Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-A, pp. 329–338
DOI : 10.47974/JDMSC-1886

Enhancing image security and privacy with hybrid double random phase encoding, lorenz maps, and compressed sensing

Anshika Malsaria *
Department of Computer and Communication Engineering
Manipal University
Jaipur
Rajasthan
India

Pankaj Vyas †
Department of Information Technology
Manipal University
Jaipur
Rajasthan
India

Manjit Kaur §
Department of Computer Engineering
SR University
Telangana
India

Abstract

The resilient and secure image encryption method presented in this research combines the benefits of Lorenz maps and double random phase encoding (DRPE) with compressed sensing. The suggested method attempts to maximize the use of storage resources while maintaining the security and integrity of sensitive image data during transmission and storage. Utilizing the energy compaction characteristics of the original image, compressed sensing with discrete cosine transform (DCT) is used in the encryption process to effectively represent and transmit the encrypted data. Lorenz maps are also used to create double random phase masks, adding high unpredictability and key sensitivity to strengthen the encryption scheme's security. Utilizing a variety of performance indicators, including the

* *E-mail:* anshika1987@gmail.com (Corresponding Author)
† *E-mail:* Pankaj.vyas@jaipur.manipal.edu
§ *E-mail:* Manjit.kr@yahoo.com

PSNR, NPCR, MSE, and SSIM, experimental investigations demonstrate the usefulness of the suggested strategy.

Subject Classification: *11T71 Algebraic coding theory; cryptography (number-theoretic aspects), 94A60 Cryptography [See also 11T71, 14G50, 68P25, 81P94], Applications to coding theory and cryptography of arithmetic geometry [See also 94A60, 94B27, 94B40].*

Keywords: *Image encryption, Double random phase encoding, Lorenz maps, Compressed sensing, Security, Robustness.*

1. Introduction

The paper addresses the pressing need for enhanced security in handling visual data, emphasizing the challenges posed by increased data sharing and the subsequent vulnerabilities. It proposes a robust encryption scheme that amalgamates three potent techniques: Double Random Phase Encoding (DRPE)[1], Chaos-based encryption using the Lorenz map, and a fusion of Compressed Sensing with Discrete Cosine Transform (DCT). DRPE, renowned for its resilience and high-security levels, operates in the Fourier domain, utilizing two RPMs generated through random integers or sequences. Chaos theory, specifically employing the chaotic behavior of the Lorenz map, further fortifies encryption by enhancing randomness and dependence on initial conditions [2]. The integration of Compressed Sensing with DCT revolutionizes picture transmission and encryption by effectively representing and reconstructing images while optimizing storage. The paper's main objective is to showcase the superiority of this combined encryption scheme through rigorous experimental evaluations and comparisons with existing methods. Section 1 introduces the challenges and the proposed solution [1,2]. Section 2 delineates the methods—DRPE, chaotic maps, and compressed sensing with DCT—providing a comprehensive understanding. Section 3 elaborates on the proposed methodology, concentrating on the combined approach's intricacies. The focal point of Section 4 is numerical simulations and outcomes, where the paper delves into the encryption procedure, key generation techniques, and performance evaluation metrics. This section serves as the cornerstone, demonstrating the security, robustness, and computational efficiency of the recommended scheme [3,4][25]. Double Random Phase Encoding (DRPE) is a prevalent technique for image encryption, employing the 4F principle, as illustrated in Figure 1. This method encrypts and decrypts images using two random phase masks and Fourier transforms [5][26]. The 4F principle comprises two lenses (F1

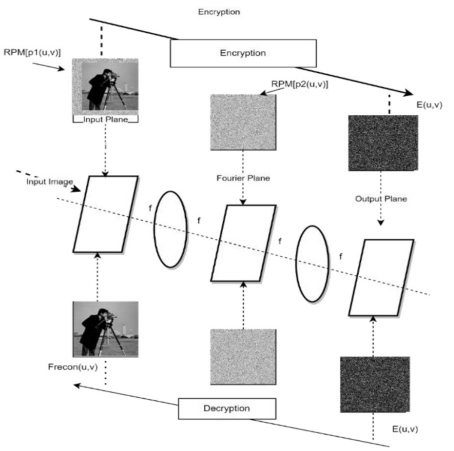

Figure 1

Double random phase encoding with 4f principle.

and F2) facilitating two Fourier transforms, forming the core of the encryption process[24]. Compressed Sensing (CS) is a signal processing approach that efficiently reconstructs sparse or compressible signals from limited observations. It operates on an original signal x ∈ R^n, assuming sparsity or compressibility.[6] Compressed measurements y ∈ R^m are derived by linearly sampling x using a matrix Φ ∈ R^(m x n), where m << n, described as y = Φ * x. This enables reconstruction of x from compressed data[7,8]. The Lorenz map, a chaotic system sensitive to initial conditions, is frequently used in cryptography for generating pseudorandom sequences. In image encryption, it constructs double random phase masks, enhancing security. Governed by nonlinear differential equations, the Lorenz map's parameters (ϑ, Ω, £) dictate its behavior, offering unpredictability crucial for encryption techniques [9].

These techniques—DRPE leveraging Fourier transforms, Compressed Sensing's sparse signal acquisition, and the Lorenz map's chaotic behavior—combine to enhance image encryption by fortifying security and efficient data representation. [21,22,23]

2. The Proposed Methodology

The proposed image encryption methodology combines compressed sensing and chaotic maps. It utilizes DCT for frequency coefficients,

compresses based on ratios, and applies chaotic maps with random phase masks for encryption. Figure 2(a) illustrates the encryption process flow, while Figure 2(b) depicts the scheme's block diagram.

Encryption Algorithm:

Step 1: Read the original image and convert it to double precision.

Step 2: Apply the Discrete Cosine Transform (DCT) to obtain the DCT coefficients. Let A_dct represent the DCT coefficients.

Step 3: Determine the desired compression ratio and calculate the number of coefficients to keep. Let num_coeffs be the number of coefficients to keep.

Step 4: Set up random phase masks A1 and A2 of the same size as the image.

Step 5: Encrypt the image using the following steps:

a. Multiply the DCT coefficients by Mask 1(A11 = exp(1i * 2 * pi * A1)).
b. Generate a chaotic key using the Lorenz chaotic map. Let the chaotic key represent the chaotic key generated.
c. Apply the chaotic key to the encrypted DCT coefficients(A111 = A_dct_cs .* exp(1i * 2 * pi * chaotic_key)).
d. Perform the Fast Fourier Transform (FFT) on the encrypted image (B = fft2(A111)).
e. Multiply the transformed image with Mask 2 (B111 = B .* A22).
f. Apply the inverse FFT to obtain the encrypted image (C = ifft2(B111)).
g. Calculate the absolute value of C to obtain the encrypted image (C1 = abs(C)).

The mathematical equation for encrypting the image using the described steps can be represented as follows:

$$C1 = \text{abs}(F\_inv(F(A) .* \exp(1i * 2\pi * K) .* M2 .* \exp(1i * 2\pi * M1))) \quad (12)$$

In this equation: A represents the DCT coefficients obtained from the original image (A_dct).K represents the chaotic key generated using the Lorenz chaotic map (chaotic_key).M1 and M2 are the random phase masks (A1 and A2).F represents the operation of Fast Fourier Transform. F_inv represents the operation of inverse Fast Fourier Transform. * Represents

element-wise multiplication. exp(1i * 2π * x) calculates the complex exponential function with x as the argument.

Decryption Algorithm:

Step 1: Decrypt the image using the following steps:

a. Perform the FFT on the encrypted image (D = fft2(C1)).
b. Multiply the transformed image by the conjugate of Mask 2 (D1 = D .* conj(A22)).
c. Generate the same chaotic key used during encryption.
d. Apply the inverse chaotic key to the decrypted image (D1 = D1 .* exp(-1i * 2 * pi * chaotic_key)).
e. Apply the inverse FFT to obtain the decrypted DCT coefficients (D11 = ifft2(D1)).
f. Multiply the decrypted DCT coefficients by the inverse of Mask 1 (D111 = D11 .* exp(-1i * 2 * pi * A1)).
g. Apply the inverse DCT transform to obtain the decrypted image (F = idct2(D111)).
h. Calculate the real part of F to obtain the decrypted image (F = real(F)).

3. Simulation Results

In evaluating the suggested picture encryption system, various standard metrics are employed to gauge image quality post-encryption [10,11]. Table 1 shows the picture specification used in the analysis of the above-mentioned method. These metrics include histogram, Peak signal-to-noise ratio (PSNR), Structural Similarity Index (SSIM), Normalized Pixel Change Rate (NPCR), Mean Squared Error (MSE), entropy, and correlational coefficient. [12,13,14] Entropy assesses data randomness, crucial in encryption performance, with our case showcasing an entropy value of 7.45, closer to the standard value of 8, signifying better encryption randomness [15,16]. PSNR measures image fidelity, indicating better quality in decrypted images with higher PSNR values, calculated using the ratio of the maximum signal value to noise in encrypted images. MSE quantifies differences between original and encrypted images by computing squared pixel deviations. NPCR, crucial in encryption contexts, indicates strong similarity between images with a high NPCR of 99.82%.

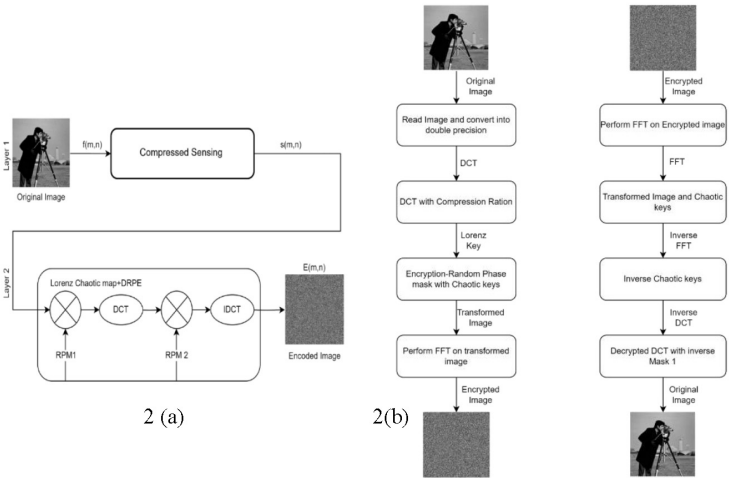

Figure 2

(a) Block diagram of proposed technique (b) Flow chart Diagram of proposed technique showing the detailed steps of encryption and decryption.

Comparing techniques like DRPE, CCS, and the Proposed work across images (Baboon, Cameraman, Boat, Barbara) via PSNR,NPCR,MSE in Table 2 provides a comprehensive assessment of encryption methodologies and histogram analysis shown in Figure 3 and Figure 4. Additionally, [17,18] SSIM and Universal Image Quality Index (UACI) contribute to image assessment. SSIM considers luminance, contrast, and structure, yielding values indicating resemblance between images, while UACI

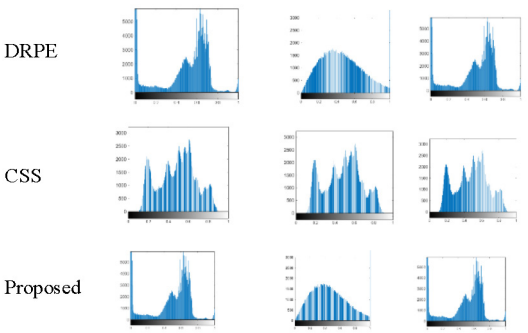

Figure 3

Show the comparative analysis of the histogram generated on the image Cameraman for different schemes.

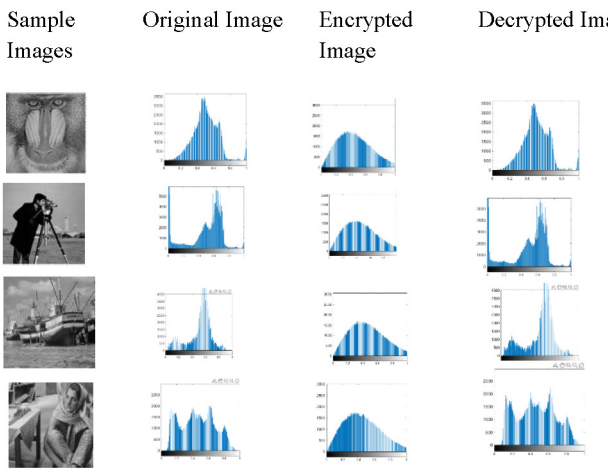

Figure 4

Show the comparative analysis of the histogram generated from the proposed technique on various images.

measures image fidelity through pixel value comparison, with higher values denoting closer resemblance to the original. [19,20]. In proposed method the UACI falls between 33.2 to 33.7 and SSIM is between 0.9234 to 0.9443 for various image dataset.

Table 1

Image specification

Images	Baboon	Cameraman	Boat	Barbara
Color	Greyscale	Greyscale	Greyscale	Greyscale
Dimension	512*512	512*512	512*512	256*256
Image Type	Bitmap	Jpg	Bitmap	Bitmap

Table 2

Comparative analysis of PSNR, NPCR, and MSE values of Techniques like DRPE, Compressed sensing, and proposed work.

Images	Techniques	PSNR	NPCR	MSE
Baboon	DRPE[2]	35.78	96.43	0.008912
	CCS[16]	37.52	98.15	0.006572
	Proposed Work	40.21	99.82	0.003992
	Standard	30-50	99-100	----------

Cameraman	DRPE[3]	32.56	95.21	0.012114
	CCS[17]	34.82	97.63	0.009561
	Proposed Work	37.29	99.42	0.007112
	Standard	30-50	99-100	----------
Boat	DRPE[5]	30.92	94.14	0.014512
	CCS[16]	33.01	96.42	0.011874
	Proposed Work	33.52	98.12	0.009112
	Standard	30-50	99-100	----------
Barbra	DRPE[22]	36.76	96.91	0.007895
	CCS[26]	38.92	98.63	0.005712
	Proposed Work	41.01	99.42	0.004111
	Standard	30-50	99-100	----------

4. Conclusion

This research introduces a robust image encryption method merging DRPE, Lorenz maps, and compressed sensing with DCT. Leveraging compressed sensing for data representation and Lorenz maps for unpredictability bolsters security. Experimental validation confirms high resilience and efficiency. This hybrid approach addresses the demand for secure image storage and transmission, ensuring data confidentiality and integrity in diverse applications. The scheme presents a significant stride in safeguarding visual data, offering a potent solution for secure encryption.

Declaration of competing interest

The authors declare that none of the work reported in this study could have been influenced by any known competing financial interests or personal relationships.

Conflict of interest

No conflicts of interest are disclosed by the writers.

References

[1] Malsaria, A. and P. Vyas. Study of Various Attacks Over Images Transferred Optically Through Communication Channel. in Interna-

tional Conference on Cyber Warfare, Security and Space Research. Springer (2021).

[2] Sharma, S.K., Kumar, A., Digital Image Transformation Using Outer Totality Cellular Automata. Machine Intelligence Techniques for Data Analysis and Signal Processing. Lecture Notes in Electrical Engineering, vol 997. Springer, Singapore (2023). https://doi.org/10.1007/978-981-99-0085-5_69.

[3] Zhang, S. and M.A. Karim, Color image encryption using double random phase encoding. *Microwave and optical technology letters*, 21(5): p. 318-323 (1999).

[4] Elshamy, E.M., et al., Efficient audio cryptosystem based on chaotic maps and double random phase encoding. *International Journal of Speech Technology*, 18: p. 619-631 (2015).

[5] Unnikrishnan, G., J. Joseph, and K. Singh, Optical encryption by double-random phase encoding in the fractional Fourier domain. *Optics letters*, 25(12): p. 887-889 (2000).

[6] Elshamy, A.M., et al., Optical image encryption based on chaotic baker map and double random phase encoding. *Journal of Lightwave Technology*, 31(15): p. 2533-2539 (2013).

[7] Sharma, N., et al., Phase-image encryption based on 3D-Lorenz chaotic system and double random phase encoding. 3D Research, 8: p. 1-17 (2017).

[8] Huang, H., et al., Chaotic image encryption based on bidimensional empirical mode decomposition and double random phase encoding. *Multimedia Tools and Applications*, 79: p. 28065-28078 (2020).

[9] Brahim, A.H., A.A. Pacha, and N.H. Said, Image encryption based on compressive sensing and chaos systems. *Optics & Laser Technology*, 132: p. 106489 (2020).

[10] Liu, Z., M.L. Yang, and W.Q. Yan. Image encryption based on double random phase encoding. in 2017 International Conference on Image and Vision Computing New Zealand (IVCNZ). 2017. IEEE.

[11] Zhu, L., et al., A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding. *Signal Processing*, 175: p. 107629 (2020).

[12] Situ, G. and J. Zhang, Double random-phase encoding in the Fresnel domain. *Optics Letters*, 29(14): p. 1584-1586 (2004).

[13] Abuturab, M.R., Securing color image using discrete cosine transform in gyrator transform domain structured-phase encoding. *Optics and Lasers in Engineering*, 50(10): p. 1383-1390 (2012).

[14] Malsaria, A., P. Vyas, and M. Kaur, Design and implementation of optical image communication encoding grounded on optical Fourier transform. *Journal of Optical Communications*, 2023(0).

[15] Abuturab, M.R., Color information security system using discrete cosine transform in gyrator transform domain radial-Hilbert phase encoding. *Optics and Lasers in Engineering*, 50(9): p. 1209-1216 (2012).

[16] Anil Kumar & Sandeep Kumar Sharma. Information cryptography using cellular automata and digital image processing, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:4, 1105-1111 (2022), DOI: 10.1080/09720529.2022.2072437.

[17] Deepan, B., et al., Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique. *Applied optics*, 53(20): p. 4539-4547 (2014).

[18] Hu, G., et al., Securing image information using double random phase encoding and parallel compressive sensing with updated sampling processes. *Optics and Lasers in Engineering,* 98: p. 123-133 (2017).

[19] Huang, H. and S. Yang, Image encryption technique combining compressive sensing with double random-phase encoding. *Mathematical Problems in Engineering,* 2018: p. 1-10 (2018).

[20] Zhou, K., et al., Secure image encryption scheme using double random-phase encoding and compressed sensing. *Optics & Laser Technology,* 121: p. 105769 (2020).

[21] Zhang, R. and D. Xiao, Double image encryption scheme based on compressive sensing and double random phase encoding. *Mathematics,* 10(8): p. 1242 (2022).

[22] Liu, Z., et al., Image encryption scheme by using iterative random phase encoding in gyrator transform domains. *Optics and Lasers in Engineering*, 49(4): p. 542-546 (2011).

[23] Huang, H. and S. Yang, Colour image encryption based on logistic mapping and double random-phase encoding. *IET Image Processing*, 11(4): p. 211-216 (2017).

[24] Fang, P., et al., A survey of image encryption algorithms based on chaotic system. *The Visual Computer*, 39(5): p. 1975-2003 (2023).

[25] Jiang, X., et al., Exploiting optical chaos for double images encryption with compressive sensing and double random phase encoding. *Optics Communications,* 484: p. 126683 (2021).

[26] Liu, H., et al., Securely compressive sensing using double random phase encoding. Optik, 126(20): p. 2663-2670 (2015).