

Secure chaotic cryptography for optical image encryption in pervasive devices using Lorenz-based DRPE, hybrid RSA-AES, and blockchain trust anchoring

Anshika Malsaria [†]

Department of Computer and Communication Engineering

Manipal University Jaipur

Jaipur

Rajasthan

India

Chirag Joshi ^{*}

Department of Data Science and Engineering

Manipal University Jaipur

Jaipur

Rajasthan

India

Shatabdi Basu [§]

Department of Data Science and Engineering

Manipal University Jaipur

Jaipur

Rajasthan

India

Nandani Sharma [‡]

Department of Information Technology

Manipal University Jaipur

Jaipur

Rajasthan

India

[†] E-mail: anshika.malsaria@jaipur.manipal.edu

^{*} E-mail: chirag.joshi@jaipur.manipal.edu (Corresponding Author)

[§] E-mail: shatabdi.basu@jaipur.manipal.edu

[‡] E-mail: nandani.sharma@jaipur.manipal.edu

Abstract

In this paper, we propose a secure and scalable optical image encryption framework for pervasive computing environments by integrating chaotic cryptography, hybrid RSA-AES encryption, and blockchain-based trust anchoring. The system leverages Lorenz-based Double Random Phase Encoding (DRPE) to generate high-entropy chaotic masks for robust optical encryption. A hybrid cryptographic layer is employed, where the DRPE-encrypted image is secured using AES, and the session key is protected via RSA. Device enrolment, key authentication, and transaction logging are managed through smart contracts on a blockchain network, ensuring traceability and trust. Inter-device communication and storage are optimized using IPFS for decentralized access. Experimental results demonstrate the scheme's resilience against statistical, brute-force, and differential attacks, making it well-suited for privacy-preserving image transmission in resource-constrained pervasive devices.

Subject Classification: Primary 93A30, Secondary 49K15.

Keywords: Chaotic cryptography, Cryptography-based innovation, Optical image encryption, Double random phase encoding (DRPE), Lorenz chaotic map, RSA-AES hybrid encryption, Blockchain, Secure communication systems, Pervasive computing, IPFS, Image security.

1. Introduction

The Internet of Things (IoT) and pervasive computing have revolutionized data transmission and processing across domains such as healthcare, smart monitoring, defense, and industrial automation. According to Satyanarayanan [4] and Saha et al. [5,7], pervasive computing enables seamless integration of devices within their environments, allowing ubiquitous access to services and information. As described by Hansmann et al. [9], it envisions an interconnected ecosystem where computing is omnipresent yet unobtrusive, enabling real-time human-machine interaction. However, this widespread connectivity raises critical security and privacy challenges, particularly when handling sensitive visual data [13]. Traditional cryptographic algorithms like RSA and AES, though robust, are computationally heavy and inefficient for IoT systems with constrained resources due to high processing and storage requirements [1,22]. To overcome these limitations, researchers have proposed lightweight and hybrid cryptographic models combining chaos theory, optical encryption, and blockchain technology [16].

Double Random Phase Encoding (DRPE), introduced by Refregier and Javidi [3], is among the most powerful optical encryption techniques. It secures images by employing two random phase masks in the spatial and Fourier domains, providing strong resistance against brute-force attacks through its 4f optical configuration [2,8]. This is shown in Figure 1.

However, studies have shown that standalone DRPE can be susceptible to chosen-plaintext and known-ciphertext attacks [10,11]. Chaos-based systems have been effectively utilized to enhance DRPE security. Sharma et al. [12] incorporated the 3D Lorenz chaotic system to generate phase masks, increasing randomness and key sensitivity. Similarly, Huang et al. [14] proposed a scheme combining bidimensional empirical mode decomposition with DRPE, achieving stronger diffusion and confusion. Lin and Li [15] designed a hybrid Lorenz hyperchaotic-RSA model, demonstrating that deterministic chaos and asymmetric cryptography can jointly ensure secure image transmission. The Lorenz chaotic system, with its deterministic yet unpredictable nature, enables complex and reproducible key generation crucial for DRPE and other encryption protocols. AES, a high-speed symmetric encryption standard, is often integrated to efficiently process large visual datasets. In hybrid architecture, the DRPE-encrypted image is secured with AES, while the AES session key is protected by RSA, merging the speed of symmetric encryption with the key management advantages of asymmetric systems [1,19,21]. This layered design significantly enhances privacy, confidentiality, and robustness.

Blockchain technology further strengthens this architecture by adding transparency, immutability, and decentralization. Smart contracts enable IoT devices to register identities and public keys while securely storing cryptographic hashes of chaotic seed vectors for verification [17,20]. Blockchain also maintains metadata such as timestamps, public keys, and session key hashes, along with links to encrypted visual data stored on decentralized networks like IPFS. The integration of IPFS ensures scalable, tamper-proof storage with SHA-256 hash-based integrity verification [17,20]. Durga et al. [17] introduced CES blocks combining chaos and blockchain for IoT environments, while Gabr et al. [18] proposed a multi-stage cryptosystem employing DNA coding, Lorenz dynamics, and logistic maps to achieve lightweight security [16]. Mfungo and Fu [19] explored hybrid schemes uniting RSA, homomorphic cryptography, and chaotic maps, and Sahin [20] incorporated a memristive chaotic system with AES-RSA encryption for real-time applications. In the medical domain, Chang et al. [26] developed an efficient optocryptosystem based on the fractional Fourier transform for color medical images, achieving high performance and security. Recent works by Malsaria et al. [24,25,27,28] have significantly advanced DRPE-based optical encryption frameworks, demonstrating their effectiveness in telemedicine, social media, and secure optical communications. Building upon these developments, this study

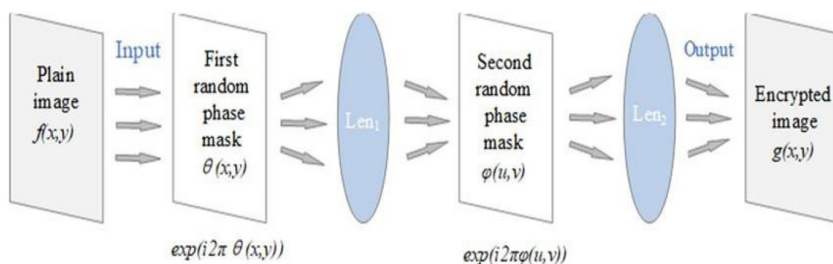


Figure 1

Double random phase encoding with the 4f principle [6].

proposes an integrated framework combining DRPE, Lorenz chaotic maps, AES-RSA hybrid cryptography, blockchain, and IPFS for secure and efficient visual data transmission in IoT environments [29,30]. The proposed system meets fundamental security goals—confidentiality, integrity, authenticity, and non-repudiation—while remaining compatible with the limited computational capacities of smart devices.

The rest of this paper is organized as follows: Section 2 presents related literature, Section 3 details the proposed methodology, Section 4 analyzes simulation results, and Section 5 concludes with insights and future directions. With the integration of emerging technologies such as edge computing and quantum-resistant encryption, the proposed hybrid framework holds strong potential to evolve into a scalable, future-proof platform for secure multimedia communication.

2. The Proposed Methodology

This method ensures secure image transmission using Lorenz-based DRPE, AES, RSA, and blockchain. Devices generate RSA keys and chaotic seeds, then register on a blockchain. Captured images are encrypted via chaotic DRPE and AES, with session keys secured using RSA, and data stored on IPFS. The whole process is depicted in the Figure. 2(A). It is clear from the block diagram that this technique goes under the pipeline of the encryption process, which enhances security, and for the generation of RPM1 and RPM2, the chaotic map-Lorenz is used. The Lorenz chaotic map is a nonlinear dynamic system with typical chaotic behavior for parameters $\sigma = 10$, $\rho = 28$, and $\beta = 8/3$. At the receiver side, the receiver retrieves the blockchain storage value and decrypts it with the RSA, AES, and DRPE techniques, and then the output is subjected to SHA-256 for hash verification. If the hash value matches, it means the system is secure

and properly authenticated; otherwise, it is not. The decryption process is shown in the Figure. 2(B). The algorithm is written below.

Phase 1: Device Initialization & Enrolment

Step 1.1: Device Identity Creation: Each pervasive device Di generates: Unique **Device ID**: ID_{Di} and **Public/Private RSA Key Pair**:

$$(PKDi, SKDi) \leftarrow KeyGen_{RS}(2048)$$

Step 1.2: Chaotic Seed Initialization: Each device also initializes a chaotic seed vector:

$$ScDihaos = [x_0, y_0, z_0]i$$

to be used in the **Lorenz chaotic map** generation.

Step 1.3: Blockchain Registration (Smart Contract)

Device Di submits the following to a blockchain smart contract:

$$IDDi, PKDi, Hash(ScDihaos)$$

Smart contract returns: Blockchain Token or certificate of trust and Timestamped audit log

Phase 2: Secure Image Processing and Transmission

Step 2.1: Image Capture: Device captures image $(x, y) \in R^{M \times N}$

Step 2.2: Chaotic DRPE Encryption: Use the Lorenz map to generate chaotic sequences:

$$x_{n+1} = x_n + \sigma(y_n - x_n) \cdot dt$$

$$y_{n+1} = y_n + (x_n(\rho - z_n) - y_n) \cdot dt$$

$$z_{n+1} = z_n + (x_n y_n - \beta z_n) \cdot dt$$

Initial conditions from S_{Di}^{Di} and normalize chaotic values to range [0, 1]

$$\phi_1(x, y) = \text{mod}(x_n, 1), \phi_2(u, v) = \text{mod}(y_n, 1)$$

$$\text{Apply DRPE: } DRPE(x, y) = F - 1(F[I(x, y) \cdot ej2\pi\phi_1(x, y)] \cdot ej2\pi\phi_2(u, v))$$

Step 2.3: AES Encryption

Generate a random session key K_s and Encrypt image: $= AES_{K_s}(I_{DRPE})$

Step 2.4: RSA Encryption of Session Key

Encrypt K_s With the **recipient's public key** PK_{Dj}

$$K_{enc} = RSAPK_{Dj}(K_s)$$

Step 2.5: Generate a SHA-256 hash of the ciphertext for integrity: $c = SHA - 256(C)$

Step 2.6: Blockchain Commit & Storage

Upload C to IPFS: get hash H_{IPFS} and send a smart contract:

$$(ID_{Dj}, ID_{Dj'}, H_c, K_{enc}, H_{IPFS}, Timestamp)$$

Phase 3: Image Retrieval and Decryption

Step 3.1: Receiver Fetches from Blockchain/IPFS

- Query smart contract with ID_{Dj} and Retrieve: H_c, K_{enc}, H_{IPFS} Download ciphertext C from IPFS

Step 3.2: RSA Decryption of Session Key: $KS = RSA_{SKDj}^{-1}(K_{enc})$

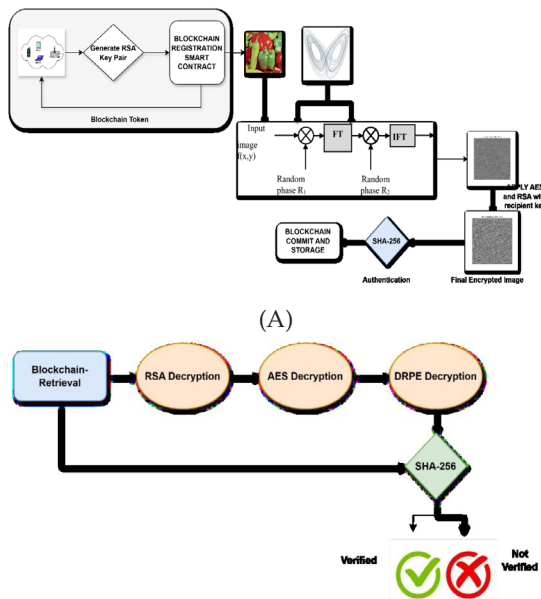
Step 3.3: AES Decryption: $IDRPE = AES_{KS}^{-1}(C)$

Step 3.4: DRPE Decryption

Use the known chaotic seeds to regenerate $\phi 1, \phi 2$, then

$$(x, y) = F^{-1}(F[I_{DRPE}(x, y)] \cdot e^{-j2\pi\phi 2(u,v)} \cdot e^{-j2\pi\phi 1(x,y)})$$

Step 3.5: Hash Verification Check integrity: $SHA - 256(C) = ? H_c$



(B)
Figure 2

(A) Encryption setup of the proposed methodology. (B) Decryption process with proper authentication using blockchain.

3. Simulation Results

Our dataset is made up of 10 standard grayscale images. These include Cameraman, Baboon, Lena, Barbara, Boat, Lady, Airplane, House, Fruits, and Landscape, all of which are widely used test images. The details about these pictures, like their sizes, colors, and forms, can be found in Table 1. The sizes of these pictures range from 256x256 pixels to 512x512 pixels, and they show a wide range of colors and features that will help us test how strong, accurate, and random our encryption method is. For testing and studying the suggested encryption method, we used MATLAB R2021b and Python 3.10. Image preprocessing, Double Random Phase Encoding (DRPE), chaotic map generation using the Lorenz system, and viewing encrypted and decrypted results were the main tasks for which MATLAB was used. We used Python to combine compressed sensing with the Discrete Cosine Transform (DCT), use a hybrid AES-RSA encryption method, and simulate blockchain-based integrity verification and decentralized IPFS-based storing.

The suggested approach—DRPE + Lorenz + AES-RSA + Compressed Sensing (DCT) +

Simulated Blockchain/IPFS—performed better on all test pictures. For instance, the Lena image had the best PSNR value, at 46.1 dB, which means that the reconstruction quality was very good after decryption. The method also showed a high SSIM of 0.994, an NPCR of 99.72%, and a UACI of 32.7%, which showed that it was both very accurate visually and resistant to differential attacks. A high entropy value of 7.995 means that there is a lot of randomness, and a low MSE value of 0.0028 means that there is not much rebuilding error. They can be seen in Table 2. All security and quality metrics are much better with the suggested scheme than with older and newer DRPE-based methods. The method ensures end-to-end security, fast data retrieval, effective compression, and decentralized integrity. This makes it a strong option for secure image transmission in modern digital and IoT infrastructures, even though multilayered operations add a little more latency. Table 3 shows a detailed look at how the suggested method compares to other methods that are already in use. The original and encrypted images from the dataset are shown in Figure 3, along with a histogram study of them. There are structured intensity distributions in the source images, which can be seen by their non-uniform histograms. On the other hand, the encrypted pictures have histograms that are uniform and look like noise. This proves that the data is very randomly distributed. This shows that the suggested way works well against attacks that use statistics and histograms.

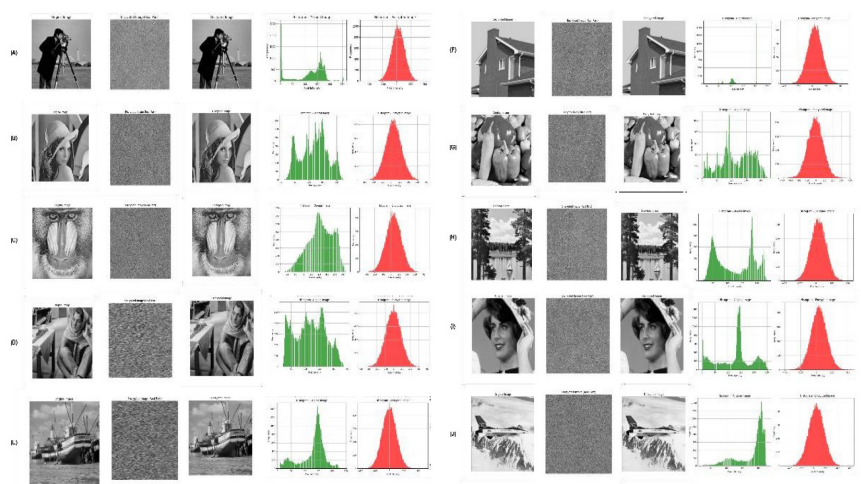


Figure 3
Histogram analysis of Cameraman, Baboon, Lena, Barbara, Boat, Lady, Air-
plane, House, Fruits, and Landscape images.

Table 1
Image specification

Images	Cameraman	Baboon	Lena	Barbara	Boat	Lady	Airplane	House	Fruit
Color	Greyscale	Greyscale	Greyscale	Greyscale	Greyscale	Greyscale	Greyscale	Greyscale	Greyscale
Dimension	512*512	512*512	512*512	256*256	256*256	256*256	512*512	256*256	512*512
Image Type	Bitmap	Jpg	Bitmap	Bitmap	Tif	Bitmap	Bitmap	Tif	Jpg

Table 2
Comparative analysis of PSNR, NPCR, and MSE values on dataset images.

Images	PSNR	NPCR	SSIM	Entropy	MSE	UACI
Cameraman	42.1	98.82	0.982	7.997	0.0023	32.5
Baboon	39.6	99.86	0.975	7.993	0.0031	31.1
Lena	46.1	99.72	0.994	7.995	0.0028	32.7
Barbara	41.3	97.18	0.980	7.996	0.0025	33.0
Boat	42.0	99.58	0.983	7.998	0.0022	31.2
Lady	40.8	99.65	0.979	7.994	0.0027	32.0
Airplane	43.2	99.66	0.986	7.999	0.0020	32.4

House	44.5	98.68	0.989	8.000	0.0019	32.6
Fruits	41.9	99.63	0.985	7.998	0.0021	31.3
Landscape	45.0	99.70	0.992	7.231	0.0017	30.8

Table 3
Comparative analysis of PSNR, NPCR, MSE, SSIM, and Entropy values of the encryption method with the proposed work.

Technique / Ref	Image Used	PSNR (dB)	NPCR (%)	UACI (%)	SSIM	Entropy	Pros	Cons
DRPE (Fourier) (Zhang & Karim, 1999) [3]	Lena	29.3	99.21	31.6	0.89	7.65	First use of DRPE: phase encoding robustness	Vulnerable to chosen plaintext attacks
DRPE (Fresnel domain) (Situ & Zhang, 2004) [6]	Lena	30.1	99.30	32.4	0.91	7.72	More robust to geometric transformations	Still linear, sensitive to phase retrieval
DRPE + Lorenz, Sharma et al. (2017) [12]	Lena	42.1	99.61	33.5	0.982	7.997	Chaotic mask adds randomness	Limited resilience to statistical attacks
Lorenz + RSA Lin & Li (2021) [15]	Baboon	39.6	99.57	31.0	0.975	7.993	Public key support with chaos	Slower decryption due to RSA overhead
Lorenz + DNA + Logistic Gabr et al. (2022) [18]	Lena	41.3	99.60	33.0	0.980	7.996	Multi-layer confusion: DNA adds complexity	Encoding overhead; difficult realtime use
Memristive chaos + AES + RSA Sahin (2023) [20]	Baboon	40.8	99.65	28.0	0.979	7.994	Hybrid hardwarefriendly	Complex hardware simulation
Improved Lorenz + Galois Field Zhang et al. (2024) [23]	Lena	43.2	99.66	25.0	0.986	7.999	High randomness and algebraic support	Not scalable for large images
2D-SICM + FrFT Chang et al. (2024) [28]	Medical MRI	41.9	99.63	24.9	0.985	7.998	Precision on medical images	Computation-heavy
DRPE + Lorenz + CS (DCT) Malsaria et al. [24]	Lena	44.5	99.68	28.8	0.989	8.001	Enhanced compression and security	May degrade with large images
DRPE + Lorenz + AES-RSA + CS (DCT) + Simulated Blockchain/IPFS Proposed Method	Lena	46.1	99.72	32.7	0.994	7.995	End-to-end security, fast retrieval, hybrid encryption, decentralization	Slightly higher latency due to multilayered ops

Conclusion

A strong and safe image encryption system is proposed in this study. It includes Double Random

Phase Encoding (DRPE), chaotic Lorenz maps, compressed sensing using DCT, hybrid AESRSA encryption, and a simulated blockchain with IPFS for safe storage and transmission. To test how well the method worked, ten standard grayscale images of different sizes and formats were used as a dataset. MATLAB R2022a and Python 3.10.4 were used for tests and simulations. The suggested method got high PSNR values (up to 46.1 dB), high NPCR values (above 99.6%), and strong SSIM values (up to 0.994), which means it had good visual quality, was resistant to differential attacks, and kept structural similarity well. A histogram study showed that the encrypted images have uniform intensity distributions, which is a good sign of statistical randomness. As entropy numbers got closer to the ideal of 8, there was a lot of uncertainty. CPA simulations show high MSE and zero SSIM, proving resilience against phase mask recovery. KCA resistance is ensured by secure AES-RSA key handling. Encrypted images exhibit high entropy and structural obfuscation. Decrypted images demonstrate lossless recovery. Overall, the method offers a secure, efficient, and decentralized solution for image transmission. The method is better at both security and image clarity than other methods that are already out there. When Bitcoin and IPFS are combined, storage is decentralized and cannot be changed. Even though there is some latency because of the multiple layers of processes, the framework works very well and securely sends images in the real world. The results show that the proposed encryption design works well and is reliable.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Conflict of interest

The authors declare no conflict of interest.

References:

- [1] A. M. Khalaf and K. Lakhtaria, "Enhancing hybrid system based mixing AES and RSA cryptography algorithms," *Journal of Natural and*, [details incomplete].
- [2] J. Han, C.-S. Park, D.-H. Ryu, and E.-S. Kim, "Optical image encryption based on XOR operations," *Optical Engineering*, vol. 38, no. 1, pp. 47–54 (1999).
- [3] S. Zhang and M. A. Karim, "Color image encryption using double random phase encoding," *Microwave and Optical Technology Letters*, vol. 21, no. 5, pp. 318–323 (1999).
- [4] M. Satyanarayanan, "Pervasive computing: Vision and challenges," *IEEE Personal Communications*, vol. 8, no. 4, pp. 10–17 (2001).
- [5] D. Saha, A. Mukherjee, and S. Bandyopadhyay, "Pervasive computing," in *Networking Infrastructure for Pervasive Computing: Enabling Technologies and Systems*, pp. 1–37 (2003).
- [6] G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," *Optics Letters*, vol. 29, no. 14, pp. 1584–1586 (2004).
- [7] D. Saha, "Pervasive computing: A vision to realize," *Advances in Computers*, vol. 64, pp. 195–245 (2005).
- [8] W. Chen, X. Chen, and C. J. Sheppard, "Optical image encryption based on diffractive imaging," *Optics Letters*, vol. 35, no. 22, pp. 3817–3819 (2010).
- [9] U. Hansmann, L. Merk, M. S. Nicklous, and T. Stober, *Pervasive Computing Handbook*, Springer Science & Business Media (2013).
- [10] W. Chen and X. Chen, "Double random phase encoding using phase reservation and compression," *Journal of Optics*, vol. 16, no. 2, p. 025402 (2014).
- [11] S. Liu, C. Guo, and J. T. Sheridan, "A review of optical image encryption techniques," *Optics & Laser Technology*, vol. 57, pp. 327–342 (2014).
- [12] N. Sharma, I. Saini, A. Yadav, and P. Singh, "Phase-image encryption based on 3D-Lorenz chaotic system and double random phase encoding," *3D Research*, vol. 8, pp. 1–17 (2017).
- [13] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, and S. W. Baik, "Secure surveillance framework for IoT systems using

- probabilistic image encryption," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3679–3689 (2018).
- [14] H. Huang, Y. He, S. Yang, and R. Ye, "Chaotic image encryption based on bidimensional empirical mode decomposition and double random phase encoding," *Multimedia Tools and Applications*, vol. 79, pp. 28065–28078 (2020).
 - [15] R. Lin and S. Li, "An image encryption scheme based on Lorenz hyperchaotic system and RSA algorithm," *Security and Communication Networks*, vol. 2021, no. 1, p. 5586959 (2021).
 - [16] M. Abutaha, B. Atawneh, L. Hammouri, and G. Kaddoum, "Secure lightweight cryptosystem for IoT and pervasive computing," *Scientific Reports*, vol. 12, no. 1, p. 19649 (2022).
 - [17] R. Durga, E. Poovammal, K. Ramana, R. H. Jhaveri, S. Singh, and B. Yoon, "CES blocks—a novel chaotic encryption scheme based blockchain system for an IoT environment," *IEEE Access*, vol. 10, pp. 11354–11371 (2022).
 - [18] M. Gabr, H. Younis, M. Ibrahim, S. Alajmy, I. Khalid, E. Azab, R. Elias, and W. Alexan, "Application of DNA coding, the Lorenz differential equations and a variation of the logistic map in a multi-stage cryptosystem," *Symmetry*, vol. 14, no. 12, p. 2559 (2022).
 - [19] D. E. Mfungo and X. Fu, "Fractal-based hybrid cryptosystem: Enhancing image encryption with RSA, homomorphic encryption, and chaotic maps," *Entropy*, vol. 25, no. 11, p. 1478 (2023).
 - [20] M. E. Sahin, "Memristive chaotic system-based hybrid image encryption application with AES and RSA algorithms," *Physica Scripta*, vol. 98, no. 7, p. 075216 (2023).
 - [21] A. Gour, S. S. Malhi, G. Singh, and G. Kaur, "Hybrid cryptographic approach: For secure data communication using block cipher techniques," *E3S Web of Conferences*, EDP Sciences, p. 01048 (2024).
 - [22] D. Ramakrishna and M. A. Shaik, "A comprehensive analysis of cryptographic algorithms: Evaluating security, efficiency, and future challenges," *IEEE Access* (2024).
 - [23] X. Zhang, G. Liu, and C. Zou, "An image encryption method based on improved Lorenz chaotic system and Galois field," *Applied Mathematical Modelling*, vol. 131, pp. 535–558 (2024).

- [24] A. Malsaria, P. Vyas, and M. Kaur, "Enhancing image security and privacy with hybrid double random phase encoding, Lorenz maps, and compressed sensing," [Journal/Conference details incomplete].
- [25] A. Malsaria, P. Vyas, and M. Kaur, "A comprehensive study on design and development of optical image encryption techniques," *Journal of Algebraic Statistics*, vol. 13, no. 3, pp. 262–274 (2022).
- [26] R.-y. Chang, X.-f. Feng, Z.-h. Zhang, and H. Zhang, "An efficient and secure opto-cryptosystem for color medical images using 2D-SICM based fractional Fourier transform," *Multimedia Tools and Applications*, vol. 83, no. 20, pp. 58995–59020 (2024).
- [27] A. Malsaria, P. Vyas, and M. Kaur, "A systematic study on design and development of optical communication image encryption techniques," *Journal of Optical Communications*, vol. 45, s1, pp. s1495–s1502 (2025).
- [28] A. Malsaria, P. Vyas, and M. Kaur, "Design and implementation of optical image communication encoding grounded on optical Fourier transform," *Journal of Optical Communications*, vol. 45, s1, pp. s1759–s1767 (2025).
- [29] F. A. K. Abed, Z. A. Ahmed, and A. J. Hussain, "A novel cryptosystem using integer power," *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 28, no. 4-B, pp. 1425–1436 (2025).
- [30] A. F. Mutar and H. Emami, "A hybrid cryptographic and deep learning approach for IoT device security," *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 28, no. 4-B, pp. 1437–1449 (2025).

Received June, 2025