

# Secure Asymmetric Image Encryption Scheme using Elliptic Curves in Fourier Domain

Shalu

Department of Mathematics, Central University of Haryana, Mahendergarh-123031, India

## Abstract:

Phase truncated Fourier transform (PTFT), introduced in 2010, is a well-known optical asymmetric key cryptosystem. PTFT has been proven susceptible to some specific attacks utilizing phase retrieval algorithms. In this paper, a new approach based on elliptic curves is introduced to secure PTFT-based asymmetric scheme. In the proposed scheme, pixel scrambling is accomplished using an elliptic curve having three highly sensitive parameters. Validation of the scheme has been performed through simulations on MATLAB 2023b software for grayscale image. The scheme's robustness against statistical attacks is evaluated using histogram plots, mesh plot analysis, entropy and correlation coefficient distribution plots. Performance metrics such as peak signal-to-noise ratio, mean squared error and correlation coefficient are evaluated to assess quality of encryption as well as decryption. The scheme exhibits a high degree of resistance against the occlusion attack and noise attacks. The results show that the new approach offers strong security against specific attacks also.

**Keywords:** Phase truncated Fourier transform, image encryption, elliptic curve, specific attack, key sensitivity.

## 1. Introduction

The increased use of digital technology in recent years has sparked a growing focus on information security research. These efforts focus on enhancing existing techniques and developing innovative methods that are both effective and safe. Over the last decade, numerous techniques for ensuring secure communication and data transmission have been introduced [1]. Broadly, these approaches can be categorized into purely optical [3], [4], [5], [6], [7], [8], [9], [10], [11], purely digital [12], [13], [14], [15], [16] and hybrid [14], [15], [16], [17], [18], [19] techniques, each offering distinct advantages. The double random phase encoding (DRPE), the first optical cryptosystem, was developed by Refregier and Javidi [23] in 1995. However, DRPE is susceptible to fundamental cryptographic attacks, such as chosen-ciphertext attack [24], known-plaintext attack [25], and ciphertext-only attack [26]. These vulnerabilities arise because DRPE is a symmetric cryptosystem using the same keys for encryption and decryption. To address the issue of key distribution, several optical asymmetric cryptosystems have been developed. The first such asymmetric cryptosystem was introduced by Qin and Peng in 2010 [27]. This cryptosystem, named as phase-truncated Fourier transform, employs two distinct keys: a public key for encryption and a private key for decryption. While this scheme enhances security and is resilient against many cryptographic attacks, it remains vulnerable to certain specific attacks [28].

This paper presents a new encryption strategy that uses two random phase masks as encryption keys whereas the PTFT technique is used for obtaining the decryption keys. The proposed asymmetric

encryption system leverages elliptic curves to scramble the pixels of the image in frequency domain, adding few extra parameters to bolster security. This additional layer of complexity enhances the overall security level compared to previous asymmetric cryptosystems. For grayscale images, the effectiveness of the proposed algorithm has been proven. Notably, this algorithm has not been previously reported in the literature.

Section 2 provides an overview of the foundational principles of the phase-truncated Fourier transform, elliptic curve, and a specific attack method utilizing a modified amplitude-phase retrieval algorithm. The proposed image encryption scheme is detailed in Section 3. Simulation results and an analysis of the scheme's resistance to attacks are presented in Section 4, validating the robustness of the scheme. The paper concludes with a summary of findings and insights in the final section.

## 2. Preliminaries

### 2.1 Basic Concept of phase-truncated Fourier transform

In the basic traditional PTFT scheme given by Qin and Peng in 2010 [27]. The encryption of an input image  $I$  can be expressed as

$$E(x_1, x_2) = \text{abs}[FT[\text{abs}\{FT(I(x_1, x_2) \times RPM_1)\}] \times RPM_2$$

Here  $RPM_1 = \exp(2\pi i \times m(x_1, x_2))$ , where  $m(x_1, x_2)$  be a random matrix with values between 0 and 1} denotes the random phase mask in spatial domain and  $RPM_2 = \exp(2\pi i \times n(u_1, u_2))$  denotes the random phase mask in frequency domain,  $\times$  represents the pixelwise multiplication, and  $E(x_1, x_2)$  represents the encrypted image.  $(x_1, x_2)$  and  $(u_1, u_2)$  denote the coordinates in the spatial and frequency domains, respectively.  $FT$  denotes the Fourier transform and the Fourier transform [29] of a function  $g(x_1, x_2)$  is calculated as

$$G(u_1, u_2) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} g(x_1, x_2) e^{-2\pi i(u_1 x_1 + u_2 x_2)} dx_1 dx_2$$

The decryption procedure is formulated as

$$I(x_1, x_2) = \text{abs}[IFT[\text{abs}\{IFT(E(x_1, x_2) \times P_1)\}] \times P_2$$

where  $IFT$  represents inverse Fourier transform, and  $P_1$  and  $P_2$  are the private keys and mathematically expressed as

$$P_1 = PR\{FT(I(x_1, x_2) \times RPM_1)\},$$

$$P_2 = PR[FT[\text{abs}\{FT(I(x_1, x_2) \times RPM_1)\}] \times RPM_2]$$

where  $PR$  represents the phase reserved component.

The PTFT algorithm has been further developed and extended by numerous researchers across a variety of fields [30], [31], [32], [33], [34], [35], [36].

### 2.2 Elliptic Curves

Elliptic curves [37] satisfy a cubic equation of the form

$$x_2^2 = x_1^3 + \alpha x_1 + \beta \pmod{p}$$

where  $\alpha$  and  $\beta$  are constants,  $x_1$  and  $x_2$  are the variables representing the coordinates of points on the elliptic curve  $E$ , and  $p$  denotes the prime number. The constants  $\alpha$ ,  $\beta$  and  $p$  satisfy the following condition:

$$4\alpha^3 + 27\beta^2 \pmod{p} \neq 0$$

There are some basic operations on elliptic curves [38]

1. Point addition: Addition of two different points  $E = (e_1, e_2)$  and  $F = (m_1, m_2)$  on elliptic curve  $E$  is given by

$$E(e_1, e_2) + F(m_1, m_2) = G(n_1, n_2)$$

$$s_1 = \frac{m_2 - e_2}{m_1 - e_1} \pmod{p}$$

$$n_1 = s_1^2 - e_1 - m_1 \pmod{p}$$

$$n_2 = s_1(e_1 - n_1) - e_2 \pmod{p}$$

2. Point doubling: Adding a point  $X = (a_1, a_2)$  into itself on elliptic curve  $E$  is given by

$$X(a_1, a_2) + X(a_1, a_2) = Y(b_1, b_2)$$

$$s_2 = \frac{3a_1^2 + \alpha}{2a_2} \pmod{p}$$

$$b_1 = s_2^2 - 2a_1 \pmod{p}$$

$$b_2 = s_2(a_1 - b_1) - a_2 \pmod{p}$$

### 2.3 Specific Attack on PTFT

The specific attack [28] process relies on the principles underlying phase retrieval algorithms [39]. The conventional optical phase truncated Fourier transform technique is vulnerable to specific attack based on modified amplitude-phase retrieval algorithm.

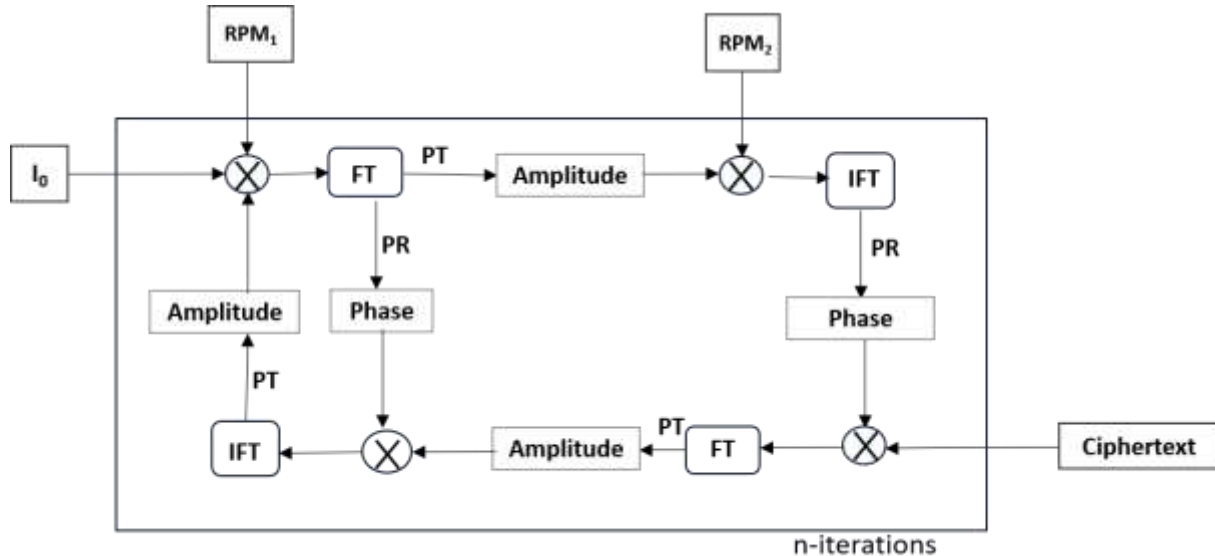


**Figure 1. Schematic diagram of specific attack algorithm based on modified amplitude-phase retrieval algorithm.**

Figure 1 shows the flowchart for the specific attack based on modified amplitude-phase retrieval algorithm. The attack procedure is described as

Step 1: A random input matrix ( $I_0$ ) is first multiplied by the first random phase mask ( $RPM_1$ ) and then transformed using the Fourier transform.

Step 2: The phase-retained component of the transformed output is extracted and stored as the key ( $Pk$ ). Subsequently, the phase-truncated component is multiplied by the second random phase mask ( $RPM_2$ ) and an inverse Fourier transform is applied on it.

Step 3: The phase-retained component obtained in Step 2 is combined with the ciphertext (the original image ciphertext to be retrieved) and transformed again using the Fourier transform.

Step 4: The amplitude component of the output bonded in Step 3 is combined with  $Pk$ , after which the inverse Fourier transform is applied.

Step 5: The amplitude component of the resulting output is considered as the input image  $I_0$ . The above procedure is iteratively repeated for  $n$  iterations.

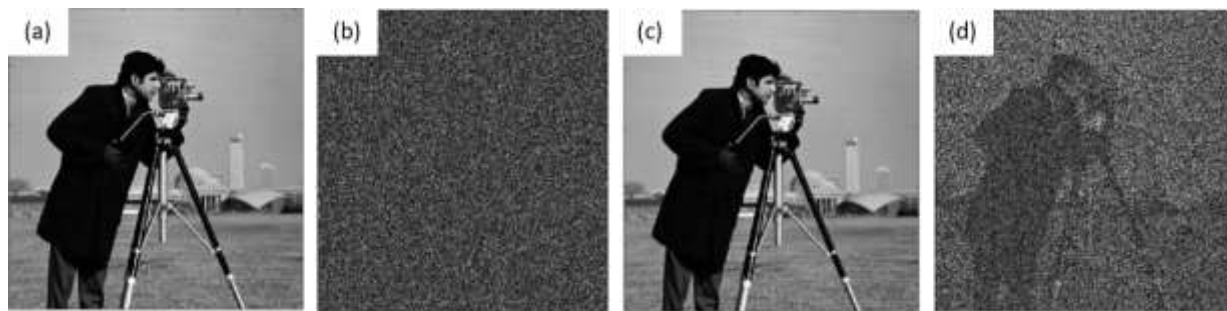


**Figure 2. (a) Input (b) encrypted (c) decrypted image by PTFT scheme (d) decrypted image by specific attack process.**

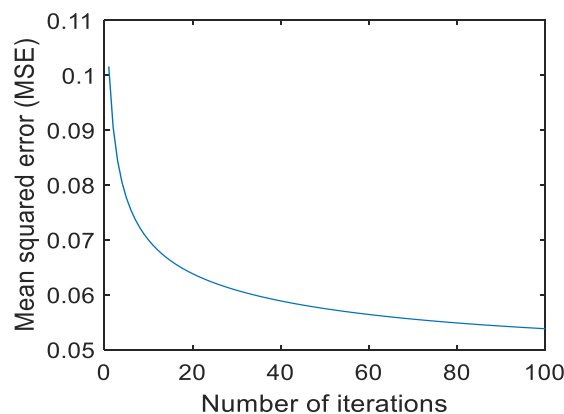


**Figure 3. Plot of mean squared error versus number of iterations.**

Figure 3 presents the variation of the mean squared error with respect to the number of iterations. It can be observed that the MSE decreases progressively as the iterations increase, eventually approaching zero. This reduction in MSE leads to a significant improvement in the quality of the reconstructed (attacked) image. The recovered image shown in Figure 2(d) demonstrates that the PTFT-based cryptosystem is vulnerable to specific attack process based on modified amplitude–phase retrieval algorithm. To secure the optical PTFT scheme, a novel encryption scheme based on elliptic curve is proposed, which is discussed in the next section.

### 3. Proposed Scheme

Steps for encryption process of proposed scheme

- Step 1: Initially, combine an input image  $f$  with first random phase mask ( $RPM_1$ ) in spatial domain.
- Step 2: Apply the Fourier transform to the resulting image. The phase retention part will be treated as the first private key ( $P_1$ ), while the truncated phase part will be used in the further encryption process.
- Step 3: Segment the resulting image into smaller blocks of dimensions  $m_l \times n_l$ , and convert each block into a column vector by sequentially concatenating its columns, producing a vector with a length of  $m_l n_l$ .
- Step 4: Generate a sequence of  $m_l n_l$  points using the elliptic curve properties.

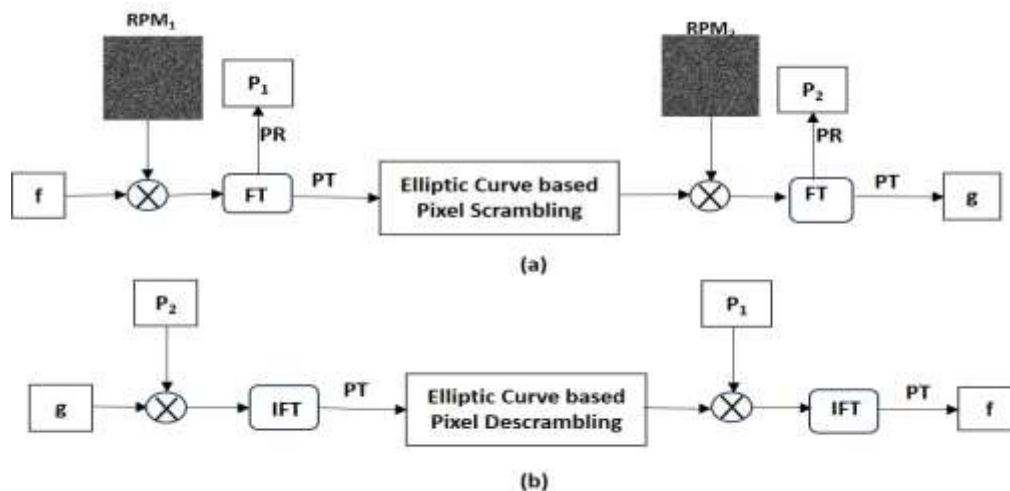


**Figure 4. Schematic diagram of (a) encryption and (b) decryption process of proposed scheme.**

- Step 5: Establish a one-to-one correspondence between the sequence produced in Step 3 and the column vector acquired in Step 4. Finally, arrange the  $m_l n_l$  elements into  $n_l$  columns sequentially, resulting in an  $m_l \times n_l$  matrix.
- Step 6: Repeat Step 4 and 5 for each block. After processing all blocks of the image, combine them to reconstruct the resulting image.
- Step 7: The image obtained by Step 6 is combined with second random phase mask ( $RPM_2$ ).
- Step 8: The resulting image is transformed through Fourier transform. The phase retention part will be treated as the second private key ( $P_2$ ), while the phase truncated part treated as encrypted image.
- The decryption procedure follows the same steps as the encryption procedure but in the reverse order as shown in Figure 4(b).

#### 4. Results and Discussion

The algorithm has been verified through simulations performed on MATLAB 2023b software using grayscale images. To validate the presented cryptosystem, we utilized the Cameraman image with size  $256 \times 256$  and set the elliptic curve parameters as  $\alpha = 5376$ ,  $\beta = 2438$ , and  $p = 123457$ .

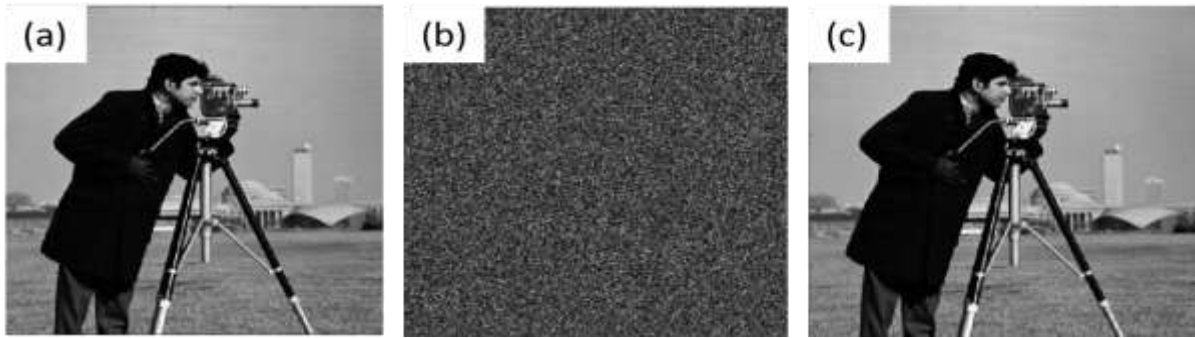


**Figure 5. The validation results include (a) input, (b) encrypted, and (c) the decrypted image obtained using the presented algorithm.**

Figure 5 represents the validation results of the presented algorithm. Figure 5(b) depicts the encrypted image of the Cameraman, which appears entirely different from the input image and resembles random white noise. Figure 5(c) presents the reconstructed image of the Cameraman, which closely resembles the original input image.

Different statistical metrics such as mean squared error (*MSE*), correlation coefficient (*CC*), and peak signal-to-noise ratio (*PSNR*), are calculated for grayscale Cameraman image.

The mathematical formula for *CC* is

$$CC = cov(I, D) / \sigma(I)\sigma(D)$$

where *cov* and  $\sigma$  represent respectively the covariance and the standard deviation between input image (*I*) and decrypted image (*D*).

Mathematically, *MSE* is given by

$$MSE = \frac{1}{256 \times 256} \sum_{x_1=0}^{256} \sum_{y_1=0}^{256} [I(x_1, y_1) - D(x_1, y_1)]^2$$

$I(x_1, y_1)$  and  $D(x_1, y_1)$  represent the pixel values of original input image and reconstructed image respectively.

The mathematical formula for *PSNR* is

$$PSNR = 10 \log_{10}(255^2 / MSE)$$

The computed values turn out to be  $CC = 1$ ,  $MSE = 3.8596 \times 10^{-27}$ ,  $PSNR = 312.26$  between input image and decrypted image. These values indicate that the proposed scheme successfully recovers the original image with high accuracy. The subsequent subsections will examine statistical attacks on the proposed scheme, focusing on histogram and 3D plot analysis, information entropy, and correlation distribution analysis.

## 4.1 Statistical Attack Analysis

A histogram in image encryption shows the distribution of pixel intensity values in an image. For grayscale images, it shows how many pixels have a particular intensity (0–255). A 3-D plot visualizes relationships between pixel intensities in the original image and encrypted image. The goodness of an

encryption scheme can be assessed using histogram and 3-D plot analysis. Figure 6(b) shows the

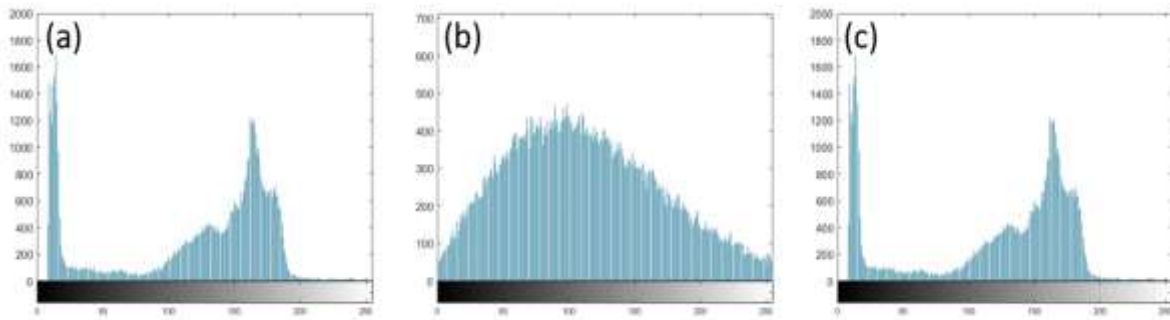


**Figure 6. Histograms of (a) an input image, (b) the encrypted image, and (c) the image that was decrypted from the proposed technique.**

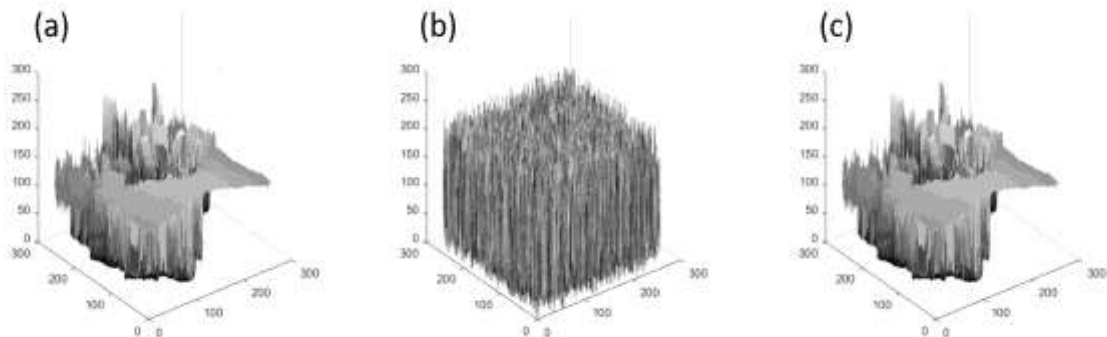


**Figure 7. Mesh plots of the presented algorithm (a) input (b) encrypted (c) decrypted image.**

histogram of encrypted image which is entirely different from the histogram plot of input image Figure 6(a). Histogram plot of encrypted image is uniform that hides the statistical properties. It demonstrates a high level of randomness with no visible patterns, ensuring resistance to statistical attacks. As shown in Figure 7 the mesh plot of encrypted image is entirely different from that of the original image. As shown in Figure 7(b), the 3-D plot of the encrypted image displays evenly distributed pixels. This distribution ensures that no patterns can be discerned. This analysis highlights the effectiveness of the encryption algorithm.

#### 4.2 Entropy

It measures the uncertainty, unpredictability, or randomness in a set of data. It is often used to quantify the amount of information contained in data or in system. Entropy values lie between 0 and 8 for grayscale (8-bit) image. Higher entropy is desirable as it implies greater unpredictability. Mathematical expression for entropy is given by

$$H(Y) = - \sum_{y \in Y} P(y) \log_2(y)$$

where  $P(y)$  denotes the probability of outcome  $y$  and  $Y$  represents the random variable.

The calculated entropy value of input Cameraman image is 7.0097. The entropy of the encrypted Cameraman image is 7.9959, which is nearly 8, signalling a strong level of randomness in the encrypted image.

### 4.3 Correlation Distribution Analysis

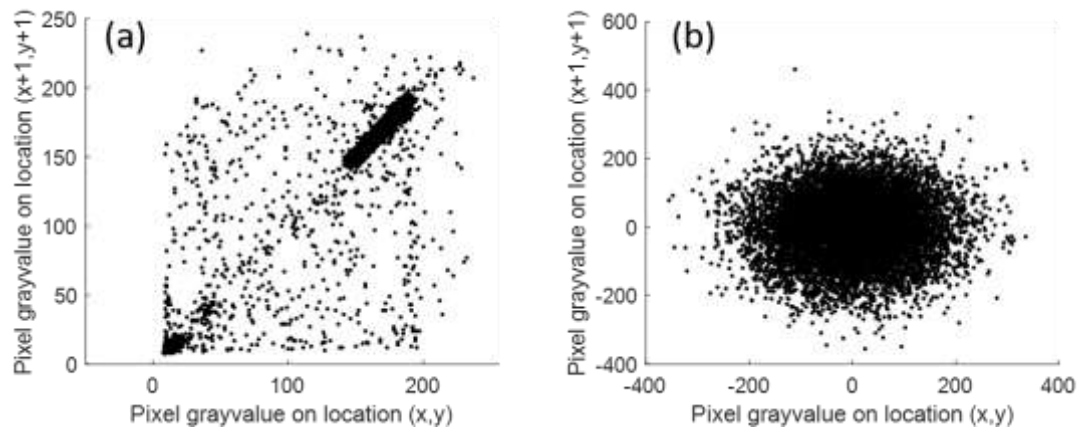


**Figure 8. Correlation Distribution plots of (a) input (b) encrypted image of presented algorithm.**

Correlation Distribution Analysis is a method used to study the relationship between variables by examining the distribution of their correlation coefficients. The effectiveness of an encryption algorithm can be demonstrated by correlation distribution analysis of nearby pixels in input and encrypted images. In this analysis 10,000 diagonal pixels from the input image are selected randomly. Figure 8(a) and 8(b) represent the correlation distribution plots of input and decrypted Cameraman image. The pixels in the input image exhibit a strong correlation with one another. The pixels in the encrypted image are scattered, random, and exhibit no correlation with one another. This demonstrates the efficacy of the encryption method.

### 4.4 Occlusion Attack Analysis

In real-world scenarios, encrypted images may be exposed to occlusion attacks during transmission. Certain parts of the encrypted data are lost or deliberately removed. Occlusion attack analysis is essential to evaluate the robustness of image encryption algorithms under such conditions.

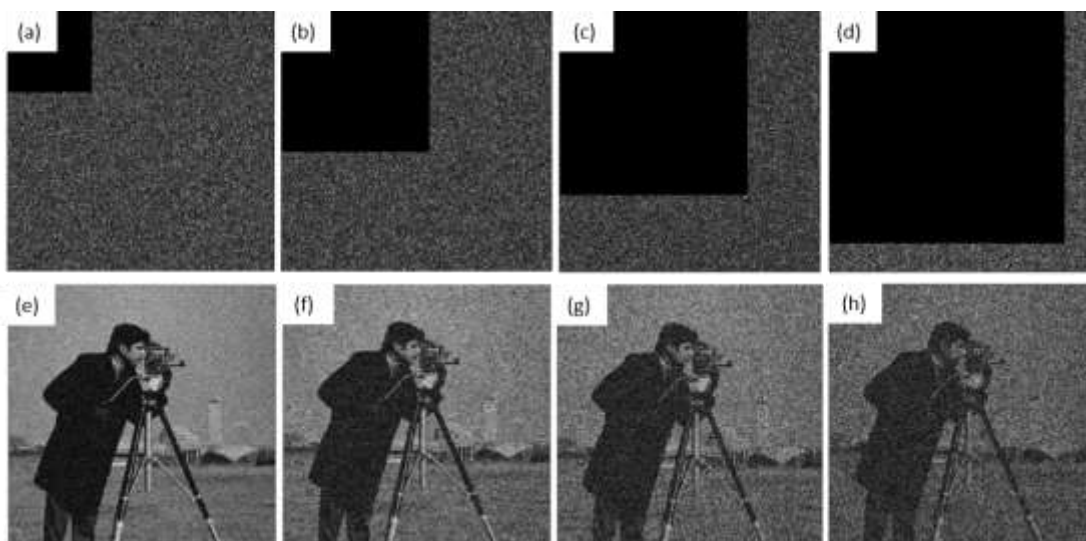


**Figure 9. Diagram showing (a)-(d) occluded encrypted images with 10%, 30%, 50%, and 80% data occlusion, while (e)-(f) corresponding decrypted images using the proposed scheme.**

Figure 9 illustrates the results of the occlusion attack. Figure 9(a-d) presents the encrypted images with 10%, 30%, 50%, and 80% data occlusion, while Figure 9(e-h) shows the corresponding decrypted

images. The original image remains visible even with up to 80% occlusion in the encrypted image. Figure 10 presents a plot of the correlation coefficient (CC) values for different percentages of occluded areas.

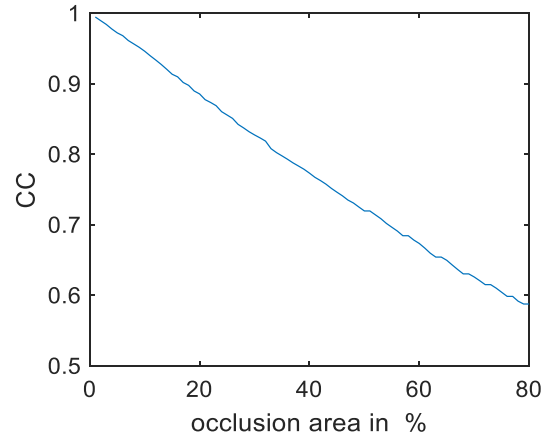


**Figure 10. Plot of CC versus occluded area percentage.**

#### 4.5 Noise Attack Analysis

When data is transmitted over the public network, it is often subject to disturbances such as signal loss, degradation, or unwanted interference. Salt-and-pepper noise is a type of impulsive noise and a most common form of interference. Salt represents white pixels, while pepper represents the black pixels. This type of noise can severely affect data corruption, especially when it is added to encrypted data.

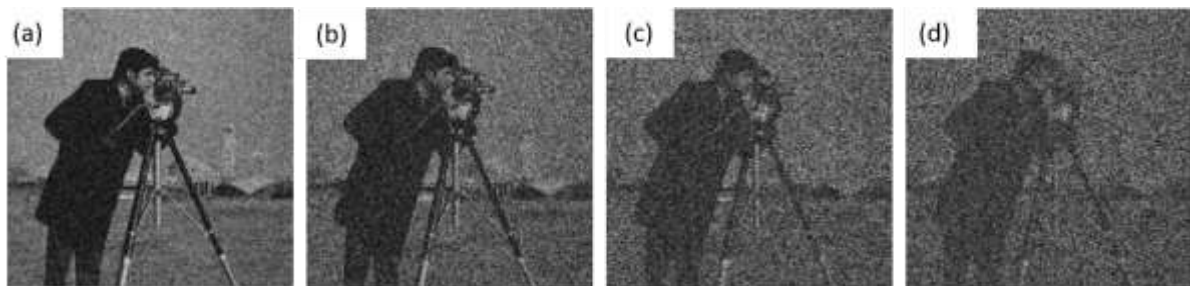


**Figure 11. Decrypted image of the Cameraman with salt and pepper noise at different densities (a) 0.02, (b) 0.2, (c) 0.5, and (d) 0.75, using the proposed scheme.**

Figure 11 presents the outcomes when varying densities of salt and pepper noise are added to the encrypted image. As shown in Figure 12, when the noise density increases, the quality of the decrypted image decreases. The decrypted image remains visible even at a salt and pepper noise density of 0.75.

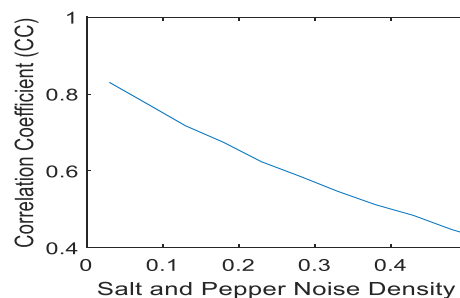


**Figure 12. Plot of CC versus salt and pepper noise density.**

## 4.6 Key Sensitivity Analysis

To assess the robustness of the secret key in the proposed method, the sensitivity of the elliptic curve parameters is analysed. Figure 13 shows the results of the key sensitivity analysis. Figure 13(b) depicts a decrypted image with the wrong parameter value of  $\alpha = 5375$  rather than the correct  $\alpha = 5376$ . Figure 13(c) depicts the decrypted picture with the wrong parameter value of  $\beta = 2437$  rather than the correct  $\beta = 2438$ . Figure 13(d) shows the decrypted image with an incorrect parameter value of  $p = 123458$  instead of the correct  $p = 123457$ . It ensures that even slight modifications to the elliptic curve parameters produce entirely different or invalid outputs, demonstrating the system's strength against brute-force attempts or the use of incorrect keys.

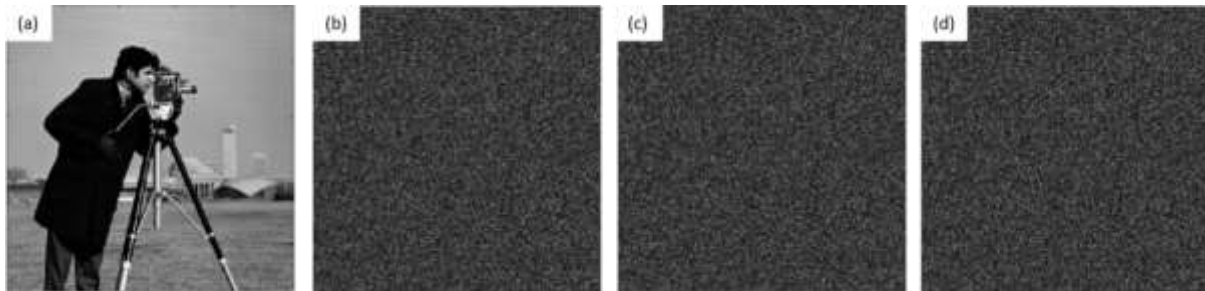


**Figure 13. (a) Input image (b) decryption with incorrect value of parameter  $\alpha$  (c) decryption with incorrect value of parameter  $\beta$  (d) decryption with incorrect value of parameter  $p$ .**

## 4.7 Specific Attack

As discussed in Section 2, the PTFT method is susceptible to a specific attack utilizing modified amplitude-phase retrieval algorithm. To address this vulnerability, we propose a new scheme. In this section, we demonstrate that the presented algorithm is resilient against this specific attack.

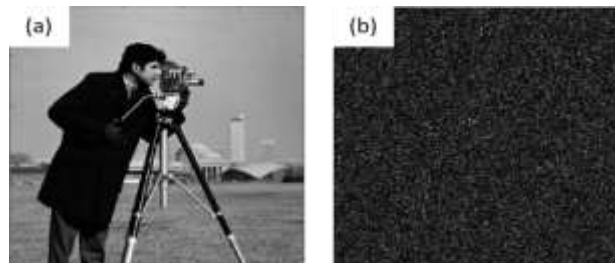


**Figure 14. (a) Input image (b) recovered image by applying specific attack on proposed scheme.**

As shown in Figure 14, the attacker is unable to retrieve any knowledge about the input image using the specific attack on the presented scheme. Figure 15(a) illustrates the plots of the CC values between the input image and the decrypted image when the proposed scheme is subjected to specific attack. In the figure, the CC values range between -0.01 and -0.002, indicating a poor correlation. This demonstrates that there is no meaningful correlation between the input Cameraman image and the recovered Cameraman image obtained through the attack process. Figure 15(b) illustrates the MSE value plots between the input image and the decrypted image when the proposed scheme is subjected to specific attack.

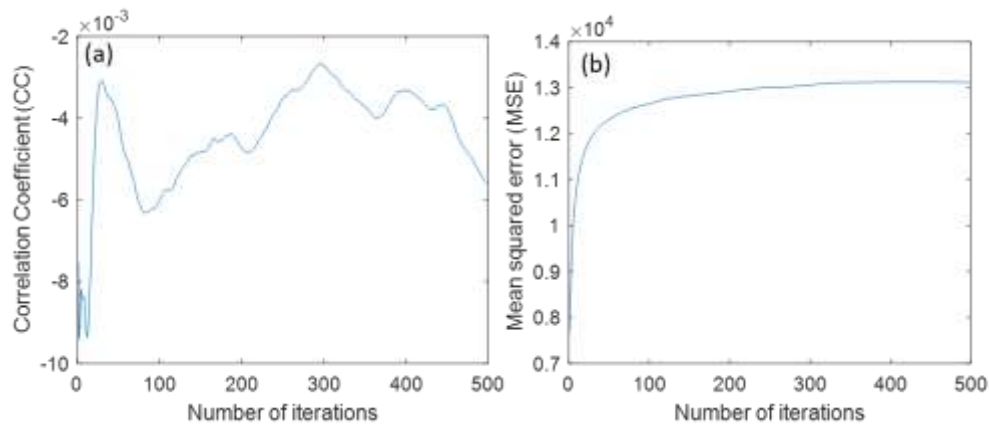


**Figure 15. Plots of (a) CC and (b) MSE values between the input image and the decrypted image under specific attack on the proposed scheme.**

The graph line representing the MSE values gradually increases as the number of iterations increase. This indicates that the MSE between the input and recovered images is significantly high. This analysis confirms that the presented method is resilient to the specific attack.

## 5. Conclusion

In conclusion, a novel asymmetric approach is presented in which we used optical asymmetric PTFT scheme along with elliptic curves. Elliptic curves are utilized for pixel scrambling in Fourier domain. The presented algorithm is validated using a grayscale Cameraman image. Its efficacy and performance are further demonstrated using statistical attacks, including histogram analysis and 3-D plots. In the simulation results, we successfully reconstructed the input image with  $PSNR = 312.26$ ,  $MSE = 3.8596 \times 10^{-27}$  and  $CC = 1$ . We have demonstrated that the algorithm is strongly sensitive to the parameters of elliptic curve ( $\alpha, \beta$  and  $p$ ). Even a slight change in these parameter values leads to the failure to reconstruct the original image. The scheme is resilient against salt-and-pepper noise and occlusion attacks. Furthermore, the proposed method demonstrates robustness against specific attack, ensuring enhanced security. The findings show that the suggested method ensures enhanced security and greater resilience

## References

1. "Optical Cryptosystems - Book - IOPscience." Accessed: May 14, 2025. [Online]. Available: <https://iopscience.iop.org/book/mono/978-0-7503-2220-1>
2. A. K. Sivarajan, H. Vardhan, S. Choudhary, S. G. Reddy, and R. Kumar, "Asymmetric optical cryptosystem using C-point polarization singularity speckles and polar decomposition in 2D-NS-LCT domain," *Phys. Scr.*, vol. 100, no. 5, p. 055504, 2025.
3. W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," *Adv. Opt. Photon., AOP*, vol. 6, no. 2, pp. 120–155, Jun. 2014, doi: 10.1364/AOP.6.000120.
4. A. M. Elshamy *et al.*, "Optical Image Encryption Based on Chaotic Baker Map and Double Random Phase Encoding," *J. Lightwave Technol., JLT*, vol. 31, no. 15, pp. 2533–2539, Aug. 2013.
5. P. Singh, A. K. Yadav, K. Singh, and I. Saini, "Asymmetric watermarking scheme in fractional Hartley domain using modified equal modulus decomposition," *J. Optoelectron. Adv. Mater.*, vol. 21, no. 7–8, pp. 848–491, 2019.

6. 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.
7. 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, p. 020017, Jan. 2017, doi: 10.1063/1.4973267.
8. G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," *Opt. Lett., OL*, vol. 29, no. 14, pp. 1584–1586, Jul. 2004, doi: 10.1364/OL.29.001584.
9. G. Unnikrishnan and K. Singh, "Double random fractional Fourier domain encoding for optical security," *OE*, vol. 39, no. 11, pp. 2853–2859, Nov. 2000, doi: 10.1117/1.1313498.
10. S. K. Rao, R. Kumar, N. K. Nishchal, and A. Alfalou, "Optical image encryption using modified GS algorithm and DNA encoding," in *Frontiers in Optics*, Optica Publishing Group, 2024, pp. JT4A-51. Accessed: May 14, 2025. [Online]. Available: <https://opg.optica.org/abstract.cfm?uri=FiO-2024-51>.
11. S. K. Rao, R. Kumar, N. K. Nishchal, and A. Alfalou, "Optical asymmetric image encryption using DNA through vortex beam encoding," *Discov Appl Sci*, vol. 6, no. 11, p. 591, Nov. 2024, doi: 10.1007/s42452-024-06215-3.
12. G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 08, pp. 2129–2151, Aug. 2006, doi: 10.1142/S0218127406015970.
13. A. Anees, "An Image Encryption Scheme Based on Lorenz System for Low Profile Applications," *3D Res*, vol. 6, no. 3, p. 24, Jul. 2015, doi: 10.1007/s13319-015-0059-2.
14. T. Gao and Z. Chen, "Image encryption based on a new total shuffling algorithm," *Chaos, Solitons & Fractals*, vol. 38, no. 1, pp. 213–220, Oct. 2008, doi: 10.1016/j.chaos.2006.11.009.
15. G. Hanchinamani and L. Kulakarni, "A Novel Approach for Image Encryption based on Parametric Mixing Chaotic System," *International Journal of Computer Applications*, vol. 96, no. 11, pp. 29–37, Jun. 2014.
16. A. Zhu and L. Li, "Improving for chaotic image encryption algorithm based on logistic map," in *2010 The 2nd Conference on Environmental Science and Information Application Technology*, Jul. 2010, pp. 211–214. doi: 10.1109/ESIAT.2010.5568374.
17. O. S. Faragallah and A. Afifi, "Optical color image cryptosystem using chaotic baker mapping based-double random phase encoding," *Opt Quant Electron*, vol. 49, no. 3, p. 89, Feb. 2017, doi: 10.1007/s11082-017-0909-7.
18. P. Rakheja, R. Vig, and P. Singh, "Optical asymmetric watermarking using 4D hyperchaotic system and modified equal modulus decomposition in hybrid multi resolution wavelet domain," *Optik*, vol. 176, pp. 425–437, Jan. 2019, doi: 10.1016/j.ijleo.2018.09.088.
19. 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.
20. P. Rakheja, R. Vig, and P. Singh, "An asymmetric hybrid cryptosystem using hyperchaotic system and random decomposition in hybrid multi resolution wavelet domain," *Multimed Tools Appl*, vol. 78, no. 15, pp. 20809–20834, Aug. 2019, doi: 10.1007/s11042-019-7406-x.
21. P. Rakheja, R. Vig, and P. Singh, "A hybrid multiresolution wavelet transform based encryption scheme," *AIP Conference Proceedings*, vol. 2061, no. 1, p. 020008, Jan. 2019, doi: 10.1063/1.5086630.

22. P. Rakheja, R. Vig, P. Singh, and R. Kumar, "An iris biometric protection scheme using 4D hyperchaotic system and modified equal modulus decomposition in hybrid multi resolution wavelet domain," *Opt Quant Electron*, vol. 51, no. 6, p. 204, Jun. 2019, doi: 10.1007/s11082-019-1921-x.
23. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett., OL*, vol. 20, no. 7, pp. 767–769, Apr. 1995, doi: 10.1364/OL.20.000767.
24. 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., OL*, vol. 30, no. 13, pp. 1644–1646, Jul. 2005, doi: 10.1364/OL.30.001644.
25. X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," *Opt. Lett., OL*, vol. 31, no. 8, pp. 1044–1046, Apr. 2006, doi: 10.1364/OL.31.001044.
26. X. Liu, J. Wu, W. He, M. Liao, C. Zhang, and X. Peng, "Vulnerability to ciphertext-only attack of optical encryption scheme based on double random phase encoding," *Opt. Express, OE*, vol. 23, no. 15, pp. 18955–18968, Jul. 2015, doi: 10.1364/OE.23.018955.
27. W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," *Opt. Lett., OL*, vol. 35, no. 2, pp. 118–120, Jan. 2010, doi: 10.1364/OL.35.000118.
28. 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., AO*, vol. 53, no. 2, pp. 208–213, Jan. 2014, doi: 10.1364/AO.53.000208.
29. R. N. Bracewell, "The Fourier Transform," *Scientific American*. Accessed: Dec. 16, 2024. [Online]. Available: <https://www.scientificamerican.com/article/the-fourier-transform/>
30. S. Sachin, P. Singh, R. Kumar, and A. K. Yadav, "Asymmetric Cryptosystem for Color Images Based on Unequal Modulus Decomposition in Chirp-Z Domain," in *Proc. Academia-Industry Consortium for Data Science: AICDS 2020*, Singapore: Springer Nature Singapore, 2022, pp. 331–344.
31. 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. Quantum Electron.*, vol. 55, no. 12, p. 1099, 2023.
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*, vol. 11509, pp. 92–101, Aug. 2020, SPIE.
33. H. Singh, A. K. Yadav, S. Vashisth, and K. Singh, "Optical image encryption using devil's vortex toroidal lens in the Fresnel transform domain," *Int. J. Opt.*, vol. 2015, no. 1, p. 926135, 2015.
34. H. Singh, "Devil's vortex Fresnel lens phase masks on an asymmetric cryptosystem based on phase-truncation in gyrator wavelet transform domain," *Opt. Lasers Eng.*, vol. 81, pp. 125–139, 2016.
35. M. Khurana and H. Singh, "An asymmetric image encryption based on phase truncated hybrid transform," *3D Res.*, vol. 8, pp. 1–17, 2017.
36. R. Kumar and C. Quan, "Optical colour image encryption using spiral phase transform and chaotic pixel scrambling," *J. Mod. Opt.*, vol. 66, no. 7, pp. 776–785, 2019.
37. N. Koblitz, A. Menezes, and S. Vanstone, "The State of Elliptic Curve Cryptography," *Designs, Codes and Cryptography*, vol. 19, no. 2, pp. 173–193, Mar. 2000, doi: 10.1023/A:1008354106356.
38. V. Kapoor, V. S. Abraham, and R. Singh, "Elliptic curve cryptography," *Ubiquity*, vol. 2008, no. May, p. 7:1-7:8, May 2008, doi: 10.1145/1386853.1378356.
39. 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.