Hazzazi, Mohammad Mazyad, Rehman, Mujeeb Ur ORCID logoORCID: https://orcid.org/0000-0002-4228-385X, Shafique, Arslan, Aljaedi, Amer, Bassfar, Zaid and Usman, Aminu ORCID logoORCID: https://orcid.org/0000-0002-4973-3585 (2024) Enhancing image security via chaotic maps, Fibonacci, Tribonacci transformations, and DWT diffusion: a robust data encryption approach. Scientific Reports, 14 (1).

RaY

Research at the University of York St John

For more information please contact RaY at ray@yorksj.ac.uk

scientific reports

OPEN

Enhancing image security via chaotic maps, Fibonacci, Tribonacci transformations, and DWT diffusion: a robust data encryption approach

Mohammad Mazyad Hazzazi[1], Mujeeb Ur Rehman[2✉], Arslan Shafique[3], Amer Aljaedi[4], Zaid Bassfar[5] & Aminu Bello Usman[6]

In recent years, numerous image encryption schemes have been developed that demonstrate different levels of effectiveness in terms of robust security and real-time applications. While a few of them outperform in terms of robust security, others perform well for real-time applications where less processing time is required. Balancing these two aspects poses a challenge, aiming to achieve efficient encryption without compromising security. To address this challenge, the proposed research presents a robust data security approach for encrypting grayscale images, comprising five key phases. The first and second phases of the proposed encryption framework are dedicated to the generation of secret keys and the confusion stage, respectively. While the level-1, level-2, and level-2 diffusions are performed in phases 3, 4, and 5, respectively, The proposed approach begins with secret key generation using chaotic maps for the initial pixel scrambling in the plaintext image, followed by employing the Fibonacci Transformation (FT) for an additional layer of pixel shuffling. To enhance security, Tribonacci Transformation (TT) creates level-1 diffusion in the permuted image. Level-2 diffusion is introduced to further strengthen the diffusion within the plaintext image, which is achieved by decomposing the diffused image into eight-bit planes and implementing XOR operations with corresponding bit planes that are extracted from the key image. After that, the discrete wavelet transform (DWT) is employed to develop secondary keys. The DWT frequency sub-band (high-frequency sub-band) is substituted using the substitution box process. This creates further diffusion (level 3 diffusion) to make it difficult for an attacker to recover the plaintext image from an encrypted image. Several statistical tests, including mean square error analysis, histogram variance analysis, entropy assessment, peak signal-to-noise ratio evaluation, correlation analysis, key space evaluation, and key sensitivity analysis, demonstrate the effectiveness of the proposed work. The proposed encryption framework achieves significant statistical values, with entropy, correlation, energy, and histogram variance values standing at 7.999, 0.0001, 0.0156, and 6458, respectively. These results contribute to its robustness against cyberattacks. Moreover, the processing time of the proposed encryption framework is less than one second, which makes it more suitable for real-world applications. A detailed comparative analysis with the existing methods based on chaos, DWT, Tribonacci transformation (TT), and Fibonacci transformation (FT) reveals that the proposed encryption scheme outperforms the existing ones.

[1]Department of Mathematics, College of Science, King Khalid University, 61413 Abha, Saudi Arabia. [2]Cyber Technology Institute, School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, UK. [3]School of Electronic and Nanoscale Engineering, University of Glasgow, Glasgow G12 8QQ, UK. [4]College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia. [5]College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia. [6]School of Computer Science, University of Sunderland, Sunderland SR1 3SD, UK. ✉email: mujeeb.rehman@dmu.ac.uk

With the exponential and, frequency use of wireless technology and digital devices, the exchange of digital data such as images has increased the demand for robust security[1,2]. As images play a vital role in communication, ensuring image security has become an important concern. Numerous approaches, such as secret image sharing[3], image steganography[4], and image encryption[5,6], proposed in the past several years to enhance the security of image transmission through wireless channels such as the Internet. Digital images are characterized by their significant data content, which exhibits high pixel correlation and redundancy. Consequently, traditional cryptographic schemes like DES and AES are not suitable for image encryption due to their high computational complexity. To address this challenge, several categories of encryption schemes have been proposed to effectively protect the image data[7–11].

The image encryption algorithm is used to convert an image into an unreadable message known as a cipher image through the utilization of secret keys[12]. This resulting cipher image bears a resemblance to a noisy image, rendering it virtually difficult for attackers to recover the plaintext image from the cipher image. This transformation is primarily achieved either by scrambling the pixels or by changing the intensity of the original pixel values. Specifically, the pixel scrambling technique plays a crucial role in breaking the correlation of the adjacent pixels. This phase, appropriately termed the confusion phase of image encryption, results in a cipher image with an entirely different appearance. In particular, this pixel scrambling process preserves the histogram of the original image since it does not alter the pixel intensity[13]. Subsequently, the diffusion phase emerges as an integral step in the image encryption process, aimed at modifying the intensity values of the pixels. This modification leads to the establishment of a uniform histogram in the cipher image, thereby enhancing the system's resilience against a spectrum of potential attacks[14]. The detailed analysis of the gray-scale images including medical images can be found in[15].

Image encryption plays a pivotal role in various essential functions within the corporate world[16]. In the realm of healthcare, the digitization of health records, which encompasses patient data, medical history, and symptoms, requires robust protection due to their sensitive nature[17]. Securing these records from unauthorized access is paramount. Likewise, in the military sector, images such as maps, building locations, and intelligence on adversaries are of the utmost importance. They play vital roles in tasks like small target identification, tracking, and missile guidance. Consequently, ensuring the security of these images is critical to national defense, as unauthorized access could pose significant threats. The media industry, characterized by round-the-clock news broadcasting, hinges on the privacy of multimedia content, be it images, audio, or video. Image encryption plays a crucial role in safeguarding this information from unwarranted intrusion. Additionally, as cloud storage becomes increasingly prevalent, third-party entities store client data in the cloud, including images. Protecting the privacy of these cloud-stored images is imperative to maintaining data security and confidentiality, making image encryption an essential component of cloud applications[18].

The proposed research introduces a novel image encryption method that employs the Fibonacci transform (FT) to scramble pixels, achieved through matrix multiplication of two matrices (2×2 and 2×1). The diffusion is created using the XOR operation in the scrambled image with a randomly generated i-key image. A key innovation lies in the utilization of the Tribonacci-based transformation (TBT) to modify pixel values, which is achieved by multiplying a 3×3 Tribonacci array with a 3×1 vector representing three consecutive pixels. Further in the diffusion process, traditional operations such as substitution box (S-box) and circular bit-shift are applied. Moreover, the proposed method demonstrates the ability to handle different categories of images, such as binary images and images with different levels of grayscale. It is lauded for its simplicity, ease of implementation, and fast execution. Experimental results show the resilience of the proposed method. The generic flow of the proposed work is displayed in Fig. 1.

The proposed research holds significant potential for various practical applications where image security is paramount. For instance, for sensitive data storage, secure communication channels, and confidential image sharing, the integration of chaotic maps, Fibonacci, Tribonacci transformations, and Discrete Wavelet Transform (DWT) diffusion provides a robust data encryption framework. The innovative fusion of these cryptographic techniques aims to provide robust security measures to ensure the protection of critical visual information. This research's findings could find application in sectors ranging from medical imaging and military communications
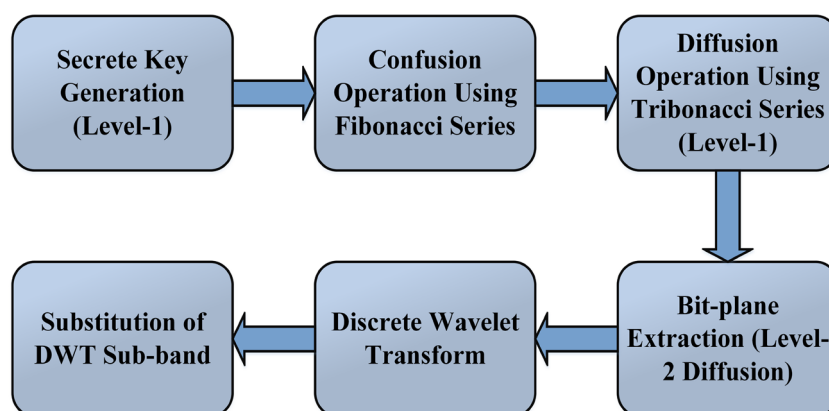

Figure 1. Generic flow of the proposed work.

to secure digital information, which contributes to the securing of sensitive visual data in an increasingly inter-connected and data-driven world.

Motivation

In today's digital age, the exchange and transmission of sensitive information, particularly through visual media like images, demands robust security measures. In the year 2020, Equifax, a leading credit reporting company, suffered a substantial data breach, leading to the compromise of private personal information, including images and credit card details, for 143 million individuals[19]. According to a study presented in[20], around 52% of digital information in several countries such as Bangladesh, Nepal, Sweden, and Denmark is categorized as facing high cyber risk, while 32% is deemed to have a moderate risk, and a mere 12% is considered to be at low risk. The study shows the considerable cyber threat landscape confronting sensitive information, with an average of 630 cyberat-tacks directed at digital data such as images and bank credit cards. Therefore, with the increasing prevalence of cyber threats and unauthorized access, the need for effective cryptographic protocols has become paramount. As per cybersecurity reports, sensitive images often become targets for malicious activities due to their vulnerability during transmission. Image encryption, when implemented effectively, secures against unauthorized access and ensures the confidentiality and integrity of the visual data.

Considering these challenges and the evolving landscape of cyber threats, the proposed research aims to address the need for a robust ecryptographic protocol that provides a strong defense against cyberattacks while maintaining a low processing time. The proposed encryption framework combines chaotic maps, Fibonacci and Tribonacci transformations, and DWT diffusion to achieve an efficient solution for enhancing image security. By integrating these elements, the proposed approach aims to surpass existing methods in terms of security and real-time applicability, which contributes to the ongoing efforts to enhance digital data protection.

Organization of the paper

The rest of the sections of this paper are structured as follows: "Related work" section provides an overview of existing encryption schemes, accompanied by a summary table outlining vulnerabilities and potential solutions. "Preliminaries" section gives the foundational knowledge essential for developing the proposed encryption scheme, detailed in "Proposed encryption procedure" section. The experimental outcomes of the proposed encryption framework are explained in "Experimental results and analysis" section. "Uniqueness and the advantages of the proposed encryption framework" section is devoted to outlining the advantages and uniqueness of the proposed work. It reveals the advantages and shows the uniqueness of the proposed encryption framework in comparison to existing studies. Finally, "Conclusion and future work" section concludes the proposed research and provides a few future recommendations aimed at enhancing the proposed encryption framework.

Related work

In the early stages of image encryption development, the focus was primarily on applying these methods to compressed data. Among the various categories of image encryption techniques, chaotic-based approaches have garnered substantial attention[21]. Their popularity stems from their sensitivity to initial parameters, the capac-ity to generate pseudorandom sequences, and the unpredictability of motion patterns. These chaotic methods involve the computation of pseudo-random sequences, which are then used to define specific permutations for tasks like pixel scrambling, bit plane permutation, and substitution matrix creation[22–24].

The chaotic behavior aligns well with the encryption requirements, improving security. Early researchers pre-dominantly used classical chaotic maps such as Baker's map[25], logistic map[26], and tent map[27]. Recently, innovative hybrid chaotic image encryption methods have emerged, combining chaotic maps with optimized substitution boxes[28–31]. Some of the recent advancements involve the adoption of high-dimensional chaotic systems[32–34]. These systems have gained popularity due to their ability to expand the key space and improve resilience against attacks. For instance, a 5D hyperchaotic system[35] has been proposed to encrypt color images, involving the decomposition of plain images into sub-bands through complex wavelet transformations. Subsequently, secret keys derived from a 5D chaotic map are used to diffuse these sub-bands. Furthermore, novel visual encryption schemes featuring 6D hyperchaotic systems[36] and image cryptosystems utilizing hyperchaotic systems in con-junction with Fibonacci Q-matrices have been introduced in recent research.

Cahos based image encryption schemes

Encryption schemes for images based on chaos utilize the inherent unpredictability and sensitivity to initial conditions present in chaotic systems to safeguard digital images. For instance, in[37], Nematzadeh et al proposed a new hybrid method based on the integration of DNA encoding and a Binary Search Tree (BST) algorithm. In[38], Yadollahi et al. proposed a two-phase secure image encryption scheme using DNA and RNA. It generates the initial cipher image using DNA rules, and a chaotic function, while the final encrypted image is obtained through the use of XOR operation. In[39], Abbasi et al. proposed a new Chaotic Evolutionary Biomolecules Model (CEBM) for image encryption, which incorporates the concepts of DNA and RNA-based encryption methods[40]. This model employs multiple chaotic maps for scrambling purposes, while DNA, RNA, and XOR operations are used to create the diffusion in the plaintext image[41–43]. In[28], Benaissi et al. proposed a novel image encryption algorithm that overcomes the limitations associated with one-dimensional (1D) maps and multidimensional (MD) maps. They adopted a hybrid approach, combining three modified and enhanced 1D chaotic maps, providing enhanced security. The encryption process utilizes a key image to initialize the chaotic maps. Moreover, the incorporation of ExtraParam extracted from the plaintext image adds sensitivity to bit changes during chaotic map initialization. This method comprises two core phases: confusion and diffusion, and it has proven its efficacy through rigorous testing and cryptanalysis. In[44], Liu et al., introduced a cluster of one-dimensional quadratic chaotic maps based on

topological conjugate theory. These 1D chaotic maps feature three tunable parameters, significantly expanding the parameter space compared to traditional 1D maps. The theoretical analysis validates their chaotic nature, as they are topologically conjugated with logistic chaotic maps. The paper presents an example of a 1D quadratic chaotic map and showcases several numerical simulations that confirm the ideal chaotic characteristics, aligning with the theoretical analysis. In[45], Shraida et al. introduced a proficient technique for encrypting color images, which integrates DNA encoding and utilizes two variations of hyper-chaotic maps. The process consists of three steps: initializing conditions for generating Lorenz chaotic maps through a Secure Hash Algorithm (SHA) applied to a plain image, performing a confusion procedure using Lorenz hyper-chaotic sequences to scramble the image's color components, and combining three approaches for diffusion: DNA encoding/decoding, addition operations between components, and XOR operations with Rossler hyper-chaotic sequences. This method ensures robust encryption for color images. In[46], Zhang et al. introduced an image encryption scheme grounded in the Sarrus rule and the theory of linear algebra. They established the Sarrus model to scramble plain images by reordering pixel positions, producing a stereo-scrambled matrix. Additionally, the two-dimensional matrix is converted into a three-dimensional (3D) space.

Fibonacci, DWT and DNA based image encryption schemes

Fibonacci-based image encryption schemes use the distinctive properties of the Fibonacci sequence to enhance security. However, DWT integrates multi-resolution analysis for encryption on different frequency components. While DNA-based encryption schemes add a biological element, transforming images into DNA-like structures and employing biological principles like encoding and decoding for enhanced cryptographic complexity. For instance, in[47], Biban et al. proposed an image encryption scheme that incorporates an 8D hyperchaotic system that integrates a Fibonacci Q-Matrix (FQ-matrix). This approach enhances the security against various cyberattacks, making it suitable for real-time applications. In[48], Zhong et al. designed a new methodology for the development of random numbers based on chaos theory. Moreover, wavelet transformations and XOR operations are also used with a chaotic matrix to enhance security. In[49], Begum et al., proposed a hybrid blind digital image watermarking technique that integrates, Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD). The encryption process starts with the use of the Arnold map to encrypt the watermark image. The remaining steps involve DCT, DWT, and SVD transformations applied to both the watermark and host image. In[50], Balasamy et al. introduced a new image watermarking method that employs fuzzy-based Region of Interest (ROI) selection and wavelet transformation to secure embed encrypted watermarks securely. The process involves fuzzification of the source image for critical ROI selection, followed by a Discrete Wavelet Transform (DWT) to rearrange sub-bands using logistic mapping-derived magnitude values. This pixel swapping ensures a fully encrypted image, enhancing security and resistance to decryption. However, the challenges may arise from relying on singular values for watermark robustness and using logistic mapping for sub-band swapping, posing susceptibility to specific attacks. More detailed explanation of ROI based techniques to secure digital images can be found in[51–53]. In[54], Chai et al. proposed a DNA-based method, involving the conversion of a plaintext image into a DNA matrix. This method employs a Chaotic Logistic Map (CLM)[55] for the scrambling of the pixel rows and columns. After that, the sequence generated using CLM is used to create the diffusion in the image pixels. The seed parameters for this method are obtained through the application of a hashing algorithm called SHA256 on the original image. In[56], Chen et al. incorporated a DNA coding and chaotic Henon-map to secure the digital images. Here, an S-box is initially applied to create cryptographic effects for complex DNA operations[57]. In[58], Ganavi et al., utilized Error-Correcting Codes (ECC) with modifications to encrypt and decrypt input plaintext images. This method transforms carrier digital images into frequency bands using the Discrete Wavelet Transform (DWT) and conceals the encrypted hash of the input within high-frequency bands using the Least-Significant-Bit (LSB) technique. The approach successfully achieves data confidentiality and verifies data integrity through SHA-256. Table 1 provides an overview of the related work, encompassing both the identified limitations and the corresponding potential solutions.

Contributions of the paper

As indicated in Table 1, most current schemes exhibit weak security vulnerabilities, high computational complexity, or infeasibility for real-world implementations. Taking into account these vulnerabilities, the novelty and contributions of the proposed research are as follows:

- The application of a Fibonacci Transform (FT) for pixel scrambling is characterized by the non-linear and complex properties of the FT. These features enable the FT to intricately scramble the pixels of an image, which enhances the level of security and the encryption process.
- Implementing the TBT involves adjusting the values of the pixels by multiplying a Tribonacci array 3×3 with a vector 3×1 representing three consecutive pixels. This optimization reduces overall computational time without compromising the strength of the security measures which makes the proposed encryption scheme suitable for real-world applications.
- The proposed encryption scheme has a high-key space, which is achieved using multiple chaotic maps. The high-key space enhances the security of the digital data against brute-force attacks.
- DWT is employed to generate secondary keys that enhance the security of the propsoed encryption framework by diversifying the encryption keys.
- The nature of certain operations, such as XOR operations and DWT, allows for parallel processing that helps reduce the overall computational time.
- The proposed method employs level-2 diffusion by decomposing the diffused image into eight-bit planes and performing XOR operations with the corresponding bit planes which are extracted from the key image. This

Methodology	Year	Application domain	Real-world performance	Robustness against attacks	Disadvantages	Potential solutions
Chai et al.[54]	2017	DNA-based encryption	Not specified	Not specified	Lack of real-world information	Investigate practical performance
Chen et al.[56]	2020	DNA and chaotic encryption	Not specified	Not specified	Security and performance validation required	conduct real-world testing
Nematzadeh et al.[37]	2020	DNA encoding and BST	Not specified	Not specified	Further practical testing nedded	Validate and optimize for real-world use
Yadollahi et al.[38]	2020	DNA and RNA	Not specified	Not specified	Lack of real-world performance data	Investigate practical performance
Abbasi et al.[39]	2021	Chaotic evolutionary model	Not specified	Not specified	Requires performance evaluation	Conduct real- world testing
Balasamy et al.[50]	2021	Image watermarking	Secure	Resistant to decryption	Relying on SV, LM for sub-band swaping	Further Research on robust algorithms
Zhong et al.[48]	2022	Random number generation	Enhanced security	Improved security	Real-world implementation challenges	Address practical implementation issues
Begum et al.[49]	2022	Image watermarking	Security watermark	Hybrid approach	Potential for complexity in the process	Streamline the watermarking process
Benaissi et al.[28]	2023	Image encryption	Efficacious	Resilient to attack	Limited to 1D chaotic maps	Explore improved encryption
Liu et al.[44]	2023	Chaotic maps	Theoretical validation	Topological conjunction	Requires further validation	Conduct real-world testing
Shraida et al.[45]	2023	Color image encryption	Robust	Resistant to cyberattacks	Complexity in diffusion method	Optimize diffusion technique
Zhang et al.[46]	2023	Image encryption	Scrambling images	Matrix-based encryption	Limited explanation of practical use	Investigate practical applications
Biban et al.[47]	2023	Image encryption	Enhanced security	Robust against attacks	Potential for Computational overhead	Optimize for performance in real-time apps
Ganavi et al.[58]	2023	Image encryption	Data confidentiality	Data integrity	Practical verification required	Conduct practical integrity test

Table 1. Summary of the related work.

step strengthens the diffusion within the plaintext image which makes it more resistant against cryptographic attacks.

Preliminaries
In the subsequent two subsections, we delve into the mathematical aspects of the Fibonacci Transform and the Tribonacci Transform.

Fibonacci transform
The Fibonacci series is a sequence of numbers ($f_l = f_1, f_2, \cdots, f_n$) in which each number is the sum of the two previous numbers. It mainly starts with $f_1 = 0$ and $f_2 = 1$, and the next numbers are generated by adding the previous two numbers in the sequence as shown in Eq. (1).

$$f_l = \left[f_1 = 0, f_2 = 1, f_3 = [f_2 + f_1] = 1, f_4 = [f_3 + f_2] = 2, \right.$$
$$\left. f_5 = [f_4 + f_3] = 3, \cdots, f_n = [f_{n-1} + f_{n-2}] \right] \tag{1}$$

The generalized form of Eq. (1) is given in Eq. (2).

$$f_l = \begin{cases} 0, & \text{if } l = 1 \\ 1, & \text{if } l = 2 \\ 1, & \text{if } l = 3 \\ f_{l-1} + f_{l-2}, & \text{Otherwise} \end{cases} \quad \text{Where i} = 1, 2, 3 \cdots \tag{2}$$

The fibonacci and tribonacci numbers are given in Table 2 when $l \in [-7 + 7]$.

The Fibonacci sequence, renowned for its remarkable properties, has been a subject of fascination for researchers. The researcher has employed matrix operations, such as determinants to derive class identities for generalized Fibonacci numbers [71]. The proposed research focuses on three key properties of generalized

i	−7	−6	−5	−4	−3	−2	−1	0	+1	+2	+3	+4	+5	+6	+7
f_i	13	−8	5	−3	2	-1	1	0	1	1	2	3	5	8	13
t_i	1	0	1	1	2	4	7	13	24	44	81	149	274	504	927

Table 2. Fibonacci and tribonacci sequences when $l = −1, \cdots l = +7$.

Fibonacci sequences, including, d'Ocagne's identity (DOi), Catalan's identity (CTi), and Cassini's identity (CAi), and the mathematical formulation of such identities are given in Eqs. (3), (4), and (5), respectively.

$$\text{DOi: } f_{i+1} \times f_i - f_i - \times f_{j+1} = (-1)^i f_{i-j} \tag{3}$$

$$\text{CTi: } f_i \times f_i - f_{i+j} \times f_{i-j} = (-1)^{i-j} f_i \times f_i \tag{4}$$

$$\text{CAi: } f_{i+1} \times f_{i-1} - f_i \times f_i = (-1)^i \tag{5}$$

The identities mentioned above can be represented in terms of determinants as follows:

$$DOi = \begin{vmatrix} f_{i+1} & f_{j+1} \\ f_i & f_j \end{vmatrix}, \quad CTi = \begin{vmatrix} f_i & f_{i+j} \\ f_{i-j} & f_i \end{vmatrix}, \quad CAi = \begin{vmatrix} f_{i+1} & f_i \\ f_i & f_{i-1} \end{vmatrix} \tag{6}$$

The matrix associated with any of the mentioned identities can be employed to manipulate data in cryptography modulo n, but only if the greatest common divisor (gcd) of the determinant (det) and n is congruent to 1 modulo n.

- If gcd(det, n) $\equiv$ 1 mod n, the matrix can be used for data transformation in cryptography.

Considering the Fibonacci series definition, where $f_1 = 1$ and $f_2 = 1$, we can make the following observations regarding the transformation matrices:

- Regardless of the value of i, CAi can take on either +1 or -1.
- When the difference between i and j equals 1 or 2, DOi may assume either +1 or -1.
- If j belongs to the set 1, 2, CTi can be either +1 or -1.

According to Eqs. (3), (4), and (5), it becomes evident that Cassini's identity can be considered a particular instance of the other two identities, as follows:

- DOi transforms into Cassini's identity when $p + 1 = q$.
- CTi becomes Cassini's identity when p equals 1.

Tribonacci transform

Tribonacci transform is the extension of the fibonacci sequence and it is defined in Eq. (7).

$$t_{l+1} = t_l + t_{l-1} + t_{l-2}, \tag{7}$$

where $t_0 = t_1 = 0, t_2 = 1$

The negative t_l, denoted as t_{-l} adheres to the recurrence relation given in Eq. (8).

$$t_{-l} = \begin{vmatrix} t_{l+1} & t_{l+2} \\ t_l & t_l + 1 \end{vmatrix} \tag{8}$$

Equations (7) and (8) yield the Tribonacci numbers, spanning values for k such as $\cdots, -7, -6, \cdots, +6, +7, \cdots$, as displayed in Table 2.

The encoding method utilizing the Tribonacci numbers relies on the Tribonacci numbers and involves the introduction of a matrix having three rows and three columns denoted as M. The matrix M is defined as follows:

$$M = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} t_3 & t_2 + t_1 & t_2 \\ t_2 & t_1 + t_0 & t_1 \\ t_1 & t_0 + t_{-1} & t_0 \end{bmatrix} \tag{9}$$

With the determinant of M equal to 1, and the inverse of H detailed in Eq. (10).

$$
\begin{aligned}
M^{-1} &= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & -1 \end{bmatrix} \\
&= \begin{bmatrix} t_0^2 - t_{-1}t_1 & t_1t_2 - t_0t_1 & t_1^2 - t_0t_2 \\ t_1^2 - t_0t_2 & t_0t_3 - t_1 - t_2 & t_2^2 - t_1t_3 \\ t_0t_2 + t_{-1}t_2 - t_1^2 - t_0t_1 & t_1^2 + t_1t_2 - t_0t_3 - t_{-1}t_3 & t_1t_3 + t_0t_3 - t_2^2 - t_1t_2 \end{bmatrix}
\end{aligned} \tag{10}
$$

The calculation of the positive powers of M, specifically M^l, for l in the set of natural numbers, is carried out as follows:

$$M^l = \begin{bmatrix} l_{l+2} & t_{l+1} + t_l & t_{l+1} \\ t_{l+1} & t_l + t_{l-1} & t_l \\ t_l & t_{l-1} + t_{l-2} & t_{l-1} \end{bmatrix} \tag{11}$$

The computation of the negative powers of M, denoted as M^l for l belonging to the set of natural numbers, is detailed in Eq. (12).

$$M^{-1} = \begin{bmatrix} t_{l-1}^2 - t_{l-2}t_l & t_{l-2}t_{l+1} - t_{l-1}t_l & t_l^2 - t_{l-1}t_{l+1} \\ t_l^2 - t_{l-1}t_{l+1} & t_{l-1}t_{l+2} - t_l t_{l+1} & t_{l+1}^2 - t_l t_{l+1} \\ (t_{l-1} + t_{l-2})t_{l+1} & t_l(t_l + t_{l+1}) & (t_l t_{l-1})t_{l+2} \\ (t_l + t_{l-1})t_l & (t_{l-1} + t_{l-2})t_{l+2} & (t_{l+1} + t_l)t_{l+1} \end{bmatrix} \quad (12)$$

Equations (11) and (12) can be readily derived through the application of mathematical induction. Utilizing the previously defined M^z for z within the set of integers, the following properties can be readily demonstrated:

Z1 : $M^p = M^{p-1} + M^{p-2} + M^{p-3}$

Z2 : $M^p M^q = M^q M^p = H^{p+q}(p, q \in (-\infty + \infty))$

Z3 : $det M^p = 1$

Hence, based on the preceding discourse, it's evident that a Tribonacci matrix M^i, regardless of the specific index i, possesses the capability to convert data into an alternate domain. Moreover, it's important to highlight that the original data can be restored, due to the invertibility of M^i. Consequently, M^i can be effectively integrated into encryption schemes.

Six-dimensional hyperchaotic map

In[59], Grassi et al. introduced a novel four-wing hyperchaotic attractor created through the coupling of two identical Lorenz systems, as described in Eq. (13).

$$\begin{cases} \dot{y}_1 = b(y_2 - y_1) \\ \dot{y}_2 = cy_1 - y_2 - y_1 y_3 + \eta_1(y_4 - y_5) \\ \dot{y}_3 = y_1 y_2 - dy_3 \\ \dot{y}_4 = b(y_5 - y_4) \\ \dot{y}_5 = cy_4 - y_5 - y_4 y_6 + \eta_2(y_1 - y_2) \\ \dot{y}_6 = y_4 y_5 - dy_6 \end{cases} \quad (13)$$

where the variables b, c, and d represent positive system parameters, while η_1 and η_2 are the coupling parameters. When specific values are assigned to these parameters, such as b = 10, c = 28, d = 8/3, and $\eta_1 = \eta_2 = 0.05$, the system given Eq. (13) produces the distinctive four-wing attractors depicted in Fig. 2. In the context of the subsequent cryptosystem, the parameters b, c, η_1 and η_2, and the initial conditions $y_\rho(0)$ (where $\rho \in [1, 6]$) are treated as secret keys. These secret keys, in combination with the plaintext image, are utilized to generate the key streams essential for confusion in the proposed encryption technique.

Proposed encryption procedure

The suggested encryption procedure comprises five primary phases:

1. The creation of initial secret keys at level-1 via the utilization of a chaotic map.
2. Implementing a confusion operation employing the Fibonacci series.
3. Employing a level-1 diffusion operation with the assistance of the Tribonacci series.
4. Level-2 diffusion operation using bit-plane extraction method.
5. Incorporating of Discrete Wavelet Transform (DWT) in the proposed encryption process.
6. Implementing S-box within DWT sub-bands for level-3 diffusion.

The illustration of the proposed encryption approach is given in Fig. 3. Further elaboration on the encryption process is provided in the subsequent sections.
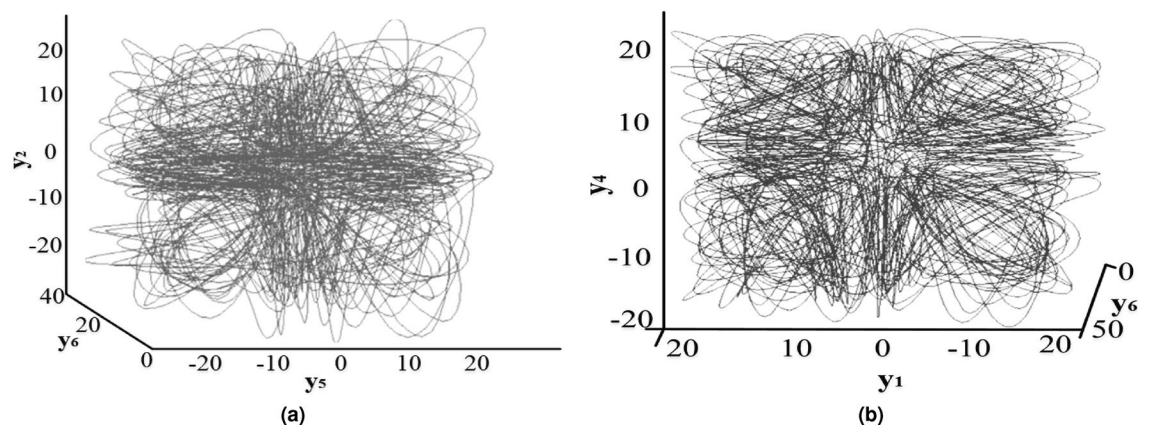

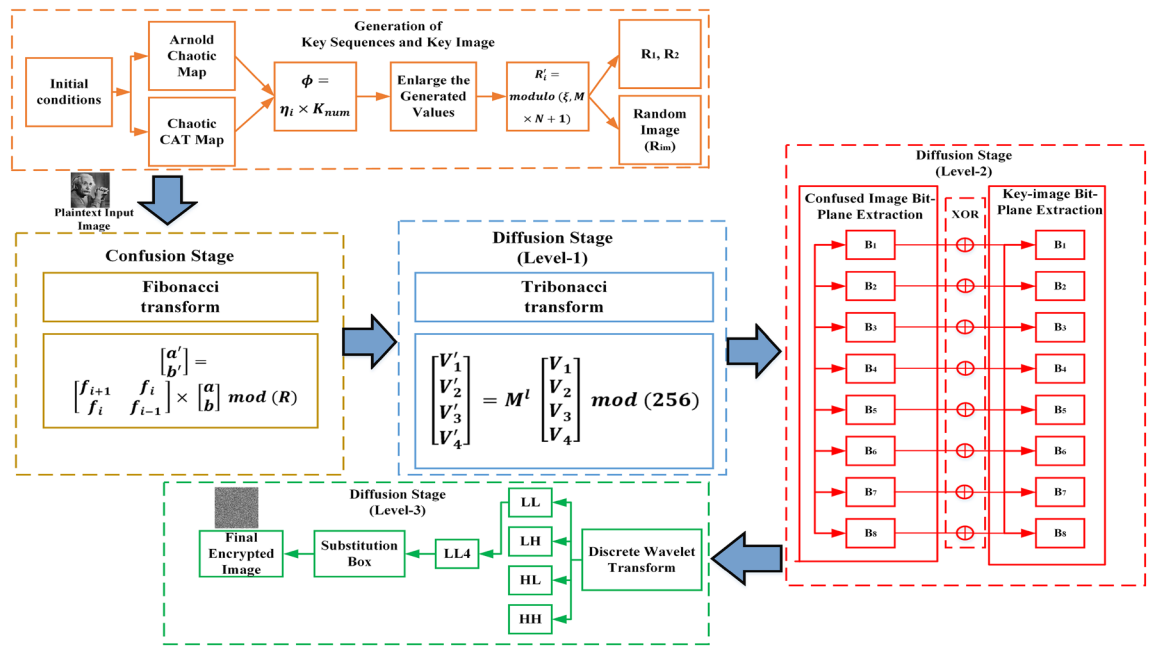**Figure 2.** The hyperchaotic attractors of the system 13.

Figure 3. Flow of the proposed encryption scheme.

Random sequences and key image generation process

In the generation of the secret of level-1, multiple henon chaotic map is used. This level-1 secret key is a two-dimensional random image having no meaningful information present in it and it will be used for incorporating the exclusive OR operation to modify the intensities of the original image. Algorithm 1 provides the step-by-step details of the key generation procedure. Additionally, a 256-bit key size is employed for both encryption and decryption operations. Various initial conditions have been utilized as secret keys to produce random sequences and a key image.

Start Input: Control parameters and initial conditions: (Set-1: $\{b_1, c_1, d_1, \eta_1 \text{ and } \eta_2\}$, and Set-2: $\{b_1', c_1', d_1', \eta_1' \text{ and } \eta_2'\}$).

$\rightarrow$ **Step 1:** Iterate Equation 13 to generate random values (i.e., $M \times N$ values).

$\rightarrow$ **Step 2:** The generated values are saved in a one-dimensional array. η.
$\rightarrow$ Update η as follows:

$$\phi = \eta_i * K_{num}$$

$\rightarrow$ **Step 3:** K_{num} denotes a significantly large value employed to increase the intensity of the stored values within η.

$\rightarrow$ **Step 4:** The floor function is utilized to eliminate the decimal fraction of the numbers, and the resultant value is then stored in ξ.

$\rightarrow$ **Step 5:** In order to constrain the generated value to fall within the range of [0, $M \times N$], apply the modulo function as illustrated below:

$$R_1' = modulo(\xi, M \times N + 1)$$

$\rightarrow$ **Step 6:** The identical steps are reiterated with distinct initial conditions and control parameter values to create the random sequence R_2'.
$\rightarrow$ Reshape the random sequence into 2-D matrix to generate a random image as follows:

$$R_{im} = reshape(R_1', M, N)$$

End

Algorithm 1. Generation of random sequences and key image K_{im}.

8

Confusion stage

During the phase of transformation, a Fibonacci transformation is introduced to scramble the positions of the pixels. It's important to highlight that any matrices corresponding to CAi, DOi, or CTi can be utilized as transformation matrices to scramble the pixels. Notably, it's possible to parameterize these transformations using a single variable. It's worth mentioning that Cassini's identity is a specific case of the other two identities.

In our experimental setup, we specifically employed CAi during the confusion phase. The key to this confusion denoted as k_c, is instrumental in determining the value of j for CAi. Subsequently, this value of i is used to scramble the pixels. To compute i, we consider the formula $i = \mod(k_c, P) + 3$, where P represents a prime number with a moderate value, and this value is made public.

For an image (I) with dimensions $R \times C$, where R and C show the number of rows and columns of the image pixels, and $R = C$. The pixel's location is indicated as (a, b), and subsequent to the transformation, the new coordinates are expressed as (a', b'). This relationship is supported by Eq. (14).

$$\begin{bmatrix} a' \\ b' \end{bmatrix} = \begin{bmatrix} f_{i+1} & f_i \\ f_i & f_{i-1} \end{bmatrix} \times \begin{bmatrix} a \\ b \end{bmatrix} \mod(R) \tag{14}$$

The procedure for the confusion process is demonstrated in Algorithm 2. It is notable that, with the same key, an identical transformation can be deduced. As a result, the confusion phase exhibits invertibility.

Start Input: Plaintext image ($R \times C$), K_c, P
Implementation of : $i = \mod(K_c, P) + 3$
    for a = 1:R
        for b = 1:C
            set initial values: f_1, R
            A = [a; b]   ▷ Input vector
            M = [f(i+1), f(i); f(i), f(i-1)]   ▷ Define the matrix
            result = M * A   ▷ Perform matrix multiplication
            result_mod = mod(result, R)   ▷ Apply modulo operation
            a'= result_mod(1);
            b'= result_mod(2);
        end
    end
Output: Confused image ($I^c(a', b')$)
End

Algorithm 2. Confusion stage (Level-1).

Diffusion stage

In order to induce level-2 confusion within $I^c(a', b')$, a pair of key sets, specifically, set-1 and set-2, are employed. Set-1 serves the purpose of conducting pixel-wise scrambling, while set-2 is applied to execute row-wise and column-wise scrambling procedures, resulting in the creation of a newly confused image denoted as $I'^c(a', b')$.

The transformation in the confusion phase retains the pixel intensities without any alteration. Consequently, the intensity profile of both the original unaltered image and the $I^c(a', b')$ image remains indistinguishable. This aspect introduces a potential security concern as an adversary might be able to make educated guesses about the original image based on the histogram profile of the scrambled image.

To address this issue, two different operations are implemented in this stage, each aimed at achieving the same objective. These operations consist of:

1. The application of XOR between the $I^c(a', b')$ and the K_{im}. This XOR operation is a pivotal step as it significantly alters the intensity values of the pixels within the $I^c(a', b')$ image. This XOR operation is executed at the initial stages of the diffusion process, and for the subsequent iterations in the diffusion phase, this operation is omitted.
2. The transformation of the image, which results from the initial XOR operation, is achieved through the application of the tribonacci transform, as given in Eq. (15).

$$\begin{bmatrix} V'_1 \\ V'_2 \\ V'_3 \\ V'_4 \end{bmatrix} = M^l \times \begin{bmatrix} V_1 \\ V_2 \\ V_3 \\ V_4 \end{bmatrix} \mod(256) \tag{15}$$

where $\begin{bmatrix} V_1 \\ V_2 \\ V_3 \\ V_4 \end{bmatrix}$ shows the set of three-pixel values and M^l is the transformation matrix. The inverse of the tribonacci transform will be:

$$\begin{bmatrix} V_1 \\ V_2 \\ V_3 \\ V_4 \end{bmatrix} = M^{-l} \times \begin{bmatrix} V'_1 \\ V'_2 \\ V'_3 \\ V'_4 \end{bmatrix} \mod(256) \tag{16}$$

These dual operations effectively modify the intensity values of the pixels in $I^c(a', b')$, ensuring that the pixel intensities become sufficiently scrambled. This process bolsters the security of the data by preventing any meaningful predictions about the original image based on the intensity profiles of the $I^c(a', b')$ image.

In the transformation described above, a set of four pixels is required simultaneously. Therefore, the image's pixels are organized into groups, each comprising four pixels. Let's assume there are N number of groups labeled as $N_1, N_2, \cdots, N_N$, and the pixels within each group N_i are represented as $\{V_1, V_2, V_3\}$ (i.e., $N_i = \{V_1, V_2, V_3\}$). There are three possible scenarios to consider:

Case-1: The image contains a total of 4L pixels.

- **(a)** During the encryption process, each group N_i (where $1 \leq i \leq L$) is subjected to transformation using Eq. (15) to yield the transformed group $N'i$, i.e., $N_i = TT(N_i)$.
- **(b)** When decrypting, the transformed group $N'i$ (for $1 \leq i \leq L$) is reversed to its original form N_i, with the assistance of Eq. (15) (i.e., $N_i = ITT(N'_i)$).

Case-2: The total number of pixels in the image is $3(L-1) + 1$, which can be expressed as $N_L = \{V_L, 1\}$. During the encryption process:

- **(a)** Initially, the first $(L-1)$ groups N_1, N_2, N_3, N_{L-1} undergo transformation using Eq. (15).
- **(b)** Subsequently, N_L is redefined as $N_L = \{V'_{L1,2}, V'_{L-1,3}, V_L, 1\}$ and subjected to transformation, resulting in $L'_L = \{V''_{L-1,2}, L''_{L,3}, L'_{L,1}\} = TT(N_L)$ using Eq. (15).
- **(c)** The resulting image with diffusion is defined as follows:

$$N'_1 N'_2 || \cdots || N'_{L-2} \{V'_{L-1}, 1\} \tag{17}$$

In the decryption process, the steps are as follows:

- (a) Begin by inversely transforming the first $L-2$ groups of the diffuse image, resulting in $\{N_1, N_2, \cdots, N_{L-2}\}$, where each N_i is obtained as $N_i = ITT(N'_i)$ for $1 \leq i \leq L2$.
- (b) Following that, calculate $\{V'_{L-1,2}, V'_{L-1,3}, V_{L,1}\}$ by applying the inverse transformation to N'_L, yielding $\{V'_{L-1,2}, V'_{L-1,3}, V_{L,1}\} = ITT(N'_L)$.
- (c) Subsequently, perform the computation for $V_{L-1,1}, V_{L-1,2}, V_{L-1,3}$ by applying the inverse transformation to the corresponding elements $[V'_{L-1,1}, V'_{L-1,2}, V'_{L-1,3}]$.

The previous version of the diffused image can be reconstructed as $N_1 || N_2 || \cdots || V_{L-2} || \{V_{L-1,1}, V_{L-1,2}, V_{L-1,3}\} || \{V_{L,1}\}$.

Case-3: In the case of $3(N-1) + 2$ pixels, which is denoted as $N_L = \{V_{L,1}, V_{L,2}\}$, during the encryption process:

- (a) Initially, the first $(L-1)$ groups are transformed, resulting in $N'_1, N'_1, \cdots, N'_{L-1}$.
- (b) The pixel $V'_{r-1,3}$ from N'_{L-1} is combined with Gr to form $N_L = \{V'_{L-1,3}, V_{L,1}, V_{L,2}\}$.
- (c) N_L is then subjected to transformation using Eq. (15), resulting in $N'_L = \{V''_{L-1,3}, V'_{L,3}, V'_{L,2}\}$.
- (d) The diffuse image is formed as $N'_1 || N'_2 || \cdots || N'_{L-2} || NL' || \{V'_{L-1,1}, V'_{L-1,2}\}$.

For the decryption process,

- (a) To begin, the first $L-2$ groups of the diffuse image are inversely transformed, resulting in $\{N_1, N_2, \cdots, N_{L-2}\}$ (where $N_i = ITT(N'_i)$ for $1 \leq i \leq L-2$).
- (b) Following that, the transformation $ITT(N'_L)$ is used to compute $\{V'_{L-1,3}, N_{L,1}, N_{L,2}\}$.
- (c) Subsequently, the transformation $ITT[N'_{L-1,1}, V'_{L-1,2}, V'_{L-1,3}]$ is applied to compute $\{V_{L-1,1}, V_{L-1,2}, V_{L-1,3}\}$.

The image that existed prior can be reconstructed as $N_1 || N_2 || \cdots || N_{L-2} || \{V_{L-1,1}, V_{L-1,2}, V_{L-1,3}\} || \{V_{L,1}, V_{L,2}\}$.

Bit-plane extraction
Bit-planes (B_i) are the binary images that can be extracted from digital images. Mathematically, B_i can be extracted using Eq. (18).

$$\begin{cases} B_1 = (\frac{P(a,b)}{2^0})mod(2), & B_2 = (\frac{P(a,b)}{2^1})mod(2) \\ B_3 = (\frac{P(a,b)}{2^2})mod(2), & B_4 = (\frac{P(a,b)}{2^3})mod(2) \\ B_5 = (\frac{P(a,b)}{2^4})mod(2), & B_6 = (\frac{P(a,b)}{2^5})mod(2) \\ B_7 = (\frac{P(a,b)}{2^6})mod(2), & B_8 = (\frac{P(a,b)}{2^7})mod(2) \end{cases} \qquad (18)$$

where $P(a, b)$ represent the plaintext image and $B_1, B_2, \cdots, B_8$ are its binary bit-planes.

The extracted B_i can exhibit variations in the quantity of information they contain. For instance, the set of the first four bit-planes (B_8, B_7, B_6, B_5) has the maximum information, while the group of the second four bit-planes (B_4, B_3, B_2, B_1) holds the minimum information, as illustrated in Fig. 4.

The percentage content within each bit-plane can be computed using Eq. (19), and the resultant numerical values are displayed in Table 3.

$$P_i = \frac{2^{i-1}}{\sum_{j=1}^{8} 2^{j-1}}, \qquad \text{where } i \in [1, 8] \qquad (19)$$

The diffused image is further encrypted using the bit-plane extraction method. The mathematical steps are given below:

To explain the mathematics behind the encryption of diffused image, a portion of the diffused image of size 3×3 is taken.

A 3×3 portion of the diffused image is:

$$D_{img} = \begin{bmatrix} 150 & 26 & 210 \\ 35 & 127 & 206 \\ 42 & 169 & 166 \end{bmatrix}$$
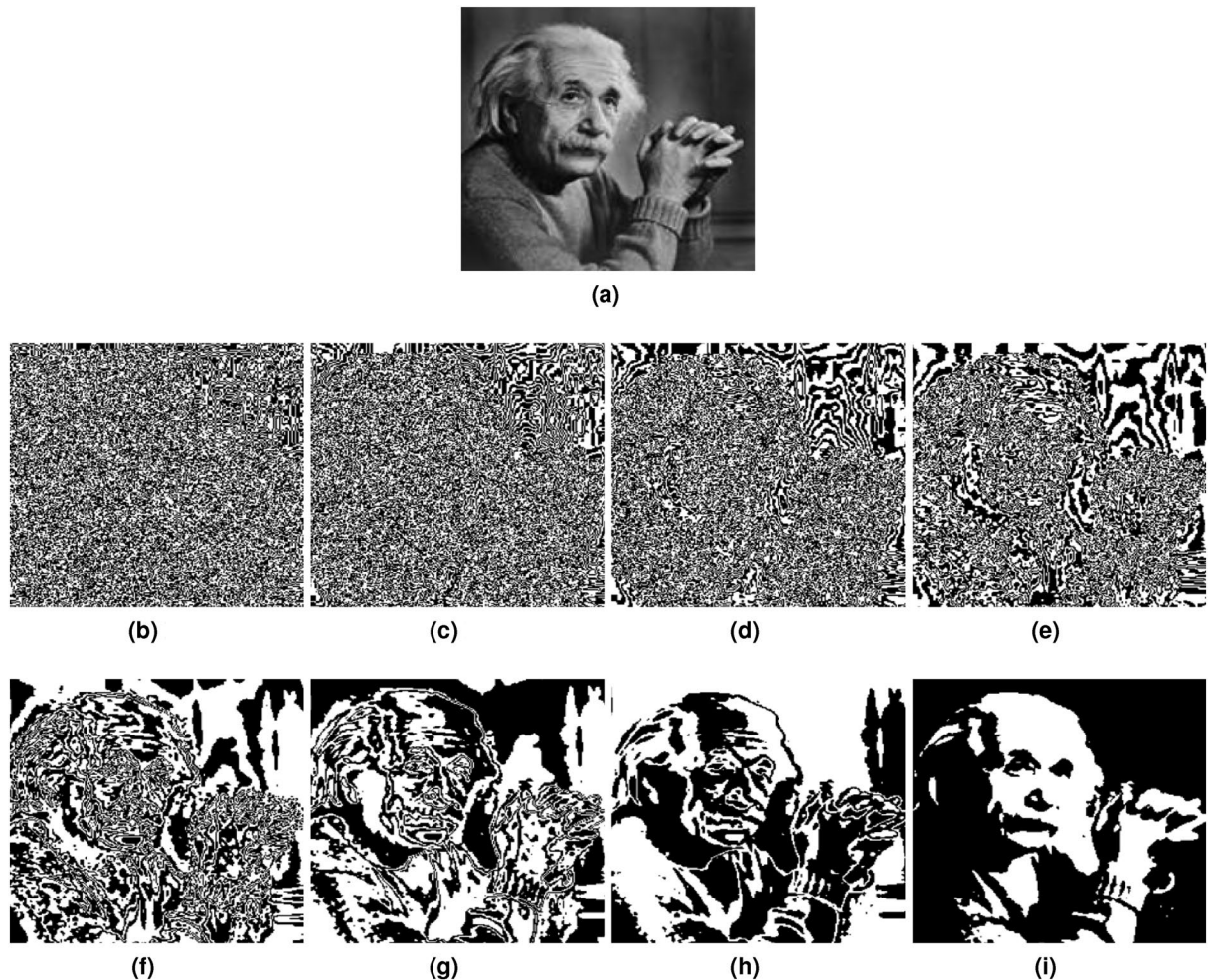
The binary representation of D_{img} will be:

(a)

(b)   **(c)**   **(d)**   **(e)**

(f)   **(g)**   **(h)**   **(i)**

Figure 4. Extracted bit-planes form plaintext image. (**a**) Plaintext image. (**b**) B1. (**c**) B2. (**d**) B3. (**e**) B4. (**f**) B5. (**g**) B6. (**h**) B7. (**i**) B8.

B_i (i = 1, 2, ···, 8)	Percentage information
1	0.392
2	0.784
3	1.568
4	3.137
5	6.274
6	12.549
7	25.098
8	50.196

Table 3. Information percentage.

$$D_{bin} = \begin{bmatrix} 10010110 & 000110100 & 11010010 \\ 00100011 & 01111111 & 11001110 \\ 00101010 & 10101001 & 10100110 \end{bmatrix}$$

To obtain the B_i from D_{bin}, examine the corresponding bit of each pixel. For example, for B_8, select the 8^{Pth} bit from every pixel. Likewise, for B_7, select the 7th bit from each pixel, and so forth. The resulting set of eight B_i derived from D_{bin} will be:

$$B_8 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, B_7 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}, B_6 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}, B_5 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

$$B_4 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}, B_3 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, B_2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, B_1 = 5 \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

If the positions of the values within the $P - SI_i$ are rearranged, the resulting permuted bit-planes, denoted as (PB_i), will be:

$$PB_8 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}, PB_7 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, PB_6 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, PB_5 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

$$PB_4 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}, PB_3 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, PB_2 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}, PB_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Following the permutation process, the binary values situated at position (1,1) within each PB_i are consolidated to form the binary numbers composing the pixel value situated at (1,1) in the permuted image. Similarly, for acquiring the pixel (1,2) in the permuted image, the binary numbers positioned at (1,2) within each PB_i are merged. This iterative process is repeated to deduce all the pixel values in the permuted image (P_{im}). Consequently, the resulting P_{im} corresponding to I_{BMI} is as follows:

$$P_{im} = \begin{bmatrix} 10010110 & 11111010 & 01010110 \\ 01100100 & 00100010 & 01111010 \\ 11001000 & 01001000 & 10101000 \end{bmatrix}$$

After the conversion from binary to decimal, the updated matrix p'_{im}, denoting the transformed version of P_{im}, is given below.

$$P'_{im} = \begin{bmatrix} 150 & 250 & 86 \\ 100 & 34 & 122 \\ 200 & 72 & 168 \end{bmatrix}$$

From the matrix P'_{im}, it can be seen that this is entirely different from the original matrix I. Likewise, the entire procedure will be reiterated for all the rows and columns.

Discrete wavelet transform

The wavelet transform (WT), developed in the 1980s, is a mathematical tool known for efficiently analyzing transient signals with wide frequency bands. The Wavelet Transform (WT) decomposes a signal into various representations of a mother wavelet, accomplished through shifts and scaling, enabling the segmentation of a signal into constituent wavelets. These component wavelets can then undergo further processing, including decimation, which removes some of the finer details. This process isolates the high-frequency sub-bands(HL and HH) and low-frequency sub-bands (LL and LH). The coarser details, containing the low-frequency components, are identified using larger wavelets, such as the LL-sub-band. In the context of images, the low-frequency

sub-band typically contains the majority of the plaintext information, whereas the high-frequency sub-bands capture finer details, such as edges as shown in Fig. 5.

The proposed encryption technique utilizes the Haar wavelet. In this method, the Haar wavelet transform is expressed through the matrix equation $G' = WGW^T$, where G denotes an image with dimensions $A \times A$, W represents the Haar transform matrix of size $A \times A$, and G' symbolizes the resultant transformed matrix of size $A \times A$, encompassing the Haar basis function $g_m(z)$. This function is defined within the interval $z \in [0, 1]$, where m ranges from 0 to M-1. The decomposition of this function can be comprehended as follows:

The Haar wavelet transformation is represented by a matrix equation, with G' denoting the transformed image having dimensions $A \times A$, W representing the Haar transformation matrix of identical size, and G signifying the resultant transformed matrix also sized $A \times A$. This matrix encompasses the Haar basis function $g_m(z)$, defined within the interval $z \in [0, 1]$, where m varies from 0 to $M - 1$. To elucidate this function's breakdown, the following explanation is provided:

$$n = 2^r + l \tag{20}$$

Here r symbolizes the highest power of 2 contained within the integer n while l represents the remainder, expressed as $l = qr - n$. Equation (21) serves to formally describe the Haar basis function.

$$h_c(a) = \frac{1}{\sqrt{P}} \begin{cases} 1 & if\, n = 0 \quad \& \quad 0 \le a \le 1 \\ 2^{r/2} & if\, z > 0 \quad \& \quad l/2^r \le a < \\ & \qquad\qquad \frac{l+0.5}{2^l} \\ -2^{r/2} & if\, n > 0 \quad \& \quad (l+0.5)/2^r \\ & \qquad \le a < \frac{l+1}{2^r} \\ 0 & \text{Elsewhere} \end{cases} \tag{21}$$

The matrix required to perform the two-dimensional discrete Haar wavelet transform (DHWT) can be derived by replacing the inverse transformation kernel, as given in Eq. (22).

$$h'(a, n) = \frac{1}{\sqrt{O}} h_n(a/O) \qquad for \ \ a = 0, 1, 2, ..., M - 1 \tag{22}$$

where $h(a, n)$ will be:

$$h(a, n) = H' = \begin{bmatrix} h_0(\frac{0}{O}) & h_0(\frac{1}{O}) & \cdots & h_0(\frac{O-1}{O}) \\ h_1(\frac{0}{O}) & h_1(\frac{1}{O}) & \cdots & h_1(\frac{O-1}{O}) \\ h_2(\frac{0}{O}) & h_2(\frac{1}{O}) & \cdots & h_2(\frac{O-1}{O}) \\ \vdots & \vdots & \ddots & \vdots \\ h_{O-1}(\frac{0}{O}) & h_{O-1}(\frac{1}{O}) & \cdots & h_{O-1}(\frac{O-1}{O}) \end{bmatrix} \tag{23}$$

In 2-D digital image processing, individual rows of the image undergo a dual filter procedure that involves both a low-pass filter and a high-pass filter. Following this filtering, the outputs are subsequently downsampled by a factor of two, which leads to the formation of two distinctive information sub-bands: L_f representing the approximate information sub-band, and H_f representing the fine detail information sub-band, both in the horizontal direction. This entire operation is then replicated for every column of these newly generated images, resulting in the creation of four distinct frequency sub-bands.

Upon subjecting the LL_1 sub-band to another round of 2D-DWT, four additional sub-bands are obtained: LL_2, LH_2, HL_2, and HH_2. This iterative process can be repeated up to T times, yielding a sequence of sub-images: LL_T, LH_T, HL_T, and HH_T. The value of T plays a significant role, as it determines the reduction in size of each sub-band by a factor of 2^n, where n ranges from 1 to $N - 1$, with n belonging to the interval $[1, N-1]$. Within the framework of the proposed approach, a value of K is designated as 3, meaning that with $K = 4$, each sub-band's dimensions are scaled down to 32×32 when the original image dimension is 256×256. Figure 6 illustrates a pyramid pattern of the DWT decomposition, covering level-2 (i.e. K=2) to level-4 (i.e. K=4).

This is performed to reduce the computational time of the encryption process. For example, to create diffusion in an image using a substitution box (S-box), a time of approximately 20 seconds will be taken to encrypt the image of size 256×256[60]. Therefore, creating diffusion using an S-box in a small frequency band having
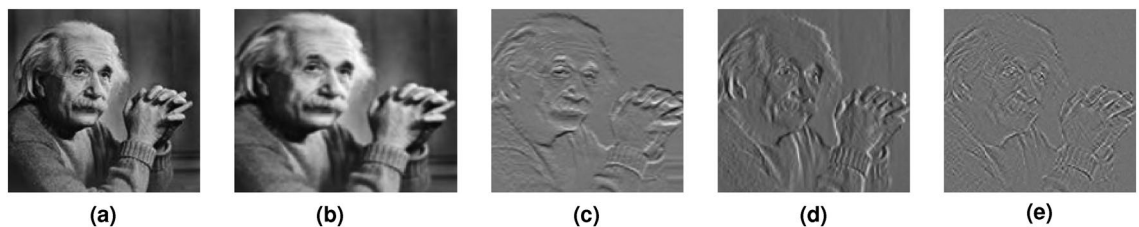

Figure 5. Decomposition of plaintext image into its four frequent sub-bands (When K=1). (**a**) Plaiontext image (256×256). (**b**) LL_1 sub-band (128×128). (**c**) LH_1 sub-band (128×128). (**d**) HL_1 sub-band (128×128). (**e**) HH_1 sub-band (128×128).
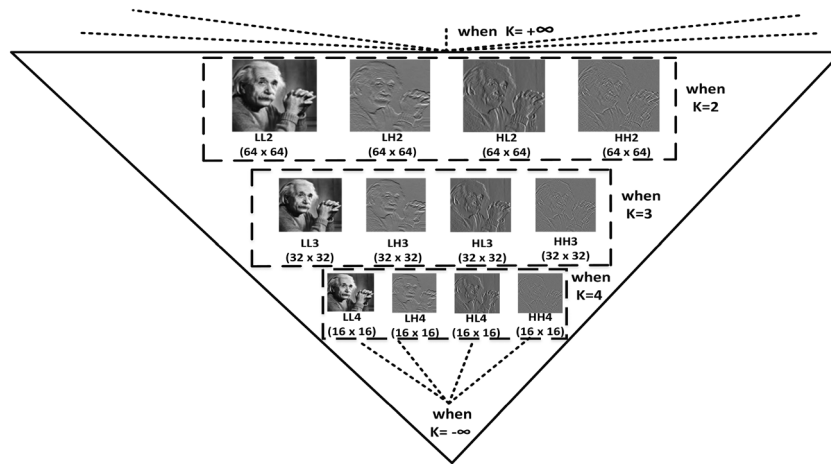
Figure 6. Pyramid behavior: DWT decomposition when the value of K gradually decreases from $+\infty$ to $-\infty$.

dimensions of 32×32 will take very little time compared to the time taken to create diffusion using an S-box in an image of size 256×256. The image P_{im} is generated in the preceding step is decomposed into its four frequency sub-bands, and then only the LL sub-band undergoes further decomposition until its size becomes 32×32 (i.e LL_4). The LL_4 is subsequently subjected to S-box substitution, as given in[61], to create the final encrypted image. The steps to perform the substitution in LL_4 are given in Algorithm 3.

The image denoted as P_{im}, which is produced in the previous stage, is subjected to decomposition into its four frequency sub-bands. Among these sub-bands, only the $LLsub-band$ is further decomposed until its dimensions reach a size of 32×32, referred to as LL_4. Following this, the LL_4 sub-band is then subjected to multiple S-box substitutions using the S-boxes i.e. S-box-1, S-box-2, and S-box-3 given in[61,62], and[63], respectively, to produce the final encrypted image (E_f). The specific steps for performing this substitution on LL_4 are given in Algorithm 3.

Input Sbox and LL_4
Output Substituted image ((E_f))
Start
R = randperm(32×32)   ▷ randperm is a MATLAB function that can be use to generate a sequence of random numbers
R' = modulo (R, 3) + 1
[ROW COL] =size(LL_4)
N=1;
 for i=1:ROW
  for j=1:COL
   $bin_p = dec2bin$(LL_4(i,j),8);
   sboxx_r_b = [bin_p(1) bin_p(2) bin_p(3) bin_p(4)];
   sboxx_c_b = [bin_p(5) bin_p(6) bin_p(7) bin_p(8)];
   sboxx_r_d = bin2dec(sboxx_r_b) + 1;
   sboxx_c_d = bin2dec(sboxx_c_b) + 1;
    if (R'(N)==1)
     $E_f(i,j)$= S-box-1(sboxx_r_d,sboxx_c_d);
    elseif (R'(N)==2)
     $E_f(i,j)$= S-box-2(sboxx_r_d,sboxx_c_d);
    elseif (R'(N)==3)
     $E_f(i,j)$= S-box-3(sboxx_r_d,sboxx_c_d);
    end
N=N+1;
  end
 end

Algorithm 3. Substitution process on LL_4.

The test images randomly sourced from Google of different sizes and the corresponding ciphertext images, which are produced using the proposed encryption method, are shown in Fig. 7. The size of each image displayed in Fig. 7a–g is 256×256. In contrast, the dimensions of each image given in Fig. 7h–j are 512×512. Upon examination of the figure, it becomes evident that there is no original plaintext image information is visible in the ciphertext images. This observation shows the efficacy of the proposed encryption scheme in successfully concealing the plaintext information.
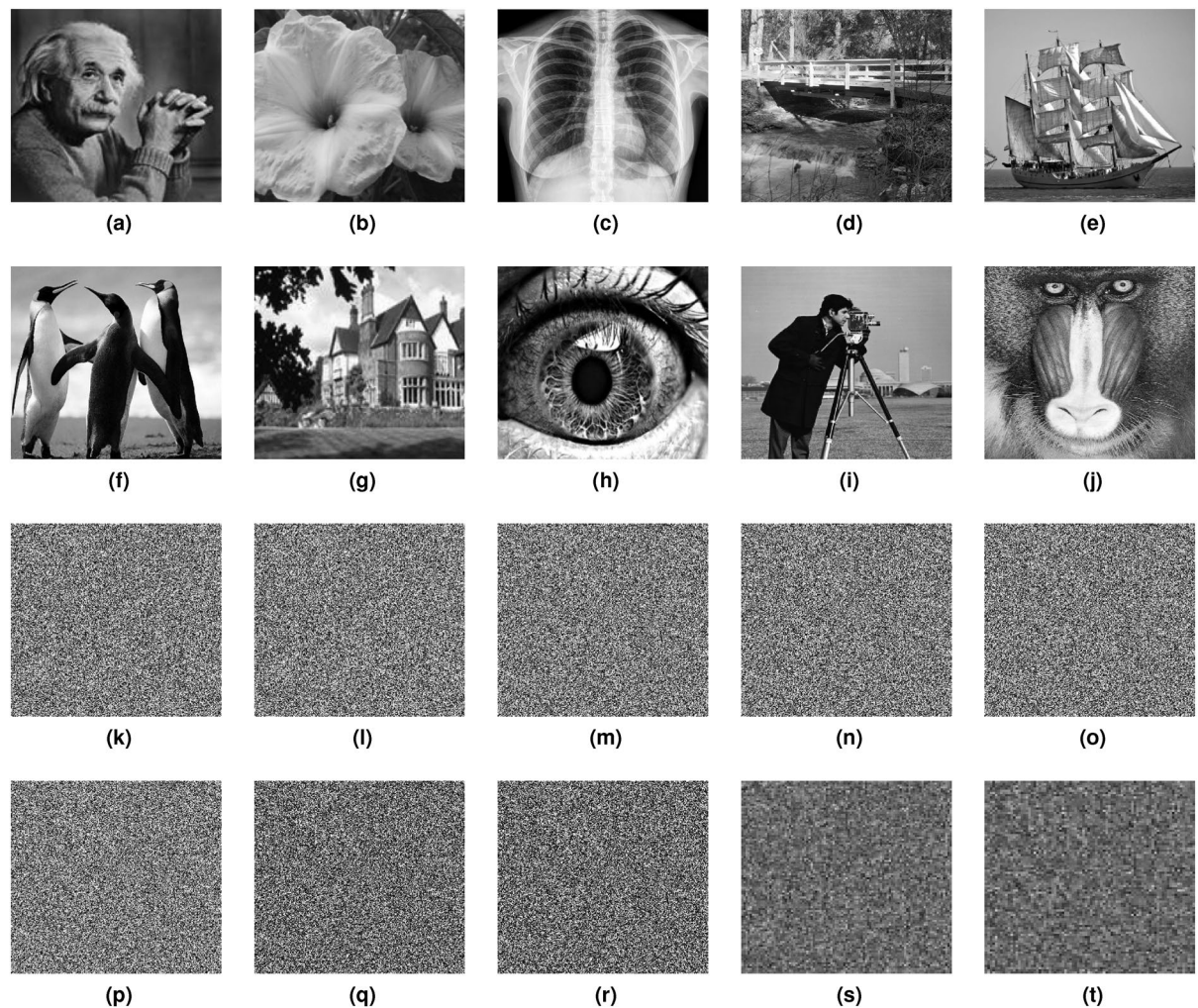
Figure 7. Visual encryption results: (**a–j**) input plaintext images, (**k–t**) corresponding ciphertext images.

Experimental results and analysis

To assess the effectiveness of the proposed encryption scheme, various statistical security analyses, including entropy, contrast, correlation, contrast, mean square error, and histogram analysis, are conducted. In addition to these statistical analyses, a series of attacks, such as cropping attacks, brute force attack, and noise addition attacks, are carried out to evaluate the robustness of the proposed encryption.

Computational time analysis

To optimize the encryption framework for real-time applications, it is necessary to minimize the computational time. This research conducts computational analyses on images of different sizes i.e. 256×256 and 512×512. Additionally, apart from assessing the computational time for encrypting images, the analysis extends to the key generation process, and decryption process. Although the key generation process is distinct from encryption, it plays a crucial role as the generated keys are utilized within the proposed encryption framework. The computational time for the propsoed encryption and decryption processes, and generating keys is measured using the built-in MATLAB command "tic toc." Table 4 presents the statistical values calculated using the MATLAB built-in command known as "tic toc". Table 4 reveals that the proposed encryption framework can encrypt images of sizes 256×256 and 512×512 in less than one second. This indicates the suitability of the proposed encryption framework for real-time applications. Moreover, it is evident that the execution times for encryption and decryption processes are approximately equal. This consistency arises because the decryption process involves the same number of mathematical steps as encryption, but in reverse order, along with the inversion of each step.

Histogram Analysis

In image processing, a histogram represents the distribution of the pixel values within an image. In the case of a robust encryption scheme, the histogram of the ciphertext image should exhibit characteristics such as flatness,

Key generation process	Size	Images	Encryption process	Decryption process
0.0001	256 × 256	Einstein	0.0020	0.0021
		Flowers	0.0021	0.0022
		Tree	0.0020	0.0021
-	512 × 512	Cameraman	0.0040	0.0042
		Eye	0.0041	0.0043
		Baboon	0.0040	0.0042

Table 4. Computational complexity analysis (sec).

In the context of a resilient encryption scheme, it is desirable that the histogram of the enciphered image shows features that include uniformity, even distribution, and a notable dissimilarity from the histogram of the original image.

Figure 8 displays different histograms, illustrating that the pixel distribution within the histogram of plaintext images is relatively uniform. Furthermore, the consistency in pixel distribution signifies the encryption scheme's capability to withstand potential histogram-based attacks.

Histogram variance analysis

Variance is used to assess the uniformity of the pixel distribution in an image. This metric is often deemed more reliable because it provides statistical values rather than relying on histogram visualizations. This metric is typically considered more reliable because it offers statistical values instead of relying on histogram visualizations. Mathematically, this metric can be calculated using Eq. (24).
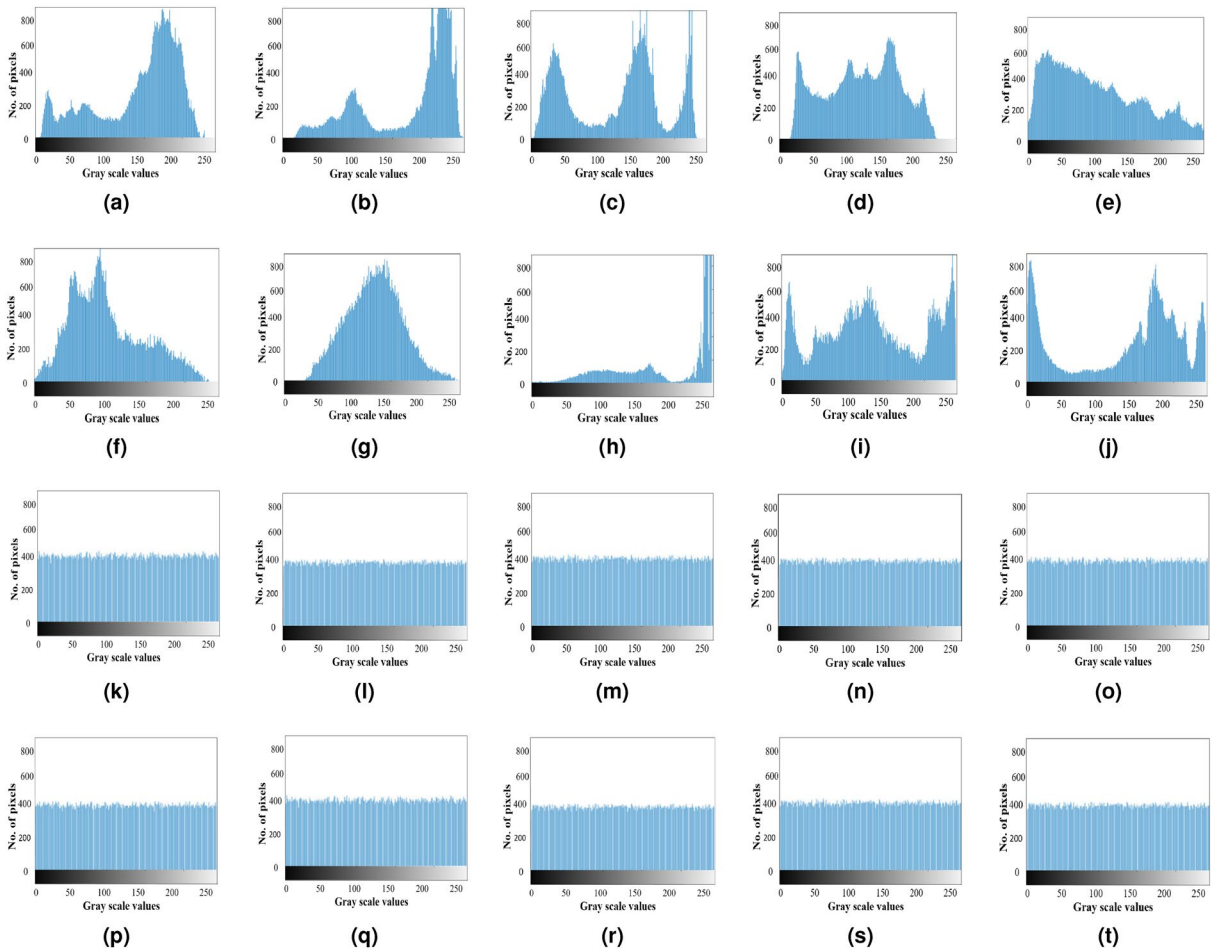

Figure 8. Histogram analysis: (**a–j**) histogram of an input plaintext images, (**k–t**) histogram of corresponding ciphertext images.

$$Var(P) = \frac{1}{256} \sum_{L=1}^{256} [p_i - E(P)]^2 \tag{24}$$

In the equation, P represents the pixel stream, where $P = \{ p_1, p_2, p_3 \cdots, p_{256}$, and p_i denotes the pixel value at the Lth position. The term $E(P)$ is computed as $E(P) = \frac{1}{256} \sum_{L=1}^{256} p_i$. In the context of robust encryption, low variance values are desirable.

Table 5 presents a range of variance values for the enciphered images produced by both the proposed and the encryption schemes presented in the past recent years. These variance values highlight the superior performance of the proposed scheme in comparison to the existing ones.

Maximum Deviation

The performance of a cryptographic algorithm can be evaluated by measuring the deviation between the pixel values of the original and enciphered images[69]. If the deviation in pixel intensities between the original and enciphered images is maximized, it indicates a higher level of security for the encryption technique. Mathematically, the maximum deviation can be expressed as

$$M_A = \frac{A_0 + A_{N-1}}{2} + \sum_{L=1}^{N-2} A_L \tag{25}$$

Here, N stands for the number of gray levels, and A_L represents the amplitude of the histogram at the Lth index. A higher value of M_A indicates a more significant difference between the ciphertext and the original image. Table 6 presents the results of M_A for the proposed scheme and the existing algorithms. The comparison reveals that the proposed encryption technique outperforms the existing schemes. However, images with high texture can yield a higher maximum deviation. Table 6 indicates a slightly higher value of the Maximum Absolute (MA) deviation compared to the proposed work. This discrepancy is attributed to the high texture present in the plaintext image employed by the authors of the existing work.

Entropy

Entropy is used to assess the level of robustness in both plaintext and ciphertext images. A higher level of randomness within an image corresponds to a higher entropy value, as illustrated in Eq. (26).

$$Entropy \propto randomness \tag{26}$$

The entropy can be calculated using Eq. (27).

Size	Images	64	65	66	67	68	Proposed
256 × 256	Einstein	272.371	273.379	265.630	273.136	277.3694	260.637
	Flowers	267.697	266.378	275.672	279.994	268.978	261.300
	Tree	274.370	275.336	270.039	274.698	272.451	260.633
	Man	275.637	276.336	279.987	274.831	275.379	259.596
	Boat	277.687	274.678	279.689	274.678	274.678	262.116
512 × 512	Cameraman	271.678	275.298	279.164	275.245	276.315	261.378
	Eye	271.335	271.189	275.269	277.591	271.679	264.501
	Baboon	273.164	275.941	276.972	271.39	270.113	266.677

Table 5. Histogram variance analysis.

Size	Images	64	65	66	67	68	Proposed
256 × 256	Einstein	25121	25881	24985	24643	25329	25989
	Flowers	25989	25787	24692	24345	25719	26793
	Tree	26180	26047	24673	24336	25014	26249
	Man	25964	26646	24370	25042	24890	26796
	Boat	25825	25144	25012	25008	25121	25598
512 × 512	Cameraman	25935	25763	25899	25864	25836	26531
	Eye	25836	25899	25968	25710	25967	26318
	Baboon	25861	25734	25931	25793	25799	26634

Table 6. Maximum deviation analysis.

$$Entropy = -\sum p(k_i) \log_2 \rho(k_i) \tag{27}$$

where ρk_i represents the probability of occurrence for variable i.

The ideal entropy value is dependent on the number of bits used to represent the image. For example, in a binary image, the ideal entropy value can be 2. In the case of eight-bit images used in the proposed work, the ideal entropy value is 8.

All images utilized in the experimental results and analysis are 8-bit images. Therefore, the ideal value for each encrypted image should approach or be approximately equal to 8. Table 7 indicates that the entropy values associated with the proposed encryption scheme exhibit a significant proximity to the value of 8. Furthermore, the existing encryption scheme also attains entropy values near eight, though these values remain slightly lower than those achieved by the proposed encryption scheme.

Correlation

The correlation among the pixel values of an image reflects the degree of the intensity relationship between them. It also quantifies how similar or dissimilar pixel values are. Greater differences between pixel values indicate lower correlation[70]. This correlation relationship can be expressed mathematically as follows:

$$Correlation \propto \frac{1}{\text{pixel divergence}}$$

The mathematical formula for determining the correlation among image pixels can be expressed as:

$$CorrCoff = \frac{Cov(w,t)}{\sigma_w \sigma_t}, \qquad \sigma_w = \sqrt{VAR_w}, \qquad \sigma_t = \sqrt{VAR_t}$$

$$VAR(n) = \frac{1}{R}\sum_{u=1}^{R}(n_s - E(n))^2, \qquad Cov(n,m) = \frac{1}{R}\sum_{u=1}^{R}(n_s - E(n))(h_s - E(m))$$

where E represents the expected value operator, and σ signifies the standard deviation.

In a plaintext image, there is typically a high correlation between pixel values because the image content is readily visible. Conversely, in a ciphertext image where pixel content is concealed, there should be a lower correlation among the pixels. Thus, it is essential that the correlation values between pixels in ciphertext images are minimized to prevent the visualization of any content in the encrypted image[71].

Table 8 presents a comparative analysis of correlation values across different encryption schemes, including the proposed encryption technique. The data presented in Table 8 indicates that the correlation values produced by the proposed scheme are less than those observed in the existing schemes.

Size	Images	64	65	66	67	68	Proposed
256 × 256	Einstein	7.9876	7.9960	7.9936	7.9942	7.9986	7.9992
	Flowers	7.9777	7.9971	7.9936	7.9989	7.9990	7.9993
	Tree	7.9789	7.9982	7.9936	7.9951	7.9973	7.9991
	Man	7.9888	7.9940	7.9946	7.9973	7.9987	7.9990
	Boat	7.9879	7.9983	7.9982	7.9990	7.9983	7.9992
512 × 512	Cameraman	7.9875	7.9961	7.9973	7.9989	7.9980	7.9994
	Eye	7.9851	7.9967	7.9941	7.9971	7.9973	7.9994
	Baboon	7.9869	7.9967	7.9982	7.9966	7.9988	7.9995

Table 7. Entropy analysis.

Size	Images	64	65	66	67	68	Proposed
256 × 256	Einstein	0.0026	0.0016	0.0017	0.0025	0.0018	0.0001
	Flowers	0.0016	0.0014	-0.0025	-0.0019	0.0010	-0.0015
	Tree	0.0022	-0.0020	-0.0012	0.0020	-0.0014	-0.0001
	Man	0.0027	-0.0019	-0.0016	-0.0013	0.0031	-0.0015
	Boat	0.0022	-0.0079	-0.0019	0.0038	0.0049	-0.0020
512 × 512	Cameraman	0.0026	-0.0036	0.0054	0.0011	0.00013	-0.0003
	Eye	0.0062	0.0012	-0.0011	-0.0032	0.001	0.0003
	Baboon	0.0046	0.0045	0.0033	0.0041	0.0034	0.0001

Table 8. Correlation analysis.

In addition to the statistical analysis of correlation, a visual assessment can be conducted using scatter plots. Figure 9(a), and 9(e) show the plaintext and ciphertext images, respectively. Whereas, Fig. 9b–d,f–h illustrate scatter diagrams for both plaintext and ciphertext images. Upon examination of these scatter diagrams, it can be seen that in Fig. 9b–d, the blue dots are closely grouped together, indicating a high pixel correlation. Conversely, in Fig. 9f–h, the blue dots are dispersed, signifying a substantial reduction in pixel correlation. This demonstrates the effectiveness of the proposed encryption scheme in mitigating pixel correlations within the images.

Noise and clipping attack analysis

To make the decryption fail, attackers commonly tamper with encrypted images by incorporating noise. An effective encryption scheme must demonstrate noise resilience to effectively mitigate noise attacks. In assessing the influence of the noise attack, 0.02 means 2% of the pixels are affected by the salt and pepper noise introduced into the encrypted image. The modified encrypted image, now impacted by salt and pepper noise, is decrypted using the proposed decryption algorithm. Figure 10a–d displays the plaintext image, the encrypted image, a noisy version of the plaintext image, and a clipped version of the encrypted image, respectively. The decryption outcomes are depicted in Fig. 10e,f, where it can be seen that although the exact pixel values are not restored, the content of the plaintext can be clearly visualized.

In contrast, attackers also attempt to compromise decryption integrity by clipping parts of the encrypted images. To evaluate the resistance of the proposed encryption framework against clipping attacks, $\frac{1}{16}$, or approximately 16.6% of the ciphertext image, is ciphered from the encrypted images. These clipped versions are then decrypted to recover the plaintext images. The decryption results from these noisy and clipped encrypted images are illustrated in Fig. 10e,f, respectively, which demonstrate that most of the content of the plaintext image remains visible in the decrypted images. Moreover, Fig. 10g,h are recovered images from noisy and cllpied encrypted images, respectively, using the encryption techniques presented in[72]. The comparison utilizes the same plaintext image, specifically a chest X-ray image, which is also used in the study presented in[72]. This comparison reveals that our proposed encryption framework is more capable of reconstructing plaintext information from both noisy and clipped versions of the encrypted images. Apart from the visual results, statistical analyses are also conducted for both noise and clipping attack analysis. The statistics are detailed in Table 9, which illustrates that the proposed method shows a slight improvement over the encryption scheme introduced in[72].

Uniqueness and the advantages of the proposed encryption framework

In this section, various features and advantages of the proposed encryption framework are provided in the domain of secure data protection, as given below:

- *Innovative techniques:* The proposed encryption framework distinguishes itself from existing encryption schemes through the strategic integration of innovative techniques. These methods are carefully chosen to concurrently enhance both security and computational efficiency.
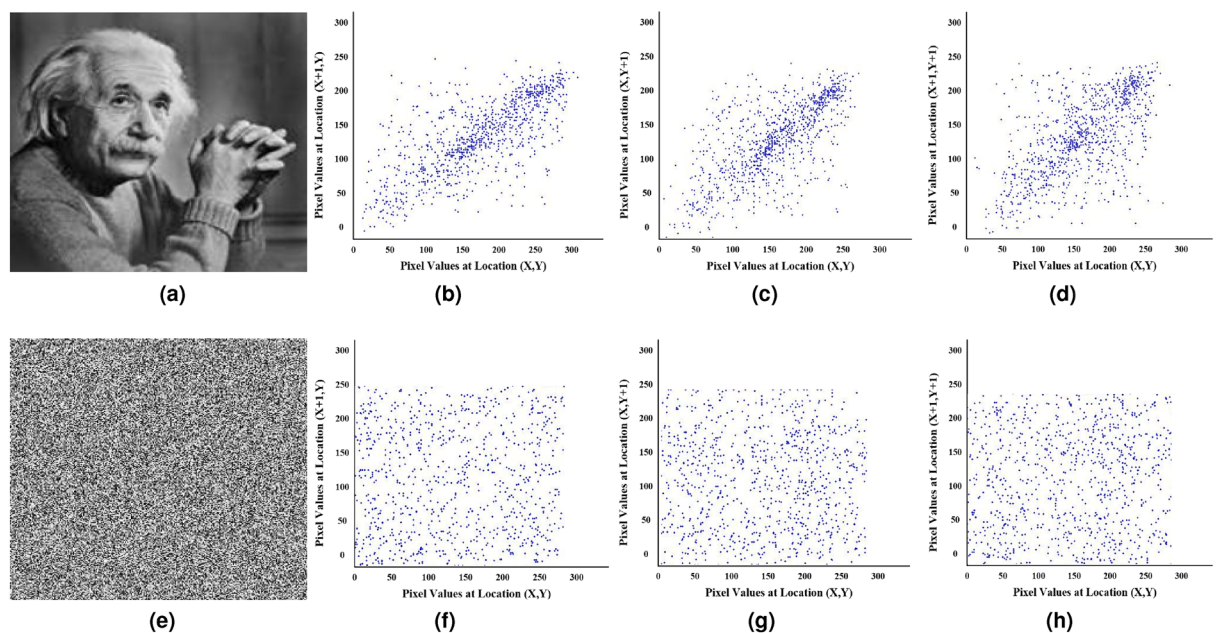

Figure 9. Pixel correlation analysis in horizontal, vertical, and diagonal directions. (**a**) Plaintext image. (**b**) Horizontal correlation. (**c**) Vertical correlation. (**d**) Diagonal correlation. (**e**) Ciphertext image. (**f**) Horizontal correlation. (**g**) Vertical correlation. (**h**) Diagonal correlation.
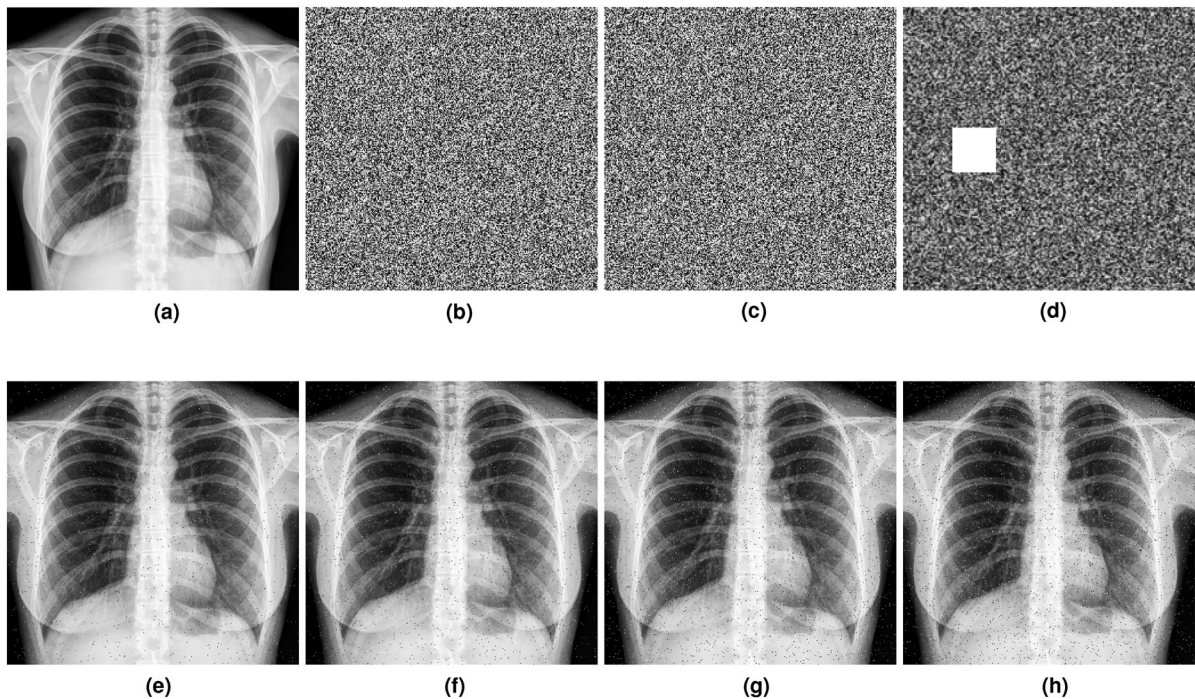
Figure 10. Noise and clipping attack analysis. (**a**) Plaintext image. (**b**) Encrypted image. (**c**) Noisy version of the encrypted image. (**d**) Clipped version of the encrypted image. (**e**) Decryption from the noisy encrypted image using the proposed framework. (**f**) Decryption from the clipped encrypted image using the proposed framework. (**g**) [Decryption from the noisy encrypted image using the encryption framework proposed in 72. (**h**) Decryption from the clipped encrypted image using the encryption framework proposed in 72.

Salt & pepper noise	Clipping area	Recover a percentage from the noisy version of the encryption using the proposed encryption framework	Recover a percentage from the clipped version of the encryption using the proposed encryption framework	Recover a percentage from the noisy version of the encryption framework proposed in[72]	Recover a percentage from the clipped version of the encryption using the encryption framework proposed in[72]
2%	$\left(\frac{1}{6}\right)^{th}$	97.8%	96.8%	97.4%	96.3%

Table 9. Percentage recovery form the noisy and clipped versions of the ciphertext images.

- *Key components:* The incorporation of chaotic maps, FT, TT, and Discrete Wavelet Transform (DWT) diffusion represents a unique amalgamation. This combination contributes significantly to fortifying the robustness against cyberattacks.
- *Dynamic pixel scrambling:* The incorporation of chaotic maps and FT ensures the dynamic behavior of initial pixel scrambling.
- *Multilayered security architecture:* The introduction of TT for level-1 diffusion, along with a level-2 diffusion in which XOR operations are involved results in a multilayered security architecture.
- *Secondary key generation:* The utilization of DWT for secondary key generation and high-frequency sub-band substitution further enhances the encryption process.
- *Statistical validation:* Impressive statistical values of security parameters consistently demonstrate the effectiveness of the proposed encryption framework compared to existing state-of-the-art methods.
- *Real-world applicability:* The proposed encryption framework is suitable for real-world applications where less processing time is a critical requirement.

Conclusion and future work

The proposed work presents a new image encryption technique that relies on several key components, including the Fibonacci transformation, chaotic maps, the DWT, bit-plane extraction, and Tribonacci transformations. To secure the image, a 2×2 Fibonacci matrix is employed for scrambling, while a 3×3 Tribonacci matrix is utilized in the diffusion phase to modify pixel values. Chaotic maps are employed to generate key sequences, which are used to introduce confusion to the image pixels. The process begins with comprehensive pixel scrambling, encompassing both row- and column-wise transformations. Therefore, the diffusion phase is initiated, which is started with the application of the TT to achieve level-1 diffusion in the scrambled image. The diffused image undergoes a level-2 diffusion through the incorporation of the bit-plane extraction technique. This involves

extracting bit planes from the level-1 diffused image and a 2-dimensional key image. For a more extensive level-3 diffusion, the DWT is utilized to decompose the diffused image into four frequency sub-bands. Among these, only the LL_1 is substituted using the S-box to reduce computational time during encryption. Several statistical analyses are conducted to evaluate the proposed encryption technique, demonstrating its superior performance in terms of both security and computational complexity compared to existing methods.

Future work may explore the application of this encryption technique in various domains, such as securing multimedia data in cloud storage or real-time image transmission. Additionally, we could focus on optimizing the computational efficiency of the color image encryption process, which will make it even more suitable for real-time applications. Investigating the potential integration of additional advanced encryption algorithms with traditional encryption techniques can enhance overall security.

Data availability
The datasets used and/or analysed during the current study available from the corresponding author on reasonable request.

References
1. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A. & Akin, E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics* **12**, 1333 (2023).
2. de Azambuja, A. J. G. *et al.* Artificial intelligence-based cyber security in the context of industry 4.0: A survey. *Electronics* **12**, 1920 (2023).
3. Rawat, A. S., Deshmukh, M. & Singh, M. A novel multi secret image sharing scheme for different dimension secrets. *Multimedia Tools Appl.* 1–37 (2023).
4. Abd-El-Atty, B. A robust medical image steganography approach based on particle swarm optimization algorithm and quantum walks. *Neural Comput. Appl.* **35**, 773–785 (2023).
5. Rezaei, B., Ghanbari, H. & Enayatifar, R. An image encryption approach using tuned Henon chaotic map and evolutionary algorithm. *Nonlinear Dyn.* **111**, 9629–9647 (2023).
6. Kocak, O., Erkan, U., Toktas, A. & Gao, S. Pso-based image encryption scheme using modular integrated logistic exponential map. *Expert Syst. Appl.* **237**, 121452 (2024).
7. Ahmad, M., Alam, M. Z., Umayya, Z., Khan, S. & Ahmad, F. An image encryption approach using particle swarm optimization and chaotic map. *Int. J. Inf. Technol.* **10**, 247–255 (2018).
8. Singh, K. N., Singh, O. P., Baranwal, N. & Singh, A. K. An efficient chaos-based image encryption algorithm using real-time object detection for smart city applications. *Sustain. Energy Technol. Assess.* **53**, 102566 (2022).
9. Zahid, A. H., Al-Solami, E. & Ahmad, M. A novel modular approach based substitution-box design for image encryption. *IEEE Access* **8**, 150326–150340 (2020).
10. Arab, A., Rostami, M. J. & Ghavami, B. An image encryption method based on chaos system and AES algorithm. *J. Supercomput.* **75**, 6663–6682 (2019).
11. Abd-El-Atty, B., Iliyasu, A. M., Alanezi, A. & Abd El-latif, A. A. Optical image encryption based on quantum walks. *Opt. Lasers Eng.* **138**, 106403 (2021).
12. Younes, M. A. B. A survey of the most current image encryption and decryption techniques. *Int. J. Adv. Res. Comput. Sci.* **10**, 9 (2019).
13. Long, M., Zhao, Y., Zhang, X. & Peng, F. A separable reversible data hiding scheme for encrypted images based on Tromino scrambling and adaptive pixel value ordering. *Signal Process.* **176**, 107703 (2020).
14. Wang, J., Geng, Y.-C., Han, L. & Liu, J.-Q. Quantum image encryption algorithm based on quantum key image. *Int. J. Theor. Phys.* **58**, 308–322 (2019).
15. Suganyadevi, S., Seethalakshmi, V. & Balasamy, K. A review on deep learning in medical image analysis. *Int. J. Multimed. Inf. Retr.* **11**, 19–38 (2022).
16. Singh, K. N., Baranwal, N., Singh, O. P. & Singh, A. K. Sielnet: 3D chaotic-map-based secure image encryption using customized residual dense spatial network. *IEEE Trans. Consum. Electron.* (2022).
17. Kamal, S. T., Hosny, K. M., Elgindy, T. M., Darwish, M. M. & Fouda, M. M. A new image encryption algorithm for grey and color medical images. *IEEE Access* **9**, 37855–37865 (2021).
18. Aruna, M., Arulkumar, V., Deepa, M. & Latha, G. C. P. Medical healthcare system with hybrid block based predictive models for quality preserving in medical images using machine learning techniques. In *2022 International Conference on Advanced Computing Technologies and Applications (ICACTA)*, 1–10 (IEEE, 2022).
19. Thakur, M. Cyber security threats and countermeasures in digital age. *Journal of Applied Science and Education (JASE)* 1–20 (2024).
20. Sayduzzaman, M., Sazzad, S., Rahman, M., Rahman, T. & Uddin, M. K. Managing escalating cyber threats: Perspectives and policy insights for bangladesh.
21. Kumari, M. & Gupta, S. Performance comparison between chaos and quantum-chaos based image encryption techniques. *Multimed. Tools Appl.* **80**, 33213–33255 (2021).
22. Zhang, L. & Zhang, X. Multiple-image encryption algorithm based on bit planes and chaos. *Multimed. Tools Appl.* **79**, 20753–20771 (2020).
23. Hua, Z., Yi, S. & Zhou, Y. Medical image encryption using high-speed scrambling and pixel adaptive diffusion. *Signal Process.* **144**, 134–144 (2018).
24. Alghamdi, Y., Munir, A. & Ahmad, J. A lightweight image encryption algorithm based on chaotic map and random substitution. *Entropy* **24**, 1344 (2022).
25. Wu, W. & Wang, Q. Quantum image encryption based on baker map and 2d logistic map. *Int. J. Theor. Phys.* **61**, 64 (2022).
26. Xiang, H. & Liu, L. An improved digital logistic map and its application in image encryption. *Multimed. Tools Appl.* **79**, 30329–30355 (2020).
27. Zhu, C. & Sun, K. Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps. *IEEE Access* **6**, 18759–18770 (2018).
28. Benaissi, S., Chikouche, N. & Hamza, R. A novel image encryption algorithm based on hybrid chaotic maps using a key image. *Optik* **272**, 170316 (2023).
29. Shafique, A. & Shahid, J. Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps. *Eur. Phys. J. Plus* **133**, 331 (2018).

30. Zhu, S., Deng, X., Zhang, W. & Zhu, C. Secure image encryption scheme based on a new robust chaotic map and strong s-box. *Math. Comput. Simul.* **207**, 322–346 (2023).
31. Shafique, A. *et al.* Detecting the security level of various cryptosystems using machine learning models. *IEEE Access* **9**, 9383–9393 (2020).
32. Sun, X., Shao, Z., Shang, Y., Liang, M. & Yang, F. Multiple-image encryption based on cascaded gyrator transforms and high-dimensional chaotic system. *Multimed. Tools Appl.* **80**, 15825–15848 (2021).
33. Xie, Y., Yu, J., Guo, S., Ding, Q. & Wang, E. Image encryption scheme with compressed sensing based on new three-dimensional chaotic system. *Entropy* **21**, 819 (2019).
34. Liu, J., Tang, S., Lian, J., Ma, Y. & Zhang, X. A novel fourth order chaotic system and its algorithm for medical image encryption. *Multidimens. Syst. Signal Process.* **30**, 1637–1657 (2019).
35. Mehdi, S. A., Jabbar, K. K. & Abbood, F. H. Image encryption based on the novel 5D hyper-chaotic system via improved AES algorithm. *Int. J. Civil Eng. Technol.* **9**, 1841–1855 (2018).
36. Zhang, Q. & Han, J. A novel color image encryption algorithm based on image hashing, 6D hyperchaotic and DNA coding. *Multimed. Tools Appl.* **80**, 13841–13864 (2021).
37. Nematzadeh, H., Enayatifar, R., Yadollahi, M., Lee, M. & Jeong, G. Binary search tree image encryption with DNA. *Optik* **202**, 163505 (2020).
38. Yadollahi, M., Enayatifar, R., Nematzadeh, H., Lee, M. & Choi, J.-Y. A novel image security technique based on nucleic acid concepts. *J. Inf. Secur. Appl.* **53**, 102505 (2020).
39. Abbasi, A. A., Mazinani, M. & Hosseini, R. Evolutionary-based image encryption using biomolecules and non-coupled map lattice. *Optics Laser Technol.* **140**, 106974 (2021).
40. Mhammad, D., Aoun, M., Nadeem, M. A. & Younus, M. U. A novel encryption scheme for secure communication based on RNA. (2023).
41. Wang, X. & Liu, L. Application of chaotic Josephus scrambling and RNA computing in image encryption. *Multimed. Tools Appl.* **80**, 23337–23358 (2021).
42. Mansoor, S. *et al.* Adaptive color image encryption scheme based on multiple distinct chaotic maps and DNA computing. *Mathematics* **10**, 2004 (2022).
43. Wang, T., Ge, B., Xia, C. & Dai, G. Multi-image encryption algorithm based on cascaded modulation chaotic system and block-scrambling-diffusion. *Entropy* **24**, 1053 (2022).
44. Liu, L. & Wang, J. A cluster of 1D quadratic chaotic map and its applications in image encryption. *Math. Comput. Simul.* **204**, 89–114 (2023).
45. Shraida, G. *et al.* An efficient color-image encryption method using DNA sequence and chaos cipher. *Comput. Mater. Contin* **75**, 2641–2654 (2023).
46. Zhang, X., Liu, M. & Tian, J. Multiple-image encryption algorithm based on Sarrus rule and 3D Fibonacci matrix. *Phys. Scr.* **98**, 055208 (2023).
47. Biban, G., Chugh, R. & Panwar, A. Image encryption based on 8d hyperchaotic system using Fibonacci q-matrix. *Chaos Solitons Fract.* **170**, 113396 (2023).
48. Zhong, H. & Li, G. Multi-image encryption algorithm based on wavelet transform and 3D shuffling scrambling. *Multimed. Tools Appl.* **81**, 24757–24776 (2022).
49. Begum, M., Ferdush, J. & Uddin, M. S. A hybrid robust watermarking system based on discrete cosine transform, discrete wavelet transform, and singular value decomposition. *J. King Saud Univ.-Comput. Inf. Sci.* **34**, 5856–5867 (2022).
50. Balasamy, K. & Suganyadevi, S. A fuzzy based ROI selection for encryption and watermarking in medical image using DWT and SVD. *Multimed. Tools Appl.* **80**, 7167–7186 (2021).
51. Shamia, D., Balasamy, K. & Suganyadevi, S. A secure framework for medical image by integrating watermarking and encryption through fuzzy based ROI selection. *J. Intell. Fuzzy Syst.* **44**, 7449–7457 (2023).
52. Balasamy, K., Krishnaraj, N. & Vijayalakshmi, K. Improving the security of medical image through neuro-fuzzy based ROI selection for reliable transmission. *Multimed. Tools Appl.* **81**, 14321–14337 (2022).
53. Balasamy, K., Krishnaraj, N. & Vijayalakshmi, K. An adaptive neuro-fuzzy based region selection and authenticating medical image through watermarking for secure communication. *Wireless Pers. Commun.* **122**, 2817–2837 (2022).
54. Chai, X., Chen, Y. & Broyde, L. A novel chaos-based image encryption algorithm using DNA sequence operations. *Opt. Lasers Eng.* **88**, 197–213 (2017).
55. Ye, G.-D., Wu, H.-S., Huang, X.-L. & Tan, S.-Y. Asymmetric image encryption algorithm based on a new three-dimensional improved logistic chaotic map. *Chin. Phys. B* **32**, 030504 (2023).
56. Chen, J., Chen, L. & Zhou, Y. Cryptanalysis of a DNA-based image encryption scheme. *Inf. Sci.* **520**, 130–141 (2020).
57. Wen, H. & Lin, Y. Cryptanalyzing an image cipher using multiple chaos and DNA operations. *J. King Saud Univ.-Comput. Inf. Sci.* 101612 (2023).
58. Ganavi, M. & Prabhudeva, S. Two-layer security of images using elliptic curve cryptography with discrete wavelet transform. *Int. J. Comput. Netw. Inf. Secur.* **13**, 31 (2023).
59. Grassi, G., Severance, F. L. & Miller, D. A. Multi-wing hyperchaotic attractors from coupled Lorenz systems. *Chaos Solitons Fract.* **41**, 284–291 (2009).
60. Shafique, A. A new algorithm for the construction of substitution box by using chaotic map. *Eur. Phys. J. Plus* **135**, 194 (2020).
61. Shafique, A. *et al.* Chaos and cellular automata-based substitution box and its application in cryptography. *Mathematics* **11**, 2322 (2023).
62. Liu, H., Liu, J. & Ma, C. Constructing dynamic strong s-box using 3D chaotic map and application to image encryption. *Multimed. Tools Appl.* **82**, 23899–23914 (2023).
63. Si, Y., Liu, H. & Zhao, M. Constructing keyed strong s-box with higher nonlinearity based on 2D hyper chaotic map and algebraic operation. *Integration* **88**, 269–277 (2023).
64. Rehman, M. U., Shafique, A., Khan, K. H. & Hazzazi, M. M. Efficient and secure image encryption using key substitution process with discrete wavelet transform. *J. King Saud Univ.-Comput. Inf. Sci.* 101613 (2023).
65. Huang, X., Dong, Y., Ye, G. & Shi, Y. Meaningful image encryption algorithm based on compressive sensing and integer wavelet transform. *Front. Comp. Sci.* **17**, 173804 (2023).
66. Li, C. & Yang, X. An image encryption algorithm based on discrete fractional wavelet transform and quantum chaos. *Optik* **260**, 169042 (2022).
67. Kiran, Parameshachari, B. & Panduranga, H. Medical image encryption using scan technique and chaotic tent map system. In *Recent Advances in Artificial Intelligence and Data Engineering: Select Proceedings of AIDE 2020*, 181–193 (Springer, 2022).
68. Alexan, W., Alexan, N. & Gabr, M. Multiple-layer image encryption utilizing fractional-order chen hyperchaotic map and cryptographically secure prngs. *Fract. Fract.* **7**, 287 (2023).
69. Ahmad, J. & Ahmed, F. Efficiency analysis and security evaluation of image encryption schemes. *Computing* **23**, 25 (2010).
70. Singh, A., Agarwal, P. & Chand, M. Image encryption and analysis using dynamic aes. In *2019 5th international conference on optimization and applications (ICOA)*, 1–6 (IEEE, 2019).
71. Khan, J. S. & Kayhan, S. K. Chaos and compressive sensing based novel image encryption scheme. *J. Inf. Secur. Appl.* **58**, 102711 (2021).

72. Singh, K. N., Singh, O., Singh, A. K. & Agrawal, A. K. EiMOL: A secure medical image encryption algorithm based on optimization and the Lorenz system. *ACM Trans. Multimed. Comput. Commun. Appl.* **19**, 1–19 (2023).

Acknowledgements

Author contributions

M.M.H. formal analysis and project administration, M.U.R. Conceptualization, editing and supervision, A.S. methodology, software, and writing, A.A. validation Z.B. review, A.B.U. visualisation. All authors reviewed the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to M.U.R.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.