JSML
Journal of Science and Mathematics Letters
ISSN 2462-2052 • eISSN 2600-8718

Research Article

An Optical Cryptosystem Based on Tent Map and Deterministic Key in Gyrator Domain

Israa M. Qasim[1], Emad A. Mohammed[2]*

[1] General Directorate of Education in Basrah, Ministry of Education, Baghdad, Iraq
[2] Department of Physics, College of Science, University of Basrah, Basrah, Iraq
* Corresponding author: emad.mohammed@uobasrah.edu.iq

ARTICLE HISTORY

Received
28 November 2025
Revised
19 April 2026
Accepted
3 June 2026
Published
1 July 2026

KEYWORDS

Optical cryptosystem
Gyrator transform domain
Deterministic phase masks
Tent chaotic map

ABSTRACT

A novel symmetric optical cryptosystem is proposed based on the integration of deterministic phase masks and a chaotic tent map within the gyrator transform domain. The encryption process employs a pair of chaotic deterministic phase keys generated through a linear combination of multiple subkeys and the tent map, enhancing key complexity and unpredictability. Decryption is achieved by applying the conjugate of the corresponding phase keys, ensuring accurate reconstruction of the original image. The incorporation of chaotic deterministic parameters significantly expands the key space and introduces additional security layers, effectively overcoming the alignment limitations associated with conventional double random phase encryption techniques. The performance and robustness of the proposed cryptosystem were evaluated through extensive computational simulations. Security analyses were conducted using multiple statistical metrics, including structural similarity index (SSIM), mean square error (MSE), relative error, histogram uniformity, correlation distribution, mesh analysis, and information entropy. The results demonstrate that the encrypted images exhibit high randomness, low pixel correlation, and strong resistance to differential, statistical, and noise contamination attacks. Furthermore, the large key space and sensitivity to initial conditions render the system highly secure against brute-force attacks under current computational capabilities. Overall, the proposed scheme offers a robust and efficient framework for secure optical image encryption, with strong potential for practical applications in optical information processing and secure communication systems.

https://doi.org/10.37134/jsml.vol14.3.1.2026

1. INTRODUCTION

The remarkable physical benefits of optical techniques such as low computational complexity, parallel processing, high speed, high efficiency, and multidimensional signal processing capabilities have made them extensively utilized in the field information security (Javidi et al., 2025, 2016; Liu et al., 2014; Sachin et al., 2024). Refregier and Javidi in 1995 first proposed a ground breaking contribution into the optical encryption field, which is known as double random phase encoding (DRPE). This technique involves encoding the plaintext into stationary white noise by employing a conventional 4f structure and pair of statistically independent random phase keys situated at the input and Fourier planes (Refregier & Javidi, 1995). In order to augment the security and further broaden the key space, the traditional DRPE method has been supplied from the Fourier to several domains, such as gyrator (Tian et al., 2023), Fresnel (Situ & Zhang, 2004), Fractional Fourier (Jassim & Mohammed, 2022; Unnikrishnan, 2000), and linear canonical domains (Mohammed & Qasim, 2025, 2024a, 2023). These enhanced cryptographic systems utilized additional secret keys in the form of structural parameters such as fractional order, diffraction system, wavelength, and linear order to overcome brute-force attacks. Besides DRPE based cryptosystems, researchers have been proposed optical image encryption methods using various techniques, including interference (Khalf & Mohammed, 2025a, 2025b; Luan et al., 2020), ptychography (Rawat et al., 2015; Shi et al., 2013), sparse representation (Mohammed & Saadon, 2016, 2019), spatial nonlinear optics (Hou & Situ, 2022), phase retrieval algorithms (Xiong, 2023), digital holography (Yadav et al., 2024), computer-generated hologram (Guo et al., 2001), joint transform correlator (Mohammed & Qasim, 2024b; Perez et al., 2023) ghost imaging (Xiao et al., 2019), phase truncation (Xiong et al., 2023), diffractive imaging (Wang et al., 2024), photon counting (Pérez-Cabré et al., 2015), and deep learning (Liao et al., 2021).

Several researchers have put forward the idea of using structured phase masks (SPMs) as a substitute for RPMs in the classical DRPE approach. These SPMs are generated using various techniques such as toroidal zone plate (Barrera et al., 2005), Fresnel zone plate (Khurana & Singh, 2018), deterministic phase mask (Girija & Singh, 2018), radial Hilbert mask (Maan & Singh, 2018), linear phase mask (Sun et al., 2018), deterministic spherical phase mask (Zamrani & Ahouzi, 2020), spiral phase mask (Abuturab, 2014), fractal zone mask, quadratic phase mask, spiral quadratic phase mask (Sun et al., 2018), and devil's vortex Fresnel lens (Singh, 2016). These types of SPMs have demonstrated significant simplicity and robustness to fulfill the requirements of high security and flexibility.

This research work presents a symmetric optical cryptosystem based on chaotic structured masks, which is called chaotic deterministic phase key in the gyrator transform domain. The use of chaotic deterministic phase masks, which are generated by a linear combination of a number of sub-keys and chaotic tent map, enables to improve the alignment tolerance of the optical system to shifts the needed phase keys when compared with the traditional DRPE system. This method leverages the high sensitivity and ergodicity of the chaotic Tent map to improve the key space and security of the system. In addition, the GT operation for different angles can only be executed by appropriately rotating the cylindrical lenses, while maintaining fixed distances between the lenses and the input-output planes.

The main objectives of this paper are to demonstrate a new symmetric cryptosystem that combines a deterministic phase mask and a chaotic tent map in the gyrator domain to enhance security; to develop a deterministic phase mask based on the linear combination of multiple subkeys, thereby increasing the complexity and unpredictability of the cryptographic keys; and to integrate deterministic and chaotic parameters to expand the key space while addressing the alignment limitations associated with conventional DRPE techniques.

2. METHODOLOGY

2.1. Gyrator Transform

The gyrator transform (GT) is a mathematical tool that is employed to analyze and process 2D signals. GT is a type of the canonical integral transform that is introduced by Rodrigo et al. (2007a, 2007b) into the optical information processing field. GT can be achieved using an optical system consisting of six thin cylinder lenses. The mathematical definition of GT for a two dimensional function $f(x,y)$ is given by (Rodrigo et al. 2007b, 2007a):

$$G(u,v) = G^{\alpha}\{f(x,y)\} = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x,y)\, k(u,v;x,y)dxdy \qquad (1)$$

Here, α refers the rotation angle of GT, $G(u,v)$ is the output of GT, x and y is the input plane coordinates, u and v is the output plane coordinates, and $k(u,v;x,y)$ is the kernel of transform can be given as follows:

$$k(u,v;x,y) = \frac{1}{|sin\ \alpha|}\exp\left\{\frac{i2\pi}{sin\ \alpha}[(uv+xy)\ cos\ \alpha\ -(vx+uy)]\right\},\ \ i=\sqrt{-1} \tag{2}$$

2.2. Generation of the Chaotic Deterministic Phase Mask

Chaos theory plays a pivotal role in the communications and information security fields. According to chaos theory, a chaotic function is one in which even a little calculation error in the input can produce an output that contains the greatest conceivable error. An illustration of an erratic behaviour is referred to as a chaotic map. The pseudo-randomness, non-correlation, and periodicity of the chaotic map are evident. Chaos has emerged as an alternative for random phase masks in optical image encryption. The significant characteristic of chaos-based random phase mask generation lies in its reliance on the parameters of the chaotic map as the sole requirement for the private key. The tent map is used in our proposed study as a 1-D chaotic map owing to its advantages such as a more uniform distribution of chaotic sequence and higher Lyapunov exponent compared that the logistic map, which contributes to robust randomness in phase encoding and increased resistance against statistical attacks. The mathematical expression of tent map can be written as (Hilborn, 2000; Layek, 2015):

$$f(x) = a.x \qquad \text{for } 0 \le x < 0.5 \tag{3}$$
$$f(x) = a(1-x_n) \qquad \text{for } 0.5 \le x \le 1 \tag{4}$$

where a denotes to the bifurcation parameter whose value lies in the interval $0 \le a \le 2$. It can be expressed iterative form as following:

$$x_{n+1} = a.x_n \qquad \text{for } 0 \le x_0 < 0.5 \tag{5}$$
$$x_{n+1} = a(1-x_n) \qquad \text{for } 0.5 \le x_0 \le 1 \tag{6}$$

where x_0 refers to the primary value (initial condition), which acts as an initial security key, x_n is the state value at the n *-th* iteration, and n represents the iteration index, where $n = 1, 2, 3, \dots$. Employing Eq. (5) and (6), the value of 1-D random sequence can be expressed as:

$$X = \{x_1, x_2, \dots\dots\dots, x_{M\times N}\} \tag{7}$$

The 2-D sequence is generated by rearrangement X and Y, which expresses as:

$$Y = \{y_{ij} |\ i = 1,2, \dots, M; j = 1,2, .., N\} \tag{8}$$

where $y_{ij}\epsilon(0,1)$. Thus, the chaotic random phase mask (CRPM) is generated by the integration of the chaotic tent map and random phase mask, which is written as follows:

$$CRPM(x,y) = exp[\text{i}2\pi y_{ij}(x,y)] \tag{9}$$

where (x,y) represents the coordinate of CRPM.

The deterministic phase mask (DPM) is constructed by setting the value of an integer n for defining the subkeys in the key. Then, we split the phase mask into a $n \times n$ grid of sub-blocks. In our study, for an image of 512×512 pixels and setting $n = 8$, the phase mask is divided into 64 independent subkeys. The final deterministic phase mask is then synthesized as a linear combination of these 64 sub-states, ensuring high complexity. Mathematically, the DMP is obtained as follows (Sun et al., 2018):

$$DPM = \sum_{i=1}^{8}\sum_{j=1}^{8} M_{ij}(x,y) \tag{10}$$
$$M_{ij}(x,y) = \exp[jk(b_1x + b_2y)] \tag{11}$$

Here, b_1 and b_2 are random parameters, and k indicates to the wave number.

Finally, the chaotic deterministic phase mask (CDPM) is acquired by multiplying the CRPM and DPM, which is expressed as follows:

$$CDPM = CRPM.DPM \tag{12}$$

The generated chaotic deterministic phase mask (CDPM), which is a combination of chaotic random phase mask (CRPM), and a deterministic phase mask (DPM), is demonstrated in Figure 1.

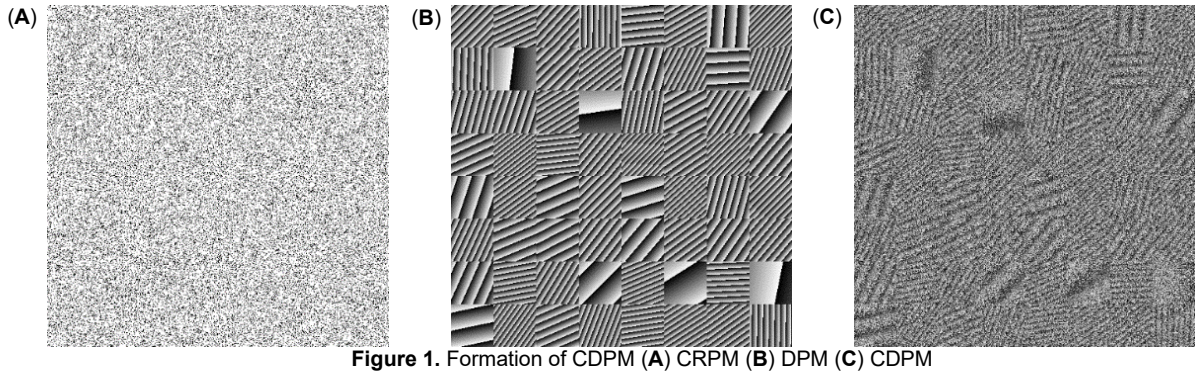

Figure 1. Formation of CDPM (**A**) CRPM (**B**) DPM (**C**) CDPM

2.3. Proposed Cryptosystem

The schematic diagram of the proposed cryptographic system is presented in Figure 2. The initial encryption and decryption procedures for the proposed method can be considered as an expansion of the DRPE scheme from the Fourier transform domain to the gyrator transform domain while also replacing the random phase mask with a chaotic deterministic phase mask.

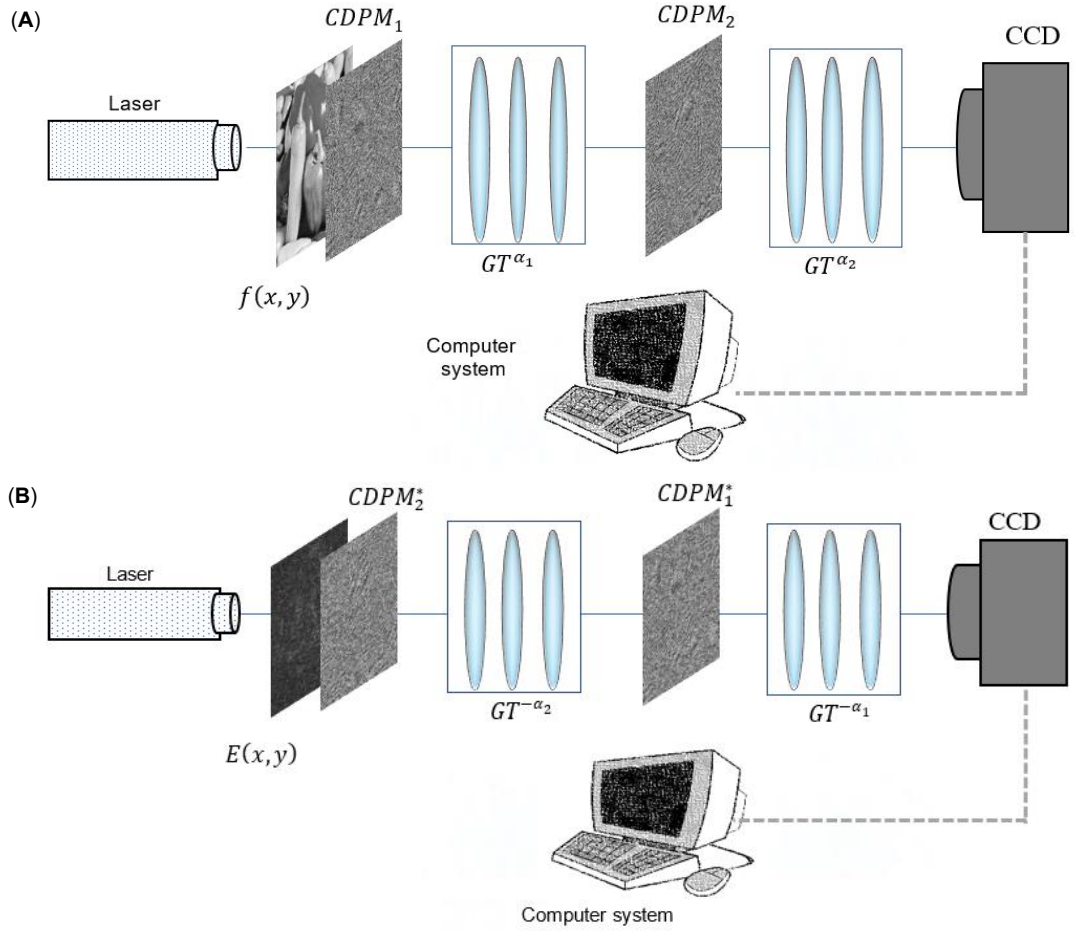

Figure 2. Schematic diagram of the proposed cryptographic system (**A**) encryption procedure (**B**) decryption procedure. f: input image, E: Encrypted image, $CDPM$: Encryption key, GT: Gyrator transform, CCD: Charge-coupled device camera

The procedural steps for proposed encryption process are outlined as follows:

Step 1: Firstly, the primary image $f(x,y)$ is bonded to the chaotic deterministic phase key $CDPM_1$, and then the gyrator transformation is applied with the transformation angle α_1.

$$g(x,y) = GT^{\alpha_1}\{f(x,y)\,.\,CDPM_1\} \tag{13}$$

Step 2: Afterward, the resulting image $g(x,y)$ is bonded to the second chaotic deterministic phase key $CDPM_2$, and then gyrator transformation is again applied with the transformation angle α_2 in the output plane. Mathematically, this procedure can be expressed as follows:

$$E(x,y) = GT^{\alpha_2}[\,g(x,y).CDPM_2] \tag{14}$$

The decryption procedure for the proposed system is the inverse procedure of the encryption. The sequence of steps for decryption process is presented below:

Step 1: Initially, the ciphered image $E(x,y)$ is multiplied by the conjugate of a second chaotic deterministic phase key $CDPM_2^*$ and then the gyrator transformation is applied with angle $-\alpha_2$.

$$g(x,y)' = GT^{-\alpha_2}\{E(x,y)\,.\,CDPM_2^*\} \tag{15}$$

Step 2: The occurred result $g(x,y)'$ is then bonded to the conjugate of the chaotic deterministic phase mask $CDPM_1^*$ and then gyrator transform is again performed with the angle $-\alpha_1$. Finally, an absolute operation is applied to the resulting image to obtain the decrypted image. Mathematically, this procedure can be written as:

$$f(x,y) = |GT^{-\alpha_1}[g(x,y)'\,.\,CDPM_1^*]\,| \tag{16}$$

3. RESULTS AND DISCUSSION

This section presents the computational simulations conducted to verify the authenticity and security of the proposed optical cryptography system. We conducted our experiments on a PC host installed with MATLAB 2019a experimental software. The secret image “Pepper” was grayscale image taken chosen from the USC Image Database with a resolution of 512×512 pixels. Also, the chaotic deterministic phase key with 512×512 pixels. The secret images are encrypted by using Eq. (12). In our numerical simulations, we have utilized the value of bifurcation parameter as $a = 1.35$ with initial condition as $x_0 = 0.61$ of chaotic tent map, and the rotation angles of gyrator transform are $\alpha_1 = 0.3\pi$ and $\alpha_2 = 0.4\pi$. Figures 3 (A-B) illustrate the images before and after encryption process, respectively. By employing the inverse optical cryptosystem and correct parameter set, the original image can be recovered, as illustrated in Figure 3(C). To validate the applicability and robustness of the proposed method, we extended our simulation to include various test image, featuring different frequency characteristics and textures such as Baboon and Camera man, as illustrated in Figure 4. The structural similarity index metric (SSIM), mean square error (MSE), root mean square error (RMSE), relative error (RE), and peak signal-to-noise ratio (PSNR) were employed to quantitatively evaluate the effectiveness of the proposed method by comparing the original and recovered images. The computed values of the SSIM, MSE, RMSE, RE, and PSNR are 1, 2.1816e-31, 4.6708e-16, 3.6071e-33, and 354.74, respectively. These obtained values indicate a high degree of similarity between the plain image and recovered image. The computed values of the SSIM, MSE, RMSE, RE, and PSNR are summarized in Table 1 in comparative with DRPE systems such as Fourier domain and fractional Fourier domain.

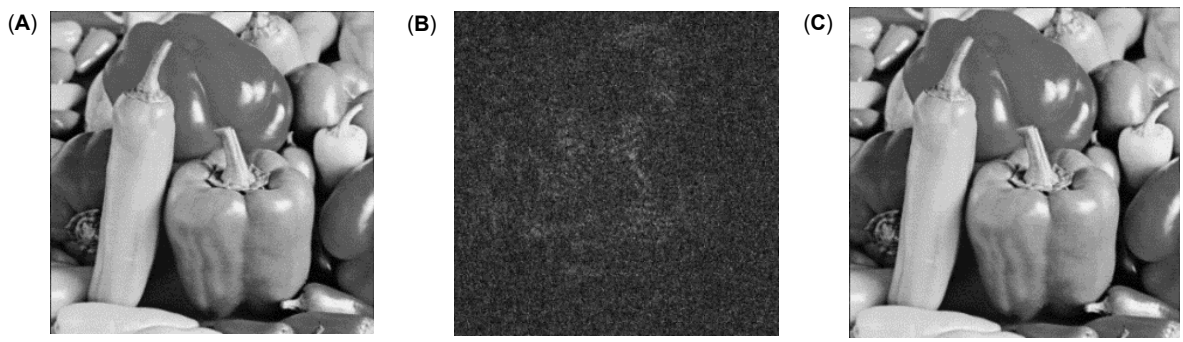

Figure 3. Encryption and decryption outcomes (**A**) input image (**B**) ciphered image (**C**) retrieved image

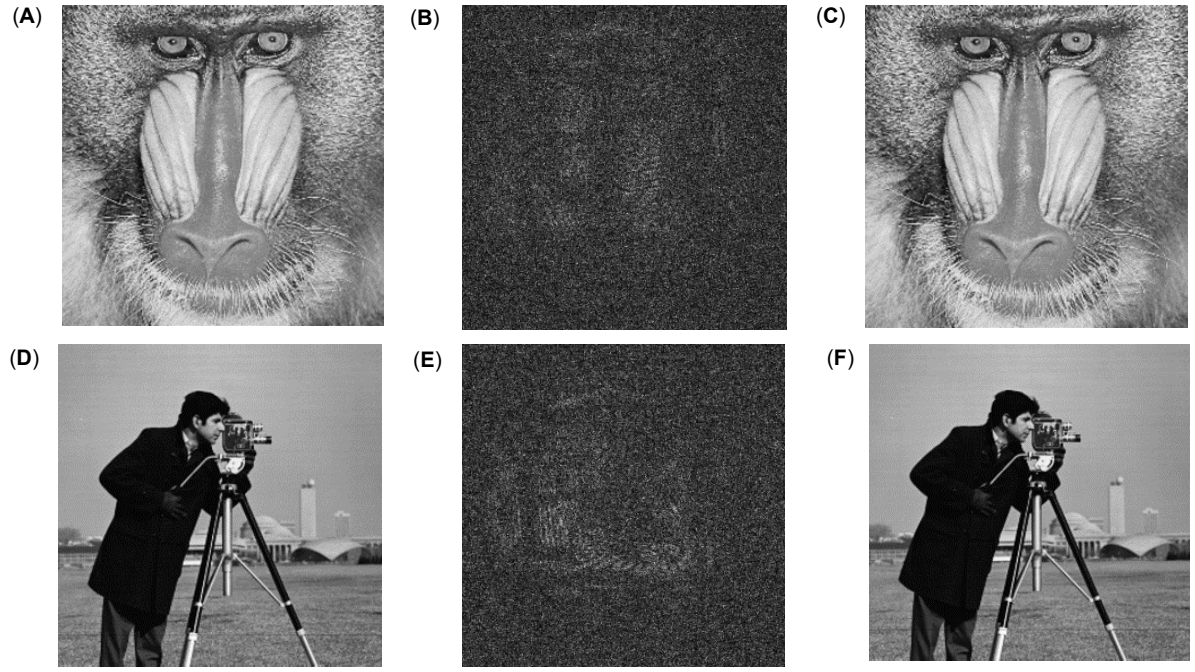

Figure 4. Validation results of the proposed cryptosystem for various test images (**A** and **D**) input images (**B** and **E**) ciphered images (**C** and **F**) retrieved images

Table 1. SSIM, MSE, RMSE, RE, and PSNR results between the primary and retrieved images for the proposed scheme and DRPE systems

Methods	SSIM	MSE	RMSE	RE	PSNR
Our proposed	1	2.1816e-31	4.6708e-16	3.6071e-33	354.74
Ref. (Unnikrishnan, 2000)	1	2.3724e-31	4.8708e-16	3.9228e-33	354.38
Ref. (Qasim & Mohammed, 2023)	1	1.3221e-31	3.6361e-16	1.9844e-33	356.92
Ref. (Mohammed & Qasim, 2024a)	1	2.7182e-31	1.6487e-16	5.6905e-34	363.79

3.1. Histogram and Mesh Plots Analysis

In the image encryption systems, histogram analysis is employed as a tool to evaluate the statistical characteristics of the encrypted images and compare them to the original images properties, including the intensity levels and pixel distribution. The importance of this analysis lies in its ability to evaluate the strength and security of image encryption systems, ensuring that the encrypted image is robust against different attacks and exhibits uniform distribution and a high level of entropy. Histograms of both the primary image and encrypted image are presented in Figure 5.

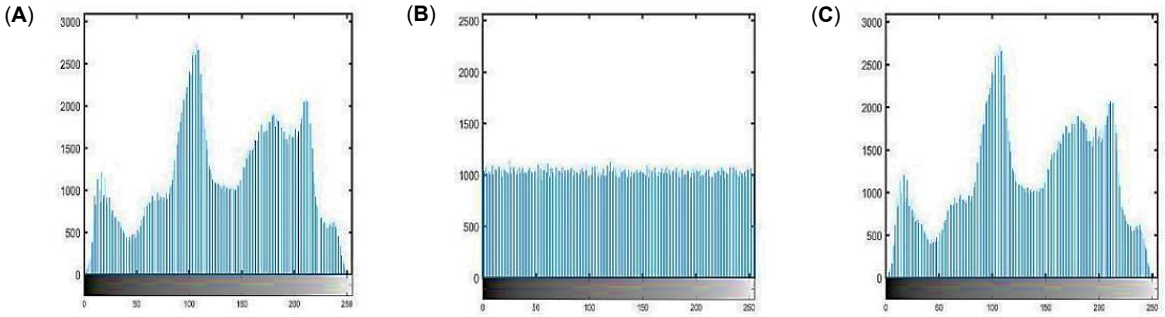

Figure 5. Pixel intensity Histograms analysis for (**A**) input image (**B**) ciphered image (**C**) retrieved image

As shown in the figure, the encrypted image's histogram exhibits a near-uniform pixel distribution, demonstrating that the system's resilience against statistical attacks and frequency analysis. To further validate the ability of the suggested system, a mesh plot was analyzed. The outputs of the mesh plots are given in Figure 6. From this figure, it can be demonstrated that the mesh plots of the primary image and ciphered image are different, which is a safeguard against any inadvertent disclosure of original image information. Thus, the histogram and 3D plots of the proposed scheme ensure that eavesdroppers cannot extract any information.

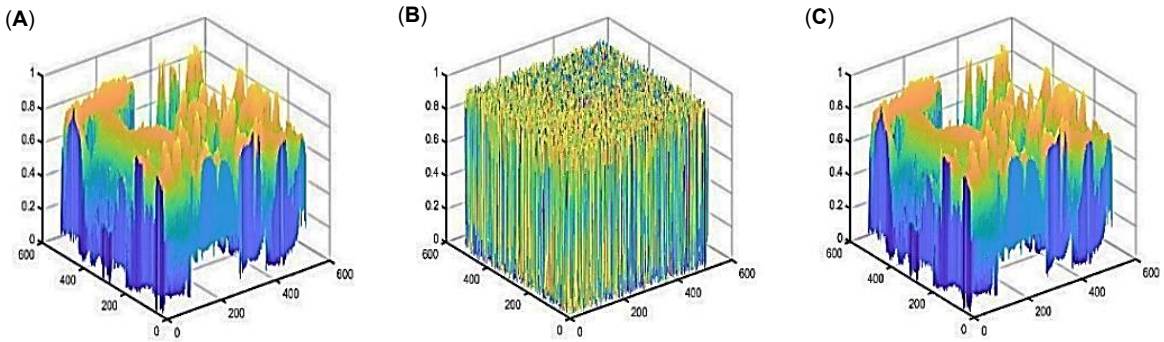

Figure 6. Mesh plots analysis for (**A**) input image (**B**) ciphered image (**C**) retrieved image

3.2. Correlation Distribution Analysis

Correlation distribution is a significant statistical measure employed to verify the effectiveness of the proposed system. In our work, we investigated the correlation distribution of adjacent pixels in different directions. 15000 adjacent pixels were randomly sampled from both the input and the ciphered images. Figure 7 displays the plots of correlation distribution. The findings depicted in Figure 7 (A-C) exhibit a linear distribution approached limit of 1, which indicates a strong correlation among pixels in the original image. In contrast, Figure 7 (D-F) shows that the pixels in the ciphered image are random and exhibit scattered distribution, demonstrating that the encryption process has eliminated all statistical patterns. These results confirm that the robustness and strength of the proposed system.

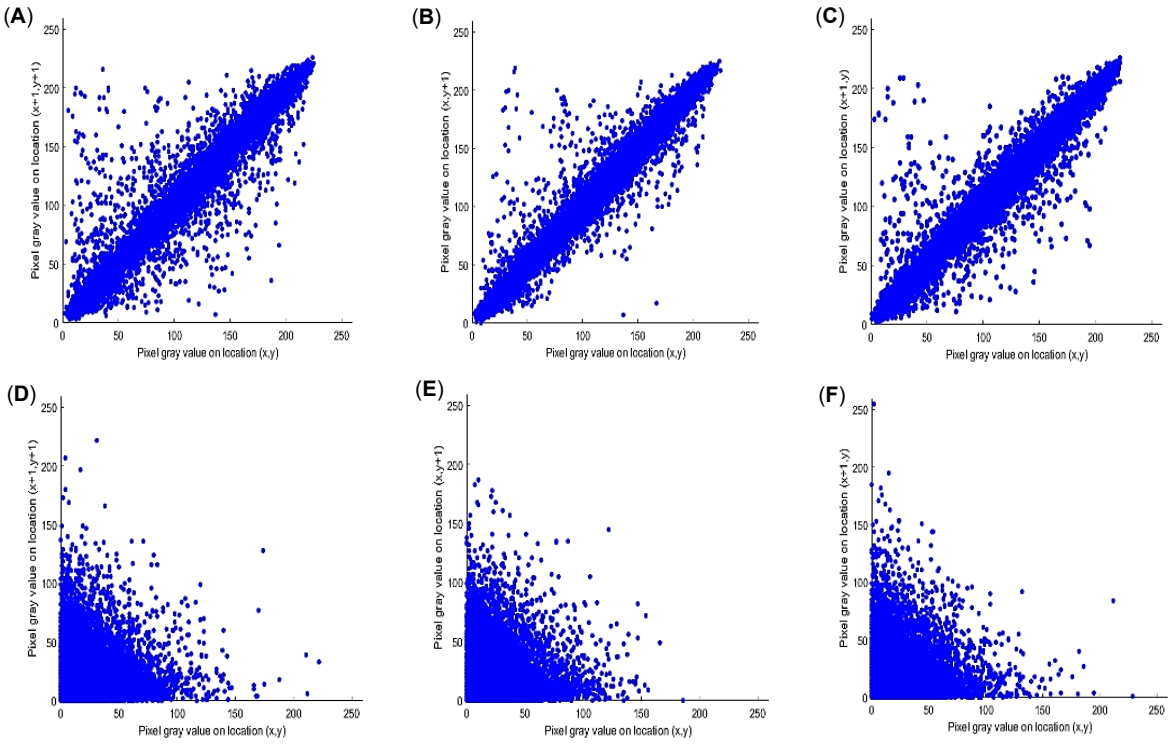

Figure 7. Correlation curves of 15000 adjacent pixels pairs (**A-C**) input image (**D-F**) encrypted image in the diagonal, vertical, horizontal directions, respectively

3.3. Information Entropy

The information entropy is a statistical measure employed to assess the level of randomness in the pixel values of the ciphered images. Mathematically, the information entropy of an image $H(k)$ of a source k can be expressed as follows:

$$H(k) = -\sum_{i=0}^{256} p(k_i) \log p(k_i) \tag{17}$$

where $p(k_i)$ represents the probability of k_i. The information entropy value of a grayscale image varies between 0 and 8. An entropy value approaching zero indicates that the image exhibits a low degree of randomness. In contrast, an entropy value nearing 8 signifies a high degree of randomness within the image. In this study, the entropy of the original image "Peppers" is 7.5925, while that of its ciphered image using the present system is 7.9977. Table 2 represents the entropy values for various test images and their corresponding encrypted images. These results demonstrate that the information entropy values for ciphertexts approached the theoretical value limit of 8, indicates a near perfect uniform gray levels distribution; thereby making the cryptosystem in this study robust against statistical cryptanalysis.

Table 2. Information entropy analysis for various test images.

Images	Original Image	Encrypted Image
Peppers	7.5925	7.9977
Baboon	7.2925	7.9976
Cameraman	7.0480	7.9974

3.4. Sensitivity Analysis

Sensitivity analysis of the proposed method of varying the gyrator angle was performed by calculating the RMSE between the initial input image and the corresponding retrieved output image. Figure 8 demonstrates the plots of the key sensitivity analysis. It can be seen that even with slight variations in the gyrator angle, the RMSE values change sharply, which verifies the efficacy of these angles in augmenting security. Also, we have tested the sensitivity keys of chaotic deterministic phase mask. The results of secret-keys sensitivity analysis are given in Figure 9. When the bifurcation parameter (a) of chaotic tent map is changed by 1.45, the decrypted image is shown in Figure 9(A). When the initial value (x_0) of tent map is altered by 0.53, the decrypted image is exhibited in Figure 9(B). When the $CDPM$ is substituted with the random phase mask, the decrypted image is given in Figure 9(C). As illustrated from this figure, the decrypted images are completely unrecognizable even slight changes in any of the secret keys. Thus, these results demonstrate that our proposed approach is valid.

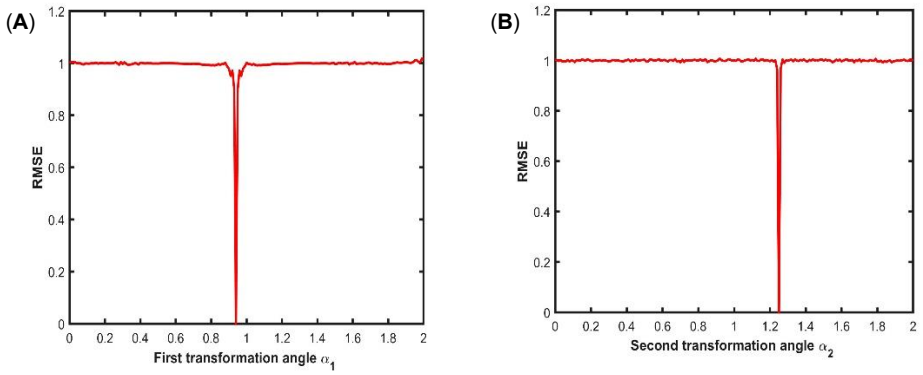

Figure 8. Key sensitivity analysis for transformation angle α versus RMSE for (**A**) rotation angle α_1 (**B**) rotation angle α_2

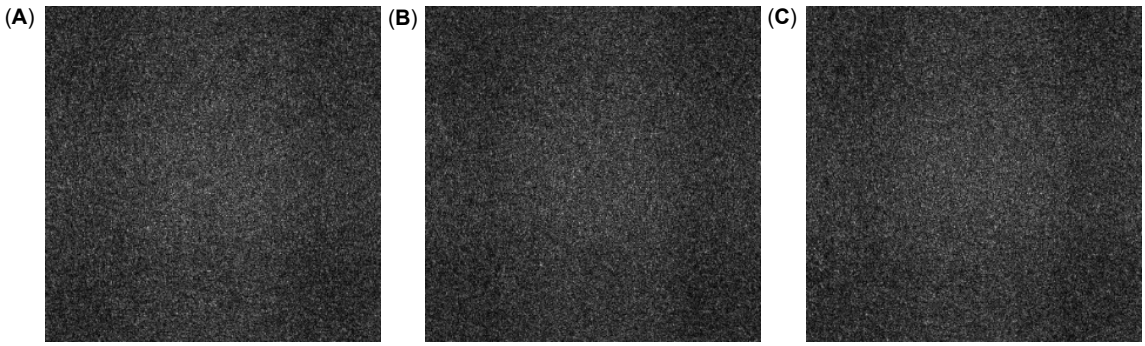

Figure 9. Decrypted images (**A**) with incorrect the bifurcation parameter (a) (**B**) with incorrect the initial value (x_0) (**C**) with wrong key (random phase mask is used in placed of $CDPM$).

3.5. NPCR and UACI Test

In this subsection, we carry out further evaluations to analyze the performance of encryption system against the differential attack by using two common metrics: number of pixel change rate

(NPCR) and unified average changing intensity (UACI). These two common metrics are defined by the following equations:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{18}$$

$$UACI = \frac{1}{M \times N} \times \left[\frac{C_1(i,j) - C_2(i,j)}{256}\right] \times 100\% \tag{19}$$

where $D(i,j) = \begin{cases} 0, & if \ C_1(i,j) = C_2(i,j) \\ 1, & if \ C_1(i,j) \neq C_2(i,j) \end{cases}$, C_1 and C_2 are different encrypted images that one pixel is different for their original images, and $M \times N$ is the size of the encrypted images. The computed values of NPCR and UACI are presented in Table 3. The proposed approach achieves high NPCR and appropriate UACI values. The high NPCR value indicates that the positioning of every pixel is extensively randomized. Also, the UACI value is within the acceptable range, showing that the whole grey levels of pixels in the ciphered image have been changed, and making it indistinguishable.

Table 3. NPCR and UACI values.

Methods	NPCR (%)	UACI (%)
Our proposed	99.63	29.20
Ref. (Unnikrishnan, 2000)	99.65	28.05
Ref. (Qasim & Mohammed, 2023)	99.69	29.11
Ref. (Mohammed & Qasim, 2024a)	99.73	30.18

3.6. Key Space Analysis

The key space of the proposed cryptosystem is examined in this section. This involves considering the entirety of possible key combinations, encompassing the *CDMPs* and the rotation angles of the *GT* operator. Both CDPMs ($CDPM_1$ and $CDPM_2$) are $M \times N$ pixels with possible values L for each pixel. The attempts number required to recover both CDPM is the $L^{5(M\times N)}$ order. When $L = 256$ gray levels and $M = N = 512\, pixels$, the total number of *CDPMs* that would need to be tested is $256^{5\times512\times512} = 256^{1310720}$. Lastly, the total key space of the suggested encryption and decryption systems is obtained by multiplying the sensitivity of the rotation angles of the *GT* operator by the combinations number of the two *CDPM*: $(10^{2(2)} \times 256^{1310720})$. Since the total key space of this work is very large, a brute force attack or exhaustive attack would be impractical for encrypting and decrypting the data contained in the work.

3.7. Robustness Analysis

The resilience of the proposed encryption method against occlusion and additive noise attacks was assessed. To evaluate the ability of the proposed method to prevent occlusion, the decryption process is performed by occluding a portion of the encrypted image. Here, we have discussed the occlusion attacks with varying degrees of data occlusion. Figure 10(A) displays the plot of the RMSE values versus as a function of the percentage of occluded pixels for the image. From this figure, it can be noted that the RMSE values increase with increasing occlusion, which indicates lower- quality recovered images. Although the recovered image quality decreases with an increase in the occluded area, it is recognizable even with an occlusion percentage greater than 50%. Thus, the proposed system is resistant to data occlusion attack. Finally, the impact of additive Gaussian noise on the feasibility of the proposed system was also tested employing the following noise model:

$$\acute{E}(x,y) = E(x,y)\left[1 + n\, \sigma_{0,1}(x,y)\right] \tag{20}$$

where $\acute{E}(x,y)$ and $E(x,y)$ refer to the encrypted image after and before adding Gaussian noise, respectively. While *n* is the noise factor and $\sigma_{0,1}(x,y)$ refers to the random information with mean value 0 and unity standard deviation. A curve of RMSE is given in Figure 10(B) employing the image $\acute{E}(x,y)$ obtained with different values n from 0 to 1. From this figure, it can be observed that the RMSE increases with an increase in noise factor (n). Thus, this proposed system is robust against Gaussian noise, which demonstrates high resilience for transmission over noisy or unsecure channels.

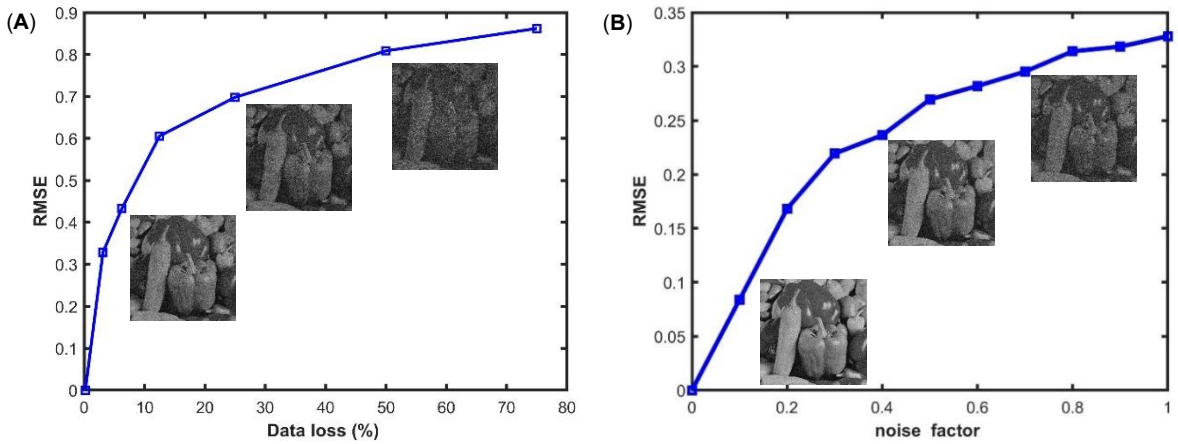

Figure 10. Robustness analysis; (**A**) RMSE as a function of data loss (**B**) RMSE as a function of noise factor

3.8. Comparison Analysis

In this subsection, we conducted a comparative analysis of the proposed scheme with existing systems introduced in (Khurana and Singh, 2022; Su et al., 2017; Yadav and Singh, 2024; Yadav et al., 2025) based on transformations, type of masks and images, chaotic maps, number of security parameters, resistance against attacks, and cryptosystem type. Table 4 presents the results of the comparison analysis. From the results, it can be demonstrated that the proposed system defends against attacks.

Table 4. Comparative analysis of the present system.

Parameters	**Schemes**				
	Khurana et al., 2022	**Yadav et al., 2024**	**Yadav et al., 2025**	**Su et al., 2017**	**Present system**
Transform domain used	Gyrator domain	Fractional Hartley domain	Fractional Hartley domain	Fresnel domain	Gyrator domain
Types of masks	Chaotic zone plate phase mask (CZPM)	Random phase mask (RPM)		Chaotic random phase masks (CRPM)	Chaotic deterministic phase mask (CDPM)
Chaotic maps	Logistic map	Umbrella map		Duffing map and Tinker bell map	Tent map
Types of images	Grayscale image	Grayscale and binary images	Grayscale and binary images	Color image	Grayscale image
Number of security parameters	Initial value and bifurcation parameter of logistic map, focal length, wavelength, two rotational angels	13 keys	9 keys	Initial values and control parameters of chaotic maps, wavelength, and Fresnel transform distance	Initial value and bifurcation parameter of tent map, number of subkeys of liner phase mask, two rotational angels
Statistical metrics	MSE	CC, entropy, 3-D plot, and histogram	CC, MSE, information entropy, histogram plots, and mesh plot	CC, SSIM	MSE, RE, SSIM, RMSE, PSNR, information entropy, histogram plot, 3-D plot
Resistance against attacks	Occlusion, KPA, CPA, and special attacks	Noise attack, cropping attack, and special iterative attack	KPA, CPA, and iterative attack analysis	Noise, and cropping attacks	Noise, cropping, and differential attacks
Cryptosystem type	Asymmetric	Asymmetric	Asymmetric	Symmetric	Symmetric

4. CONCLUSION

Our study proposes an optical image cryptographic system that employs a chaotic deterministic phase key in the gyrator domain transform. The chaotic deterministic phase key is based on a linear combination of the number of subkeys and chaotic tent map, which enhances the security of the encryption system by expanding the key space and offers extra security parameters. The experimental numerical findings in this study show that the suggested chaotic deterministic phase mask based

cryptographic system has many advantages compared with the traditional double random phase encryption. First, the proposed system outcomes resemble to the conventional DRPE technique in terms of image retrieval. Second, our findings demonstrate the efficacy of the proposed method in recovering the primary image even when subjected to distortions resulting from occlusion in the ciphered image. Third, the generation of a phase mask is based on a simple set of numeric parameters. Consequently, the recovery of the image does not require the transmission of the enter mask but only the relevant set of parameters. Fourth, the proposed system avoids problems that result from misalignment. Finally, the GT operation for various angels can only be achieved by appropriately rotating cylindrical lenses, while maintaining fixed distances between the lenses and the input-output planes. Moreover, the proposed cryptosystem is secure in real time breaches due to its substantial key space of $10^{2(2)} \times 256^{1310720}$, which is sufficiently large. Moreover, our proposed system is a suitable for securing sensitive information transmission, such as satellite communication, biometric techniques, and medical imaging, owing to its exceptional resistance against 50% data occlusion, Gaussian noise, and brute force attacks. Future research study will focus on expanding the proposed approach to multi- channel color image encryption. Additionally, we aim to study deep learning algorithms to evaluate the resistance of cryptosystem against advanced chosen plaintext and known plaintext attacks.

ACKNOWLEDGEMENT
The author would like to thank the referees for helpful comments.

CONFLICT OF INTEREST
The authors declare no conflicts of interest.

AUTHOR CONTRIBUTION
Israa M. Qasim: conducted data recording and validation, developed methodology, and wrote original draft preparation. Emad A. Mohammed: conducted data validation, and reviewed and edited the writing.

DATA AVAILABILITY
The supporting information is available from the corresponding author upon reasonable request.

DECLARATION OF GENERATIVE AI
During the preparation of this work the authors used Paperpal in order to enhance language clarity, correct grammar, and improve overall readability. After using this tool/service, the author(s) reviewed and edited the content as needed and take full responsibility for the content of the published article.

ETHICS
Not applicable.

REFERENCES

Abuturab MR. (2014). Securing multiple color information by optical coherent superposition based spiral phase encoding. *Optics and Lasers in Engineering*, 56, 152–163. doi:10.1016/j.optlaseng.2013.12.018

Barrera JF, Henao R, Torroba R. (2005). Optical encryption method using toroidal zone plates. *Optics Communications*, 248(1–3), 35–40. doi:10.1016/j.optcom.2004.11.086

Girija R, Singh H. (2018). A cryptosystem based on deterministic phase masks and fractional Fourier transform deploying singular value decomposition. *Optical and Quantum Electronics*, 50, 210. doi:10.1007/s11082-018-1472-6

Guo Y, Huang Q, Du J, Zhang Y. (2001). Decomposition storage of information based on computer-generated hologram interference and its application in optical image encryption. *Applied Optics*, 40(17), 2860–2863. doi:10.1364/AO.40.002860

Hilborn RC. (2000). *Chaos and nonlinear dynamics: an introduction for scientists and engineers*. Oxford university press.

Hou J, Situ G. (2022). Image encryption using spatial nonlinear optics. eLight, 2(1), 3. doi:10.1186/s43593-021-00010-y

Jassim RA, Mohammed EA. (2022). Asymmetric optical cryptosystem in the fractional fourier domain using photon counting imaging. *Basrah Journal of Science*, 40, 512–525. doi:10.29072/basjs.20220218

Javidi B, Carnicer A, Ahmadi K, Awatsuji Y, Chen W, Fournel T, Genevet P, Guo J, He W, Hébert M, Jana A, Lam EY, Long GL, Matoba O, Mi Z, Moon I, Nishchal NK, Pan D, Peng X, Pinkse PWH, Shi Y, Situ G, Stern A, Wang X, Xia T, Xiao Y, Zhenwei X, Zh S. (2025). Roadmap on optics and photonics for security and encryption. *IEEE Access*, 13, 140087–140117. doi:10.1109/ACCESS.2025.3597226

Javidi B, Carnicer A, Yamaguchi M, Nomura T, Pérez-Cabré E, Millán MS, Nishchal NK, Torroba R, Barrera JF, He W, Peng X, Stern A, Rivenson Y, Alfalou A, Brosseau C, Guo C, Sheridan JT, Situ G, Naruse M, Matsumoto T, Juvells I, Tajahuerce E, Lancis J, Chen W, Chen X, Pinkse PWH, Mosk AP, Markman A. (2016). Roadmap on optical security. *Journal of Optics*, 18(8), 083001. doi:10.1088/2040-8978/18/8/083001

Khalf HA, Mohammed EA. (2025a). Optical asymmetric cryptosystem based on interference and spatial encoding for two user authenticators. In *Innovative Computing and Communications*. Springer Nature Singapore, p. 609–624. doi:10.1007/978-981-96-7137-3_42

Khalf HA, Mohammed EA. (2025b). Optical double-image cryptosystem based on interference principle and spatial encoding. *Optik*, 329, 172344. doi:10.1016/j.ijleo.2025.172344

Khurana M, Singh H. (2018). Optical image encryption using fresnel zone plate mask based on fast walsh hadamard transform. *AIP Conference Proceedings*, 1953, 140043. doi:10.1063/1.5033218

Khurana M, Singh H. (2022). Asymmetric image cryptosystem based on chaotic zone plate phase mask and arnold transform. In *Lecture Notes on Data Engineering and Communications Technologies*, 73, 45–51. doi:10.1007/978-981-16-3961-6_5

Layek GC. (2015). *An Introduction to Dynamical Systems and Chaos*. *An Introduction to Dynamical Systems and Chaos*. New Delhi: Springer India. doi:10.1007/978-81-322-2556-0

Liao M, Zheng S, Pan S, Lu D, He W, Situ G, Peng X. (2021). Deep-learning-based ciphertext-only attack on optical double random phase encryption. *Opto-Electronic Advances*, 4(5), 200016–200016. doi:10.29026/oea.2021.200016
Liu S, Guo C, Sheridan JT. (2014). Introduction to optical signal processing. *Asian Journal of Physics*, 23(3), 303–332.
Luan G, Li A, Chen Z, Huang C. (2020). Asymmetric optical image encryption with silhouette removal using interference and equal modulus decomposition. *IEEE Photonics Journal*, 12(2), 1–8. doi:10.1109/JPHOT.2020.2963921
Maan P, Singh H. (2018). Non-linear Cryptosystem for image encryption using radial hilbert mask in fractional fourier transform domain. *3D Research*, 9, 53. doi:10.1007/s13319-018-0205-8
Mohammed EA, Saadon HL. (2019). Simultaneous verification of optical triple-image encryption using sparse strategy. *Journal of Physics: Conference Series*, 1234(1), 012037. doi:10.1088/1742-6596/1234/1/012037
Mohammed EA, Qasim IM. (2024a). Security augmenting of optical cryptosystem based on linear canonical transform domain using a full phase encoding technique. *Physica Scripta*, 99(6), 065112. doi:10.1088/1402-4896/ad4316
Mohammed EA, Qasim IM. (2024b). Optical double-image cryptosystem based on a joint transform correlator in a linear canonical domain. *Applied Optics*, 63(22), 5941. doi:10.1364/AO.525462
Mohammed EA, Saadon HL. (2016). Optical double-image encryption and authentication by sparse representation. *Applied Optics*, 55(35), 9939–9944. doi:10.1364/AO.55.009939
Mohammed EA, Saadon HL. (2019). Sparse phase information for secure optical double-image encryption and authentication. *Optics & Laser Technology*, 118, 13–19. doi:10.1016/j.optlastec.2019.04.035
Pérez-Cabré E, Mohammed EA, Millán MS, Saadon HL. (2015). Photon-counting multifactor optical encryption and authentication. *Journal of Optics*, 17(2), 025706. doi:10.1088/2040-8978/17/2/025706
Perez RA, Pérez-Cabré E, Vilardy JM, Millán MS, Torres CO. (2023). Double image encryption system using a nonlinear joint transform correlator in the fourier domain. *Sensors*, 23(3), 1641. doi:10.3390/s23031641
Qasim IM, Mohammed EA. (2023). Optical image encryption based on linear canonical transform with sparse representation. *Optics Communications*, 533, 129262. doi:10.1016/j.optcom.2023.129262
Qasim IM, Mohammed EA. (2025). Secure optical image encryption and authentication based on phase information and Collins diffraction transform. *Journal of Theoretical and Applied Physics*, 19(1), 1–10. doi:10.57647/j.jtap.2025.1901.08
Rawat N, Hwang I, Shi Y, Lee B. (2015). Optical image encryption via photon-counting imaging and compressive sensing based ptychography. *Journal of Optics*, 17(6), 065704. doi:10.1088/2040-8978/17/6/065704
Refregier P, Javidi B. (1995). Optical image encryption based on input plane and Fourier plane random encoding. *Optics Letters*, 20(7), 767–769. doi:10.1364/OL.20.000767
Rodrigo JA, Alieva T, Calvo ML. (2007a). Applications of gyrator transform for image processing. *Optics Communications*, 278(2), 279–284. https://doi.org/10.1016/j.optcom.2007.06.023
Rodrigo JA, Alieva T, Calvo ML. (2007b). Gyrator transform: properties and applications. *Optics Express*, 15(5), 2190–2203. doi:10.1364/oe.15.002190
Sachin, Kumar R, Sakshi, Yadav R, Reddy SG, Yadav AK, Singh P. (2024). Advances in optical visual information security: a comprehensive review. *Photonics*, 11(1), 99. doi:10.3390/photonics11010099
Shi Y, Li T, Wang Y, Gao Q, Zhang S, Li H. (2013). Optical image encryption via ptychography. *Optics Letters*, 38(9), 1425–1427. doi:10.1364/OL.38.001425
Singh H. (2016). Devil's vortex Fresnel lens phase masks on an asymmetric cryptosystem based on phase-truncation in gyrator wavelet transform domain. *Optics and Lasers in Engineering*, 81, 125–139. doi:10.1016/j.optlaseng.2016.01.014
Situ G, Zhang J. (2004). Double random phase encoding in the Fresnel domain. *Optics Letters*, 29(14), 1584–1586.
Su Y, Tang C, Li B, Chen X, Xu W, Cai Y. (2017). Single-lens Fourier-transform-based optical color image encryption using dual two-dimensional chaotic maps and the Fresnel transform. *Applied Optics*, 56(3), 498–505. doi:10.1364/AO.56.000498
Sun W, Wang L, Wang J, Li H, Wu Q. (2018). Optical image encryption technique based on hybrid-pattern phase keys. *Current Optics and Photonics*, 2(6), 540–546. doi:10.3807/COPP.2018.2.6.540
Tian M, Sun G, Song W, Liu Z, Chen H. (2023). Image cryptosystem in optical gyrator transform domain using audio keys. *Electronics*, 12(13), 2816. doi:10.3390/electronics12132816
Unnikrishnan G. (2000). Double random fractional Fourier-domain encoding for optical security. *Optical Engineering*, 39(11), 2853. doi:10.1117/1.1313498
Wang X, Zhang Y, Zhang L, Zhou Q, Yao M. (2024). Encoded-image-based authentication utilizing diffractive-imaging scheme and secret-key-assisted phase retrieval. *Optics and Laser Technology*, 168, 110013. doi:10.1016/j.optlastec.2023.110013
Wang Y, An B, Xu W, Zhang H, Li F, Su Y. (2024). Optical image hiding based on chaotic fingerprint phase mask and diffractive imaging. *Journal of Optics*, 53(3), 1994–2004. doi:10.1007/s12596-023-01353-0
Xiao Y, Zhou L, Chen W. (2019). Experimental demonstration of ghost-imaging-based authentication in scattering media. *Optics Express*, 27(15), 20558–20566. doi:10.1364/oe.27.020558
Xiong Y. (2023). Security analysis on optical cryptosystem based on interference and phase-retrieval technique. *Optics & Laser Technology*, 158, 108917. doi:10.1016/j.optlastec.2022.108917
Xiong Y, Gu J, Kumar R. (2023). Collision in a phase-only asymmetric cryptosystem based on interference and phase-truncated Fourier transforms. *Optical and Quantum Electronics*, 55(8), 667. doi:10.1007/s11082-023-04943-1
Yadav R, Sachin, Singh P. (2024). Multiuser medical image encryption algorithm using phase-only CGH in the gyrator domain. *Journal of the Optical Society of America A*, 41(3), 63–72. doi:10.1364/JOSAA.507308
Yadav R, Singh SP. (2024). Multidomain asymmetric image encryption using phase - only CGH , QZS method and Umbrella map. *Journal of Optics*, 54(5), 3108–3125. doi:10.1007/s12596-024-02106-3
Yadav R, Singh P. (2025). Security enhancement of three POMs based interference algorithm using elliptic curve cryptography. *Journal of Optics*, 1-18. doi:10.1007/s12596-025-02962-7
Zamrani W, Ahouzi E. (2020). Optical image encryption process using triple deterministic spherical phase masks array. *Communications in Computer and Information Science*, 1264, 241–250. doi:10.1007/978-3-030-61143-9_20