Multi-Image Cryptosystem through Wavelength Multiplexing and QZ Algorithm using Multiple Random Phase Masks

[1]Nagander Singh Tomer

Assistant Professor of Mathematics

Department of Mathematics

Guru Gorakhnath ji Govt. College, Hisar, Haryana, India 125001

Email: tomar.smart@gmail.com

Abstract

With the increasing generation and exchange of visual data, there is a growing need for encryption techniques capable of securely handling multiple images simultaneously. In this paper, a multi-image cryptosystem based on multiple random phase masks is proposed to enhance both security and information capacity. The proposed scheme encrypts four grayscale images into a single ciphertext through a series of mathematical transforms and decompositions. Initially, pairs of images are combined using a phase retrieval algorithm in the Fresnel domain with the help of two random phase masks. The resulting outputs are further processed through iterative phase retrieval operations and merged into a single image using the QZ algorithm. To strengthen security, an additional random phase mask is introduced before applying the Fourier transform to generate the final ciphertext. Although the encryption process involves several stages, the decryption procedure is straightforward and enables accurate recovery of all original images. The effectiveness of the proposed cryptosystem is demonstrated through experiments on four grayscale images, where complete reconstruction of the plaintext images is achieved. Furthermore, the scheme is evaluated against statistical, noise, occlusion, and brute-force attacks. The results indicate strong robustness and a high sensitivity to encryption parameters, ensuring that even minor deviations in the secret keys lead to unsuccessful reconstruction. These characteristics make the proposed cryptosystem a promising solution for secure, high-capacity image encryption in future multimedia and communication applications.

Keywords: Multi-image, Wavelength multiplexing, QZ algorithm, Fresnel transform, Random phase masks.

1. Introduction

Today, people increasingly depend on digital technologies, including Smartphone's, smart watches, online communication platforms, electronic banking, healthcare systems, social media platforms, personal records, corporate databases, government services, and many other digital applications. This growing need for secure data transmission and storage has motivated extensive research in the field of information security. Several conventional cryptographic algorithms, such as the Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Rivest–Shamir–Adleman (RSA), have been widely employed for data protection. Although these techniques provide reliable security for textual data, they often suffer from high computational complexity and increased processing time when applied to large multimedia data such as images and videos. In contrast, optical cryptosystems have attracted considerable attention due to their inherent parallel processing capability.

A major breakthrough in optical encryption was achieved in 1995 when Refregier and Javidi proposed the double random phase encoding (DRPE) technique[1], which soon became a cornerstone of optical cryptography. In the DRPE scheme, the plaintext image is first modulated using a random phase mask and transformed through a Fourier optical system. The transformed output is then multiplied by a second random phase mask and processed through another Fourier transform. By employing two successive random phase

modulations in a 4f optical setup, DRPE produces an encrypted image that closely resembles stationary white noise, thereby providing a high degree of security. Owing to its effectiveness, numerous extensions and modifications of DRPE have been proposed to expand its applications and improve its capability to encode both amplitude and phase information. However, subsequent investigations revealed several security limitations of the DRPE scheme. Due to its linear and symmetric structure, DRPE is vulnerable to various cryptographic attacks, including known-plaintext attacks (KPA)[2], [3], ciphertext-only attacks (COA)[4], and chosen-plaintext attacks (CPA)[5], [6].

To address these security weaknesses, researchers developed asymmetric optical encryption techniques with improved resistance against conventional cryptographic attacks. In 2010, Qin and Peng[7] introduced the phase-truncated Fourier transform (PTFT), which is recognized as the first asymmetric optical encryption algorithm. Their pioneering work opened a new research direction in asymmetric optical cryptography. The nonlinear characteristics of PTFT significantly enhance its resistance to attacks that compromise the security of DRPE. Nevertheless, Wang and Zhao[8], [9], [10] later demonstrated that PTFT remains vulnerable to certain attacks because of the correlation between the retained and truncated phase components. To further improve the security and robustness of optical cryptosystems, several decomposition-based encryption techniques have been proposed. These include singular value decomposition (SVD)[11], [12], [13], [14], [15], [16], equal modulus decomposition (EMD)[17], [18], random modulus decomposition (RMD)[19], [20], unequal modulus decomposition (UMD)[21], [22], [23], [24], [25], [26], polar decomposition (PD)[27], [28], and numerous other matrix decomposition[29], [30], [31], [32], [33], [34] methods.

Since modern communication systems continuously generate and transmit massive amounts of multimedia data, encrypting a single image at a time is often insufficient for practical applications. Multi-image encryption has therefore emerged as an efficient approach that enables multiple images to be encrypted simultaneously, thereby improving transmission efficiency, reducing computational overhead, and increasing storage utilization. In addition to enhancing throughput, multi-image encryption also increases security by introducing inter-image correlations and expanding the key space, making cryptographic attacks more difficult. Among the various multiplexing techniques, wavelength multiplexing has attracted significant attention in optical encryption due to its ability to exploit the wavelength degree of freedom. In wavelength multiplexing, multiple plaintext images are encoded using different illumination wavelengths and combined into a single ciphertext, allowing independent recovery of each image with the corresponding wavelength key. This approach not only increases the information-carrying capacity of the optical cryptosystem but also improves encryption efficiency without requiring additional optical channels. Furthermore, the incorporation of wavelength as an additional security parameter enlarges the key space and enhances resistance against brute-force and statistical attacks. Owing to these advantages, wavelength multiplexing has become a promising strategy for developing high-capacity, secure, and efficient multi-image optical encryption systems suitable for modern multimedia communication and storage applications.

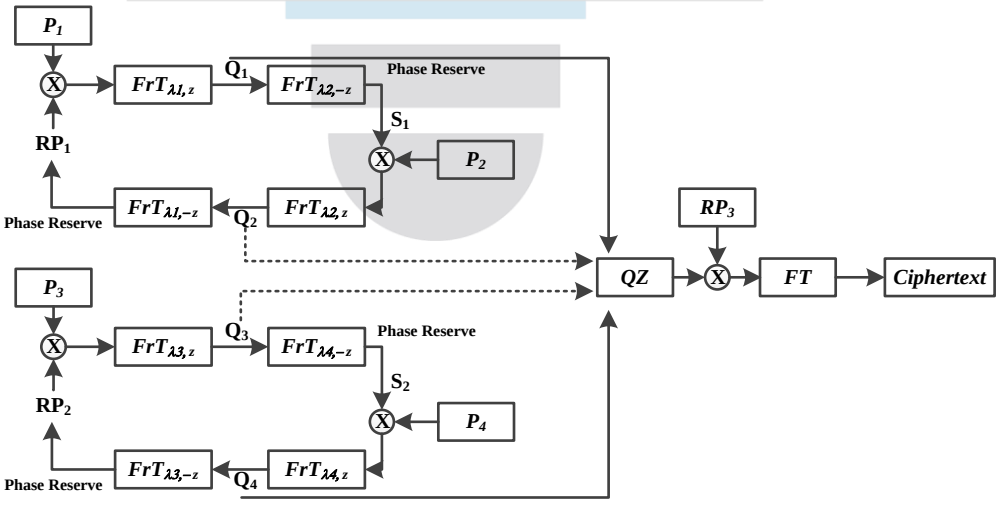
Motivated by the increasing demand for secure and high-capacity image encryption, this paper proposes a novel multi-image optical cryptosystem based on multiple random phase masks. The proposed scheme encrypts four grayscale images into a single ciphertext through a combination of Fresnel-domain[35], [36], [37], [38], [39] iterative phase retrieval, QZ decomposition[40], [41], and Fourier transform[42], [43], [44], [45], [46], [47]. Initially, two pairs of plaintext images are independently encoded using iterative phase retrieval with random phase masks in the Fresnel domain. The resulting intermediate outputs are subsequently combined through another phase retrieval process and fused into a single image using the QZ algorithm. To further enhance the security of the cryptosystem, an additional random phase mask is incorporated prior to the Fourier transform, producing the final encrypted image. Compared with conventional multi-image encryption techniques, the proposed approach provides higher information capacity, increased key diversity, and improved resistance against various cryptographic attacks while maintaining a simple and efficient decryption procedure. Extensive simulation results demonstrate that the proposed cryptosystem accurately reconstructs all plaintext images and exhibits strong robustness against statistical, noise, occlusion, and brute-force attacks, making it a promising candidate for secure multimedia communication and storage applications. The remainder of this paper is organized as follows. Section II describes the proposed multi-image encryption and decryption

procedures in detail. Section III discusses the experimental results and security analyses. Finally, Section IV concludes the paper and outlines potential directions for future research.

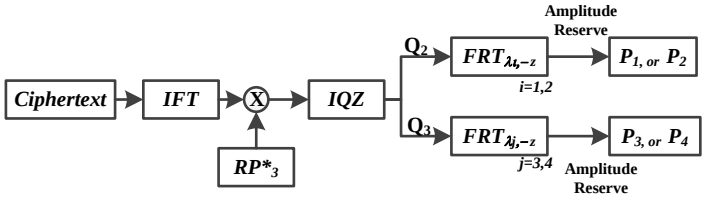
2. Proposed Cryptosystem

The plaintext image P1 is first modulated by a random phase mask RP1, and a Fresnel transform with wavelength λ1 and propagation distance z is applied on them to give F1 as shown in Fig. 1. Subsequently,Q1 is propagated through another Fresnel transform with wavelength λ2 and propagation distance z. The phase component of the resulting complex field is combined with the second plaintext image P2 (usually referred to as the target image in the phase retrieval algorithm).Fresnel transform with wavelength λ2 and distance z applied on them to give Q2. It undergoes another Fresnel transform with wavelength λ1 and propagation distance z. Amplitude truncated part of the resulting image updates the RP1.It makes a loop of phase retrieval algorithm for wavelength multiplexing. One should come out of the loop if the sum of correlation coefficients between P1 and PT(FrT(λ1, z)(Q1)), and P2 and PT(FrT(λ2, z)(Q2)) reached a threshold value. Here PT denotes the phase truncation operator. In this work, the threshold value is set to 1.99, corresponding to the combined correlation coefficient of the two reconstructed images. Same procedure is repeated for another set of images P3 and P4. Q1 and Q4 is combined using QZ algorithm. Random phase mask 3 is bonded with combined QZ image and Fourier transform is applied on it to give the ciphertext.

Although the proposed encryption process is computationally intensive due to the iterative phase retrieval algorithm, the corresponding decryption procedure is relatively simple and computationally efficient. The decryption begins by applying the inverse Fourier transform to the ciphertext. The resulting complex field is then multiplied by the complex conjugate of the third random phase mask (RP3). Subsequently, inverse QZ decomposition is performed to separate the multiplexed information, yielding either the pair (Q1,Q4) or (Q2,Q3) depending on the selected decomposition branch. For simplicity, Fig. 1(b) illustrates the decryption process corresponding to the pair (Q2,Q3). Finally, the original plaintext images P1, P2, P3and P4 are recovered by propagating the respective intermediate images through the Fresnel transform using their corresponding wavelengths. Since each plaintext image is associated with a unique wavelength, only the correct wavelength key enables successful reconstruction, thereby providing an additional layer of security to the proposed cryptosystem. The complete decryption procedure is illustrated in Fig. 1(b).



(a) Encryption



(b) Decryption

Fig. 1. Proposed encryption (a) and decryption algorithm (b).

3. Results and discussion

In this section, numerical simulations are carried out to assess the effectiveness and robustness of the proposed algorithm based on multiple images and multiple phase masks. The proposed cryptographic framework has been validated using diverse range of image categories; however, the results corresponding to the grayscale images are presented in the manuscript. In the simulations, several combinations of Fresnel transform parameters, including propagation wavelength and distances were considered. For the results presented in the manuscript, a propagation wavelength of 632.8 nm was employed, while the Fresnel propagation distances were propagation distance Z_1 and Z_2 is taken as 20 cm and 30 cm respectively. The simulations were conducted using MATLAB software. The validation outcomes obtained using the proposed algorithm is illustrated in Fig. 2. Figure 2(I-IV) presents the original input images, Fig. 2(V) depicts the encrypted image, and Fig. 2(VI-IX) illustrates the corresponding recovered images obtained after decryption process. Result validates that ciphertext is completely different form the plaintext image. Figure 2(V) demonstrates that no meaningful information related to the plaintext can be inferred from the encrypted image. The various statistical measures such as information entropy, mean squared error, and correlation coefficient are analyzed. The security of proposed algorithm is also validated using cryptographic attacks, such as noise, occlusion, bruteforce, and key sensitivity analysis. The statistical and cryptographic attack results show that proposed cryptosystem is robust and effective.

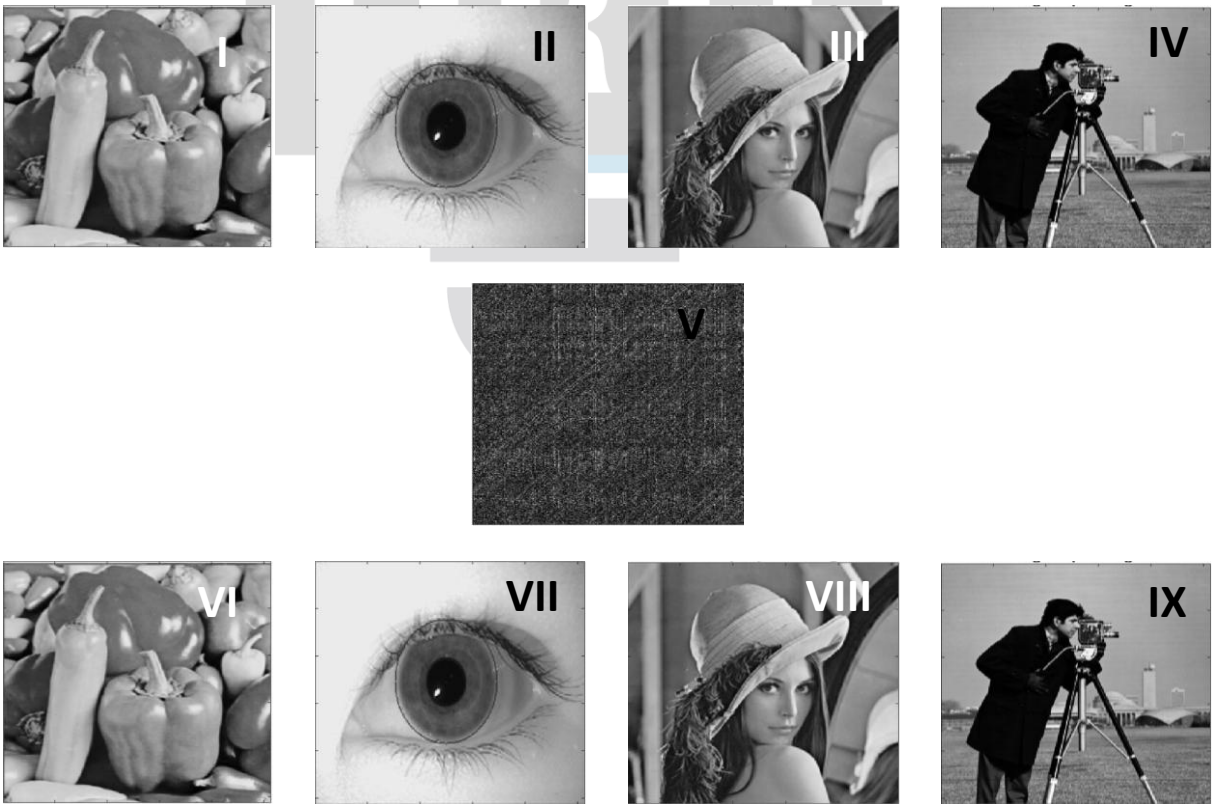


Fig 2: Validation results of the proposed framework. Figure 2(I-IV) presents original input images, Fig. 2(V) depicts the encrypted image, and Fig. 2(VI-IX) illustrates the corresponding recovered images.

The performance of the proposed encryption framework is quantitatively assessed using statistical metrics, including mean squared error (MSE) and the correlation coefficient (CC). The CC plays a vital role in statistically analyzing the similarity between images. The value of CC spans between -1 and 1. When the correlation coefficient approaches 1, it demonstrates high similarity between images, whereas values approaching zero suggest minimal correlation or no correlation. The mathematical formulation of CC is expressed in equation 11.

$$CC = \frac{Cov(I_1, I_2)}{\sigma(I_1)\sigma(I_2)} \quad (1)$$

In this formulation, I_1 and I_2 represent the two images being compared, while Cov denotes covariance and σ signifies standard deviation.

The MSE quantifies reconstruction accuracy by calculating the average squared difference between originall and reconstructed pixel values. The mathematical representation of the mean squared error is provided in equation (12).

$$MSE = \frac{1}{m \times n} \sum \sum |I_1 - I_2|^2 \quad (2)$$

The CC and MSE between original and encrypted image is 0.08 and 10^6 respectively. The correlation coefficient and MSE between plaintext and recovered image is 0.99 and 0.0045, respectively. The substantial MSE values and minimal CC scores observed between original and encrypted images demonstrate complete dissimilarity, proving the ciphertext successfully obscures all identifiable patterns from the plaintext.

During real-world data transmission, signals are often degraded by random disturbances introduced by communication channels and external factors. Such disturbances are generally modeled as noise. To investigate the resilience of the proposed encryption scheme, noise attack analysis were conducted by incorporating normally distributed random noise into the ciphertext. The additive noise process is mathematically described in equation 3.

$$C^* = C + \alpha N \quad (3)$$

here, N denotes the normal random noise which is generated using the unit variance and zero mean, C is ciphertext, C^* is the ciphertext mixed with noise. The simulation results of noise attack analysis are depicted in Fig. 3. Figure 3(I-IV) presents recovered images after noise 10000, Fig. 3(V-VIII) depicts recovered images after noise 50000, and Fig. 3(IX-XII) illustrates recovered images after noise 80000, and Fig. 3(XIII-XVI) depicts recovered image after noise 100000. Figure 4. depicts the plot between CC and additive noise strength for the four input images. The results indicate that the proposed cryptosystem maintains satisfactory reconstruction performance under noisy conditions, confirming its robustness against noise attacks.

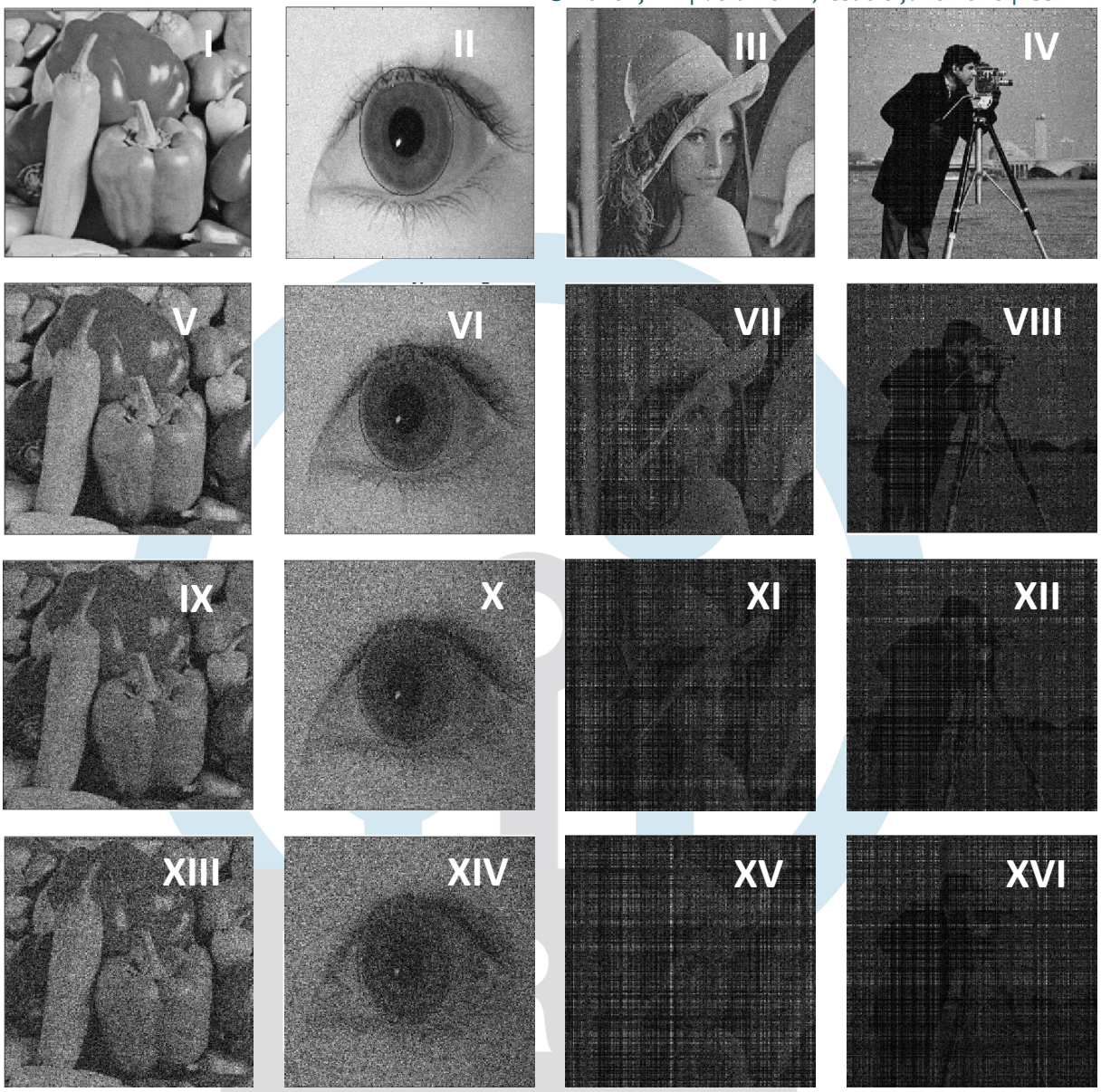


Fig.3.: Results of noise attack analysis. Figure 4(I-IV) presents recovered images after noise 10000, Fig. 4(V-VIII) depicts recovered images after noise 50000, and Fig. 4(IX-XII) illustrates recovered images after noise 80000, and Fig. 4(XIII-XVI) depicts recovered image after noise 100000.

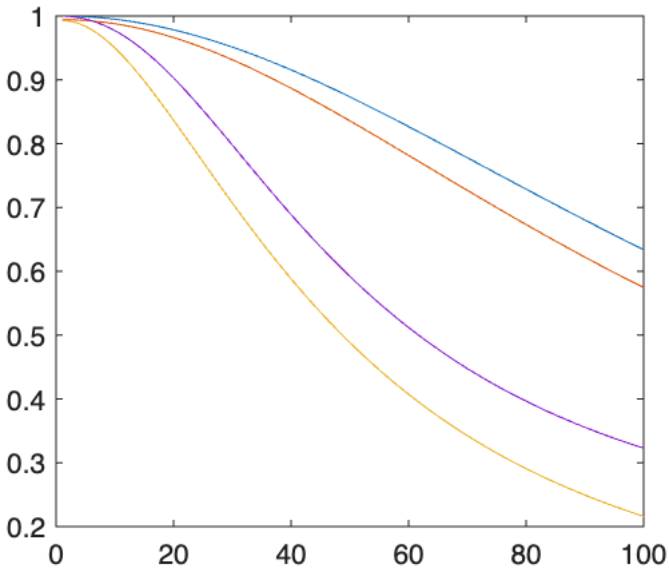


Fig 4.: Plot between CC and additive noise strength for four input images.

In practical communication environments, ciphertext data may undergo partial loss or corruption due to transmission noise, channel disturbances, or unexpected system failures. Therefore, a reliable cryptographic scheme should preserve plaintext recoverability even in the presence of incomplete ciphertext information. In cryptanalysis, such situations are commonly referred to as occlusion attacks. To evaluate the robustness of the proposed scheme against these attacks, controlled occlusion experiments were performed as part of the security analysis. The performance of the proposed scheme was investigated under three levels of ciphertext data loss, namely 20%, 50%, and 75%. The corresponding simulation results are presented in Fig. 5. Figure 5(I-a) be ciphertext and Fig.5(I-(b-e)) be recovered images after 20.3% dataloss, Figure 5(II-b) be ciphertext and Fig.5(II-(b-e)) be recovered images after 50% dataloss, Figure 5(III-a) be ciphertext and Fig.5(III-(b-e)) be recovered images after 75% dataloss. It can be observed that the proposed scheme successfully reconstructs recognizable plaintext images even when 75% of the ciphertext data is missing, thereby demonstrating strong resistance to occlusion attacks.

Image histograms provide a statistical description of the distribution of pixel intensities within an image by indicating the occurrence frequency of each gray level. In an 8-bit grayscale image, pixel intensities range from 0 to 255. In addition to histograms, three-dimensional (3D) mesh plots offer a visual representation of image characteristics, where the spatial coordinates are represented on the x and y axis, while the corresponding pixel intensity values are mapped onto the z axis. For a secure encryption system, the ciphertext should exhibit a nearly uniform histogram and a highly irregular 3D mesh structure, thereby concealing all perceptual information associated with the original image.Figures 6 and 7 present the histogram and 3D mesh plot analysis, respectively. Figure 6(I-IV) shows the histograms of the original plaintext images, whereas Fig. 6(V) illustrates the histograms corresponding to the encrypted image, and Fig. 6(VI-IX) shows the histograms of the recovered images. Similarly, Fig. 7(I-IV) depicts the 3D mesh plots of the plaintext images, Fig. 7(V) presents the mesh plots of the encrypted image, and Fig. 7(VI-IX) shows the mesh plots of the recovered images. It can be observed from Figs. 6 and 7 that significant differences exist between the plaintext and ciphertext representations in terms of both histogram distributions and 3D surface structures. The encrypted images exhibit uniform intensity distributions and randomized surface patterns, indicating that the statistical and structural information of the original images has been effectively concealed. These results confirm the strong resistance of the proposed cryptographic framework against statistical attacks.

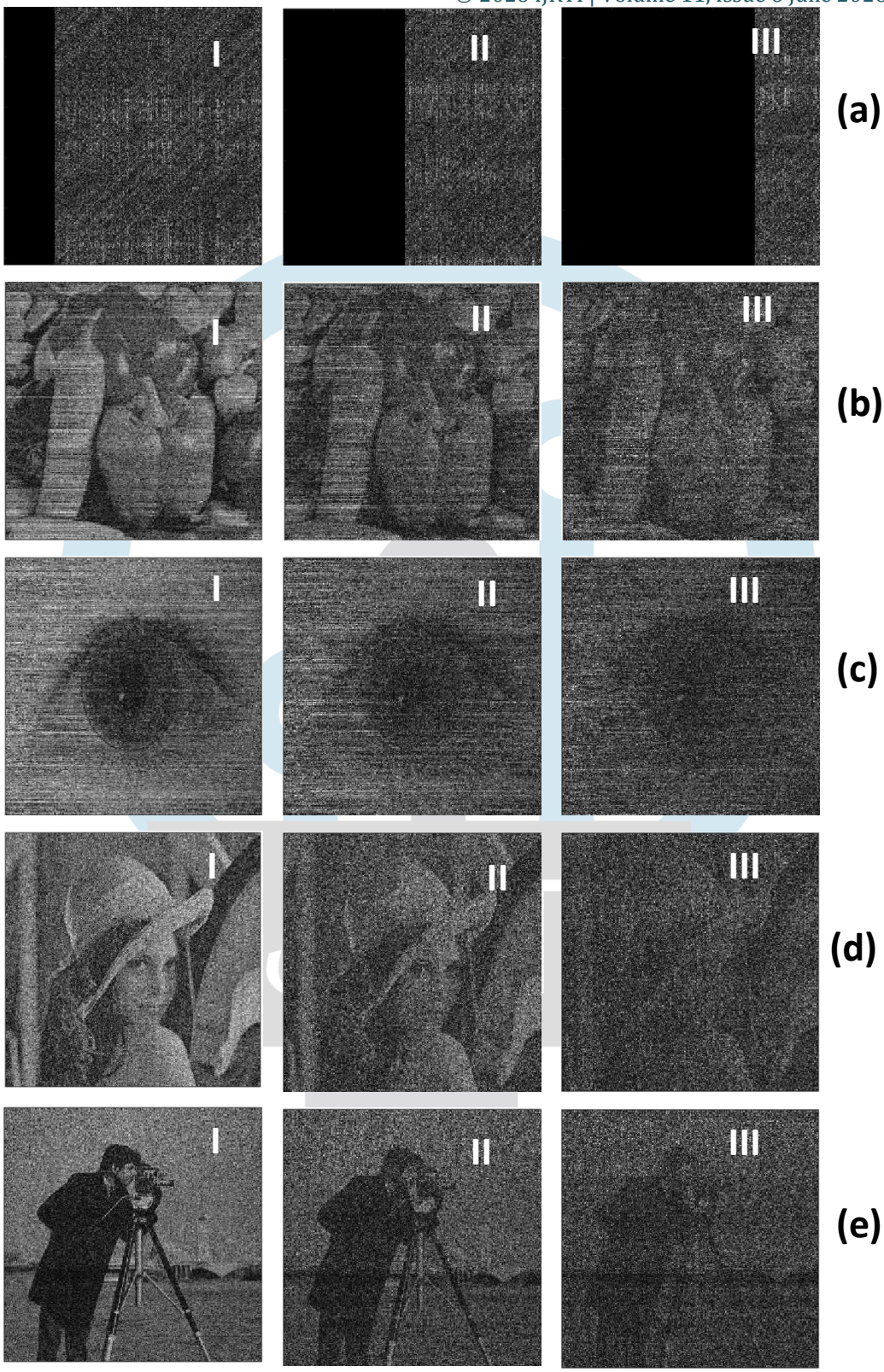


Fig.5.: Results of occlusion attack analysis. Figure 6(I-a) be ciphertext and Fig.6(I-(b-e)) be recovered images after 20.3% dataloss, Figure 6(II-b) be ciphertext and Fig.6(II-(b-e)) be recovered images after 50% dataloss, Figure 6(III-a) be ciphertext and Fig.6(III-(b-e)) be recovered images after 75% dataloss.

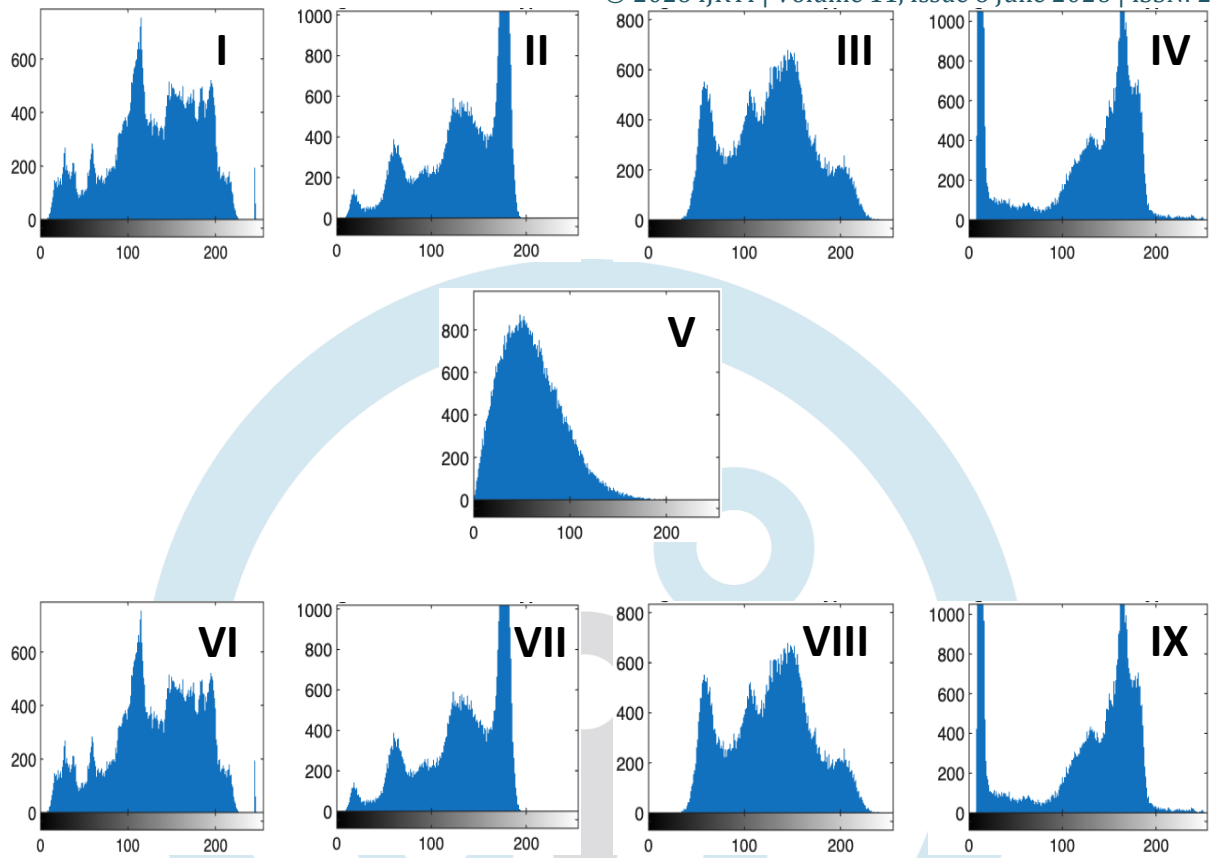


Fig. 6.: Histogram plots of the proposed algorithm. Figure 6(I-IV) shows the histograms of the original plaintext images, Fig. 6(V) illustrates the histograms corresponding to the encrypted image, and Fig. 6(VI-IX) shows the histograms of the recovered images.

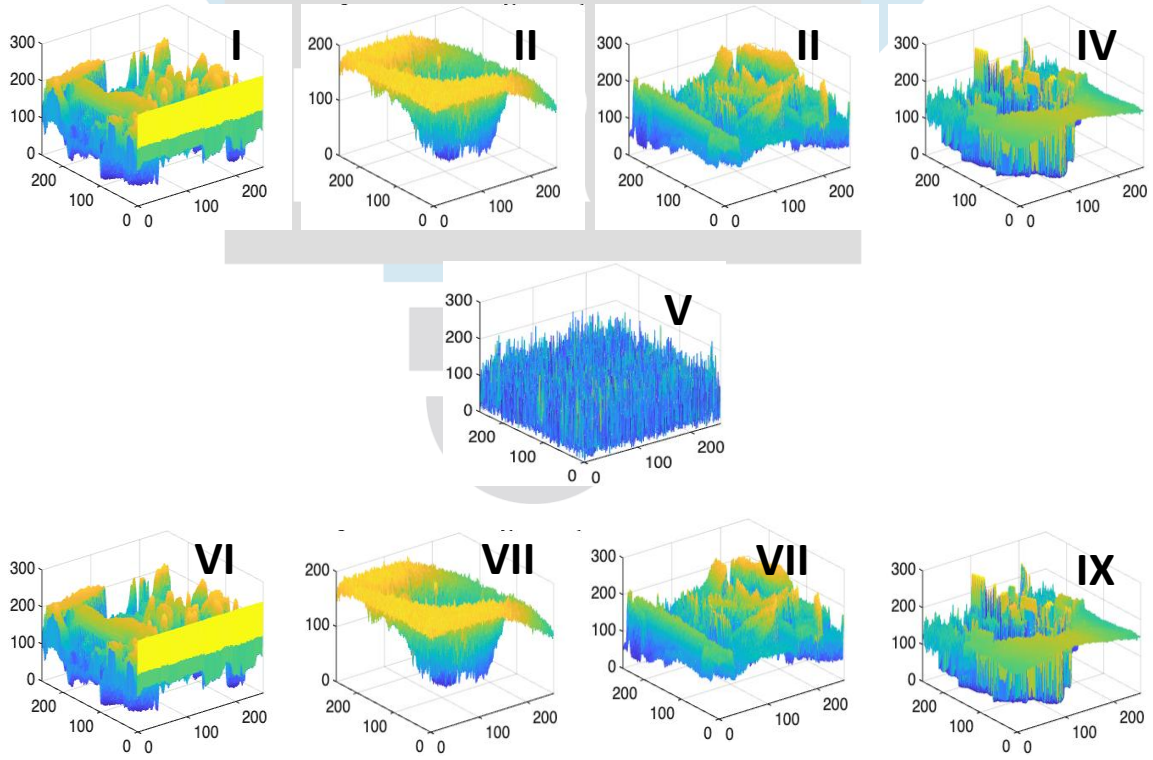


Fig.7: 3D plots of the proposed algorithm. Figure 7(I-IV) shows the 3D plots of the original plaintext images, Fig. 7(V) illustrates the 3D plots corresponding to the encrypted image, and Fig. 7(VI-IX) shows the 3D plots of the recovered images.

4. Conclusion

In this paper, a novel multi-image optical cryptosystem based on multiple random phase masks has been proposed for secure and high-capacity image encryption. The proposed scheme encrypts four grayscale images into a single ciphertext by integrating Fresnel-domain iterative phase retrieval, QZ decomposition, and Fourier transform. The use of wavelength multiplexing and multiple random phase masks increases the information capacity while introducing additional security parameters that enlarge the key space. Although the encryption process involves iterative computations, the decryption procedure remains simple and enables accurate recovery of all plaintext images using the corresponding wavelength keys. The performance of the proposed cryptosystem has been validated through extensive numerical simulations and security analyses. Experimental results demonstrate that the decrypted images exhibit high reconstruction quality, while the encrypted image possesses desirable statistical characteristics. Furthermore, the proposed scheme shows strong robustness against statistical, noise, occlusion, and brute-force attacks, with high sensitivity to the secret keys ensuring that even slight deviations prevent successful image reconstruction. These results confirm that the proposed cryptosystem provides a secure, efficient, and high-capacity solution for multi-image encryption. Future work may focus on extending the proposed framework to color images, hyperspectral images, and real-time optical encryption systems for next-generation multimedia communication and secure data transmission.

References

[1] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, vol. 20, pp. 767–769, 1995, doi: 10.1364/OL.20.000767.

[2] X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," *Optics Letters*, vol. 31, pp. 1044–1046, 2006, doi: 10.1364/OL.31.001044.

[3] 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.

[4] G. Li, W. Yang, D. Li, and G. Situ, "Ciphertext-only attack on the double random-phase encryption: Experimental demonstration," *Optics Express*, vol. 25, no. 8, pp. 8690–8697, Apr. 2017, doi: 10.1364/OE.25.008690.

[5] X. Peng, H. Wei, and P. Zhang, "Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain.," *Optics letters*, 2006, doi: 10.1364/OL.31.003261.

[6] A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," *Opt. Lett.*, vol. 30, no. 13, p. 1644, Jul. 2005, doi: 10.1364/OL.30.001644.

[7] W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," *Opt. Lett.*, vol. 35, no. 2, p. 118, Jan. 2010, doi: 10.1364/OL.35.000118.

[8] X. Wang and D. Zhao, "A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms," *Optics Communications*, vol. 285, no. 6, pp. 1078–1081, Mar. 2012, doi: 10.1016/j.optcom.2011.12.017.

[9] Y. Wang, C. Quan, and C. J. Tay, "New method of attack and security enhancement on an asymmetric cryptosystem based on equal modulus decomposition," *Appl. Opt.*, vol. 55, no. 4, p. 679, Feb. 2016, doi: 10.1364/AO.55.000679.

[10] X. Wang, Y. Chen, C. Dai, and D. Zhao, "Discussion and a new attack of the optical asymmetric cryptosystem based on phase-truncated Fourier transform," *Appl. Opt.*, vol. 53, no. 2, p. 208, Jan. 2014, doi: 10.1364/AO.53.000208.

[11] J. Kumar, P. Singh, and A. K. Yadav, "Asymmetric color image encryption using singular value decomposition and chaotic Tinkerbell map in fractional Fourier domain," in *Optics and Photonics for Information Processing XIV*, K. M. Iftekharuddin, A. A. S. Awwal, A. Márquez, and V. H. Diaz-Ramirez, Eds., Online Only, United States: SPIE, Aug. 2020, p. 10. doi: 10.1117/12.2568447.

[12] R. Kumar, B. Bhaduri, and N. K. Nishchal, "Nonlinear QR code based optical image encryption using spiral phase transform, equal modulus decomposition and singular value decomposition," *Journal of Optics*, vol. 20, no. 1, p. 015701, Jan. 2018, doi: 10.1088/2040-8986/aa9943.

[13] 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.

[14] 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.

[15] 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.

[16] H. Singh, K. S. Gaur, S. Thakran, and K. Singh, "An asymmetric phase image encryption technique using Arnold transform, singular value decomposition, Hessenberg decomposition, and fractional Hartley transform," *Appl. Phys. B*, vol. 130, no. 10, p. 186, Oct. 2024, doi: 10.1007/s00340-024-08312-y.

[17] J. Kumar, A. Yadav, P. Singh, and K. Kumar, "Phase image asymmetric encryption using Lorenz transform and modified equal modulus decomposition in fractional Fourier domain," *Solid State Technology*, vol. 63, no. 5, Art. no. 5, 2020.

[18] P. Singh, A. K. Yadav, K. Singh, and I. Saini, "Asymmetric watermarking scheme in fractional Hartley domain using modified equal modulus decomposition," *Journal of Optoelectronics and Advanced Materials*, vol. 21, no. 7–8, pp. 484–491, 2019.

[19] 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.

[20] 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.

[21] 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.

[22] Archana, Sachin, and P. Singh, "Cascaded unequal modulus decomposition in Fresnel domain based cryptosystem to enhance the image security," *Optics and Lasers in Engineering*, vol. 137, pp. 106399–106411, Feb. 2021, doi: 10.1016/j.optlaseng.2020.106399.

[23] 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.

[24] S. Sachin, R. Kumar, and P. Singh, "Unequal modulus decomposition and modified Gerchberg Saxton algorithm based asymmetric cryptosystem in Chirp-Z transform domain | SpringerLink." Accessed: Dec. 03, 2022. [Online]. Available: https://link.springer.com/article/10.1007/s11082-021-02908-w

[25] I. Saini and N. Sharma, "Asymmetric multi-image wavelength multiplexing cryptosystem using QZ algorithm and unequal modulus decomposition," *Optics & Laser Technology*, vol. 172, p. 110505, May 2024, doi: 10.1016/j.optlastec.2023.110505.

[26] R. Yadav, S. Sachin, Archana, P. Singh, and A. K. Yadav, "Image encryption algorithm for color images based on cascaded unequal modulus decomposition in Fourier domain," *Asian Journal of Physics*, vol. 30, no. 7, pp. 1071–1082, Jul. 2021.

[27] Sachin, R. Kumar, and P. Singh, "Multiuser optical image authentication platform based on sparse constraint and polar decomposition in Fresnel domain," *Phys. Scr.*, vol. 97, no. 11, pp. 115101–115116, Oct. 2022, doi: 10.1088/1402-4896/ac925d.

[28] S. P. Singh, G. Bhatnagar, and D. K. Gurjar, "A secure image encryption algorithm based on polar decomposition," in *2018 IEEE 14th International Colloquium on Signal Processing & Its Applications (CSPA)*, Batu Feringghi: IEEE, Mar. 2018, pp. 135–139. doi: 10.1109/CSPA.2018.8368700.

[29] H. Kumar, H. Singh, and V. K. Yadav, "Vortex array-based cryptosystem using Thue-Morse zone plate, SVD and QZ decomposition in the fractional Fourier transform domain," *Journal of Optics*, 2025, doi: 10.1007/S12596-025-02899-X.

[30] 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.

[31] H. Singh and P. Yadav, "An optical vortex-based asymmetric cryptosystem using QZ modulation for the double image encryption in the gyrator transform," *Iran J Comput Sci*, vol. 7, no. 4, pp. 829–842, Dec. 2024, doi: 10.1007/s42044-024-00196-7.

[32] 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.

[33] V. Yadav, H. Singh, and S. Thakran, "A dual-protection approach to enhance optical image encryption using QZ decomposition and generalized Reed–Muller codes," *J Opt*, May 2025, doi: 10.1007/s12596-025-02771-y.

[34] R. Yadav, Sachin, and P. Singh, "Asymmetric encryption-cum-authentication scheme using computational ghost imaging assisted by QZ algorithm in gyrator domain," *Optics Communications*, vol. 618, p. 133464, Nov. 2026, doi: 10.1016/j.optcom.2026.133464.

[35] E. Kumari, S. Mukherjee, P. Singh, and R. Kumar, "Asymmetric color image encryption and compression based on discrete cosine transform in Fresnel domain," *Results in Optics*, vol. 1, p. 100005, Nov. 2020, doi: 10.1016/j.rio.2020.100005.

[36] Shalu, A. K. Yadav, and P. Singh, "Nonlinear multiple color image encryption using Quasinormal-Zernike Algorithm in Fresnel transform domain," *J Opt*, Oct. 2025, doi: 10.1007/s12596-025-02940-z.

[37] H. Singh, "Double-phase image encryption using interference concept, Devil's fractional vortex Fresnel lens phase masks, and the gyrator transform," *Optik*, 2025, doi: 10.1016/J.IJLEO.2025.172289.

[38] H. Singh, "Cryptanalysis of a double-image symmetric optical cryptosystem utilizing devil's vortex Fresnel array and the linear canonical transform," *Journal of Modern Optics*, 2025, doi: 10.1080/09500340.2024.2448577.

[39] 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.

[40] H. Singh and P. L. Yadav, "An optical vortex-based asymmetric cryptosystem using QZ modulation for the double image encryption in the gyrator transform," *Iran Journal of Computer Science*, 2024, doi: 10.1007/S42044-024-00196-7.

[41] R. Yadav, Sachin, and P. Singh, "Multidomain asymmetric image encryption using phase-only CGH, QZS method and Umbrella map," *Journal of Optics*, 2024, doi: 10.1007/S12596-024-02106-3.

[42] S. Anjana, K. S. Gaur, H. Singh, P. Singh, and A. K. Yadav, "Security-enhanced optical nonlinear cryptosystem based on phase-truncated Fourier transform," *Opt Quant Electron*, vol. 55, no. 12, p. 1099, Nov. 2023, doi: 10.1007/s11082-023-05385-5.

[43] S. Anjana, I. Saini, P. Singh, and A. K. Yadav, "Asymmetric Cryptosystem Using Affine Transform in Fourier Domain," in *Advanced Computational and Communication Paradigms*, vol. 706, S. Bhattacharyya, N. Chaki, D. Konar, U. Kr. Chakraborty, and C. T. Singh, Eds., Singapore: Springer Singapore, 2018, pp. 29–37. Accessed: May 23, 2018. [Online]. Available: http://link.springer.com/10.1007/978-981-10-8237-5_4

[44] P. Singh, A. K. Yadav, P. Rakheja, K. Singh, and Sachin, "Asymmetric image encryption algorithm based on elliptic curve cryptography and phase- truncated Fourier transform," *Asian Journal of Physics*, vol. 30, no. 5, pp. 747–758.

[45] 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, pp. 1094–1107, 2021, doi: 10.1080/09500340.2021.1977404.

[46] 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.

[47] P. Singh, A. K. Yadav, and J. Kumar, "Asymmetric cryptosystem using double random-decomposition in fractional Fourier transform domain," in *Optics and Photonics for Information Processing XII*, San Diego, United States: SPIE, Sep. 2018, pp. 1075101–1075110. doi: 10.1117/12.2321973.