Asian Journal of Physics
Vol. 32, Nos 3 & 4 (2023) A11 - A24
Available on: www.asianjournalofphysics.com

ap

An asymmetric hybrid image encryption algorithm using fractional Hartley transform, Bird Wings Map, and embedded watermarking

Joyti[1], Sachin[2], Phool Singh[3], and Kehar Singh[4]

[1]*Department of Mathematics, Government College Barota, Gohana, Haryana-131 301, India*

[2]*Department of Mathematics, IIHS, Kurukshetra University, Kurukshetra, Haryana-136 119, India*

[3]*Department of Mathematics, SOET, Central University of Haryana, Mahendergarh-123 031, India*

[4]*Optics and Photonics Center, Indian Institute of Technology Delhi, New Delhi-110 016, India*

Dedicated to Prof Jay M Enoch

We present an improved security algorithm based on fractional Hartley transform, phase truncation and phase reservation, newly developed 'Bird Wings Map'(BWM), and watermarking. The BWM enhances security of the proposed algorithm by providing additional parameters to the cryptosystem. The effectiveness of the scheme is validated through simulations conducted on a pair of grayscale images, namely Cameraman and Baboon. The Cameraman is used as the target image, while the Baboon serves as the host image in the watermarking process. The proposed scheme is tested against various statistical attacks, using mean-squared-error, correlation coefficient, information entropy, and peak signal-to-noise ratio. Additionally, the histogram and mesh plots are also provided. Real-time attacks such as noise-, and occlusion attacks are also applied to validate the robustness of the proposed scheme. Furthermore, the strength of the scheme is tested against the well-known attacks, such as known-plaintext-, chosen-plaintext-, and special iterative attack. Key sensitivity analysis is performed to analyze the key-space of the proposed scheme. The simulation results demonstrate the robustness and effectiveness of the scheme which exhibits resilience against the statistical attacks, real-time attacks, and cryptographic attacks.

Keywords: Asymmetric image encryption, Fractional Hartley transform, Phase truncation and phase reservation, Bird Wings Map, Watermarking, Key sensitivity.

1 Introduction

In the present big data-era, the security of sensitive information contained in images, audios, and videos, has become a major concern for stake holders. With growth of the multimedia technology, a major part of the sensitive data remains in the form of images and/or videos. Consequently, there has been an upsurge in investigations to ensure the data security, for which we need efficient and robust cryptosystems. Image encryption plays a crucial role in safeguarding the valuable information from unauthorized access, ensuring its confidentiality, integrity, and authenticity. Moreover, watermarking allows for the embedding of additional information in images, enabling various applications such as copyright protection, content authentication, and data integrity verification. There are various digital image encryption algorithms such as data encryption standard (DES), advanced encryption standard (AES), and Rivest-Shamir-Adleman (RSA) algorithm that are used to secure the data [1-4]. The images may have complex data, and therefore require more time, space, computation, and power for processing. It is now well-known that the digital image encryption algorithms have difficulties in real-time implementation due to slow computation and high-power consumption. Therefore, researchers in various countries have been developing optical image encryption

Corresponding author
e mail: sachinmaths@kuk.ac.in (Sachin)

techniques that have features such as parallel processing, low power consumption, fast computations, and enhanced key-space, with a view to overcoming the bottlenecks of digital processing-based techniques. In certain situations, working in a hybrid mode is the only possibility.

In 1995, Refregier and Javidi [5] published the first optical image encryption method known as the double random phase encoding (DRPE) in the Fourier domain. Due to the advantages of the optical image encryption, a number of encryption methods have been developed based on the DRPE [6-11]. The DRPE-based algorithms have also proposed in various other domains, such as fractional Fourier [12,13], Fresnel [14-16], Gyrator [17-20], Hartley [21], fractional Hartley [22-25], Mellin, and fractional Mellin [26-29], and Radon transform [30]. In course of further research, it was found that the DRPE based encryption systems could be breached by the basic cryptographic attacks [31-38] such as chosen-plaintext attack (CPA), known-plaintext attack (KPA), and cipher-text only attack (COA).

It is well-established that the concept of chaos has now grown into a full-fledged subject and finds applications in many disciplines of science and engineering [39]. To improve security of the DRPE-based encryption algorithms, researcher developed the chaos-based image encryption algorithms [40-57]. However, many of the chaos-based encryption algorithms also suffer from inherent linearity, and are therefore susceptible to differential attacks [54,55]. So, researchers proposed asymmetric image encryption algorithms to get rid of the linearity and symmetric nature inherent in the DRPE-based encryption algorithms. The phase truncation in Fourier transform (PTFT) was the first optical asymmetric image encryption algorithm [58]. It turned out that the PTFT-based encryption algorithms are also weak in security due to the relationship between phase and amplitude [59]. As a result, the PTFT- based encryption algorithms are vulnerable to special iterative attacks.

In this manuscript, we discuss an improved hybrid scheme for the security of phase truncation and phase reservation-based image encryption algorithm using chaotic Bird Wings Map (BWM), fractional Hartley transform, and incorporation of watermarking that provides an additional layer of security and enables data authentication. Watermarking [11,53,60-62] allows for the embedding of information, such as digital signatures or copyright marks, into the encrypted image. This embedded watermark can later be extracted for verification purposes, ensuring the authenticity and integrity of the decrypted image. Rest of the manuscript is arranged in the following manner. In section 2, we have discussed the Hartley transform and chaotic BWM. The proposed security algorithm has been discussed in Section 3. The validation results of the proposed security algorithm have been discussed in Section 4, and the conclusions of the study have been provided in the last section of the manuscript.

2 Basic principle

In this section, we discuss the fractional Hartley transform and the chaotic Bird Wings Map.

2.1 Fractional Hartley Transform (*FHT*)

The *FHT* [22-25] is widely used in the field of image-, and signal processing. A two-dimensional *FHT* for an image $I(x, y)$ is given by the following expression,

$$FHT^{p,q}(u,v) = \frac{\sqrt{(1-i\cot\beta_1)(1-i\cot\beta_2)}}{2\pi} \times \exp\left[i\pi\left(\frac{u^2\cot\beta_1}{\lambda f_1} + \frac{v^2\cot\beta_2}{\lambda f_2}\right)\right]$$
$$\times \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \exp\left(\frac{i\pi x^2\cot\beta_1}{\lambda f_1} + \frac{i\pi y^2\cot\beta_2}{\lambda f_2}\right) \times \left\{\frac{1 - iexp\left[i(\beta_1+\beta_2)/2\right]}{2} \times \mathrm{cas}\left(\frac{uxcsc\,\beta_1}{\lambda f_1} + \frac{vycsc\beta_2}{\lambda f_2}\right)\right.$$
$$\left. + \frac{1 + iexp\left[i(\beta_1+\beta_2)/2\right]}{2} \times \mathrm{cas}\left(-\frac{uxcsc\beta_1}{\lambda f_1} - \frac{vy\mathrm{csc}\beta_2}{\lambda f_2}\right)\right\} I(x,y)\,dx\,dy \qquad (1)$$

where p and q represent the fractional orders of the *FHT*, $\beta_1 = p\pi/2$ and $\beta_2 = q\pi/2$, λ is the wavelength of the input light, and cas = cos + sin. Here, f_1 and f_2 are standard focal lengths of the lenses, respectively in x and y directions.

In terms of the fractional Fourier transform (*FrFT*), the 2-D *FHT* can be deduced as follows:

$$FHT^{p,q}(u,v) = \frac{1 + \exp[i(\beta_1 + \beta_2)/2]}{2} F^{p,q}(u, v) + \frac{1 - \exp[i(\beta_1 + \beta_2)/2]}{2} F^{p,q}(-u, -v)$$

It may be noted that for computing *FHT*, we need to calculate two fractional Fourier transforms used in the expression above. The *FHT* is reversible since it satisfies the additive property. Thus, the inverse transform of 2-D *FHT* of order (p, q) is obtained by taking the orders as $(-p, -q)$. An optical implementation of the *FHT* is possible and is discussed in several references [22,23] on the *FHT*.

2.2 Chaotic Bird Wings Map (*BWM*)

We propose a new chaotic map based on Tinkerbell map [48,56] and name it as 'Chaotic Bird Wings Map'. It is a two-dimensional discrete time map which is used for generating a random sequence. The parameters of the BWM are used as key in the chaos-based cryptosystem. Mathematically, the Chaotic BWM is given by,

$$x_{n+1} = \tanh(x_n^2) - y_n^2 - a \tanh(x_n) + b y_n \tag{2a}$$

$$y_{n+1} = \tanh(2x_n)\, y_n + c \tanh(x_n) + d y_n \tag{2b}$$

Here, x_0 and y_0 are the initial values of the map variables which work as a main key in sequence generation, and a, b, c, and d are parameters. Mostly the initial values of the parameters are: $b = 0.9$, $a = -0.6013$, $c = -1.5$ and $d = 0.5$. For the purpose of getting bifurcation diagram of the map, parameter a varies in the interval $(-0.6013, -0.54791)$ and initial values of x_0, y_0 are 0.1787. We use 50000 iterations to generate a random sequence using the Chaotic BWM. The chaotic behavior of the map is also analyzed using the Lyapunov exponent. The value of the Lyapunov exponent for the x series is 0.92695 and for y series is 0.802713. Since values of the Lyapunov exponent are positive for both series, it indicates that the chaotic nature is inherent in the proposed BWM. The chaotic behavior is also analyzed using chaos decision tree algorithm [57]. The value of permutation entropy is 5.6558, value of K [57] is 0.9917, and nature is chaotic for $x(t)$ series. Also, for the $y(t)$ series value of permutation entropy is 3.8776, value of K is 0.9962, and thus nature is chaotic. The results validate that the proposed BWM is chaotic in nature. The bifurcation diagram of the Chaotic BWM map is shown in Fig 1.

3 Proposed image encryption scheme

In this section, we discuss the encryption and decryption processes of the proposed scheme. The encryption and watermark embedding processes are shown in Fig 2(a) as follows:

Step 1: An input image $I(x, y)$ is bonded with the first random phase mask (RPM1) of size of the input image and its *FHT* is obtained. Mathematically, Step 1 is given by Eq (3).

$$E_1 = FHT^{p_1,q_1}(I(x, y)*(\text{RPM1})) \tag{3}$$

here p_1 *and* q_1 are fractional orders of the *FHT*.

Step 2: By virtue of the phase-truncation (PT) and phase-reservation (PR) processes, the phase reserved part of E_1 is stored as a private key (PK) and the phase truncated part is further processed in the encryption process. Mathematically, Step 2 is given by Eqs (4) and (5).

$$E_2 = PT(E_1) \tag{4}$$

$$PK = PR(E_1) \tag{5}$$

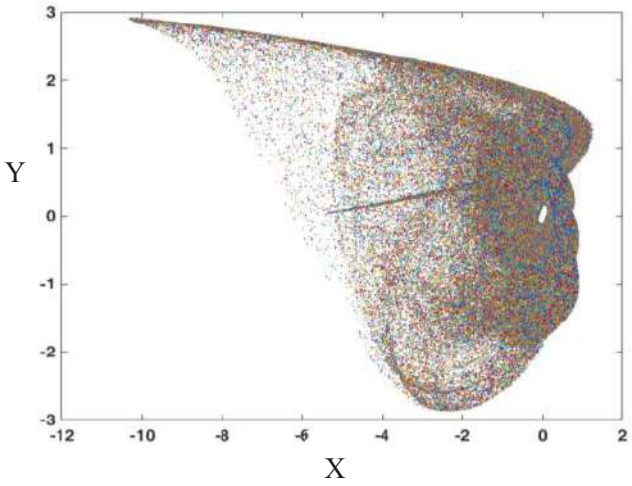

Fig 1. Bifurcation digram of the proposed Bird Wings Map.

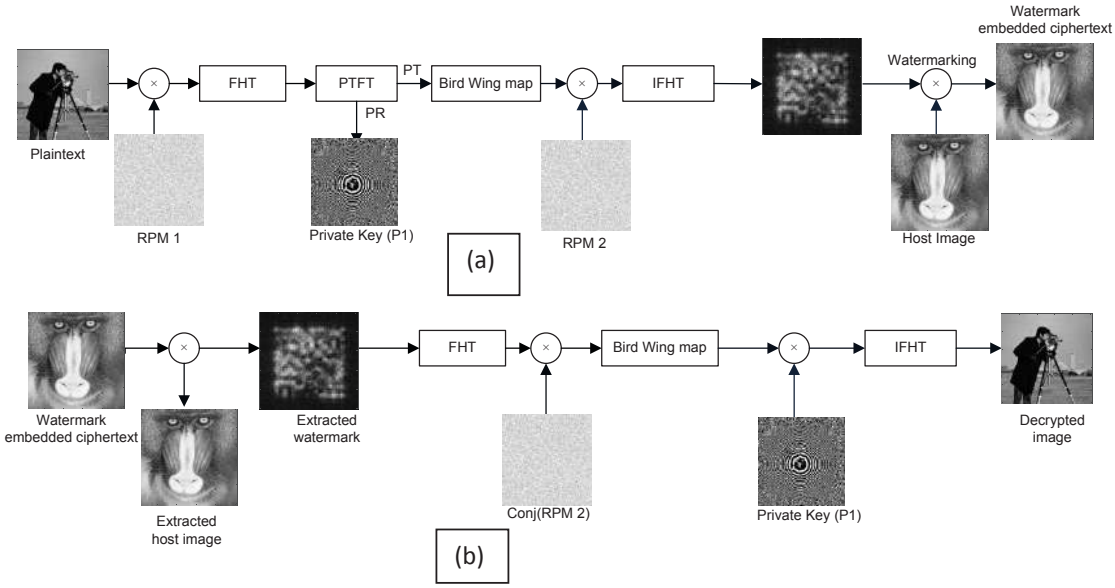

Fig 2. Schematic diagram of: (a) proposed encryption and watermarking processes, and (b) decryption and watermark extraction processes.

Step 3: E_2 undergoes the pixel scrambling operation using the BWM in order to improve the security of phase-truncation and phase reservation-based encryption algorithm. Mathematically, Step 3 is given by Eq (6).

$$E_3 = PS(E_2) \tag{6}$$

here *PS* stands for the pixel scrambling operation using the BWM.

Step 4: E_3 is bonded with the second random phase mask (RPM2) and its inverse *FHT* (*IFHT*) is obtained. Mathematically, Step 4 is described by Eq (7).

$$E_4 = IFHT^{p_2, q_2}(E_3 * \text{RPM2}) \tag{7}$$

here p_2 and q_2 are fractional orders of the *IFHT*.

Step 5: In order to confuse the attacker, we embedded the ciphertext E_4 in the host image of Baboon with an attenuation factor α. Value of the attenuation factor α varies between 0 and 2. For blind watermark, value of the attenuation factor should be close to zero. Mathematically, step 5 is given by Eq (8).

$$E_5 = \text{Host image} + \alpha * E_4 \tag{8}$$

E_5 contains the watermark embedded ciphertext and is transmitted over the communication network. The decryption process of the proposed algorithm is achieved by performing steps shown in Fig 2(b).

4 Results and Validation

In this section, we discuss results of the proposed security scheme. Simulations of the scheme have been performed in Matlab2022a, for various type of images but here we have presented results for Cameraman as the target image and Baboon as the watermarked image. To validate the robustness of our scheme, we also performed the statistical analysis such as correlation-coefficient and mean-square-error between the input and decrypted images. We also evaluated the information entropy for the input, encrypted, and decrypted images. The histogram and mesh plot are also presented. The scheme is also tested against basic cryptographic-, and contamination attacks. As the keys play an important role in any security algorithm, the key space for the scheme is also analyzed. The validation results are presented in Fig 3.

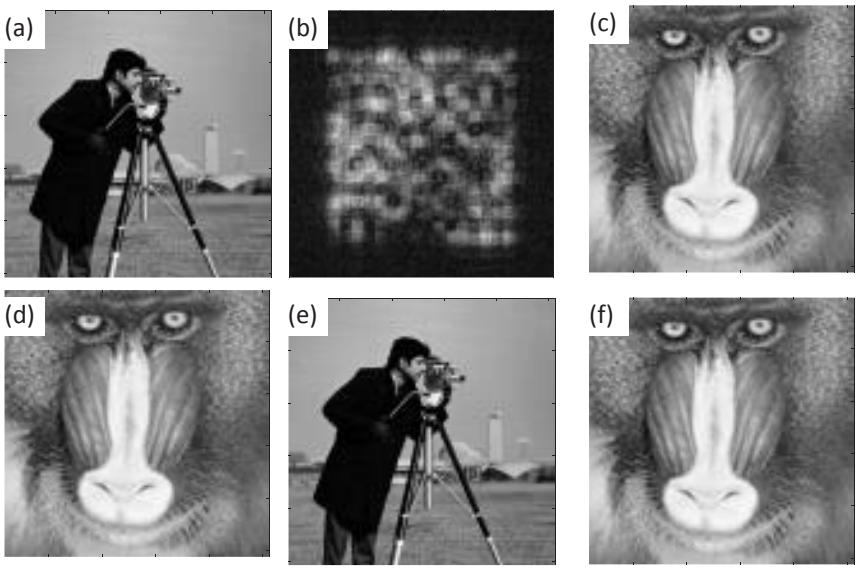

Fig 3. Result of the proposed algorithm; (a) Input image of Cameraman, (b) ciphertext image, (c) host image, (d) ciphertext embedded as watermark with attenuation factor, (e) decrypted image, and (f) extracted watermarked image.

4.1 Effect of the attenuation factor

As pointed out by Kishk and Javidi [60], the choice of attenuation factor α depends on the relative importance of keeping the appearance of the transmitted image unchanged and the ability to recover the hidden image under severe distortion. As the value of α is increased, the embedded watermark appears clearly on the host image. Result of the ciphertext embedding for different values of α are presented in Fig 4 for the values of being 0.1, 0.3, 0.6 and 0.9. The peak signal-to-noise ratio (*PSNR*) plots for the host-watermarked image pair, and the input-recovered image pair for different values of α are shown in Fig 5.

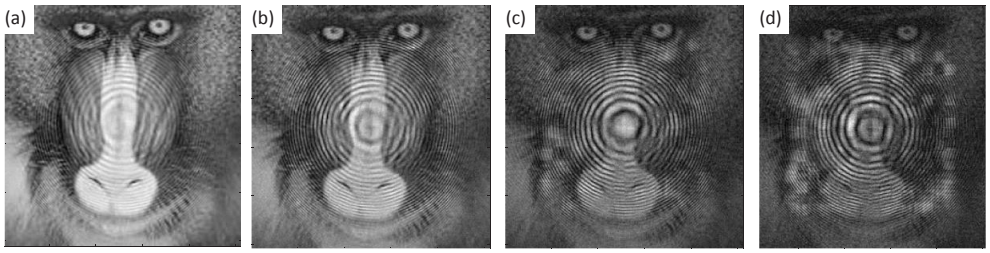

Fig 4. Ciphertext embedded as watermark in Baboon image with attenuation factor: (a) 0.1,(b) 0.3, (c) 0.6, and (d) 0.9, respectively.

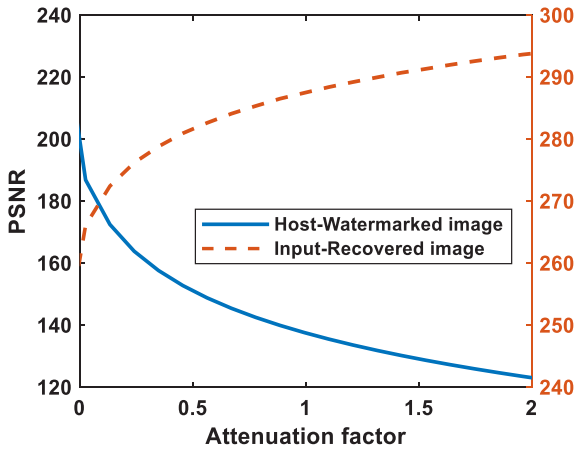

Fig 5. *PSNR* plot for the Cameraman image for the host-watermarked image pair, and input-recovered image pair.

4.2 Statistical analysis

Efficacy of the proposed scheme is also analyzed on the basis of statistical parameters such as mean-squared-error (*MSE*), correlation-coefficient (*CC*), peak signal-noise-ratio (*PSNR*), and information entropy [63,64]. The *CC*, *MSE*, and *PSNR* are defined as follows:

$$CC = \frac{cov(I_0, I_r)}{\sigma(I_0)\,\sigma(I_r)}$$

$$MSE = \frac{1}{N \times M} \sum_{x=1}^{N} \sum_{y=1}^{M} |I_0(x, y) - I_r(x, y)|^2$$

$$PSNR = 10 * \log\left(\frac{255^2}{\frac{1}{N \times M}\left[\sum_{x=0}^{N-1} \sum_{y=0}^{M-1} |I_0(x, y) - I_r(x, y)|^2\right]}\right)$$

where I_0, I_r are, respectively input and recovered images of size $N \times M$, cov is covariance, and σ is the stadard deviation. $I_0(i, j)$ is a pixel in row i and column j of the image I_0. Similarly, $I_r(i, j)$ is a pixel in row i and column j of image I_r. N and M are, respectively the number of rows and columns.

The *CC* between plaintext and recovered image is nearly 1, which indicates the faithful recovery of the decrypted image. The value of information entropy for grayscale image lies in the interval 0 to 8. The randomness inherent in the image is measured by using the information entropy. If the value of information entropy approaches 8, the image is highly random, and no neighboring pixels have relationship with each other. The value of the information entropies for input-, ciphertext-, watermark embedded ciphertext-, and

decrypted images are 7.01, 7.998, 7.547, and 7.024, respectively. The *MSE* between plaintext and ciphertext is $1.34 * 10^{6}$ and *MSE* between plaintext and recovered image is $1.3543 * 10^{-4}$ which shows that the *MSE* between plaintext and ciphertext are high whereas *MSE* between plaintext and recovered image is low. The results of *MSE* validate the efficacy of the proposed security algorithm. The value of the *PSNR* between plaintext and watermark embedded ciphertext is 9.087 dB, whereas value of the *PSNR* for plaintext and recovered image is 297dB. The statistical analysis results validate the efficacy and robustness of the security algorithm

4.3 Histogram and mesh plot analysis

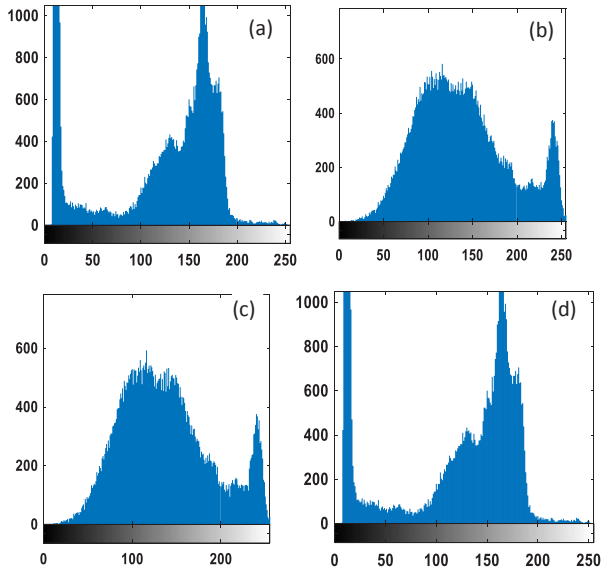

Fig 6. Histogram plots of: (a) plaintext image of Cameraman, (b) host image of Baboon, (c) host image after ciphertext embedding, and (d) decrypted image.

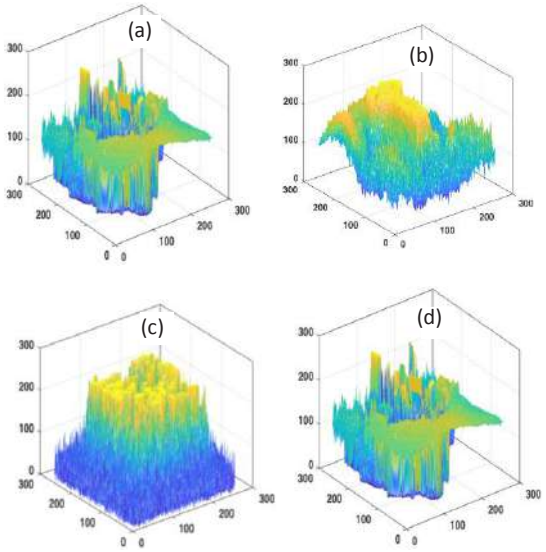

Fig 7. Mesh plots of: (a) plaintext image of Cameraman, (b) host image of Baboon, (c) host image after ciphertext embedding, and (d) decrypted image.

The histogram and mesh plots are used to assess the effectiveness of the proposed scheme. For a robust encryption algorithm histogram and mesh plots of plaintext and ciphertext should be different, whereas these should be similar for the plaintext and recovered image. The results of histogram and mesh plots are presented, respectively in Figs 6 and 7. The results demonstrate that the histogram and mesh plots do not reveal any information regarding the plaintext.

4.4 Contamination attack

In real-time transmission of data, some unwanted noise may pollute the transmitted data or some data may be lost due to network error [65]. The decrypted image with noise polluted ciphertexts is depicted in Fig 8 and the process of mixing noise in the ciphertext is described by Eq (9). The noise-attack results indicate that the proposed scheme resists a wide range of noise strength.

$$C = E_s + \beta G \tag{9}$$

where E_s is the watermark-embedded ciphertext, β is the noise strength, and G is random Gaussian noise with zero mean and unit variance. The decrypted images recovered from partial ciphertext are shown in Fig 9. The result of data loss indicates that decrypted result is faithful even if more than 60% of the data is lost.

4.5 Attack analysis

The security of the proposed scheme is tested for the basic cryptographic attacks such as the known-plaintext attack (KPA), chosen-plaintext attack (CPA), and iterative attack. Since the proposed scheme is asymmetric, the KPA and CPA are not likely to be successful. Nevertheless, we still test the vulnerability of the scheme to the KPA and CPA. In CPA attack, a Dirac delta image is chosen assuming that the attacker has access to the cryptosystem and tries to guess the decryption keys. In the KPA, the attacker has knowledge of the plaintext and cryptosystem, and tries to estimate the decryption keys. The proposed cryptosystem is asymmetric in nature and the private keys used in the decryption process change with the plaintext image. Therefore, these attacks do not work for the proposed cryptosystem. The results of the KPA and CPA are demonstrated in Fig 10. As is known, the PTFT-based cryptosystems are vulnerable to the iterative attack.

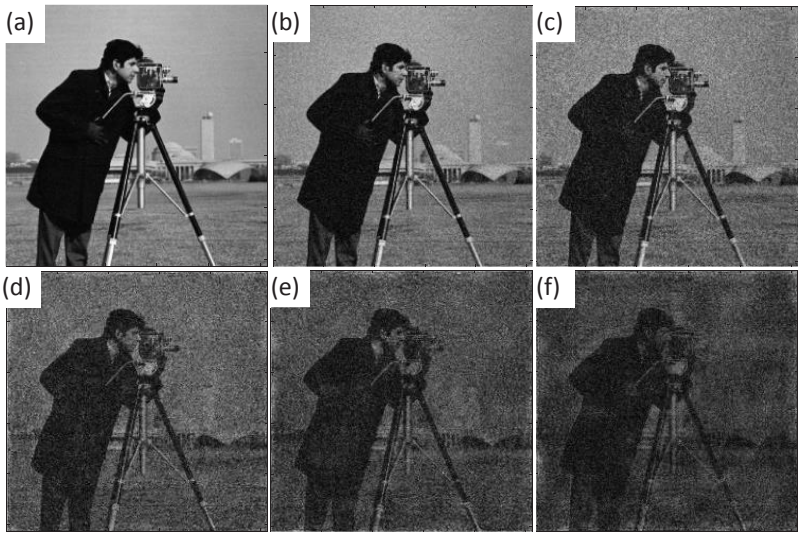

Fig 8. (a-f) Decrypted images retrieved from the ciphertext mixed with noise strength β = 10 dB, 50 dB, 100 dB, 200 dB,300 dB and 500 dB, respectively.

However, our proposed encryption algorithm enhances the security of phase truncation-, and phase reservation-based cryptosystem. We test the proposed cryptosystem for the iterative attack, and the results

are presented in Fig 11. The attack analysis results demonstrate that the proposed scheme is robust against basic cryptographic attacks, and does not reveal any valuable information regarding the plaintext.

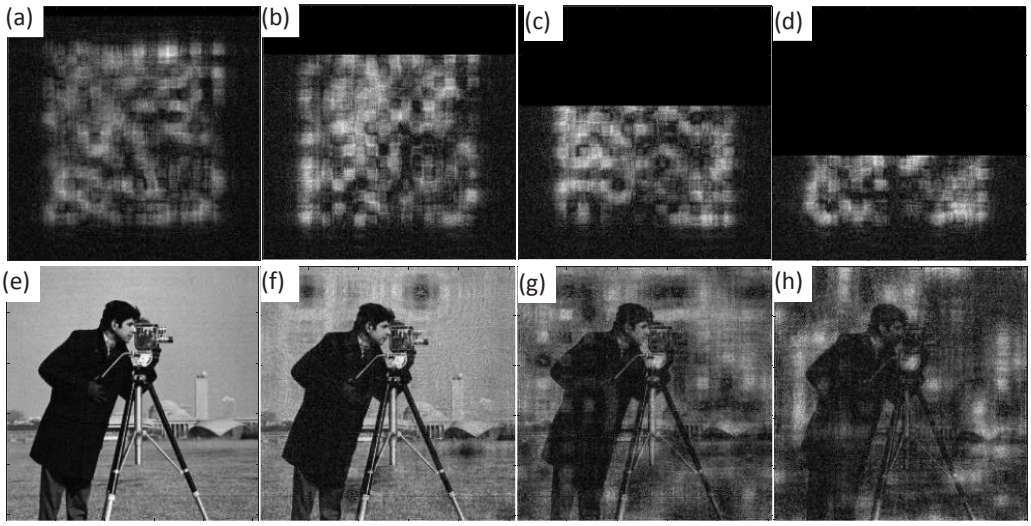

Fig 9. Data loss result; (a-d) ciphertext with data loss 5%, 20%, 40%, and 60%; and (e-h) corresponding recovered images.

4.6 Decryption key sensitivity analysis

In a robust security algorithm, decryption keys play an important role because the keys are strength of any cryptographic algorithm. In order to test security of the proposed algorithm, we analyze the sensitivity of the decryption keys. In the proposed algorithm, one phase, one private key, four orders of the *FHT*, and six parameters of chaotic BWM act as the decryption keys. The decrypted image retrieved from wrong keys are demonstrated in Fig 12. The decrypted images do not reveal any valuable information regarding the plaintext until all correct decryption keys are used in the decryption process. The chaotic parameters are sensitive to the extent of 10^{-9}. So, the total key space of the proposed algorithm is $10^{60} * 255^{256}$. The Key space indicates that it is very difficult to breach the proposed cryptosystem.

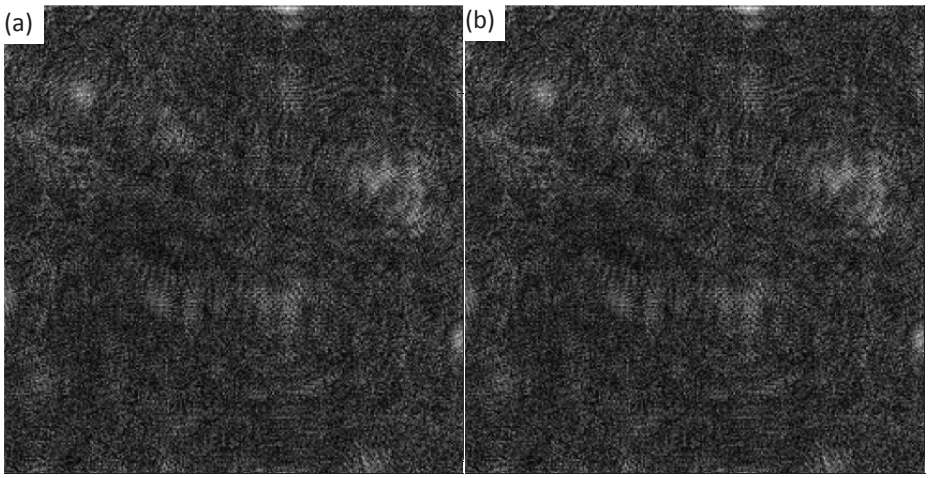

Fig 10. Recovered image in case of (a) known-plaintext attack, and (b) chosen-plaintext attack.

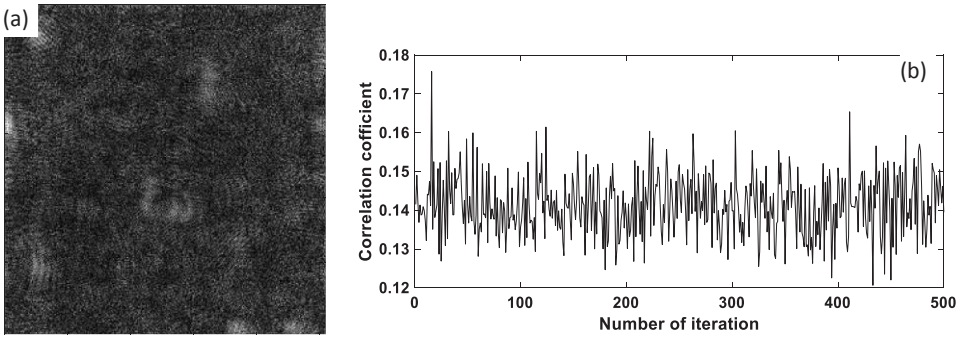

Fig 11. Iterative attack on the proposed encryption algorithm: (a) Recovered image after 500 iterations, and (b) Plot of *CC* versus number of iterations.

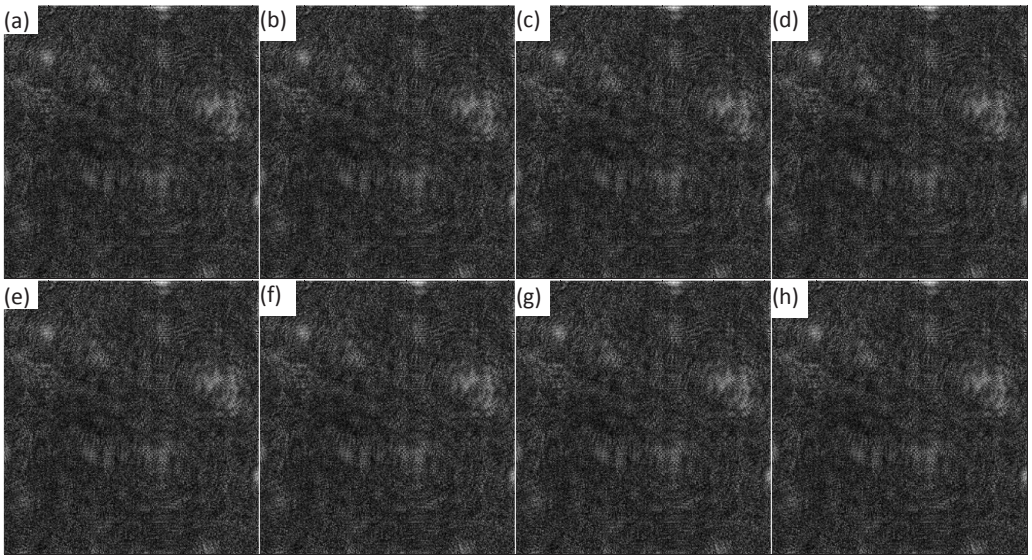

Fig 12. Retrieved image for: (a-f) incorrect value of the parameters, $a = 0.9 \times 10^{-9}$, $b = -0.60239 \times 10^{-9}$, $c = 2 \times 10^{-9}$, $d = 0.5 \times 10^{-9}$, $x = 0.1787 \times 10^{-9}$, and $y = 0.178 \times 10^{-9}$, (g) incorrect value of the *FHT* order $p = 0.5 \times 10^{-2}$, and (h) wrong private key.

5 Conclusion

In conclusion, this paper shows an enhanced security of the phase truncation and phase reservation-based algorithm through the utilization of the newly developed Birds Wing Map and watermark embedding in the fractional Hartley domain. A pair of grayscale images, namely Cameraman and Baboon, were employed, with Cameraman serving as the target image and Baboon as the host image in the watermarking process. The proposed scheme underwent rigorous testing against various statistical attacks, including mean-squared-error, correlation coefficient, information entropy, and peak signal-to-noise ratio. Furthermore, the scheme was validated using histogram and mesh plots to assess its performance. Real-time attacks such as noise and occlusion attacks were also applied to evaluate the robustness of our proposed scheme. Additionally, the scheme was tested against cryptographic attacks, such as known-plaintext, chosen-plaintext, and special iterative attack, to assess its resilience in the context of information security. The key sensitivity analysis was conducted to analyze the key space of the proposed scheme. Results demonstrate the robustness and

effectiveness of the proposed scheme. Therefore, the proposed scheme is suitable for secure image processing applications.

With rapidly astonishing advances in artificial intelligence, it seems that no cryptosystems (except probably quantum cryptosystems) are safe from attacks. At the same time, artificial intelligence tools also allow us to design much better security systems [66-70]. We also plan to explore the exciting possibilities offered by these tools.

References

1. Hasib A A, Haque, A A Md M, A comparative study of the performance and security issues of AES and RSA crypog -raphy, in 2008 Third Int'l Conference on Convergence and Hybrid Information Technology, Busan, Korea: IEEE, Nov 2008, pp 505–510; doi: 10.1109/ICCIT.2008.179.
2. Biryukov A, The boomerang attack on 5 and 6-round reduced AES, in Advanced Encryption Standard – AES, Hutchison D, Kanade T, Kittler J, Kleinberg J M, Mattern F, Mitchell J C, Naor M, Nierstrasz O, Pandu Rangan C, Steffen B, Sudan M, Terzopoulos D. Tygar D, Vardi M Y, Weikum G, Dobbertin H, Rijmen V, Sowa A, (Eds), Springer Berlin Heidelberg, 2005, pp 11–15; doi:10.1007/11506447_2.
3. Kou W, Data Encryption Standards, in *Networking Security and Standards*, Kou W, Ed., The Springer International Series in Engineering and Computer Science, Boston, MA: 1997, pp. 49–67. doi: 10.1007/978-1-4615-6153-8_4.
4. Rivest R L, Shamir A, Adleman L, A method for obtaining digital signatures and public-key cryptosystems, *Commun ACM*, 21(1977)120–134.
5. Refregier P, Javidi B, Optical image encryption based on input plane and Fourier plane random encoding, *Opt Lett*, 20(1995)767–769.
6. Al Falou A, Brosseau C, Optical image compression and encryption, *Adv Opt Photon*, 1(2009)589–636.
7. Kumar A, Singh M, Singh K, Speckle coding and digital data security applications, in 'Advances in Speckle Metrology and Related Techniques', Chap 6, pp 239–299, (ed) Kaufmann G H, (Wiley-VCH Weinheim), 2011.
8. Kumar P, Joseph J, Singh K, Double random phase encoding based optical encryption systems using some linear canonical transforms: weaknesses and countermeasures, in ' Linear canonical transforms: Theory and applications' (eds) Healy J J, Kutay M A, Ozaktas M, Sheridan J T, (Springer N Y), 2016, 367–396.
9. Chen W, Javidi B, Chen X, Advances in optical security systems, *Adv Opt Photon*, 6(2014)120–155.
10. Al Falou A(Ed), Advanced Secure Optical Image Processing for Communications, (IOP Publ Bristol U K), 2018.
11. Nishchal N K, Optical Cryptosystems,(IOP Publ. Bristol U K), 2000.
12. Unnikrishnan G, Singh K , Double random fractional Fourier-domain encoding for optical security, *Opt Eng*, 39(2000)2853–2859.
13. Unnikrishnan G, Joseph J, Singh K, Optical encryption by double-random phase encoding in the fractional Fourier domain, *Opt Lett*, 25(2000)887–889.
14. Situ G, Zhang J, Double random-phase encoding in the Fresnel domain, *Opt Lett*, 29(2004)1584–1586.
15. Shi Y, Situ G, Zhang J, Multiple-image hiding in the Fresnel domain, *Opt Lett*, 32 (2007)1914–1916.
16. Maan P, Singh H, Kumari A C, Symmetric cryptosystem to secure images utilizing chaotic deterministic phase mask in Fresnel transform domain employing singular value decomposition, *Proc Comput Sci*, 167(2020)860–869.
17. Rodrigo J A, Alieva T, Calvo M L, Gyrator transform: properties and applications, *Opt Express*, 15(2007)2190–2203.
18. Abuturab M R, Information authentication system using interference of two beams in gyrator transform domain, *Appl Opt*, 52(2013)5133–5142.
19. Singh H, Yadav A K, Vashisth S, Singh K, Fully phase image encryption using random-structured phase masks in gyrator domain, *Appl Opt*, 53(2014)6472–6481.
20. Kumar J, Singh P, Yadav A K, Kumar A, Asymmetric image encryption using gyrator transform with singular value decomposition, in Engineering Vibration, Communication and Information Processing, Ray K, Sharan S N, Rawat S, Jain S K, Srivastava S, Bandyopadhyay A, (eds), (Singapore: Springer), 2019, pp 375–383.

21. Chen L F, Zhao D, Optical image encryption with Hartley transform, *Opt Lett*, 31(2006)3438–3440.
22. Zhao D, Li X, Chen L, Optical image encryption with reduced fractional Hartley transform, *Opt Commun*, 281(2008)5326–5329.
23. Singh P, Yadav A K, Singh K, Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition, *Opt Lasers Eng*, 91(2017)187–195.
24. Yadav A K, Singh P, Saini I, Singh K, Asymmetric encryption algorithm for color images based on fractional Hartley transform, *J Mod Opt*, 66(2019)629–642.
25. Kaur G, Agarwal R, Patidar V, Multiple image encryption with fractional Hartley transform and robust chaotic mapping, in 2019 6th Int'll Confer on 'Signal Processing and Integrated Networks (SPIN)', Mar. 2019, pp. 399–403. doi: 10.1109/SPIN.2019.8711777.
26. Zhou N R, Wang Y, Gong L, Novel optical image encryption scheme based on fractional Mellin transform, *Opt Commun*, 284(2011)3234–3242.
27. Vashisth S, Singh H, Yadav A K, Singh K, Image encryption using fractional Mellin transform, structured phase filters, and phase retrieval, *Optik*, 125(2014)5309–5315.
28. Singh P, Yadav A K, Singh K, Security-analysis of a nonlinear mask-based cryptosystem in fractional Mellin transform, *Asian J Phys*, 30(2021)1397–1406.
29. Sachin, Singh P, Singh K, Nonlinear image authentication algorithm based on double fractional Mellin domain, Nonlinear Dynamics 2023, doi.org/10.1007/s11071-023-08540-5.
30. Kumar R, Sakshi, Singh K, An asymmetric optical cryptosystem based on Radon transform for phase image encryption, *Asian J Phys*, 31(2022) A1–A12.
31. Peng X, Wei H, Zhang P, Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain, *Opt Lett*, 31(2006)3261–3263.
32. Barrera J F, Vargas C, Tebaldi M, Torroba M, Chosen-plaintext attack on a joint transform correlator encrypting system, *Opt Commun*, 283(2010)3917–3921.
33. Zhang Y, Xiao D, Wen W, Liu H, Vulnerability to chosen-plaintext attack of a general optical encryption model with the architecture of scrambling-then-double random phase encoding, *Opt Lett*, 38(2013)4506–4509.
34. Peng X, Chang P, We H, Yu B, Known-plaintext attack on optical encryption based on double random phase keys, *Opt Lett*, 31(2006)1044–1046.
35. Gopinathan U, Monaghan D S, Naughton T J, Sheridan J T , A known-plaintext heuristic attack on the Fourier plane encryption algorithm, *Opt Express*, 14(2006)3181–3186.
36. Tashima H, Takeda M, Suzuki H, Obi T, Yamaguchi M, Ohyama N, Known-plaintext attack on double random phase encoding using finger print as key and a method for avoiding the attack, *Opt Express*, 18(2010)13772–1381.
37. Nakano K, Takeda M, Suzuki H, Yamaguchi M, Security analysis of phase-only DRPE based on known-plaintext attack using multiple known plaintext–ciphertext pairs, *Appl Opt*, 53(2014)6435–6443.
38. Carnicer A, Usategui M M, Arcos S, Juvells I, Vulnerability to chosen-ciphertext attacks of the optical encryption schemes based on double random phase keys, *Opt Lett*, 30(2005)1644–1646.
39. Alligood K T, Saeur T D, Yorke J A, Chaos: An Introduction to Dynamical Systems, (Springer N Y), 2001.
40. Larger L, Goedgebuer, J P, Delorme F, Optical encryption system using hyperchaos generated by an optoelectronic wavelength oscillator, *Phys Rev E*, 57(1998)6618–6624.
41. Cuenot J B, Larger L, Goedgebuer J P, Rhodes W T , Chaos shift keying with an optoelectronic encryption system using chaos in wavelength, IEEE *J Quant Electron*, 37(2001)849–855.
42. Pareek N K, Patidar V, Sud K K, Image encryption using chaotic logistic map, *Image Vis Comput*, 24(2006)926–934.
43. Lang J, Tao R, Wang Y, Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function, *Opt Commun*, 283(2010)2092–2096.
44. Wang X, Zhao J, Liu H, Anew image encryption algorithm based on chaos, *Opt Commun*, 285(2012)562–566.
45. Liu J, Jin H, Ma L, Jin W, Optical color image encryption based on computer generated hologram and chaotic theory, *Opt Commun*, 307(2013)76–79.

46. Abuturab M R, Group-multiple-image encoding and watermarking using coupled logistic maps and gyrator wavelet transform, *J Opt Soc Am A*, 32(2015)1811–1820.
47. Liu X, Mei W, Du H, Simultaneous image compression, fusion and encryption algorithm based on compressive sensing and chaos, *Opt Commun*, 366(2016)22–32.
48. Sachin, Archana, Singh P, 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*, Ray K, Roy K C, Toshniwal S K, Sharma H, Bandyopadhyay A, Eds, (Springer Singapore), 2021, pp. 249–262. doi: 10.1007/978-981-15-7561-7_20.
49. Archana, Sachin, Singh P, Cryptosystem based on triple random phase encoding with chaotic Henon map, in *Proceedings of International Conference on Data Science and Applications*, K. Ray K, K. C. Roy K C , S. K. Toshniwal S K, Sharma H, Bandyopadhyay A, Eds., in Lecture Notes in Networks and Systems, vol. 148, (Singapore: Springer), 2021, pp. 73–84. doi: 10.1007/978-981-15-7561-75.
50. Ai-hong Zhu and Lian Li, Improving for chaotic image encryption algorithm based on logistic map, in *2010 The 2nd Conference on Environmental Science and Information Application Technology*, Wuhan, China: IEEE, Jul. 2010, pp. 211–214. doi: 10.1109/ESIAT.2010.5568374.
51. Sachin, Singh P, A novel chaotic Umbrella map and its application to image encryption, *Opt Quant Electron*, 54 (2022), Art ID: 266; doi: 10.1007/s11082-022-03646-3.
52. Abundiz-Pérez F, Cruz-Hernández C, Murillo-Escobar M A, López-Gutiérrez R M, Arellano-Delgado A, A fingerprint image encryption scheme based on hyperchaotic Rössler map, *Math Probl Eng,* vol 2016, pp 1–15, 2016; doi. 10.1155/2016/2670494.
53. Rakheja P, Vig R, Singh P, Optical asymmetric watermarking using 4D hyperchaotic system and modified equal modulus decomposition in hybrid multi resolution wavelet domain, *Optik*, 176(2019)425–437.
54. Dou Y, Liu X, Fan H, Li M, "Cryptanalysis of a DNA and chaos-based image encryption algorithm, *Optik*, 145 (2017); doi: 10.1016/j.ijleo.2017.08.050.
55. Chen H, Liu Z, Tanougast C, Liu F, Blondel W, A novel chaos based optical cryptosystem for multiple images using DNA-blend and gyrator transform, *Opt Lasers Eng*, 138(2021) Art ID: 106448; doi: 10.1016/j.optlaseng.2020.106448.
56. Ding K, Xu X, Chaotic synchronization of modified discrete-time Tinkerbell systems, Discrete Dynamics in Nature and Society, vol 2016, pp 1–7, 2016; doi. 10.1155/2016/5218080.
57. Toker D, Sommer F T, D'Esposito M, A simple method for detecting chaos in nature, *Commun Biology*, 3(2020) 11; doi. 10.1038/s42003-019-0715-9.
58. Qin W, Peng X, Asymmetric cryptosystem based on phase-truncated Fourier transforms, *Opt Lett*, 35(2010)118; doi.: 10.1364/OL.35.000118.
59. Xiong Y, Kumar R, Quan C, Security analysis on an optical encryption and authentication scheme based on phase-truncation and phase-retrieval algorithm, *IEEE Photon J*, 11(2019)1–14.
60. Kishk S, Javidi B, Information hiding technique with double phase encoding, *Appl Opt*, 41(2002)5462–5470.
61. Yadav A K, Vashisth S, Singh H, Singh K, A phase-image watermarking scheme in gyrator domain using devil's vortex Fresnel lens as a phase mask, *Opt Commun,* 344(2015)172–180.
62. Singh P, Yadav A K, Singh K, Saini I, Asymmetric watermarking scheme in fractional Hartley domain using modified equal modulus decomposition, *J Optoelectron Adv Mater*, 21(2019)484–491.
63. Sachin, Kumar R, Singh P, Multiuser optical image authentication platform based on sparse constraint and polar decomposition in Fresnel domain, *Phys Scripta*, 97(2022) Art ID: 115101; doi. 10.1088/1402-4896/ac925d.
64. Rakheja P, Vig R, Singh P, Double image encryption using 3D Lorenz chaotic system, 2D non-separable linear canonical transform and QR decomposition, *Opt Quant Electron*, 52(2020)103; doi. 10.1007/s11082-020-2219-8.
65. Gong L, Liu X, Zheng F, Zhou N X Flexible multiple-image encryption algorithm based on log-polar transform and double random phase encoding technique, *J Mod Opt*, 60(2013)1074–1082.
66. Wang Y, Ren Z, Zhang L, Li D, Li X, 3Dimage hiding using deep demosaicking and computational integral imaging, *Opt Lasers Eng*, 148(2022) Art ID:106722; doi.org/10.1016/j.optlaseng.2021.106772.

67. Wang X, Wei H, Jin M, Xu B, Chen J, Experimental optical encryption based on random mask encoding and deep learning, *Opt Express*, 30(2022)11165–11173.
68. Zhao Q, Li H, Yu Z, Woo C M, Zhong T, Cheng S, Zheng Y, Liu H, Tian J, Lai P, Speckle-based optical cryptosystem and its application for human face recognition via deep learning, *Adv Sci*, 2022. Art ID: 2202407; doi.org/10.1002/advs.202202407.
69. Zhuang X, Yan A, Deep-learning-based ciphertext-only attack on optical cryptosystem, *Opt Laser Technol*, 157(2023) 108744; doi.org/10.1016/j.optlastec.2022.108744.
70. Ahmadi K, Carnicer A, Optical visual encryption using focused beams and convolutional neural networks, *Opt Lasers Eng*, 161(2023)107321; doi.org/10.1016/j.optlaseng.2022.107321.

[*Received*: 15.04.2023; *accepted*: 30.04.2023]