage. Numerical simulations verify the resistance of the system against noise, cropping attacks, and potential attacks.

Keywords: Optical image encryption; Collins diffraction transform; Phase information; Nonlinear optical correlation

1. Introduction

In the digital age, securing information shared over the internet has become increasingly challenging, particularly with the widespread use of social media. This data can be easily accessed by malicious individuals if transmitted through unsecured channels. Moreover, attackers can gain access to personal information such as credit card numbers, passports, and other identity related data, which can be used for illegal activities. To prevent such breaches, encryption algorithms are essential for ensuring data privacy and security. Over the last few decades, there has been growing interest among researchers in information encryption techniques based on optical principles because of their unique advantages [1–5]. One such technique is the double random phase encryption (DRPE), which was firstly proposed by Javidi group of the University of Connecticut in 1990s to convert an image into a noise-like pattern in the Fourier domain [6]. This phenomenal technique has garnered significant attention among researchers in the area of optical image encryption and has been further developed and extended into many domains such as fractional Fourier domain [7, 8], Fresnel domain [9], gyrator domain [10–12], Collins diffraction domain [13–19], and gyrator wavelet transform domain [20, 21]. These series of extensions have enabled the researchers to apply the DRPE method to a wide range of application from secure image transmission to optical data storage.

Despite this, cryptanalysis studies have revealed that the DRPE-based schemes are susceptible to various attack attacks owing to their inherent linearity [22–26]. Therefore, several nonlinear operations have been applied to the traditional 4 focal length (4-f) optical system in order to break down the linearity and increase the security level, such as phase truncated technique (PT) [27, 28], pixel scrambling operator [29], compressive sensing [30, 31], s-box [16, 32], sparse strategy [14, 33–35].

Moreover, in previous years, several optical authentication approaches in conjunction with image ciphering systems have been proposed which can add an extra level of security to information transmissions [36–39]. In the authentication systems based on the sparse strategy, the decrypted image could not be recognized visually but it was verified using a nonlinear correlation algorithm. Thus, this procedure confuses an attacker and enhances the security of the encryption system. In spite of their respective features, the aforemen-

tioned schemes still possess some shortcomings regarding complex ciphering operations, difficulty in the distribution of keys, and practical execution challenges.

This paper presents an innovative optical asymmetric scheme for image encryption and authentication that employs partial phase components obtained from a double random phase encrypted image data in the Collins diffraction domain (CDD). The proposed approach preserves only a small part of the phase of the ciphered information while removing all the amplitude information. In this instance the decrypted image visually unrecognizable, thereby enhancing the security of the cryptosystem. Nonetheless, the decrypted image can be authenticated utilizing a nonlinear optical correlation technique. The phase only component of encrypted data will be considered in this work because optical systems are relatively insensitive to phase variations and can tolerate small errors or perturbations in the phase values.

Moreover, this approach shows that even a small part of the phase of the encrypted information is sufficient for successful image authentication. Therefore, the proposed method enhances the efficiency of optical information transmission and storage by utilizing only portion of the ciphered data. It has been demonstrated to be both effective and feasible, offering an extra layer of security for optical systems.

The outline of this paper is arranged as follows. Section 2 provides the detailed theoretical background of the Collins diffraction transform and authentication process using the DRPE in the *CDT* domain. Experimental simulation results that verify the robustness of the proposed system are presented in section 3. Finally, section 4 concludes by summarizing the major ideas of this paper.

2. Theoretical background

In this section, we describe the proposed optical cryptosystem, as demonstrated in figure 1, the primary image is first ciphered into noise like a pattern by the ciphering process of amplitude-DRPE in the Collins diffraction domain, and then used the partial phase information from the ciphered image and removed the magnitude information values. Then, the sparsity-limited encrypted image is decrypted by using the inverse process of the encryption stage. Finally, the decrypted information is authenticated by a non-linear correlation process with an appropriate amount of sparse encrypted data and a suitable non-linear parameter.

2.1 Collins diffraction transform

Collins diffraction transform (*CDT*) is an essential theoretical tool in the fields of optics and signal processing. *CDT* is a parameterized general linear integral transform characterized by three degrees of freedom. The *CDT* is a generalization version of the fractional Fourier transform and classic Fourier transform. It can be utilized to model a coherent wave field using a paraxial optics system. For sake of simplicity, we will describe *CDT* of the image to be encrypted ($f(x)$) in one-dimensional notation

$$\begin{aligned} f(u) =& CDT_{\alpha,\beta,\gamma}\{f(x)\} \\ =& K\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x)\exp\{i\pi[\alpha(x^2)-2\beta(xu)+\gamma(u^2)]\}dx, \end{aligned} \tag{1}$$

where a constant factor K will neglect because it isn't significant in our analysis. The $CDT_{\alpha,\beta,\gamma}\{-\}$ represents the *CDT* operator with three transform parameters α, β, and γ that are independent of the signal in the input (x) and the output (u) domains. The *CDT* orders α, β, and γ are related to the focal length (f), and the propagation distances (d_1) and (d_2) as written [40]:

$$\begin{aligned} \alpha =& \frac{d_1 - f}{\lambda[f(d_1+d_2)-d_1d_2]}, \\ \beta =& \frac{f}{\lambda[f(d_1+d_2)-d_1d_2]}, \\ \gamma =& \frac{d_2 - f}{\lambda[f(d_1+d_2)-d_1d_2]}. \end{aligned} \tag{2}$$

where λ represents the wavelength. The invers transformation operation of *CDT* is expressed as

$$\begin{aligned} f(x) =& \frac{1}{CDT_{\alpha,\beta,\gamma}}\{f(u)\} \\ =& K\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(u)\exp\{-i\pi[\alpha(x^2)-2\beta(xu)+\gamma(u^2)]\}dx \end{aligned} \tag{3}$$

2.2 DRPE in Collins diffraction transform

This section describes the ciphering scheme using DRPE in the *CDT* domain. Let $f(x)$ be the primary image to be ciphered, and $R_1(x)$ and $R_2(u)$ be pair random phase masks (RPMs) expressed by

$$R_1(x) = \exp\{i2\pi r(x)\}, \tag{4}$$

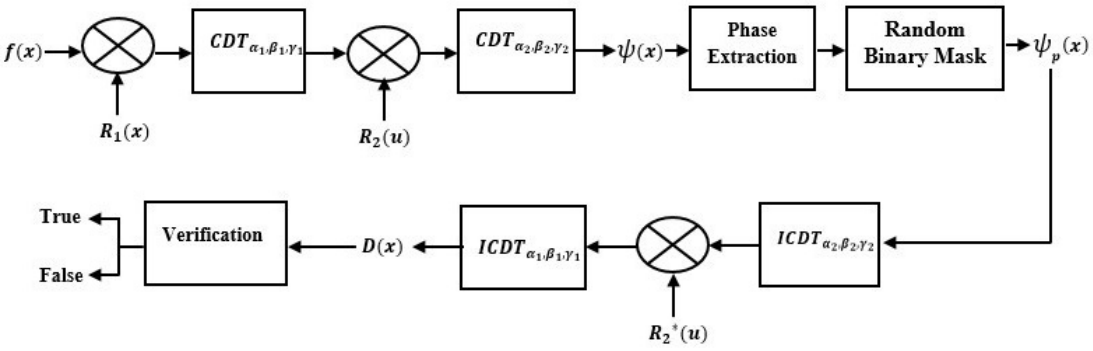

Figure 1. Flowchart of the proposed system.

$$R_2(u) = \exp\{i2\pi p(u)\}, \quad (5)$$

where $r(x)$ and $p(u)$ are two statistically independent white sequences uniformly distributed over the interval [0, 1] which are defined in the spatial and spatial frequency domains, respectively. In the ciphering scheme, the input image $f(x)$ is first multiplied by the first random phase mask $R_1(x)$ and this result is Collins transformed with the order $(\alpha_1,\ \beta_1,\ \gamma_1)$. The output of the previous CDT is manipulated by the second random phase mask $R_2(u)$, and this final distribution is again Collins transformed with CDT order $(\alpha_2,\ \beta_2,\ \gamma_2)$. Finally, the ciphered image is complex-valued and written as

$$\psi(x) = CDT_{\alpha_2,\beta_2,\gamma_2}\{CDT_{\alpha_1,\beta_1,\gamma_1}[f(x)R_1(x)]R_2(u)\} \quad (6)$$

The ciphered image $\psi(x)$ consists of the amplitude $|\psi(x)|$ and phase information $\varphi_\psi(x)$. Thus, this image can be given by

$$\psi(x) = |\psi(x)|\exp\{i\varphi_\psi(x)\} \quad (7)$$

The CDT orders and the second phase mask $R_2(u)$ serve as the security keys to the ciphering scheme. These keys are necessary in the decryption stage.

To obtain the partial phase of the ciphered image $\psi_p(x)$, we used partial information over the phase of the ciphered image using a random binary mask (RBM). In this operation, we randomly selected parts of the phase values of the ciphered image and removed the amplitude component information. This operation can be mathematically described as

$$\psi_p(x) = \exp\{i\varphi_\psi(x)\}\cdot \mathrm{RBM} \quad (8)$$

The decryption scheme employs a reverse operation of the ciphering image. The inputs of the decryption scheme are the partially ciphered image $\psi_p(x)$, CDT orders $(\alpha_1,\beta_1,\gamma_1,\alpha_2,\beta_2,\gamma_2)$, and the complex conjugate of $R_2(u)$. For the amplitude DRPE with partial information in the Collins diffraction domain, function $\psi_p(x)$ is firstly inverse CDT with orders $(\alpha_2,\beta_2,\gamma_2)$ and this output is multiplied by $R_2^*(u)$. The output product is an inverse Collins transformation with orders $(\alpha_1,\beta_1,\gamma_1)$. Finally, decrypted image $D(x)$ is obtained, which can be expressed as

$$D(x) = ICDT_{\alpha_1,\beta_1,\gamma_1}\{ICDT_{\alpha_2,\beta_2,\gamma_2}[\psi_p(x)]R_2^*(u)\} \quad (9)$$

The decrypted image appears noise. Consequently, the decrypted image $D(x)$ is not meant for visualization but contains sufficient information for verification.

2.3 Authentication process

In order to validate the decrypted image, an optical verification procedure based on a nonlinear correlation algorithm was performed. We employ the kth-law nonlinear correlation to evaluate the similarity between the original input image and the decrypted image. When there is a high degree of similarity between the primary and decrypted images, a single peak with low side lobes will appear in the nonlinear correlation authentication plot. Conversely, if the peak is not formed and a noisy background is found, it signifies either a false class or a failure in authentication. Nonlinear correlation (NC) is expressed mathematically as [41]

$$NC = IFT\{|D(u)F(u)|^k \exp[j(\varphi_D(u) - \varphi_F(u))]\} \quad (10)$$

here

$$D(u) = FT[D(x)] \quad (11)$$

$$F(u) = FT[f(x)] \quad (12)$$

where FT and IFT indicates the $2D$ Fourier transform and inverse Fourier transform, $|\cdot|$ is the modulus operator, the parameter k represents the nonlinearity parameter, and φ_D and φ_F denote the phase parts of the $D(u)$ and $F(u)$ functions. A linear filtering technique is obtained at $k = 1$, whereas $k = 0$ leads to a phase extractor that typically enhances high frequency contact. Values of k between these extremes allow for variation in the processor's features.

3. Simulation results and discussion

To demonstrate the effectiveness and robustness of the proposed system, multiple simulations were performed using the scheme shown in figure 1. The MATLAB® (R2019a) platform was employed for the experimental numerical simulation on a 64-bits Windows 10 OS computer. We chose the standard 256 gray-level "pirate" and "dark-women hair" [42] with a size of 512×512 pixels as authentic and a counterfeit class test images, respectively (see figure 2), and the RPMs are created in the MATLAB. Firstly, we use Eq. (6) to encrypt the true image in the Collins diffraction domain. The Collins transform orders are defined as $\alpha_1 = 0.3$, $\beta_1 = 0.5$, $\gamma_1 = 0.7$, $\alpha_2 = 0.5$, $\beta_2 = 0.7$, and

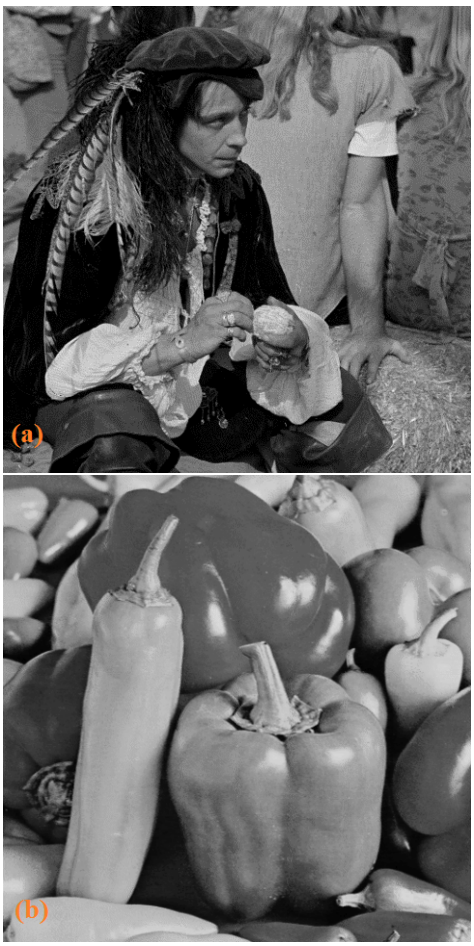

Figure 2. The standard grayscale images of size 512×512 pixels: (a) an authentic class test image (b) a counterfeit class test image [**?**].

$\gamma_2 = 0.9$. Figure 3 shows an encrypted result image. The plain image can be exactly retrieved when utilizing full encrypted image and correct encryption keys, as shown in figure 4.

In this part, we are utilized a number of statistical metrics to check the feasibility of the proposed method such as information entropy, MSE (mean square error), PSNR (peak to signal noise ratio), and *CC* (Correlation coefficient) between the original image and decrypted image, which mathematical are formulas defined as follow:

$$\mathrm{MSE} = \sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|\text{plain image}(x,y) - \text{decrypted image}(x,y)|^2}{M \times N} \tag{13}$$

$$\mathrm{PSNR} = 10 \times \log_{10}\left(\frac{(255)^2}{\mathrm{MSE}}\right) \tag{14}$$

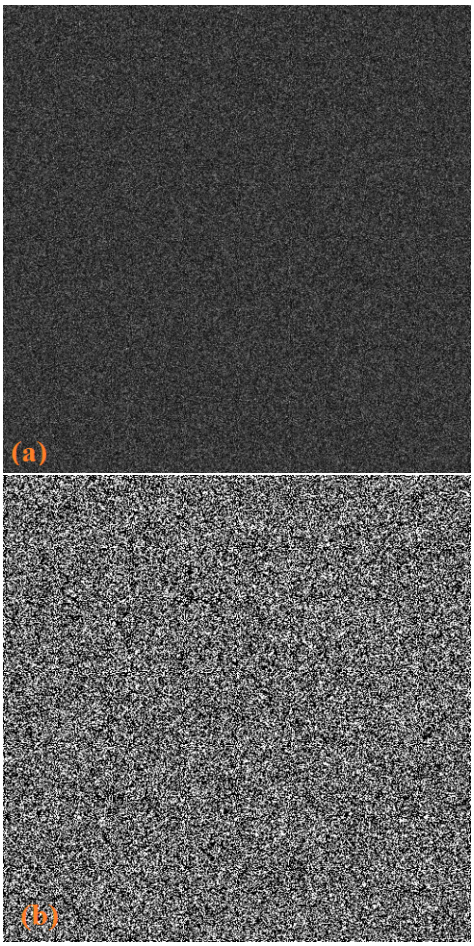

Figure 3. Encrypted images: (a) amplitude component information (b) phase component information.

Figure 4. Decrypted image.

$$CC = \frac{\mathrm{cov}(x,y)}{\sigma(x)\sigma(y)} \tag{15}$$

where $\mathrm{cov}(x,y)$ represents the covariance and σ is the standard deviation of x and y. The computed values of information entropy, MSE, PSNR, and *CC* are given in Table 1.

In our proposal, the phase only component of encrypted information is kept whilst the amplitude component is removed. The proposed method involves the application of the RBM on the phase information of the ciphered function. Figure 5 illustrates the partial phase information, which is generated by random selection of 2% of the phase component of the ciphered function.

To verify the idea of the proposed approach, we used the optical authentication process which is shown in Eq. (10). Consequently, the output correlation of the partial data was computed by using 2% of phase information for the ciphered image. The significant outcome of the nonlinear correlation (*NC*) between the reference image and decrypted image for both an authentic class image and a counterfeit class image is shown in figure 6. From this figure, it is observed that a clear signal of autocorrelation peak is achieved for the authentic class-decrypted image with the reference image as shown in figure 6 (a). However, figure 6 (b) demonstrates a noisy distribution when the counterfeit class image is subjected to nonlinear correlation with the reference image. This result shows that a successful authentication process was achieved with only 2% of the ciphered information.

In order to study a good effectiveness of the proposed scheme, we computed the ideal nonlinearity, appropriate partial data amount, and the peak-to-correlation energy (PCE) [43] based on the partial phase information ratio at different values of k. Figure 7 shows the PCE value obtained from a series of numerical simulations as a function

Table 1. Computed values of information entropy, MSE, PSNR, and *CC*.

Information entropy			MSE between plaintext and decrypted text	PSNR between plaintext and decrypted text	*CC* between plaintext and decrypted text
Original image	Encrypted image	Decrypted image			
7.2367	7.9977	7.2367	6.0081e-32	360.34	1

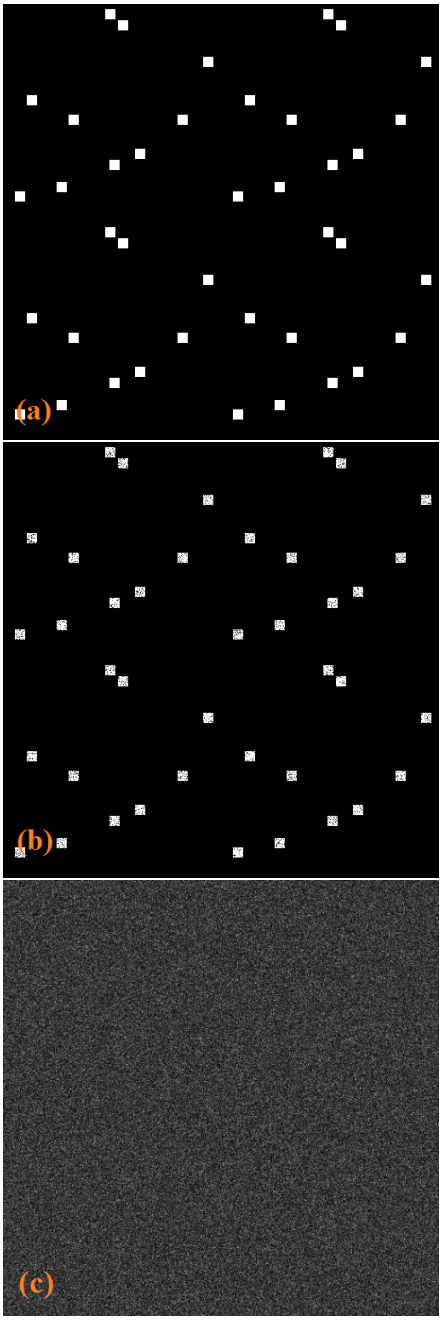

Figure 5. (a) Random binary mask (RBM) (b) partial phase information for the ciphered image (c) decrypted image using partial phase information.

of the percentage of partial phase information with different values of k. As can be seen from this figure, the PCE values increase by increasing the percentage of the partial selected data and have a large value when $k = 0.5$ for a partial data percentage equal to 2% which offers an intense and sharp correlation peak.

We evaluated the ability to withstand noise when using only 2% of the phase distribution of the ciphertext. The additive noise was white Gaussian noise with a mean of zero and the standard deviations are 0.1, 0.3, and 0.5. The results illustrate that the proposed scheme is highly noise-robust, as depicted in figure 8. It can be noted that the normalized peak value (NPV) of the auto-correlation (positive validation) decreases as the standard deviation increased.

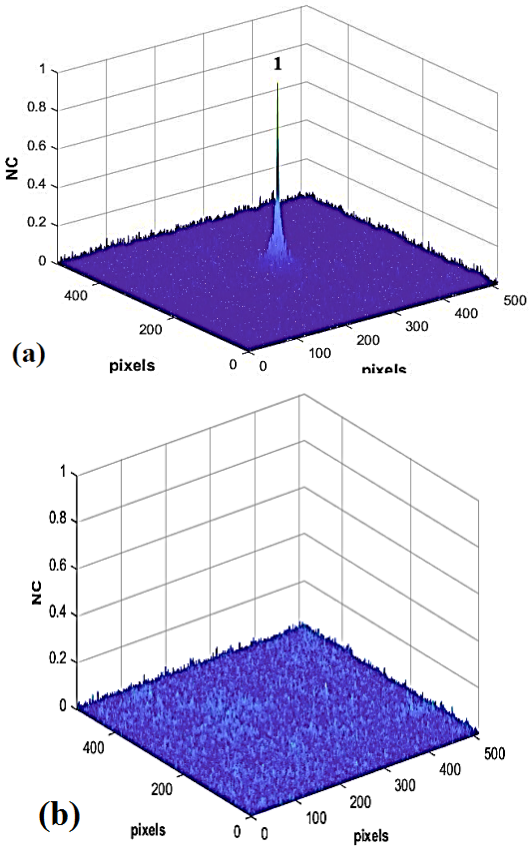

Figure 6. The result correlation plane of validation: (a) an authentic class test image (b) a counterfeit class test image.

To test the robustness of the proposed scheme against cropping attacks, an experiment was conducted by obscuring some parts of the encrypted data image (as shown in figure 9), establishing the robustness of our scheme against cropping attacks. Additionally, the effect of a uniform occlusion attack with 25% loss at different positions on the partial encrypted data ($\psi_p(x)$) was examined and the results are shown in figure 10. Figures 10 (a)-(d) show uniform occluded symbols with 25% losses at different positions. After the loss of information, the resultant decrypted image was employed as the primary input image for the correlator scheme to authenticate its veracity. Figures 10 (e)-(h) depict

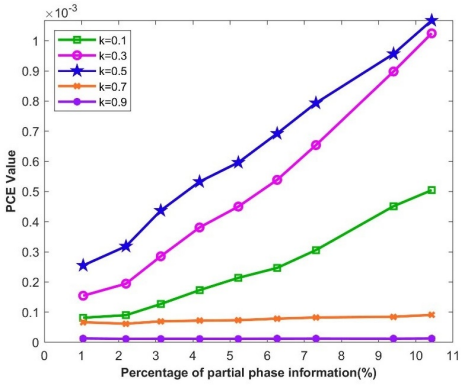

Figure 7. The PCE versus percentage of the selected data of the ciphered image with various nonlinearity factors (k).

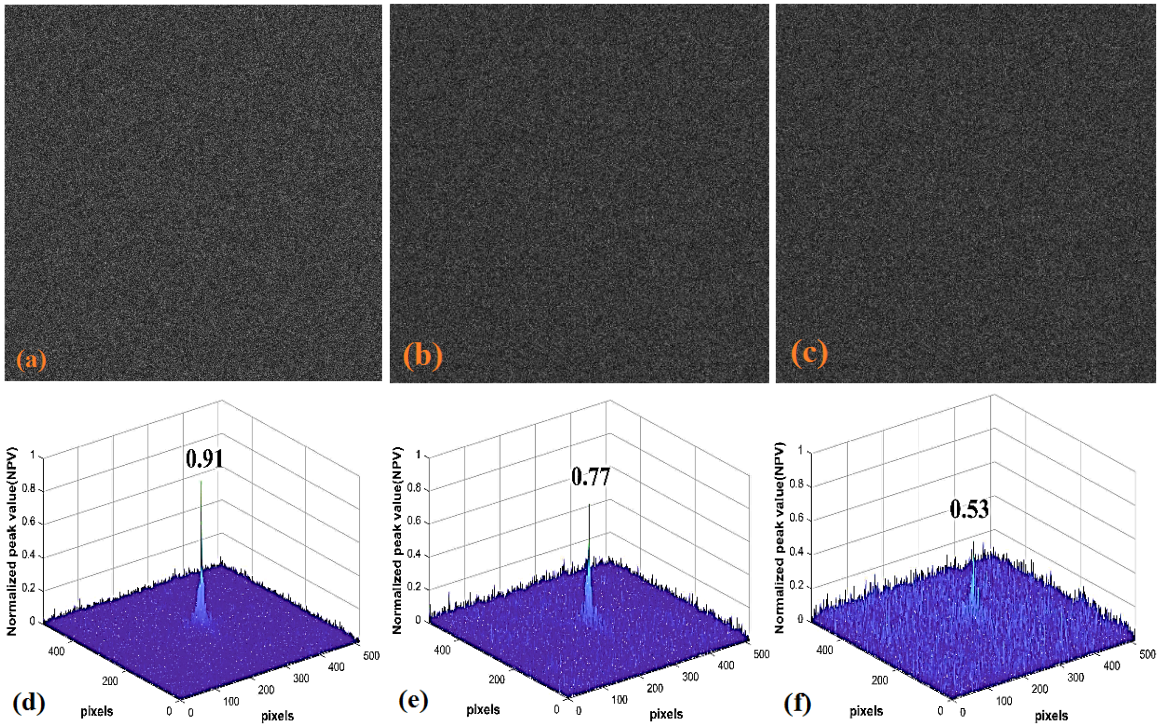

Figure 8. The partial-limited decrypted images are contaminated by white Gaussian noise with the standard deviation of (a) 0.1 (b) 0.3, and (c) 0.5 and (d-f) the authentication distributions corresponding to them.

the corresponding correlation planes of this occlusion at various positions in the ciphertext. From these figures, It can be noted that the performance of the correlation scheme is not significantly affected by the 25% information loss in the encrypted image. Finally, it can be concluded that the performance of the verification processes for the proposed method is not affected by the positions of the occluded pixels resulting from the cropping.

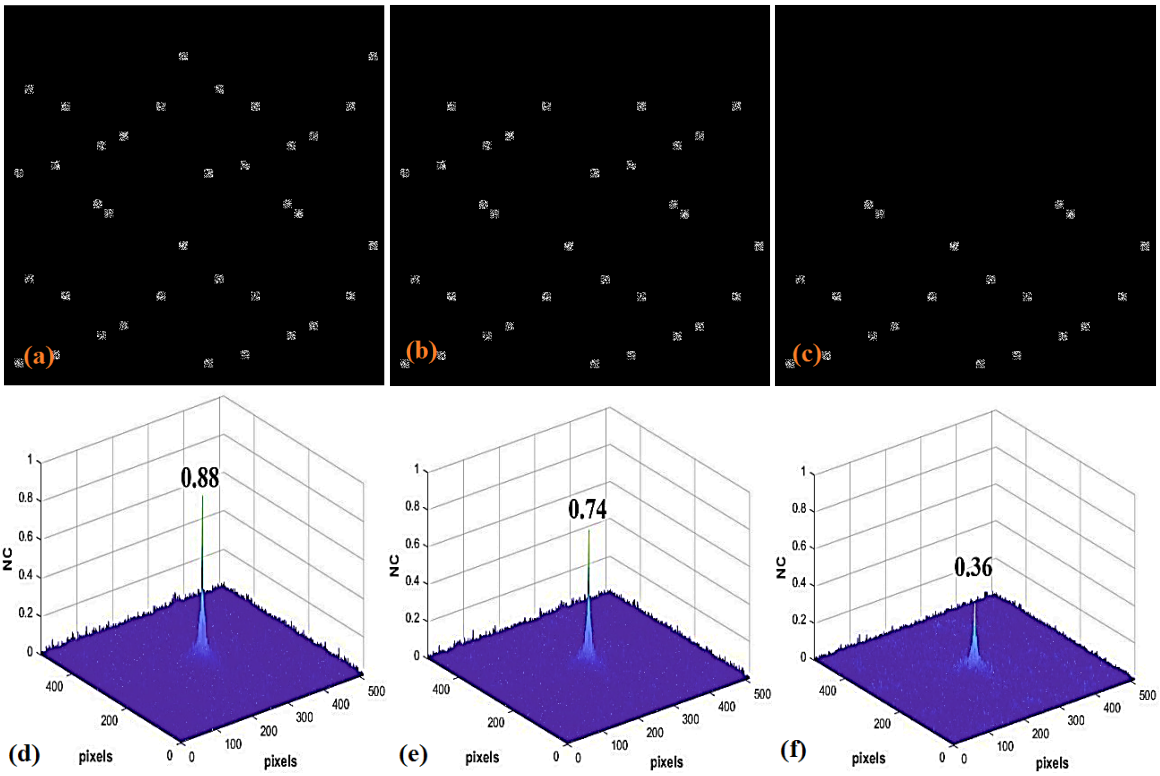

Figure 9. The occluded partial phase encrypted data with (a) 12.5%, (b) 25%, and (c) 50% occlusion areas, and (d-f) the authentication distributions corresponding to them.

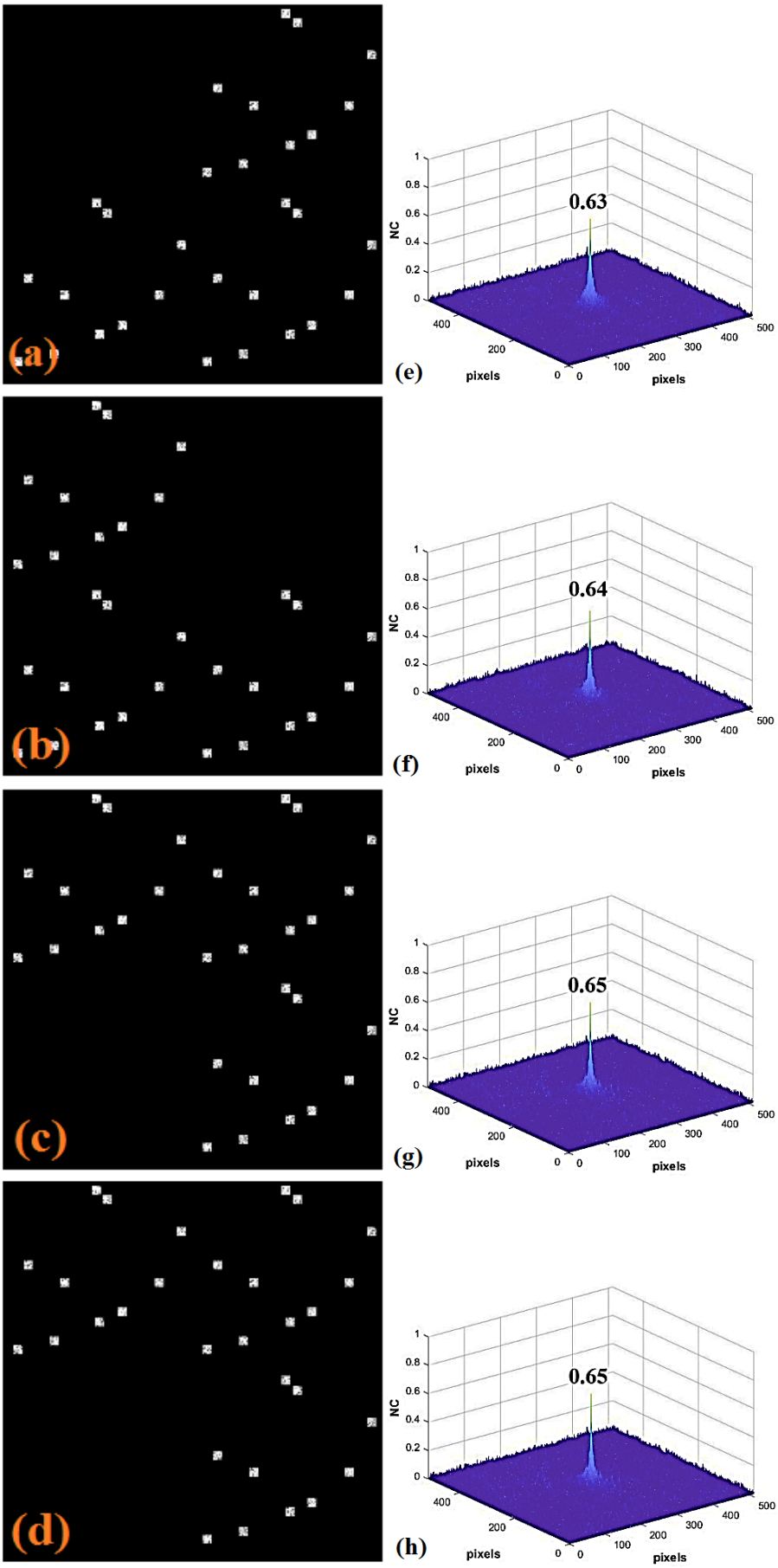

Figure 10. (a-d) Experimental results for the proposed scheme against uniform occlusion attacks for 25% cropped variant locations in the ciphertext and (e-h) the authentication distributions corresponding to them.

Figure 11. (a) Dirac delta function (b) Baboon image.

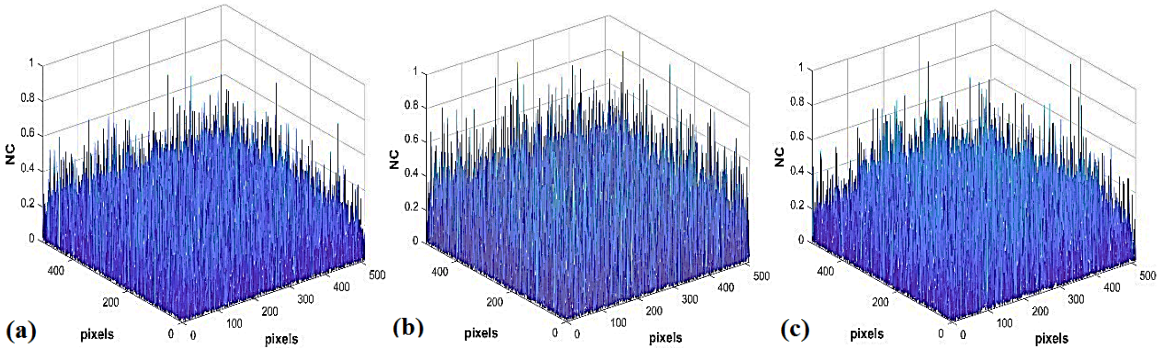

Figure 12. The *NC* distribution plots for validation (a) CPA (b) CCA (c) KPA.

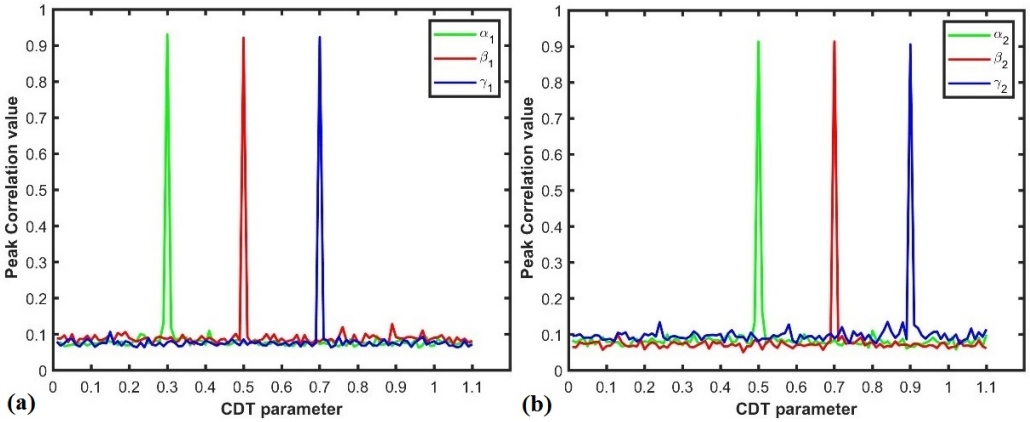

Figure 13. Key sensitivity plots for CDT parameters.

To further confirm the robustness of the proposed strategy, the chosen plaintext attack (CPA), chosen ciphertext attack (CCA), and known plaintext attack (KPA) have been tested. The Dirac delta function (as shown in Fig. 11 (a)) was utilized as an attacker for CPA and CCA, whereas known plaintext (Baboon image as shown in Fig. 11 (b)) was used as an attacker for KPA. The results for the CPA, CCA, and KPA are presented in Fig. 12. This figure demonstrated that the validation results are negative and no sharp correlation peak are obtained.

Finally, we have analyzed the performance of our proposed method against the sensitivity of security parameters (*CDT* parameters) by conducting the decryption procedure with slight variations in the original values of these parameters. Figure 13 presents the results of the analysis. It can be observed from this result that the proposed cryptosystem is highly sensitive to slight change in the originals values of the CDT parameters.

4. Conclusion

In our work, we propose an image authentication system that uses a double random phase encryption method in

the Collins diffraction transform domain. The randomly selected parts from the encrypted image add an extra layer of security and also reduced bandwidth information. The recovered image using this method cannot be visually recognized. However, it is adequate to establish authentication. Therefore, a nonlinear correlation metric is used to authenticate the primary input image with the decrypted image. The experimental simulations demonstrated that the metric parameter PCE obtained good values when the nonlinearity was 0.5 and the selected percentage was 2% of the phase information for the ciphered function. Also, the proposed method exhibited robustness against noise and occlusion attacks and basic cryptographic attacks. Furthermore, this proposal was consisted of phase only components which was easily for implementation without the highly requirements of alignment process.

Authors Contribution
Israa Mohammed Qasim: Methodology (lead); Validation (lead); Writing-original draft (lead). Emad Abdulzahra Mohammed: Supervision (lead); Writing- review & editing (lead).

Availability of data and materials
Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Conflict of interests
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] W. Chen, B. Javidi, and X. Chen. "Advances in optical security systems. ". *Adv. Opt. Photonics*, **6**:120–155, 2014.
DOI: https://doi.org/10.1364/AOP.6.000120.

[2] B. Javidi. "Securing information with optical technology.". *PhysToday*, **50**:27–32, 1997.
DOI: https://doi.org/10.1063/1.881691.

[3] B. Javidi, A. Carnicer, M. Yamaguchi, T. Nomura, E. Pérez-Cabré, M. S. Millán, N. K. Nishchal, R. Torroba, J. F. Barrera, W. He, X. Peng, A. Stern, et al. "Roadmap on optical security.". *J. Opt*, **18**: 083001, 2016.
DOI: https://doi.org/10.1088/2040-8978/18/8/083001.

[4] S. Liu, C. Guo, and J. T. Sheridan. "A review of optical image encryption techniques. ". *Opt. Laser Technol*, **57**:327–342, 2014.
DOI: https://doi.org/10.1016/j.optlastec.2013.05.023.

[5] Sachin, R. Kumar, Sakshi, R. Yadav, S. G. Reddy, A. K. Yadav, and P. Singh. "Advances in optical visual information security: A comprehensive review.". *Photonics*, **11**:99, 2024.
DOI: https://doi.org/10.3390/photonics11010099.

[6] P. Refregier and B. Javidi. "Optical image encryption based on input plane and Fourier plane random encoding.". *Opt. Lett*, **23**:767–769, 1995.
DOI: https://doi.org/10.1364/ol.20.000767.

[7] G. Unnikrishnan and K. Singh. "Double random fractional Fourier-domain encoding for optical security.". *Opt. Eng*, **39**:2853–2859, 2000.
DOI: https://doi.org/10.1117/1.1313498.

[8] R. A. Jassim and E. A. Mohammed. "Asymmetric optical cryptosystem in the fractional Fourier domain using photon counting imaging.". *Basrah J. Sci*, **40**:512–525, 2022.
DOI: https://doi.org/10.29072/basjs.202202178.

[9] B. M. Hennelly. "Random phase and jigsaw encryption in the Fresnel domain. ". *Opt. Eng*, **43**:2239, 2004.
DOI: https://doi.org/10.1117/1.1790502.

[10] H. Singh, A. K. Yadav, S. Vashisth, and K. Singh. "Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane.". *Opt. Lasers Eng*, **67**:145–156, 2015.
DOI: https://doi.org/10.1016/j.optlaseng.2014.10.011.

[11] N. Singh and A. Sinha. "Gyrator transform-based optical image encryption, using chaos. ". *Opt. Lasers Eng*, **47**:539–546, 2009.
DOI: https://doi.org/10.1016/j.optlaseng.2008.10.013.

[12] R. Yadav, Sachin, and P. Singh. "Multiuser medical image encryption algorithm using phase-only CGH in the gyrator domain.". *J. Opt. Soc. Am. A*, **41**:A63–A72, 2024.
DOI: https://doi.org/10.1364/JOSAA.507308.

[13] I. Muniraj, C. Guo, R. Malallah, J. P. Ryle, J. J. Healy, B.-G. Lee, and J. T. Sheridan. "Low photon count based digital holography for quadratic phase cryptography. ". *Opt. Lett*, **42**:2774–2777, 2017.
DOI: https://doi.org/10.1364/ol.42.002774.

[14] I. M. Qasim and E. A. Mohammed. "Optical image encryption based on linear canonical transform with sparse representation.". *Opt. Commun*, **533**:129262, 2023.
DOI: https://doi.org/10.1016/j.optcom.2023.129262.

[15] A. Sangwan and H. Singh. "A secure asymmetric optical image encryption based on phase truncation and singular value decomposition in linear canonical transform domain.". *Int. J. Opt*, **2021**:1–19, 2021.
DOI: https://doi.org/10.1155/2021/5510125.

[16] R. Girija, H. Singh, and G. Abirami. "Cryptanalysis of DRPE using complex S-Box based on linear canonical transform". *Multimed. Tools Appl*, **82**:12151–12166, 2023.
DOI: https://doi.org/10.1007/s11042-022-13752-9.

[17] E. A. Mohammed and I. M. Qasim. "Optical double-image cryptosystem based on a joint transform correlator in a linear canonical domain.". *Appl. Opt*, **63**:5941, 2024.
DOI: https://doi.org/10.1364/AO.525462.

[18] J. M. Vilardy O, R. A. Perez, and C. O. Torres M. "Optical image encryption using a nonlinear joint transform correlator and the Collins diffraction transform. ". *Photonics*, **6**:115, 2019.
DOI: https://doi.org/10.3390/photonics6040115.

[19] E. A. Mohammed and I. M. Qasim. "Security augmenting of optical cryptosystem based on linear canonical transform domain using a full phase encoding technique.". *Phys. Scr*, **99**:065112, 2024.
DOI: https://doi.org/10.1088/1402-4896/ad4316.

[20] I. Mehra and N. K. Nishchal. "Fingerprint image encryption using phase retrieval algorithm in gyrator wavelet transform domain using QR decomposition.". *Opt. Commun*, **533**:129265, 2023.
DOI: https://doi.org/10.1016/j.optcom.2023.129265.

[21] Anshula and H. Singh. "Ensuring security of cryptosystems with DVFM-, modified equal modulus decomposition in the domain of gyrator wavelet transform.". *Multimed. Tools Appl*, **82**:5965–5985, 2023.
DOI: https://doi.org/10.1007/s11042-022-13584-7.

[22] W. Qin and X. Peng. "Vulnerability to known-plaintext attack of optical encryption schemes based on two fractional Fourier transform order keys and double random phase keys.". *J. Opt. A Pure Appl. Opt*, **11**:075402, 2009.
DOI: https://doi.org/10.1088/1464-4258/11/7/075402.

[23] K. Nakano, M. Takeda, and H. Suzuki. "Security analysis of phase-only DRPE based on known-plaintext attack using multiple known plaintext – ciphertext pairs. ". *Applied Optics*, **53**:6435–6443, 2012.
DOI: https://doi.org/10.1364/AO.53.006435.

[24] X. Peng, P. Zhang, H. Wei, and B. Yu. "Known-plaintext attack on optical encryption based on double random phase keys.". *Opt. Lett.*, **31**:1044, 2006.
DOI: https://doi.org/10.1364/OL.31.001044.

[25] 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.*, **30**:1644, 2005.
DOI: https://doi.org/10.1364/OL.30.001644.

[26] J. Wu, W. Liu, Z. Liu, and S. Liu. "Correlated-imaging-based chosen plaintext attack on general cryptosystems composed of linear canonical transforms and phase encodings. ". *Opt. Commun*, **338**:164–167, 2015.
DOI: https://doi.org/10.1016/j.optcom.2014.10.050.

[27] W. Qin and X. Peng. "Asymmetric cryptosystem based on phase-truncated Fourier transforms. ". *Opt. Lett*, **35**:118–120, 2010.
DOI: https://doi.org/10.1364/OL.35.000118.

[28] H. Singh, R. Girija, and M. Kumar. "A cryptoanalysis of elliptic curve cryptography based on phase truncation in the domain of hybrid gyrator Hartley transform. ". *Opt. Quantum Electron*, **55**:487, 2023.
DOI: https://doi.org/10.1007/s11082-023-04765-1.

[29] Z. Zhong, J. Chang, M. Shan, and B. Hao. "Fractional Fourier-domain random encoding and pixel scrambling technique for double image encryption. ". *Opt. Commun*, **285**:18–23, 2012.
DOI: https://doi.org/10.1016/j.optcom.2011.08.068.

[30] R. Zhang and D. Xiao. "Double image encryption scheme based on compressive sensing and double random phase encoding. ". *Mathematics*, **10**:1242, 2022.
DOI: https://doi.org/10.3390/math10081242.

[31] X. Chai, J. Bi, Z. Gan, X. Liu, Y. Zhang, and Y. Chen. "Color image compression and encryption scheme based on compressive sensing and double random encryption strategy. ". *Signal Processing*, **176**: 107684, 2020.
DOI: https://doi.org/10.1016/j.sigpro.2020.107684.

[32] R. Girija and H. Singh. "Enhancing security of double random phase encoding based on random S-Box.". *3D Res*, **9**:15, 2018.
DOI: https://doi.org/10.1007/s13319-018-0165-z.

[33] W. Chen, X. Chen, A. Stern, and B. Javidi. "Phase-modulated optical system with sparse representation for information encoding and authentication.". *IEEE Photonics J*, **5**:6900113, 2013.
DOI: https://doi.org/10.1109/JPHOT.2013.2258144.

[34] E. A. Mohammed and H. L. Saadon. "Simultaneous verification of optical triple-image encryption using sparse strategy. ". *J. Phys. Conf. Ser*, **1234**:012037, 2019.
DOI: https://doi.org/10.1088/1742-6596/1234/1/012037.

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

[36] E. Pérez-Cabré, M. Cho, and B. Javidi. "Information authentication using photon-counting double-random-phase encrypted images.". *Opt. Lett*, **36**:22, 2011.
DOI: https://doi.org/10.1364/ol.36.000022.

[37] W. Wang, X. Wang, B. Xu, and J. Chen. "Optical image encryption and authentication using phase-only computer-generated hologram.". *Opt. Lasers Eng*, **146**:106722, 2021.
DOI: https://doi.org/10.1016/j.optlaseng.2021.106722.

[38] J. Chen, Z. Zhu, Fu. C. liang, L. bo Zhang, and Y. Zhang. "Information authentication using sparse representation of double random phase encoding in fractional Fourier transform domain.". *Optik*, **136**: 1–7, 2017.
DOI: https://doi.org/10.1016/j.ijleo.2017.02.001.

[39] E. A. Mohammed. "Optical information authentication of triple-image encryption. ". *J. Kufa Phys*, **10**:60–67, 2018.
DOI: https://doi.org/10.31257/2018/JKP/100108.

[40] G. Unnikrishnan and K. Singh. "Optical encryption using quadratic phase systems.". *Opt. Commun*, **193**:51–67, 2001.
DOI: https://doi.org/10.1016/S0030-4018(01)01224-X.

[41] A. Markman, B. Javidi, and M. Tehranipoor. "Photon-counting security tagging and verification using optically encoded QR codes. ". *IEEE Photonics J*, **6**:1–9, 2013.
DOI: https://doi.org/10.1109/JPHOT.2013.2294625.

[42] "The USC-SIPI Image Database.". URL https://sipi.usc.edu/database.

[43] E. Pérez-Cabré, E. A. Mohammed, M. S. Millán, and H. L. Saadon. "Photon-counting multifactor optical encryption and authentication.". *J. Opt*, **17**:025706, 2015.
DOI: https://doi.org/10.1088/2040-8978/17/2/025706.