IRAQI JOURNAL OF APPLIED PHYSICS
Vol. 22, No. 2, April-June 2026, pp. 178-190

Optical Double-image Cryptosystem Based on Phase-truncated Using Random Modulus Decomposition and Polar Decomposition

Abbas F. Mohammed [1,2*]
Emad A. Mohammed [1]

[1] Department of Physics, College of Science, University of Basrah, Basrah, IRAQ
[2] General Directorate of Education in Najaf, Ministry of Education, Najaf, IRAQ
* Corresponding author email: abbasfadel918514@gmail.com

A novel optical double-image encryption is proposed, combining phase truncation with spatial encoding, random modulus decomposition, and polar decomposition. Two plaintext images are encrypted into a single ciphertext using three public keys and four private keys, ensuring enhanced security against tampering and unauthorized access. Robustness was verified through simulations under noise and occlusion, with results showing high resilience and reliability. Statistical analysis revealed that minor key variations significantly affect decryption, reinforcing security. Comparative evaluations demonstrated superior performance over existing techniques in robustness, attack resistance, and mitigation of the silhouette problem. Quality assessment using MSE, PSNR, and SSIM confirmed near-perfect reconstruction, with MSE values of 1.57479e-25 and 6.82889e-26, SSIM of 1, and PSNR values of 296 and 299. These findings validate the proposed method's high precision, security, and efficiency for advanced optical encryption applications.

Keyword: Encryption; Cryptosystem; Modulus decomposition, Polar decomposition
Received: 15 June 2025; Revised: 31 August 2025; Accepted: 7 September 2025

1. Introduction

Optical encryption has attracted considerable interest for enhancing cryptographic systems. Its distinct physical properties, including parallel processing, multiple degrees of freedom (such as phase, wavelength, and polarization), fast computation, and multidimensional functionality, make it a powerful tool for secure data encryption [1-5]. Refreger and Javidi introduced the double random phase encoding DRPE optical cryptosystem in 1995, and it has since gained widespread recognition [6]. In DPRE, an input image is encrypted into ciphertext by applying white stationary noise. This process uses two random phase masks, one in the input domain and the other in the Fourier domain. Many transform domains, have been applied in DRPE such as fractional Fourier [7], Fresnel [8], Gyrator [9], and Collins diffraction [10]. However, the linear properties of DPRE-based cryptosystems make them vulnerable to different cryptographic attacks such as known plaintext attack (KPA) [11], chosen plaintext attack (CPA) [12], and chosen ciphertext attack (CCA) [13]. The security of these cryptosystems has been strengthened using various methods, such as optical interference [14], joint transform correlators [15], sparse representation [16,17], and photon counting [18]. The triple random phase masks encoding (TRPE), introduced by Ahouzi et al. [19], was claimed to be resistant to KPA, CPA, and CCA. However, it was later found that the symmetric TRPE is still vulnerable to deep learning attacks [20]. An analysis of TRPE in the Fresnel domain was performed by Kumari et al. to improve security by using parameters from the Fresnel transform [21]. Later, observed that the third random phase mask in this scheme does not affect the image decryption process [22]. To address this weakness, an asymmetric cryptosystem based on phase truncation in the Fourier domain was proposed by Qin and Peng [23]. In this cryptosystem, the encryption keys are not same in decryption process. However, it was later discovered that the asymmetric cryptosystem based on phase-truncated in Fourier transform remains vulnerable to KPA [24] and specific attacks [25]. To enhanced the security, various encryption systems have been introduced, such as asymmetric double image algorithm system [26], and phase truncation methods applied in fractional Fourier domain [27], and Fresnel domain [28]. Although their advantages, these cryptosystems susceptible to information leakage [29]. Therefore, several optical encryption methods have been developed to mitigate this issue. In [30], a two images encryption approach based on the Fresnel phase truncation technique has been proposed. For this reason, many techniques applied to processing the linearity problem. A number of asymmetric cryptosystem have been suggested, such as those polar decomposition [31], and modulus decomposition techniques based on asymmetric methods, including singular value decomposition [32], equal modulus

decomposition [33], and random modulus decomposition [34].

In this study, an advanced optical cryptosystem has been introduced by integrating phase truncation in the Fresnel domain with random modulus decomposition, polar decomposition, and spatial encoding. This integration has been employed to overcome the linearity of conventional systems and to reduce the risk of information leakage. Within the proposed design, two plaintext images have been encrypted into a single ciphertext. Decryption has been structured to depend on four private keys, ensuring that unauthorized recovery remains infeasible without full key knowledge. The combined use of these complementary techniques has been shown to enhance robustness and increase sensitivity to key variations. As a result, reliable protection against common vulnerabilities in optical encryption schemes has been effectively achieved.

The structure of this article is as follows: Section 2 offers a comprehensive explanation of the theoretical framework and the steps involved in the encryption and decryption processes. Section 3 focuses on numerical experiments and includes a security analysis. Lastly, section 4 presents the conclusion.

2. Related Principles

In this section, the methodology of the proposed cryptosystem scheme is outlined, with particular emphasis on the integration of spatial encoding, random modulus decomposition, and polar decomposition. As illustrated in Fig. (3a), the encryption procedure begins with the spatial encoding of two plaintext images, which are subsequently processed through the phase truncation method to generate an intermediate ciphertext representation. To address the inherent vulnerability of phase truncation to information leakage, additional layers of security have been incorporated by employing random modulus decomposition and polar decomposition. The former introduces nonlinearity and amplitude complexity, while the latter ensures key diversification and structural obfuscation, thereby strengthening resistance against cryptanalytic and statistical attacks. Through this carefully structured combination of techniques, the system is designed to achieve both high robustness and improved security, while simultaneously ensuring reliable image recovery under authorized decryption conditions.

2.1 Spatial Encoding Technique (SE)

Spatial encoding is employed to interleave the pixel information of $f_1(x)$ and $f_2(x)$, within a unified composite plane, thereby allowing both images to be processed concurrently in subsequent modulation stages. The spatial encoding is carried out using a random amplitude mask (RAM) placed along the encoding path. One plaintext is transformed into a pseudorandom amplitude mask, while the other becomes a pseudorandom phase mask. For simplicity, we will represent the coordinates using a one-dimensional notation. Let the two plaintexts, denoted as $f_1(x)$ and $f_2(x)$, have pixel values normalized between 0 and 1. The random amplitude mask, represented as $M(x)$, is defined as $M(x)$=rand(x), where the function rand generates a uniform distribution over the range [0, 1]. Here, (x) refers to the coordinates within the image domain. By using the RAM, the two plaintexts are encrypted into a complex-valued distribution, $\xi(x)$ through spatial encoding. The amplitude and phase components of $\xi(x)$ are represented as:

$$A(x) = |\xi(x)| = \sin\theta_1(x) \quad (1a)$$

$$\gamma(x) = arg[\xi(x)] = exp\,[i.\theta_2(x)] \quad (1b)$$

Here $A(x)$ and $\gamma(x)$ are the amplitude and phase information of a complex function ($\xi(x)$), and $\theta_1(x)$ and $\theta_2(x)$ are defined as follows:

$$\theta_1(x) = M(x) + \frac{1}{2\pi} arcsin\frac{f_1(x)}{2};$$

$$\theta_2(x) = 2\pi M(x) + \frac{1}{2\pi} arcsin\frac{f_2(x)}{2} \quad (2)$$

where $arcsin\{.\}$ refers to the inverse sin function. Then

$$\xi(x) = sin[M(x) + \frac{1}{2\pi} arcsin\frac{f_1(x)}{2}].exp\left[i.\{2\pi M(x) + \frac{1}{2\pi} arcsin\frac{f_2(x)}{2}\}\right] \quad (3)$$

2.2 Random Modulus Decomposition (RMD)

The complex distribution $\xi(x)$ is separated into two complex-valued masks, $PK_1(x)$ and $PK_2(x)$, using random modulus decomposition, as illustrated in Fig. (1). Based on the geometric relationship and the random distribution of $\alpha(x)$ and $\beta(x)$, $PK_1(x)$ and $PK_2(x)$ can be represented as:

$$PK_1(x) = \frac{A(x)\sin\beta(x)}{\sin(\alpha(x)+\beta(x))}\, exp[\, i\gamma(x) - \alpha(x)] \quad (4)$$

$$PK_2(x) = \frac{A(x)\sin\alpha(x)}{\sin(\alpha(x)+\beta(x))} exp[\, i\gamma(x) + \beta(x)] \quad (5)$$

here, $\alpha(x)$ and $\beta(x)$ are the random phase distribution function in the range [0, 2π], $PK_2(x)$ represented as private key [35]

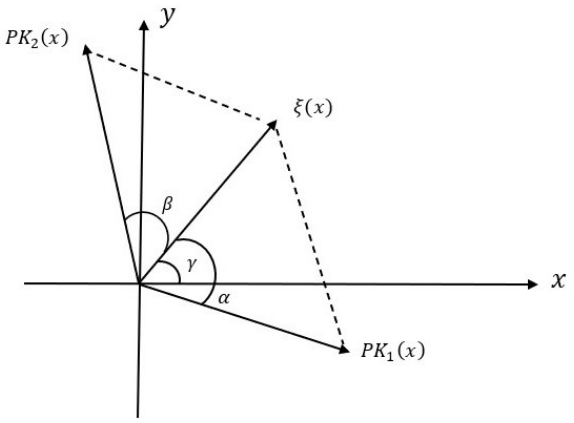


Fig. (1) Principle of random modulus decomposition

2.3 Polar Decomposition (PD)

The polar decomposition of the complex image $PK_1(x)$ is separated into linearly independent factors [31,36]. PD of matrix $PK_1(x)$ can be shown as [31]:

$$PD[PK_1(x)] = [SUV] \quad (6)$$

$$PK_1 = U * S \quad (7a)$$

$$PK_1 = V * S \quad (7b)$$

here, S is a rotational matrix, and U and V known as the stretching matrices. The input matrix $PK_1(x)$ can be reconstructed by using S matrix as private key, and one of stretching matrices (U or V). Figure (2) shows the geometrical representation of polar decomposition and equation (6) shows the PD operation process. In this proposed cryptosystem, three public keys (M, θ, β) are utilized for encryption, and four private keys ($PK_2(x)$, $PK_3(x)$, $PK_4(x)$, S) are employed for decryption procedure.

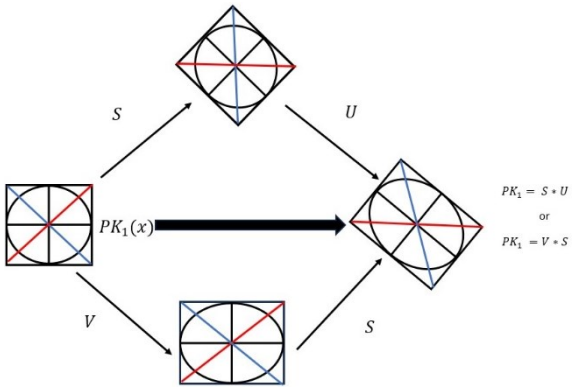


Fig. (2) Representation of polar decomposition

3. Proposed Cryptosystem

The proposed cryptosystem consists of the following encryption and decryption processes. In the encryption process, as shown in Fig. (1a), after encoding the two input images in one plaintext according to the Eq. (3), the result $\xi(x)$ separates into two complex functions by RMD, as illustrate in Eqs. (4) and (5), then applied PD on $PK_1(x)$, as given in Eq. (6), the signal V is further modulated with Fresnel transform (FST) followed by phase truncation and phase reservation which produce $G(u_1)$ and $PK_3(u_1)$, respectively, this process can be mathematically represented as:

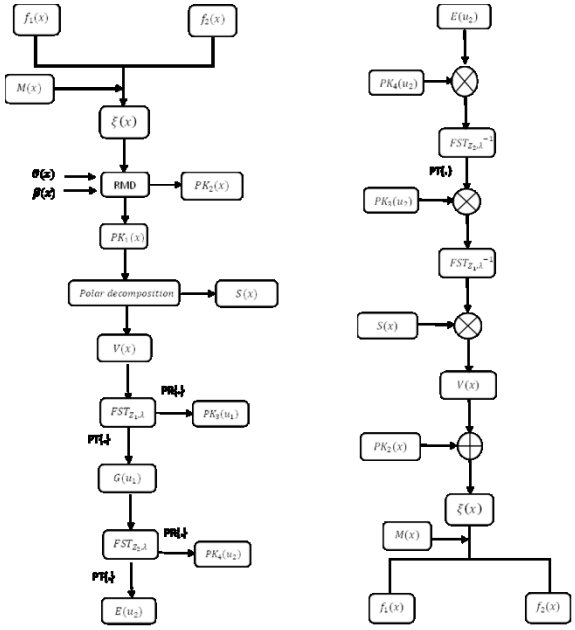
$$G(u_1) = PT\{FST_{(Z_1,\lambda)}[V]\} \quad (8)$$

$$PK_3(u_1) = PR\{FST_{(Z_1,\lambda)}[V]\} \quad (9)$$

here, (u) represent the coordinates in the Fresnel domain, while $FST_{Z1,\lambda}\{.\}$ refer to the Fresnel transform operator, which depends on the diffraction distance Z_1 and the wavelength λ. The function $PK_3(u_1)$ is extracted and serves as private key. Figure (3a) shows all details about encryption process. Then, the second Fresnel transform operation with the diffraction distance Z_2 is applied to the function $G(u_1)$. Finally, the ciphertext $E(u_2)$ and the private key $PK_4(u_2)$ are generated by performing phase truncation and phase reservation as following relation:

$$E(u_2) = PT\{FST_{(Z_2,\lambda)}[G(u_1)]\} \quad (10)$$

$$PK_4(u_2) = PR\{FST_{(Z_2,\lambda)}[G(u_1)]\} \quad (11)$$



(a) **(b)**

Fig. (3) Flowchart of provided cryptosystem: (a) encryption process, (b) decryption process

In the decryption process as shown in Fig. (3b), the users with authorized access can be retrieve the input complex function $\xi(x)$ as:

$$\xi(x) = \left\{FrT_{(-Z_1,\lambda)}\left[PT\left[FrT_{(-Z_2,\lambda)}[\,E(u_2).\exp[iPK_4(u_2)]]\right]\right.\right.$$
$$\left.\left.\cdot\exp[iPK_3(u_1)] * S\right\} + PK_2 \quad (12)$$

Then, the recovered image according to Eq. (1) and Eq. (2) can be obtained as:

$$f_1(x) = 2\sin[\,2\pi\,.\theta_1(x) - 2\pi\,.M(x)]$$
$$f_2(x) = 2\sin\,[\,\theta_2(x) - 2\pi\,.M(x)] \quad (13)$$

Here, $\theta_1(x)$ and $\theta_2(x)$ are given by:

$$\theta_1(x) = arcsin\,\{PT[\xi(x)]\}$$
$$\theta_2(x) = arcsin\,\{PR[\xi(x)]\} \quad (14)$$

The two original images are retrieved by extracting the real and imaginary components of $\xi(x)$ and Eq. (14).

4. Results and Discussion

To assess the effectiveness of the proposed method, numerical simulations were conducted using MATLAB (R2014b). The simulations ran on a 64-bit operating system equipped with an Intel Core i5-8250U processor (1.60 GHz, up to 1.80 GHz), Windows 10 pro, and 12 GB of RAM. Two grayscale images, each measuring 512×512 pixels, were used as input images in the evaluation, as shown in Figs. (4a) and 4(b). Figure (4c) represents the random amplitude mask $M(x)$ that used in spatial encoding. Two public keys $\alpha(x)$ and

$\beta(x)$, are used in RMD process as shown in Figs. (4d) and (4e) to generate two complex valued masks $PK_1(x)$ and $PK_2(x)$ as shown in Figs. (4f) and (4g), respectively. Then, $PK_1(x)$ separated into three matrices by act polar decomposition into S as a rotational matrix which used as private key, and U and V known as the stretching matrices utilized one of them with $PK_1(x)$. Figures (4h), (4i), and (4j) represent U, V, and S, respectively. After that, the phase-truncated in Fresnel domain is applied to obtained two private keys $PK_3(u_1)$ and $PK_4(u_2)$, as shown in Figs. (4k) and (4l), respectively. Finally, the encrypted image is obtained as in Fig. (4m). In the decryption process, the input images are retrieved by acting the correctly security keys as in Figs. (4n) and (4o).

4.1 Performance Analysis

The quality of the decrypted images was assessed using widely recognized quantitative metrics, including mean squared error (MSE) [37], peak signal to noise ratio (PSNR) [38], and structural similarity index measure (SSIM) [39]. The corresponding results, obtained from the proposed phase-truncation-based cryptosystem, are summarized, and compared with other cryptosystems in table (1). These metrics demonstrate that the reconstructed image exhibit exceptionally high resolution and near-perfect fidelity to the originals.

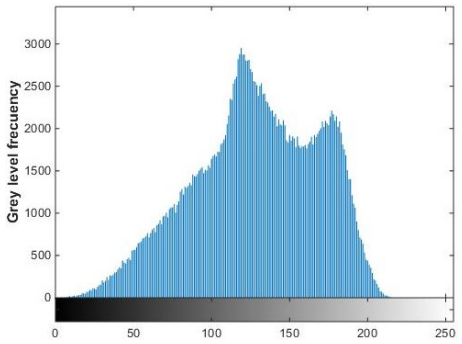
Table (1) Comparative MSE, RMSE, RE, PSNR, and SSIM for different cryptosystems

Method	Images	Quality performance parameters		
		MSE	PSNR	SSIM
Ref.[29]	1st	1.1397e-26	307	1
	2nd	9.2059e-30	338	1
Ref.[14]	1st	3.6214e-23	261	1
	2nd	7.5783e-17	209	1
Our results	1st	1.57479e-25	296	1
	2nd	6.82889e-26	299	1

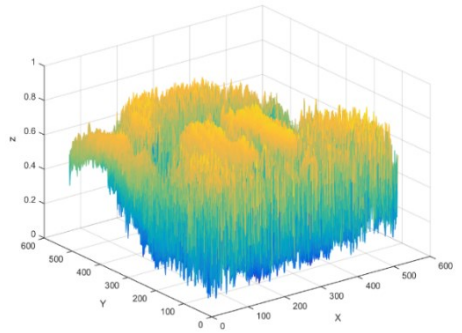
The calculated MSE values for the two test images were 1.57479e-25 and 6.82889e-26, respectively, indicating negligible difference between the original and recovered images. For structural fidelity assessment, the SSIM values computed between the decrypted images Figs. (4n) and (4o), and their corresponding originals Figs. (4a) and (4b) were both equal to 1, confirming perfect structural similarity. Likewise, the PSNR values for the same comparisons reached 296 and 299, further validating the exceptional visual and statistical agreement between the plaintext and decrypted outputs.

4.2 Statistical analysis

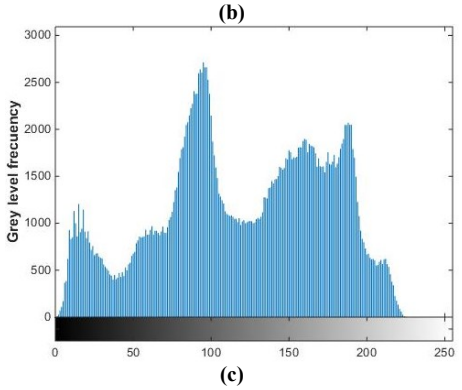
The effectiveness of the provided scheme was assessed using statistical analysis methods such as histogram evaluation, entropy measurement, and correlation analysis for input and encrypted images. Histogram plots illustrate the frequency distribution of intensity levels, where an 8-bit grayscale image has intensity values ranging from 0 to 255. Additionally, the mesh plot proposes a 3D representation of the image, displaying intensity values along with their corresponding positions. Figures (5a-d) present the histogram and mesh plots of the original images, while figures (5e) and (5f) display the corresponding plots for the encrypted image. It is worth note, a significant difference is observed in the intensity distribution between the original and encrypted images. Thus, these characteristics prevent an attacker from extracting any meaningful information.



(a)



(b)



(c)

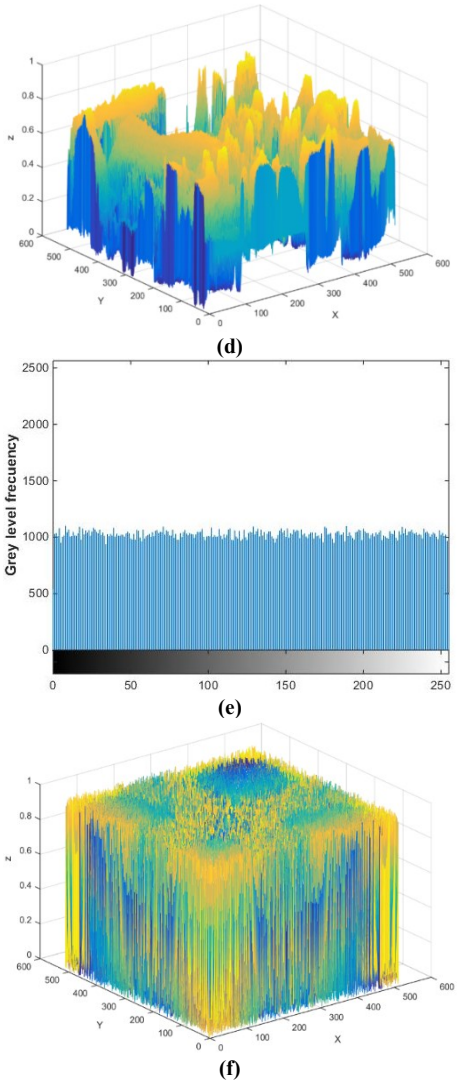


Fig. (5) Histogram and mesh plots of the (a, b) first input image (f_1), (c, d) second input image (f_2), (e, f) encrypted image

The standard information entropy for a uniformly distributed random variable is typically 8 bits. This value is determined mathematically using Shannon entropy

$$H = -\sum_{k=0}^{255} p_k \log_2 p_k \qquad (15)$$

where, H represent entropy, and p_k indicates the probability of pixel (k). The entropy of the original encrypted image is 7.4582, this indicates a high degree of randomness in the encrypted data. Table (2) shows the comparative results of entropy for the proposed scheme with other cryptosystem methods.

Table (2) Comparative results of entropy for the proposed scheme with other cryptosystem methods

Method	Information Entropy		
	1st Image	2nd Image	Encrypted Image
Ref.[29]	7.2925	7.5925	7.0615
Ref.[14]	7.2925	7.5925	7.9978
Our results	7.2925	7.5925	7.4582

4.3 Correlation coefficient analysis

The correlation coefficient (CC) is determined by randomly selecting 15,000 adjacent pixel pairs (horizontal, vertical, or diagonal) from both the original and encrypted images. The CC is then calculated using the following equations [10]

$$\bar{x} = \frac{1}{N}\sum_{k=1}^{N} x_k$$

and

$$\bar{y} = \frac{1}{N}\sum_{k=1}^{N} y_k \qquad (16)$$

$$\sigma(x) = \left[\frac{1}{N}\sum_{k=1}^{N}\{x_k - \bar{x}\}\right]^{\frac{1}{2}}$$

and

$$\sigma(y) = \left[\frac{1}{N}\sum_{k=1}^{N}\{y_k - \bar{y}\}\right]^{\frac{1}{2}} \qquad (17)$$

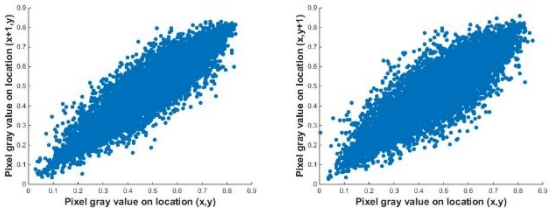
$$cov(x,y) = \frac{1}{N}\sum_{k=1}^{N}(x_k - \bar{x})\,(y_k - \bar{y}) \qquad (18)$$

$$CC = \frac{cov(x,y)}{\sigma(x)\sigma(y)} \qquad (19)$$

Here, $\sigma(x)$ and $\sigma(y)$ represents the standard deviations of x and y, respectively, where $\sigma(x)\neq 0$ and $\sigma(y)\neq 0$, the values x_k and y_k conform to the grayscale intensities of two neighboring pixels, N indicates the total number of pixels pairs (x_k, y_k), ($\bar{x}$ and $\bar{y}$) shows the mean values of x_k and y_k, respectively. Figure (6) shows that the neighboring pixels in the original image maintain a strong correlation in all three directions, whereas the corresponding directions in the encrypted image exhibit low correlation, highlighting the effectiveness of the encryption process. Table (3) shows the CC values between neighboring pairs of 15000 pixels in the primary and encrypted images. These values present that the nearby pixels of the original images have a high correlation in each direction, but the CC values for ciphered image are approximately zero.

Table (3) Comparative results of correlation coefficient for different methods

Methods	Correlation Coefficient			
	Metrices	Horizontal	Vertical	Diagonal
	Input image	0.9368	0.9133	0.8636
Ref.[29]	Encrypted Image	-0.0072	-0.0021	-0.0152
Ref.[14]	Encrypted Image	-0.0012	-0.0019	0.0014
Our results	Encrypted Image	-0.0504	-0.0486	0.0829



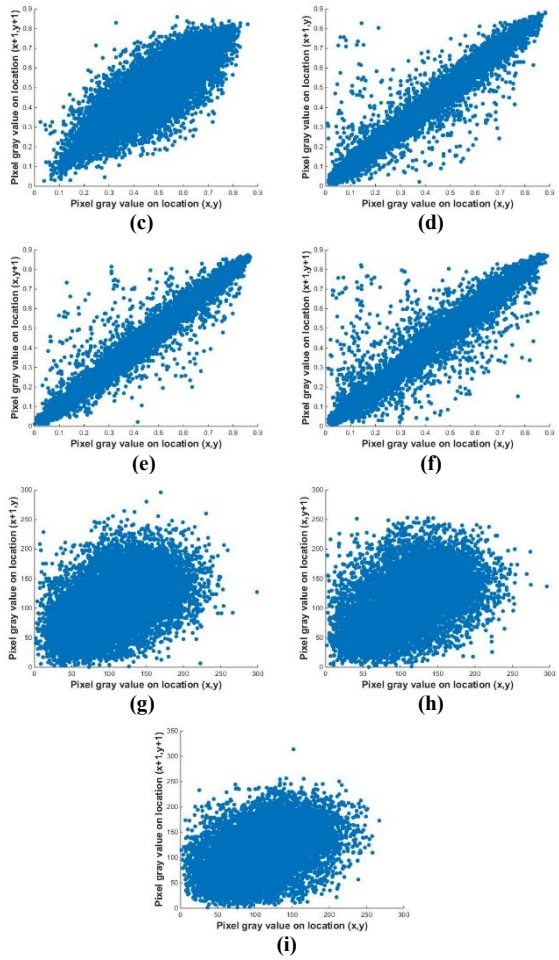


Fig. (6) Analysis of the correlation distribution in the horizontal, vertical and diagonal directions for (a-c) the first input image $f_1(x)$, (d-f) the second input image $f_2(x)$ and (g-i) the encrypted image

4.4 Key sensitivity analysis

To evaluate the key sensitivity of the proposed cryptosystem, the effect of removing one of the private keys or ciphertext is analysis by calculating the cross-correlation values. Table (4) presents the cross-correlation values corresponding to different cases of private key or ciphertext removal. Figures (7a-j) provide the decrypted images when any of PK_2, S, PK_3, PK_4, and E is removed. In addition, the effect of removing two of the private keys or ciphertext is analysis as in table (5) and Figs. (8a-t). As observed in Figs. (7) and (8), none of the decrypted images display any identifiable features or outlines of the original plaintexts. This confirms that the proposed method successfully prevents information leakage.

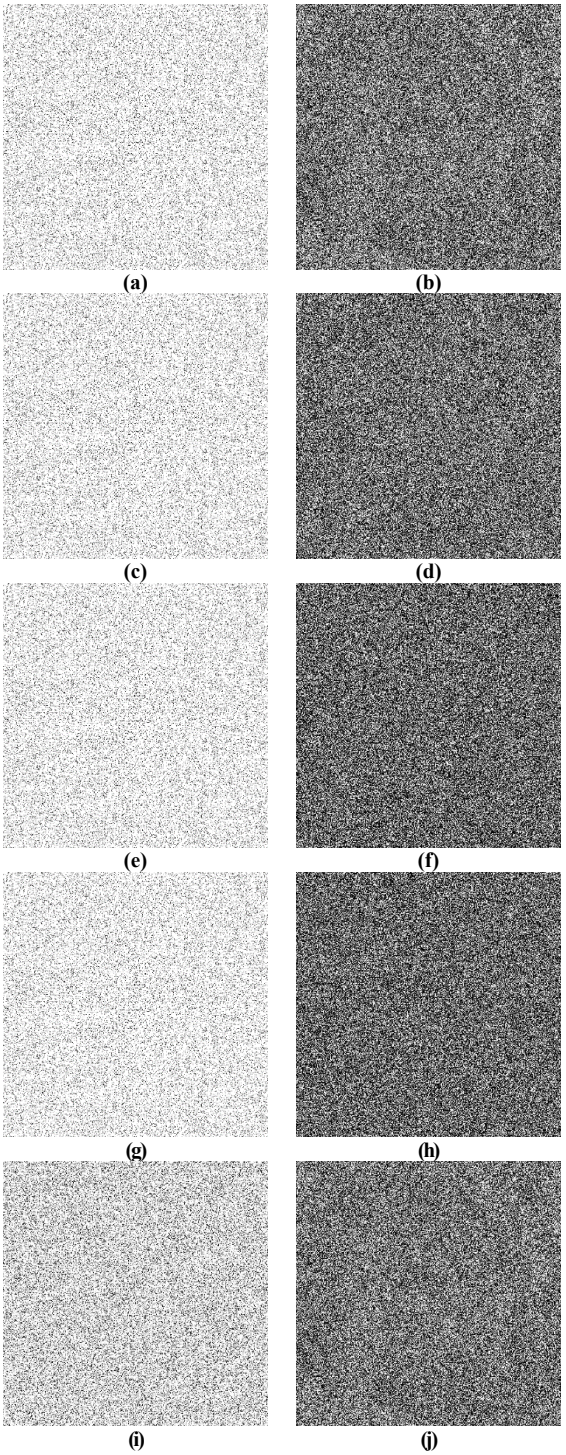


Fig. (7) Resistance to keys and ciphertext removal: retrieved images f_1 and f_2 when; (a) and (b) removed PK_2, (c) and (d) removed S, (e) and (f) removed PK_3, (g) and (h) removed PK_4, (i) and (j) removed E ciphertext

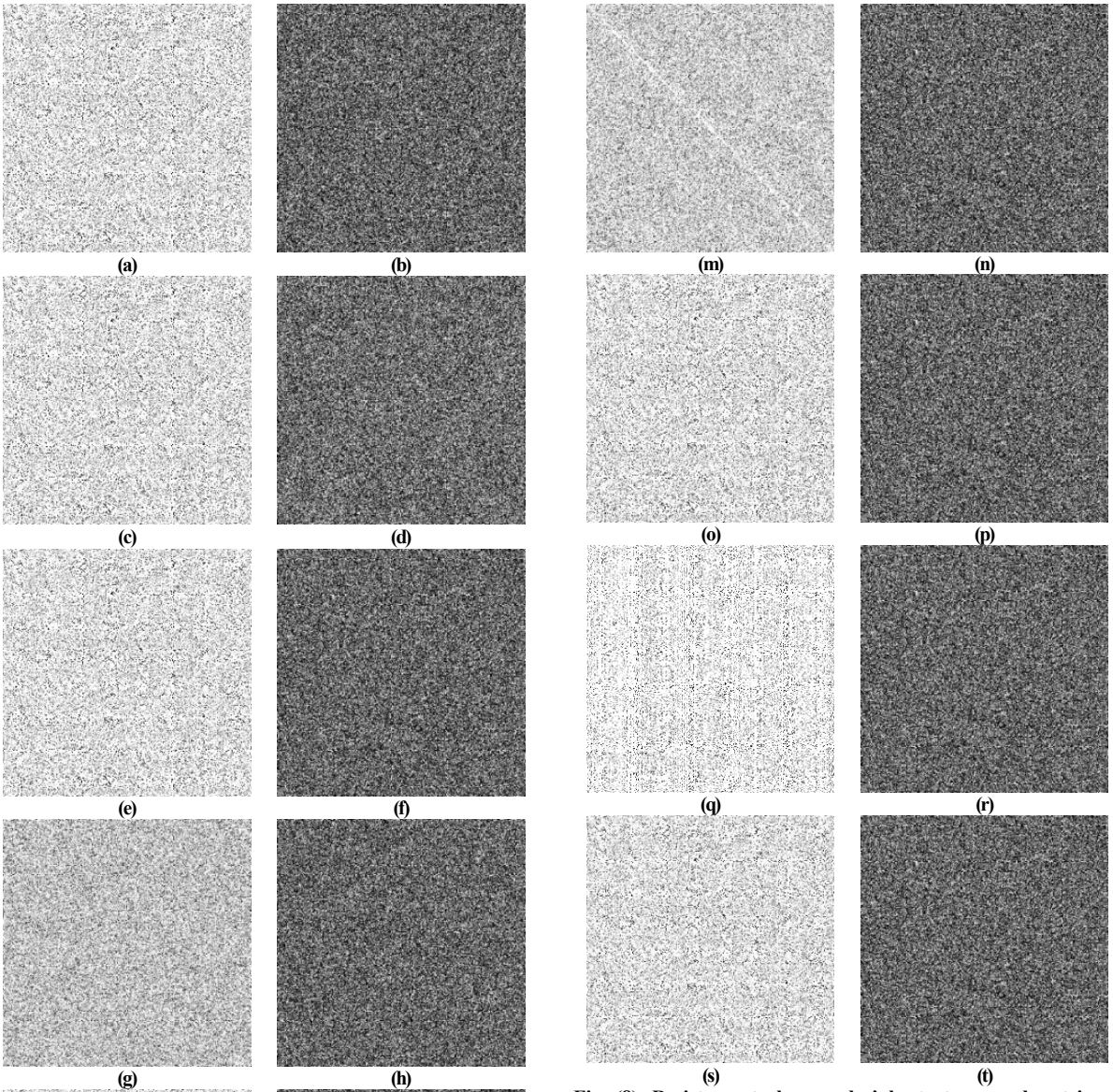


Fig. (8). Resistance to keys and ciphertext removal: retrieved images f_1 and f_2 when; (a) and (b) removed PK_2 and S, (c) and (d) removed PK_2 and PK_3, (e) and (f) removed PK_2 and PK_4, (g) and (h) removed PK_2 and E, (i) and (j) removed S and PK_3, (k) and (l) removed S and PK_4, (m) and (n) removed S and E, (o) and (p) removed PK_3 and PK_4, (q) and (r) removed PK_3 and E, (s) and (t) removed PK_4 and E

Table (4) A summary of the correlation coefficient outcomes corresponding to different cases of key removal

Removed Parameter	CC values	
	1st image	2nd image
PK_2	0.0004	0.00008
S	0.0021	-0.0021
PK_3	0.0004	0.0013
PK_4	0.0033	0.0014
E	0.0004	- 0.0005

Table (5) A summary of the correlation coefficient outcomes corresponding to different cases of removing two keys

Removed Parameter		CC values	
		1st image	2nd image
PK_2	S	0.0026	0.0009
PK_2	PK_3	0.0034	0.0018
PK_2	PK_4	0.0004	0.0004
PK_2	E	0.0004	-0.0002
S	PK_3	0.0003	0.0017
S	PK_4	0.0021	-0.0019
S	E	0.0004	-0.0002
PK_3	PK_4	0.0004	0.0007
PK_3	E	0.0004	-0.0042
PK_4	E	0.0033	0.0014

The sensitivity of the proposed method was also assessed for additional keys, including the illuminating wavelength λ and the diffraction distances Z_1 and Z_2. The accurate wavelength was set to 632 nm, while the correct axial distance for Z_1 and Z_2 were 50 mm and 90 mm, respectively. Figures (9) and (10) present the sensitivity analysis of these keys, demonstrating that even slight inaccuracies in any of them hinder the retrieval of the original images. Consequently, the proposed method incorporates three highly sensitive additional keys, significantly strengthening its overall security.

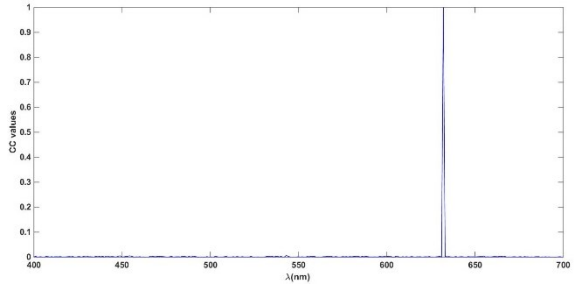


Fig. (9). Relationship between correlation coefficients and wavelength when lambda λ = 632 nm, ($\Delta\lambda = 1\ nm$)

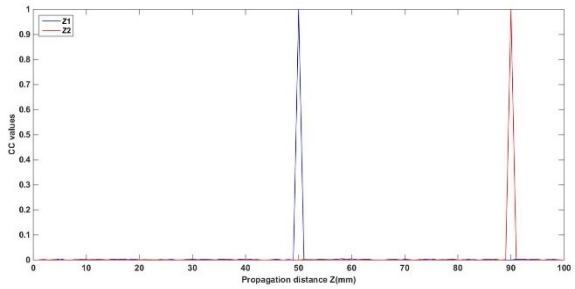


Fig. (10). Relationship between correlation coefficients and propagation distance when propagation distance Z_1 = 50 mm and Z_2 = 90 mm, ($\Delta Z = 1mm$)

4.5 Robustness against contamination attacks

This section evaluates the resilience of the proposed method against contamination attacks. To assess its robustness to cropping, the encrypted image was partially occluded at varying levels 6%, 12%, 25%%, 50%, and 70% of the total pixels. Figures (11a-e) present the progressively occluded cyphertext, while figures (11f-j) display the corresponding reconstructions of the first plaintext image f_1. Similarly, figures (11k-o) illustrate the recovered outputs of the second plaintext image f_2 under identical occlusion conditions.

The results demonstrate that for occlusion below 50%, the first recovered image preserved clear and meaningful visual information, with minimal structural degradation. Remarkably, the second image remained partially recognizable even under 70% ciphertext loss, although the overall quality was reduced due to significant data removal. Despite the evident loss of resolution, the essential structural content of both plaintexts could still be visually identified. In addition, figure (12) illustrates the effect of cropping on the reconstructed image. A detailed analysis of these results shows that the correlation coefficient experiences only slight degradation for both recovered images as the occlusion percentage increase.

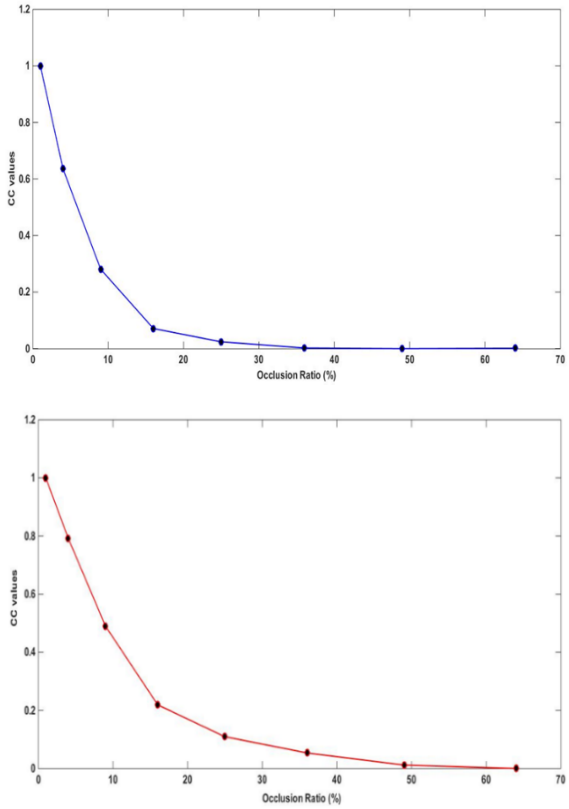


Fig. (12) Analysis results of occlusion attack for: (a) first decoded image f_1 , (b) second decoded image f_2

Also, to evaluate the robustness of the proposed method, its performance was tested against Gaussian noise attacks, with a mean of zero and a standard deviation of one. The Gaussian noise was introduced into the encrypted image to assess the system ability to recover the original data, using the following relation:

$$E' = E(1 + KG) \qquad (20)$$

where *E'* represents the encrypted image with noise, *E* is the encrypted image, *K* is the strength of the Gaussian noise, and *G* is the Gaussian white noise. Figure (13) shows the decrypted images affected by Gaussian noise when the strengths were 0.1, 0.3, 0.5 and 0.7. Figure (14) depicts the impact of noise strength on the reconstructed images. Analyzing these results reveals minimal degradation in the CC for both the first recovered image f_1 and the second recovered image f_2 as the noise intensity increases. This outcome highlights the effectiveness and robustness of the proposed system against noise attacks.

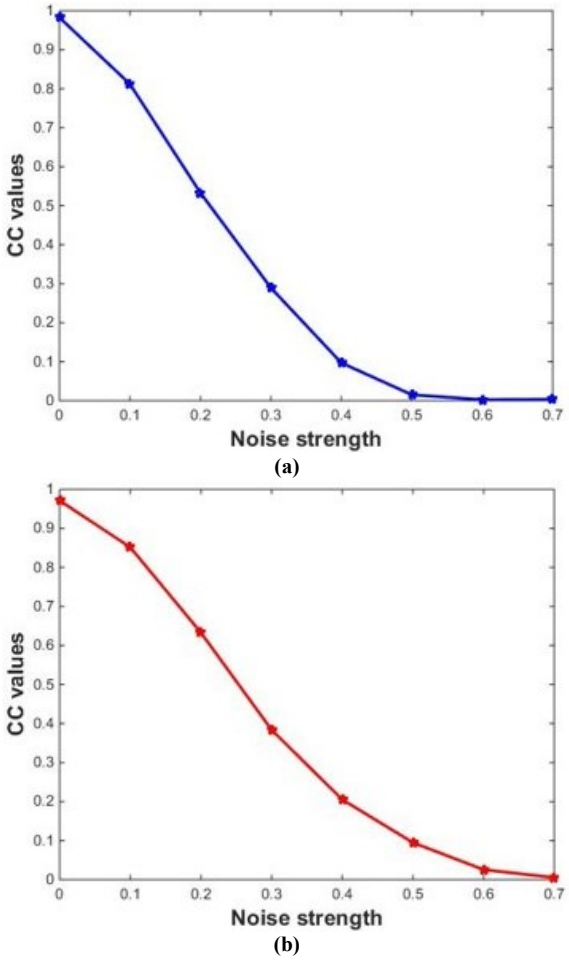


Fig. (14) Analysis results of noise attack for: (a) first decrypted image f_1, (b) second decrypted image f_2

4.6 Known Plaintext Attack (KPA)

In this subsection, the proposed method was tested against a known-plaintext attack (KPA). Under such an attack, it was assumed that attackers possess prior knowledge of both the original and encrypted images, along with details of the encryption method. Attackers then attempt to uncover the encryption keys used in the process. Figures (15a) and (15f) display the input images to be ciphered and the corresponding encrypted images. By applying the correct private keys and parameters, the decrypted images were obtained, as shown in Figs. (15g-i). These results confirm that no recognizable details from the original images could be recovered, indicating the robustness of the proposed method against known plaintext attacks.

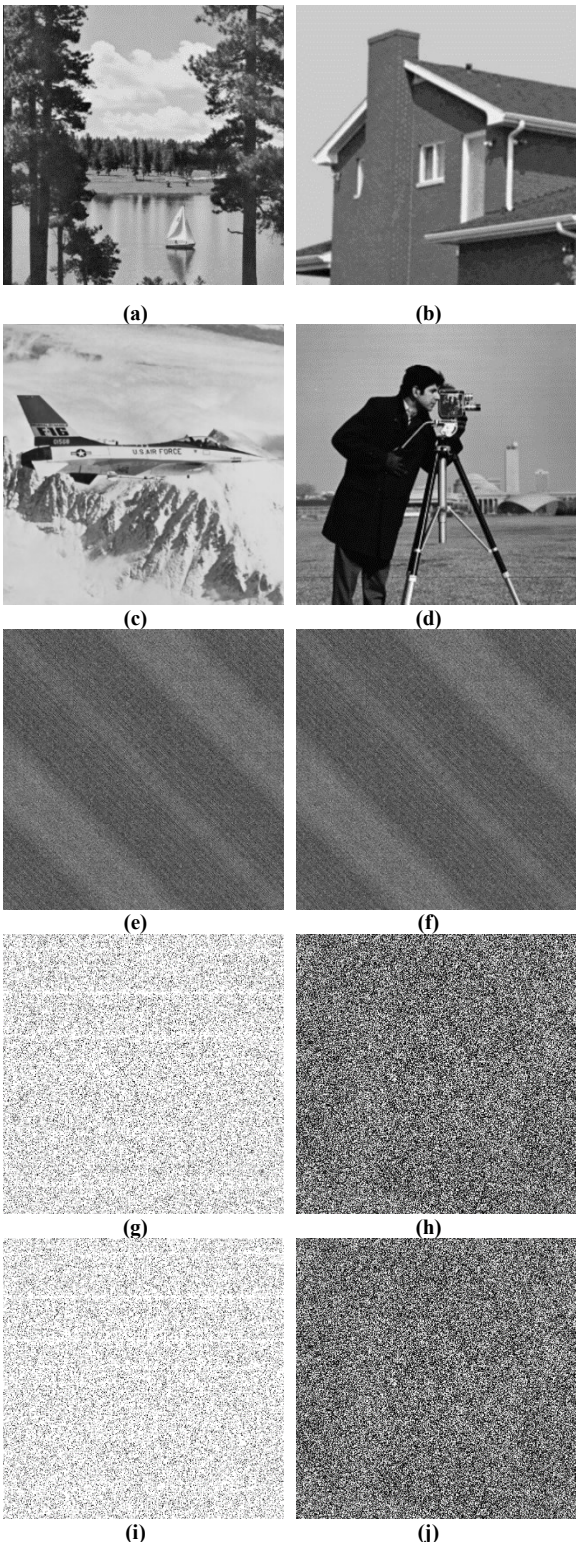


Fig. (15) Known plaintext attack: (a-d) two pairs of plaintexts used as original images; (e) and (f) matching encrypted images, (g-j) retrieved images

5. Conclusion

A double-image cryptosystem based on phase-truncated Fresnel domain with random modulus decomposition and polar decomposition is presented. In this scheme utilized three public keys to generate four private keys. The results demonstrate that the proposed approach effectively enhanced the security of provided cryptosystem compared with classical phase-truncated cryptosystems. Through extensive simulation and statistical evaluations, the robustness of the method was confirmed, particularly in its ability to withstand information leakage and presents strong resistance to specific attacks. Additionally, the wavelength of the light and the two diffraction distances act as extra keys to further enhance security. Moreover, the proposed method enhanced the systems flexibility against unauthorized access. The method has also proven effective in dealing with various forms of noise and blockages, making it a reliable choice for secure optical cryptosystems. Our proposed scheme has been compared with other cryptosystems, and the results are presented in table (6).

References

[1] Sachin et al., "Advances in Optical Visual Information Security: A Comprehensive Review", *Photonics*, 11(1) (2024) 1.
[2] S. Liu, C. Guo and J. T. Sheridan, "A review of optical image encryption techniques", *Opt. Laser Technol.*, 57 (2014) 327-342.
[3] M. Kaur, S. Singh and M. Kaur, "Computational Image Encryption Techniques: A Comprehensive Review", *Math. Probl. Eng.*, 2021 (2021) 1-17.
[4] O. Matoba et al., "Optical Techniques for Information Security", *Proc. IEEE*, 97(6) (2009) 1128-1148.
[5] W. Chen, B. Javidi and X. Chen, "Advances in optical security systems", *Adv. Opt. Photon.*, 6(2) (2014) 120.
[6] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding", *Opt. Lett.*, 20(7) (1995) 767.
[7] R. A. Jassim and E. A. Mohammed, "Asymmetric Optical Cryptosystem in the Fractional Fourier Domain Using Photon Counting Imaging", *Basrah J. Sci.*, 40(2) (2022) 2.
[8] G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain", *Opt. Lett.*, 29(14) (2004) 1584.
[9] H. Singh et al., "Fully phase image encryption using double random-structured phase masks in gyrator domain", *Appl. Opt.*, 53(28) (2014) 6472.
[10] I.M. Qasim and E.A. Mohammed, "Secure optical image encryption and authentication based on phase information and Collins diffraction transform", *J. Theor. Appl. Phys.*, 19(1) (2025) 1-10.
[11] U. Gopinathan et al., "A known-plaintext heuristic attack on the Fourier plane encryption algorithm", *Opt. Exp.*, 14(8) (2006) 3181-3186.
[12] X. Peng, H. Wei and P. Zhang, "Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain", *Opt. Lett.*, 31(22) (2006) 3261.
[13] A. Carnicer et al., "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys", *Opt. Lett.*, 30(13) (2005) 1644-1646.
[14] H.A. Khalf and E.A. Mohammed, "Optical double-image cryptosystem based on interference principle and spatial encoding", *Optik*, 329 (2025) 172344.
[15] 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(22) (2024) 5941.
[16] E.A. Mohammed and H.L. Saadon, "Sparse phase information for secure optical double-image encryption and authentication", *Opt. Laser Technol.*, 118 (2019) 13-19.
[17] E.A. Mohammed and H.L. Saadon, "Simultaneous verification of optical triple-image encryption using sparse strategy", *J. Phys. Conf. Ser.*, 1234(1) (2019) 012037.
[18] E. Pérez-Cabré et al., "Photon-counting multifactor optical encryption and authentication", *J. Opt.*, 17(2) (2015) 025706.
[19] E. Ahouzi et al., "Optical triple random-phase encryption", *Opt. Eng.*, 56(11) (2017) 1.
[20] H. Hai et al., "Cryptanalysis of random-phase-encoding-based optical cryptosystem via deep learning", *Opt. Exp.*, 27(15) (2019) 21204-21213.
[21] E. Kumari et al., "Analysis of triple random phase encoding cryptosystem in Fresnel domain", *Result Opt.*, 1 (2020) 100009.
[22] M. Khurana and H. Singh, "Asymmetric Optical Image Triple Masking Encryption Based on Gyrator and Fresnel Transforms to Remove Silhouette Problem", *3D Res.*, 9(3) (2018) 38.
[23] W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms", *Opt. Lett.*, 35(2) (2010) 118.
[24] S.K. Rajput and N.K. Nishchal, "Known-plaintext attack-based optical cryptosystem using phase-truncated Fresnel transform", *Appl. Opt.*, 52(4) (2013) 871-878.
[25] X. Wang and D. Zhao, "A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms", *Opt. Commun.*, 285(6) (2012) 1078-1081.
[26] I. Mehra and N.K. Nishchal, "Asymmetric cryptosystem for securing multiple images using two beam interference phenomenon", *Opt. Laser Technol.*, 60 (2014) 1-7.

[27] S. Yadav and H. Singh, "Asymmetric cryptosystem based on fractional Fourier transform domain using triple random phase masks", in **Communication and Computing Systems**, CRC Press (2019), pp. 105-111.
[28] W. Chen and X. Chen, "Optical color image encryption based on an asymmetric cryptosystem in the Fresnel domain", *Opt. Commun.*, 284(16) (2011) 3913-3917.
[29] Y. Xiong, J. Gu, and R. Kumar, "Collision in double-image encryption scheme based on spatial encoding and phase-truncation Fourier transforms", *Appl. Opt.*, 62(31) (2023) 8416-8425.
[30] G. Luan and C. Quan, "Optical double-image cryptosystem based on phase truncation in the Fresnel domain", *Appl. Phys. B*, 129(8) (2023) 130.
[31] K.S. Gaur et al., "An asymmetric hybrid cryptosystem based on triple random phase encoding using polar decomposition, QZ modulation, and gyrator domain", *Optik*, 299 (2024) 171602.
[32] M.R. Abuturab, "Color information verification system based on singular value decomposition in gyrator transform domains", *Opt. Lasers Eng.*, 57 (2014) 13-19.
[33] X. Deng, "Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition: Comment", *Opt. Lett.*, 40(16) (2015) 3913.
[34] M. Rafiq Abuturab, "Asymmetric multiple information cryptosystem based on chaotic spiral phase mask and random spectrum decomposition", *Opt. Laser Technol.*, 98 (2018) 298-308.
[35] S. Singh and A.B. Joshi, "Novel asymmetric cryptosystem to secure the digital images using QZS and random modulus decomposition", *Opt. Quantum Electron.*, 56(5) (2024) 867.
[36] N.J. Higham, "Computing the Polar Decomposition—with Applications", *SIAM J. Sci. Stat. Comput.*, 7(4) (1986) 1160-1174.
[37] U. Qidwai and C.H. Chen, **"Digital Image Processing: An Algorithmic Approach with MATLAB"**, Chapman and Hall/CRC (NY, 2009), doi: 10.1201/9781420079517.
[38] R. Perez, J.M. Vilardy and C.J. Jimenez, "Nonlinear image encryption system using the Gyrator transform and truncation operations," *J. Phys. Conf. Ser.*, 792(1) (2017) 012046.
[39] Z. Wang et al., "Image Quality Assessment: From Error Visibility to Structural Similarity", *IEEE Trans. Image Process.*, 13(4) (2004) 600-612.
[40] H. Xu et al., "Phase-only asymmetric optical cryptosystem based on random modulus decomposition", *J. Mod. Opt.*, 65(10) (2018) 1245-1252.

Table (6) Comparison analysis of proposed cryptosystem with other cryptosystems

Indicators	Luan et al. [30]	Wang et al. [40]	Proposed method
Transform domain	Fresnel domain	Fresnel domain	Fresnel domain
Types of images	Grayscale	Grayscale	Grayscale
Number of images	One Image	One image	Double image
Encryption keys	Three RPM, the illuminating wavelength, two diffraction distances d_1 and d_2, and three parameters of Chaotic pixel scrambling (CPS)	Random modulus decomposition, the illuminating wavelength, two diffraction distances d_1 and d_2, and phase encoding	Random amplitude mask, Random modulus decomposition, Polar decomposition, the illuminating wavelength, two diffraction distances Z_1 and Z_2
Decomposition in method	(RMD)	2 RMD	RMD, and PD
Applied strategy	Asymmetric	Asymmetric	Asymmetric
Advantages	Improved resistance to silhouette problem, and robust against the specific attack	Improved the capacity to resist various attacks, including the attack of iterative algorithms	Enhanced resistance to silhouette problem, robust against various attacks

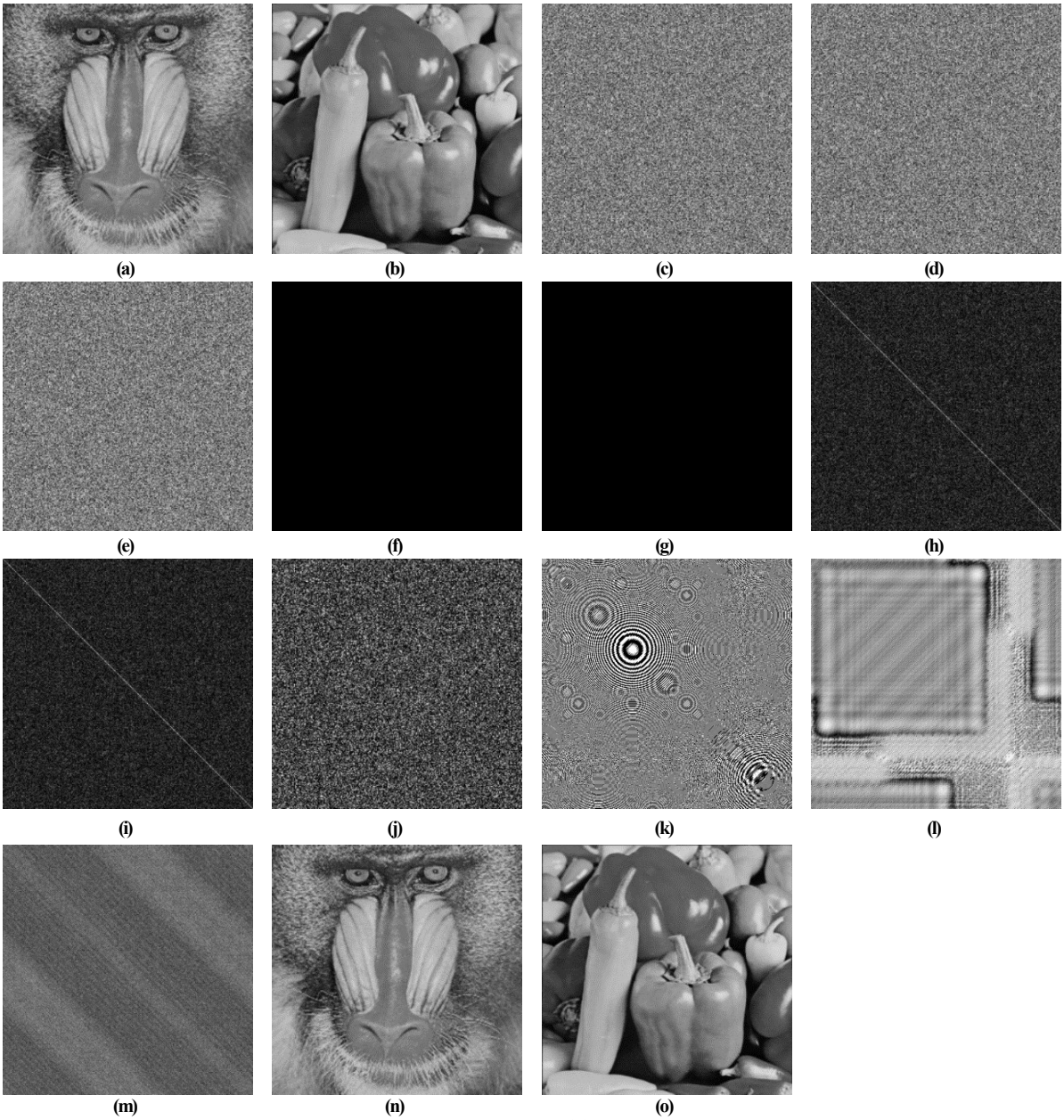


Fig. (4) (a) and (b) input images, (c) $M(x)$, (d) and (e) two public keys $\alpha(x)$ and $\beta(x)$, (f) distribution function $PK_1(x)$, (g) the private key $PK_2(x)$, (h) and, (i) two matrices U and V, respectively, (j) the private key matrix S, (k) and (l) the private keys $PK_3(u_1)$ and $PK_4(u_2)$, respectively, (m) the encrypted image, (n) and (o) the decrypted images with the corrected keys

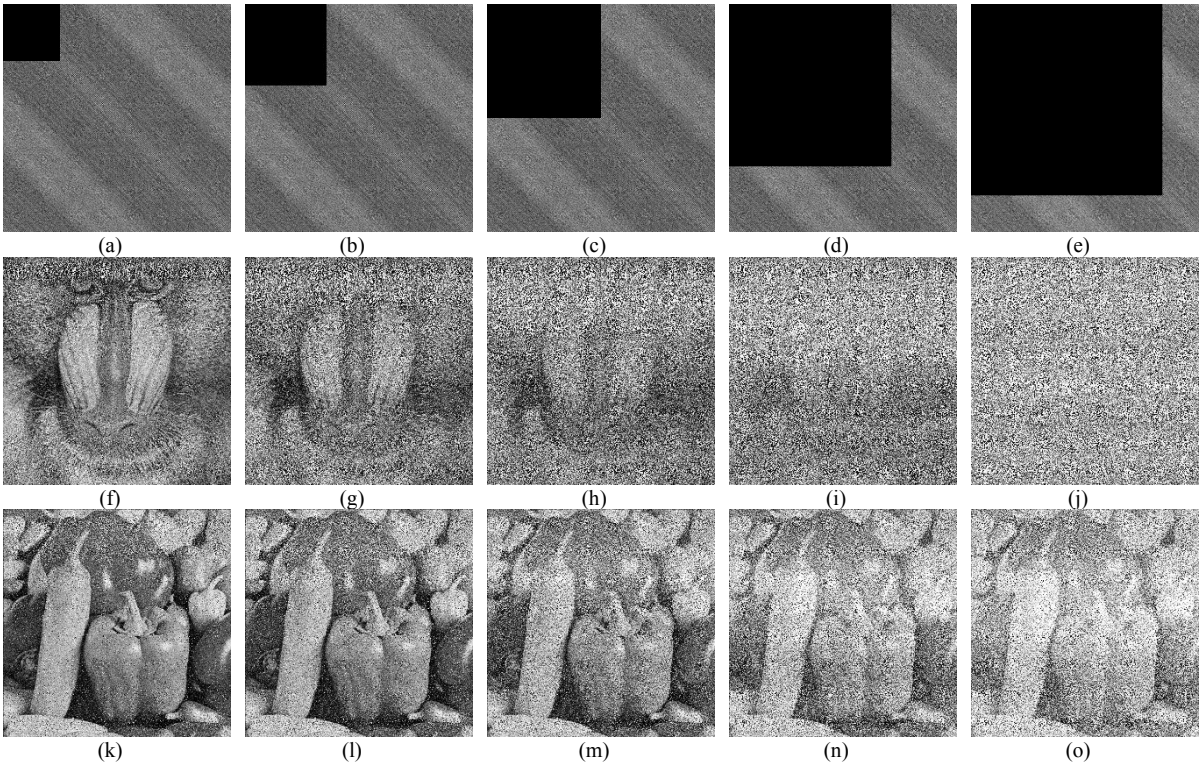


Fig. (11) Occlusion results for the encrypted image with varying degree of occlusion: (a-e) encrypted image with 6%, 12%, 25%, 50% and 70% occluded area; (f-j) decoded image f_1; (k-o) decoded image f_2

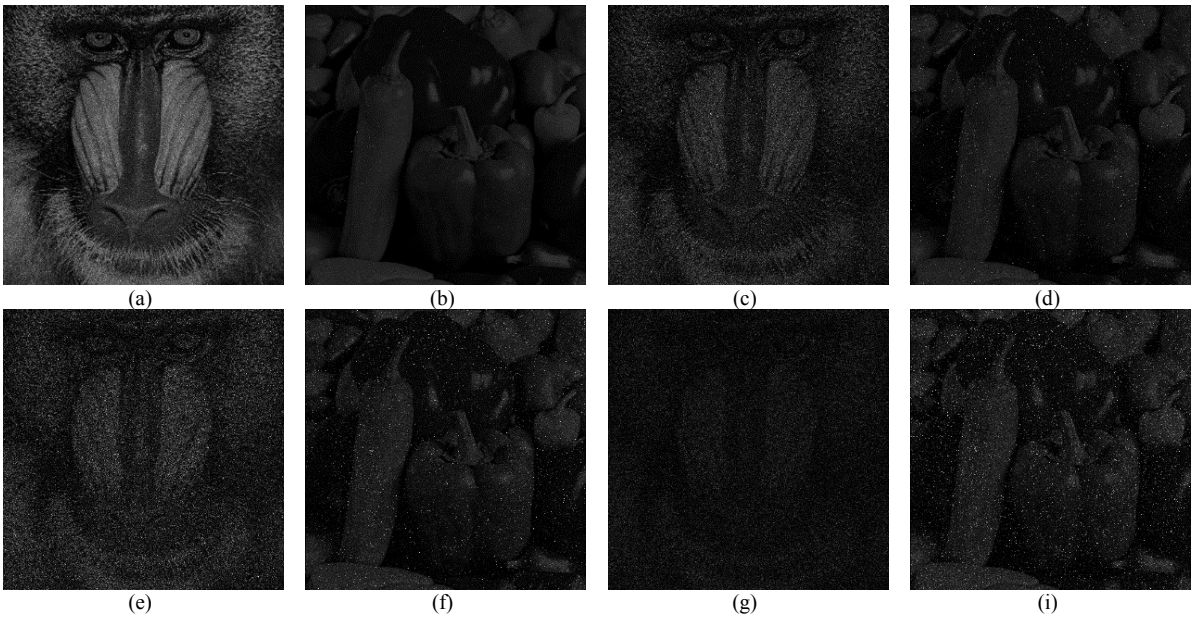


Fig. (13) Decrypted results in the presence of Gaussian noise with strength noise (K): (a, b) 0.1; (c, d) 0.3; (e, f) 0.5; (g, h) 0.7

