Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

An Efficient Phase Image Encryption Scheme Based on Hessenberg Decomposition and Henon Map in Fresnel-Domain

Nagander Singh Tomer[1], Deepak Yadav[2]

[1]Department of Mathematics, Guru Gorakhnath ji Govt. College, Hisar, Haryana, India
[2]Department of Mathematics, Central University of Haryana, Mahendergarh, India

Abstract:
With the rapid growth of digital communication, ensuring the secure transmission of image data has become increasingly important. This paper proposes an optical image encryption that combines phase encoding, Fresnel transform, Hessenberg decomposition and a chaotic Henon map to achieve enhanced security. By combining these techniques, the scheme effectively obscures the visual and statistical characteristics of the original image and generates a highly randomized ciphertext. The performance of the proposed cryptosystem has been validated through extensive simulation studies. Histogram, mesh-plot, and correlation analyses demonstrate that the encrypted images contain no recognizable information about the original images. Furthermore, the high values of CC, PSNR, and SSIM, together with the low MSE values, confirm the accurate reconstruction of the original image after decryption. The results obtained under noise and occlusion attacks indicate that the scheme possesses strong robustness against data corruption and partial information loss. Therefore, the proposed encryption method provides an effective and reliable framework for secure image transmission and storage in modern digital communication systems.

Keywords: Phase image, Fresnel transform, Hessenberg decomposition, Chaotic Henon map.

1. Introduction

The rapid growth of digital technologies has significantly increased the use of images for storing and sharing information. Digital images are now widely used in many fields such as banking, healthcare, remote sensing, defence and social media. As these images often contain confidential information, protecting them from unauthorised access during transmission and storage has become an important research challenge. Therefore, the development of reliable and secure image encryption techniques has gained considerable attention in recent time.

Optical image encryption has emerged as an important research area owing to its capability of providing high security and parallel processing. A major breakthrough in this field was achieved by Refregier and Javidi in 1995 with the introduction of the double random phase encoding technique (DRPE) [1]. In which Fourier transform and two random phase masks are used to obtained the encrypted image. Because of its simplicity and effectiveness, DRPE has become the foundation for many optical encryption methods. The success of DRPE encouraged researchers to extend it to several other transform in effort to improve

security and flexibility. Various optical transforms, including the Fractional Fourier transform [2], [3] Fresnel transform [4], [5],[6], [7], [8] Hartley transform [9], [10], Gyrator transform [11], [12], [13], [14],[15] fractional Hartley transform [16], [17], [18], Discrete Cosine transform [19] and fractional Hermite transform [20], [21], have been successfully incorporated into image encryption schemes. Among these the Fresnel transform has attracted significant attention because its propagation distance and wavelength provide additional security parameter, thereby, increase the available key space. Also, no lens is required in optical setup which reduce the complexity, cost and alignment requirements of the optical system, and enhances the feasibility of practical implementation.

Although DRPE and its variants offer satisfactory encryption performance, several studies have revealed that the DRPE is vulnerable to cryptographic attacks, including chosen-plaintext attack (CPA) [22], known-plaintext attack (KPA) [23], [24] and ciphertext-only attack (COA) [25]. These security limitations have motivated researchers to develop asymmetric optical encryption. As a result, in 2010 Qin and Peng [26] proposed an asymmetric optical encryption method based on phase truncation. Although, this method improved the security compared with conventional DRPE, subsequent investigations demonstrated that it remained susceptible to iterative reconstruction attacks. These findings indicate that developing optical image encryption scheme with improved security and robustness continue to be an active research challenge.

In recent years, phase encoding [27] has been widely employed in optical image encryption because it transforms the intensity information of an image into a complex phase representation. The encoded phase image preserves the image information while concealing its visual content, thereby improving the security of the encryption process. Furthermore, phase encoding can be efficiently integrated with optical transforms, random phase masks, and chaotic systems to increase encryption complexity and enhance resistance against various cryptographic attacks. Owing to these advantages, it has become an effective preprocessing stage in many modern optical encryption techniques.

Chaotic systems have also been extensively employed in image encryption systems, because of their inherent randomness and extreme sensitivity to initial conditions. These properties enable chaotic maps to generate pseudo-random sequences that are highly suitable for image permutation and diffusion. Thereby, improving the confusion and diffusion characteristic of encryption algorithm. A variety of chaotic map Henon map [28], Umbrella map [29], [30], Tinkerbell map [31], [32], logistic map [33] and Bird wing map [34] etc. have been successfully incorporated into optical and digital image encryption scheme to enhance their security. In addition to chaotic system, matrix decomposition techniques have been widely incorporated into optical encryption systems to further strengthen their security. Different decomposition approaches, such as equal modulus decomposition [35], [36], [37], singular value decomposition [38], [39], unequal modulus decomposition [40], [41], [42], [43], [44], random modulus decomposition [45], [46] and Hessenberg decomposition (HD) [47] have been employed in different transform domains. These techniques not only introduce additional secret keys into the encryption process but also increase the complexity of the cryptosystem, enlarge the key space and improve resistance against attacks.

From the above discussion, it is clear that although a wide range of optical image encryption techniques have been developed, there is still a demand for encryption schemes that provide higher security, improved computational efficiency and strong robustness against various cryptographic attacks. Motivated by these

challenges, this paper proposes a secure optical image encryption scheme based on Fresnel transform, Hessenberg decomposition and Henon map based chaotic pixel scrambling. In the proposed approach, phase encoding, random phase modulation, chaotic scrambling and matrix decomposition are jointly employed to enhance the confusion and diffusion properties of the cryptosystem. The effectiveness of the proposed scheme is verified through comprehensive security and performance analyses, including statistical analyses, reconstruction quality and robustness test under noise and occlusion attacks.

The remainder of this paper is organised as follows. Section 2, presents the theoretical background of the Fresnel transform, Henon map and Hessenberg Decomposition. Section 3 describe the proposed encryption and decryption procedures in details. Section 4 discuss the simulation results together with the security and performance analyses. Finally, section 5 concludes the paper, following the references.

2. Fundamental Concepts

This section briefly introduces the fundamental concepts employed in the proposed encryption method, namely the Fresnel transform, Hessenberg Decomposition and Henon map.

2.1 Fresnel Transform

The Fresnel transform is an important diffraction-based mathematical tool widely used in optical image processing. It describes the propagation of an optical wave from one plane to another over a certain distance. For an input image $V(x, y)$, the Fresnel transform at a propagation distance η and wavelength ϑ can be expressed as

$$V(u, v) = \mathrm{FrT}\{V(x, y)\} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} V(x, y)K_{\vartheta,\eta}(u, v, x, y)\mathrm{d}x\mathrm{d}y \qquad (1)$$

where $K_{\vartheta,\eta}(u, v, x, y)$ is the kernel of Fresnel transform and it is given by:

$$K_{\vartheta,\eta}(u, v, x, y) = \frac{1}{\sqrt{i\vartheta\eta}}\exp\left(i\frac{2\pi\eta}{\vartheta}\right)\exp\left(\frac{i\pi}{\vartheta\eta}(u - x)^2 + (v - y)^2\right) \qquad (2)$$

In these expressions, (x, y) represent the coordinates in the input plane, whereas (u, v) denote the coordinates in the observation plane after propagation. The parameters ϑ and η correspond to the wavelength of light and the propagation distance, respectively. Since the Fresnel transform depends on both parameters, they can serve as effective secret keys in optical image encryption systems.

2.2 Hessenberg Decomposition

Hessenberg Decomposition (HD) is a matrix factorization method that transforms a square matrix into a Hessenberg matrix through a similarity transformation involving a unitary matrix. This decomposition is widely used in numerical linear algebra because it simplifies matrix operations while preserving the eigenvalues of the original matrix. The decomposition of a square matrix A can be expressed as

$$A = PHP^* \qquad (3)$$

Here, A is any square matrix, P is unitary matrix i.e. $PP^* = P^*P = I$ and H is Hessenberg matrix i.e. H is a matrix in which all entries below the first sub-diagonal are zero.

2.3 Henon Map

The Henon map is a two-dimensional discrete chaotic system that exhibits sensitive dependence on initial conditions and control parameters. Because of its chaotic behavior and pseudo-random sequence generation capability, it is widely used in image encryption for permutation and diffusion operations. Which is mathematically defined as

$$x_{n+1} = 1 - ax_n^2 + y_n \quad (4)$$
$$y_{n+1} = bx_n \quad (5)$$

where, x_n and y_n represents the state variables at the nth iteration and a and b are control parameters. The map exhibits chaotic behaviour for certain parameter values, commonly $a = 1.4$ and $b = 0.3$.

3. Proposed scheme

This section describes the encryption and decryption procedures of the proposed optical image encryption scheme, which integrates Henon map and Hessenberg Decomposition (HD) within the Fresnel transform domain.

3.1 Encryption Process

The complete encryption process is discussed in detail below and its corresponding flowchart is presented in Fig. 1 for better understanding.

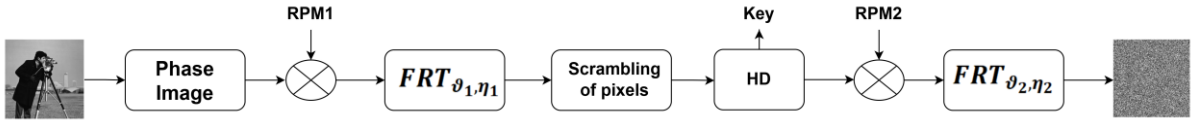


Figure 1 Schematic flow-chart of encryption process.

Step 1 First of all, an input image I' grayscale image is converted into phase image, which is mathematically defined as

$$I_1' = \exp(i2\pi I') \quad (6)$$

Step 2 The phase image I_1' is bonded with first random phase mask (RPM1), which is given by

$$I_2' = I_1' \times \text{RPM1} \quad (7)$$

Step 3 Obtained result in step 2 undergoes Fresnel transform with propagation distance η_1 and wavelength ϑ_1. The result is stored as I_3', which is mathematically written as:

$$I_3' = \text{FRT}_{\vartheta_1,\eta_1}(I_2') \quad (8)$$

Step 4 Henon map is applied on I_3', to scramble the pixels, after that Hessenberg decomposition is applied on the scrambled image, this process mathematically given by

$$[P, I_4'] = \text{HD (Scrambled } I_3' \text{)} \quad (9)$$

P is stored as private key and I_4' is further processed.

Step 5 I_4' is again bonded with second random phase mask (RPM2), which is mathematically given by equation 10.

$$I_5' = I_4' \times \text{RPM2} \quad (10)$$

Step 6 I_5' is propagated through Fresnel transform with propagation distance η_2 and wavelength ϑ_2.

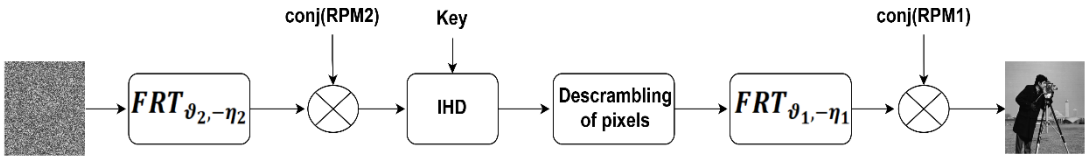
$$I_6' = \text{FRT}_{\vartheta_2,\eta_2}(I_5') \quad (11)$$

This I_6' is the obtained encrypted image.

3.2 Decryption Process

Decryption is the reverse process of encryption. The detailed decryption steps are described below and illustrated in Fig. 2.

Figure 2 Schematic flow-chart of decryption process.



Step 1 First of all, inverse of Fresnel transform is applied on the encrypted image I_6'
By taking negative propagation distance $(-\eta_2)$ and wavelength ϑ_2.The mathematical form of this step is given by equation 12.

$$DI_1 = FRT_{\vartheta_2,-\eta_2}(I_6') \quad (12)$$

Step 2 Second phase mask (RPM2) is removed by multiplying DI_1 by conjugate of RPM2,

$$DI_2 = DI_1 \times \text{conj}(\text{RPM2}) \quad (13)$$

Step 3 Inverse Hessenberg decomposition is applied on DI_2 by multiplying the private key (P) and its transpose, which is stored at the time of encryption.

$$DI_3 = PDI_2P' \quad (14)$$

Step 4 Now, the pixels are descrambled by using inverse Henon map, with the same parameters and initial conditions used for encryption. After descrambling of pixels again inverse Fresnel transform is applied with propagation distance $-\eta_1$ and wavelength ϑ_1.
This is mathematically expressed as

$$DI_4 = FRT_{\vartheta_1,-\eta_1}(\text{Descrambled } DI_3) \quad (15)$$

Step 5 DI_4 is multiplied by random phase mask one to remove its effect and we get the decrypted image by taking phase part and divide it by π. In mathematical form it can be expressed as

$$DI_5 = \frac{\text{angle}\left(DI_4 \times \text{conj}(\text{RPM1})\right)}{\pi} \quad (16)$$

DI_5 is our decrypted image.

4 Simulation Results

The proposed encryption scheme was simulated using MATLABR2024a on a computer equipped with an Intel Core i7 processor, 16GB RAM and the window 11 operating system. The simulation results obtained from the proposed method are presented and analyzed in detail in this section.'

4.1 Visual Assessment

To evaluate the security, robustness and computational efficiency of the proposed cryptosystem, extensive simulations were conducted using different grayscale images of different dimensions. For illustrative purpose, the results corresponding to Cameraman image of size 256×256 pixels, are presented in this section. The input image, its encrypted and decrypted images are shown in Fig. 3. A visual comparison reveals that the encrypted

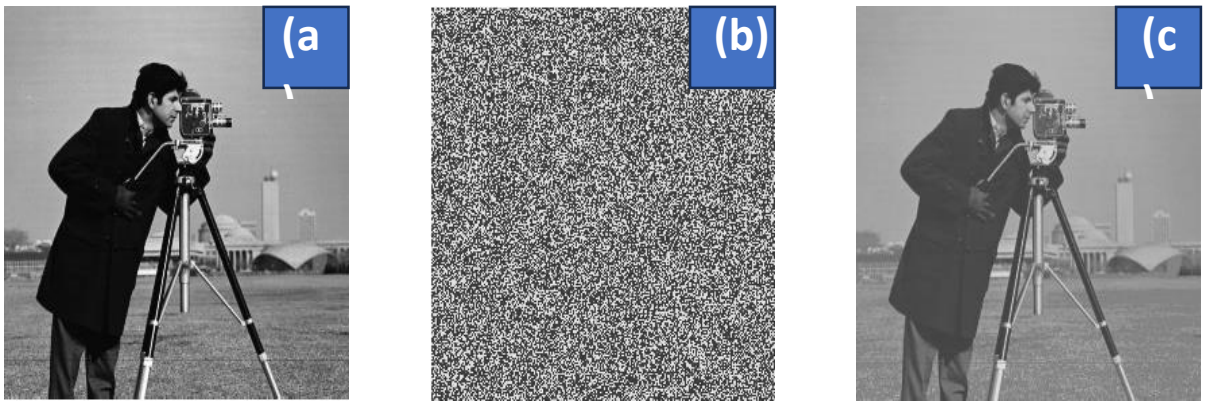


Figure 3 Visual results of (a) input image, (b) encrypted image and (c) decrypted image.

image exhibits a noise-like appearance with no visual structural information or recognizable pattern. In contrast the decrypted image closely matches the input image, indicating the effectiveness of the proposed algorithm. This demonstrates that the proposed algorithm successfully conceals the visual content of the input image, thereby preventing unauthorized access to sensitive information.

4.2 Correlation Coefficient

The Correlation Coefficient (CC) is an important statistical measure used to determine the degree of similarity between two images. mathematically the CC is calculated using the formula

$$\mathrm{CC} = \frac{\mathrm{cov}(\mathrm{I}', \mathrm{DI}_5)}{\sigma_{\mathrm{I}'}\, \sigma_{\mathrm{DI}_5}} \qquad (17)$$

where, I' denote input image and DI_5 denote decrypted image. The term $\mathrm{cov}(\mathrm{IP}, \mathrm{DI})$ represents the covariance between input and decrypted images, while $\sigma_{\mathrm{IP}}, \sigma_{\mathrm{DI}}$ correspond to the standard deviations of the input and decrypted images. A CC value close to unity indicating a high degree of similarity and a value close to zero indicates that the images are not correlated while if CC value is close to negative one implies strong negative correlation. In our proposed algorithm the CC value between input and decrypted images is 1, this implies the two images are highly correlated. Also, the CC values between input and encrypted images is 0.0031, close two zero, therefore the two images are not correlated.

4.3 Mean Squared Error

The mean squared error (MSE) is a widely used quantitative metric for evaluating the reconstruction accuracy of an image. It measures the average squared difference between the pixel intensities of the input and the decrypted images. The MSE is defined as

$$\mathrm{MSE} = \frac{1}{\mathrm{M} \times \mathrm{N}} \sum_{\mathrm{i}=0}^{\mathrm{M}-1} \sum_{\mathrm{j}=0}^{\mathrm{N}-1} [\mathrm{I}'(\mathrm{i},\mathrm{j}) - \mathrm{DI}_5(\mathrm{i},\mathrm{j})]^2 \qquad (18)$$

where, $\mathrm{I}'(\mathrm{i},\mathrm{j})$ and $\mathrm{DI}_5(\mathrm{i},\mathrm{j})$ denotes the pixel values at position (i,j) in the input and decrypted images respectively. While, M and N represent the dimensions of the image. A lower MSE value indicates a smaller reconstruction error and higher degree of similarity between the input and decrypted images. For our proposed algorithm the value of MSE is 1.5259×10^{-5}, which approaches zero. An MSE value approaching zero signifies near-perfect reconstruction, demonstrating the effectiveness of the proposed algorithm.

4.4 Peak Signal to Noise Ratio

The Peak Signal to Noise Ratio (PSNR) is a statistical metric that measures the similarity between an input image and its reconstructed image. It provides an indication of the fidelity of the recovered image by comparing the maximum possible pixel intensity with the reconstruction error. The PSNR is defined as

$$\mathrm{PSNR} = 10.\log_{10}\left(\frac{\mathrm{L}^2}{\mathrm{MSE}}\right) \qquad (19)$$

where, L represents the maximum allowable pixel value of the image and MSE denotes the mean squared error between the input and reconstructed images. For an 8-bit grayscale image, $\mathrm{L} = 255$. The PSNR value of our proposed algorithm is 70.5553. This high PSNR value corresponds to better reconstruction quality and indicates that the recovered image resemble the input image.

4.5 Structural Similarity Index Metric

The Structural Similarity Index Metric (SSIM) is an adopted metric for evaluating the visual quality of a reconstructed image by comparing it with the corresponding input image. Unlike error-based measures, SSIM assesses image quality by considering structural information, luminance and contrast. The SSIM value typically lies between -1 and 1, with values closer to 1 indicating a greater degree of similarity between the input and reconstructed image. The SSIM between the original image I' and the decrypted image DI_5 is given by

$$\mathrm{SSIM}(\mathrm{I},\mathrm{D}) = \frac{(2\mu_{\mathrm{I}'}\mu_{\mathrm{DI}_5} + \mathrm{A}_1)(2\mathrm{cov}(\mathrm{I}',\mathrm{DI}_5) + \mathrm{A}_2)}{(\mu_{\mathrm{I}'}^2 + \mu_{\mathrm{DI}_5}^2 + \mathrm{A}_1)(\sigma_{\mathrm{I}'}^2 + \sigma_{\mathrm{DI}_5}^2 + \mathrm{A}_2)} \qquad (20)$$

where, $\mu_{\mathrm{I}'}$ and μ_{DI_5} denote the mean intensity values of the input and decrypted images, respectively. The term $\mathrm{cov}(\mathrm{I}',\mathrm{DI}_5)$ represents the covariance between the two images, while $\sigma_{\mathrm{I}'}^2$ and $\sigma_{\mathrm{DI}_5}^2$ correspond to their variances. The constants A_1 and A_2 are small positive values introduced to maintain numerical stability and avoid division by zero issues when the denominator become very small. An SSIM value of 0.9999 is achieved by the proposed algorithm, indicating an almost perfect structural similarity between the input and decrypted images. this confirms that the proposed algorithm effectively preserves the structural characteristic of the input image during the encryption and decryption processes.

4.6 Histograms and Mesh-plots

The histogram analysis is used to evaluate the capability of the proposed algorithm to hide the statistical information of the input image. For a secure cryptosystem, the histogram of the encrypted image should be significantly different from that of the input image. As shown in Fig. 4, the histogram of the encrypted image differs significantly from that of the input image and exhibits a nearly uniform distribution, also the histogram of decrypted image is same as that of input image. This indicates that the statistical characteristics of the input image are effectively concealed, thereby providing strong resistance against statistical attacks.

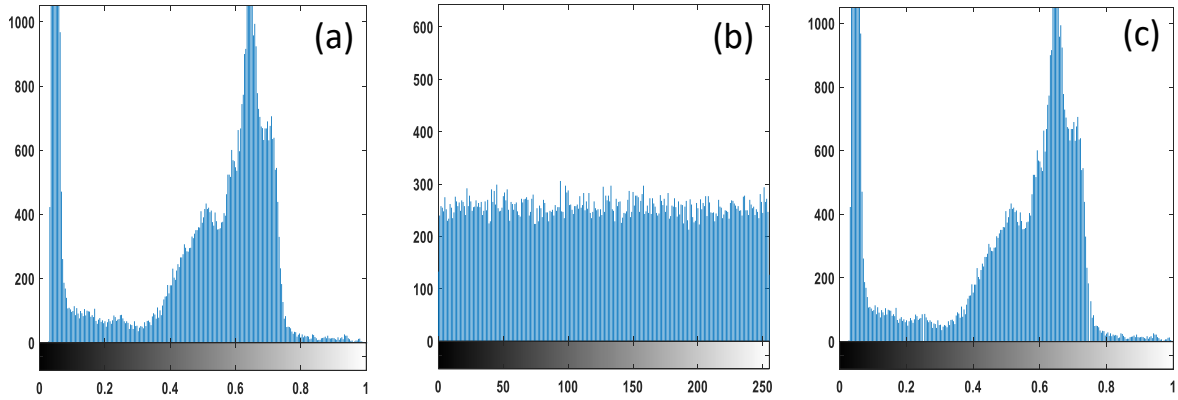


Figure 4 Histogram plots of (a) input image, (b) encrypted image and (c) decrypted image.

Mesh-plots provides a three-dimensional visualization of image intensity variations and are useful for assessing the randomness introduced by the encryption process. As shown in Fig. 5, the mesh plot of the input image exhibits a smooth and structured surface, indicating strong spatial relationships among neighbouring pixels. In contrast, the encrypted image produces an irregular and highly distorted mesh structure with no recognizable patterns. This significant transformation demonstrates that the proposed encryption scheme effectively disrupts the input image characteristics, thereby improving its resistance to statistical and structural attacks.

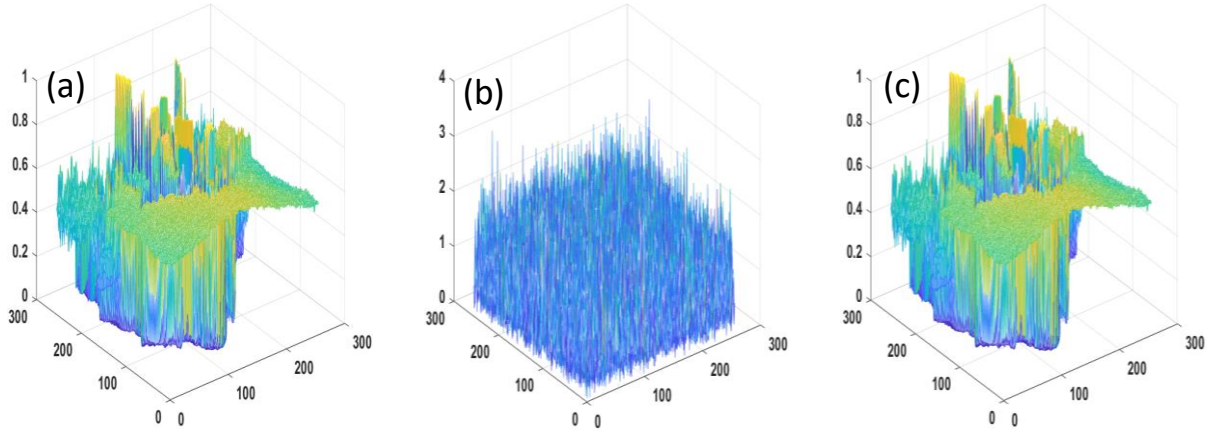


Figure 5 Mesh plots of (a) input image, (b) encrypted image and (c) decrypted image

4.7 Occlusion Attack Analysis

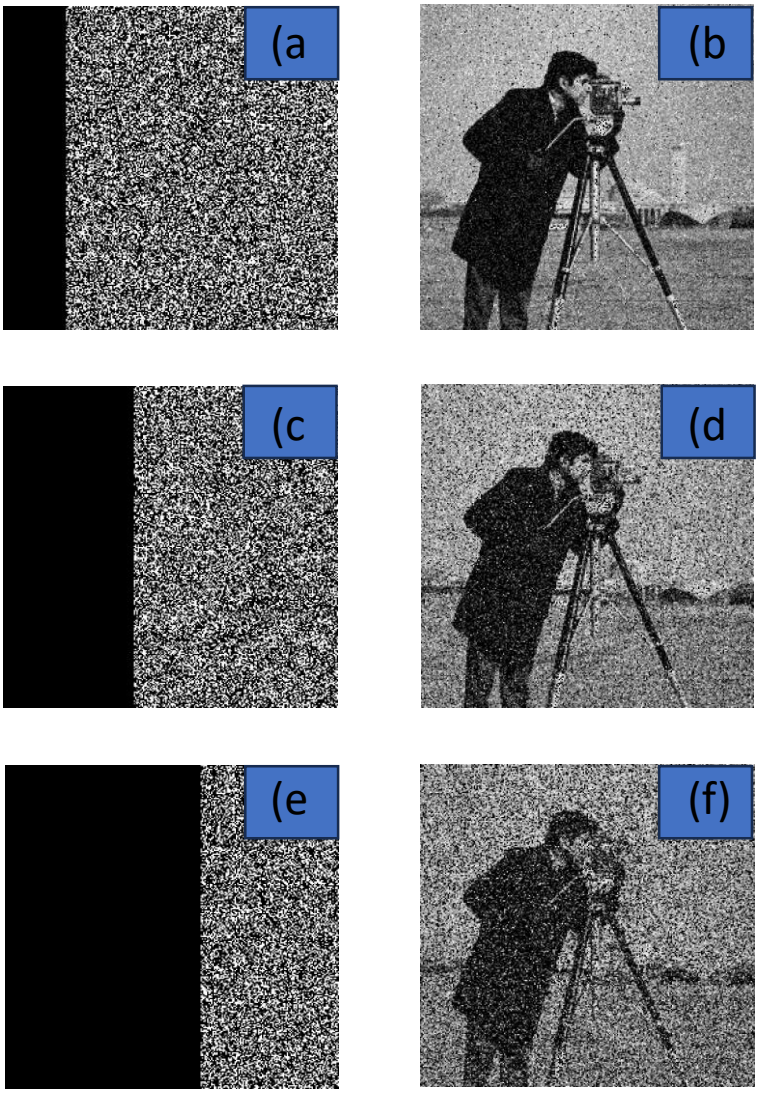


Figure 6 Effect of occlusion attack (a), (c) and (e) are occluded image with occlusion 19.53%, 39.06% and 58.59 % (b), (d) and (f) are their respective decrypted images

To examine the resilience of the proposed algorithm against data loss, occlusion attack is performed by intentionally removing 19.53%, 39.06% and 58.59% of the pixels from the encrypted image. The occluded encrypted images are shown in Fig. 6(a), Fig. 6(c) and Fig. 6(e), while the corresponding decrypted images are presented in Fig. 6(b), Fig. 6(d) and Fig. 6(f), respectively. Despite the loss of a considerable portion of the encrypted data, the decrypted images retain their essential visual information and remain easily identifiable. These results demonstrate the ability of the proposed algorithm to withstand occlusion attacks and successfully reconstruct meaningful image content even under adverse conditions.

4.8 Noise Attack Analysis

During transmission, encrypted image may be corrupted by channel noise, which can affect the quality of the decrypted image. Therefore, an effective encryption scheme should be capable of maintaining acceptable reconstruction performance even in the presence of noise. To evaluate the noise tolerance of

the proposed method, additive Gaussian noise with zero mean and unit variance is introduced into the ciphertext according to

$$\text{Noisy encrpted image} = \text{encrypted image} + \kappa \times \mathrm{N}(0,1) \qquad (21)$$

where, κ denotes the noise strength and $\mathrm{N}(0,1)$ represents a Gaussian random variable with zero mean and unit variance. The proposed scheme is tested under various noise levels. As strength reaches 1.5, demonstrating the strong robustness of the proposed algorithm against noise attack

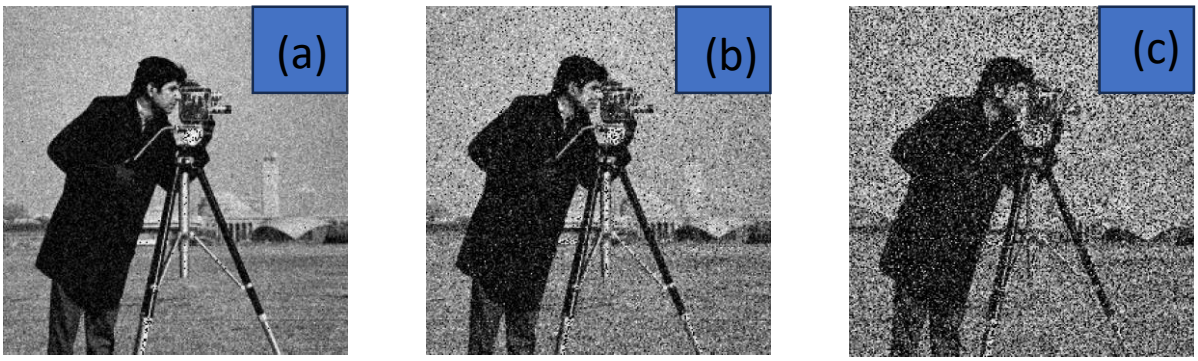


Figure 7 Decrypted images when additive Gaussian noise is added with strength (a) $\kappa = 0.5$, (b) $\kappa = 0.9$ and (c) $\kappa = 1.5$.

5 Conclusion

A secure optical phase-image encryption scheme combining Fresnel transform, pixel scrambling by chaotic Henon map and Hessenberg decomposition has been presented. The proposed method utilizes two random phase masks to increase the complexity of the encryption process. The incorporation of Hessenberg decomposition introduces asymmetry and an additional secret key through the generated unitary matrix, while chaotic Henon map effectively disrupts the spatial relationship among pixels, thereby enhancing the security of the encrypted image.

Extensive simulation results verify the effectiveness of the proposed cryptosystem. The encrypted images exhibit random noise-like characteristics and reveal no perceptible information about the original image. Statistical analyses demonstrate significant decorrelation and effective concealment of image features. Furthermore, the decrypted images show excellent reconstruction quality, as evidenced by high CC, PSNR, and SSIM values together with low MSE values. The scheme also maintains satisfactory performance under noise attack with noise strength 1.5 and occlusion attack when more than 50% of pixels are occluded, indicating strong robustness against channel impairments and partial data loss. Therefore, the proposed encryption framework offers a reliable and efficient solution for secure image transmission and storage in modern optical and digital communication systems.

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. N. K. Nishchal, J. Joseph, and K. Singh, “Fully phase encryption using fractional Fourier transform,” Optical Engineering, vol. 42, no. 6, pp. 1583–1588, Jun. 2003, doi: 10.1117/1.1570429.

3. S. Anjana, I. Saini, P. Singh, and A. K. Yadav, “Asymmetric enciphering of images using affine transform and fractional Fourier transform,” Int. J. Advanced Intelligence Paradigms, vol. 29, no. 1, pp. 28–45, Sep. 2024, doi: 10.1504/IJAIP.2024.141523.
4. S. K. Rajput and N. K. Nishchal, “Optical asymmetric cryptosystem based on photon counting and phase-truncated Fresnel transforms,” Journal of Modern Optics, vol. 64, no. 8, Art. no. 8, Apr. 2017, doi: 10.1080/09500340.2016.1265677.
5. Q. Wang, Q. Guo, L. Lei, and J. Zhou, “Multiple-image encryption based on interference principle and phase-only mask multiplexing in Fresnel transform domain,” Appl. Opt., AO, vol. 52, no. 28, pp. 6849–6857, Oct. 2013, doi: 10.1364/AO.52.006849.
6. 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.
7. Archana, S. Sachin, and P. Singh, “Cascaded unequal modulus decomposition in Fresnel domain-based cryptosystem to enhance the image security,” Optics and Lasers in Engineering, 2021, doi: 10.1016/J.OPTLASENG.2020.106399.
8. 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.
9. A. K. Yadav, P. Singh, I. Saini, and K. Singh, “Asymmetric encryption algorithm for colour images based on fractional Hartley transform,” Journal of Modern Optics, vol. 66, no. 6, pp. 629–642, Mar. 2019, doi: 10.1080/09500340.2018.1559951.
10. 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.
11. J. A. Rodrigo, T. Alieva, and M. L. Calvo, “Applications of gyrator transform for image processing,” Optics Communications, vol. 278, pp. 279–284, 2007, doi: 10.1016/j.optcom.2007.06.023.
12. A. Yadav, S. Vashisth, H. Singh, and Singh Kehar, “An asymmetric cryptography system for watermarking of phase-images using gyrator transform,” Asian Journal of Physics, vol. 24, no. 12, Art. no. 12, 2015.
13. R. Yadav, S. Sachin, and P. Singh, “Multiuser medical image encryption algorithm using phase-only CGH in the gyrator domain.,” Journal of The Optical Society of America A-optics Image Science and Vision, 2024, doi: 10.1364/JOSAA.507308.
14. A. Tobria and P. Singh, “A comparative analysis of phase retrieval algorithms in asymmetric double image cryptosystem in gyrator domain,” Optical and quantum electronics, 2023, doi: 10.1007/S11082-023-05524-Y.
15. 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.
16. A. K. Yadav, P. Singh, I. Saini, and K. Singh, “Asymmetric encryption algorithm for colour images based on fractional Hartley transform,” Journal of Modern Optics, vol. 66, pp. 629–642, 2019, doi: 10.1080/09500340.2018.1559951.

17. R. Yadav, Sachin, and P. Singh, “Watermarking algorithm based on phase-only CGH in fractional Hartley domain for DICOM images,” J. Opt., vol. 26, no. 6, p. 065703, May 2024, doi: 10.1088/2040-8986/ad3a77.
18. A. Yadav, P. Singh, and K. Singh, “Cryptosystem based on devil’s vortex Fresnel lens in the fractional Hartley domain,” Journal of Optics, vol. 47, no. 2, pp. 208–219, Nov. 2017, doi: 10.1007/s12596-017-0435-9.
19. 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.
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. 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.
26. 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.
27. 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.
28. 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, K. Ray, K. C. Roy, S. K. Toshniwal, H. Sharma, and A. Bandyopadhyay, Eds., in Lecture Notes in Networks and Systems. Singapore: Springer, 2021, pp. 73–84. doi: 10.1007/978-981-15-7561-7_5.
29. Sachin and P. Singh, “A novel chaotic Umbrella map and its application to image encryption,” Opt Quant Electron, vol. 54, no. 5, p. 266, May 2022, doi: 10.1007/s11082-022-03646-3.

30. 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.
31. 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.
32. 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.
33. K. Kapil and Sachin, “Cryptanalysis of cryptosystem based on phase mask generation using chaotic map and hash function,” Journal of Modern Optics, pp. 1–16, Jun. 2026, doi: 10.1080/09500340.2026.2677080.
34. Sachin and P. Singh, “Analysis of chaotic patterns in the Bird wing map and implications in image security,” Journal of Modern Optics, vol. 72, pp. 603–628, May 2025, doi: 10.1080/09500340.2025.2508790.
35. 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.
36. 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.
37. 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.
38. 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, 2017, doi: 10.1016/j.optlaseng.2016.11.022.
39. 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,” 2017, doi: 10.1063/1.4973267.
40. 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.
41. S. Sachin, R. Kumar, and P. Singh, “Unequal modulus decomposition and modified Gerchberg Saxton algorithm based asymmetric cryptosystem in Chirp-Z transform domain,” Opt Quant Electron, vol. 53, no. 5, pp. 254–274, May 2021, doi: 10.1007/s11082-021-02908-w.
42. 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.

43. 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.
44. 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.
45. 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.
46. 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.
47. R. Girija, K. S. Gaur, and H. Singh, “Hybrid image encryption based on Hessenberg decomposition and chaotic structured phase masks in Fresnel transform domain,” Multidim Syst Sign Process, vol. 37, no. 1, p. 3, Dec. 2026, doi: 10.1007/s11045-025-00902-z.