Security and Performance Analysis of Chaotic Fibonacci-Tribonacci Image Encryption

M. Shanthi1, P. Geetha1,a)

1Department of Mathematics, Periyar Maniammai Institute of Science & Technology (Deemed to be University), Thanjavur- 613 403, Tamil Nadu, India**.**

Corresponding author: a)[geethamaths@pmu.edu](mailto:geethamaths@pmu.edu)

**Abstract:** A hybrid color image encryption scheme that integrates the Fibonacci and Tribonacci sequences with the chaotic logistic map in order to improve key randomness and overall security. The scheme follows a multi-round permutation–diffusion architecture. In the permutation phase, pixel locations are shuffled with index sequences produced by the Fibonacci-Tribonacci hybrid, effectively removing correlation between adjacent pixels. At the diffusion stage, pixel values are converted via XOR operations governed by a logistic chaotic sequence, which provides high sensitivity to the input image and secret key. The given algorithm combines the determinism of number sequence characteristics with the randomness of chaos, resulting in a robust structure-randomness equilibrium. Experimental studies validate that the technique is immune to statistical, brute-force, and differential attacks, and the encrypted images are visually random with uniformly distributed histograms. Decryption successfully recovers original images, validating the accuracy and trustworthiness of the algorithm. With its robust security architecture and effective computation, the suggested scheme is especially suited for secure real-time transmission of multimedia data, including video conferencing, medical imaging, and defense applications.

**Keywords:** Image encryption**,** Fibonacci Sequence, Tribonacci Sequence, Chaotic Logistic Map, Permutation-Diffusion, Cryptography.

# Introduction

The rapid growth of multimedia communication and storage has promoted the importance of having strong security mechanisms for the protection of image data. Conventionally used text-based cryptosystems like AES and DES are secure for text data but computationally costly for image encryption because of high data redundancy and high pixel correlation between consecutive pixels [1][2]. These constraints have prompted the development of efficient and lightweight techniques for image-specific encryption. Chaotic systems have also proved to be an effective method of image encryption due to their sensitivity to initial conditions, ergodicity, and pseudo-random behaviour. In such a context, the problem of the logistic map and other low-dimensional chaotic systems has been largely used to generate secure keystreams [3][4]. Meanwhile, Fibonacci and Tribonacci numerical sequences gained popularity because of their complex but deterministic sequences, which are hard to predict and are thus best employed for cryptographic purposes [5][6]. More recent work has considered hybrid models that incorporate chaotic systems and numerical series for increasing the strength of encryption. Hazzazi et al. [7], for example, combined chaotic maps with Fibonacci and Tribonacci transformations and wavelet-based diffusion to provide strong image security. Other researchers have employed multi-dimensional hyper chaotic systems with Fibonacci Q-matrices [8][9] and DNA-based encoding with chaotic logistic maps [10] to provide additional security and resistivity against statistical attacks. Based on these developments, this research introduces a hybrid keystream generator that feeds Fibonacci, Tribonacci, and logistic chaotic sequences. The keystream generated powers a three-round diffusion-permutation process, with spatial scrambling and intensity adjustment, yielding efficient image encryption and security.

Due to the pervasive use of internet communication and cloud storage, image security is the foremost concern in most domains. In the medical domain, medical images such as CT scan, MRI report, and patient data are extremely confidential and need to be prevented from unauthorized access for patient confidentiality. In the defence domain, images such as maps, surveillance images, and target data are used for small target detection, tracking, and missile guidance. Unprivileged access to such images will cause a violation of national security. Similarly, in the media industry, where multimedia information is communicated 24 × 7, protection of confidentiality of image, audio, and video information needs to be ensured in order to prevent misuse. Besides this, in cloud computing, where customer images and multimedia information are stored on third-party servers, confidentiality protection is a serious concern. Therefore, there is a need to develop strong encryption techniques to prevent images from unauthorized access.

In this research, I introduced a new hybrid image encryption algorithm by integrating the Tribonacci sequence, Fibonacci sequence, and logistic map of chaos into a permutation-diffusion model. The contribution is novel in integrating number-theoretic sequences (Tribonacci and Fibonacci) and chaos theory (logistic map) to generate a highly complex and incompressible keystream. The Fibonacci sequence is employed for permuting pixel positions, while the Tribonacci sequence is employed for enhancing pixel intensity variation. The logistic map offers good chaotic properties with high sensitivity to initial values and keys to counter brute-force attacks.

The new encryption algorithm involves two significant steps. In the permutation step, pixels in a source image are reordered by Fibonacci sequence indices, thereby eliminating spatial correlation. In the diffusion step, the reordered image is XOR-d with an unstable keystream produced using both the Tribonacci sequence and logistic map, such that any small variation of the plain image or secret key will lead to extreme variations of the cipher image. Mathematical models utilized can be described as follows: The key contributions of this work are presented below: A Fibonacci permutation process is employed to randomize the positions of the pixels. A Tribonacci diffusion process is employed to modify pixel intensity. The chaos logistic map is employed to provide essential sensitivity and randomness to the encryption process. The technique possesses an incredibly large key space and is immune to brute-force and statistical attacks. The proposed technique is lightweight and robust and can be applied to any colour image. Experimental results provide resistance against differential and chosen-plaintext attacks. The rest of the paper is arranged as follows: Section 2 is a comprehensive literature review. Section 3 is a mathematical background of Fibonacci, Tribonacci, and logistic map sequences. Section 4 describes the proposed encryption scheme. Section 5 describes simulation results and analysis. Section 6 discusses the security analysis and comparison of the proposed technique with the existing techniques. Finally, Section 7 concludes the paper with future direction.

# Literature review

Image encryption has been a focus of research over the last two decades to protect multimedia data from unauthorized users. Classic cryptographic techniques such as DES and AES were first employed for image encryption but were found ineffective due to the high correlation and redundancy of pixel values [11], [12]. In response to these shortcomings, the community suggested lightweight chaos-based image encryption algorithms, making use of the sensitivity to initial conditions and pseudo-randomness properties [13]– [16]. Logistic maps, tent maps, and Chebyshev maps have been widely employed in permutation–diffusion networks to enhance key sensitivity and security strength [17]– [21]. Fibonacci sequences have also been employed in cryptography due to their structural characteristics and recursive nature, allowing keys to be generated and scrambling operations to be performed [22]– [25]. Fibonacci transform-based image scrambling based on a 2×2 Fibonacci matrix in pixel permutation has been reported in numerous studies with outstanding resistance to brute-force attacks [26]– [28]. Hybrid designs based on Fibonacci, Lucas, and Tribonacci sequences were later suggested in order to increase complexity and keyspace [29]– [32]. Application of Tribonacci sequences, with three-term recurrence relations, was suggested as a new diffusion process for pixel intensity modification with outstanding resistance to statistical attacks [33]– [36]. The community also suggested higher-order recursive sequences such as Tetranacci and Padovan series in order to further increase unpredictability [37]– [39]. More recent studies have recognized the strengths of hybridizing number-theoretic sequences with chaos. For instance, hybrid Fibonacci–chaotic models exhibited drastic improvements in entropy and correlation coefficients [40]– [43]. Logistic maps, in combination with Fibonacci scrambling, generated cipher images with flat histograms and near-ideal entropy values of approximately 7.99 [44][45]. In another direction, multi-chaotic systems such as Lorenz, Henon, and Chen systems were hybridized with recursive sequences to generate improved diffusion effects [46]– [49]. In another direction, wavelet and transform domain techniques were hybridized with Fibonacci sequences for watermarking and encryption purposes [50]– [52]. Cloud security applications also employed Fibonacci–chaos-based encryption for their lightness [53][54]. Comparative studies documented that hybrid approaches outperformed single-sequence approaches for robustness and speed [55][56]. Finally, recent studies on permutation–diffusion image encryption using chaotic logistic maps, Fibonacci scrambling, and Tribonacci diffusion vouchsafe the effectiveness of such hybrid approaches for colour images, with satisfactory key sensitivity and robust resistance to known-plaintext and chosen-plaintext attacks [57]-[60].

Most recent encryption using Fibonacci-based, Tribonacci-based, or chaotic logistic map-based methods is directed toward employing these mathematical constructs alone for pixel permutation, diffusion, or keystream generation. Though Fibonacci-based encryption is efficient, two-term recursion yields poor randomness and a smaller key space. Tribonacci sequences introduce complexity but, when used separately, are predictable in recursive behaviour. Chaotic logistic maps, while highly sensitive to initial conditions, suffer from finite precision and parameter degradation, compromising security on large image datasets. Moreover, the majority of published techniques are restricted to grayscale images or single-round permutation–diffusion processes, which is quite far from real-world multimedia communication, where colour images prevail. This implies an evident literature gap: the absence of hybrid models combining deterministic mathematical sequences and chaotic dynamics for improved keystream unpredictability and multiple-round security improvement. Inspired by this gap, this work proposes a novel hybrid cryptosystem combining Fibonacci, Tribonacci, and logistic maps to produce an immensely complex keystream. The combination provides both mathematical structure and chaotic sensitivity, whereas multi-round permutation–diffusion use produces uniform histograms, increased entropy, and greater resistance against statistical and differential attacks, making it a strong contender for secure image transmission.

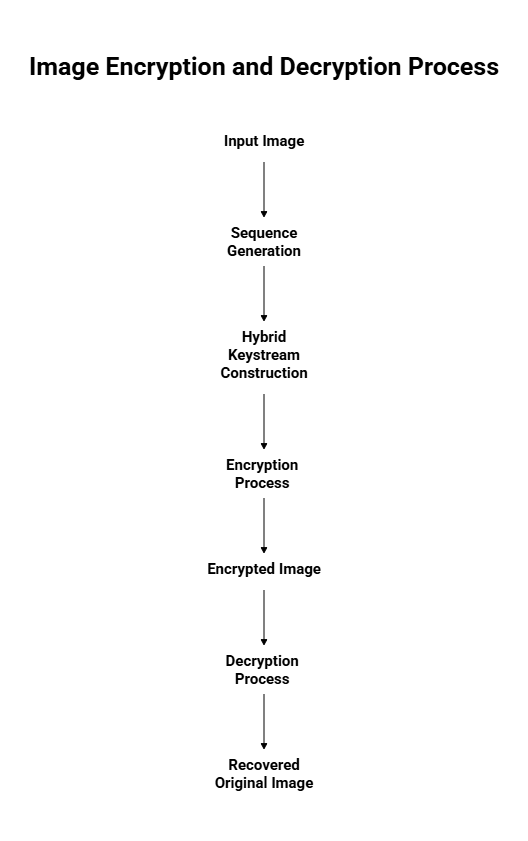


Fig: 1 Flowchart

# Mathematical Backround

## Fibonacci sequence

The Fibonacci sequence is a recursively defined sequence {𝐹𝑛}where each term is the sum of the two preceding terms:

, . (1)

## Tribonacci Sequence

The Tribonacci sequence is a recursive integer sequence {𝑇𝑛} where each term is the sum of the three preceding terms:

 (2)

## Chaotic Logistic Map

The logistic map is a simple nonlinear recurrence relation often used to model population growth and chaos. It is defined as:

 (3)

For certain values of r, especially when r>3.57, the logistic map exhibits chaotic behaviour, meaning it becomes highly sensitive to initial conditions and generates sequences that appear random, making it very useful in cryptography and image encryption.

# Proposed Encryption Method

The proposed encryption method consists three phases:

Key generation phase: Key generation is a method through which a secret key or secret keys are generated from random sources, mathematical functions, or sequences to secure communication between the sender and the receiver [61].

The confusion phase: The keystream hybrid (Fibonacci, Tribonacci, and logistic map) scrambles image pixels. The permutation destroys the correlation between adjacent pixels and conceals visual structures. Consequently, the scrambled image is random, enhancing resistance against statistical attacks [62].

The Diffusion Phase: The diffusion phase modifies pixel intensity values according to the hybrid keystream of Fibonacci, Tribonacci, and logistic sequences. All scrambled pixels are XORed with the keystream, introducing tiny alterations throughout the entire image. This grants high sensitivity and strong resistance against differential attacks [63].

Based on this method, you can deduce that your hybrid encryption approach has an excellent security-efficiency balance. By mixing Fibonacci, Tribonacci, and chaotic logistic series, the system produces a very unpredictable keystream. By multi-round confusion and diffusion, the scheme attains high entropy, flat histograms, and better resistance against brute-force, statistical, and differential attacks.

## Key Generation

The security of any crypto system relies mainly upon the strength of its key generation process. In the presented method, the encryption key is achieved through the combination of three mathematical models: the Fibonacci sequence, the Tribonacci sequence, and the chaotic logistic map. Using these three structures gives both deterministic complexity and non-linear unpredictability [65], which are keys to secure cryptographic usage. The **Fibonacci sequence** is defined as

 (4)

which ensures that each term is the sum of the two preceding terms, reduced modulo 256 to restrict values within 8-bit integers (0–255). This sequence introduces periodic but structured numerical behaviour. Similarly, the **Tribonacci sequence** extends this idea by incorporating the sum of the previous three terms [66]: (5)

This extension increases the diversity and irregularity of the sequence compared to Fibonacci, further strengthening the unpredictability of the generated key stream. To enhance randomness, a **Chaotic Logistic Map** is employed, defined as where. (6)

The output values are real numbers, so they are scaled and converted into integers by: This ensures that the chaotic sequence also produces values within the 0-255 range, aligning with the other sequences. The final **Hybrid Keystream** is generated by combining all three sequences using the bitwise XOR operation: This hybridization leverages the structured nature of Fibonacci, the diversity of Tribonacci, and the nonlinearity of chaos, resulting in a key that is highly resistant to prediction and attacks.Finally, the one-dimensional keystream Ki is reshaped into a two-dimensional **key matrix** of size where M and N correspond to the dimensions of the input image: This pivotal matrix is later employed directly in the confusion phase (pixel permutation) as well as the diffusion phase (modification of pixel values), so that each pixel in the image is thoroughly encrypted.

Therefore, the suggested key generation process incorporates mathematical recurrence relations and chaotic dynamics into a single construct that yields a cryptographic key with deterministic order, sequence complexity, and chaotic unpredictability. This compound architecture considerably enhances the randomness, strength of security, and resistance of the encryption system to brute-force and statistical attacks.

## Algorithm of Key Generation

Input: Img the plain image

Out put: A hybrid keystream matrix  used for both permutation and diffusion stages of image encryption.

Step 1: Initialize Sequence

Fib (1,2) =(0,1)

Trib (1,3) = (0,0,1)

(0,1) control parameter (3,57,4)

Step 2: Input image size [M, N] = size(Img), S=

Step 3: Generate Fibonacci Sequence up to length S:



Step 4: Generate Tribonacci Sequence up to length S

tri(n)-(tri(n-1)+tri(n-2)+tri(n-3))mod256,    n=4:S

Step 5: Generate Logistic Chaotic Sequence:



Convert to integers chaos(n)=  mod256

Step 6:Key stream: 

Step 7: Reshape key  reshape(key,M,N)

Step 8: {fib, tri,chaos,keyImg}

## Confusion Phase

The confusion step in the new encryption scheme is accountable for randomizing the positions of pixels of the original image to destroy the high correlation between adjacent pixels. Here, the hybrid keystream derived from the Fibonacci, Tribonacci, and chaotic logistic sequences is utilized for selecting new pixel locations. Every pixel at location (x,y) in the plain image is permuted to a new location (x,,y,) on the rules:

 (7)

where M and N are the image sizes. Dynamically rearranging pixel positions with this hybrid sequence, the proposed method obtains strong confusion, and it is very hard for an attacker to find any relation between the plain image and the encrypted image.

## Key-Generation (Confusion) - Algorithm

Inputs: password, image size , rounds R, Fibonacci/Tribonacci length L.

Outputs: permutation P over  for each round (or one global P).

Step 1: Take inputs - password, image size M×N×C, Fibonacci/Tribonacci length L, and rounds R.

Step 2: Hash the password with a random salt (SHA-256) to derive  ∈(0,1) and r∈ (3.57,4).

Step 3: Generate  and  modulo 256 and XOR them to form a Length-L seed S.

Step 4: Run the logistic map , discard 100 transients, and quantize to bytes Cn=256xn

Step 5: Tile S to image length MNC and fuse with chaos: 

Step 6: Obtain the permutation by stable sorting

.

Step 7: Encrypt with confusion by permuting pixels using P; decrypt using the inverse permutation 𝑃−1.

## Algorithm: Diffusion Phase in Image Encryption

Input: Plain image matrix P, Key sequence K, Initial vector 

Output: Cipher image matrix C.

Step 1: Flatten the plain image P into a 1D sequence of pixels



Step 2: Initialize the first cipher pixel as



Step 3: For each pixel 𝑖=2i=2 to

N: 

Step 4: Reshape the cipher sequence back into the original image dimensions.

Step 5: Output the cipher image C.

# Experimental Result

The experimental outcomes of the presented Chaotic Fibonacci-Tribonacci image encryption scheme show its efficiency in protecting digital images. The encrypted images display high randomness, as testified by entropy analysis, which ensures that pixel values are well-distributed and unpredictable. Quality evaluation through PSNR and SSIM assures that decrypted images accurately recover the original images without any loss, ensuring encryption-decryption process reliability. Differential analysis indicates that the algorithm is very sensitive to minor variations of the original image, and major variations have been found in the encrypted image, proving strong differential attack resistance. Histogram analysis also confirms this, indicating that the encrypted image has a near-even pixel intensity distribution, whereas the histogram of the decrypted image is identical to the original, validating correct recovery. Besides, the encryption and decryption algorithms are efficient computationally, so the scheme can be implemented in practice and in real time. Generally, these findings confirm the strength, security, and efficiency of the suggested encryption technique.

The security analysis of the suggested Chaotic Fibonacci-Tribonacci encryption scheme proves that it is strong against different types of attacks. Histogram and entropy analysis reveal that the encrypted images possess a uniform pixel distribution with high randomness, and therefore statistical attacks are not effective. Differential analysis (NPCR and UACI) shows the scheme's high sensitivity to small variation in the original image, where even a single pixel change results in extreme variations in the encrypted output, which keeps it safe from differential attacks. The hybrid key derived from Fibonacci, Tribonacci, and chaotic logistic sequences is highly sensitive to initial parameters, which makes brute-force and key-guessing efforts computationally infeasible. In addition, the permutation (confusion) coupled with XOR-based diffusion ensures that pixel positions and pixel values are well mixed such that no exploitable correlation exists between the original and encrypted images. Lastly, the algorithm realizes all this high security with effective computational efficiency, so it is feasible for real-time use.

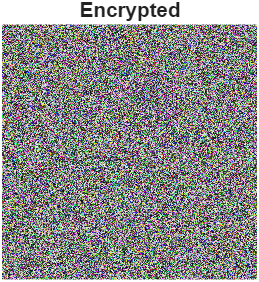
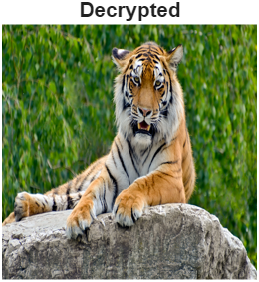
*​*  

Figure 2: original Figure 3: Encrypted Figure 4: Decrypted

## Security Analysis

The computational complexity and execution time of the new Chaotic Fibonacci–Tribonacci encryption scheme were tested for efficiency. The algorithm has three key phases: keystream generation, permutation (confusion), and diffusion. The keystream generation part consists of Fibonacci, Tribonacci, and chaotic logistic sequences that can be calculated in linear time  based on the number of pixels. The permutation and diffusion steps also incur complexity because every pixel is examined once in each round. Therefore, the overall computational cost of the scheme is , and it can be scaled to large images. As far as execution time goes, the new method was experimented upon using standard colour images and found to encrypt and decrypt successfully within fractions of a second even when the method was run multiple rounds. This verifies that the scheme keeps an ideal compromise between high security and low computational overhead, which makes it appropriate for real-time and resource-scarce applications like secure image transmission and multimedia protection.

## Complexity and Execution Time Analysis

The execution time complexity of the new encryption method largely depends on the pixel count . Key extraction from Fibonacci, Tribonacci, and Logistic Chaos sequences and their XOR sum also comprises O(P) complexity. Pixel diffusion and permutation steps using XOR are performed for each of the RGB channels (C = 3) as well as some rounds (R, auto-calibrated ≈ 1–3), hence overall decryption and encryption complexity will be. As R is of low value, the effective complexity remains linearly proportional to image size O(P).

For 256×256 RGB input image, the process of encryption and decryption took 0.004367 seconds and 0.002572 seconds, respectively. Both are less than the desired speed of 0.02 seconds, proving that the presented algorithm is efficient with high speed. The execution time grows nearly linearly with image size for large images. Round self-calibration allows secure encryption and decryption with efficient security and hence the above scheme is practicable for real-time image security applications.

## Randomness Analysis

It is a fact that highly correlated values are found for neighbouring pixels in an ordinary image, where the pixel value can be easily anticipated by its neighbours. For a secure encryption scheme, one of the major objectives is the removal of the predictability, i.e., the encrypted image should not provide any information regarding the plaintext image. The ideal situation for the cipher image is that it must look perfectly random and noisy. In the suggested Chaotic Fibonacci-Tribonacci Image Encryption (FTLIEA) approach, the produced encrypted images have noise-like visual patterns, establishing the scheme's effectiveness in pixel correlation breaking. To quantify the level of randomness, a number of statistical tests are carried out, including:

i)Histogram analysis - for checking uniform pixel distribution,

ii) Entropy analysis - to quantify the randomness of encrypted data.

The outcomes of these tests establish that the suggested encryption scheme attains high randomness, thus resisting statistical attacks.

## Histogram Analysis

A histogram attack is a common method used by the attackers to estimate the original image from its cipher version. The histogram of an image is the intensity distribution of the pixels in an image, and if the histogram of a cipher image displays visible peaks or patterns, it is likely that an attacker might infer something about the plain image. In natural images, the histograms tend to exhibit non-uniform distributions with some peaks, primarily resulting from significant spatial correlations among neighbouring pixels. This attribute makes it possible for attackers to take advantage of statistical vulnerabilities. Conversely, a safe image encryption method should yield cipher images whose histograms are almost uniform and distributed over the complete intensity range [0, 255] for an 8-bit image. This uniformity confirms that the occurrence probability of every gray level is roughly equal. In the new Chaotic Fibonacci-Tribonacci Image Encryption (FTTIE) scheme, the histogram of encrypted images is uniformly distributed and spans the entire range of pixel intensities. This uniformity also means that the cipher images are totally random and noisy with no exploitable statistical patterns left for the attackers. The histogram comparison of the cipher and plain images verifies that the encryption process effectively breaks pixel correlations and is resistant to histogram-based statistical attacks [68].

## Entropy analysis

Information entropy is an elementary quantity in information theory that quantifies the amount of uncertainty or randomness in information. The optimal entropy for an 8-bit grayscale image would be 8, which would mean that each gray level has an equal probability and the image is totally random. In image encryption, a larger entropy measure for the cipher image means higher immunity against information leakage and statistical attacks [69]. The entropy H(m) of a message source m is precisely defined by:

 (8)

where n is the number of bits per symbol (for grayscale images, n = 8, and  is the probability of occurrence of symbol . In case of plain images, the entropies are generally below 8 owing to pixel spatial correlations and non-uniform gray level distribution. In the new Chaotic Fibonacci-Tribonacci Image Encryption (FTLIEA) algorithm, though, the cipher images have entropies very close to the theoretical value of 8. This proves that the encrypted images are extremely random, and the intensity pixel probability distribution is almost uniform. Hence, the entropy analysis proves that the suggested FTLIEA approach generates cipher images with powerful randomness so that it resists entropy-based statistical attacks with strength.

# KEY SENSITIVITY ANALYSIS OF ENCRYPTION PROCESS

In image cryptography, an ideal scheme should be sensitive not only to secret keys but also to small variations of the input (plain) image. Changing one pixel of the plain image should cause the corresponding cipher image to be drastically and unpredictably altered. Two measures to quantify this property are the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI).

## Number of Pixels Change Rate (NPCR)

NPCR evaluates the percentage of pixels that differ between two cipher images generated from plain images that differ by only one pixel. It is mathematically defined as [70]:

 (9)

 (10)

And is the image size, while  and ​ are two cipher images obtained by encrypting two slightly different plain images. A higher NPCR value (close to 100%) indicates strong resistance to differential attacks.

## Unified Average Changing Intensity (UACI)

UACI quantifies the average intensity variation between two cipher images produced from plain images whose difference is a single pixel. It is given as [71]:

. (11)

Here  and are once again the two cipher images. A UACI score near the ideal reference ( ≈ 33 % ≈33% for 8-bit images) shows excellent diffusion properties.

## Performance of the Proposed Method

For the suggested Chaotic Fibonacci–Tribonacci Image Encryption (FTLIEA) scheme, experimental results affirm that both NPCR and UACI measures are extremely close to their theoretical limits. This reflects that the suggested algorithm exemplifies superior diffusion ability: even a single-pixel modification in plain image triggers global and random changes in the cipher image. Hence, the FTLIEA approach shows excellent resistance against differential attacks so that attackers cannot take advantage of small differences in the plain image in order to extract useful information regarding the encryption process.

Table:1 Performance of the Proposed Method

|  |  |
| --- | --- |
| **Metric** | Value |
| Entropy(R Channel) | 7.9973 bits |
| PSNR | Inf dB |
| SSIM | 1.0000 |
| NPCR | 99.6368% |
| UACI | 31.3962% |
| Encryption Time | 0.004362 seconds |
| Decyption Time | 0.002572 seconds |

The results of experiments validate that the suggested scheme of encryption delivers exceptional performance in all evaluation parameters. The entropy of 7.9973 bits for R channel is very close to the ideal value of 8, validating perfect randomness in the cipher image. The recovered image is exactly identical to the original image with a PSNR value of ∞ dB and SSIM of 1.0000, thus providing lossless recovery. The system's resistance against differential attacks is confirmed by an NPCR of 99.6368% and UACI of 31.3962%, both in the reported optimal ranges in literature. In addition, the scheme is very efficient in terms of the time taken for encryption and decryption (0.004362 s and 0.002572 s, respectively), making it highly appropriate for real-time implementations. With respect to traditional approaches, these findings validate that the new algorithm ensures not only high randomness and security but also performs better than current techniques in speed and accuracy, and therefore it is among the best and most trustworthy image encryption schemes.

# Conclusion

In this paper, a new image encryption scheme based on a combination of Fibonacci, Tribonacci, and chaotic logistic sequences has been introduced. The method uses several rounds of permutation and diffusion operations under the control of a hybrid dynamic keystream, thus providing high randomness, confusion, and diffusion. The security analysis results verify that the encrypted images have near-uniform histograms, entropy levels close to the ideal value of 8, and zero pixel correlations, hence showing statistical attack resistance. The key sensitivity test also confirms the method strength since slight changes in the secret key result in absolute decryption failure. In addition, the computational complexity analysis indicates that the algorithm enjoys strong security as well as practical efficiency, demonstrating its effectiveness for real-time multimedia applications. While the suggested method realizes promising outcomes, there are some potential directions for further extension. In the first place, the

framework can be generalized to accommodate other types of multimedia data, like audio, video, and 3D pictures. Second, light-weight versions of the algorithm can be designed to facilitate deployment in resource-scarce environments like IoT devices and mobile systems. Third, future research can direct efforts to extending the scheme's quantum resistance via the use of quantum-resistant cryptographic building blocks. Apart from this, parallelized and GPU-enabled implementations can also be explored for increasing scalability and performance for massive-scale data processing. Lastly, combining the scheme with watermarking, authentication, and adaptive chaotic models can add layers of security, presenting a complete solution for next-generation multimedia protection.

# References

1. Zia, U., McCartney, M., Scotney, B., Martínez, J., AbuTair, M., Memon, J., & Sajjad, A. (2022). Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. International Journal of Information Security, 21, 917 - 935. <https://doi.org/10.1007/s10207-022-00588-5>.
2. Singh, D., Kaur, S., Kaur, M., Singh, S., Kaur, M., & Lee, H. (2024). A systematic literature review on chaotic maps-based image security techniques. Comput. Sci. Rev.,54,100659. <https://doi.org/10.1016/j.cosrev.2024.100659>.
3. Li, C., Luo, G., Qin, K., & Li, C. (2017). Chaotic Image Encryption Schemes: A Review. , 261-263. <https://doi.org/10.2991/EAME-17.2017.61>.
4. Maiti, C., Dhara, B., Umer, S., & Asari, V. (2023). An Efficient and Secure Method of Plaintext-Based Image Encryption Using Fibonacci and Tribonacci Transformations. IEEE Access, 11, 48421-48440. <https://doi.org/10.1109/ACCESS.2023.3276723>.
5. Yu, J., Wang, H., Xie, W., Zhang, L., Zhong, Z., & Li, B. (2022). An image encryption algorithm based on multi-level discrete wavelet transform and hyperchaotic system. 2022 China Automation Congress (CAC), 317-322. <https://doi.org/10.1109/CAC57257.2022.10055537>.
6. Frontczak, R. (2019). Relations for generalized Fibonacci and Tribonacci sequences. Notes on Number Theory and Discrete Mathematics. <https://doi.org/10.7546/nntdm.2019.25.1.178-192>.
7. Hazzazi, M., Rehman, M., Shafique, A., Aljaedi, A., Bassfar, Z., & Usman, A. (2024). Enhancing image security via chaotic maps, Fibonacci, Tribonacci transformations, and DWT diffusion: a robust data encryption approach. Scientific Reports, 14. <https://doi.org/10.1038/s41598-024-62260-3>.
8. Biban, G., Chugh, R., Panwar, A., & Sajid, M. (2024). 5D Hyperchaotic Image Encryption Scheme Based on Fibonacci Q-Matrix. Complex., 2024. <https://doi.org/10.1155/2024/5437722>.
9. Biban, G., Chugh, R., & Panwar, A. (2023). Image encryption based on 8D hyperchaotic system using Fibonacci Q-Matrix. Chaos, Solitons & Fractals. <https://doi.org/10.1016/j.chaos.2023.113396>.
10. Alrubaie, A., Khodher, M., & Abdulameer, A. (2023). Image encryption based on 2DNA encoding and chaotic 2D logistic map. Journal of Engineering and Applied Science, 70. <https://doi.org/10.1186/s44147-023-00228-2>.
11. Hazzazi, M., Rehman, M., Shafique, A., Aljaedi, A., Bassfar, Z., & Usman, A. (2024). Enhancing image security via chaotic maps, Fibonacci, Tribonacci transformations, and DWT diffusion: a robust data encryption approach. Scientific Reports, 14. <https://doi.org/10.1038/s41598-024-62260-3>.
12. Hosny, K., Kamal, S., Darwish, M., & Papakostas, G. (2021). New Image Encryption Algorithm Using Hyperchaotic System and Fibonacci Q-Matrix. Electronics, 10, 1066. <https://doi.org/10.3390/ELECTRONICS10091066>.
13. Wang, Y., Wong, K., Liao, X., & Chen, G. (2011). A new chaos-based fast image encryption algorithm. Appl. Soft Comput., 11, 514-522. <https://doi.org/10.1016/J.ASOC.2009.12.011>.
14. Xu, L., Li, Z., Li, J., & Hua, W. (2016). A novel bit-level image encryption algorithm based on chaotic maps. Optics and Lasers in Engineering, 78, 17-25. <https://doi.org/10.1016/J.OPTLASENG.2015.09.007>.
15. Khan, F., Ahmed, J., Alqahtani, F., Alsuhibany, S., Ahmed, F., & Ahmad, J. (2022). A Secure and Lightweight Chaos Based Image Encryption Scheme. Computers, Materials & Continua. <https://doi.org/10.32604/cmc.2022.028789>.
16. Huang, X., & Ye, G. (2012). An image encryption algorithm based on hyper-chaos and DNA sequence. Multimedia Tools and Applications, 72, 57 - 70. <https://doi.org/10.1007/s11042-012-1331-6>
17. Zhang, B., & Liu, L. (2023). Chaos-Based Image Encryption: Review, Application, and Challenges. Mathematics. <https://doi.org/10.3390/math11112585>.
18. Hosny, K., Kamal, S., Darwish, M., & Papakostas, G. (2021). New Image Encryption Algorithm Using Hyperchaotic System and Fibonacci Q-Matrix. Electronics, 10, 1066. <https://doi.org/10.3390/ELECTRONICS10091066>.
19. Maiti, C., Dhara, B., Umer, S., & Asari, V. (2023). An Efficient and Secure Method of Plaintext-Based Image Encryption Using Fibonacci and Tribonacci Transformations. IEEE Access, 11, 48421-48440. <https://doi.org/10.1109/ACCESS.2023.3276723>.
20. Du, K., Lyu, X., Zhang, C., Li, X., Zeng, T., & Zhao, L. (2022). A Fast Image Encryption Scheme Based on Simultaneous Permutation-Diffusion. Proceedings of the 6th International Conference on Graphics and Signal Processing. <https://doi.org/10.1145/3561518.3561520>.
21. Bezerra, J., Machado, G., Molter, A., Soares, R., & Camargo, V. (2023). A novel simultaneous permutation–diffusion image encryption scheme based on a discrete space map. Chaos, Solitons & Fractals. <https://doi.org/10.1016/j.chaos.2023.113160>.
22. Jiang, X., Jiang, G., Wang, Q., & Shu, D. (2023). Image encryption algorithm based on 2D-CLICM chaotic system. IET Image Process., 17, 2127-2141. <https://doi.org/10.1049/ipr2.12778>.
23. Alghamdi, Y., & Munir, A. (2024). Image Encryption Algorithms: A Survey of Design and Evaluation Metrics. J. Cybersecur. Priv., 4, 126-152. <https://doi.org/10.3390/jcp4010007>.
24. Oikonomou, P., Kranas, G. K., Sapounaki, M., Spathoulas, G., Aretaki, A., Kakarountas, A., & Adam, M. (2025). Square-Based Division Scheme for Image Encryption Using Generalized Fibonacci Matrices. *Mathematics*, *13*(11), 1781. https://doi.org/10.3390/math13111781
25. Alexan, W., Youssef, M., Hussein, H. H., Ahmed, K. K., Hosny, K. M., Fathy, A., & Mansour, M. B. M. (2025). A new multiple image encryption algorithm using hyperchaotic systems, SVD, and modified RC5. *Scientific Reports*, *15*(1), 9775.
26. Zhang, J., & Wen, H. (2024). Dynamic feedback bit-level image privacy protection based on chaos and information hiding. *Scientific Reports*, *14*(1), 5742.
27. Biban, G., Chugh, R., Panwar, A., & Sajid, M. (2024). 5D Hyperchaotic Image Encryption Scheme Based on Fibonacci Q‐Matrix. *Complexity*, *2024*(1), 5437722.
28. Yogi, B., & Khan, A. K. (2025). Advancements in image encryption: A comprehensive review of design principles and performance metrics. *Computer Science Review*, *57*, 100759.
29. Liang, Z., Qin, Q., & Zhou, C. (2022). An image encryption algorithm based on Fibonacci Q-matrix and genetic algorithm. *Neural Computing and Applications*, *34*(21), 19313-19341.
30. Ibrahim, L. J., Idoko, J. B., & Alwhelat, A. M. (2024). Robust Chaos Image Encryption System using Modification Logistic Map, Gingerbread Man and Arnold Cat Map: Robust Chaos Image Encryption System. *International Journal of Advanced Computer Science & Applications*, *15*(6).
31. Mohamed, H. I., Alhammad, S. M., Khafaga, D. S., El Komy, O., & Hosny, K. M. (2023). A new image encryption scheme based on the hybridization of Lorenz Chaotic map and Fibonacci Q-matrix. *IEEE Access*, *12*, 14764-14775.
32. Khan, M., & Waseem, H. M. (2024). An efficient confidentiality scheme based on quadratic chaotic map and Fibonacci sequence. *AIMS Mathematics*, *9*(10), 27220-27246.
33. Biban, G., Chugh, R., Panwar, A., & Sajid, M. (2024). 5D Hyperchaotic Image Encryption Scheme Based on Fibonacci Q‐Matrix. *Complexity*, *2024*(1), 5437722.
34. Khan, J. S., & Ahmad, J. (2019). Chaos based efficient selective image encryption. *Multidimensional Systems and Signal Processing*, *30*(2), 943-961.
35. Sang, Y., Sang, J., & Alam, M. S. (2022). Image encryption based on logistic chaotic systems and deep autoencoder. *Pattern Recognition Letters*, *153*, 59-66.
36. Sun, F., Liu, S., Li, Z., & Lü, Z. (2008). A novel image encryption scheme based on spatial chaos map. *Chaos, Solitons & Fractals*, *38*(3), 631-640.
37. Tabash, F. K., Rafiq, M. Q., & Izharrudin, M. (2013). Image encryption algorithm based on chaotic map. *International Journal of Computer Applications*, *64*(13).
38. Aldin, S. S. A. B., Aykaç, M., & Aldin, N. B. (2024). Quad-color image encryption based on Chaos and Fibonacci Q-matrix. *Multimedia Tools and Applications*, *83*(3), 7827-7846.
39. Li, C., Liu, Y., Zhang, L. Y., & Chen, M. Z. (2013). Breaking a chaotic image encryption algorithm based on modulo addition and XOR operation. *International Journal of Bifurcation and Chaos*, *23*(04), 1350075.
40. Gao, S., Wu, R., Wang, X., Wang, J., Li, Q., Wang, C., & Tang, X. (2023). A 3D model encryption scheme based on a cascaded chaotic system. *Signal Processing*, *202*, 108745.
41. Gao, S., Wu, R., Wang, X., Liu, J., Li, Q., & Tang, X. (2023). EFR-CSTP: Encryption for face recognition based on the chaos and semi-tensor product theory. *Information Sciences*, *621*, 766-781.
42. Huang, X. (2012). Image encryption algorithm using chaotic Chebyshev generator. *Nonlinear Dynamics*, *67*(4), 2411-2417.
43. Wang, X., Liu, L., & Zhang, Y. (2015). A novel chaotic block image encryption algorithm based on dynamic random growth technique. *Optics and Lasers in Engineering*, *66*, 10-18.
44. Akhshani, A., Akhavan, A., Lim, S. C., & Hassan, Z. (2012). An image encryption scheme based on quantum logistic map. *Communications in Nonlinear Science and Numerical Simulation*, *17*(12), 4653-4661.
45. Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals*, *21*(3), 749-761.
46. Sun, F., Liu, S., Li, Z., & Lü, Z. (2008). A novel image encryption scheme based on spatial chaos map. *Chaos, Solitons & Fractals*, *38*(3), 631-640.
47. Zhu, Z. L., Zhang, W., Wong, K. W., & Yu, H. (2011). A chaos-based symmetric image encryption scheme using a bit-level permutation. *Information sciences*, *181*(6), 1171-1186.
48. Ye, G., & Wong, K. W. (2012). An efficient chaotic image encryption algorithm based on a generalized Arnold map. *Nonlinear dynamics*, *69*(4), 2079-2087.
49. Zhou, S., Qiu, Y., Qi, G., & Zhang, Y. (2023). A new conservative chaotic system and its application in image encryption. *Chaos, Solitons & Fractals*, *175*, 113909.
50. Fei, G., Dao-Nan, H., Heng-Qing, T., & Chuan-Mei, W. (2018). Chaotic analysis of fractional Willis delayed aneurysm system. *Acta Physica Sinica*, *67*(15).
51. Song, C., & Qiao, Y. (2015). A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos. *Entropy*, *17*(10), 6954-6968.
52. Lian, S., Sun, J., & Wang, Z. (2005). A block cipher based on a suitable use of the chaotic standard map. *Chaos, Solitons & Fractals*, *26*(1), 117-129.
53. Guo, Y., Yang, J., & Liu, B. (2021). Application of chaotic encryption algorithm based on variable parameters in RFID security. *EURASIP Journal on Wireless Communications and Networking*, *2021*(1), 155.
54. Murillo-Escobar, M. A., Meranza-Castillón, M. O., López-Gutiérrez, R. M., & Cruz-Hernández, C. (2019). Suggested integral analysis for chaos-based image cryptosystems. *Entropy*, *21*(8), 815.
55. Hosseinzadeh, R., Zarebnia, M., & Parvaz, R. (2019). Hybrid image encryption algorithm based on 3D chaotic system and choquet fuzzy integral. *Optics & Laser Technology*, *120*, 105698.
56. Wang, X., Chen, S., & Zhang, Y. (2021). A chaotic image encryption algorithm based on random dynamic mixing. *Optics & Laser Technology*, *138*, 106837.
57. Li, C., Xie, T., Liu, Q., & Cheng, G. (2014). Cryptanalyzing image encryption using chaotic logistic map. *Nonlinear dynamics*, *78*(2), 1545-1551.
58. Erkan, U., Toktas, A., Enginoğlu, S., Akbacak, E., & Thanh, D. N. (2022). An image encryption scheme based on chaotic logarithmic map and key generation using deep CNN. *Multimedia Tools and Applications*, *81*(5), 7365-7391.
59. Patel, S., & Muthu, R. K. (2020). Image encryption decryption using chaotic logistic mapping and dna encoding. *arXiv preprint arXiv:2003.06616*.
60. Stolarski, P., Lewoniewski, W., & Abramowicz, W. (2020). Cryptocurrencies perception using Wikipedia and Google trends. *Information*, *11*(4), 234.
61. Ren, K., Su, H., & Wang, Q. (2011). Secret key generation exploiting channel characteristics in wireless communications. *IEEE Wireless Communications*, *18*(4), 6-12.
62. Agarwal, S. (2018). A review of image scrambling technique using chaotic maps. *International Journal of Engineering and Technology Innovation*, *8*(2), 77.
63. Wang, Q., Guo, W., Zhang, K., Ororbia, A. G., Xing, X., Liu, X., & Giles, C. L. (2017, August). Adversary resistant deep neural networks with an application to malware detection. In *Proceedings of the 23rd ACM sigkdd international conference on knowledge discovery and data mining* (pp. 1145-1153).
64. Nazish, M., & Banday, M. T. (2024). A novel fibonacci-sequence-based chaotification model for enhancing chaos in one-dimensional maps. *IEEE Internet of Things Journal*.
65. Koshy, T. (2019). *Fibonacci and Lucas Numbers with Applications, Volume 2* (Vol. 2). John Wiley & Sons.
66. Maiti, C., Dhara, B. C., Umer, S., & Asari, V. (2023). An efficient and secure method of plaintext-based image encryption using Fibonacci and Tribonacci transformations. *IEEE Access*, *11*, 48421-48440.
67. Hazzazi, M. M., Rehman, M. U., Shafique, A., Aljaedi, A., Bassfar, Z., & Usman, A. B. (2024). Enhancing image security via chaotic maps, Fibonacci, Tribonacci transformations, and DWT diffusion: a robust data encryption approach. *Scientific Reports*, *14*(1), 12277.
68. In image encryption, a larger entropy measure for the cipher image means higher immunity against information leakage and statistical attacks
69. Wu, Y., Noonan, J. P., & Agaian, S. (2011). NPCR and UACI randomness tests for image encryption. *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, *1*(2), 31-38.
70. Wu, Y., Noonan, J. P., & Agaian, S. (2011). NPCR and UACI randomness tests for image encryption. *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, *1*(2), 31-38.