Int. J. Adv. Res. Sci. Technol. Volume 15, Issue 6, 2026, pp.2142-2152.

IJARST

International Journal of Advanced Research in Science and Technology

https://doi.org/10.62226/ijarst20262724

ISSN 2319 – 1783 (Print)

ISSN 2320 – 1126 (Online)

A Secure Multi – Image Optical Encryption Scheme Based on Quasi – Zernike Synthesis, Cascaded Equal Modulus Decomposition, and the Gyrator Transform

Ajay Singh[1], and Nagander Singh Tomer[2*]

[1]Department of Applied Sciences and Humanities, SoET, Central University of Haryana, Mahendergarh, India, 123031

[2]Department of Mathematics, Guru Gorakhnath Ji Government College, Hisar, Haryana, India, 125001

Email Id: *tomar.smart@gmail.com*

ARTICLEINFO

Article history:

Received	21 June 2026
Accepted	29 June 2026
Available online	30 June 2026

Keywords:

Multi – image encryption, Gyrator transform, Quasinormal – Zernike algorithm, Equal Modulus Decomposition.

Indexed in:

and in major libraries

ABSTRACT

The widespread transmission and storage of digital images over open communication networks have made secure image encryption an essential research topic. Although numerous optical encryption techniques have been reported, many existing methods are constrained by limited key diversity, insufficient resistance to cryptanalytic attacks, and reduced robustness under adverse transmission conditions. This paper proposes a multi – image encryption framework by integrating Quasi – Zernike (QZ) synthesis, the gyrator transform (GT), random phase mask (RPMs), and equal modulus decomposition (EMD). Initially, two plaintext images are fused using QZ synthesis to generate multiple private keys. The synthesized output is then combined with a phase image and encrypted through dual GT operations interleaved with RPM modulation and EMD, producing additional secret keys and a highly randomized ciphertext. The original images are recovered by performing the inverse operations using the corresponding private keys. The effectiveness of the proposed framework is validated through CC, MSE, PSNR, SSIM, information entropy, histogram, pixel correlation, and key sensitivity analyses, together with brute – force, noise and occlusion attack evaluations. Experimental results demonstrate near – lossless image reconstruction, high ciphertext randomness, and strong robustness against statistical and differential attacks. The proposed framework offers a secure and efficient solution for optical multi – image encryption and protected image communication.

1. Introduction

The rapid advancement of multimedia technologies and communication networks has significantly increased the transmission and storage of digital images. Consequently, ensuring the confidentially and integrity of image data has become a critical requirement in applications such as medical imaging, military communications, remote sensing, cloud computing, and intelligence surveillance. Owing to their high pixel redundancy and strong spatial correlation, digital images cannot be efficiently protected using conventional text – oriented cryptographic algorithms, thereby necessitating the development of dedicated image encryption techniques.

In this context, Optical image encryption has been extensively investigated owing to its capability to provide high – level security through transform – domain processing. Among the existing approaches, Double Random Phase Encoding (DRPE) [1] introduced by Refregier and Javidi in 1995, is one of the most influential techniques, as it converts plaintext images into complex noise – like distributions by employing random phase masks in both the spatial and transform domains. Despite its initial success, subsequent studies revealed that the linear architecture and symmetric encryption mechanism of DRPE expose it to several cryptanalytic attacks. To address these shortcomings, numerous enhanced variants have been developed by implementing DRPE in different transform domains, including the Fractional Fourier Transform (FrT) [2], Fresnel Transform [4], Gyrator Transform (GT) [5], [6], Hartley Transform [7], Fractional Hartley Transform [3], Hermite Transform [8], Fractional Hermite Transform [9], [10], Wavelet Transform [11] and Discrete Wavelet Transform [12]. Although transform – domain implementations increase the key space through additional parameters such as fractional orders and rotations angles, the inherent linearity and symmetric architecture of DRPE remain major security concern. Consequently, DRPE – based schemes are still vulnerable to known – plaintext attack (KPA) [13], chosen – plaintext attack (CPA) [14], chosen – ciphertext attack (CCA) [15] and ciphertext – only attack (COA) [16], motivating the development of non – linear and asymmetric optical encryption techniques.

To overcome the limitation of linear DRPE, Qin and Peng introduced the Phase – Truncated Fourier Transform (PTFT) [17] in 2010 as the first non – linear asymmetric optical encryption scheme. By truncating the phase information, PTFT breaks the linearity of DRPE and employs distinct keys for encryption and decryption, with the retained phase serving as the private decryption key. Although PTFT represented a significant milestone in asymmetric optical encryption, subsequent studies demonstrated its susceptibility to iterative and optimized – based attacks, indicating that non – linearity alone is insufficient to ensure robust cryptographic security.

To further enhance the security of optical image encryption, researchers have incorporated additional mathematical operations beyond conventional transform – domain processing. Among these, decomposition techniques, including Equal Modulus Decomposition (EMD) [18], Unequal Modulus Decomposition (UMD) [19], [20], Random Modulus Decomposition (RMD) [21], [22], Singular Value Decomposition (SVD) [23], [24], Hessenberg Decomposition [25] and QR decomposition [26], [27], have been extensively employed to increase key diversity and cryptographic strength. Likewise, matrix synthesis and factorization methods, such as QZ synthesis [28], and Schur decomposition [29], have attracted growing attention due to their capability to generate multiple secret keys and improve reconstruction security. Furthermore, the integration of these techniques with nonlinear chaotic systems, including the Tinkerbell map [30], Umbrella map [31], [32], Henon map [33], Bird wing map [34] and Arnold map [35], substantially enlarges the key space and enhances resistance against statistical, differential and brute – force attacks.

Building upon this concept, Cai et al. [36] proposed an asymmetric optical encryption scheme based on coherent superposition and Equal Modulus Decomposition (EMD) [37]. In their approach, a random phase mask was applied to the input image to generate two equal modulus components, where one component was transmitted as the ciphertext and the other was retained as the private decryption key, thereby establishing an asymmetric encryption architecture. To further enhance cryptographic security, subsequent studies introduced Cascaded Equal Modulus Decomposition (CEMD), in which multiple EMD stages are performed sequentially to generate additional private keys and increase encryption complexity. The cascaded structure enlarges the effective key space and improves resistance against statistical, differential and brute – force attacks while preserving accurate image reconstruction.

The work presents a secure multi – image encryption framework based on QZ synthesis, the gyrator transform, random phase mask and cascaded equal modulus decomposition. Initially, two plaintext images are synthesized using the QZ algorithm, which simultaneously generates multiple private keys while preserving the information required for lossless reconstruction. The synthesized matrix is subsequently combined with a phase – only image and encrypted through two successive GT operations. At each stage, random phase modulation is employed to enhance the randomness of the complex – valued data, followed by cascaded EMD to generate additional private keys further strengthen the asymmetric encryption architecture. The final ciphertext is obtained after the second EMD stage, whereas the decryption process performs the exact inverse operations using the corresponding QZ keys, EMD keys, GT rotation angles and RPMs to recover the original images with high fidelity. The integration of QZ synthesis, dual GT processing, random modulation, and cascaded EMD significantly enlarges the effective key space, improve ciphertext randomness, and enhances robustness against statistical, brute – force, noise and occlusion attacks. Experimental results demonstrates that the proposed framework achieves near – lossless image reconstruction while providing a high level of security for optical multi – image encryption.

The remainder of this paper is structured as follows. Section 2 introduces the fundamental principles of Quasi – Zernike (QZ) synthesis, the Gyrator Transform (GT), and Equal Modulus Decomposition (EMD). Section 3 details the proposed encryption and decryption framework. Section 4 presents the experimental results together with comprehensive security and performance analyses. Finally, Section 5 provides the concluding remarks.

2. Basic Fundamental Principles

2.1 Quasinormal – Zernike algorithm

The Quasinormal – Zernike (QZ) algorithm [38], [39] is a nonlinear mathematical framework consisting of two primary operations: QZ synthesis and QZ decomposition. The QZ synthesis process takes two input images I_1 and I_2, and transforms them into a pair of upper triangular (or quasi – triangular) matrices, denoted by AA and BB. Simultaneously, two corresponding unitary matrices, Q and Z, are generated. These matrices collectively characterize the relationship between the input images and form the basis for the subsequent QZ decomposition process.

Depending on the nature of the input matrices, AA and BB are quasi – triangular for real valued I_1 and I_2, and upper triangular for complex – valued I_1 and I_2. The QZ synthesis is mathematically given by:

$$[AA, BB, Q, Z] = QZS(I_1, I_2) \tag{1}$$

By transposing BB and eliminating its diagonal elements (stored as private – key components), the lower triangular matrix $BB1$ is generated as:

$$BB1 = (BB)' - diag(BB) \tag{2}$$

The synthesized matrix H is constructed from the upper and lower triangular matrices AA and $BB1$, respectively. The QZ synthesis simultaneously generates three private keys: Q, Z and $diag(BB)$.

As the inverse of QZ synthesis, the QZ decomposition process reconstructs the upper triangular matrix AA form the synthesized matrix H through sub – diagonal element elimination. This process can be expressed as

$$AA = Tril(H) \tag{3}$$

Subsequently, the matrix BB can be recovered using the following operation:

$$BB = (H - AA)' + diag(BB) \tag{4}$$

By employing the unitary matrices Q and Z, the original images I_1 and I_2 can be successfully recovered.

$$I_1 = Q^{-1}(AA)Z^{-1} \quad (5)$$

$$I_2 = Q^{-1}(BB)Z^{-1} \quad (6)$$

2.2 Gyrator Transform (GT)

The gyrator transform (GT) [26], [40], [41] is a two – dimensional linear canonical transform that performs a rotational mapping in the spatial – frequency domain, providing strong decorrelation and a large key space determined by its rotational angle θ. Owing to these properties, GT has extensively employed in cryptography, optical image encryption and digital watermarking. The transform operates between the spatial co – ordinates (p, q) and the mixed domain (a, b). When $\theta = 0$, GT reduces to the identity transform, whereas $\theta = \pi/2$ yields the Fourier transform. By redistributing image information across the spatial – frequency domain, GT generates noise like outputs that significantly enhance the security of encrypted data. The GT of a two – dimensional function $f(r_1, s_1)$ is mathematically expressed as:

$$G_\theta\big(f(r_1, s_1)\big) = \iint f(r_1, s_1) Ker_\theta(r_1, s_1, r_2, s_2) dr_1 ds_1 \quad (7)$$

Where, Kernal $Ker_\theta(r_1, s_1, r_2, s_2)$ is defined as:

$$Ker_\theta(r_1, s_1, r_2, s_2) = \frac{1}{2\pi|sin\theta|} exp\left(\frac{2\pi i(r_2 s_2 + r_1 s_1)cos\theta - (r_1 s_2 + r_2 s_1)}{sin\theta}\right) \quad (8)$$

Here (r_1, s_1) and (r_2, s_2) are the input and output co – ordinates. The linear additive property of GT is expressed as:

$$G_\theta(G_\phi(f)) = G_{\theta+\phi}(f) \quad (9)$$

A key characteristic of the GT is its reversibility, which enables lossless recovery of the original image through the inverse gyrator transform (IGT), defined as:

$$f(r_1, s_1) = G_{-\theta}(G_\theta(f(r_1, s_1))) \quad (10)$$

The GT output is highly sensitive to slight variations in the rotation angle, leading to substantial variations in the resulting transformed data.

2.3 Equal Modulus Decomposition

Equal Modulus Decomposition (EMD) [42] is a decomposition technique that separates a complex – valued matrix into two components having identical modulus values and different phase distributions. The decomposition process generates a private key that is essential for exact reconstruction. Due to its reversibility and key – generation capability, EMD is widely used in optical image encryption to enhance security and increase key – space complexity. Mathematically it is defined as:

$$P_{11}(x, y) = \frac{A(x,y)/2}{\cos[\phi(x,y) - \alpha(x,y)]} \cdot e^{i.\alpha(x,y)} \quad (11)$$

$$P_{22}(x, y) = \frac{A(x,y)/2}{\cos[\phi(x,y) - \alpha(x,y)]} \cdot e^{i.[2\phi(x,y) - \alpha(x,y)]} \quad (12)$$

Here, $A(x, y)$ and $\phi(x, y)$ denote the amplitude and phase distribution of the original matrix $P(x, y)$, respectively. The decomposed component $P_{11}(x, y)$ and $P_{22}(x, y)$ represents the secret key and encrypted image, while $\alpha(x, y)$ is treated as a public key for the reconstruction process. **3. Proposed optical Encryption and Decryption Scheme**

This section provides a detailed description of the proposed encryption and decryption processes.

3.1 Encryption Procedure

Step 1. Initially, two input images, I_1 and I_2, are combined using QZ synthesis, producing a synthesized matrix and three private keys Q, Z and $diag(BB)$, mathematically we have:

$$[AA, BB, Q, Z] = QZS(I_1, I_2) \quad (13)$$

Step 2. The synthesized matrix is obtained by combining AA and $(BB)'$ with the subtraction of diagonal component of BB. Mathematically, it is expressed as:

$$M_0 = AA + (BB)' - diag(BB) \quad (14)$$

Reserve phase part of M_0 as private key named as M_1.

Step 3. The synthesized output is then merged with a phase image I_3. And output is stored as E_1 mathematically defined as:

$$E_1 = abs(M_0 \times I_3) \quad (15)$$

Step 4. Next, a gyrator transform with rotation angle θ_1 is applied, followed by modulation with the first random phase mask $(RPM1)$ and stored as E_2, defined as:

$$E_2 = GT(E_1, \theta_1) \times RPM1 \quad (16)$$

Step 5. The resulting data are decomposed using EMD, generating a private key P_{11}, And proceed P_{22} for further encryption process mathematically defined as:

$$[P_{11}, P_{22}] = EMD_{\theta_1, \phi_1}(E_2) \quad (17)$$

Step 6. Subsequently, the decomposed output undergoes a second gyrator transform with rotation angle θ_2 and is further modulated by a second random phase mask $(RPM2)$, and output is stored as E_3 mathematically defined as:

$$E_3 = GT(P_{22}, \theta_2) \times RPM2 \quad (18)$$

Step 7. A second EMD operation is then performed to obtain another private key P_{44}, and the final encrypted image. Mathematically:

$$[P_{33}, P_{44}] = EMD_{\theta_2, \phi_2}(E_3) \quad (19)$$

Therefore, the encryption process generates six private keys as $(Q, Z, diag(BB), angle(M_0), P_{11}\ and P_{44})$ along with the gyrator rotation angles and random phase masks, which are required for successful decryption. As shown in figure 1.

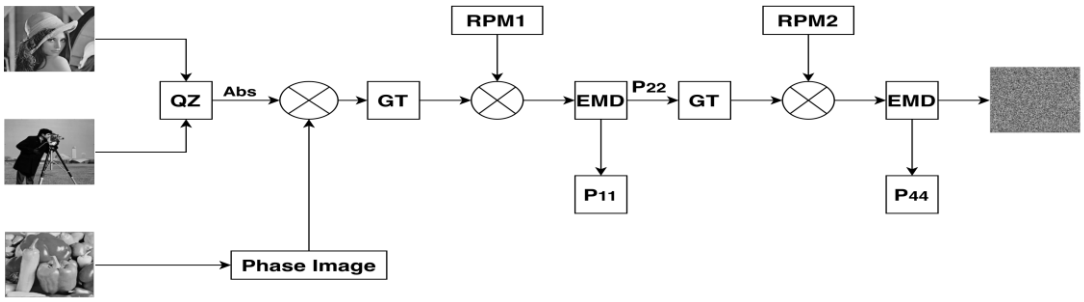

Fig 1. Schematic diagram of the proposed encryption framework.

3.2 Decryption Procedure

Decryption is performed by reversing the encryption steps using the corresponding private keys, enabling successful recovery of the original images.

Step 1. The procedure starts with the private key generated from the second EMD stage is combined with the encrypted image to reconstruct the corresponding decomposed data. The recovered output is then multiplied by the complex conjugate of $RPM2$. The resulting matrix is denoted as D_1, mathematically:

$$D_1 = (P_{33} + P_{44}) \times conj(RPM2) \quad (20)$$

Step 2. Thereafter, the inverse gyrator transform is performed on D_1. By applying the corresponding EMD private key to the recovered data, the intermediate matrix D_2 is obtained. Mathematically,

$$D_2 = IGT(D_1) + P_{11} \quad (21)$$

Step 3. Subsequently, the output is multiplied by conjugate of $RPM1$, yielding the intermediate matrix D_3, which is defined as

$$D_3 = D_2 \times conj(RPM1) \quad (22)$$

Step 4. Finally, an inverse gyrator transform is applied to D_3, and the output is denoted as D_4. The phase image is then retrieved by extracting the phase component of D_4, expressed as

$$D_4 = IGT(D_3) \quad (23)$$

Step 5. The absolute component of D_4 is modulated with the QZS private key M_1, yielding the final matrix D_5 given by

$$D_5 = abs(D_4) \times M_1 \quad (24)$$

Step 6. Finally, QZ decomposition is applied to D_5 to recover the input images.

$$[I_1, I_2] = QZD(D_5) \quad (25)$$

As shown in figure 2.

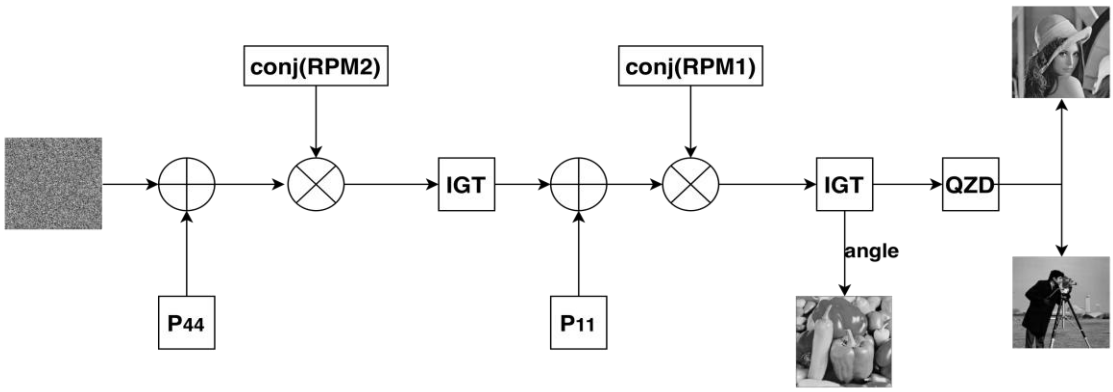

Fig 2. Schematic diagram of the proposed decryption framework.

4. Simulation Results and Discussion

This section presents the simulation results obtained to validate the effectiveness and security of the proposed image encryption scheme. All experiments were conducted in MATLAB R2025b on a computer equipped with Intel Core i7 processor. Three grayscale images with a resolution of 256×256 pixels were employed as test images. Figure 3, illustrates the original input images, the encrypted image, and the corresponding decrypted images produced by the proposed framework. The encrypted image exhibits noise – like characteristics and reveals no visual information about the original images. In contrast, the decrypted images closely resemble the original images, confirming the accuracy of the proposed decryption process.

The quantitatively evaluate the performance of the proposed scheme, several statistical and security metrices are employed, including the correlation coefficient (CC), mean squared error (MSE), and peak signal – to – noise ratio (PSNR). The statistical randomness of the encrypted image is assessed using information entropy analysis. In addition, the robustness of the proposed encryption scheme is investigated under occlusion and noise attacks to evaluate its ability to withstand data loss and transmission distortions. The effectiveness of the scheme in preserving recoverable image information under these adverse conditions demonstrates its reliability and resilience in practical communication environments.

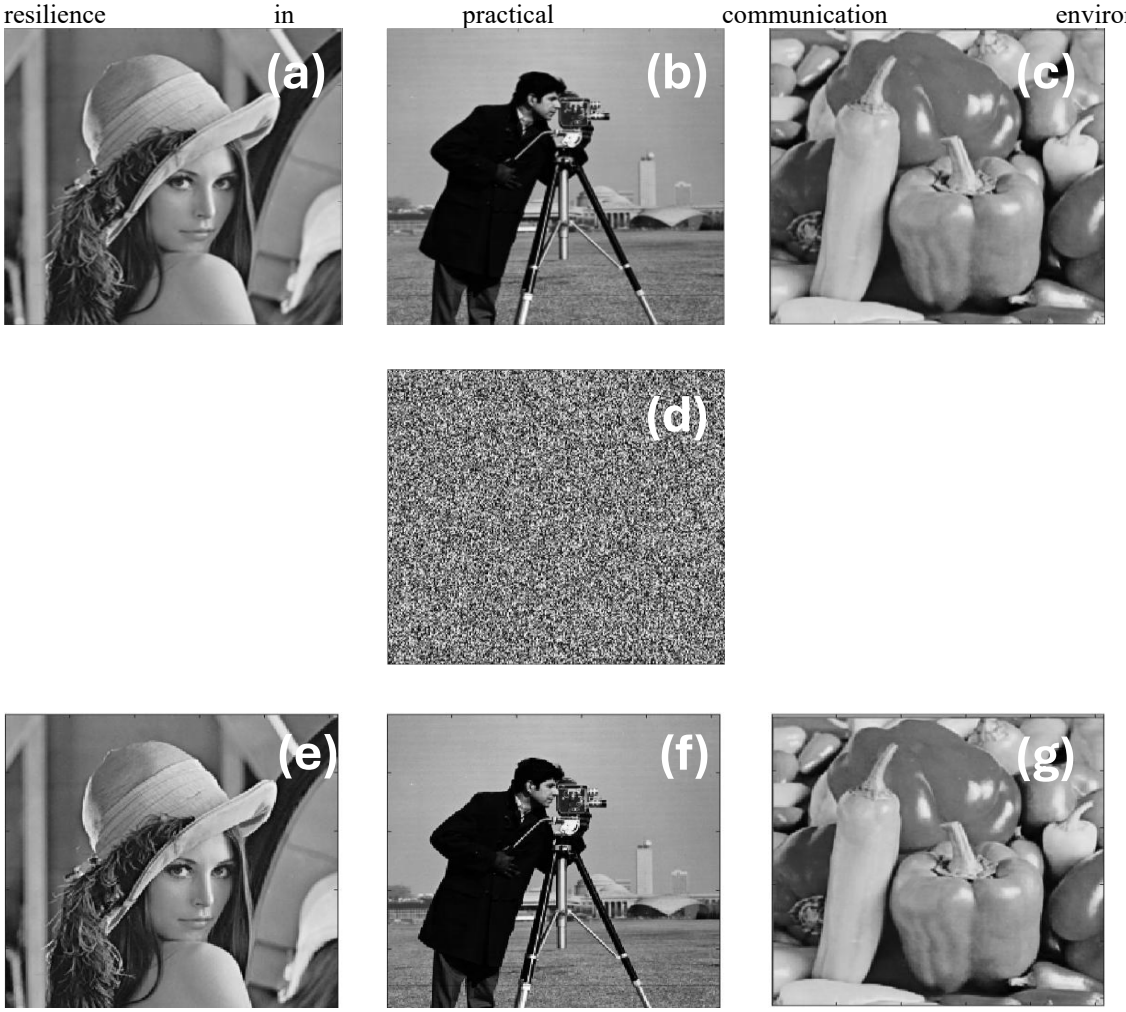

Fig 3. Original input images (a, b, c), encrypted image (d), and corresponding decrypted images (e, f, g).

4.1 Correlation Coefficient (CC)

The correlation coefficient (CC) is employed to assess the similarity between the plaintext and decrypted images. A CC value approaching 1 indicates a strong linear relationship and high – quality image reconstruction. The CC is calculated as follows:

$$\mathrm{CC} = \frac{\mathrm{cov(A,Dec)}}{\sigma(\mathrm{A})\sigma(\mathrm{Dec})} \tag{26}$$

In the above expression, (A) and (Dec) denote the plaintext and decrypted images respectively, whereas $\sigma(.)$ and $\mathrm{cov}(.)$ represent the standard deviation and covariance. The CC value varies between -1 and 1; values close to 1 indicate similarity and successful reconstruction, whereas values near 0 imply low statistical dependence.

For the proposed scheme, the CC values between the original images and their corresponding encrypted images are $(0.0048), (0.0044) and (-0.0018)$, respectively, indicating an almost negligible correlation. This demonstrates that the encryption process effectively removes the statistical relationship between the plaintext and ciphertext. In contrast, the CC values between the original and decrypted images are 1, 1 and 0.999, respectively, confirming highly accurate reconstruction and successful recovery of the original images.

4.2 Mean-Square-Error (MSE)

The mean squared error (MSE) measures the average squared difference between the original and reconstructed images. A lower MSE value signifies better reconstruction performance and greater similarity between the two images.

$$\mathrm{MSE} = \frac{1}{q_1 \times q_2} \sum_{\mathrm{x}=1}^{q_1} \sum_{\mathrm{y}=1}^{q_2} |\mathrm{A(x,y)} - \mathrm{Dec(x,y)}|^2 \tag{27}$$

Here $A(x, y)$ and $Dec(x, y)$ corresponds to the original an decrypted images, respectively, while q_1 and q_2 represents the image dimensions in terms of rows and columns.

For the proposed scheme the MSE values obtained for Lena, Cameraman and peppers image (Phase image) and their decrypted images are 1.6686×10^{-29}, 1.3874×10^{-29}, 1.4103×10^{-5}, respectively. These extremely low

values indicate negligible reconstruction error, confirming near lossless recovery. The results demonstrate high numerical precision and stability of the method, ensuring accurate and faithful restoration of the original images without any significant degradation.

4.3 Peak Signal-To-Noise Ratio (PSNR)

The peak signal – to – noise ratio (PSNR) is a standard metric used to evaluate the quality of the reconstruction image by measuring the level of distortion relative to the original image. It is given as:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{K}^2}{\mathrm{MSE}}\right) \tag{28}$$

Here, K denotes the maximum possible pixel intensity value. A higher PSNR indicates lower reconstruction error and better fidelity between the original and decrypted images.

For the proposed scheme, the PSNR values obtained for Lena, Cameraman and peppers image (Phase image) are $2.8779 \times 10^2 db$, $2.8857 \times 10^2 db$ and $48.5068\, db$ respectively. These significantly high values confirms near – perfect reconstruction, demonstrating that the decrypted images closely match the original inputs and validating the effectiveness of the proposed encryption – decryption framework.

4.4 Structural Similarity Index Measure (SSIM)

The structural similarity index measure (SSIM) is commonly used to evaluate the quantity of a reconstructed image by comparing it with the original input. An SSIM value of 1 indicates perfect structural similarity, while values closer to 1 represent higher fidelity and better reconstruction quality. The SSIM value typically lies in the range $[-1,1]$. The metric is defined as:

$$\mathrm{SSIM(M,N)} = \frac{(2\mathrm{u_M u_N}+\mathrm{V_1})(2\sigma_{\mathrm{M,N}}+\mathrm{V_2})}{(\mathrm{u_M^2}+\mathrm{u_N^2}+\mathrm{V_1})(\sigma_{\mathrm{M}}^2+\sigma_{\mathrm{N}}^2+\mathrm{V_2})} \tag{29}$$

In the SSIM formulation $\mathrm{u_M}$ and $\mathrm{u_N}$ denote the main intensity of images M and N, while σ_{M}^2 and σ_{N}^2 represent their variances. The term $\sigma_{\mathrm{M,N}}$ denotes the cross – correlation between the two images. The stabilizing constants are defined as $\mathrm{V_1} = (L_1 k)^2$ and $\mathrm{V_2} = (L_2 k)^2$, where k is the dynamic range of pixel values and $L_1 = 0.01, L_2 = 0.03$. For the proposed scheme, SSIM values between the plaintext and encrypted images are $1.4911 \times 10^{-5}, 1.2980 \times 10^{-4}, -4.4520 \times 10^{-4}$ respectively, indicating negligible structural similarity after encryption. In contrast, SSIM values close to 1 for the decrypted images confirm almost perfect structural reconstruction and accurate recovery of the original inputs.

4.5 Evaluation of Information Entropy

Information entropy, introduced by Shannon, is a key measure used to quantify the randomness and uncertainty in a data distribution. In image cryptography, it is employed to evaluate the statistical uniformity of ciphertext images. For an ideal 8 – bit encrypted image, the entropy value should be close to 8, indicating a uniform pixel distribution and minimal redundancy. This reduces information leakage and enhances resistance to statistical attacks, thereby reflecting the security strength of the encryption scheme. The entropy is defined as:

$$\mathrm{IE} = -\sum_{\mathrm{x}=0}^{\mathrm{Z}-1} \mathrm{W(x)}\log_2 \mathrm{W(x)} \tag{30}$$

Here, W(x) denotes the probability of occurrence of the x^{th} Gray level, and Z represents the total number of possible intensity levels. The entropy values of Lena, Cameraman and peppers images are 7.3522, 7.0097 and 7.6023 respectively, whereas the encrypted image achieves an entropy of 7.9838. The value being close to theoretical maxima confirms high randomness and strong resistance against statistical attacks.

4.6 Histogram Uniformity Analysis

Histogram analysis is a standard tool in image encryption for accessing security and algorithm performance. It reflects the distribution of pixel intensity and helps detect possible information leakage. For a secure scheme, the ciphertext histogram should differ significantly from that of the plaintext, eliminating exploitable statistical patterns. As shown in figure 4, the encrypted image histogram is nearly uniform and clearly distinct from the original images, indicating strong randomness and effective concealment of statistical features. This uniformity confirms resistance to statistical attacks. In contrast, the accurate and lossless reconstruction.

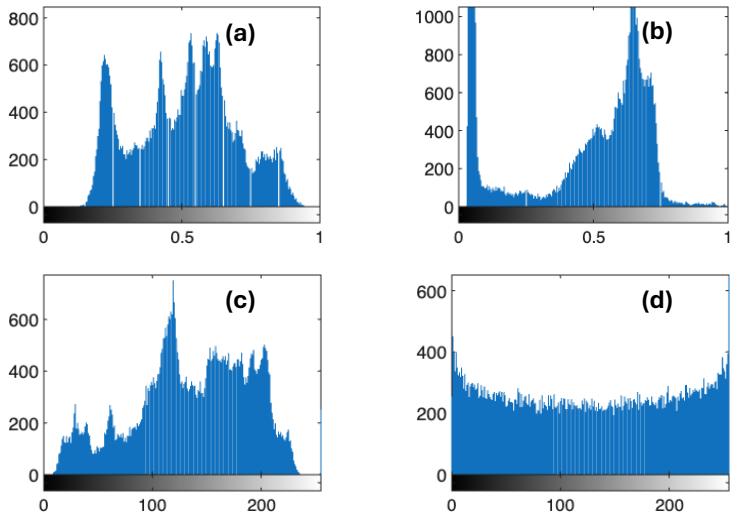

Fig 4. Histogram of Original input images (a, b, c), encrypted image (d).

4.7 3D Pixel Intensity Distribution Analysis

Three dimensional surface plot illustrate pixel intensity variations and provide a qualitative assessment of image structure in encryption analysis. As shown in figure 5, the original image exhibits a smooth surface due to spatial correlation, while the encrypted image displays a chaotic and irregular structure, indicating effective randomization and strong resistance to statistical and structural attacks. The decrypted image closely resembles the original, confirming accurate reconstruction and preservation of image fidelity. Overall, the 3D analysis validates the robustness of the proposed cryptosystem.

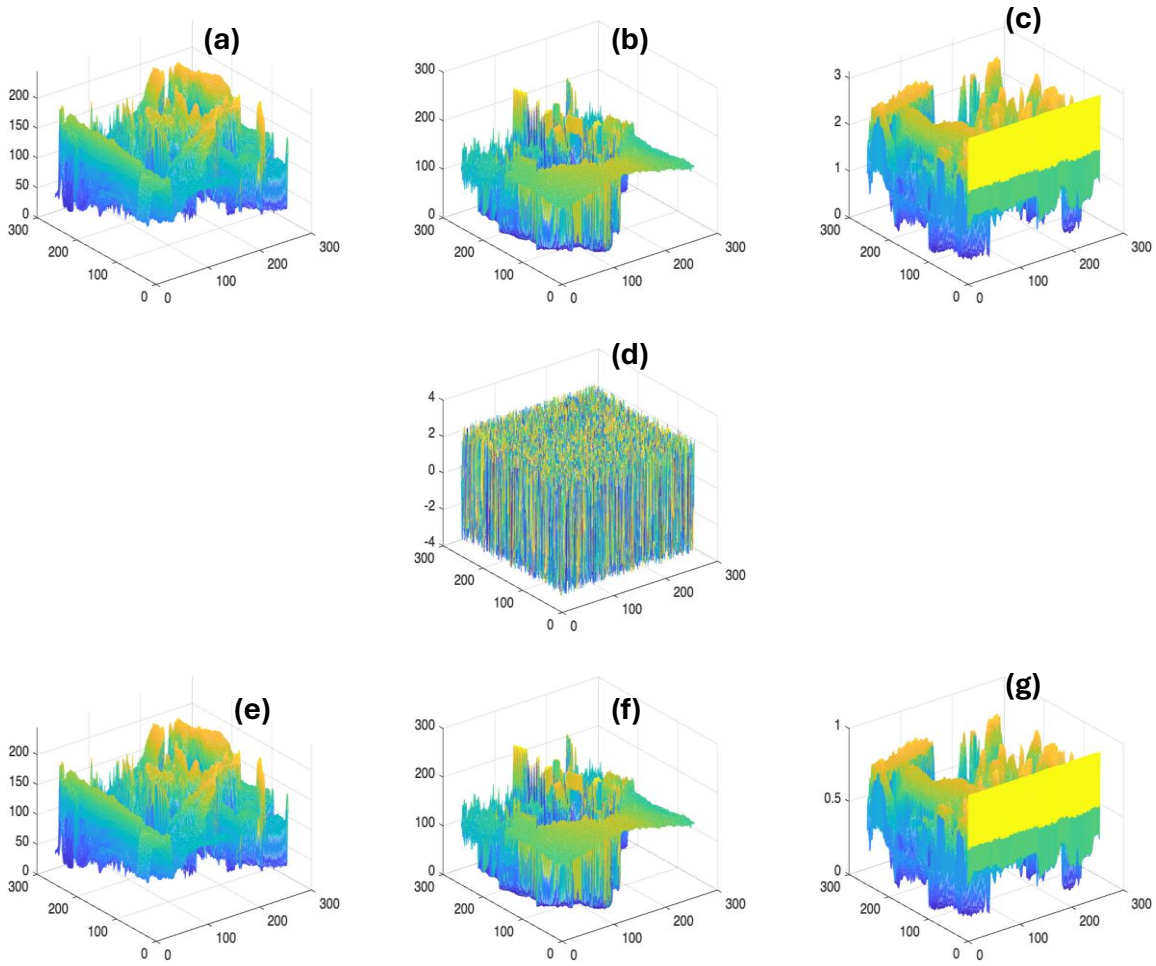

Fig 5. 3D surface plots of Original input images (a, b, c), encrypted image (d) and decrypted image (e, f, g).

4.8 Noise Robustness Analysis

In practical communication environments, encrypted images may be corrupted by channel noise during transmission. Therefore, an effective encryption scheme should be capable of recovering recognizable image information even in presence of noise. To evaluate the robustness of the proposed framework, additive Gaussian noise with zero mean and unit variance is introduced into the ciphertext according to equation 31

$$C_n = C + n \times N(0,1) \quad (31)$$

Where C and C_n denote the original and noisy ciphertext respectively, and n represents the noise strength. The decryption process is then performed on the noisy ciphertext for various noise levels. As illustrated in figure 6, the decrypted images remain visually recognizable even at a noise strength of 20000, demonstrating the strong robustness of the proposed scheme against noise – induced distortions.

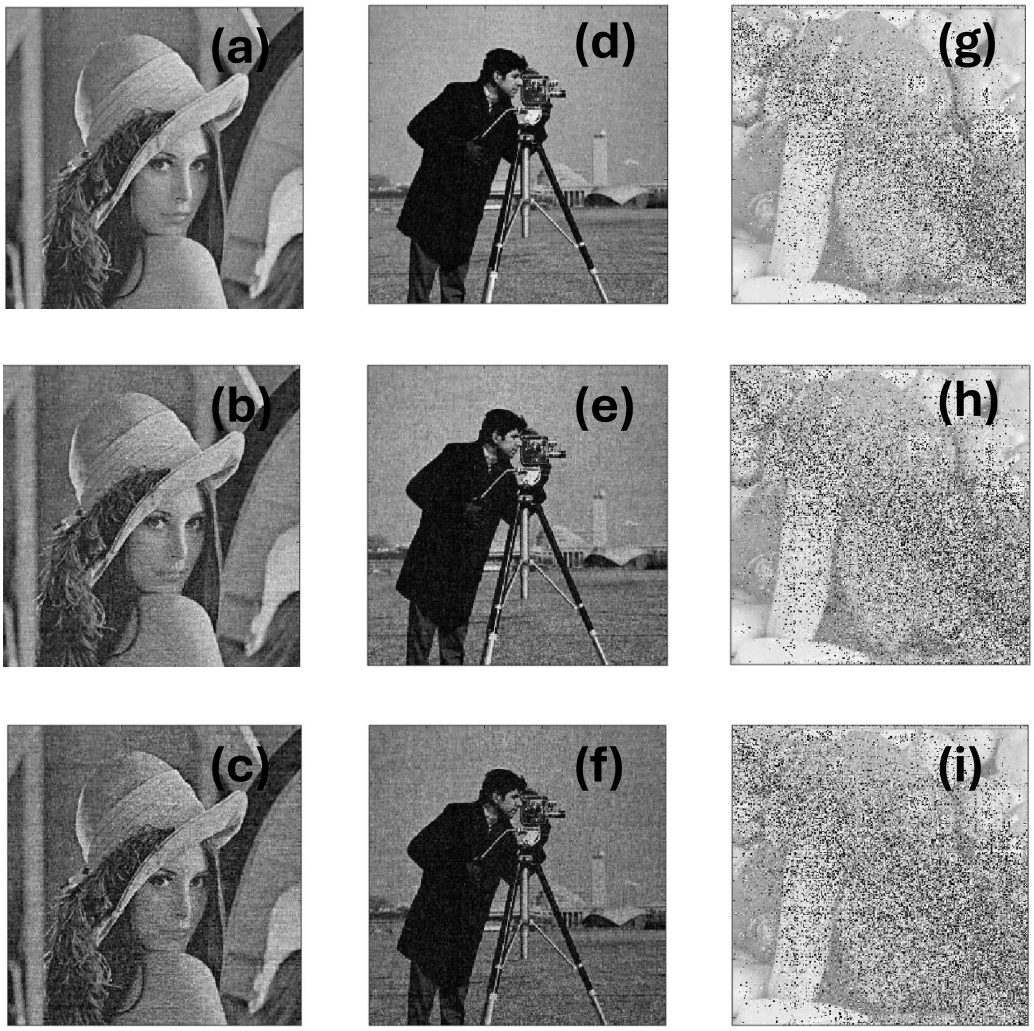

Fig 6. Decrypted images of Lena (a-c), Cameraman (d-f) and Peppers (g-i) under Gaussian noise attacks with noise strength $10^4, 1.5 \times 10^4 and\ 2 \times 10^4$, respectively.

4.9. Evaluation of Occlusion Resistance

To assess the resilience of the proposed scheme against partial data loss, occlusion attack are performed by masking 20.3%, 50% and 70.3% of the ciphertext pixels. The corresponding occluded ciphertexts and their decrypted outputs are shown in figure 7, Despite the substantial loss of encrypted data, the decrypted images remain visually recognizable and preserve the major image features. These results demonstrate the strong robustness and fault – tolerance capability of the proposed encryption framework against occlusion attacks.

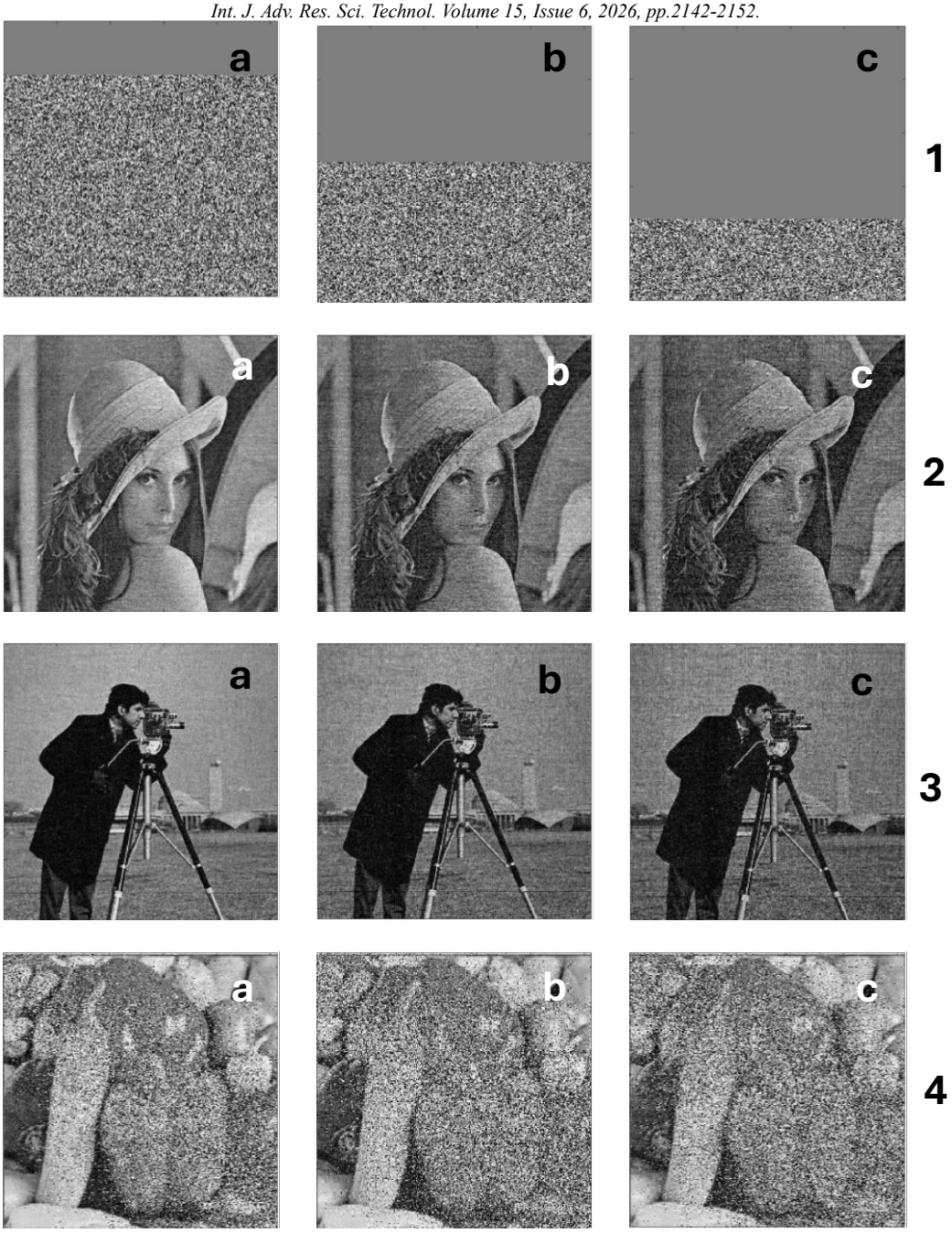

Fig 7. Occlusion attack analysis: (1-4) encrypted images with respectively 20.3%, 50% and 70.3% occlusion, (a) occluded encrypted image, while (b), (c) and (d) show the corresponding decrypted images.

5. Summary and Conclusion

A robust optical multi – image encryption framework has been developed by combining Quasi – Zernike (QZ) synthesis, the Gyrator Transform (GT), random phase masks (RPMs), and cascaded Equal Modulus Decomposition (EMD). The proposed framework exploits QZ synthesis to simultaneously fuse two plaintext images and generate multiple private keys, while the subsequent GT, random modulation, and cascaded EMD stages introduce multiple layers of encryption and additional secret keys, thereby significantly enhancing cryptographic complexity. The original images are successfully recovered only when all secret parameters are correctly specified, demonstrating the asymmetric nature and high key sensitivity of the proposed framework. The effectiveness of the proposed method has been validated through extensive security and performance analyses. The ciphertext exhibits high randomness, a uniform intensity distribution, negligible statistical correlation, and information entropy approaching theoretical limit, confirming its resistance to statistical cryptanalysis. The framework further maintains reliable performance under noise and occlusion attacks while achieving near lossless image reconstruction , as evidenced by the obtained CC, MSE, PSNR and SSIM values. These results establish the proposed framework as an efficient and secure approach for optical multi – image encryption and secure communication.

References

[1] P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random

encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, Apr. 1995, doi: 10.1364/OL.20.000767.

[2] R. Girija and H. Singh, "A cryptosystem based on deterministic phase masks and fractional Fourier transform deploying singular value decomposition," *Opt Quant Electron*, vol. 50, no. 5, Art. no. 5, May 2018, doi: 10.1007/s11082-018-1472-6.

[3] P. Singh, A. K. Yadav, K. Singh, and I. Saini, "Optical image encryption in the fractional Hartley domain, using Arnold transform and singular value decomposition," *AIP Conference Proceedings*, vol. 1802, no. 1, pp. 020017-1–7, Jan. 2017, doi: 10.1063/1.4973267.

[4] H. Singh, A. K. Yadav, S. Vashisth, and K. Singh, "Optical image encryption using devil's vortex toroidal lens in the Fresnel transform domain," *International Journal of Optics*, vol. 2015, pp. 1–13, 2015, doi: 10.1155/2015/926135.

[5] Anshula and H. Singh, "Cryptanalysis for double-image encryption using the DTLM in frequency plane with QR decomposition and gyrator transform," *Opt Rev*, vol. 28, no. 6, pp. 596–610, Dec. 2021, doi: 10.1007/s10043-021-00705-0.

[6] H. Singh, "Hybrid structured phase mask in frequency plane for optical double image encryption in gyrator transform domain," *Journal of Modern Optics*, vol. 0, no. 0, pp. 1–14, Jul. 2018, doi: 10.1080/09500340.2018.1496286.

[7] M. R. Abuturab, "An asymmetric single-channel color image encryption based on Hartley transform and Gyrator transform," *Optics and Lasers in Engineering*, vol. 69, pp. 49–57, Jun. 2015, doi: 10.1016/j.optlaseng.2015.01.001.

[8] A. Lopez-Caloca and B. Escalante-Ramirez, "The Hermite Transform: An Efficient Tool for Noise Reduction and Image Fusion in Remote-Sensing," in *Image Processing for Remote Sensing*, C. Chen, Ed., CRC Press, 2007, pp. 273–291. Accessed: Mar. 21, 2020. [Online]. Available: http://www.crcnetbase.com/doi/10.1201/9781420066654.ch12

[9] Shalu, A. K. Yadav, and P. Singh, "Uniquely designed optical cryptosystem for watermarking of double-color images in the fractional Hermite-transform domain," *Opt. Eng.*, vol. 64, no. 09, Sep. 2025, doi: 10.1117/1.OE.64.9.093101.

[10] Shalu, P. Singh, and A. K. Yadav, "Watermarking based on asymmetric dual-image encryption using QZ algorithm and vortex toroidal lenses in fractional Hermite transform domain," *Optik*, vol. 342–343, p. 172598, Dec. 2025, doi: 10.1016/j.ijleo.2025.172598.

[11] P. Rakheja, R. Vig, and P. Singh, "Asymmetric hybrid encryption scheme based on modified equal modulus decomposition in hybrid multi-resolution wavelet domain," *Journal of Modern Optics*, vol. 66, no. 7, pp. 799–811, Apr. 2019, doi: 10.1080/09500340.2019.1574037.

[12] M. Agoyi, E. Çelebi, and G. Anbarjafari, "A watermarking algorithm based on chirp z-transform, discrete wavelet transform, and singular value decomposition," *SIViP*, vol. 9, no. 3, pp. 735–745, Mar. 2015, doi: 10.1007/s11760-014-0624-9.

[13] P. Singh, A. K. Yadav, and K. Singh, "Known-Plaintext Attack on Cryptosystem Based on Fractional Hartley Transform Using Particle Swarm Optimization Algorithm," in *Engineering Vibration, Communication and Information Processing*, vol. 478, K. Ray, S. N. Sharan, S. Rawat, S. K. Jain, S. Srivastava, and A. Bandyopadhyay, Eds., Singapore: Springer Singapore, 2019, pp. 317–327. doi: 10.1007/978-981-13-1642-5_29.

[14] X. Peng, H. Wei, and P. Zhang, "Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain," *Optics letters*, vol. 31, no. 22, pp. 3261–3263, Nov. 2006, doi: 10.1364/OL.31.003261.

[15] 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," *Optics letters*, vol. 30, no. 13, pp. 1644–1646, 2005, doi: https://doi.org/10.1364/OL.30.001644.

[16] S. Jiao, G. Li, C. Zhou, W. Zou, and X. Li, "Special ciphertext-only attack to double random phase encryption by plaintext shifting with speckle correlation," *J. Opt. Soc. Am. A, JOSAA*, vol. 35, no. 1, pp. A1–A6, Jan. 2018, doi: 10.1364/JOSAA.35.0000A1.

[17] W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," *Optics letters*, vol. 35, no. 2, pp. 118–120, Jan. 2010, doi: 10.1364/OL.35.000118.

[18] J. Cai, X. Shen, M. Lei, C. Lin, and S. Dou, "Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition," *Optics letters*, vol. 40, no. 4, pp. 475–478, Feb. 2015, doi: 10.1364/OL.40.000475.

[19] Archana, P. Singh, and P. Rakheja, "Asymmetric watermarking scheme for color images using cascaded unequal modulus decomposition in Fourier domain," *Journal of Modern Optics*, vol. 68, no. 20, pp. 1094–1107, Nov. 2021, doi: 10.1080/09500340.2021.1977404.

[20] Sachin, P. Singh, R. Kumar, and A. K. Yadav, "Asymmetric cryptosystem for color images based on unequal modulus decomposition in Chirp-z domain," in *Proceedings of Academia-Industry Consortium for Data Science*, G. Gupta, L. Wang, A. Yadav, P. Rana, and Z. Wang, Eds., in Advances in Intelligent Systems and Computing, vol. 1411. Singapore: Springer Nature, 2022, pp. 331–344. doi: 10.1007/978-981-16-6887-6_27.

[21] R. Yadav and P. Singh, "Asymmetric image authentication algorithm using double random modulus decomposition and CGI," *Computational and Applied Mathematics*, vol. 42, no. 7, p. 305, Sep. 2023, doi: 10.1007/s40314-023-02443-2.

[22] S. Anjana, A. Yadav, P. Singh, and H. Singh, "Audio and image encryption scheme based on QR decomposition and random modulus decomposition in Fresnel domain," *Optica Applicata*, vol. 52, no. 3, pp. 359–374, 2022, doi: 10.37190/oa220303.

[23] P. Singh, A. K. Yadav, and K. Singh, "Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition," *Optics and Lasers in Engineering*, vol. 91, pp. 187–195, Apr. 2017, doi: 10.1016/j.optlaseng.2016.11.022.

[24] P. Singh, A. K. Yadav, and K. Singh, "Phase image encryption in the fractional Hartley domain using

Arnold transform and singular value decomposition," *Optics and Lasers in Engineering*, vol. 91, pp. 187–195, Apr. 2017, doi: 10.1016/j.optlaseng.2016.11.022.

[25] Q. Su, G. Wang, G. Lv, X. Zhang, G. Deng, and B. Chen, "A novel blind color image watermarking based on Contourlet transform and Hessenberg decomposition," *Multimed Tools Appl*, vol. 76, no. 6, pp. 8781–8801, Mar. 2017, doi: 10.1007/s11042-016-3522-z.

[26] Anshula and H. Singh, "Cryptanalysis for double-image encryption using the DTLM in frequency plane with QR decomposition and gyrator transform," *Opt Rev*, vol. 28, no. 6, pp. 596–610, Dec. 2021, doi: 10.1007/s10043-021-00705-0.

[27] P. Rakheja, P. Singh, and R. Vig, "An asymmetric image encryption mechanism using QR decomposition in hybrid multi-resolution wavelet domain," *Optics and Lasers in Engineering*, vol. 134, p. 106177, Nov. 2020, doi: 10.1016/j.optlaseng.2020.106177.

[28] R. Yadav, Sachin, and P. Singh, "Multidomain asymmetric image encryption using phase-only CGH, QZS method and Umbrella map," *J Opt*, Aug. 2024, doi: 10.1007/s12596-024-02106-3.

[29] M. R. Abuturab, "An asymmetric color image cryptosystem based on Schur decomposition in gyrator transform domain," *Optics and Lasers in Engineering*, vol. 58, pp. 39–47, Jul. 2014, doi: 10.1016/j.optlaseng.2014.01.025.

[30] Sachin, Archana, and P. Singh, "Optical image encryption algorithm based on chaotic Tinkerbell map with random phase masks in Fourier domain," in *Proceedings of International Conference on Data Science and Applications*, K. Ray, K. C. Roy, S. K. Toshniwal, H. Sharma, and A. Bandyopadhyay, Eds., in Lecture Notes in Networks and Systems, vol. 148. Singapore: Springer, 2021, pp. 249–262. doi: 10.1007/978-981-15-7561-7_20.

[31] Sachin and P. Singh, "A novel chaotic Umbrella map and its application to image encryption," *Opt Quant Electron*, vol. 54, no. 5, p. 266, Apr. 2022, doi: 10.1007/s11082-022-03646-3.

[32] P. Rakheja, S. Yadav, and A. Tobria, "A novel image encryption mechanism based on umbrella map and Yang-Gu algorithm," *Optik*, vol. 271, p. 170152, Dec. 2022, doi: 10.1016/j.ijleo.2022.170152.

[33] Archana, Sachin, and P. Singh, "Cryptosystem based on triple random phase encoding with chaotic Henon map," in *Proceedings of International Conference on Data Science and Applications*, vol. 148, K. Ray, K. C. Roy, S. K. Toshniwal, H. Sharma, and A. Bandyopadhyay, Eds., Singapore: Springer Singapore, 2021, pp. 73–84. Accessed: Jan. 03, 2021. [Online]. Available: http://link.springer.com/10.1007/978-981-15-7561-7_5

[34] Sachin and P. Singh, "Analysis of chaotic patterns in the Bird wing map and implications in image security," *Journal of Modern Optics*, vol. 0, no. 0, pp. 1–26, Jul. 2025, doi: 10.1080/09500340.2025.2508790.

[35] P. Singh, A. K. Yadav, K. Singh, and I. Saini, "Optical image encryption in the fractional Hartley domain, using Arnold transform and singular value decomposition," *AIP Conference Proceedings*, vol. 1802, no. 1, pp. 020017-1–7, Jan. 2017, doi: 10.1063/1.4973267.

[36] J. Cai, X. Shen, and C. Lin, "Security-enhanced asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition," *Opt. Commun.*, vol. 359, pp. 26–30, Jan. 2016, doi: 10.1016/j.optcom.2015.09.058.

[37] S. P. Barfungpa and M. R. Abuturab, "Asymmetric cryptosystem using coherent superposition and equal modulus decomposition of fractional Fourier spectrum," *Opt Quant Electron*, vol. 48, no. 11, Art. no. 11, Nov. 2016, doi: 10.1007/s11082-016-0786-5.

[38] H. Singh and K. Singh, "A watermarking-based asymmetric cryptosystem using gyrator transform, QZ modulation, and fractional vortex toroidal phase mask," *J Opt*, vol. 54, no. 2, pp. 300–313, Apr. 2025, doi: 10.1007/s12596-024-02329-4.

[39] R. Yadav, Sachin, and P. Singh, "Multidomain asymmetric image encryption using phase-only CGH, QZS method and Umbrella map," *J Opt*, pp. 1–18, Aug. 2024, doi: 10.1007/s12596-024-02106-3.

[40] M. R. Abuturab, "Color information verification system based on singular value decomposition in gyrator transform domains," *Optics and Lasers in Engineering*, vol. 57, pp. 13–19, Jun. 2014, doi: 10.1016/j.optlaseng.2014.01.006.

[41] J. Kumar, P. Singh, A. K. Yadav, and A. Kumar, "Asymmetric Image Encryption Using Gyrator Transform with Singular Value Decomposition," in *Engineering Vibration, Communication and Information Processing*, vol. 478, K. Ray, S. N. Sharan, S. Rawat, S. K. Jain, S. Srivastava, and A. Bandyopadhyay, Eds., Singapore: Springer Singapore, 2019, pp. 375–383. doi: 10.1007/978-981-13-1642-5_34.

[42] S. P. Barfungpa and M. R. Abuturab, "Asymmetric cryptosystem using coherent superposition and equal modulus decomposition of fractional Fourier spectrum," *Opt Quant Electron*, vol. 48, no. 11, Art. no. 11, Nov. 2016, doi: 10.1007/s11082-016-0786-5.