Optica Applicata, Vol. LV, No. 3, 2025
DOI: 10.37190/oa/207387

Multi-image asymmetric encryption algorithm based on phase truncation and pixel scrambling in the gyrator domain

Eakta Kumari*, Saurabh Mukherjee

Department of Computer Science, Banasthali Vidyapith, India

*Corresponding author: eaktayadav19@gmail.com

This manuscript proposes a multi-image security algorithm based on phase truncation and pixel scrambling in the gyrator domain. The algorithm utilizes chaotic maps to improve key strength and phase truncation to provide asymmetric nature to the proposed algorithm. These features make proposed algorithm secure encryption algorithms for multiple images simultaneously. The algorithm utilized affine chaotic map for pixel scrambling. The proposed algorithm is tested with different types of images. The efficacy and robustness of proposed algorithm is tested through statistical and visual attacks such as correlation coefficient, information entropy, mean squared error, peak signal-to-noise ratio, histogram, mesh and correlation distribution plots. Efficacy of proposed algorithm is also analysed using the contamination and cryptographic attack such as known plaintext, chosen plaintext, and brute force attack. Results show that proposed algorithm is robust and secure to use in real-time applications.

Keywords: cryptography, gyrator transform, affine map.

1. Introduction

With the rapid advancement of technology and social networking has increase the need of secure data transmission and storage algorithms. As images and videos are effective ways to express the information, so, most of data transmitted over internet as either in form of images or videos. The images and videos transferred over the internet are widely used in fields such as medical, forensics, military, banking, education, healthcare, transport, and various other departments. However, the widespread use of images has raised major concerns regarding their security and authenticity, as privacy breach or data tampering may raze the serious issues. So, data encryption is an effective way to safeguard the data from unauthorized users during transmission and storage.

In the literature, it is evident that various techniques are available to secure the data, such as data encryption standard (DES), Rivest–Shamir–Adleman (RSA), advance encryption standard (AES) and various other digital algorithms. The available digital cryptographic algorithms have major concerns such as high-power consumption, complex computation, and slow. In the modern era, there is high demand of transmission and storage of data. Chaos theory [1-3] plays important role in the field of cryptography [4]. Various algorithms have been proposed for image encryption [5-8]. Moreover, pixel permutation [9-10], DNA coding [11-13], compressed sensing [14-16] and frequency transformation [17-20] based security algorithms are also proposed for safeguarding the data. Due to the sensitivity of parameters, chaotic maps sufficiently increase the keyspace of an encryption algorithm. So, the chaotic maps improve the key strength of the security algorithms [21-24]. For multiple image encryption Zhang *et al.* [25] developed a technique based on piecewise linear chaotic map. Another multiple image encryption algorithm is proposed using the concept of chaotic map with DNA encoding reported by Zhang *et al.* [26]. A cryptosystem using the concept of mixed hash function and cyclic shift, reported by Wang *et al.* [27]. Karawia [28], proposed a technique using 2-D economic map and mixed image elements. These algorithms are exposed against common cryptographic attacks. Enayatifar *et al.* [29] proposed a multi-image encryption technique using DNA encoding in which multiple plain images are used to create an augmented image. Another security algorithm proposed by Zarebnia *et al.* [30] used the concept of XOR and cyclic shift with Arnold cat map. Various other schemes using the concept of chaotic maps were reported [31-37]. Gao *et al.* [38] proposed a technique for multiple image encryption utilizing the concept of channel scrambling. Hosny *et al.* [39] developed a security algorithm for multiple image encryption (MIE) based on the concept of confusion-diffusion using ASLT map. A security algorithm based on permutation-diffusion algorithm proposed by Zhou *et al.* [40] Sabir *et al.* [41] proposed a MIE using 2-D discrete fractional Hartly transform, affine hill cipher and 2-D Arnold map. Another technique utilizing permutation-diffusion concept reported by Xu [42] in which pixel diffusion operation is performed by generating pseudo-random sequence and after that, permutation is used for scrambling. Zhang *et al.* [43] proposed a system for multiple grayscale images initially used for creating a cube and then applying zigzag transformation for scrambling on the cube sides. Ye *et al.* [44] proposed a multiple image hiding using 3D-CCM and 3D-DCT. Hosny *et al.* [39] proposed encryption scheme for multiple color images using ASLT map.

All methods demonstrate efficacy but some are prone to brute-force attack due to their limited key-space. Furthermore, optical techniques are expensive and require a complex setup to encrypt multiple images simultaneously. Another major concern in optical security algorithm is the number of multiple images taken simultaneously for encryption, but it is found to be very costly and time taking. So, there is a need of technique which can address these issues. The primary contribution of this study addresses the above discussed issues and the proposed scheme simultaneously secures any number and any type of images.

In this paper, an encryption algorithm for multiple images based on chaotic map and phase truncation and phase reservation in gyrator domain is presented. The chaotic map improves the key-space and phase truncation provides the asymmetric characteristic to the proposed algorithm. The rest of the paper is organized as follows. Section 2 describes the basic terminologies such as chaotic map and gyrator transform. Section 3 deals with the encryption and decryption technique of proposed algorithm. Simulation results and cryptanalysis of the proposed algorithm are elaborated in Section 4. In the last section, the conclusion of article is presented followed by references.

2. Basic terminologies

2.1. Gyrator transform

The gyrator transform (GT) [18] is one type of linear canonical transform, which has been widely used for image encryption algorithms. Mathematically, gyrator transform of any image $f(x, y)$ is defined as

$$\begin{aligned} F(u, v) &= G^{\alpha}\Big[f(x, y)\Big](u, v) \\ &= \frac{1}{|\sin\alpha|}\iint f(x, y)\exp\left[2\pi i\,\frac{(xy+uv)\cos\alpha-(xv+yu)}{\sin\alpha}\right]\mathrm{d}x\,\mathrm{d}y \end{aligned} \tag{1}$$

here, α stands for rotation angle, lies in the range of 0 to 2π and provides additional decryption keys to the encryption algorithm. The (x, y) and (u, v) represent the horizontal and vertical coordinates in spatial and frequency domain, respectively. In Fig. 1(b), the effect of GT on the image of *Cameraman* with dimension 256×256 is demonstrated. The recovered image corresponding to Fig. 1(b) is shown in Fig. 1(c).

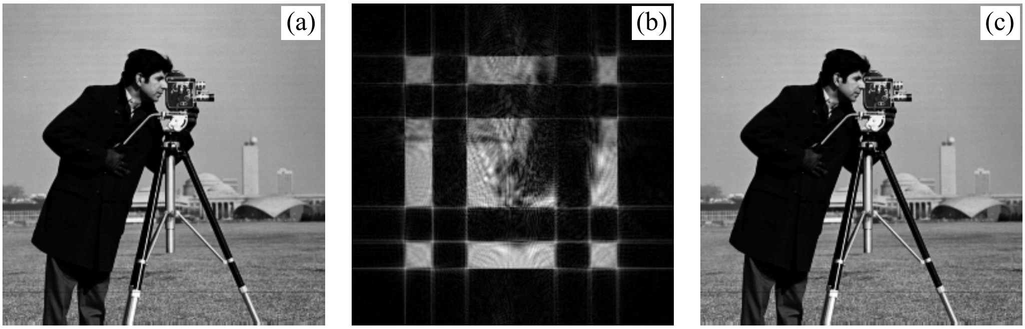

Fig. 1. (a) *Cameraman* image, (b) GT transformed image with angle $\alpha = 1.57\frac{\pi}{2}$, and (c) recovered image.

2.2. Affine map

Affine mapping (or affine transformation) is a type of transformation combined with a translation. It is used in many image processing tasks, including pixel scrambling [45], where the pixel positions in an image are rearranged to make the image appear scrambled. In matrix form, the map is represented as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} p+qx \\ r+sy \end{bmatrix}\langle \mathrm{mod}\, N\rangle \tag{2}$$

Here, p, q, r, and s are integers chosen between 1 and N (the size of the image, typically the dimension of the image or a wrapping factor for coordinates) such that $\gcd(q, s) = 1$ which ensures that the transformation is invertible and thus one-to-one. This means that no two points should map to the same location after transformation, which is critical for encryption to preserve information.

3. Proposed scheme

In this section, we will discuss the encryption and decryption process of the proposed algorithm whose flow-chart is shown in Fig. 2.

3.1. Encryption process

The encryption process of proposed algorithm utilized the affine map and gyrator transform. Step wise complete encryption process is discussed as below.

Step 1: First select the source images which are to be encrypted and an augmented image is created using the source images and stored as plaintext image $I(x, y)$ of size $n \times n$.

Step 2: A random phase mask (RPM1) of same size as that of plaintext image is created and bonded with I and output is stored as E_1. Mathematically,

$$E_1 = I(x, y) \times \mathrm{RPM1} \tag{3}$$

here, $\mathrm{RPM1} = \exp(1\mathrm{i}\pi R_1)$, and R_1 represents the random matrix of size $n \times n$.

Step 3: E_1 is propagated through gyrator transform and output is masked with random phase mask (RPM2) and undergoes phase truncation operation. Mathematically,

$$E_2 = \mathrm{GT}_{\lambda}(E_1) \tag{4}$$

$$E_3 = E_2 \times \mathrm{RPM2} \tag{5}$$

here, $\mathrm{RPM2} = \exp(1\mathrm{i}\pi R_2)$ and R_2 is random matrix of size $n \times n$.

Now, phase truncation and phase reservation operation is performed on E_3. In the proposed algorithm, phase part is reserved as private key (PK) and amplitude part is further propagated through the gyrator transform which is stored as ciphertext.

$$\mathrm{PK} = \mathrm{angle}(E_3) \tag{6}$$

$$E_4 = \mathrm{abs}(E_3) \tag{7}$$

Step 4: E_4 undergoes pixel scrambling operation using the affine map and the resultant is propagated through gyrator transform and we got the final encrypted image. Mathematically,

$$E_5 = \text{pixel scrambling}(E_4, \text{affine map}) \tag{8}$$

$$E = \mathrm{GT}_{\lambda}(E_5) \tag{9}$$

3.2. Decryption process

The decryption procedure follows just the reverse steps of the encryption which is summarized in below steps.

Step 1: The received encrypted image is first propagated in gyrator domain with inverse parameters

$$D_1 = \mathrm{GT}_{-\lambda}(E) \tag{10}$$

Step 2: D_1 undergoes again pixel scrambling using inverse affine map and then the PK stored in the encryption procedure is bonded with the resultant which is mathematically represented as

$$D_2 = \text{pixel scrambling}(D_1, \text{affine map}) \tag{11}$$

$$D_3 = D_2 \times \mathrm{PK} \tag{12}$$

Step 3: In the next step the conjugate of RPM2 which is also stored as the encryption key is bonded with D_3 and undergoes gyrator transform with negative values of parameters which are used in the encryption process and we got the recovered image which is mathematically represented as

$$D_4 = D_3 \times \mathrm{RPM2} \tag{13}$$

$$D = \mathrm{GT}_{-\lambda}(D_4) \tag{14}$$

The process of proposed security algorithm is depicted in Fig. 2 and the result of proposed algorithm is demonstrated in Fig. 3. The validation results of proposed algorithm validate that proposed algorithm is robust and secure.

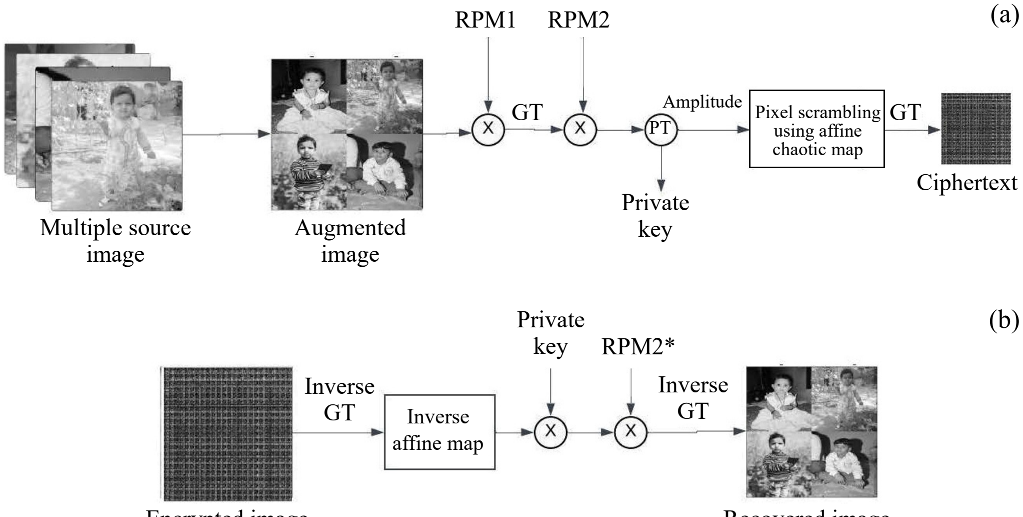

Fig. 2. Proposed scheme. (a) Encryption flow-chart, and (b) decryption flow-chart.

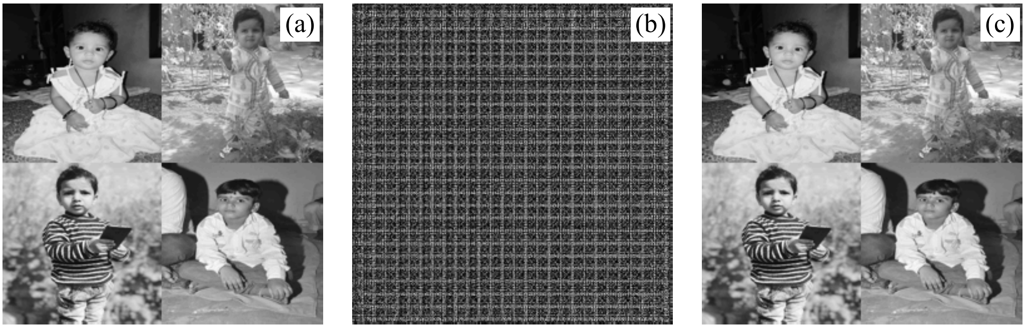

Fig. 3. (a) Augmented image created from multiple source images, (b) ciphertext using proposed scheme, and (c) recovered image using proposed scheme.

4. Simulation and results

In this section, we will discuss the simulation results of proposed algorithm. Simulation of the proposed algorithm has been carried out in MATLAB 2022A software on a computer having 8GB RAM with Intel® core™ @ 2.40GHz processor. During the simulation, various type and size of images are chosen but in this manuscript simulation results of four images are presented. The augmented image could be created of any size here we present the results for 256 × 256 image. The result of statistical analysis such as mean squared error (MSE), correlation coefficient (CC), information entropy (IE), peak signal-to-noise ratio (PSNR), mesh and histogram plots are analysed in this section. The security of proposed algorithm is also analysed using cryptographic attacks. In this section, results for chosen, known plaintext, contamination and brute force attack are also discussed. The efficacy and robustness of any cryptographic algorithm are depending on decryption keys. In this section, results of keyspace sensitivity are also discussed.

The results are further discussed through various metrics, including mean squared error (MSE), correlation coefficient (CC), and peak signal-to-noise ratio (PSNR) which are defined as

$$\mathrm{MSE} = \frac{1}{N \times N} \sum_{x=1}^{N} \sum_{y=1}^{N} |f(x,y) - f'(x,y)|^2 \tag{15}$$

$$\mathrm{CC} = \frac{\mathrm{cov}(f(x,y),\ f'(x,y))}{\sigma(f(x,y))\,\sigma(f'(x,y))} \tag{16}$$

$$\mathrm{PSNR} = 10 \log_{10} \frac{255^2}{\mathrm{MSE}} \tag{17}$$

Here, $f(x,y)$ denotes input image pixel values and $f'(x,y)$ denotes the pixel values of recovered image having size $n \times n$, cov represents covariance, and σ represents the standard deviation.

Table 1. Statistical parameters (CC, MSE, PSNR) are computed between plaintext and recovered images of *Cameraman*.

Statistical measure	Values
CC	1
PSNR	587.80
MSE	1.927×10^{-21}
Computational time	0.7789 s

Performance metrics MSE, PSNR and CC are calculated between the plaintext and recovered image and the values are tabulated in Table 1. Here, very high value of PSNR, almost reaching zero value of MSE and value of CC is 1 that shows that the recovered image is similar to the source image.

4.1. Pixel data analysis

The effectiveness of a data security algorithm is also analysed using the histogram and mesh plots. The histogram of ciphertext obtained by a security algorithm should be significantly different from that of the original image. Figure 4(a)–(c) demonstrated the histogram of plaintext (created from multiple input images), encrypted image and recovered image obtained in proposed algorithm. It is evident that the histogram plot of ciphertext does not provide any information regarding plaintext. Moreover, the effectiveness of proposed algorithm is also analysed using the 3-D plot shown in Fig. 4(d)–(f). It is observed that 3-D plot of encrypted image does not provide any valuable information/clue regarding plaintext. The results confirm that the proposed algorithm is both secure and resistant to statistical attacks.

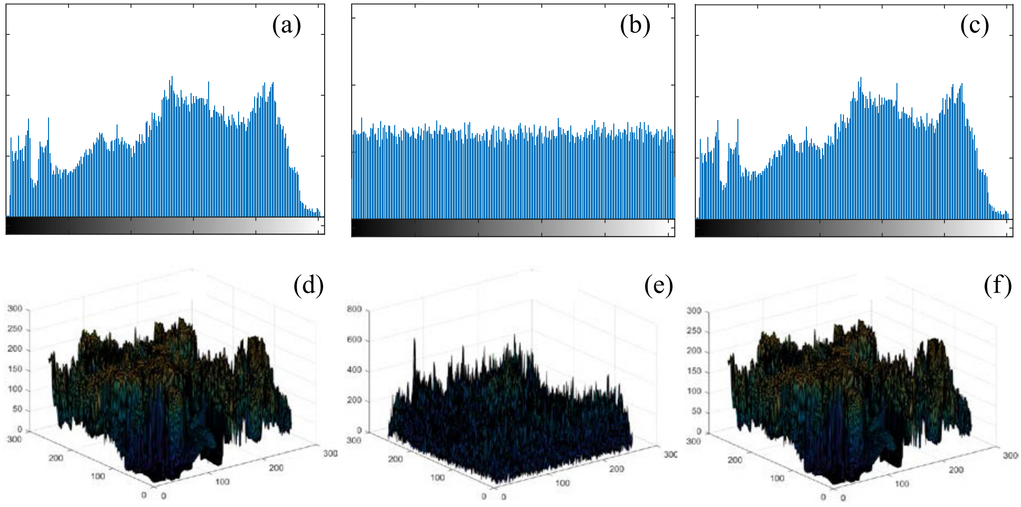

Fig. 4. Histogram of (a) augmented image created from input images, (b) cipher text, and (c) recovered image. 3D-plot of (d) augmented image, (e) cipher text, and (f) recovered image.

4.2. Information entropy

The information entropy of an image measures the degree of randomness inherent within the image. The value of information lies in the range of 0 to 8. The value of information 8 indicting the pixels of image have maximum distortion. The information entropy is computed using the following equation:

$$H(k) = \sum_{i=0}^{2n-1} -p(k_i) \log p(k_i) \tag{18}$$

Here, $H(k)$ denoted the information entropy of source k, $p(k_i)$ denoted the probability of each symbol of information source. In our case, information source is our augmented image. The value of information entropy for plaintext is 7.86 and ciphertext 7.996. Thus, results indicate that proposed algorithm is robust and secure.

4.3. Key sensitivity analysis

In this section, the effectiveness of encryption keys used in the decryption process is tested by using the incorrect encryption key at the decryption end and the results are presented in below cases.

Case 1: Another secret key used in the decryption process is private key (PK) which is obtained in the step 3 of the encryption procedure. In this case, again we had used RPM3 in place of PK and the obtained decrypted image is shown in Fig. 5(a).

Case 2: Another key used in the decryption procedure is the angle of propagation used in the gyrator transform. If we use a different angle rather than the one used in the encryption process, then the obtained recovered image is shown in Fig. 5(b).

From all the above cases, it is very clear that the proposed scheme is very sensitive to its secret keys used in the encryption process and the same keys required to be used in order to get the data at the receiver end. Also, the sensitivity graph shown in Fig. 5(c) is plotted for the angle used in gyrator transform and the deviation analysis from the

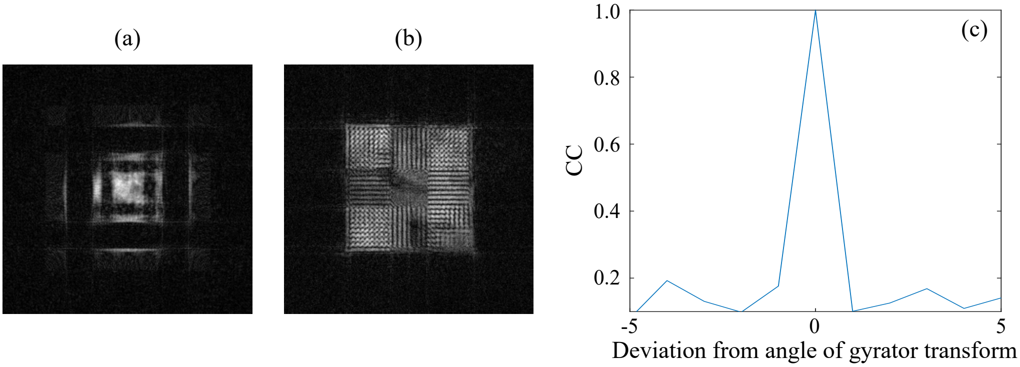

Fig. 5. (a) Recovered image using incorrect private key (case 1); (b) recovered image using incorrect value of gyrator transform angle (case 2); (c) sensitivity of gyrator transform angle deviated unit step from the value used in encryption algorithm.

correct value which is used in the encryption process is checked and observed that correlation coefficient approaches to almost zero for a slight change in the angle and hence, gyrator transform angle is very sensitive to its original value.

4.4. Correlation distribution analysis

Another metric used to validate the efficacy of security algorithm is the correlation distribution. In our case, we have plotted 7000 adjacent pixels from augmented image

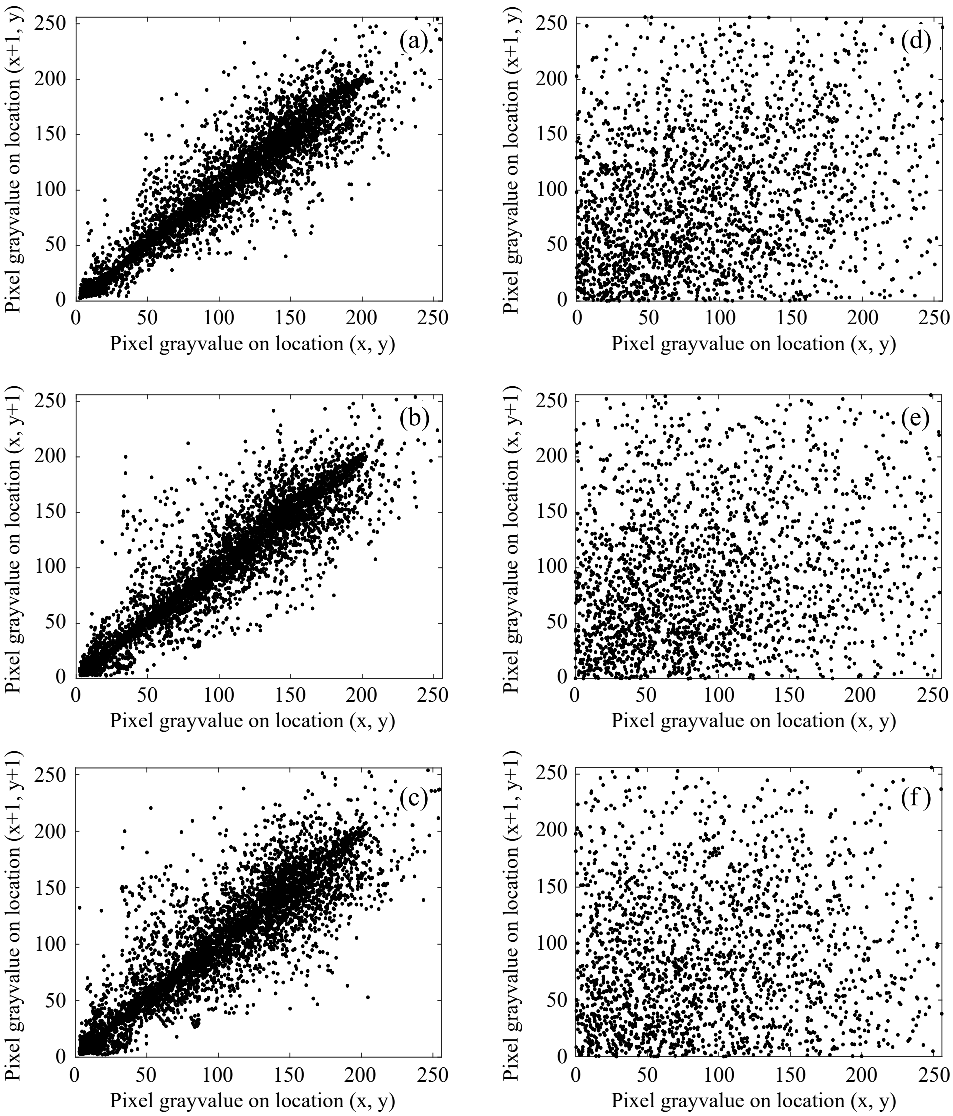

Fig. 6. Correlation distribution analysis plot of 7000 pixels. (a)–(c) Plaintext and (d)–(f) ciphertext in diagonal, vertical and horizontal direction, respectively.

and ciphertext, considering in diagonal, vertical, horizontal directions. As shown in Fig. 6(a)–(c), the pixels in the input image exhibit strong correlation with their adjacent pixels in all three directions. However, in the corresponding encrypted image plots (Fig. 6(d)–(f)), no discernible correlation is observed. These results clearly demonstrate that the proposed algorithm is robust against correlation distribution analysis.

4.5. Security analysis of proposed scheme

In this sub-section, the proposed scheme resistance to various attacks, including occlusion attack, noise attack, known-plaintext attack (KPA), chosen-plaintext attack (CPA) and iterative attack is discussed.

4.5.1. Occlusion attack

Data occlusion refers to data loss during the transmission. Sometimes, the data/image gets hidden or overwritten by an intruder with the aim to corrupt the data/image. Sometimes due to the channel abnormalities the data may be lost. This sub-section analysed the proposed scheme against the data lose attack. In our case to occlude the data, we have replaced the pixel values with zero in encrypted image obtained using proposed scheme as shown in Fig. 7(a)–(c) and recovered images shown in Fig. 7(d)–(f). From the results, it is evident that recovered images are visible to human eye and hence the proposed scheme resists occlusion attack up to 50% data loss.

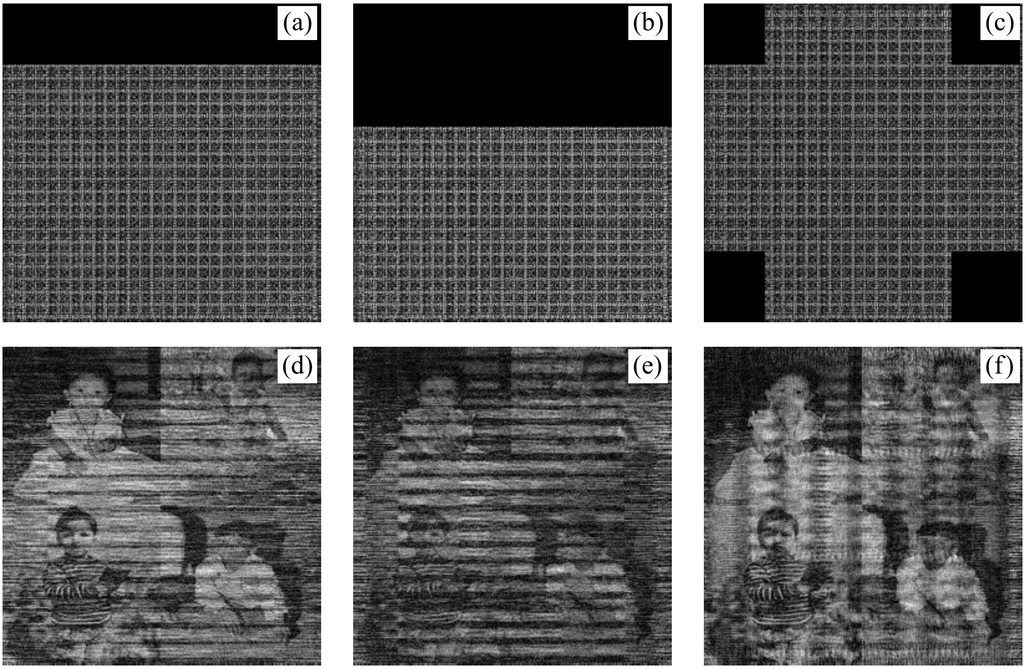

Fig. 7. Occlusion attack analysis results. (a)–(c) Occluded encrypted images. (d)–(f) Recovered images corresponding to occluded images using proposed scheme.

4.5.2. Noise attack

In the process of sending the data over internet, we had a chance to mix unwanted data due to noise in the communication channel or other causes. Therefore, it is crucial to assess how robust our proposed algorithm is against such noise attacks. In this scenario, ciphertext is tested with salt-and-pepper noise in the following manner:

$$\mathrm{EN} = E(1 + kN) \tag{19}$$

Here, E and EN refers to the ciphertext and noise polluted ciphertext, respectively, N is the noise present in the channel, and k is the coefficient used to represent the strength of noise. We have tested the algorithm for various types of noise attack but the results are presented for salt-and-pepper noise.

Figure 8(a) and (b) shows the results of recovered images corresponding to the noise polluted ciphertext with value of $k = 20$ and the varying values of noise density. The value 0.3 of noise density means 30% of the pixels in encrypted image are altered during transmission due to noise. From the results in Fig. 8(c) it is clear that even after 0.9 value of noise density, the recovered image also provides clues about the source images.

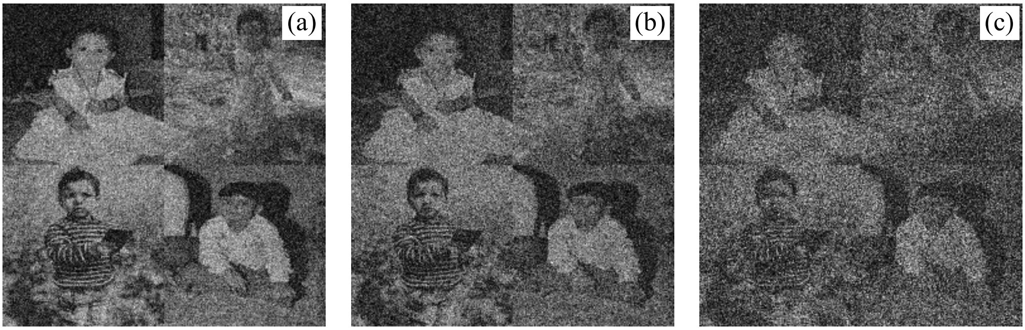

Fig. 8. Noise attack analysis results. (a)–(c) Recovered image with noise strength $k = 20$ and noise density 0.3, 0.5 and 0.9, respectively.

4.5.3. Cryptanalysis of proposed algorithm

In this section, proposed multi-image encryption algorithm is tested with chosen and know plaintext attack, and iterative attack. In known plaintext attack, the attacker tries to retrieve the decryption keys using pair of plaintexts and ciphertext. In our case, we have applied KPA to retrieve the value of RPM2 which is used as a decryption key. Using the obtained decryption key, results are not faithful. The results of recovered image obtained using known plaintext attack are demonstrated in Fig. 9(a). Results demonstrated that no valuable information could be figured out from retrieved image. Proposed algorithm is also tested with chosen plaintext attack. In chosen plaintext attack, a Dirac delta function image is chosen and tries to retrieve the plaintext. The result of chosen plaintext attack is presented in Fig. 9(b). Since, the proposed algorithm is asymmetric in nature. So, the proposed algorithm is also tested with iterative attack

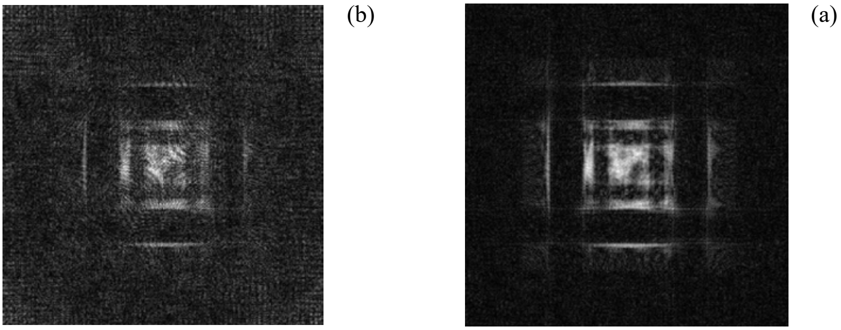

Fig. 9. Recovered image using (a) known-plaintext and (b) chosen plaintext attack.

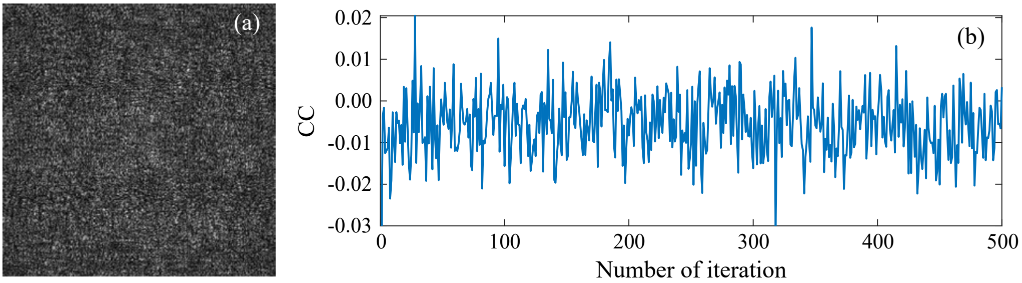

Fig. 10. (a) Decrypted image using iterative attack and (b) plot of correlation coefficient (between plaintext recovered image) *versus* number of iterations.

using Gerchberg–Saxton algorithm. In iterative attack, 500 iterations are performed and the results indicate that no valuable information is find out regarding plaintext. The result of iterative attack is presented in Fig. 10. The results of the cryptographic attack confirm the robustness and effectiveness of the proposed multi-image encryption algorithm.

4.5.4. Comparison analysis

A comparative analysis of the proposed scheme with various other schemes is presented in below tables highlighting the mechanism used, provided security level, their computational speed and complexity and advantages (see Table 2).

5. Conclusion

The proposed multi-image security algorithm effectively secures multiple images using affine map and phase truncation in the gyrator domain. The asymmetric nature and pixel scrambling ensure robust data protection. The performance of the proposed scheme is evaluated using statistical analysis such as information entropy, and key sensitivity demonstrates high security, and resistance to cryptographic attacks. The histo-

Table 2. Comparison analysis of proposed scheme with existing schemes.

Method	Core mechanism	Security level	Decryption quality	Resistance to attacks	Speed and complexity	Advantages
Phase truncation (PT-based)	Encrypts by modifying phase spectrum	High	Medium to low	Moderate	Fast	Strong obfuscation, simple implementation
Double random phase encoding (DRPE)	Uses two random masks in the optical/digital domain	Very high	High (if both keys are known)	High	Medium to high	High security, supports optical implementation
Phase retrieval-aided PT	Uses GS/HIO algorithm to recover phase	Medium	Medium -high	Medium	High (iterative)	Balances security and recoverability
Proposed scheme	Combines optical DRPE with chaotic scrambling	Very high	High	Very high	High	Strengthens both scrambling and transformation security

gram and mesh plot of the encrypted image are completely different from the histogram and mesh plot of plaintext image that indicating proposed algorithm does not provide any information regarding plaintext. The value of information entropy is 7.996, which is very close to 8. The value of the correlation coefficient is the one between plaintext and recovered image that show the decrypted image is reliable and similar to plaintext. The contamination results also validate the proposed algorithm to be highly efficient and robust. The cryptanalysis results also validate that the proposed algorithm is robust and secure against existing cryptographic attacks. Thus, results validate that the algorithm is highly efficient, scalable, and adaptable to varying image numbers and sizes, making it suitable for secure image transmission and storage across various fields.

References

[1] Layek G.C., *An Introduction to Dynamical Systems and Chaos*, Springer India, New Delhi, 2015. https://doi.org/10.1007/978-81-322-2556-0

[2] Li L., *A novel chaotic map application in image encryption algorithm*, Expert Systems with Applications **252**, 2024: 124316. https://doi.org/10.1016/j.eswa.2024.124316

[3] Bezerra J.I.M., Molter A., Machado G., Iankowski Soares R., de Almeida Camargo V.V., *A novel single kernel parallel image encryption scheme based on a chaotic map*, Journal of Real-Time Image Processing **21**(4), 2024: 129. https://doi.org/10.1007/s11554-024-01506-9

[4] Chen B., Huang L., Cai S., Xiong X., Zhang H., *A lightweight symmetric image encryption cryptosystem in wavelet domain based on an improved sine map*, Chinese Physics B **33**(3), 2024: 030501. https://doi.org/10.1088/1674-1056/ad1030

[5] Zia U., McCartney M., Scotney B., Martinez J., AbuTair M., Memon J., Sajjad A., *Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains*, International Journal of Information Security **21**(4), 2022: 917-935. https://doi.org/10.1007/s10207-022-00588-5

[6] Sachin, Singh P., Singh K., *Nonlinear image authentication algorithm based on double fractional Mellin domain*, Nonlinear Dynamics **111**(14), 2023: 13579-13600. https://doi.org/10.1007/s11071-023-08540-5

[7] Yadav R., Sachin, Singh P., *Multidomain asymmetric image encryption using phase-only CGH, QZS method and Umbrella map*, Journal of Optics, 2024. https://doi.org/10.1007/s12596-024-02106-3

[8] Lai Q., Liu Y., Yang L., *Remote sensing image encryption algorithm utilizing 2D Logistic memristive hyperchaotic map and SHA-512*, Science China Technological Sciences **67**(5), 2024: 1553-1566. https://doi.org/10.1007/s11431-023-2584-y

[9] Qiu H., Xu X., Jiang Z., Sun K., Xiao C., *A color image encryption algorithm based on hyperchaotic map and Rubik's Cube scrambling*, Nonlinear Dynamics **110**(3), 2022: 2869-2887. https://doi.org/10.1007/s11071-022-07756-1

[10] Wei D., Jiang M., Deng Y., *A secure image encryption algorithm based on hyper-chaotic and bit-level permutation*, Expert Systems with Applications **213**, 2023: 119074. https://doi.org/10.1016/j.eswa.2022.119074

[11] Yang C., Taralova I., El Assad S., Loiseau J.-J., *Image encryption based on fractional chaotic pseudo-random number generator and DNA encryption method*, Nonlinear Dynamics **109**(3), 2022: 2103-2127. https://doi.org/10.1007/s11071-022-07534-z

[12] Shraida G.Kh., Younis H.A., Al-Amiedy T.A., Anbar M., Younis H.A., Hasbullah I.H., *An efficient color-image encryption method using DNA sequence and chaos cipher*, Computers, Materials & Continua **75**(2), 2023: 2641-2654. https://doi.org/10.32604/cmc.2023.035793

[13] Chen X., Mou J., Cao Y., Banerjee S., *Chaotic multiple-image encryption algorithm based on block scrambling and dynamic DNA coding*, International Journal of Bifurcation and Chaos **33**(16), 2023: 2350190. https://doi.org/10.1142/S0218127423501900

[14] Wang X., Liu C., Jiang D., *A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT*, Information Sciences **574**, 2021: 505-527. https://doi.org/10.1016/j.ins.2021.06.032

[15] Hadj Brahim A., Ali Pacha A., Hadj Said N., *Image encryption based on compressive sensing and chaos systems*, Optics & Laser Technology **132**, 2020: 106489. https://doi.org/10.1016/j.optlastec.2020.106489

[16] Wang C., Song L., *An image encryption scheme based on chaotic system and compressed sensing for multiple application scenarios*, Information Sciences **642**, 2023: 119166. https://doi.org/10.1016/j.ins.2023.119166

[17] Wen H., Chen Z., Zheng J., Huang Y., Li S., Ma L., Lin Y., Liu Z., Li R., Liu L., Lin W., Yang J., Zhang C., Yang H., *Design and embedded implementation of secure image encryption scheme using DWT and 2D-LASM*, Entropy **24**(10), 2022: 1332. https://doi.org/10.3390/e24101332

[18] Yadav R., Sachin, Singh P., *Multiuser medical image encryption algorithm using phase-only CGH in the gyrator domain*, Journal of the Optical Society of America A **41**(3), 2024: A63-A72. https://doi.org/10.1364/JOSAA.507308

[19] Kumari E., Singh P., Mukherjee S., Purohit G.N., *Analysis of triple random phase encoding cryptosystem in Fresnel domain*, Results in Optics **1**, 2020: 100009. https://doi.org/10.1016/j.rio.2020.100009

[20] Kolivand H., Hamood S.F., Asadianfam S., Mohd Rahim M.S., Hurst W., *Image encryption framework based on multi-chaotic maps and equal pixel values quantization*, Multimedia Tools and Applications **84**, 2025: 17769-17804. https://doi.org/10.1007/s11042-024-19771-y

[21] Singh P., Yadav A.K., Singh K., *Color image encryption using affine transform in fractional Hartley domain*, Optica Applicata **47**(3), 2017: 421-433. https://doi.org/10.5277/oa170308

[22] Yadav A.K., Singh P., Saini I., Singh K., *Asymmetric encryption algorithm for colour images based on fractional Hartley transform*, Journal of Modern Optics **66**(6), 2019: 629-642. https://doi.org/10.1080/09500340.2018.1559951

[23] Pourasad Y., Ranjbarzadeh R., Mardani A., *A new algorithm for digital image encryption based on chaos theory*, Entropy **23**(3), 2021: 341. https://doi.org/10.3390/e23030341

[24] Wu W.Q., Kong L.S., *Image encryption algorithm based on a new 2D polynomial chaotic map and dynamic S-box*, Signal, Image and Video Processing **18**, 2024: 3213-3228. https://doi.org/10.1007/s11760-023-02984-3

[25] Zhang X., Wang X., *Multiple-image encryption algorithm based on mixed image element and chaos*, Computers & Electrical Engineering **62**, 2017: 401-413. https://doi.org/10.1016/j.compeleceng.2016.12.025

[26] Zhang H., Wang X.Q., Wang X.Y., Yan P.F., *Novel multiple images encryption algorithm using CML system and DNA encoding*, IET Image Processing **14**(3), 2020: 518-529. https://doi.org/10.1049/iet-ipr.2019.0771

[27] Wang X., Zhu X., Wu X., Zhang Y., *Image encryption algorithm based on multiple mixed hash functions and cyclic shift*, Optics and Lasers in Engineering **107**, 2018: 370-379. https://doi.org/10.1016/j.optlaseng.2017.06.015

[28] Karawia A.A., *Encryption algorithm of multiple-image using mixed image elements and two dimensional chaotic economic map*, Entropy **20**(10), 2018: 801. https://doi.org/10.3390/e20100801

[29] Enayatifar R., Guimarães F.G., Siarry P., *Index-based permutation-diffusion in multiple-image encryption using DNA sequence*, Optics and Lasers in Engineering **115**, 2019: 131-140. https://doi.org/10.1016/j.optlaseng.2018.11.017

[30] Zarebnia M., Pakmanesh H., Parvaz R., *A fast multiple-image encryption algorithm based on hybrid chaotic systems for gray scale images*, Optik **179**, 2019: 761-773. https://doi.org/10.1016/j.ijleo.2018.10.025

[31] Sharma N., Saini I., Yadav A.K., Singh P., *Phase-image encryption based on 3D-Lorenz chaotic system and double random phase encoding*, 3D Research **8**(4), 2017: 39. https://doi.org/10.1007/s13319-017-0149-4

[32] Abuturab M.R., *Multiple-information security system using key image phase and chaotic random phase encoding in Fresnel transform domain*, Optics and Lasers in Engineering **124**, 2020: 105810. https://doi.org/10.1016/j.optlaseng.2019.105810

[33] Chen H., Zhu L., Liu Z., Tanougast C., Liu F., Blondel W., *Optical single-channel color image asymmetric cryptosystem based on hyperchaotic system and random modulus decomposition in Gyrator domains*, Optics and Lasers in Engineering **124**, 2020: 105809. https://doi.org/10.1016/j.optlaseng.2019.105809

[34] Liu H., Wang X., *Color image encryption based on one-time keys and robust chaotic maps*, Computers & Mathematics with Applications **59**(10), 2010: 3320-3327. https://doi.org/10.1016/j.camwa.2010.03.017

[35] ul Haq T., Shah T., *Algebra-chaos amalgam and DNA transform based multiple digital image encryption*, Journal of Information Security and Applications **54**, 2020: 102592. https://doi.org/10.1016/j.jisa.2020.102592

[36] Gao X., Yu J., Banerjee S., Yan H., Mou J., *A new image encryption scheme based on fractional -order hyperchaotic system and multiple image fusion*, Scientific Reports **11**, 2021: 15737. https://doi.org/10.1038/s41598-021-94748-7

[37] Zhang X., Zhang L., *Multiple-image encryption algorithm based on chaos and gene fusion*, Multimedia Tools and Applications **81**, 2022: 20021-20042. https://doi.org/10.1007/s11042-022-12554-3

[38] Gao X., Mou J., Xiong L., Sha Y., Yan H., Cao Y., *A fast and efficient multiple images encryption based on single-channel encryption and chaotic system*, Nonlinear Dynamics **108**(1), 2022: 613-636. https://doi.org/10.1007/s11071-021-07192-7

[39] Hosny K.M., Kamal S.T., *A new four-tier technique for efficient multiple images encryption*, Multimedia Tools and Applications **84**, 2025: 26797-26815. https://doi.org/10.1007/s11042-024-20125-x

[40] Zhou Z., Xu X., Jiang Z., Sun K., *Multiple-image encryption scheme based on an N-dimensional chaotic modular model and overlapping block permutation–diffusion using newly defined operation*, Mathematics **11**(15), 2023: 3373. https://doi.org/10.3390/math11153373

[41] Sabir S., Guleria V., *Multi-layer security based multiple image encryption technique*, Computers & Electrical Engineering **106**, 2023: 108609. https://doi.org/10.1016/j.compeleceng.2023.108609

[42] Xu M., *A multiple-image encryption algorithm based on orthogonal arrays with strength 3*, Optics & Laser Technology **167**, 2023: 109746. https://doi.org/10.1016/j.optlastec.2023.109746

[43] Zhang X., Liu M., *Multiple-image encryption algorithm based on the stereo Zigzag transformation*, Multimedia Tools and Applications **83**, 2024: 22701-22726. https://doi.org/10.1007/s11042-023-16404-8

[44] Ye G., Guo L., *A visual meaningful encryption and hiding algorithm for multiple images*, Nonlinear Dynamics **112**(16), 2024: 14593-14616. https://doi.org/10.1007/s11071-024-09790-7

[45] Anjana S., Saini I., Singh P., Yadav A.K., *Asymmetric enciphering of images using affine transform and fractional Fourier transform*, International Journal of Advanced Intelligence Paradigms **29**(1), 2024: 28-45. https://doi.org/10.1504/IJAIP.2024.141523

Received March 19, 2025
in revised form May 26, 2025