INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

DNA Encoding and Chaos based Image Encryption Technique for Cloud Storage and Communications

J Helen Arokia Selvi[1]*, **T Rajendran**[1]

1 PG and Research Department of Computer Science, Government College of Arts and Science, Kangeyam, Tamil Nadu, India

OPEN ACCESS

Received: 30-10-2024

Accepted: 31-01-2025

Published: 14-03-2025

Citation: Selvi JHA, Rajendran T (2025) DNA Encoding and Chaos based Image Encryption Technique for Cloud Storage and Communications. Indian Journal of Science and Technology 18(9): 734-744. https://doi.org/10.17485/IJST/v18i9.3557

* **Corresponding author**.

helenkiru@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: To suggest an image encryption system that uses DNA encoding and chaotic maps with SHA -512 secret key to provide a secure, efficient, and deterministic mechanism for protecting digital RGB images from unwanted access, manipulation during transmission and cloud storage. **Methods:** This strategy uses the distinctive features of DNA encoding and chaotic systems to improve image encryption performance. The hybrid technique in the present study uses DNA Encoding with 4 rules and a chaotic mechanism with SHA-512 secret key for image encryption. This technique is compared with Advanced Encryption Standard (AES) and Data Encryption Standard (DES). The methods are evaluated using histogram analysis, Encryption /Decryption time and throughput to test the performance of the suggested approach with AES and RSA. The whole experiment is simulated in CloudSim using the test images gathered from an extensively utilized image repository known as the ”SIPI image database” and also with the user generated images for validating the results. **Findings:** The suggested hybrid approach is found to have moderate performance in terms of encryption/decryption time of around 350 ms and throughput of 18000 Mbps. The encrypted image’s histogram is uniform, which implies it exhibits no patterns that are related to the original image. It also shows that the DNA encoding, and chaotic mapping techniques are more resistant to attacks. The encrypted image’s histogram is uniform, which implies it exhibits no patterns that are related to the original image, and this is essential for maintaining the validity and integrity of multimedia in sensitive applications, making it ideal for secure multimedia encryption, especially with sensitive images. **Novelty:** The hybrid method uses a DNA encoding scheme with chaotic maps and a SHA-512 secret key, which can offer a large key space and create an advanced and secure mechanism for encrypting RGB images. Unlike conventional encryption methods such as AES and DES, which rely primarily on mathematical transformations, this hybrid approach takes advantage of DNA encoding’s randomness and enormous store capacity, as well as the unpredictable nature of chaotic maps. This combination increases resilience against cryptographic attacks while maintaining efficient encryption and decryption efficiency. The work particularly differentiates out for analyzing

its approach in a cloud storage environment with CloudSim, confirming its real-world application in multimedia data security.

Keywords: Cloud Storage; Image Encryption; DNA Encoding; Chaotic Map; Advanced Encryption standard; RSA; Histograms; Encryption and Decryption time; Throughput

1 Introduction

Cloud computing has become increasingly popular in the modern day and provides users with a range of on-demand services. Cloud storage facility data security has grown to be a significant issue, especially for highly confidential information that needs additional protection while stored there, like multimedia files, films, and medical images[(1)]. The key objective of image encryption methods is to safeguard image data during transmission and storage across unprotected networks. Through the transformation of image data into a format that can only be interpreted by authorized users, image encryption effectively inhibits illegal access. When processing enormous quantities of data, high data significance, and redundancy, image encryption presents more sophisticated challenges than typical text encryption approaches. Additionally, visual information helps communicate ideas more clearly and naturally. But it also highlights a number of security issues[(2)]. As a result, creating effective and safe image encryption methods has emerged as a crucial and pressing problem in this area.

Chaotic systems are commonly used in image cryptography research due to their ease of implementation and ability to provide safe key sequences. One-dimensional and multi-dimensional chaotic systems are also considered chaotic systems. Since chaotic systems are easily controlled with a limited number of parameters, they are frequently utilized in various image encryption schemes[(3)]. Two broad categories can be used to categorize chaos-based encryption operations: bit-level one and pixel-level encryption. Bit-level encryption procedures provide a better encryption effect than pixel-level encryption because they can simultaneously change the values and positions of the pixels.

Chaotic approaches are commonly employed in decoding massive information because their features are very consistent with cryptosystem requirements; in particular, chaos-based picture encryption is particularly practical. Zhou et al., 2023 proposes an improved chaotic feature, a limited unpredictability (PWQPCM) in one dimension (1D). The suggested PWQPCM system performs more dynamically than certain other 1D chaotic systems that are currently in existence[(4)].

Abdul Kareem et al., 2024[(5)] suggest a hybrid encryption technique utilizing Discrete Hartley Transforms, the Sea Lion Optimization (SLO) algorithm, and various chaotic systems is implemented. The input image is split into four equal portions and subjected to confusion using the Lorenz chaotic system before being converted to the frequency domain. After the four parts are converted into the frequency domain, the confusion operations on each section are carried out using the chaotic sequences of the Uruk 4D chaotic system. A DNA coding-based bit- and pixel-level double-permutation[(6)] image encryption system with coupled chaotic map[(7)] and double permutation scheme[(8)] has been studied. Su et al., 2024 suggested a chaotic systems and DNA sequences based ”one-image, one-secret” image encryption technique to solve the issues of a smaller key space and the incapacity of encryption algorithms to withstand cropping attacks. A new 2-D chaotic system is used to transform the color image into a 2-D random matrix of identical size[(7)].

Jiang et al., 2024 studied a paradigm known as double quantum images representation (DNEQR), which allows the two digital images to be stored simultaneously in a quantum superposition state[(9)]. Additionally, a different type of 2D-hyperchaotic system based on logistic and sine maps is investigated. This system offers a better chaotic

behavior and a larger parameter space than the original and logistic maps. Wen et al., 2024 suggested a double quantum image encryption technique based on the hyperchaotic system and the DNEQR model. A chaotic map-based bit-level image encryption technique called BCIEA has been introduced[10]. Diffusion and confusion comprise BCIEA, and the dynamic processes incorporated during each are primarily responsible for the security performance of the system.

Alkhonaini et al., (2024) suggest encrypting grayscale images using a method that combines two-way chaotic maps for byte-level image confusion and reversible cellular automata (RCA) for image diffusion. According to the findings, the proposed method is a convincing image encryption algorithm that is highly resistant to brute-force, statistical, and differential attacks[11]. Aqeel et al., (2024) highlights the promise of DNA encoding schemes as an alternate approach to classic encryption techniques for improving cyber security while using less energy than present approaches. The findings may motivate academics to pursue new pathways for data encryption and decryption utilizing synthetic DNA patterns. DNA, as a long-lasting storage medium that can withstand extreme environmental conditions, provides a potentially efficient in terms of energy solution for storing data for a long time[12].

Wu et al. (2024) develop a chaotic image encryption technique based on dynamic Hachimoji DNA coding and computation to safeguard photos. This method offers more coding rules to automatically encode images than the standard DNA coding method, increasing the level of complexity and security of the encryption process[13]. The Table 1 lists the related works in this study.

Table 1. Related works in the literature

Author	Method	Purpose	Limitations
Zhou et al.,[4]	PWQPCM	Encryption	limited unpredictability
Kareem et al.,[5]	Discrete Hartley Transforms and SLO	Encryption	Computational overhead
Zhang et al.,[6]	DNA Encoding and Chaos	Cloud storage encryption	High computational overhead
Su et al.,[7]	Bit level Chaotic	Image encryption	sensitive to small perturbations,
Li et al.,[8]	2-D chaotic system and DNA Encoding	Image Encryption	Computational complexity
Jiang et al.,[9]	DNEQR	Image Encryptions	Computationally expensive and limited quantum resources
Wen et al.,[10]	hyperchaotic system and the DNEQR model, BCIEA	double quantum image encryption	Computationally expensive and limited quantum resources
Alkhonaini et al.,[11]	Chaotic maps and RCA	Image encryption	Key sensitivity
Aqeel et al.,[12]	DNA encoding	Data Encryption	Complex to implement
Wu et al.[13]	Dynamic Hachimoji DNA coding	Image encryption	Limited standardization

While previous research has focused on either DNA encoding or chaotic maps, this work takes a hybrid method, integrating both techniques with SHA-512 for increased security. The earlier research used symmetric encryption techniques such as AES and DES, which are subject to brute-force and differential attacks. Furthermore, previous research frequently lacked cloud-based implementation, whereas this study tests the encryption framework in CloudSim using real-world photos from the SIPI database and user-generated material. The comparison analysis of AES and RSA provides a thorough performance evaluation, ensuring that the suggested approach is both secure and efficient for cloud storage applications.

Many current encryption algorithms, such as AES and DES, have predictable structures, making them vulnerable to cryptanalysis. Previous research on DNA-based encryption lacked a uniform framework, resulting in inconsistent performance. The chaotic-based encryption solutions suffer from key sensitivity concerns, making them untrustworthy in high-security environments.Few researches have examined encryption algorithms in cloud storage environments, limiting their real-world usefulness. The major contributions of the study includes the following:

- The proposed method improves security by bringing more randomness and unpredictability by combining DNA encoding with chaotic maps and SHA-512.
- The introduction of SHA-512 improves key management and reduces the weaknesses observed in standalone chaotic encryption solutions.
- The use of CloudSim for testing verifies the method in a real-world cloud context, making it more suitable for protecting multimedia content in cloud storage.

The remainder of this study is structured as follows: The proposed approach utilizing chaos-based cryptography and DNA encoding is covered in Section 3. Section 4 discusses experimental data and evaluation parameters, and Section 5 concludes the study.

2 Methodology

2.1 DNA Encoding and Chaotic Map

DNA encoding is a new method of cloud storage for image encryption based on the basic tenets of DNA sequences (A, T, C, G) and increasing security. It involves converting image data into binary format encrypting it with DNA sequences and using cryptographic methodologies such as chaotic maps and XOR operations for strong encryption. The image to be encrypted is converted to a one dimensional array and it is fed as an input for the DNA encoding scheme. DNA coding is one of the coding techniques utilized, which uses the fundamental rules of DNA to convert a plain image's pixels into DNA format. The binary values are mapped with the four letters corresponding to the type of DNA nucleotide used [8,14]. The Figure 1 presents the overall workflow of the hybrid method.

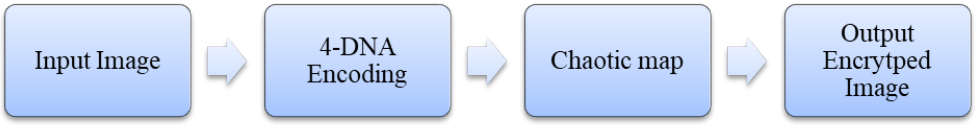

Fig 1. Overall workflow of the proposed encryption scheme

Figure 1 depicts the method of encrypting an image using a combination method that combines DNA encoding with chaotic mapping. The method starts with an encrypted digital RGB image that must be protected. This image is usually expressed in pixel values and is used as inputs for the encryption mechanism. In 4-DNA Encoding, the input image's pixel values are transformed to binary form before being encoded using a DNA encoding scheme. The term "4-DNA Encoding" refers to the usage of four nucleotides (A, T, C, and G) to represent binary data. During this step, several DNA encoding rules are used to improve unpredictability and security. A chaotic map is a mathematical function characterized by sensitivity to initial conditions and unpredictability. These systems will be used in this phase to further scramble the data encoded in DNA. By combining chaotic maps with a SHA-512, thus further complicating the method and making encryption even more secure against potential attackers. The creation of the encrypted image is by the combination of DNA encoding and chaotic mapping. It bears no relation or resemblance to the original; it is completely devoid of any patterns. The encrypted image is then either securely stored or transmitted over a network.

Deoxyribonucleic acid (DNA) is composed of four distinct nucleotides: adenine (A), guanine (G), cytosine (C), and thymine (T). The binary sequence of each nucleotide is represented in Table 2. The architecture of the hybrid DNA Encoding with Chaotic map is depicted in Figure 2.

Table 2. Binary Sequence of nucleotide

Nucleotide	Binary Sequence	Rule 1	Binary Sequence Rule 1	Binary Sequence Rule 1	Binary Sequence Rule 1
A	00		01	11	10
T	01		00	10	11
C	10		11	00	01
G	11		10	01	00

A chaotic map is a type of cryptosystem that encrypts original data by creating complex, nonlinear random sequences. A chaos-based image cryptosystem's design consists of two primary stages: the process of diffusion and the confusion. The schematic layout of the architecture is shown in Figure 2. The term "confusion phase" also refers to the "pixel permutation," a process that turns an image into an unidentified form by rearranging the pixel positions over the entire image while maintaining the pixel values. The diffusion phase is then implemented since the earlier phase was insufficiently secure and was readily breached by an attacker. Consequently, when the diffusion process is conducted with the help of a chaotic map, the sequence generated by the chaotic systems sequentially alters the values of every pixel in the image. Until a satisfactory level of security is achieved, the confusion-diffusion process is carried out multiple times [15]. Because fewer chaotic map runs are required, the

encryption/decryption process is faster and requires less memory. SHA-512 is the secret key utilized in the process of confusion and diffusion [16].

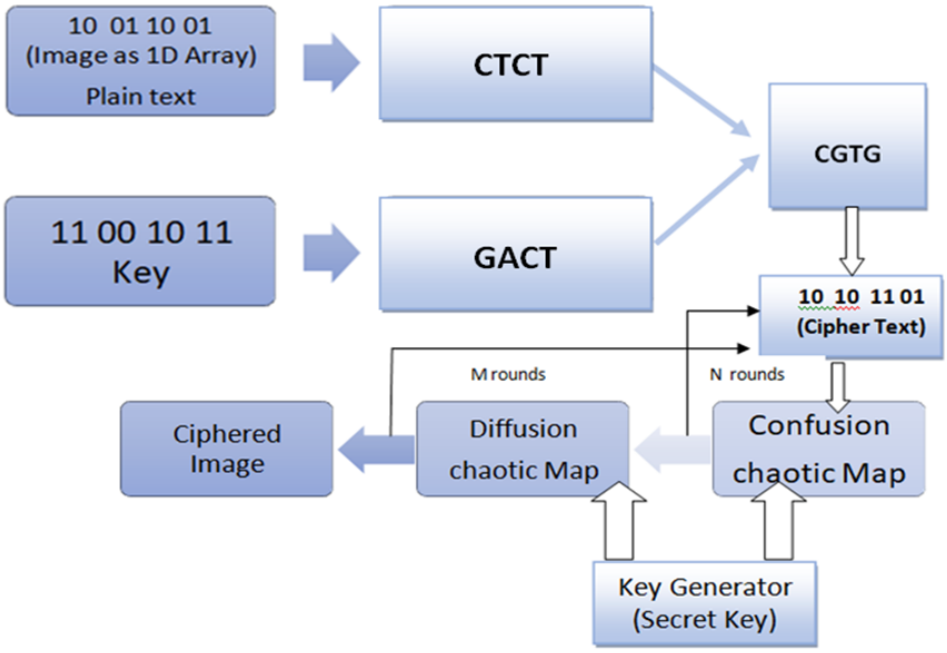

Fig 2. Architecture of Hybrid DNA-Chaotic Cryptosystems

2.2 Advanced Encryption Standard (AES)

The AES is a commonly used symmetric encryption technique for securely encrypting and decrypting data [17,18]. The Algorithm for AES is as follows

Algorithm EncryptImage
Input: Plain image I, AES key, hyperchaotic system parameters
Output: Cipher image CImage.
● Divide the plain image I into blocks of size 128 bits each.
If the image size is not a multiple of 128 bits,
pad with zeros or appropriate padding scheme.
● Initialize the hyperchaotic system with secret parameters and initial conditions using the AES key.
● Generate the first chaotic sequence S using the hyperchaotic system.
● Create the first S-box:

- Sort the values in S in ascending order.
- Map the sorted values to form a 256-element S-box.

● For each block Bi in the plain image:
a. Use the current S-box for AES encryption.
b. Encrypt the block Bi using AES with: -

- The secret key
- The current S-box

c. Store the encrypted block Bi_cipher.
d. Update the S-box:

- - Use the final value of the current sequence S as the new initial condition.
- - Create a new sequence S using the hyperchaotic system.
- - Design the next S-box by sorting and mapping the new sequence.

● Combine all encrypted blocks Bi_cipher to form the cipher image Icipher.
● Return CImage.

2.3 RSA Algorithm

The RSA algorithm is a popular public-key encryption system for reliable data transmission. It is based on the mathematical complexity of factoring huge composite numbers into prime factors, resulting in strong encryption [19,20].

Algorithm RSA
Input: Message M
Output: Ciphertext C (encrypted message), Decrypted message M_decrypted
1. Key Generation

- Randomly generate two large prime numbers p and q.
- Compute n = p * q.
- Compute φ(n) = (p - 1) * (q - 1).
- Choose an integer e such that:- 1 < e < φ(n)

- gcd(e, φ(n)) = 1 (e is not a divisor of φ(n)).

- Compute the private key d such that:

- (e * d) $\equiv$ 1 (mod φ(n)) (modular multiplicative inverse of e mod φ(n)).
Public Key: (e, n)
Private Key: (d, n)
2. Encryption

- Convert the plaintext message M to numerical format if not already done.
- Compute the ciphertext C:

C = (M^e) mod n.
3. Decryption

- Use the private key (d, n) to compute the original message M_decrypted:

M_decrypted = (C^d) mod n.

- Convert M_decrypted back to its original message format.

4. Return Ciphertext C and Decrypted Message M_decrypted

3 Results and Discussion

CloudSim framework is used to provide simulation services in cloud computing settings. The experiments are simulated using CloudSim Simulator. The results from several testing show that the proposed algorithm offers robust protection against statistical and differential assaults, making it suitable for the encryption of images. Test images have been collected from an extensively used image repository known as the ”SIPI image database”, which are the standard images used by the majority of existing works to assess the strength of image encryption algorithms [21]. The sample input images, encrypted images, and decrypted images are displayed in Figure 3.

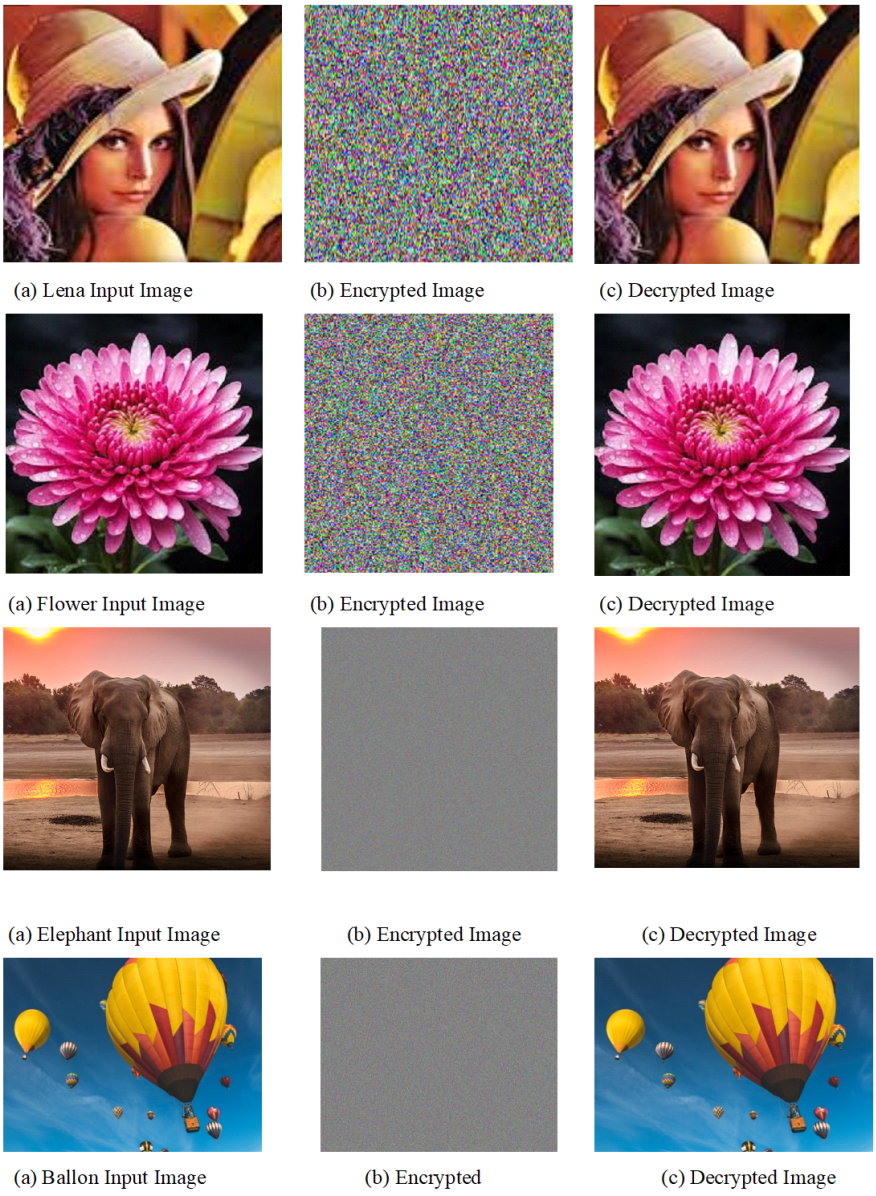

Fig 3. Sample Input/Encrypted and Decrypted Images

(i) Histogram Analysis

An analytical graph that displays the distribution of color values in a digital image is called a histogram. A flat histogram is the result of every pixel in a perfect cryptosystem having the same probability of occurring[22]. Figure 4 depicts the histogram analysis of the hybrid DNA encoding and Chaotic methods for the sample input images to be encrypted and the encrypted image.

For the encrypted images, the suggested encryption approaches generate histograms in such a way that the encrypted images yield no meaningful information, demonstrating the algorithm's resilience against statistical attacks. The application of chaotic maps for pixel scrambling and substitution disrupts statistical relationships in the image, rendering it resilient to attacks based on analyses of frequencies or histograms.

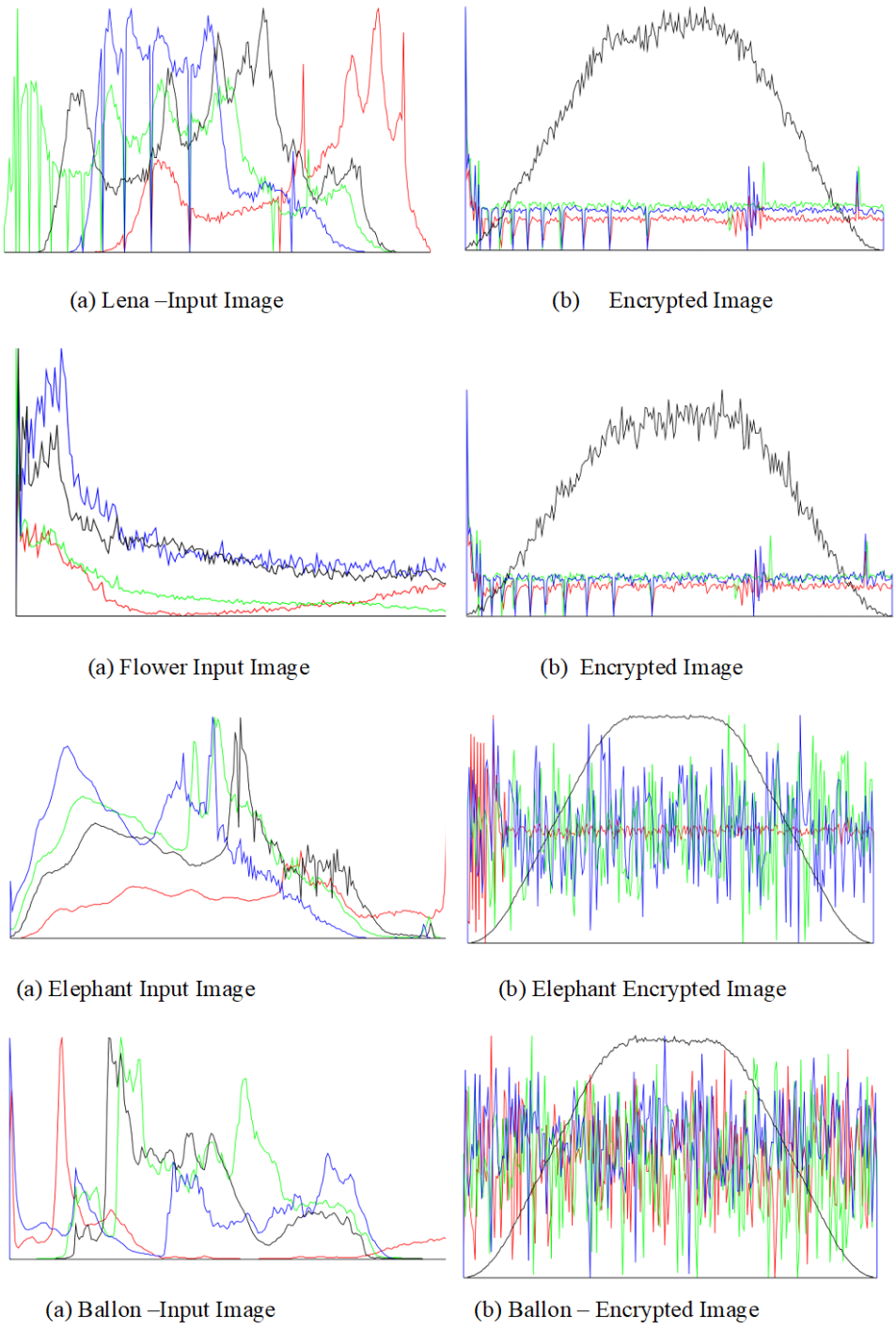

Fig 4. Suggested Method- Histogram Analyses – Input and Decrypted Image

(ii) Encryption/decryption time

An encryption algorithms runtime is a crucial component. Everyone has connected a timer to the project in order to track the encryption time. This made it possible for us to determine how many cycles would be required for the encryption and decryption processes[21]. The processing time is computed for the encryption and decryption process as follows.

$$Processing\ time\ (T) = N_c * T_{Cycle} = \frac{N_c}{CPU_{Freq}} \quad (1)$$

In Equation (1) N_c is the total number of cycles required to encrypt the entire image, T_{cycle} is the clock cycle time which is equal to $\frac{1}{CPU_{freq}}$. Table 2 presents the encryption and decryption time for the hybrid DNA and chaotic map, AES and DES methods.

Table 3. Encryption and Decryption time

Methods/Measures	Encryption time	Decryption time
Hybrid-DNA Encoding and Chaotic Map with SHA-512 secret key (512 *512 RGB images)	~350 milliseconds ~18,000 Mbps	~400 ms milliseconds
AES(512 *512 RGB images with 128 bit key)	~180 milliseconds 34000 Mbps	~185 milliseconds
RSA(1 KB message with 2048 bit key)	~3 Seconds 2100 Mbps	~3.5 Seconds

From the Table 3 values, it is found that the encryption /decryption time for the suggested method is moderate than that of AES and RSA. Encrypting and decrypting a 512×512 image with RSA is time-consuming and impracticable owing to modular arithmetic limitations. However, it is most suitable for securing small bits of data, such as keys, using a hybrid encryption method. The preferred method for encrypting the image is AES and the suggested hybrid technique using DNA and chaotic maps provides higher security for multimedia data.

(iii) Throughput

The throughput of an algorithm can be used to determine its performance. Because throughput and efficiency of an algorithm are closely related, better throughput translates into higher performance. The equation that follows can be utilized for calculating the encryption techniques performance[23].

$$Throughput\ = \frac{Total\ \ file\ size\ (MB)}{Total\ Evaluation\ time\ of\ \ algorithms\ (ms)}$$

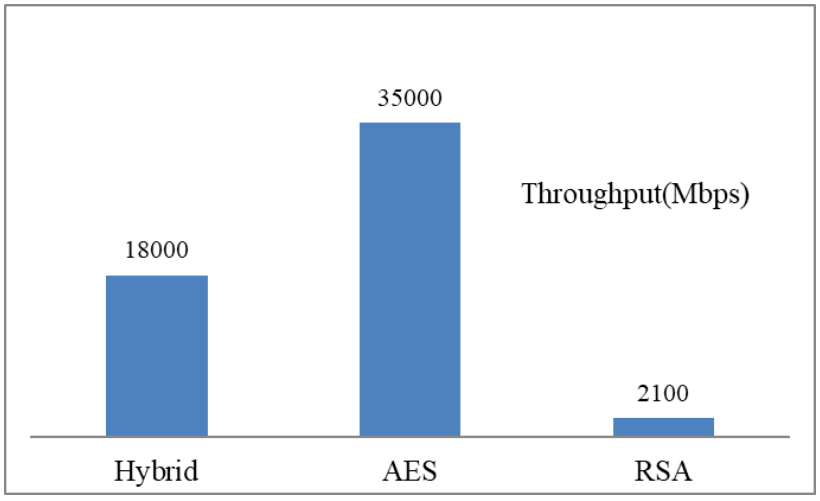

Fig 5. Throughput Analysis

The method's performance will increase with increased throughput. Figure 5 shows that the DNA Encoding with chaotic maps is moderate than the AES and RSA. RSA is the slowest method of image encryption, because it is not designed for images and is suitable for encrypting only small data, particularly keys. The suggested DNA with chaotic maps with SHA technique is especially designed for encrypting multimedia content, because of the distinct obstacles and hazards related to the storage and dissemination of multimedia content.

Moreover, DNA-based storage provides great data density, parallelism, and resistance to attacks, making it perfect for secure cloud storage. This technology improves secrecy, integrity, and cyber threat prevention by combining biological computing and encryption, while also maximizing storage economy.

The Table 4 shows the comparison chart for the hybrid DNA encoding and Chaotic maps with SHA-512 with the other state of art cryptographic techniques.

Table 4. Comparison of suggested hybrid multimedia encryption with existing methods

Methods/ Measures	Encryption time	Decryption time	Throughput	Remarks
Hybrid-DNA Encoding and Chaotic Map with SHA-512 secret key	~500	~500	~11	Throughout is high with accelerating the hardware. Effective for multimedia encryption
BlowFish	~50	~50	~126	Although faster than AES for smaller datasets, it lacks advanced hardware acceleration.
DES (Data Encryption Standard)	~200	~200	~31	Outdated and less secure; slower than AES on larger datasets.
3DES	~300	~300	~21	Stronger than DES. However, triple encryption makes it slower.

DNA Encoding and Chaotic Maps with SHA-512 secret key strikes a mix between security and performance, and its moderate throughput makes it useful for safe multimedia encryption, particularly of sensitive images. Furthermore, DNA encrypts data with less complexity and cost effective. The distinct characteristics of chaotic systems, namely their determinacy, ergodicity, and sensitivity to initial conditions, render them a valuable option for the development of cryptosystems. These attributes bear resemblance to the diffusion and confusion characteristics of a well-designed cryptosystem. Numerous chaotic image encryption algorithms and enhanced techniques have been developed with the ongoing advancements in the field of cryptanalysis and image encryption, and they have the ability to counter a wide range of security risks.

The proposed hybrid encryption approach has some potential drawbacks. One of the main problems is computational complexity, as the amalgamation of DNA encoding and chaotic maps could bring down encryption and decryption times, making it more resource-intensive than existing approaches such as AES or DES. This may cause scalability concerns, especially in cloud storage systems where the overhead of processing huge datasets might strain system resources. Furthermore, while DNA encoding provides enormous key spaces and unpredictability, it is also a relatively new technology that could be vulnerable to new cryptographic attacks, jeopardizing its security. In addition, the absence of widely recognized standards for DNA encoding and chaotic mapping, as opposed to well-established approaches such as AES, can make integration difficult and restrict compatibility with existing cryptographic systems. These considerations underscore the importance of careful planning in real-world implementation, particularly when scaling in cloud-based settings or integrating with current systems.

4 Conclusion

The study has presented a hybrid image encryption algorithm for cloud storage. The study employs DNA encoding and chaotic map with SHA-512 key for encrypting the color images and compared it with the AES, RSA and other state of art methods. It is found that the suggested hybrid technique shows the moderate performance in terms of encryption/decryption time and throughput. The histogram analysis reveals that the DNA encoding, and chaotic maps technique is more resistive to attacks. This is critical for preserving the validity and integrity of multimedia in sensitive applications, making it perfect for secure multimedia encryption, particularly with sensitive images. DNA's lightweight nature and chaotic maps make them perfect for safeguarding multimedia in IoT devices and cloud systems. The use of DNA encoding in conjunction with chaotic maps for the encryption of images is a developing field with tremendous potential for improving safety and effectiveness in multimedia encryption. Because both DNA encoding and chaotic systems have distinct traits such as high unpredictability along with robust security features, there are numerous avenues for further study and development to improve and perfect image encryption

approaches.

References

1) Umar T, Nadeem M, Anwer F. Chaos based image encryption scheme to secure sensitive multimedia content in cloud storage. *Expert Systems with Applications*. 2024;257. Available from: https://doi.org/10.1016/j.eswa.2024.125050.
2) Ye G, Guo L. A visual meaningful encryption and hiding algorithm for multiple images. *Nonlinear Dynamics*. 2024;112:14593–14616. Available from: https://doi.org/10.1007/s11071-024-09790-7.
3) Zhou NR, Hu LL, Huang ZW, Wang MM, Luo GS. Novel multiple color images encryption and decryption scheme based on a bit-level extension algorithm. *Expert System and Applications*. 2024;238(Part C). Available from: https://doi.org/10.1016/j.eswa.2023.122052.
4) Zhou NR, Hu LL, Huang ZW, Wang MM, Luo GS. Novel multiple color images encryption and decryption scheme based on a bit-level extension algorithm. *Expert Systems with Applications*. 2024;238(Part C):122052. Available from: https://doi.org/10.1016/j.matcom.2022.12.025.
5) Abdul-Kareem AA, Al-Jawher WAM. An image encryption algorithm using hybrid sea lion optimization and chaos theory in the hartley domain. *International Journal of Computers and Applications*. 2024;46(5):324–337. Available from: https://doi.org/10.1080/1206212X.2024.2313300.
6) Zhang H, Hu H. An image encryption algorithm based on a compound-coupled chaotic system. *Digital Signal Processing*. 2024;146. Available from: https://doi.org/10.1016/j.dsp.2023.104367.
7) Su Y, Wang X, Gao H. Chaotic image encryption algorithm based on bit-level feedback adjustment. *Information Sciences*. 2024;679. Available from: https://doi.org/10.1016/j.ins.2024.121088.
8) Li P, Qian J, Xu TT. New chaotic systems and application in DNA colored image encryption. *Multimedia Tools and Applications*. 2024;83:50023–50045. Available from: https://doi.org/10.1007/s11042-023-17605-x.
9) Jiang SX, Li Y, Shi J, Zhang R. Double quantum images encryption scheme based on chaotic system. *Chinese Physics B*. 2024;33(4). Available from: https://doi.org/10.1088/1674-1056/ad1174.
10) Wen H, Lin Y, Feng Z. Cryptanalyzing a bit-level image encryption algorithm based on chaotic maps. *Engineering Science and Technology, an International Journal*. 2024;51:1–8. Available from: https://doi.org/10.1016/j.jestch.2024.101634.
11) Alkhonaini MA, Gemeay E, Mahmood FMZ, Ayari M, Alenizi FA, Lee S, et al. A new encryption algorithm for image data based on two-way chaotic maps and iterative cellular automata. *Scientific reports*. 2024;14:1–15. Available from: https://doi.org/10.1038/s41598-024-64741-x.
12) Aqeel S, Khan SU, Khan AS, Alharbi M, Shah S, Affendi ME, et al. DNA encoding schemes herald a new age in cybersecurity for safeguarding digital assets. *Scientific Reports*. 2024;14(1). Available from: https://doi.org/10.1038/s41598-024-64419-4.
13) Wu X, Zhong C, Long B, Liu T, He C, Wang L. Chaotic image encryption algorithm based on dynamic Hachimoji DNA coding and computing. *Physica Scripta*. 2024;99(4). Available from: https://doi.org/10.1088/1402-4896/ad3245.
14) Mou D, Dong Y. Color image encryption algorithm based on novel dynamic DNA encoding and chaotic system. *Physica Scripta*. 2024;99(6). Available from: https://doi.org/10.1088/1402-4896/ad3ff1.
15) Zia U, Mccartney M, Scotney B, Martinez J, Abutair M, Memon J, et al. Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. *International Journal of Information Security*. 2022;21(4):917–935. Available from: https://doi.org/10.1007/s10207-022-00588-5.
16) Rezaei B, Mobasseri M, Enayatifar R. A secure, efficient and super-fast chaos-based image encryption algorithm for real-time applications. *Journal of Real-Time Image Processing* . 2023;20. Available from: https://doi.org/10.1007/s11554-023-01289-5.
17) Brahim AH, Pacha AA, Said AH. An image encryption scheme based on a modified AES algorithm by using a variable S-box. *Journal of Optics*. 2024;53(2):1170–1185. Available from: https://doi.org/10.1007/s12596-023-01232-8.
18) Inam S, Kanwal S, Firdous R, Zakria K, Hajjej F. A new method of image encryption using advanced encryption Standard (AES) for network security. *Physica Scripta*. 2023;98(12). Available from: https://doi.org/10.1088/1402-4896/ad0944.
19) Du S, Ye G. IWT and RSA based asymmetric image encryption algorithm. *Alexandria Engineering Journal*. 2023;66:979–991. Available from: https://doi.org/10.1016/j.aej.2022.10.066.
20) Guleria V, Kumar Y, Mishra DC. Multiple colour image encryption using multiple parameter FrDCT, 3D Arnold transform and RSA. *Multimedia Tools and Applications* . 2024;83:48563–48584. Available from: https://doi.org/10.1007/s11042-023-17166-z.
21) Weber AG. The USC-SIPI Image Database: Version 5. 2006. Available from: http://sipi.usc.edu/database/.
22) Maazouz M, Toubal A, Bengherbia B, Houhou O, Batel N. FPGA implementation of a chaos-based image encryption algorithm. *Journal of King Saud University - Computer and Information Sciences*. 2022;34(10):9926–9941. Available from: https://dx.doi.org/10.1016/j.jksuci.2021.12.022.
23) Al-Hyari A, Obimbo C, Abu-Faraj MM, Al-Taharwa I. Generating Powerful Encryption Keys for Image Cryptography With Chaotic Maps by Incorporating Collatz Conjecture. *IEEE Access*. 2024;12:4825–4844. Available from: https://dx.doi.org/10.1109/access.2024.3349470.