Triple Color Image Encryption Using Hybrid Digital/Optical Scheme Supported by High-Order Chaos

Rusul Abdulridha Muttashar[*], Raad Sami Fyath[**]

*Department of Computer Engineering, College of Engineering, Al-Nahrain University, Iraq
Email: rusul97.abd@gmail.com
https://orcid.org/0000-0002-0348-1685

**Department of Computer Engineering, College of Engineering, Al-Nahrain University, Iraq
Email: raad.s.fyath@nahrainuniv.edu.iq
https://orcid.org/0000-0002-1029-3471

Abstract

Image security has attracted increasing interest, wherein image encryption is an effective and direct method that can be implemented using digital, optical, or hybrid techniques. The challenge is how to design a high-speed, and high-security level multiple color image encryption scheme which makes use of advanced techniques such as chaotic system and deep learning. This issue is addressed in this paper where a nine-dimensional (9D) chaotic-based Hybrid Digital/Optical Encryption (HDOE) scheme is proposed for triple color images. The scheme consists of cascading digital and optical encryption parts controlled separately by the chaotic sequences. The nine chaotic sequences are grouped into three sets, and each set is responsible for the encryption of one of the RGB channels independently. The digital part uses fusion, XOR operation, and scrambling. The optical part uses two independent chaotic phase masks in the optical Fourier transforms domain. A Denoising Convolution Neural Network (DnCNN) is designed to assist the robustness of the decrypted images against Gaussian noise. The simulation results reveal that the proposed triple-image HDOE scheme offers entropy of 7.9991, 7.9987, and 7.9991 bits for R, G, and B channels, respectively, and infinite Peak Signal-to-Noise Ratio (PSNR) for the decrypted images.

Keywords- 9D-chaotic system, triple color image encryption, HDOE schemes, DnCNN.

I. INTRODUCTION

Encryption-based secure image transmission is an important research topic for advanced multimedia, healthcare, and Internet applications [1]. Recently, there has been increasing interest in implementing gray- and color-image encryption using optical technology to achieve high-speed operation [2][3][4]. The Optical Encryption (OE) process treats the image directly as a two-dimensional (2D) object and therefore, it does not use image digitization as done in the Digital Encryption (DE) counterpart [5][6]. Further, OE methods have some characteristic features due to the used optical devices [7][8]. For example, the amplitude and phase information of all image pixels can be processed simultaneously. Further, image encryption can be processed in various matrix spaces such as phase and polarization, which offers additional security level and reliability. The general structure of OE schemes consists of lasers, spatial light modulators (SLMs), lenses, beam splitters, and detectors [7] as shown in Fig. 1. A simple presentation for this figure is given in Fig. 2 which depicts a Double Random Phase Mask (DRPM)-based encryption scheme. Spatial light modulator is a general term describing devices that are used to modulate the amplitude, phase, or polarization of light waves. The SLM produces transparency controlled by the computer according to the image or mask required to modulate the light beam [9]. It is worth mentioning here that the operation of the OE scheme may be assisted by DE algorithms to support certain functions which cannot be implemented using the available optical and/or photonic techniques [10][11][12]. In this case, the system is called a Hybrid Digital/Optical Encryption (HDOE) scheme.

The main challenge facing researchers working in optical image encryption is how to design efficient OE and HDOE schemes incorporating the following issues (which have been usually suggested as future work in their publications).

i. Developing the existing designs or suggesting new designs to support multiple color image encryption. Most of the related work reported in the literature has been concerned mainly with single color image [13], and to less extent for double color image [10]. Very few works have been reported on multiple color images [2].

ii. Incorporating advanced encryption-assisted techniques such as Deep Learning (DL) and chaos. These two techniques have already been adopted in digital image encryption and need to be modified for OE. Few publications have been appeared in the literature describing the design of DL-assisted OE schemes, which concerned mainly with single color image [14]. Although chaotic dynamical systems have already been adopted in OE, the dimension (order) of these dynamics does not exceed five. This is also true for DE counterparts. A higher-order chaotic system is expected to play a key role in increasing the encryption level and robustness.

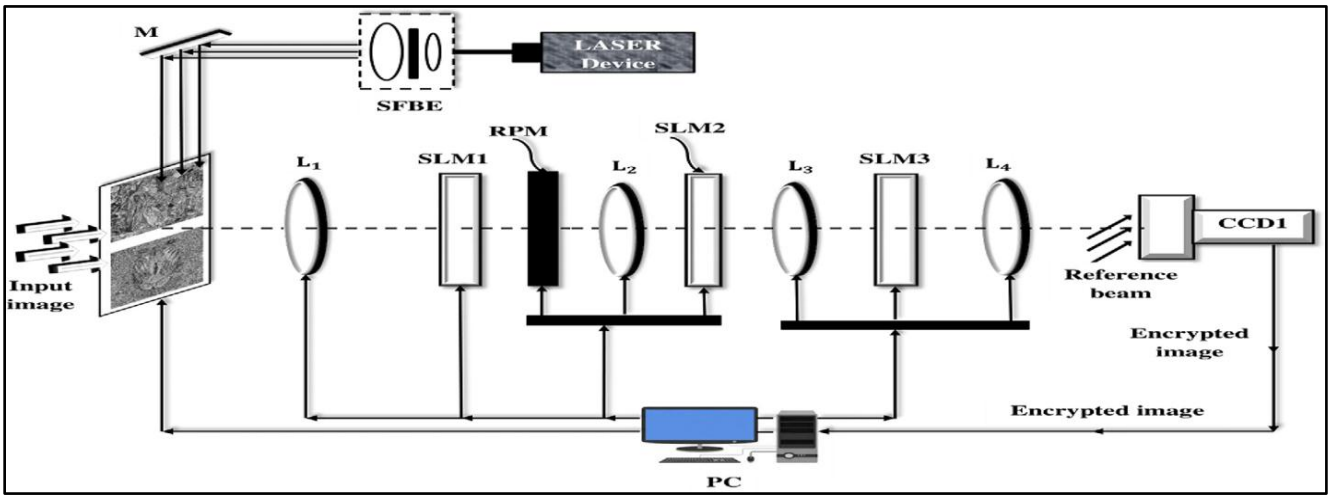


Fig. 1. General optical configuration for the image encryption method [15]. SLM: Spatial Light Modulator), SFBE: Spatial Filter Beam Expander assembly, M: Plane Mirror), L_1, L_2, L_3, L_4: Various Lenses), PC: Personal Computer, CCD: Charge-Coupled Device

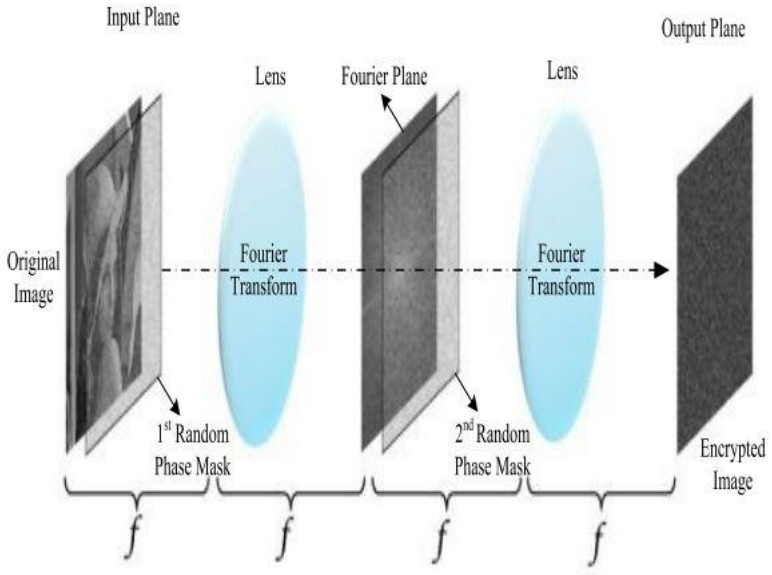


Fig. 2. Simplified schematic diagram of a Double Random Phase Mask (DRPM)-based encryption scheme

iii. Recently, there has been increasing interest in using chaotic dynamical systems in the design of image encryption/decryption schemes to increase the level and robustness of security [16][17]. The dynamic of a chaotic system is very sensitive to initial

conditions. To ensure a successful image decryption, two identical chaotic sources with the same initial conditions are used, one on the encryption side and the other on the authorized user decryption side. Different chaotic-based algorithms have been proposed for DE [18][19], OE [20][21][22], and hybrid HDOE [23] [15] [16]. Increasing the dimension (i.e., order) of the chaotic system will play a key role and enhance the encryption efficiency. For example, Kumar et al. proposed in 2020 an HDOE encryption algorithm for a double color image using a three-dimensional (3D) chaotic map and 2D-multiple parameter Fractional Fourier Transform (FrFT) [15]. Man et al. proposed a double grayscale image encryption algorithm based on dynamic adaptive diffusion, five-dimensional (5D) chaos, and CNN [10]. In 2022, Zhang et al. [24] proposed a secure double grayscale image encryption scheme based on a novel fusion application of Compressive Sensing (CS), Double Random Phase Encoding (DRPE) and optical transformation technology. Scanning the literature for optical image encryption reveals that most of the related work were concerned mainly with a single-color image, and to less extent with a double color image. Very few work were reported for multiple color images [2]. Further, although chaotic dynamical systems already adopted in OE, the dimension (order) of these dynamics does not exceed five. This is also true for DE counterparts. A higher-order chaotic system is expected to play a key role in increasing the encryption level and robustness. A few Triple-Image Encryptions (TIE) algorithms, that encrypt three images synchronously, were also proposed for both OE [25][26] and DE [27][29] schemes. Some of these algorithms are supported by less than 5-order chaos.

This paper proposes a high-security 9D chaotic-based HDOE scheme for a color triple image supported by a Denoising Convolutional Neural Network (DnCNN). The network can handle Gaussian denoising with unknown noise levels (i.e., blind Gaussian denoising). The 9D chaotic system offers a high–security level and high robustness against various security attacks.

II. PROPOSED TRIPLE IMAGE ENCRYPTION

This section presents the main concepts of the proposed encryption and decryption schemes for color triple images. The explanation is supported by simulation results corresponding to a triple-color image plaintext of a sailboat, Lena, and Baboon images, each of 256X256 dimensions. The proposed encryption scheme is classified as an HDOE scheme and constructed by cascading a Digital Encryption Subscheme (DEsS) with an Optical Encryption Subscheme (OEsS) as shown in Fig. 3. A 9D chaotic system is used to control the encryption process with each of three chaotic sequences are grouped in one set which is directed independently to one of the RGB color channels. One sequence is used to construct a chaotic image for XOR operation in the DEsS and the other two sequences are used the construct the two independent Chaotic Phase Masks (CPMs) implemented in the optical Fourier transform domain of the OEsS. A DL-based denoising system is also designed to enhance the performance of the decryption process against Gaussian noise introduced in the transmission channel. The nine dynamical equations describing the chaotic system are described in [25] and not repeated here for space limitation.

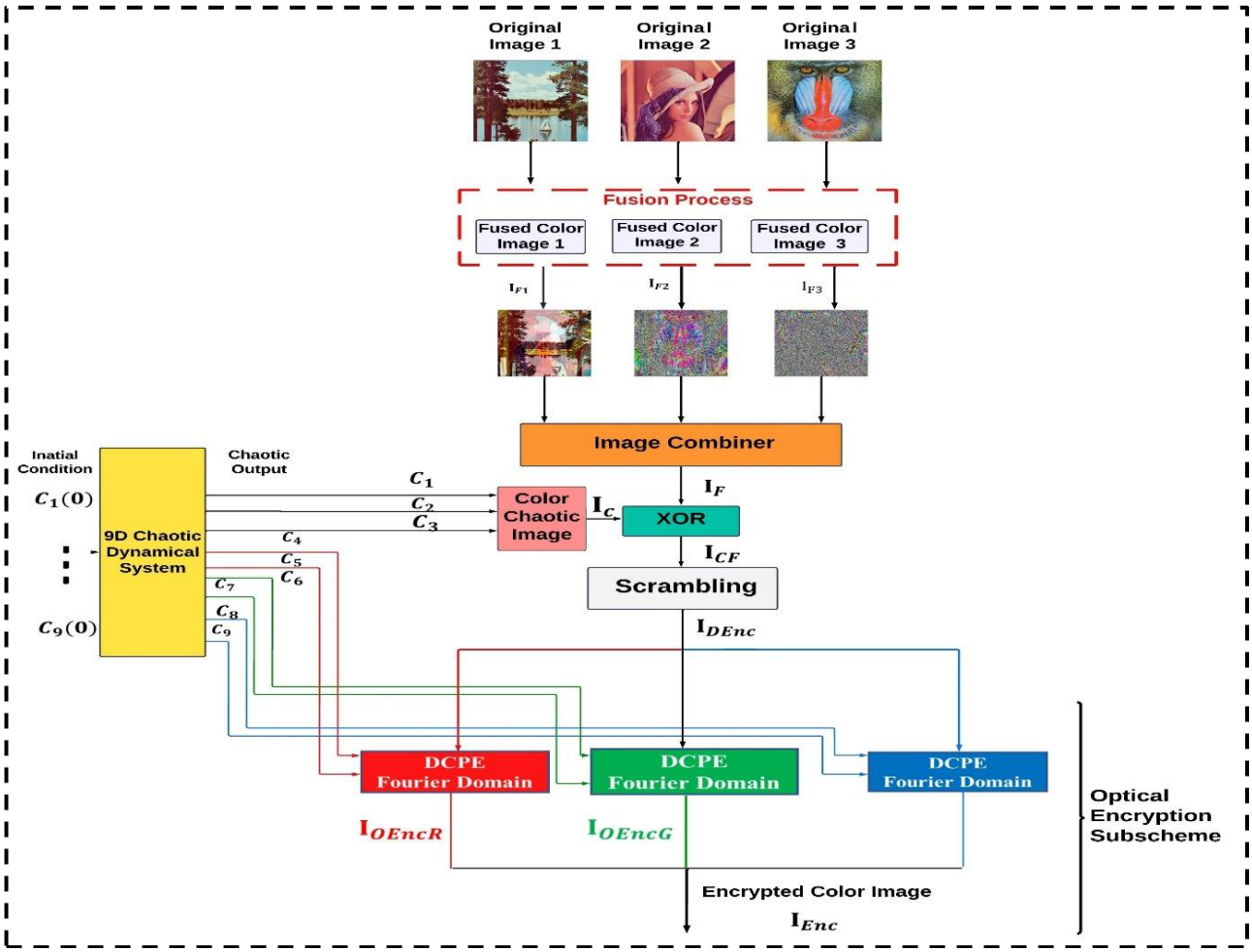


Fig. 3. Blok diagram of the proposed HDOE scheme for triple image encryption process

A. Digital Encryption Subscheme

The following steps are followed in this subscheme.

i. A novel fusion process is applied to the input triple color image yielding three new color images I_{F1}, I_{F2} and I_{F3}. This process is adopted according to the amount of information carried by various binary bits of image pixels. Figure 4 illustrates the proposed triple fusion process where b_j (j= 1, …, 8) represents the jth bit corresponding to the intensity of a single pixel of the image. Fig. 5 shows the resultant high-bit, medium-bit, and low-bit fused images I_{F1}, I_{F2} and I_{F3}, respectively, for the input triple image.

ii. The image combiner gathers the three fused images I_{F1}, I_{F2} and I_{F3} to construct a single fused image I_F. The construction process is displayed graphically in Fig. 6a. The third fused image I_{F3} is divided into two equal sub-images, $I_{F3\text{-}I}$ and $I_{F3\text{-}II}$. The fused image I_F is shown in Fig. 6b which has a size of 512x384.

iii. A virtual chaotic color image I_C is constructed as an encryption key by using three of the nine chaotic system outputs (C_1, C_2 and C_3), where each output is responsible for one of the RGB channels. The chaotic image I_C is XORing with the color fused image I_F to get a chaotic fused image I_{CF} (Fig. 7a). The chaotic gray images I_{CR}, I_{CG} and I_{CB}, corresponding to the RGB channels, are constructed based on the sequences C_1, C_2 and C_3, respectively. This is done after using integer sequencing according to Equations (1) to (3)

$$I_{CR}(i) = fix(mod(C_1(i) \times 10^{15}, 255) \quad (1)$$

$$I_{CG}(i) = fix(mod(C_2(i) \times 10^{15}, 255) \quad (2)$$

$$I_{CB}(i) = fix(mod(C_3(i) \times 10^{15}, 255) \quad (3)$$

vi. Finally, a random image scrambling technique is applied to the image I_{CF} to produce the encrypted digital image I_{DEnc} (Fig. 7b).

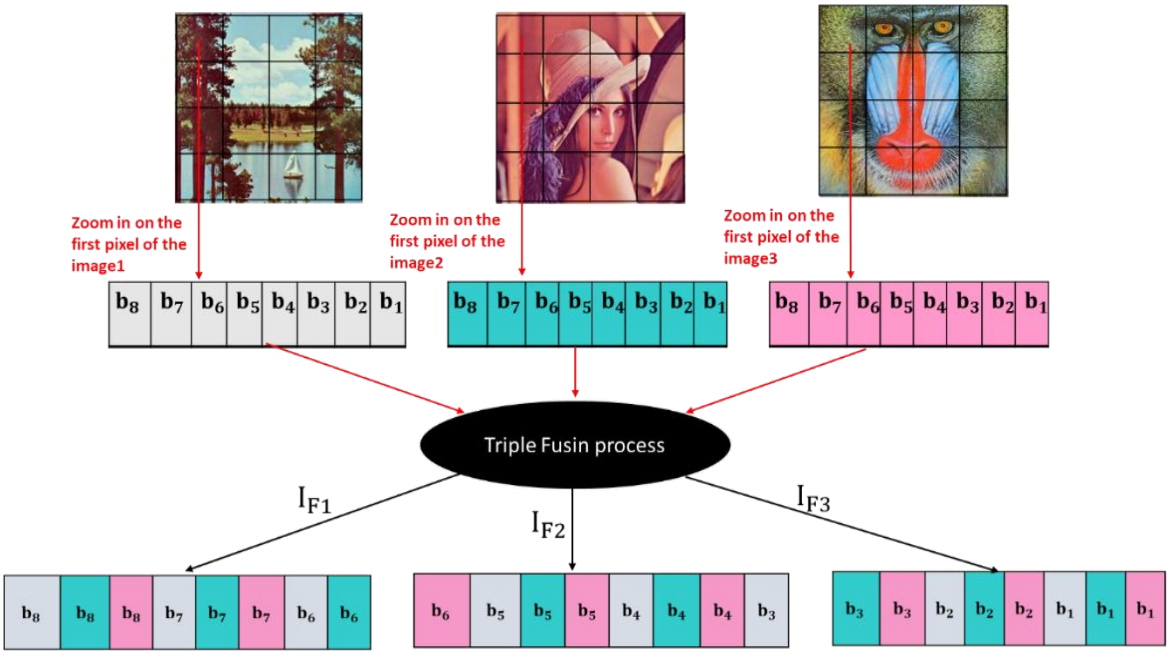


Fig. 4. Triple fusion process.

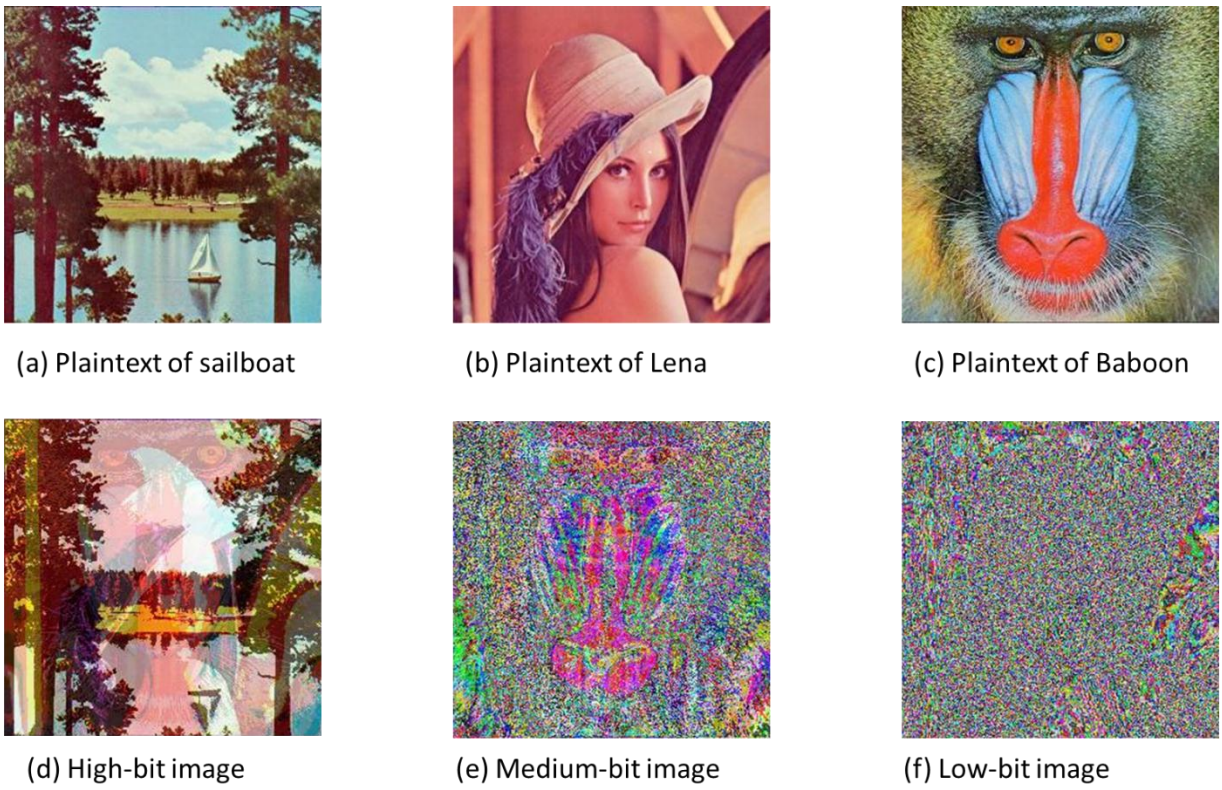
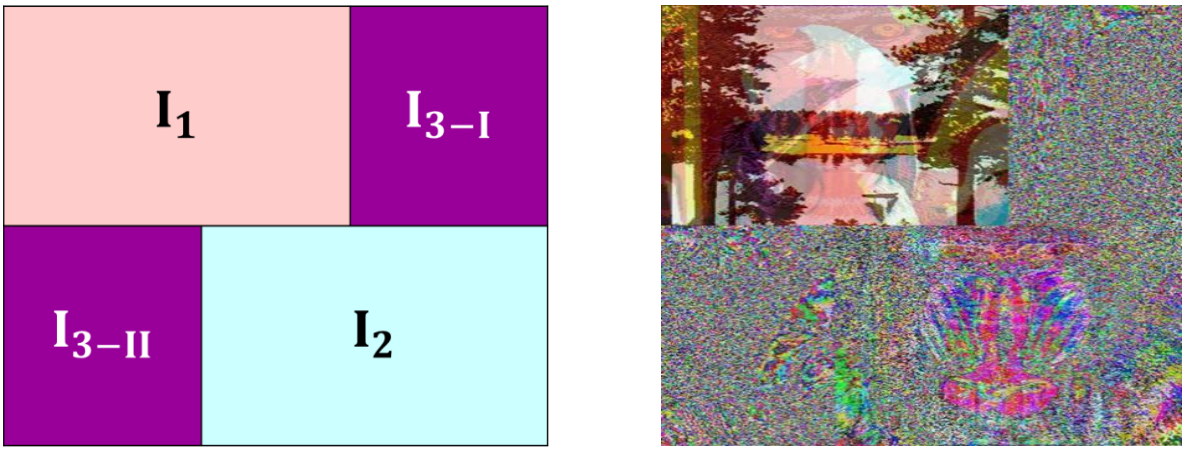
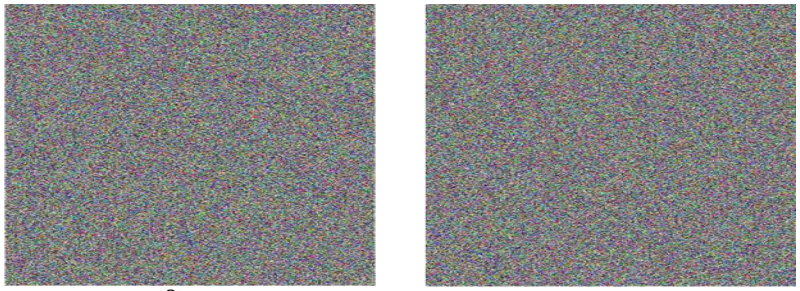


Fig. 5. Triple fusion results. (a)-(c) plaintext images, (d) high-bit image, (e) medium-bit image (f) low-bit image.



a b

Fig. 6. Results for the combined triple image (a) graphical presentation of the combining process (b) final fused image I_F.



a b

Fig. 7. Results of DEsS (a) chaotic fusion image, (b) scrambled image.

B. Optical Encryption Subscheme

The OEsS is based on Double Chaotic Phase Encoding (DCPE) implemented in the 2D optical Fourier transform (FT) domain for each RGB channel of the received digital encrypted image. Note that the 2D optical FT can be implemented using a single lens. The lens produces an FT image at the back focal plane for an image located at the front focal plane. For each color channel, the OE is implemented by cascading two FTs and supported by two CPMs. Each CPM is generated by one output of the chaotic system. One CMP is bonded with the primary image, and another is placed in the Fourier domain. The results of the OEsS are shown in Fig. 8. The mathematician framework describing the operation of DCPE-based FT encryption can be formed using the concepts reported in [26] for the DRPE counterpart. Consider the green channel as an example, the CPMs are expressed as

$$C_{PM1}(x,y) = \exp(j\emptyset_1(x,y)) = \exp(j2\pi C_6(x,y)) \quad (4)$$

$$C_{PM2}(x,y) = \exp(j\emptyset_2(x,y)) = \exp(j2\pi C_7(x,y)) \quad (5)$$

where C_6 and C_7 are the sixth and seventh chaotic outputs, respectively.

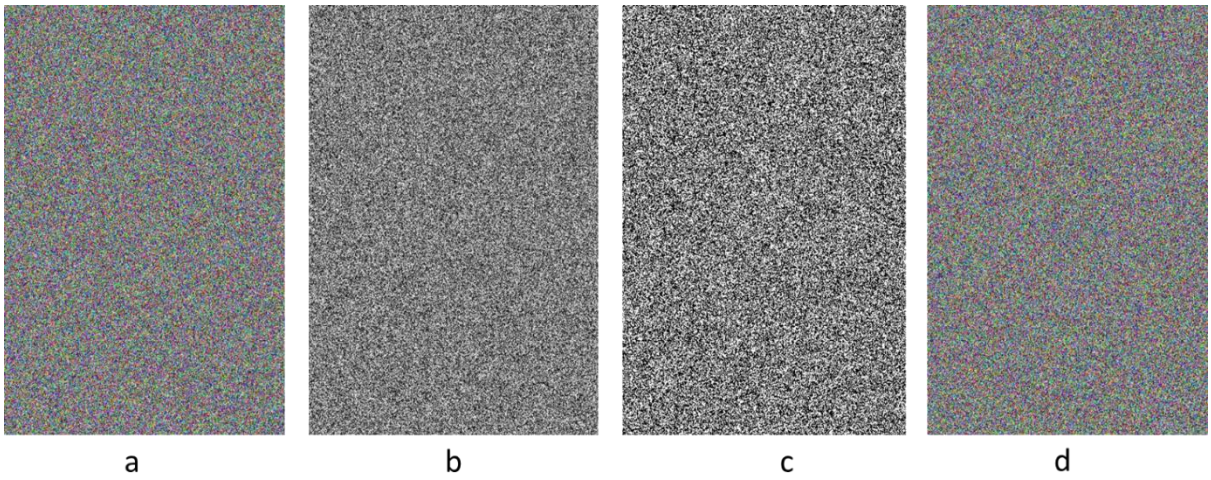


Fig. 8. Optical encryption results of (sailboat, Lena, and Baboon). (a) scrambled image, (b) image after mask1, (c) image after mask2, (d) encrypted image.

III. DECRYPTION PROCESS AND SECURITY TEST RESULTS

All the operational steps described during encryption are performed in reverse order as shown in Fig. 9. Both the encryption key and the decryption key are identical, and the chaotic sequence produced during the decryption process matches the chaotic sequence produced during the encryption process. Some of the results of the decryption process are presented in Fig. 10. Note that the decryption process may use only CPM2 to perform the decryption since CPM1 only varies the phase without affecting the image intensity.

A security analysis is provided to evaluate the algorithm's performance as given in the following.

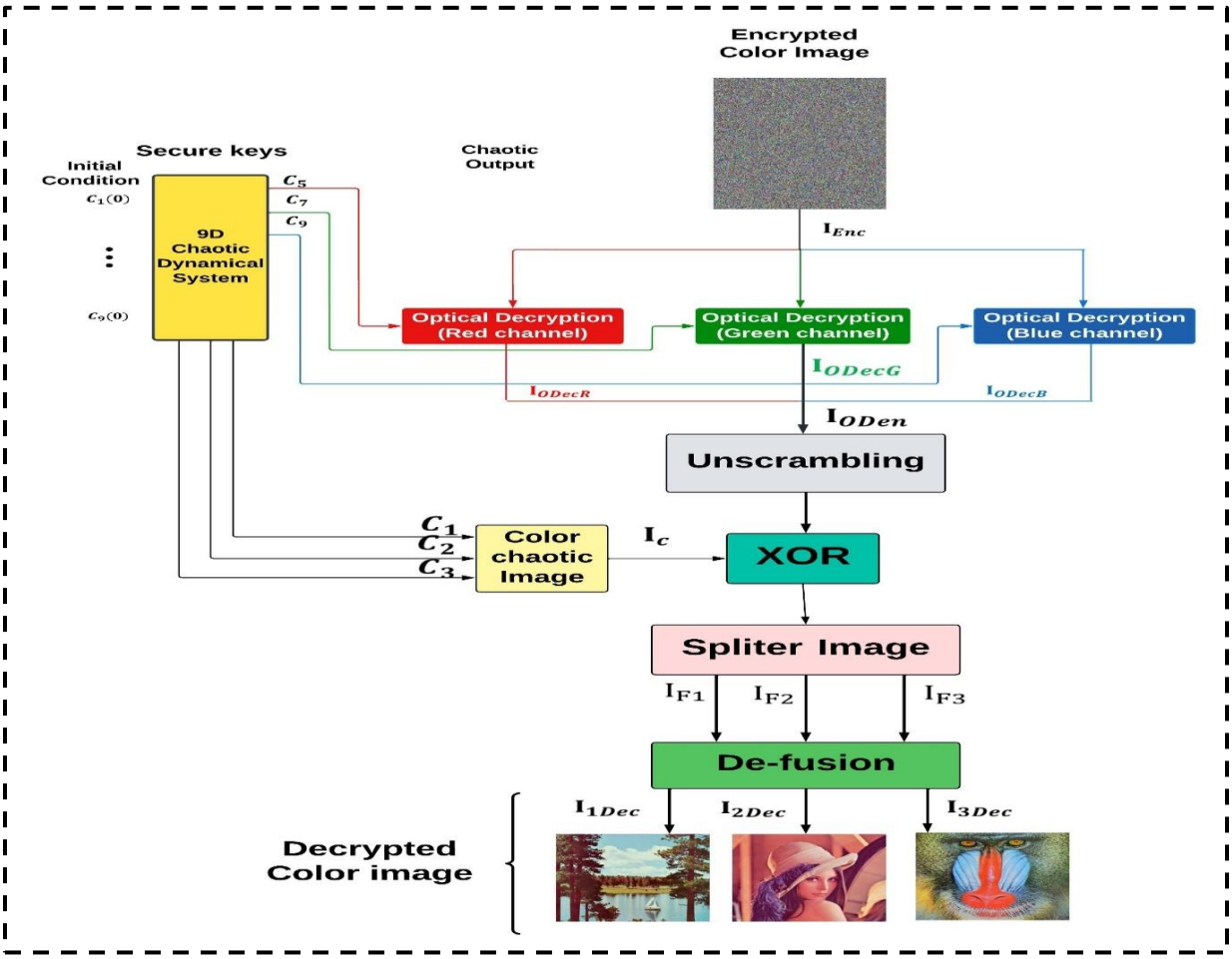


Fig. 9. Block diagram of the hybrid optical/digital decryption scheme.

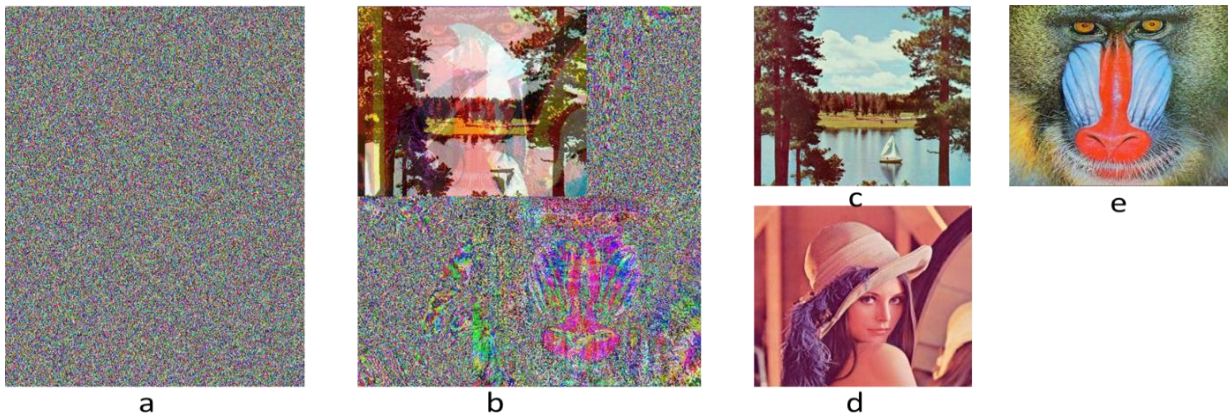


Fig. 10. Decryption results for triple color image (a) unscrambling images, (b) defused image, (c) decrypted sailboat, (d) decrypted Lena, (e) decrypted Baboon.

a. Information Entropy

The entropy of the encrypted image is calculated for each color channel using the following Equation [27]

$$H(x) = -\sum_{i=1}^{N} P(xi) \log_2 P(xi) \quad (6)$$

where *N* refers to the total number of pixels in the image, and *P*(*xi*) refers to the probability of *xi*. The entropy of the proposed scheme is 7.9991, 7.9987, and 7.9991 for R, G, and B channels, respectively assuming a triple image of the sailboat-Lena-baboon. The results indicate that the entropy approaches the ideal case of 8 since 256-graylevel values are used ($\log_2 256 = 8$).

b. Correlation Coefficient

The correlation between adjacent pixels in an original image is typically very high. This association between adjacent pixels should be eliminated by a good encryption scheme. The correlation between adjacent pixels in an encrypted image is approximately zero in correctly encrypted images. The correlation between any two neighbouring pixels, x and y, is computed as follows

$$r_{x,y} = \frac{E((x-E(x))-(y-E(y)))}{\sqrt{D(x)D(y)}} \quad (7)$$

where $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$, $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$ (8)

Table 1 lists the three-directional correlation coefficients of the encrypted image corresponding to a triple image of a sailboat, Lena, and Baboon. Note that the values of the correlation coefficient are close to zero, which means there is no correlation between adjacent pixels, indicating the strength of the encryption process. Not that the correlation coefficient depends on the channel under observation. This result is expected since the three channels have their individual histogram.

Table 1. Three-direction correlation coefficients of the encrypted image related to a color triple image.

Images	Channels	Vertical	Horizontal	Diagonal
Sailboat-Lena-Baboon	Red	-0.0009	0.0036	-0.0022
	Green	0.0003	-0.0012	0.0015
	Blue	-0.0027	0.0006	-0.0057

c. Noise Attack Analysis

Figure 11 shows how the decrypted triple image resists Gaussian noise that accurses through transmission from sender to receiver. Results are given for zero-mean Gaussian noise standard deviation (σ) equals 0.5, 5, 10, 15, and 20.

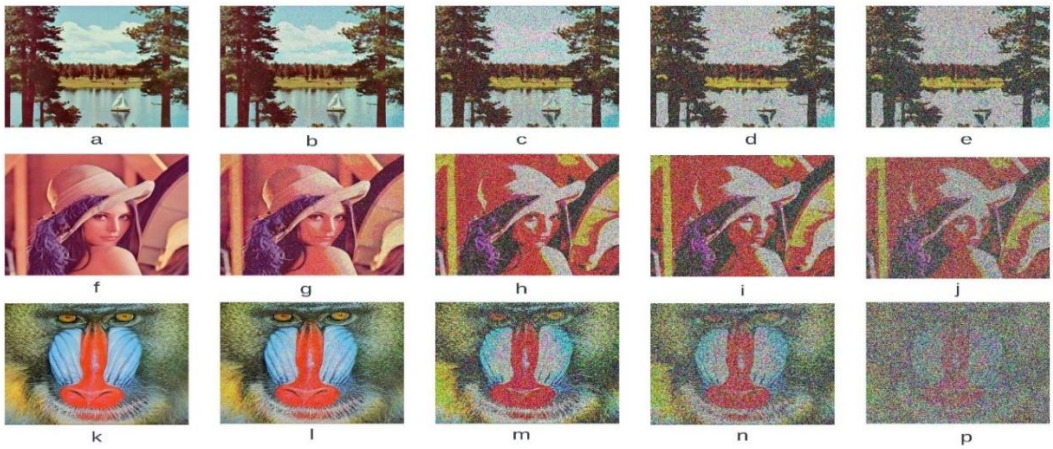


Fig. 11. Decrypted images (sailboat, Lena, and Baboon) with different values of standard deviation (a, f, k) σ=0.5, (b, g, l) σ=5, (c, h, m) σ=10, (d, i, n) σ=15, and (e, j, p) σ=20.

d. Cropping Attack Analysis

To test the effectiveness of the proposed method against cropping attacks, the quality of the decrypted images is tested when the encrypted image is cropped with various formats as shown in Fig 12. Parts a-e of this figure depict the encrypted image cropped with size 32×32 from the upper left, 64×64 from the upper left, 128×128 from the upper left, 256×256 from the upper left, and 128×128 from the middle image right, respectively. The decrypted images of the sailboat, Lena, and Baboon are displayed in parts (f)-(t) of this figure. The deciphered images are still recognizable and keep the majority of the original visual information. It indicates that the proposed method of encryption is resistant to occlusion attacks.

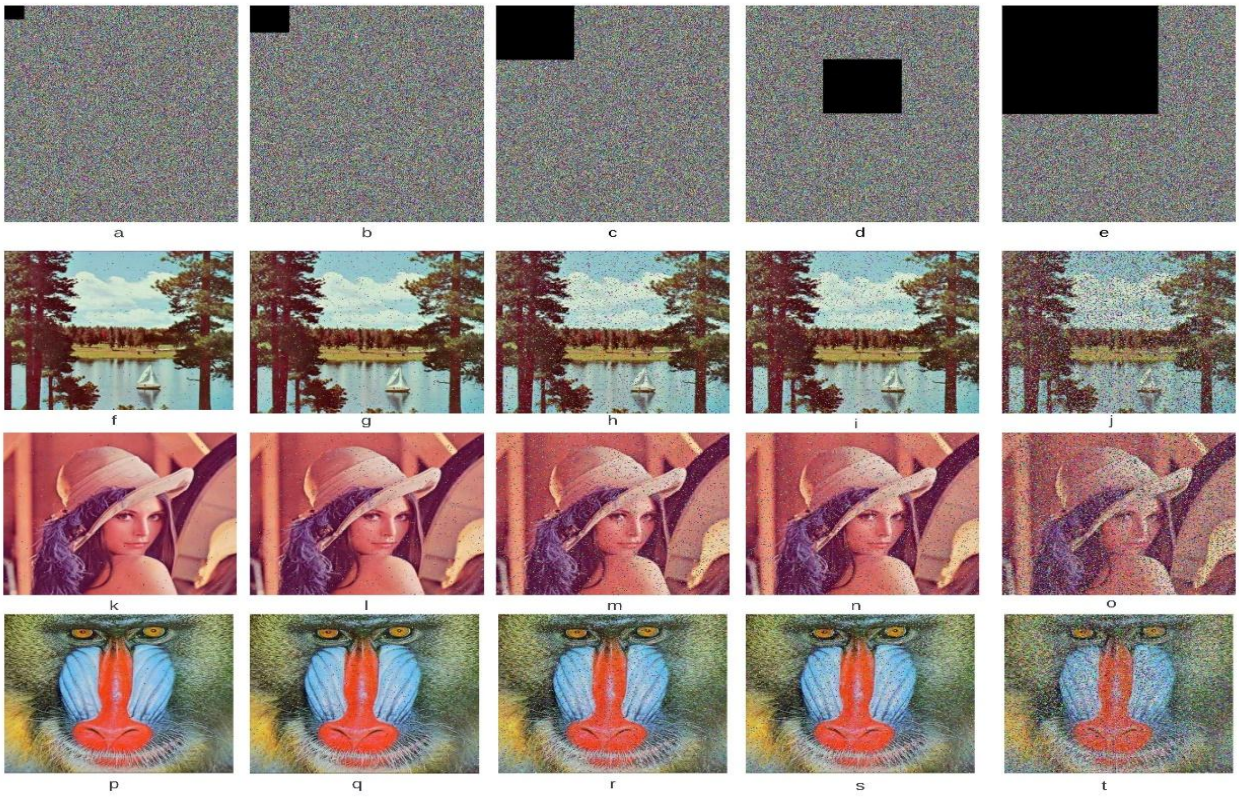


Fig. 12. Experimental results showing triple images in the presence of cropping attack.

e. DnCNN Results

A DnCNN is designed and trained to enhance the performance of decrypted images against additive Gaussian noise embedded with the received encrypted image. The network consists of four stacked layers. The first layer contains from input image layer and "Convolution + ReLU ". The middle layers include the same layer of "Convolution + ReLU", and each layer produces 64 feature maps. The last layer has the "Regression Layer". Zero padding is implemented to ensure that each feature map and input image are of the same size. and trained by 931 noisy images. The PSNRs of the decrypted images corresponding to an encrypted image received with additive Gaussian noise of different standard deviations are listed in Table 2. The results are given in the absence and presence of the DnCNN. Table 3 also contains the percentage improvement in PSNR due to applying DnCNN. Note that the designed DnCNN offers about 5dB improvement in PSNR. Table 3 contains the percentage improvement in PSNR due to applying DnCNN which is calculated using Equation 9

$$PSNR_{Improvement} = \frac{(PSNR)_{with\ DnCNN} - (PSNR)_{without\ DnCNN}}{(PSNR)_{without\ DnCNN}} \times 100 \quad (9)$$

The main findings of the test results are that the proposed scheme offers high-level security where the entropy and correlation coefficients approach 8 and zero, respectively, for the three-color channels of the encrypted image. The proposed scheme has high-level robustness against various attacks and the designed DnCNN offers about 5 dB improvement in the PSNR of the decrypted image when the received encrypted image has a Gaussian noise.

Table 2: PSNR values in dB for a triple image before and after applying DnCNN.

Name of Images	Before DnCNN					
	σ = 0	σ = 0.5	σ = 5	σ = 10	σ = 15	σ = 20
Sailboat	∞	24.07	15.73	13.73	12.19	12.41
Lena	∞	21.05	13.60	12.26	11.48	10.87
Baboon	∞	21.72	12.66	11.10	10.04	9.42
After DnCNN						
Sailboat	∞	26.60	21.37	18.74	17.70	17.21
Lena	∞	27.28	18.59	17.70	16.77	16.14
Baboon	∞	21.86	17.62	16.00	14.53	13.55

Table 3: Percentage improvement in PSNR due to applying DnCNN.

	σ = 0.5	σ = 5	σ = 10	σ = 15	σ = 20
Sailboat	10.52 %	35.86 %	36.49 %	45.20 %	38.68 %
Lena	29.60 %	36.69 %	44.73 %	46.08 %	48.48 %
Baboon	0.64 %	39.81 %	44.14 %	44. 72 %	38.54 %

IV. CONCLUSION

An HDOE scheme supported by a 9D chaotic system and DnCNN has been proposed for color triple image. Both DEsS and OEsS operate in an independent chaotic environment. The results indicate the high-level security of the prosed scheme where the entropy and correlation coefficients approach 8 and zero, respectively, for the three-color channels of the encrypted image. The scheme has high-level robustness against various attacks and the designed DnCNN offers about 5 dB improvement in the PSNR of the decrypted image when the received encrypted image has a Gaussian noise.

REFERENCES

[1] J. Wei, M. Zhang, and X. Tong, "Multi-image compression–encryption algorithm based on compressed sensing and optical encryption," *Entropy*, vol. 24, no. 784, pp. 1–22, 2022.

[2] M. R. Abuturab and A. Alfalou, "Multiple color image fusion, compression, and encryption using compressive sensing, chaotic-biometric keys, and optical fractional Fourier transform," *Optics and Laser Technology*, vol. 151, no. 108071, pp. 1–13, 2022.

[3] A. E. Willner, A. Fallahpour, K. Zou, F. Alishahi, and H. Zhou, "Optical signal processing aided by optical frequency combs," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 27, no. 7700916. pp. 1–16, 2021.

[4] G. S. Yadav, "A genetic algorithm based image steganography scheme with high embedding capacity and low distortion," *Imaging Science Journal*, vol. 0, no. 0, pp. 1–10, 2023.

[5] I. Khalid, T. Shah, S. M. Eldin, D. Shah, M. Asif, and I. Saddique, "An Integrated Image Encryption Scheme Based on Elliptic Curve," *IEEE Access*, vol. 11, no. December 2022, pp. 5483–5501, 2022.

[6] M. Kaur and V. Kumar, "Parallel non-dominated sorting genetic algorithm-II-based image encryption technique," *Imaging Science Journal*, vol. 66, no. 8, pp. 453–462, 2018.

[7] A. Hazer and R. Yildirim, "A review of single and multiple optical image encryption techniques," *Journal of Optics (United Kingdom)*, vol. 23, no. 113501, pp. 1–93, 2021.

[8] B. Zolfaghari and T. Koshiba, "Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap," *Applied System Innovation*, vol. 5, no. 3, pp. 1–38, 2022.
[9] Y. Zhao *et al.*, "High-precision calibration of phase-only spatial light modulators," *IEEE Photonics Journal*, vol. 14, no. 7402508, pp. 1–8, 2022.
[10] Z. Man, J. Li, X. Di, Y. Sheng, and Z. Liu, "Double image encryption algorithm based on neural network and chaos," *Chaos, Solitons and Fractals*, vol. 152, no. 111318. Elsevier Ltd, pp. 1–16, 2021.
[11] F. Musanna, D. Dangwal, S. Kumar, and V. Malik, "A chaos-based image encryption algorithm based on multiresolution singular value decomposition and a symmetric attractor," *Imaging Science Journal*, vol. 68, no. 1, pp. 24–40, 2020.
[12] M. Rezai and J. A. Salehi, "Fundamentals of Quantum Fourier Optics," *IEEE Transactions on Quantum Engineering*, vol. 4, no. June, pp. 1–22, 2022.
[13] J. Arif *et al.*, "A Novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution," *IEEE Access*, vol. 10. IEEE, pp. 12966–12982, 2022.
[14] J. Chen, X. W. Li, and Q. H. Wang, "Deep learning for improving the robustness of image encryption," *IEEE Access*, vol. 7, pp. 181083–181091, 2019.
[15] D. Kumar, A. B. Joshi, and V. N. Mishra, "Optical and digital double color-image encryption algorithm using 3D chaotic map and 2D-multiple parameter fractional discrete cosine transform," *Results in Optics*, vol. 1, no. 100031, pp. 1–16, 2020.
[16] B. Gulbahar and A. E. Oksuz, "Theory and Experiment of Spatial Light Modulation and Demodulation with Multi-plane Diffraction and Applications," *IEEE Access*, vol. 11, no. December 2022, pp. 872–889, 2022.
[17] A. Kumar and M. Dua, "A novel chaos map based medical image encryption scheme," *Imaging Science Journal*, pp. 1–20, 2022.
[18] B. Ge, Z. Shen, and J. Zhang, "Fast chaotic image encryption algorithm using a novel divide and conquer diffusion strategy," *IEEE Access*, vol. 10. pp. 95986–96005, 2022.
[19] A. K. Singh, K. Chatterjee, and A. Singh, "An Image Security Model Based on Chaos and DNA Cryptography for IIoT Images," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1957–1964, 2022.
[20] G. Li and M. Talha, "Research on multilevel chaotic image encryption algorithm based on optical processing technology," *Mathematical Problems in Engineering*, vol. 2022, no. 9076305, pp. 1–9, 2022.
[21] P. Tian and R. Su, "A Novel virtual optical image encryption scheme created by combining chaotic S-Box with double random phase encoding," *Sensors*, vol. 22, no. 5325. pp. 1–24, 2022.
[22] H. Shi, K. Yan, B. Hu, J. Qin, and Z. Feng, "Integrating multi-predictions encryption with histogram shifting secret-sharing for high-capacity two-layer image data hiding," *Imaging Science Journal*, 2022.
[23] P. K. Naskar and A. Chaudhuri, "Secured secret sharing technique based on chaotic map and DNA encoding with application on secret image," *Imaging Science Journal*, vol. 64, no. 8, pp. 460–470, 2016.
[24] R. Zhang and D. Xiao, "Double image encryption scheme based on compressive sensing and double random phase encoding," *Mathematics*, vol. 10, no. 8, pp. 1–23, 2022.
[25] P. Reiterer, C. Lainscsek, F. Schürrer, C. Letellier, and J. Maquet, "A nine-dimensional lorenz system to study high-dimensional chaos," *Journal of Physics A: Mathematical and General*, vol. 31, no. 34, pp. 7121–7139, 1998.
[26] N. K. Nishchal, *Optical cryptosystems*, no. IOP Publishing. 2019.
[27] K. M. Hosny, S. T. Kamal, and M. M. Darwish, "Novel encryption for color images using fractional-order hyperchaotic system," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 2, pp. 973–988, 2022.