

Lightweight HECC-DWT-based secure image encryption with integrity verification and access control

Anshika Malsaria [†]

*Department of Computer and Communication Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India*

Vijay Kumar Sharma ^{*}

*Department of IoT and Intelligence systems
Manipal University Jaipur
Jaipur 303007
Rajasthan
India*

Pankaj Dadheech [§]

*Department of Computer Science & Engineering
Swami Keshvanand Institute of Technology,
Management & Gramothan (SKIT)
Jaipur 302017
Rajasthan
India*

Praveen Kumar Yadav [‡]

Sanwta Ram Dogiwal [@]

*Department of Information Technology
Swami Keshvanand Institute of Technology,
Management & Gramothan (SKIT)
Jaipur 302017
Rajasthan
India*

This article has been corrected with minor changes. These changes do not impact the academic content of the article.

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

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

[§] E-mail: pankajdadheech777@gmail.com

[‡] E-mail: praveenyaadavskit@gmail.com

[@] E-mail: dogiwal@gmail.com

Bhanu Pratap Soni [#]

School of Electrical and Electronics Engineering

College of Engineering, Technical Vocational Education & Training

Fiji National University

000

Fiji

Abstract

This paper presents a secure and lightweight image encryption framework combining Hyperelliptic Curve Cryptography (HECC) and Discrete Wavelet Transform (DWT) for optical images. The proposed method begins with HECC-based key generation, ensuring efficient encryption using compact key sizes. The image undergoes ASCII conversion, followed by encryption using the recipient's public key. To enhance security, DWT is applied, embedding encrypted data in the frequency domain, followed by inverse DWT reconstruction. SHA-2 hashing ensures integrity verification, preventing unauthorized modifications. Decryption is performed using HECC, restoring the original image upon hash verification. A Boolean search mechanism also enables efficient retrieval of encrypted images, while proxy re-encryption facilitates dynamic key updates. The proposed system ensures lightweight, secure, and efficient optical image encryption.

Subject Classification: 94A60.

Keywords: Double random phase encoding, Hyper elliptic curve, Cryptography, DCT, DWT, Data integrity, Cyber bullies.

1. Introduction

Every day, a vast number of photographs are shared online. To protect their data, many people employ optical image processing technology. There is a growing risk that data transmitted over networks will be hacked. It is necessary to protect sensitive information from unwanted access over insecure mediums like the internet. Implementing data protection techniques during transmission has proven to be one of the challenges. Some of the techniques used to identify data security vulnerabilities are cryptographic [1]. For safe data transfer across networks, it focuses on data encryption and decryption algorithms. Cryptography comes in two categories: symmetric and asymmetric. In the asymmetric method, one must enter a private key to encode and decode text. It is better than symmetric encryption, where a shared key is used between the sender and receiver [2].

[#] E-mail: bhanu.soni@fnu.ac.fj

A method is thought to be good if it can be used to figure out data completion without a useful key. Because of this, a lot of work needs to go into making a very advanced crypto algorithm instead of using common ones like AES, DES, and so on. Due to this reason, in the past decade, researchers have shown interest in optical encryption techniques like DRPE (Double Random Phase Encoding). Large key sizes, multilayer designs, and encrypting lightweight optical pictures for ptychography devices all cost a lot to compute and store [1-3].

This work focuses on an optical image encryption system that can protect images containing private data from theft and send them only to the intended recipient. In this paper, a methodology is proposed by combining Hyperelliptic Curve Cryptography (HECC) and DWT for optical images.

2. DRPE (Double Random Phase Encoding)

In the DRPE method, image waves of one color move through propagator 1 (P1), which is in the spatial plane, then go through OFT (optical Fourier transform) on P1, then move through propagator 2 (P2), which is also in the same plane, then go through OFT2 of the white image, and finally go through Fourier plane OFT2 of the encrypted image. $P1(x,y)$ and $P2(x,y)$ are two separate phase functions that work in both the frequency and space domains [4].

3. DCT & DWT

This section provides conceptual explanations for mathematical methods such as Discrete Cosine Transform (DCT) and DWT. The DCT performs best when utilizing cosine functions with many wavenumbers, each with spectral coefficients and actual value warnings [6-7]. The inverse discrete cosine transforms (IDCT) and 1-dimensional (1-d) DCT collection are used to recover real signals from DCT coefficients. Two of the most important DCT packages are image and signal compression [5-6]. Basic information related to DRPE based image encryption is explained in [8]. DRPE with DWT is Explained in [9]. DWT Decompose image into different frequency components. In DWT based Image encryption, wavelet coefficients are manipulated to enhance security and make attacks more difficult [8, 10].

4. SHA-256

SHA-256 (Secure Hash Algorithm 256-bit) is an example of a hash algorithm used for data integrity and security. SHA-256 implementation is shown in [11-13]

5. Literature Survey

In response to the growing need for secure image transmission, numerous optical encryption techniques have been proposed using transformations such as Fresnel, Fourier, Hartley, and Double Random Phase Encoding (DRPE) to enhance security. One early method by Liang et al. introduced a key rotation, multiplexing technique in Fresnel domain, generating white noise ciphertexts for Boolean images using rotating phase masks, although it was unsuitable for grayscale (i.e. gray image) data [14]. Elshamy et al. proposed a DRPE-based method combined with chaotic baker mapping and random phase mask, which increasing randomness and robustness against cryptanalysis, though real-time applications suffered due to increased complexity [15]. Similarly, Pan et al. used a double-stranded visual coding scheme that encrypts image halves using different phase masks, boosting privacy [16]. Hybrid approach for image encryption followed by image compression operation is explained in [17].

6. Proposed Methodology

The main limitations of Double Random Phase Encoding require multiple keys for encryption and decryption, increasing system complexity, and its optical implementation is difficult, making practical deployment challenging. So here is the need to develop more secure techniques. The proposed technique results in hiding information in such a way that only authorized users will be able to retrieve it, whereas the encrypted information will still have hidden statistical properties, it will be resistant to destruction by potential attackers.

Step 1: Key Generation using Hyperelliptic Curve Cryptography (HECC): A process in which cryptography keys are generated based on a hyperelliptic curve C , a prime number p , and a divisor D . The sender will then choose randomly a prime number K_A within the previously specified field Z_N and it must ensure randomness and unpredictability. The formulae used in generating the public key P_A are:

$$P_A = K_A \cdot D$$

where P_A is represented as two polynomials $(u(x), v(x))$. This key pair, (K_A, P_A) , serves as the foundation for secure encryption and decryption.

Step 2: Image Preprocessing and ASCII Conversion: The original image (say $I(x, y)$) is initially converted into the ASCII form of the image, in which each pixel intensity value is assigned a distinct ASCII code. The resulting ASCII values are converted to sequences, (U_x, V_y) , such that numeric encryption can be achieved using HECC.

Step 3: Encryption Process using HECC: After preprocessing, encryption is performed using P_B , which is the recipient's public key. Both sender and recipient agree on a shared key using the equation

$$Q_A = K_A \cdot P_B$$

where P_B is the receiver's public key. The plaintext message E_m (ASCII representation of the image) is encrypted using:

$$C_m = (Q_A, E_m \cdot P_A)$$

where C_m represents the encrypted ciphertext and is stored as a pair of polynomials, $(u(x), v(x))$, ensuring lightweight security with minimal computational cost.

Step 4: Image Encryption using Discrete Wavelet Transform (DWT):

The image that was encrypted is also processed under Discrete Wavelet Transform (DWT) to provide security and attack resistance. The picture is divided into two parts: Section A (where encrypted data is embedded) and Section B (which is not manipulated and remains unchanged to make the whole thing more robust). The DWT operation breaks the image into frequency components, and the encrypted message is injected into the frequency domain by a comparison-based technique. The final encrypted image comes by way of Inverse DWT (IDWT), which is saved or sent.

Step 5: Integrity Verification using SHA-2 Hashing: To prevent tampering and ensure data integrity, the SHA-2 hashing algorithm is applied before encryption. The sender generates a unique hash of (M) of the image:

$$H(M) = \text{SHA2}(M)$$

This hash is transmitted alongside the encrypted data. The recipient, after decrypting the image, recomputes the hash and compares it $H(M)$ to verify integrity. Any mismatch indicates data manipulation.

Step 6: Decryption Process using HECC: At the recipient's end, decryption follows the reverse process and applies the validation process to validate the secrete image. Validation process is presented in fig. 1(b). The recipient extracts Q_A and applies their private key K_b to decrypt the message.

The decrypted ASCII values are converted back into an image format to retrieve the original image. If the SHA-2 hash matches, the integrity is verified, ensuring a successful and tamper-proof decryption.

Step 7: Optimized Search and Access Control Using Boolean Search & Proxy Re-Encryption: A Boolean search mechanism is integrated into the encryption model to retrieve encrypted images without decryption efficiently. Users can search encrypted images using homomorphic Boolean queries without accessing plaintext data. A proxy re-encryption mechanism also allows for fast key updates without decrypting stored images. The block diagram of the proposed methodology encryption is shown in Fig. 1(a) and Validation scheme of decryption process in Fig. 1(b).

7. Numerical Analysis

A comprehensive comparative analysis has been conducted to evaluate the effectiveness of the proposed image encryption technique against the traditional Double Random Phase Encoding (DRPE) method. The numerical simulations for image encryption were conducted in Python using a set of standard 512×512 test images, namely *Baboon*, *Fruits*, *Plane*, *House*, *Cameraman*, and *Boat*. The evaluation was based on widely accepted performance metrics, these are: (1) Peak Signal-to-Noise Ratio (PSNR), (2) Number of Pixels Change Rate (NPCR), (3) Unified Average Changing Intensity (UACI), (4) entropy, [18], and (5) Structural Similarity Index Measure (SSIM)[19].

Proposed technique gives lesser PSNR then DRPE, indicating higher distortion and thus stronger encryption (PSNR is calculated between original image and encrypted image). Proposed technique gives higher UACI (i.e. 32.66%), and good NPCR (i.e. 96.55%). entropy values near the theoretical maximum of 8, and high SSIM values, demonstrating strong security, good visual quality where needed, and computational efficiency.

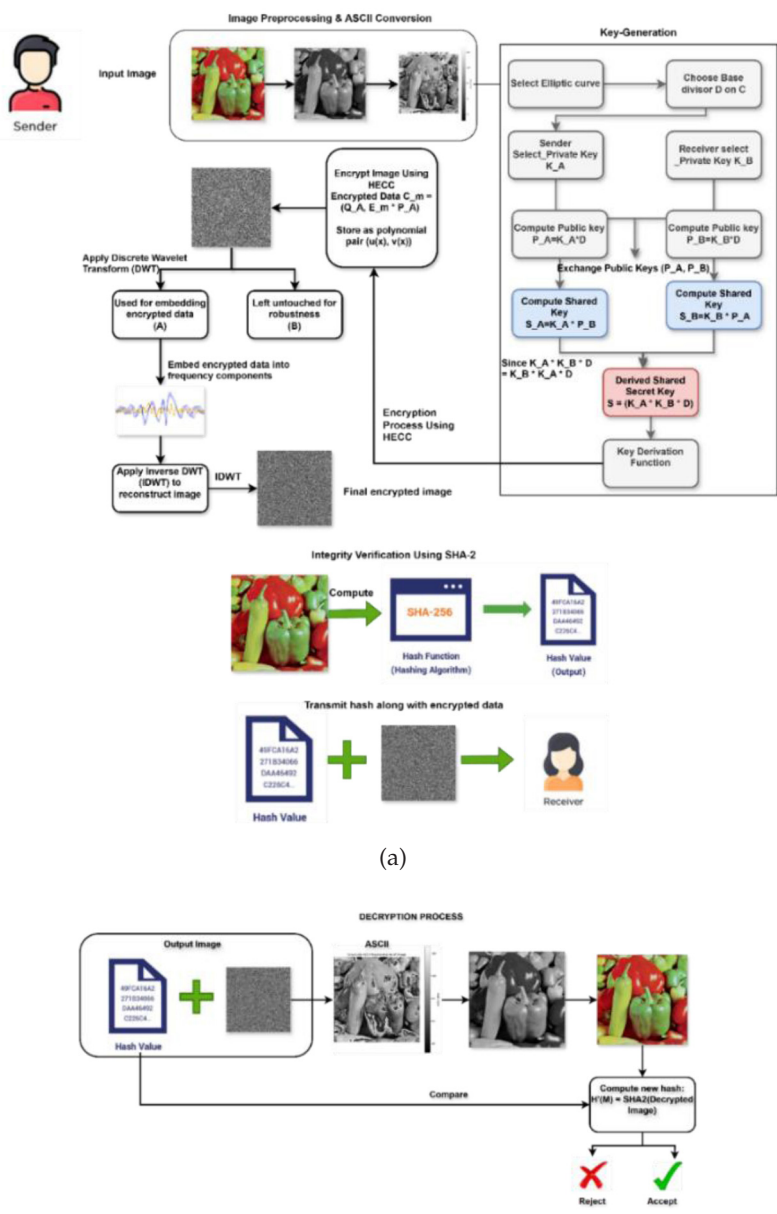
These matrices are shown in Table 1 and Table 2. Histogram analysis further validates the effectiveness of the encryption process; this is depicted in Fig.2. In terms of attack resistance, the encryption method exhibits strong resilience. Ciphertext-Only Attack (COA) values average around 127.5, demonstrating a high degree of randomness. Known-Plaintext Attack (KPA) values range from 85.1847 to 85.9183, while Chosen-Plaintext Attack (CPA) values remain consistent around 85.07–85.6, all indicating robust diffusion and minimal information leakage. Chosen-Ciphertext Attack (CCA) values are stable at approximately 81.82, showing that ciphertext modifications have no exploitable impact on decryption. Finally, Mean Absolute Difference (MAD) values from 5 attempts further confirm the consistency and unpredictability of the encryption, this is shown in Table 3. Overall, the proposed method offers superior security, reduced execution time, and strong resistance to a wide range of cryptographic attacks and cyber bullies.

Table 1
Metrics of encrypted images

Images	Size	PSNR	NPCR	UACI	Entropy	SSIM
Baboon	512x512	9.52	99.62	29.23	7.3579	0.0079
Fruits	512x512	8.22	98.53	31.67	7.8843	0.0082
Plane	512x512	7.31	99.87	31.54	7.9933	0.0091
House	512x512	8.21	97.45	31.45	7.8876	0.0099
Cameraman	512x512	7.77	96.55	32.66	7.9973	0.0093
Boat	512x512	9.32	97.34	29.44	7.1914	0.0094

Table 2
Comparative analysis of proposed technique and DRPE technique.

Cameraman Image(512x512)							
	PSNR	SSIM	UACI	NPCR	Entropy	MSE	Exec Time (sec.)
DRPE	8.0661	0.008906	31.12	97.44	7.99935	10150.100613	0.021943
Proposed	7.7740	0.0093	32.66	96.55	7.9973	10856.164219	0.000170



(b)
Figure 1(a)

Block diagram of the proposed methodology for encryption. 3(b) Validation scheme of decryption process.

Figure 2 shows the obtained results and their histogram analysis.



Figure 2
Original and encrypted image generated from the proposed work and their Histogram analysis

Table 3 shows the results after applying attack for 5 attempts.

Table 3
MAD—Mean Absolute Difference for 5 attempts

Attack attempt	COA	KPA	CPA	CCA
1	127.422	85.9183	85.0702	81.8282
2	127.56	85.6046	85.5667	81.8282
3	127.292	85.1847	85.3749	81.8282
4	127.753	85.1588	85.632	81.8282
5	127.667	85.5216	85.6445	81.8282

8. Conclusion

The comparative evaluation of the proposed Hyperelliptic Curve Cryptography (HECC) with Discrete Wavelet Transform (DWT) encryption scheme against the Double Random Phase Encoding (DRPE) method on the Cameraman (512×512) image confirms the superior security performance of the proposed approach. When measuring the PSNR between the original and encrypted images, the proposed method yields 7.7740 dB, which is slightly lower than DRPE’s 8.0661 dB. This intentional reduction ensures higher visual distortion in the encrypted image, thereby enhancing resistance to statistical and visual reconstruction attacks. The SSIM improves from 0.008906 in DRPE to 0.0093 in the proposed method, indicating slightly better preservation of structural information during

encryption. Security metrics remain strong, with NPCR at 96.55% and UACI at 32.66%, reflecting high sensitivity to pixel changes and excellent diffusion properties. Execution time is notably improved in the proposed method. Overall, the HECC-DWT scheme achieves a better balance between encryption robustness, computational efficiency, and attack resistance, making it a strong candidate for secure image transmission applications.

References

- [1] B. Javidi, G. Zhang, and J. Li, "Encrypted optical memory using double random phase encoding," in *Conf. Proc. LEOS'96 9th Annual Meeting IEEE Lasers and Electro-Optics Society*, vol. 1, pp. 364–365 (1996).
- [2] A. Alfalou and A. Mansour, "Double random phase encryption scheme to multiplex and simultaneously encode multiple images," *Appl. Opt.*, vol. 48, no. 31, pp. 5933–5947 (2009).
- [3] A. Malsaria, P. Vyas, and M. Kaur, "Enhancing image security and privacy with hybrid double random phase encoding, Lorenz maps, and compressed sensing," Unpublished.
- [4] A. Malsaria, P. Vyas, and M. Kaur, "Design and implementation of optical image communication encoding grounded on optical Fourier transform," *J. Opt. Commun.*, vol. 45, no. s1, pp. s1759–s1767 (2025).
- [5] H.-E. Hwang, "Optical color image encryption based on the wavelength multiplexing using cascaded phase-only masks in Fresnel transform domain," *Opt. Commun.*, vol. 285, no. 5, pp. 567–573 (2012).
- [6] Z. Liu, M. L. Yang, and W. Q. Yan, "Image encryption based on double random phase encoding," in *Proc. 2017 Int. Conf. Image and Vision Computing New Zealand (IVCNZ)*, Christchurch, New Zealand, pp. 1–6 (2017).
- [7] J. M. Vilaridy O., C. J. Jimenez, and C. O. Torres M., "Optical image encryption system using several tilted planes," *Photonics*, vol. 6, no. 4, p. 116 (2019).
- [8] Q. Gong, H. Wang, Y. Qin, and Z. Wang, "Modified diffractive-imaging-based image encryption," *Opt. Lasers Eng.*, vol. 121, pp. 66–73 (2019).
- [9] J. Liu, M. Zhang, X. Tong, and Z. Wang, "Image compression-encryption algorithm based on 2D compressive sensing and double random

- phase encoding," in *J. Phys.: Conf. Ser.*, vol. 1684, no. 1, IOP Publishing, p. 012123 (2020).
- [10] V. Rajasekar, J. Premalatha, and K. Sathya, "Cancelable iris template for secure authentication based on random projection and double random phase encoding," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 2, pp. 747–762 (2021).
 - [11] S. Gueron, S. Johnson, and J. Walker, "SHA-512/256," in *Proc. 2011 8th Int. Conf. Information Technology: New Generations*, IEEE, pp. 354–358 (2011).
 - [12] H. Yoshida and A. Biryukov, "Analysis of a SHA-256 variant," in *Int. Workshop on Selected Areas in Cryptography*, Springer, pp. 245–260 (2005).
 - [13] H. Gilbert and H. Handschuh, "Security analysis of SHA-256 and sisters," in *Int. Workshop on Selected Areas in Cryptography*, Springer, pp. 175–193 (2003).
 - [14] X. Yong-Liang, X. Su, S. Li, X. Liu, and S. Zeng, "Key rotation multiplexing for multiple-image optical encryption in the Fresnel domain," *Opt. Laser Technol.*, vol. 43, no. 4, pp. 889–894 (2011).
 - [15] A. M. Elshamy, A. M. Abd El-Hamid, A. A. M. Khalil, and A. A. A. El-Latif, "Optical image encryption based on chaotic baker map and double random phase encoding," *J. Lightw. Technol.*, vol. 31, no. 15, pp. 2533–2539 (2013).
 - [16] W. Pan and J. Qiao, "An iterative optical image encryption based on double random phase," in *Proc. 2010 Int. Conf. Computer Application and System Modeling (ICCASM)*, vol. 14, IEEE, pp. V14-80–V14-83 (2010).
 - [17] N. V. Thakur, K. Deshmukh, S. A. Shah, and V. B. Semwal, "A scheme for encrypted image data compression," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 2A, pp. 409–420 (2024).
 - [18] H. Bourekouche, S. Belkacem, and N. Messaoudi, "Design and analysis of a pseudo random number generator based on the logistic-sine system and a nonlinear feedback shift register: Application to image encryption," *J. Discrete Math. Sci. Cryptogr.*, pp. 1–26 (2025).
 - [19] U. Pilia, M. Kumar, and V. Mittal, "Performance evaluation of LSB steganography based on multiple image formats," *J. Discrete Math. Sci. Cryptogr.*, vol. 26, no. 7, pp. 1911–1924 (2023).