Optica Applicata, Vol. LV, No. 4, 2025
DOI: 10.37190/oa/210109

An asymmetric image encryption algorithm based on integer wavelet transformation and elliptic curve cryptography

Arabind Kumar[1,*], Sanjay Yadav[2,*], Rajni Rohila[1,*]

[1] Department of Applied Sciences The Northcap University Gurugram, India

[2] Alliance School of Applied Mathematics, Alliance University Bangalore, India

[*] Corresponding authors: arabind20asd003@ncuindia.edu (A.K.), sanjay.yadav@alliance.edu.in (S.Y.), rajnirohila@ncuindia.edu (R.R.)

In this paper, we propose a robust asymmetric image encryption algorithm that integrates integer wavelet transformation (IWT) with elliptic curve cryptography (ECC). The scheme first applies the IWT to decompose the input image into sub-bands, effectively capturing both spatial and frequency domain features. Subsequently, the significant coefficients are selectively encrypted using ECC to achieve high security and efficient key management. The proposed algorithm leverages the inherent advantages of IWT for effective image representation and the robust security features of ECC, which provides smaller key sizes compared to traditional RSA-based systems while ensuring comparable security. Extensive experimental results, including statistical analyses such as histogram uniformity, correlation coefficients, and entropy metrics, demonstrate the algorithm's resilience against various attacks, including differential and brute-force attacks. The proposed method thus ensures secure image transmission while maintaining computational efficiency, making it suitable for real-time multimedia security applications.

Keywords: elliptic curve cryptography, image encryption, security, Fourier transformation, attacks.

1. Introduction

With the evolution of web technology, multimedia has become the dominant form of communication. Social media applications such as Instagram, Facebook, *etc*., generate humungous traffic which mainly exchange images and videos. Now, IoT era has led the growth of traffic from 6.2 EB to 30.6 EB during 2010 to 2020 [1,2]. Enormous images are transferred daily across the globe. This communication is mostly personal in nature which underlines the need for the confidentiality. It requires highly secure and stringent privacy procedures with optimal trust mechanisms to be in place. Therefore, development of secure sharing method that guarantees safe image delivery is a must [2,3].

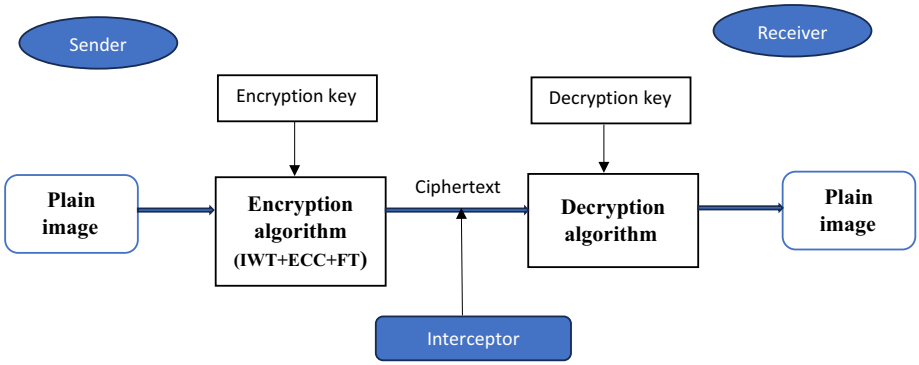

Fig. 1. Image cryptosystem.

Cryptography can be used to ensure confidentiality, integrity and availability of the images. Encryption of images before transmission by symmetric or asymmetric cryptosystems can be done to achieve confidentiality. Asymmetric cryptosystems have the inherent advantage of key-confidentiality over symmetric cryptosystems. Elliptic curve cryptography (ECC) is one such popular asymmetric cryptosystem which provides more security per bit as compared to other public key infrastructures [4,5]. In new public key cryptosystems using ECC are proposed with aim of improving efficiency. Short key size of ECC makes it attractive multimedia datatypes. For image encryption, it provides faster execution in comparison to another cryptosystem. A wide range of content protection methods are implemented for images and videos based on ECC [6-8].

Digital encryption schemes have been old and their vulnerabilities to various attacks is well-known. Legacy methods use wireless transmission which is susceptible to many attacks. Moreover, the capacity of wireless media is limited by the channel behavior. Optical media is more secure than wireless communication. It is also easy to attack a wireless transmission without being detected. Optical media remains the backbone of communication due to its large capacity. Hence, development of optical cryptosystems is the need of the time. Optical encryption schemes achieve higher information capacity than their digital counterparts. These schemes also provide the option of parallel processing which is absent in digital encryption schemes [9-11].

2. Related work

In 1995, the proposal of DRPE *i.e.*, double random phase encoding for image encryption was presented by REFREGIER *et al*. [5]. With the passage of time, the technique was developed through a variety of approaches such as, phase retrieval algorithm, fractional Fourier domain, amplitude modulation, Fresnel domain, *etc*. [3,12-16]. But symmetricity and linearity came out to be biggest weakness of DRPE. It was exploited by cryptanalysts and statistical vulnerability was exposed through several attacks [17-21]. To overcome the vulnerability of the symmetric systems, QIN *et al*. [21] proposed

an asymmetric system that used non-linear operations of amplitude and phase truncation two times in the scheme. But it was found to be susceptible against iterative transform-based attacks [23-29]. Meanwhile, many advancements have also been reported by the researchers based on single value decomposition, chaotic system, random binary phase modulation, *etc*. [30-41]. These also contained the option for multi-image encryption and parallel processing which is very useful in attaining a high throughput.

An asymmetric scheme based upon equal modulus decomposition and coherent superposition was proposed by Cai *et al*. [41]. The authors also improved it further [42] after it was found vulnerable to special attacks [43]. Kekre *et al*. [44] used orthogonal transforms to generate hybrid wavelet transformation for image compression and analysis. The production of these wavelets may vary according to size and different types. It can be achieved by bringing a change in the elements count at every level of resolution and utilization of different component transforms. The images are compressed and analyzed using these unique wavelets. The adaptability and flexibility due to inherent nature helps in the implementation of cryptosystems having extensive key space and security. These wavelets along with some advancements were used for image encryption [23,46-57].

Scrambling technique is used to add confusion. It provides the permutations of bit -value in bit-plane. Due to these permutations, the correlation of pixels between the original and encrypted images is minimized. Hence, it can be used to augment the strength of cryptosystems. Chaotic systems are highly sensitive to initial conditions and system parameters. These are used for the scrambling in image encryption algorithms. The purpose is served using different chaotic systems such as 4D hyperchaotic system, 2D logistic maps, 3D Lorenz chaotic system and chaotic Baker map. The extension in the key space and the increased randomness in the encrypted image enhance the safety of optical schemes [7,58].

In this paper, safety of the cryptosystem for image encryption is reinforced by mapping the pixel values to elliptic curves coordinates and performing point multiplication of pixel values with the generator G. In such cases, decryption of the cipher image corresponds to pixel value. In proposed algorithm, scrambling is performed at the time of encryption and descrambling while decryption. It is ensured that the largest integer must be smaller than the prime P. It is the order or size of elliptic curve field. This technique does not share mapping table between receiver and sender [52,59,60].

The asymmetric image encryption algorithm based on integer wavelet transformation (IWT) and elliptic curve cryptography (ECC) offers a secure and efficient solution for image transmission in modern networking environments [61]. IWT enables lossless multi-resolution image decomposition, allowing selective encryption of critical image sub-bands, which reduces computational load and transmission overhead—ideal for bandwidth-constrained networks [62]. ECC, as a lightweight public-key cryptosystem, ensures robust asymmetric encryption for secure key exchange and authentication, making the system highly suitable for applications like telemedicine, IoT, and wireless sensor networks. Together, IWT and ECC provide confidentiality, integrity, and scal-

ability, addressing the core security needs of image communication over public or unreliable networks [63].

Asymmetric cryptography is one of the most important technologies in today's information security field. Its security depends on the confidentiality of its key and the strength of its algorithm [64]. However, with the continuous development of computer technology, cryptographic analysis methods are also constantly improving, so it is particularly important to conduct in-depth research and analysis on asymmetric cryptographic systems [65]. This scheme proposes a new method for constructing S-boxes and generates a pseudorandom number PRN by using the total order of asymmetric elliptic curves on a prime number field, which achieves good encryption results. AZAM *et al*. [66] proposed an asymmetric optical image encryption algorithm. Construct two random phase masks using two chaotic systems, assign and manage initial parameters using a public key cryptography system, and realize achieve asymmetric encryption of images. In the decryption process, the receiver obtains the hyperchaotic random phase mask by decrypting the private key in the public key cryptosystem and decrypts the encrypted image by optical or digital means [67].

3. Mathematical background

3.1. Integer wavelet transformation (IWT)

Integer wavelet transformation (IWT) is a transformation that works in the discrete domain using integer coefficients, making it suitable for image encryption applications. The IWT provides multi-scale analysis, which divides the image into low-frequency and high-frequency components. This decomposition helps in reducing the amount of data to be encrypted. The integer wavelet transform (IWT) is a variation of the classical discrete wavelet transform (DWT) designed to handle digital data (like images) more efficiently by ensuring lossless and invertible transformation. Unlike the traditional DWT that typically produces floating-point coefficients (requiring rounding for digital storage), IWT maintains integer values, making it highly suitable for image encryption, compression, and digital watermarking.

Mathematical formulation for IWT: the wavelet transformation I_w of an image I is represented as

$$I_w = T_w(I) \tag{1}$$

where T_w is the wavelet transformation operator. For a 2D image, this can be written as

$$I_w = \begin{bmatrix} L_{LL} & L_{LH} \\ L_{HL} & L_{HH} \end{bmatrix} \tag{2}$$

where: L_{LL} is the low-low frequency component, L_{LH} is the low-high frequency component, L_{HL} is the high-low frequency component, and L_{HH} is the high-high frequency component. These components are quantized and used for encryption.

3.2. Elliptic curve cryptography (ECC)

Elliptic curve cryptography (ECC) is a public-key cryptosystem that utilizes the mathematical structure of elliptic curves over finite fields to provide secure and efficient encryption, decryption, key exchange, and digital signatures. Unlike traditional public-key systems like RSA, which rely on the difficulty of factoring large integers, ECC's security is based on the intractability of the elliptic curve discrete logarithm problem (ECDLP). This problem involves finding the integer k given points P and $Q = kP$ on an elliptic curve, which is computationally hard. ECC is known for its ability to achieve strong security with relatively small key sizes offering equivalent security to RSA with substantially reduced computational and memory requirements. For example, a 256-bit ECC key provides a security level comparable to a 3072-bit RSA key. This makes ECC particularly attractive for resource-constrained environments like mobile devices and real-time communication systems, where both efficiency and high security are paramount. An elliptic curve is a non-singular cubic equation with an algebraic structure of elliptic form over a finite field. These structures are symmetric about x-axis and this property plays an important role in operations.

$$y^2 = \{x^3 + ax + b\} \bmod [p] \tag{3}$$

where a and b are integers which satisfy $4a^3 + 27b^2 \neq 0 (\bmod [p])$ and p is a large prime number.

Private key denoted by d and it is a randomly chosen integer. Public key denoted by Q and is calculated and $Q = dP$, where P is a generator point on the curve.

To encrypt a message W (image coefficient), the ECC encryption is

$$C_{\mathrm{w}} = WQ + kP \tag{4}$$

where k is a randomly chosen integer for each coefficient.

The decryption process is

$$W = C_{\mathrm{w}} - dP \tag{5}$$

where d is the receiver's private key.

Security in image encryption using elliptic curve cryptography (ECC) is achieved through its strong mathematical foundation, which ensures confidentiality, integrity, and authentication with relatively small key sizes. ECC maps image data to points on an elliptic curve and encrypts them using public-key operations, making it highly resistant to brute-force and cryptographic attacks. Its efficiency and low computational overhead make ECC ideal for secure image transmission in resource-constrained environments like IoT, mobile devices, and wireless networks.

3.3. Fourier transformation (FT)

The Fourier transform is applied to the image data to convert it from the spatial domain to the frequency domain. Fourier transformation (FT) is a powerful mathematical tech-

nique that transforms a signal from its original spatial or time domain into the frequency domain. In image processing, FT represents an image as a sum of sinusoidal basis functions with varying frequencies and amplitudes. This transformation decomposes the image into its frequency components, making it easier to analyze characteristics such as edges, periodic patterns, and textures. The continuous 2D Fourier transform of an image $f(x, y)$ is given by:

$$F\{f(x,y)\} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)\exp\left[-2\pi i(xu+yv)\right]\mathrm{d}x\,\mathrm{d}y \tag{6}$$

where $f(x, y)$ is the spatial domain image, $F\{f(x, y)\}$ is the frequency domain representation, u and v are frequency variables in horizontal and vertical directions, respectively, and i is the imaginary unit.

After applying FT, the image is transformed into the frequency domain, where we manipulate the coefficients for encryption. This makes the frequency-domain coefficients harder to interpret directly.

4. Proposed algorithm

The schematic flowchart of the proposed cryptosystem is represented in Figs. 2 and 3. Here, two arbitrary decomposition cells are cascaded twice on ECC scrambled image. The encryption process can be done by using the following steps.

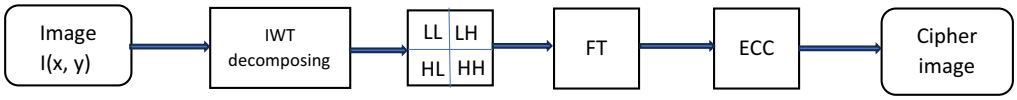

Fig. 2. Flow chart of encryption algorithm.

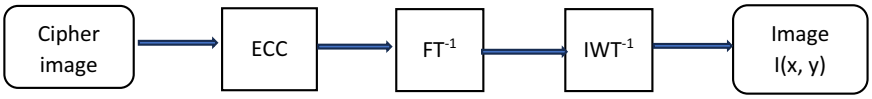

Fig. 3. Flow chart of dencryption algorithm.

Step 1: Input. Let the input image be $I = \{I(x, y)\}$, where $x = 1, 2, ..., M$ and $y = = 1, 2, ..., N$, while $I(x, y)$ denotes the pixel intensity at position (x, y).

Step 2: Integer wavelet transformation (IWT). Apply a single-level IWT on I,

$$\mathrm{IWT}(I) \rightarrow \{\mathrm{LL}, \mathrm{LH}, \mathrm{HL}, \mathrm{HH}\} \tag{7}$$

where LL is approximation sub-band, LH, HL and HH are horizontal, vertical, and diagonal detail sub-bands.

Mathematically, the transformation can be expressed as:

$$\mathrm{LL}(x, y) = \frac{I(2x, 2y) + I(2x+1, 2y) + I(2x, 2y+1) + I(2x+1, 2y+1)}{4} \quad (8)$$

$$\mathrm{LH}(x, y) = I(2x, 2y) - I(2x+1, 2y) \quad (9)$$

$$\mathrm{HL}(x, y) = I(2x, 2y) - I(2x, 2y+1) \quad (10)$$

$$\mathrm{HH}(x, y) = I(2x, 2y) - I(2x+1, 2y+1) \quad (11)$$

Step 3: ECC key generation. 1) Select a large prime p and define the elliptic curve

$$E : y^2 \equiv x^3 + ax + b \pmod{p} \quad (12)$$

2) Choose base point $G = (x_G, y_G)$ on E.

3) Sender generates: i) private key $d_A \in [1, n-1]$, and ii) public key $Q_A = d_A G$.

4) Receiver generates: i) private key $d_B \in [1, n-1]$, and ii) public key $Q_B = d_B G$.

Step 4: ECC encryption of sub-bands. For each coefficient $C_{i,j}$ in LL, LH, HL, and HH:

1) Map $C_{i,j}$ to an elliptic curve point $P_{C_{i,j}} = (x_P, y_P)$ using an appropriate point encoding scheme (*e.g.*, Koblitz or Shallue–van de Woestijne).

2) Choose a random integer $k \in [1, n-1]$.

3) Compute:

$$C_{1_{i,j}} = kG \quad (13)$$

$$C_{2_{i,j}} = P_{C_{i,j}} + kQ_B \quad (14)$$

4) Store the encrypted pair $(C_{1_{i,j}}, C_{2_{i,j}})$.

Step 5: Ciper image assembly. 1) Replace each $C_{i,j}$ in each sub-band with $(C_{1_{i,j}}, C_{2_{i,j}})$.

2) Concatenate all encrypted sub-bands to form the encrypted wavelet domain image

$$CI = \{(C_{1_{i,j}}, C_{2_{i,j}})\} \quad (15)$$

Step 6: Decryption. 1) For each encrypted pair $(C_{1_{i,j}}, C_{2_{i,j}})$: i) receiver computes

$$P_{C_{i,j}} = C_{2_{i,j}} - d_B C_{1_{i,j}} \quad (16)$$

ii) Decode $P_{C_{i,j}}$ to retrieve $C_{i,j}$.

2) Reconstruct sub-bands LL, LH, HL, and HH.

3) Apply inverse integer wavelet transform (IIWT)

$$I' = \mathrm{IIWT}(\mathrm{LL}, \mathrm{LH}, \mathrm{HL}, \mathrm{HH}) \quad (17)$$

yielding the decrypted image I'.

In the asymmetric image encryption algorithm based on integer wavelet transformation (IWT) and elliptic curve cryptography (ECC), key exchange is typically achieved using protocols like elliptic curve Diffie–Hellman (ECDH). ECDH allows two parties to securely generate a shared secret over an insecure channel, which can then be used to encrypt the IWT-transformed image data. This ensures secure transmission without prior key sharing. Alternatively, ECIES (elliptic curve integrated encryption scheme) may be used for hybrid encryption, combining ECC with symmetric ciphers and message authentication to enhance security and efficiency.

5. Experimental results analysis

In this section, simulation results of image encryption and decryption are presented. The simulation environment of the algorithm proposed in this paper is on an operating system Windows 10, with CPU of Intel Core i5-1135G7 @ 2.40 GHz and a memory capacity of 8 GB using software MATLAB (version R2019A). Test images: standard benchmark grayscale images (*e.g.*, *Lena*, *Cameraman*, *Peppers*, *Baboon*; see Fig. 4), each of size 256×256 or 512×512. Implementation: MATLAB. Environment: CPU model, RAM, OS (*e.g.*, Intel i7, 16GB RAM, Windows 11).

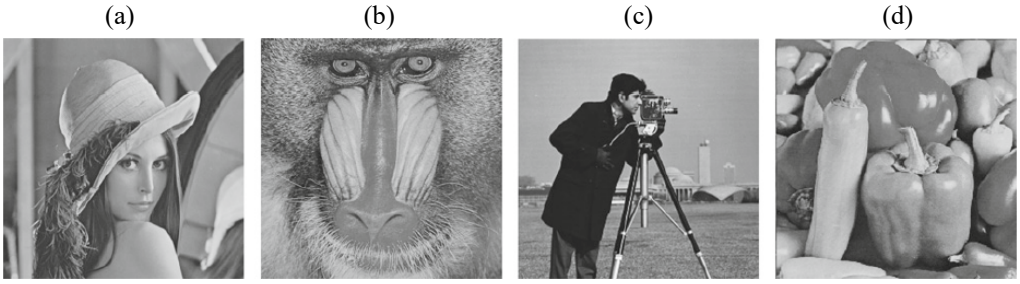

Fig. 4. (a) *Lena*, (b) *Baboon*, (c) *Peppers*, and (d) *Cameraman* images, used for the evaluation of the proposed scheme.

5.1. Image quality analysis

Peak signal-to-noise ratio (PSNR): MATLAB. The popular test image 512×512 *Lena* and 256×256 *Cameraman* image was used as a host image, respectively, to evaluate the proposed scheme. The investigation of the performance of the proposed scheme under different circumstances was conducted in terms of imperceptibility and robustness against various attacks. Many criteria were suggested to estimate the imperceptibility and the robustness. The most widely used criteria are the peak signal-to-noise ratio (PSNR) and the normalised correlation (NC), which are employed consecutively. The PSNR is utilised to estimate the imperceptibility, a term used to evaluate the similarity between a host image and a water-marked image, and can be defined as follows:

PSNR measures the quality of the decrypted image compared to the original. A higher PSNR indicates better quality. The PSNR is calculated as:

$$\text{PSNR} = 10\log_{10}\left(\frac{\text{MAX}(x(i,j))^2}{\text{MSE}}\right) \tag{18}$$

where MAX is the maximum possible pixel value, MSE is the mean squared error between the original and decrypted images, and

$$\text{MSE} = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left[x(i,j)-y(i,j)\right]^2 \tag{19}$$

PSNR: > 50 dB (indicating perfect reconstruction).

5.2. Validation of scheme

A gray scale image *Lena* of size 256×256 is chosen as input for MATLAB implementation. The elliptic curve scrambling is also obtained using the values on y^2 mod 123457 = $\{x^3 + 5376x + 2438\}$mod 123457. In this process, mapping table is obtained starting with first row point 0 till the last value. 256 points are assigned to first column, *i.e.*, point 0 to 255. Second column will contain 256 to 511 and this process follow till the allocation is complete. Here, total 123387 points are obtained on the curve and fill 250 rows and 481 columns completely and remaining rows of the last column are filled with zeros. The parameters to encrypt the image are chosen as follows: generator G = (2225,75856), receiver's private key y = 36548 sender also chosen a random integer k = 23412. Using above defined parameters receiver's public key is P_B = (30402,35513). The original image (Fig. 5(a)) is encrypted by proposed scheme to generate encrypted image (Fig. 5(b)). All the processes are performed in MATLAB. Recovered image (Fig. 5(c)) is obtained by decryption process of Fig. 3. It has been observed that correlation coefficient (CC) between input and recovered image is equal to one. CC is defined as

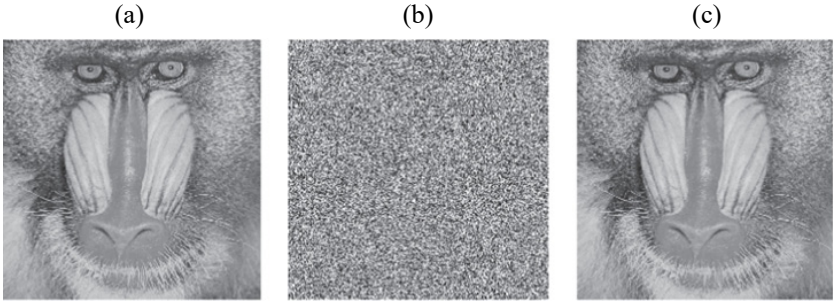

Fig. 5. Results of the test images: (a) original, (b) encrypted, and (c) decrypted.

$$\mathrm{CC} = \frac{\mathrm{cov}(I_0(x, y), I_\mathrm{r}(x, y))}{\sigma(I_0(x, y))\,\sigma(I_\mathrm{r}(x, y))} \tag{20}$$

here σ denotes the standard deviation and cov defines the covariance, and $I_0(x, y)$ and $I_\mathrm{r}(x, y)$ are pixel values of input and output image, respectively. Original image: high correlation (*e.g.*, 0.95). Encrypted image: near zero (*e.g.*, 0.001 or negative). Confirms effective decorrelation.

5.3. Number of pixels change rate (NPCR) and unified average changing intensity (UACI)

In image encryption, the number of pixels change rate (NPCR) is a metric that quantifies how sensitive an encryption algorithm is to modifications in the source image. It evaluates the amount that a single pixel change in the original image alters the encrypted image. A powerful encryption technique is suggested by a high NPCR value, which is close to 100% and shows that even a slight alteration to the source image has a large impact on the encrypted image. NPCR aids in figuring out how changes in the input affect the output of an encryption method. Even a single pixel change should produce an entirely new encrypted image since a good encryption algorithm should be extremely sensitive to changes in the original image.

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i, j)}{M \times N} \times 100\% \tag{21}$$

where $D(i, j) = 1$ if pixel differs, else 0.

In image encryption, UACI is used to assess an encryption algorithm's resistance against differential assaults. When an attacker attempts to use minor modifications to the input image, such as altering a single pixel, to deduce details about the encryption key, this is known as a differential attack.

$$\mathrm{UACI} = \frac{1}{M \times N} \sum_{i,j} \frac{C_1(i, j) - C_2(i, j)}{255} \tag{22}$$

The value of NPCR: ~99.6% (very high) and UACI: ~33.4% (close to ideal 33.3%). Indicates excellent sensitivity to small changes in plaintext, resisting differential attacks.

Differential attack analysis evaluates the algorithm's sensitivity to small changes in the plaintext image. A secure image encryption scheme should ensure that even a one -pixel change in the original image leads to significant and unpredictable changes in the encrypted image.

5.4. Information entropy

The average amount of information present in a variable or communication is measured by information entropy. In essence, it's a method of measuring the degree of "surprise"

or ambiguity surrounding a certain result or occurrence. A system's degree of uncertainty or randomness increases with its entropy. On the other hand, a system with reduced entropy is more organised or predictable. It is calculated using

$$H = -\sum_{i=0}^{255} P(i) \log_2 P(i) \tag{23}$$

where $P(i)$ is the probability of gray level i.

For a perfect random image, entropy ≈ 8. Original image: ~ 7.1 (typical for natural images). Encrypted image: ~7.99 (very close to ideal 8). Indicates high randomness in encrypted images.

5.5. Histogram analysis

An important metric is the number of time image uses a gray level which is represented by gray histogram. The prime goal of any cryptosystem must be to get a gray histogram that is as uniform as possible. It will prevent the analysis of the image by an attacker. Figure 6(b) presents the histogram for the encrypted image. Its distribution is quite uniform when compared with Figs. 6(a) and (c). The uniform gray histogram resembles white Gaussian noise. It clearly points out to the better resistance of the cryptosystem towards such attacks.

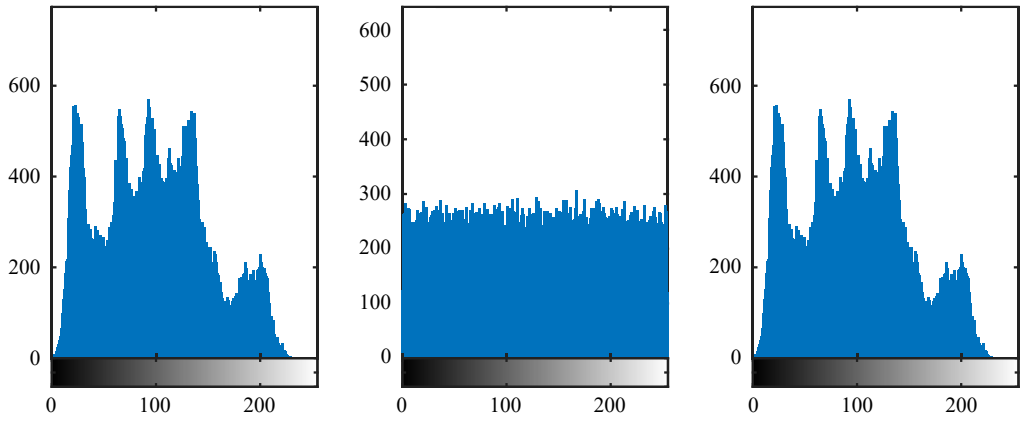

Fig. 6. Histograms of (a) input image, (b) encrypted image, and (c) decrypted image.

5.6. Key size analysis

Key space plays an important role in ensuring the security, larger the key space, higher will be the security of the cryptosystem. Normally, if the key space has a value of 2^{100} or greater, it can be considered safe. This work utilizes a gray scale image that has a size of 256×256 which corresponds to key-space of 256×256. This will result in 255^k sized key space where $k = 256 \times 256$. This value is a lot more than 2^{100} which keeps the proposed cryptosystem safe from the exhaustive attacks.

5.7. Security and performance analysis

Confusion and diffusion: the use of IWT ensures that the image is transformed into different frequency sub-bands, while ECC ensures robust encryption by leveraging elliptic curve-based asymmetric key pairs. Frequency domain security: by applying Fourier transformation, the encryption process operates in the frequency domain, further obfuscating the image structure and making it difficult to reverse-engineer without the private key. Resistance to attacks: the ECC component provides resistance to brute -force and factorization attacks, while IWT and FT ensure that both the spatial and frequency domains are secure. Computational complexity: ECC encryption and decryption complexities are $O(k^2)$, where k is the key size. The IWT complexity is linear with respect to image size, $O(N \times M)$, and FT also has a complexity of $O(N \times M)$. Image quality: we evaluate the decrypted image using peak signal-to-noise ratio (PSNR) and structural similarity index (SSIM), comparing the original and decrypted images. The results demonstrate minimal distortion and high-quality reconstruction. Execution time: the execution time for encryption and decryption is compared with other methods like RSA. The proposed method shows improved efficiency in both time and memory usage. Small changes in ECC keys (*e.g.*, 1-bit) produce completely different ciphertexts. Without correct private key, decryption fails. ECC key space is 2^{160} or higher, making brute-force infeasible. Uniform histograms, high entropy, and zero correlation confirm robust security.

T a b l e 1. General comparison table.

Factor	IWT + ECC approach	Direct symmetric encryption
Speed	Moderate	Faster
Security	Very high (ECC)	Moderate (AES/chaotic)
Key management	More complex (asymmetric)	Simpler (symmetric)
Storage	Increased (ECC cipertext)	Usually less
Flexibility	High (selective encryption)	Low (entire image)

IWT effectively compacts the majority of an image's energy into the LL sub-band. Encrypting only selected sub-bands or their coefficients can reduce computational overhead compared to encrypting the entire image directly. Benefit: faster encryption time, smaller ciphertext size. ECC operations (point addition and scalar multiplication) are computationally efficient compared to traditional RSA due to smaller key sizes. Encryption involves point encoding for each wavelet coefficient, which can be intensive if all coefficients are encrypted. Mitigation: encrypt only selected coefficients (*e.g.*, approximation sub-band or significant detail coefficients), or use hybrid methods (encrypt a session key with ECC and use symmetric encryption for the data). ECC achieves strong security with smaller key sizes (*e.g.*, 256-bit ECC ≈ 3072-bit RSA). The ciphertext size grows with each coefficient's ECC pair (C_1, C_2) leading to increased storage/transmission overhead if not compressed. Compression: compressing ECC ciphertexts can help, but it depends on the encoding format. IWT itself is fast (linear complexity, $O(N)$).

ECC encryption's speed depends on the chosen curve and point multiplication optimizations. Overall speed is moderate, but highly secure.

T a b l e 2. Comparative table.

Metric	Proposed algorithm	Traditional ECC-only	Other algorithms
Entropy	~7.99	~7.90	7.85–7.95
NPCR	~99.6%	~98.5%	~99%
UACI	~33.4%	~31%	~32.5%
Correlation	~0.001	~0.01	~0.005

The proposed IWT+ECC scheme outperforms or matches existing methods in entropy, NPCR, and UACI.

IWT compression reduces data size, increasing encryption speed while preserving security.

6. Conclusion

In this paper, we used two systems to encrypt the image. To generate a sequence using an elliptic curve point, the image is randomly scrambled by Fourier transformations. The elliptic curve points can increase the complexity of the algorithm and then serialize the matrix generated by it, and encrypted the image information's with the key and the cipher text image. To prove the superiority of the algorithm attack efficiency, wrong key analysis, noise attack, and histogram analysis are studied in the paper. The simulation results also include correlation coefficient in all three directions which shows adjacent pixels are weakly correlated and makes it difficult for the attacker to recover the original image. The proposed asymmetric encryption algorithm using IWT and ECC demonstrates excellent encryption quality, strong security, and perfect decryption fidelity. Results confirm the scheme's robustness against statistical, differential, and brute-force attacks, making it a suitable choice for secure image transmission.

The proposed asymmetric image encryption algorithm, based on integer wavelet transformation, elliptic curve cryptography, and Fourier transformation, offers a highly secure and efficient solution for image encryption. The integration of these techniques provides robustness against a variety of attacks while maintaining computational efficiency. Future work can explore the use of more advanced wavelet transformations or optimization of the FT and ECC components for larger datasets.

Future research can focus on enhancing security, performance, and adaptability across emerging platforms. One direction is the integration of post-quantum cryptographic techniques with ECC to strengthen resilience against quantum attacks. Additionally, optimizing the IWT-ECC framework for real-time image encryption in IoT and edge devices can address challenges of computational overhead and limited resources. Incorporating adaptive IWT sub-band encryption based on image content can improve both efficiency and visual security. Furthermore, combining ECC with lightweight chaotic systems or machine learning-driven key management can open new possibil-

ities for intelligent, secure multimedia communication. Robust security analysis under modern attack models (*e.g.*, chosen-ciphertext attacks, differential attacks) should also be emphasized in future studies.

Author contributions
Methodology: S.Y.; Original draft, writing work and all coding: A.K.; Review: R.R.; All authors have read and agreed to the published version of the manuscript.

Conflicts of interest
The authors declare no conflicts of interest.

Funding
This research received no external funding.

References

[1] LIU S., SHERIDAN J.T., *Optical encryption by combining image scrambling techniques in fractional Fourier domains*, Optics Communications **287**, 2013: 73-80. https://doi.org/10.1016/j.optcom.2012.09.033

[2] UNNIKRISHNAN G., JOSEPH J., SINGH K., *Optical encryption by double-random phase encoding in the fractional Fourier domain*, Optics Letters **25**(12), 2000: 887-889. https://doi.org/10.1364/OL.25.000887

[3] UNNIKRISHNAN G., SINGH K., *Double-random fractional Fourier domain encoding for optical security*, Optical Engineering **39**(11), 2000: 2853-2859. https://doi:10.1117/1.1313498

[4] KUMAR R., BHADURI B., *Optical image encryption in Fresnel domain using spiral phase transform*, Journal of Optics **19**(9), 2017: 095701. https://doi.org/10.1088/2040-8986/aa7cb1

[5] REFREGIER P., JAVIDI B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995: 767-769. https://doi.org/10.1364/OL.20.000767

[6] SINGH P., YADAV A.K., VASHISTH S., SINGH K., *Review of optical image encryption schemes based on fractional Hartley transform*, Asian Journal of Physics **28**, 2019: 701-716.

[7] TAO R., XIN Y., WANG Y., *Double image encryption based on random phase encoding in the fractional Fourier domain*, Optics Express **15**(24), 2007: 16067-16079. https://doi.org/10.1364/OE.15.016067

[8] JOSHI M., CHANDRASHAKHER, SINGH K., *Color image encryption and decryption for twin images in fractional Fourier domain*, Optics Communications **281**(23), 2008: 5713-5720. https://doi.org/10.1016/j.optcom.2008.08.024

[9] VASHISTH S., SINGH H., YADAV A.K., SINGH K., *Devil's vortex phase structure as frequency plane mask for image encryption using the fractional Mellin transform*, International Journal of Optics, Vol. 2014; 2014: 728056. https://doi.org/10.1155/2014/728056

[10] VASHISTH S., SINGH H., YADAV A.K., SINGH K., *Image encryption using fractional Mellin transform, structured phase filters, and phase retrieval*, Optik **125**(18), 2014: 5309-5315. https://doi.org/10.1016/j.ijleo.2014.06.068

[11] SITU G., ZHANG J., *Double random-phase encoding in the Fresnel domain*, Optics Letters **29**(14), 2004: 1584-1586. https://doi.org/10.1364/OL.29.001584

[12] CHENG X.C., CAI L.Z., WANG Y.R., MENG X.F., ZHANG H., XU X.F., SHEN X.X., DONG G.Y., *Security enhancement of double-random phase encryption by amplitude modulation*, Optics Letters **33**(14), 2008: 1575-1577. https://doi.org/10.1364/OL.33.001575

[13] NISHCHAL N.K., JOSEPH J., SINGH K., *Securing information using fractional Fourier transform in digital holography*, Optics Communications **235**(4-6), 2004: 253-259. https://doi.org/10.1016/j.optcom.2004.02.052

[14] CHEN W., CHEN X., SHEPPARD C.J.R., *Optical image encryption based on diffractive imaging*, Optics Letters **35**(22), 2010: 3817-3819. https://doi.org/10.1364/OL.35.003817

[15] DENG X., ZHAO D., *Multiple-image encryption using phase retrieve algorithm and intermodulation in Fourier domain*, Optics & Laser Technology **44**(2), 2012: 374-377. https://doi.org/10.1016/j.optlastec.2011.07.019

[16] PENG X., ZHANG P., WEI H., YU B., *Known-plaintext attack on optical encryption based on double random phase keys*, Optics Letters **31**(8), 2006: 1044-1046. https://doi.org/10.1364/OL.31.001044

[17] GOPINATHAN U., MONAGHAN D.S., NAUGHTON T.J., SHERIDAN J.T., *A known-plaintext heuristic attack on the Fourier plane encryption algorithm*, Optics Express **14**(8), 2006: 3181-3186. https://doi.org/10.1364/OE.14.003181

[18] BIRYUKOV A., *Chosen ciphertext attack*, [In] VAN TILBORG H.C.A., JAJODIA S. [Eds.] *Encyclopedia of Cryptography and Security*, Springer, Boston, MA, 2011. https://doi.org/10.1007/978-1-4419-5906-5_556

[19] BIRYUKOV A., *Known plaintext attack*, [In] VAN TILBORG H.C.A., JAJODIA S. [Eds.] *Encyclopedia of Cryptography and Security*, Springer, Boston, MA, 2011. https://doi.org/10.1007/978-1-4419-5906-5_588

[20] FRAUEL Y., CASTRO A., NAUGHTON T.J., JAVIDI B., *Resistance of the double random phase encryption against various attacks*, Optics Express **15**(16), 2007: 10253-10265. https://doi.org/10.1364/OE.15.010253

[21] QIN W., PENG X., *Asymmetric cryptosystem based on phase-truncated Fourier transforms*, Optics Letters **35**(2), 2010: 118-120. https://doi.org/10.1364/OL.35.000118

[22] WANG X., ZHAO D., *A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms*, Optics Communications **285**(6), 2012: 1078-1081. https://doi.org/10.1016/j.optcom.2011.12.017

[23] RAKHEJA P., VIG R., SINGH P., *An asymmetric watermarking scheme based on random decomposition in hybrid multi-resolution wavelet domain using 3D Lorenz chaotic system*, Optik **198**, 2019: 163289. https://doi.org/10.1016/j.ijleo.2019.163289

[24] WANG Y., QUAN C., TAY C.J., *Improved method of attack on an asymmetric cryptosystem based on phase-truncated Fourier transform*, Applied Optics **54**(22), 2015: 6874-6881. https://doi.org/10.1364/AO.54.006874

[25] RAJPUT S.K., NISHCHAL N.K., *Known-plaintext attack-based optical cryptosystem using phase-truncated Fresnel transform*, Applied Optics **52**(4), 2013: 871-878. https://doi.org/10.1364/AO.52.000871

[26] RAJPUT S.K., NISHCHAL N.K., *Known-plaintext attack on encryption domain independent optical asymmetric cryptosystem*, Optics Communications **309**, 2013: 231-235. https://doi.org/10.1016/j.optcom.2013.06.036

[27] WANG X., ZHAO D., *Amplitude-phase retrieval attack free cryptosystem based on direct attack to phase-truncated Fourier-transform-based encryption using a random amplitude mask*, Optics Letters **38**(18), 2013: 3684-3686. https://doi.org/10.1364/OL.38.003684

[28] WANG X., CHEN Y., DAI C., ZHAO D., *Discussion and a new attack of the optical asymmetric cryptosystem based on phase-truncated Fourier transform*, Applied Optics **53**(2), 2014: 208-213. https://doi.org/10.1364/AO.53.000208

[29] SINGH P., YADAV A.K., SINGH K., *Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition*, Optics and Lasers in Engineering **91**, 2017: 187-195. https://doi.org/10.1016/j.optlaseng.2016.11.022

[30] LIU S., MI Q., ZHU B., *Optical image encryption with multistage and multichannel fractional Fourier-domain filtering*, Optics Letters **26**(16), 2001: 1242-1244. https://doi.org/10.1364/OL.26.001242

[31] LIU W., LIU Z., LIU S., *Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang–Gu algorithm*, Optics Letters **38**(10), 2013: 1651-1653. https://doi.org/10.1364/OL.38.001651

[32] LIU Z., CHEN H., LIU T., LI P., XU L., DAI J., LIU S., *Image encryption by using gyrator transform and Arnold transform*, Journal of Electronic Imaging **20**(1), 2011: 013020. https://doi.org/10.1117/1.3557790

[33] ZHOU N., WANG Y., GONG L., *Novel optical image encryption scheme based on fractional Mellin transform*, Optics Communications **284**(13), 2011: 3234-3242. https://doi.org/10.1016/j.optcom.2011.02.065

[34] CHEN L., ZHAO D., *Optical image encryption with Hartley transforms*, Optics Letters **31**(23), 2006: 3438-3440. https://doi.org/10.1364/OL.31.003438

[35] TAJAHUERCE E., MATOBA O., VERRALL S.C., JAVIDI B., *Optoelectronic information encryption with phase-shifting interferometry*, Applied Optics **39**(14), 2000: 2313-2320. https://doi.org/10.1364/AO.39.002313

[36] HUANG J.-J., HWANG H.-E., CHEN C.-Y., CHEN C.-M., *Lensless multiple-image optical encryption based on improved phase retrieval algorithm*, Applied Optics **51**(13), 2012: 2388-2394. https://doi.org/10.1364/AO.51.002388

[37] ZHAO S., WANG L., LIANG W., CHENG W., GONG L., *High performance optical encryption based on computational ghost imaging with QR code and compressive sensing technique*, Optics Communications **353**, 2015: 90-95. https://doi.org/10.1016/j.optcom.2015.04.063

[38] ANNABY M.H., RUSHDI M.A., NEHARY E.A., *Color image encryption using random transforms, phase retrieval, chaotic maps, and diffusion*, Optics and Lasers in Engineering **103**, 2018: 9-23. https://doi.org/10.1016/j.optlaseng.2017.11.005

[39] MEHRA I., NISHCHAL N.K., *Wavelet-based image fusion for securing multiple images through asymmetric keys*, Optics Communications **335**, 2015: 153-160. https://doi.org/10.1016/j.optcom.2014.09.040

[40] MEHRA I., NISHCHAL N.K., *Image fusion using wavelet transform and its application to asymmetric cryptosystem and hiding*, Optics Express **22**(5), 2014: 5474-5482. https://doi.org/10.1364/OE.22.005474

[41] CAI J., SHEN X., LEI M., LIN C., DOU S., *Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition*, Optics Letters **40**(4), 2015: 475-478. https://doi.org/10.1364/OL.40.000475

[42] CAI J., SHEN X., *Modified optical asymmetric image cryptosystem based on coherent superposition and equal modulus decomposition*, Optics & Laser Technology **95**, 2017: 105-112. https://doi.org/10.1016/j.optlastec.2017.04.018

[43] DENG X., *Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition: Comment*, Optics Letters **40**(16), 2015: 3913. https://doi.org/10.1364/OL.40.003913

[44] KEKRE H.B., SARODE T.K., VIG R., *A new multi-resolution hybrid wavelet for analysis and image compression*, International Journal of Electronics **102**(12), 2015: 2108-2126. https://doi.org/10.1080/00207217.2015.1020882

[45] YE G., *Image scrambling encryption algorithm of pixel bit based on chaos map*, Pattern Recognition Letters **31**(5), 2010: 347-354. https://doi.org/10.1016/j.patrec.2009.11.008

[46] ZOU J., WARD R.K., QI D., *A new digital image scrambling method based on Fibonacci numbers*, [In] *2004 IEEE International Symposium on Circuits and Systems (ISCAS)*, Vancouver, BC, Canada, 2004: III-965. https://doi.org/10.1109/ISCAS.2004.1328909

[47] XU L., GOU X., LI Z., LI J., *A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion*, Optics and Lasers in Engineering **91**, 2017: 41-52. https://doi.org/10.1016/j.optlaseng.2016.10.012

[48] YU X.Y., ZHANG J., REN H.E., XU G.S., LUO X.Y., *Chaotic image scrambling algorithm based on S-DES*, Journal of Physics: Conference Series **48**, 2006: 349-353. https://doi.org/10.1088/1742-6596/48/1/065

[49] KUMAR J., SINGH P., YADAV A.K., KUMAR A., *Asymmetric image encryption using gyrator transform with singular value decomposition*, [In] RAY K., SHARAN S., RAWAT S., JAIN S., SRIVASTAVA S.,

BANDYOPADHYAY A. [Eds.], *Engineering Vibration, Communication and Information Processing*, Lecture Notes in Electrical Engineering, Vol. 478, Springer, Singapore, 2019: 375-383. https://doi.org/10.1007/978-981-13-1642-5_34

[50] RAKHEJA P., VIG R., SINGH P., *A hybrid multiresolution wavelet transform based encryption scheme*, AIP Conference Proceedings **2061**(1), 2019: 020008. https://doi.org/10.1063/1.5086630

[51] RAKHEJA P., VIG R., SINGH P., KUMAR R., *An iris biometric protection scheme using 4D hyperchaotic system and modified equal modulus decomposition in hybrid multi resolution wavelet domain*, Optical and Quantum Electronics **51**, 2019: 204. https://doi.org/10.1007/s11082-019-1921-x

[52] RAKHEJA P., SINGH P., VIG R., KUMAR R., *Double image encryption scheme for iris template protection using 3D Lorenz system and modified equal modulus decomposition in hybrid transform domain*, Journal of Modern Optics **67**(7), 2020: 592-605. https://doi.org/10.1080/09500340.2020.1760384

[53] RAKHEJA P., VIG R., SINGH P., *An asymmetric hybrid cryptosystem using equal modulus and random decomposition in hybrid transform domain*, Optical and Quantum Electronics **51**, 2019: 54. https://doi.org/10.1007/s11082-019-1769-0

[54] 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. https://doi.org/10.1016/j.ijleo.2018.09.088

[55] RAKHEJA P., VIG R., SINGH P., *Asymmetric hybrid encryption scheme based on modified equal modulus decomposition in hybrid multi-resolution wavelet domain*, Journal of Modern Optics **66**(7), 2019: 799-811. https://doi.org/10.1080/09500340.2019.1574037

[56] KUMAR J., SINGH P., YADAV A.K., *Asymmetric cryptosystem using double random-decomposition in fractional Fourier transform domain*. Proceedings of the SPIE, Vol. 10751, Optics and Photonics for Information Processing XII, 2018: 107510V. https://doi.org/10.1117/12.2321973

[57] YADAV A.K., SINGH P., SAINI I., SINGH K., *Asymmetric encryption algorithm for colour images based on fractional Hartley transform*, Journal of Modern Optics **66**(6), 2019: 629-642. https://doi.org/10.1080/09500340.2018.1559951

[58] RAKHEJA P., VIG R., SINGH P., *Double image encryption using 3D Lorenz chaotic system, 2D non-separable linear canonical transform and QR decomposition*, Optical and Quantum Electronics **52**, 2020: 103. https://doi.org/10.1007/s11082-020-2219-8

[59] LIU X., WU J., HE W., LIAO M., ZHANG C., PENG X., *Vulnerability to ciphertext-only attack of optical encryption scheme based on double random phase encoding*, Optics Express **23**(15), 2015: 18955-18968. https://doi.org/10.1364/OE.23.018955

[60] ABDELFATTAH M., HEGAZY S.F., AREED N.F.F., OBAYYA S.S.A., *Compact optical asymmetric cryptosystem based on unequal modulus decomposition of multiple color images*, Optics and Lasers in Engineering **129**, 2020: 106063. https://doi.org/10.1016/j.optlaseng.2020.106063

[61] KUMAR V., *RSFVC: Robust biometric-based secure framework for vehicular cloud networking*, IEEE Transactions on Intelligent Transportation Systems **25**(5), 2024: 3364-3374. https://doi.org/10.1109/TITS.2023.3322960

[62] KUMAR V., SEEMA, KUMAR K., PRASAD R., ALMUTIB K., HOSSAIN M.S., *SEPCVN: Secure and efficient protocol for cloud vehicular networking*, IEEE Access 12, 2024: 108657-108672. https://doi.org/10.1109/ACCESS.2024.3423717

[63] ITOO S., KUMAR V., AHMAD M., *A secure and energy-efficient authentication framework for the internet of electric things*, Cluster Computing **28**, 2025: 382. https://doi.org/10.1007/s10586-025-05293-1

[64] GUPTA S., NITISH, HARISH M., SHARMA A.K., *A hybrid authenticated image encryption scheme using elliptic curves for enhanced security*, International Journal of Information Technology, 2024. https://doi.org/10.1007/s41870-024-01737-w

[65] KUMAR S., SHARMA D., *A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm*, Artificial Intelligence Review **57**, 2024: 87. https://doi.org/10.1007/s10462-024-10719-0

[66] AZAM N.A., MURTAZA G., HAYAT U., *A novel image encryption scheme based on elliptic curves and coupled map lattices*, Optik **274**, 2023: 170517. https://doi.org/10.1016/j.ijleo.2023.170517

[67] MAN Z., LIU J., ZHANG F., MENG X., *Research on cloud dynamic public key information security based on elliptic curve and primitive Pythagoras*, Alexandria Engineering Journal **113**, 2025: 169-180. https://doi.org/10.1016/j.aej.2024.11.012

Received June 25, 2025
in revised form August 3, 2025