International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 22s, 2025
https://theaspd.com/index.php

A Robust Golden Matrix Based T-Dna Rules for Securing Medical Images

K. Sudha Kumari[1], C. Nagaraju[2]
[1]Research Scholar, YSR Engineering College of Yogivemana University, Proddatur, Andhra Pradesh, India
[2]Professor, YSR Engineering College of Yogivemana University, Proddatur, Andhra Pradesh, India
Corresponding Author Email: Sudhakumari.kanchegara@gmail.com

Abstract
This paper presents a novel hybrid image encryption technique that integrates the Logistic Map, Golden Matrix transformation, and Reversible T-DNA rules to ensure enhanced security and efficiency in medical image protection. The proposed method leverages the chaotic behavior of the Logistic Map for generating sensitive key streams, while the Golden Matrix, based on the golden ratio and Lucas balancing numbers, introduces complex pixel transformations. Additionally, the T-DNA transformation, inspired by DNA computing, enables robust and reversible encryption at the nucleotide level. Our approach achieves strong cryptographic properties including high entropy values (~7.99), reduced pixel correlation, and significant resistance to statistical and differential attacks. Comparative experiments demonstrate that the proposed method outperforms traditional Fibonacci-based ciphers in both security strength and execution time, reducing computational time by over 50% for 255×255 images. Furthermore, the framework is adaptable to various image sizes and formats. These results establish the proposed method as a secure, efficient, and bio-inspired solution for safeguarding sensitive medical images in modern cryptographic applications.

Keywords: *Image Encryption, Golden Matrix, T-DNA Transformation, Logistic Map, DNA Cryptography, Medical Image Security.*

1. INTRODUCTION

In modern cryptographic image encryption techniques, a two-dimensional image can be represented as a one-dimensional textual bitstream, allowing the application of conventional ciphers such as DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), and AES (Advanced Encryption Standard) for data protection [1]. Image encryption methods are generally categorized into seven major types: (i) mathematically based algorithms, (ii) secret segmentation and sharing techniques, (iii) compression-based encryption, (iv) transform-domain approaches, (v) chaos-based methods, (vi) DNA cryptographic techniques, and (vii) modern secure communication mechanisms.

Mathematical image encryption methods aim to develop secure algorithms rooted in mathematical problem-solving frameworks [2]. Secret segmentation techniques divide image data into meaningless fragments to obscure meaningful patterns, thus enhancing security [3,4]. Transform-domain techniques process images using transformations such as DWT or FRT before encryption. Chaos-based encryption methods apply chaotic maps to introduce confusion and diffusion properties [5,6]. In compression-based approaches, encryption is applied directly to compressed image data to optimize storage and security efficiency [7].

DNA cryptographic methods utilize the four nucleotides adenine (A), cytosine (C), guanine (G), and thymine (T)—to encode image data at a molecular level. By applying DNA pairing rules and binary substitution schemes, images are encoded as DNA sequences and subsequently transformed into ciphertext to resist cryptanalysis. This bio-inspired approach combines the principles of molecular biology and computational encryption, offering a promising yet complex solution. Although practical DNA-based encryption is still limited due to biological constraints, such as operational complexity and laboratory feasibility, the concept remains theoretically secure. Future advancements in biotechnology may lead to DNA chips replacing traditional silicon-based processors [8–10].

Preprocessing techniques such as the fractional Fourier transform (FRT), discrete wavelet transform (DWT), and others have also been integrated into hybrid encryption schemes. Despite the rapid growth of chaos-based algorithms, many have shown vulnerabilities under advanced attacks [11–14]. Likewise, while DNA-based methods provide novel security paradigms, their current limitations stem from experimental constraints rather than computational capability [15–21]. Moreover, although chaotic map-based algorithms offer robustness against cryptographic attacks, they often suffer from performance delays and susceptibility to plaintext and differential attacks under certain conditions [22,23].

Among all encryption techniques, the one-time pad (OTP) is considered the most secure due to its theoretical unbreakability. However, its practical implementation is limited, as managing and securely distributing a large number of keys is highly challenging. While DNA cryptography has recently gained attention as a promising alternative, it still faces several technical and biological limitations. These include high error rates in biological operations, complex encoding procedures, and significant experimental costs.

To address some of these challenges, a novel image encryption method combining Fibonacci Q-Matrix (FibQM) with Transpose T-DNA Cellular Automata (TT-DNA CA) has been proposed. This hybrid approach leverages the strength of natural DNA sequences to function as high-entropy, one-time-like pads. By integrating the robustness of T-DNA cellular automata and the mathematical unpredictability of FibQM, the scheme not only inherits the security features of OTP systems but also demonstrates resilience against common threats such as plaintext and differential attacks. This innovation marks a significant step toward the practical realization of bio-inspired cryptographic systems.

2. PRELIMINARIES

There is a sophisticated method in cryptographic imaging that uses techniques such as the logistic map, Golden Matrix, cellular automata, and Reverse T-DNA cellular automata to encrypt and decrypt images. By integrating the concepts of cellular automata, linear algebra, and chaos theory, these techniques improve image processing security. The following summarizes the functions of each of these elements in image encryption and decryption:

2.1Logistic Map

Using a Logistic map to generate random keys

A straightforward mathematical function called the logistic map is frequently employed to create chaotic sequences that seem random. The recurrence relation defines it:

The formula

$$x_{n+1} = \mu * x_n(1 - x_n) \quad (1)$$

where n = 0, 1, 2, ... and $\mu \in [0, 4]$. According to the study's findings, the system is in a random state when $3.5699 < \mu \leq 4$.

2.2 Golden Matrix

In order to improve the security and effectiveness of encryption methods, the Golden Matrix concept uses the golden ratio in image encryption. Using the golden ratio to encrypt images can make it more complicated and unpredictable.

Golden Ratio (ϕ):

The golden ratio is given by:

$$\phi = \frac{1+\sqrt{5}}{2} \approx 1.618$$

properties or relationships involving ϕ

Golden Ratio Matrix

The simplest form is a 2×2 matrix whose eigen values include the golden ratio ϕ and its conjugate $\phi = \frac{1+\sqrt{5}}{2}$

$$M = \begin{bmatrix} \phi & 1 \\ 1 & \phi \end{bmatrix}$$

This matrix has:

- Eigen values ϕ and inverse ϕ
- Eigen vectors that reflect Fibonacci-like recursive properties.

Golden Powers and Fibonacci Relation

Golden matrices are often linked to the Fibonacci sequence through powers of matrices. Consider:

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

The power matrix is $A^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$, $n = 0, \pm 1, \pm 2, \ldots$

where F_n is the nth Fibonacci number. The eigenvalues of A are also ϕ and inverse ϕ

Generalized Golden Matrices

Other forms of golden matrices might take the form:

$$M_{\phi} = \begin{bmatrix} a & b \\ b & a+b \end{bmatrix}, \quad (2)$$

where a and b are chosen to involve ϕ (e.g., a/b = ϕ).

Lucas Balancing Numbers

Lucas Balancing numbers are a sequence of integers derived with different recurrence relations. The sequence is defined as: $L_n = P.L_{n-1} + Q.L_{n-2}$ (3)

where P and Q are constants. Commonly, P = 2 and Q = 1.

2.3 DNA Cellular Automata:

Cellular automata are computational systems that consist of a grid of cells, each of which can be in a finite number of states. The state of each cell changes over time based on a set of rules and the states of its neighbouring cells. When applied to DNA, cellular automata are used to model or simulate processes like DNA replication, transcription, self-assembly, or pattern formation in a simplified, discrete framework. Each cell represents a nucleotide or symbolic unit (e.g., A, T, G, C in the context of DNA) or a simpler binary state (0 or 1). The automaton evolves in a one-dimensional line, with each cell interacting with its neighbours. The state of a cell at the next time step is determined by: Its current state and the states of its neighboring cells (e.g., left and right neighbours). Nucleotide presence or absence is represented by the states 0 and 1.

A cell is considered to be 1 if exactly one of its neighbors is 1; if not, it is considered to be 0.

According to Wolfram's notation, Rule 150 might be this: The {left, center, right} neighbourhood {000 → 0, 001 → 1, 010 → 1, 011 → 0, 100 → 1, 101 → 0, 110 → 0, 111 → 0} are the updates $z \in Z = \{A, C, G, T\}$ and radius is x The nodes on the left and right of node z are the closest to it. Thus, node z is the transfer function at discrete time and has a local neighborhood of $2x$ cells. The states of the nearby cells at time t determine the state of z at time of, and let

$$z_i^{t+1} = f\left(z_{i-x}^t, \ldots., z_{i-1}^t, z_i^t, z_{i+1}^t, \ldots., z_{i+x}^t\right) \quad (4)$$

Where z_i^{t+1} represents the state of the i[th] cell at discrete time $t+1$.

Examine a DNA cellular automaton that is one dimensional and has $x = 1$. The state of the i[th] cell at discrete time t is z_i^t, while the states of its two neighbors are z_{i-1}^t and z_{i+1}^t. The expression of the cellular automata's evolution

$$z_i^{t+1} = f\left(z_{i-1}^t, z_i^t, z_{i+1}^t\right) \quad (5)$$

One specific kind of DNA cellular automaton is called T-DNA cellular automaton (T-DNA CA). A T-shaped neighborhood is formed by the designated node s and its three closest neighbors (bottom, right, and left). The states of the nodes within the specified node z at time t + 1 will be used to calculate its state. All cells' state values are updated synchronously at distinct intervals in accordance with a predetermined rule. Any of the four bases {A, C, G, T} can be taken by any cell using a T-DNA cellular automaton. The T-DNA cellular automaton is referred to as an elementary T-DNA cellular automaton (ET-DNA CA) when the radius x = 1. In that scenario, the nodes to the left, right, and bottom of node are the closest to it. At a discrete time t, the cell's position (i, j) is in the state $z_{i,j}^t$, while its three nearest nodes are in the states $z_{i,j-1}^t$, $z_{i,j+1}^t$, and $z_{i+1,j}^t$. The expression of T-DNA cellular automata evolution

$$z_{i,j}^{t+1} = f\left(z_{i,j-1}^t, z_{i,j}^t, z_{i,j+1}^t, z_{i+1,j}^t\right) \quad (6)$$

Cellular automata that completely preserve information are known as invertible cellular automata, or reversible cellular automata. We offer a special design approach for T-DNA CA that makes it appropriate for picture encryption, based on the concepts of T-DNA CA and EDNA CA. Here, a unique T-DNA CA using DNA XOR operation was employed, together with the guidelines for an EDNA CA and a $(x = 0)$ DNA CA. An ST-DNA cellular automaton (ST-DNA CA) is the name given to this kind of cellular automaton. The discrete time transfer functions of EDNA CA and ST-DNA CA are denoted by the letters f and F, respectively. The evolution is articulated.

$$z_i^{t+1} = f\left(z_{i,j-1}^t, z_{i,j}^t, z_{i,j+1}^t\right) \oplus z_{i+1,j}^t = F\left(z_{i,j-1}^t, z_{i,j}^t, z_{i,j+1}^t, z_{i+1,j}^t\right) \quad (7)$$

In order to further enhance the aforesaid ST-DNA CA and create the avalanche effect of encryption processes, the other $(x = 0)$ DNA CA is then employed (z_2 is the node of this DNA CA, $z_2 \in Z_2$ = {A, C, G, T}).

$$z_{1(i,j)}^{t+1} = f\left(z_{1(i,j-1)}^{t+1}, z_{1(i,j)}^{t}, z_{1(i,j+1)}^{t}\right) \oplus z_{2(i,j)}$$
$$= F\left(z_{1(i,j-1)}^{t+1}, z_{1(i,j)}^{t}, z_{1(i,j+1)}^{t}, z_{2(i,j)}\right) \quad (8)$$

An RT-DNA cellular automaton (RT-DNA CA) is a reversible cellular automaton, like the ST-DNA CA mentioned above. Each cell in the reverse process is swapped out for its predecessor cell. It might be expressed as

$$z_{1(i,j)}^{t+1} = f^{-1}\left(z_{1(i,j-1)}^{t+1}, z_{1(i,j)}^{t+1}, z_{1(i,j+1)}^{t}\right) \oplus z_{2(i,j)}$$
$$= F^{-1}\left(z_{1(i,j-1)}^{t+1}, z_{1(i,j)}^{t+1}, z_{1(i,j+1)}^{t}, z_{2(i,j)}\right) \quad (9)$$

2.4 Dynamic DNA Rules:

(A)Adenine, (G)guanine, (C)cytosine, and (T)thymine are the four nucleic bases that make up DNA. As per DNA base pairing rules, a doublestranded DNA molecule forms when the complementary chemical nitrogenous bases of the two components are bonded together, matching A with T and C with G. The binary coding rules for DNA sequences created by applying matching sequence rules and corresponding binary system rules are shown in below table.

Rule	**A**	**C**	**T**	**G**
Rule 0	00	11	10	01
Rule 1	00	11	01	10
Rule 2	11	00	10	01
Rule 3	11	00	01	10
Rule 4	10	01	00	11
Rule 5	01	10	00	11
Rule 6	10	01	11	00

The dynamic rule selection is typically governed by a formula such as:

Rule number=Pixel value (or key) mod 8

This dynamic selection mechanism introduces randomness and unpredictability in the DNA encoding process, enhancing the security of image encryption schemes by making the mapping dependent on pixel intensity or key stream values.

XOR	**A**	**T**	**C**	**G**
A	A	T	C	G
T	T	A	G	C
C	C	G	A	T
G	G	C	T	A

This table defines the resultant base when two DNA bases are XORed.

For example: A⊕T=T

C⊕G=T

G⊕G=A

2.5. Existing Method

Despite being novel, the Fibonacci Q-matrix image encryption technique has a number of shortcomings. Because it depends on dependable Fibonacci sequences, it is susceptible to cryptanalysis, in which case the encryption key could be recovered by an adversary who is conversant with the mathematical characteristics of the sequences. Additionally, if there is not enough randomness or entropy in the key generation process, the encryption process may not be resilient against common assaults like chosen-plaintext and differential attacks. When compared to other contemporary encryption methods, matrix operations' computational complexity may also result in slower performance, particularly for high-resolution photos. Lastly, its practical uses in real-world circumstances may be hindered by its low scalability and adaptability to a variety of encryption needs.

3. Proposed framework

Here is a description of the essential procedures and the theoretical framework for developing a flowchart that combines the Reverse T-DNA encryption method with the Golden matrix methodology for image encryption. The Golden matrix is used for cryptographic transformation, and the T-DNA concept is used as an additional layer for enhanced encryption.

Description of the Encryption Steps:

3.1. Input Image: Convert the image into a **grayscale** or **RGB matrix** of pixel values.

Grayscale: Each pixel is an integer value between 0 and 255.

RGB: Represent each pixel as a tuple of three values (R, G, B).

3.2. Generate a Pseudo-Random Sequence Using the Logistic Map

The **Logistic Map** is defined by the equation:

$$x_{n+1} = \mu * x_n(1 - x_n)$$

where

r is the control parameter $3.9 \leq r \leq 4$ for chaotic behaviour.

x_n is the current value in the sequence $(0 < x_n < 1)$

3.3. Construct the Golden Matrix transformation

The Golden Matrix is based on Golden Ratio $= \frac{1+\sqrt{5}}{2}$. A 2×2 Golden Matrix is

$$G = \begin{bmatrix} \phi & 1 \\ 1 & \phi - 1 \end{bmatrix}$$

Extend G to a $N \times N$ matrix to permute the pixel positions or values

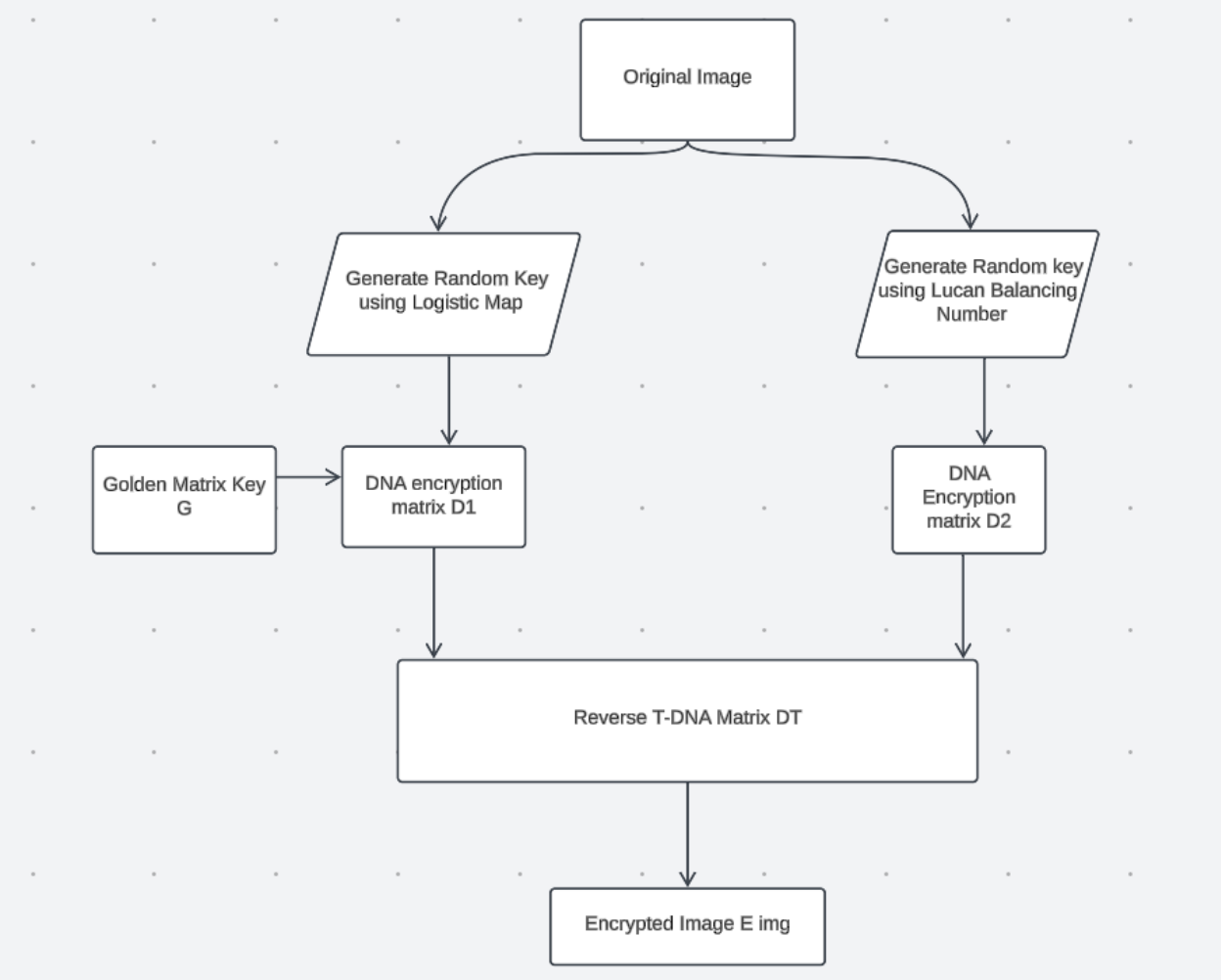
3.4. Using Lucas Balancing Numbers

Generate a sequence $\{L_n\}$ and map it to the size of M. Use $\{L_n \bmod 256\}$ as keys for pixel diffusion Generate a DNA encoded matrix on binary matrix based on the DNA sequence rules, say as D1 and D2. Apply Reverse T-DNA encryption process on the D1 and D2, which generates the DNA encryption matrix E img

In order to decrypt:

1. Use the inverse CA rule to reverse the T-DNA cellular automaton.
2. To restore the initial values or positions, use the Golden Matrix changes in reverse.
3. To replicate the precise key stream, apply the logistic map modifications in reverse, utilizing the same initial conditions and parameter.

3.5. Flowchart:



Working example:

Grey image = $\begin{bmatrix} 85 & 78 & 57 \\ 65 & 120 & 156 \\ 222 & 168 & 210 \end{bmatrix}$

Chaotic random values K (normalized values) = $(6,2,1,5,3,8,4,7,0)$

= $(222,57,78,156,65,210,120,168,85)$

Golden Matrix key: A 3 × 3 Golden Matrix expands the principles of the Golden Ratio into a larger matrix. Its entries incorporate ϕ, ϕ', and combinations of integers to preserve the Golden Ratio's properties.

$$\begin{bmatrix} \phi & 1 & \phi' \\ 1 & \phi' & \phi \\ \phi' & \phi & 1 \end{bmatrix}$$

$$\phi = 1.618$$

$$G = \begin{bmatrix} 222 & 57 & 78 \\ 156 & 65 & 210 \\ 120 & 168 & 85 \end{bmatrix} * \begin{bmatrix} 1.618 & 1 & 0.618 \\ 1 & 0.618 & 1.618 \\ 0.618 & 1.618 & 1 \end{bmatrix} \bmod 256$$

We get G= $\begin{bmatrix} 103 & 57 & 48 \\ 156 & 40 & 84 \\ 74 & 16 & 85 \end{bmatrix}$

Now apply the DNA dynamic rules on the Golden matrix

D1 = [ACATACGTACAAACGTATTACCCTGCTTATAAAAAA]

Now find Lucas Balancing numbers by using $L_n = 3L_{n-1} + L_{n-2}$ where L0=2,L1=1

$\{L_n \bmod 256\}$ = $\begin{bmatrix} 2 & 1 & 5 \\ 14 & 41 & 122 \\ 109 & 70 & 185 \end{bmatrix}$

Generate DNA matrix using dynamic rules say D2,

D2 = [CCCTAAATTTAAGGTAAGGTGATTACGACGCAGCGT]

Now apply reverse T-DNA process on D1 and D2 and generate matrix DT using equation (6), let [ACAT] and [CCCT] are first elements from D1 and D2 then after applying Reverse T-DNA the element becomes [ACTT]

Final DT =[ACTTGCATTTACACTGTGACGGTAGGATCATGTAGC]

4. Experiment results

4.1. Properties of the parameters

To determine the similarity between original image and encrypted eleven parameters are applied. higher values of parameter represent high similarity and lower values represents lower similarity. According to security lower values produce high security with high randomness in encrypted image and vice versa. the table values represent our method provides better security.

$$\text{jaccard} = \frac{a}{a+b+c}$$

a = quantity of variables that both object I and object J have one of them

b = quantity of variables in which item I is 1 and object J is 0

c = quantity of variables in which object i is equal to 0 and object j to 1

d = quantity of variables in which i and j are both zero

The number of variables is p, which is equal to a+b+c+d.

$$\text{Kulczynski1} = \frac{a}{b+c}$$

$$\text{Kulczynski2} = 0.5 * \left(\frac{a}{a+b} + \frac{a}{a+c}\right)$$

Braun = If $(a+b) > (a+c)$then

$$\text{Braun} - \text{Blanquet} := \frac{a}{a+b}$$

else

$$\text{Braun} - \text{Blanquet} := \frac{a}{a+c}$$

$$\text{Dice} = 2 * \frac{a}{(2*a+b+c)}$$

$$\text{Ochiai} = \frac{a}{\sqrt{(a+b)*(a+c)}}$$

$$\text{Sokmich} = \frac{a+d}{a+b+c+d}$$

$$\text{Simpson} = \text{If } (a+b) < (a+c) \text{ then}$$

$$\text{Simpson} := \frac{a}{a+b}$$

$$\text{else}$$

$$\text{Simpson} := \frac{a}{a+c}$$

$$\text{Rogers \& Tanimoto} = \frac{(a+d)}{(a+2*(b+c)+d)}$$

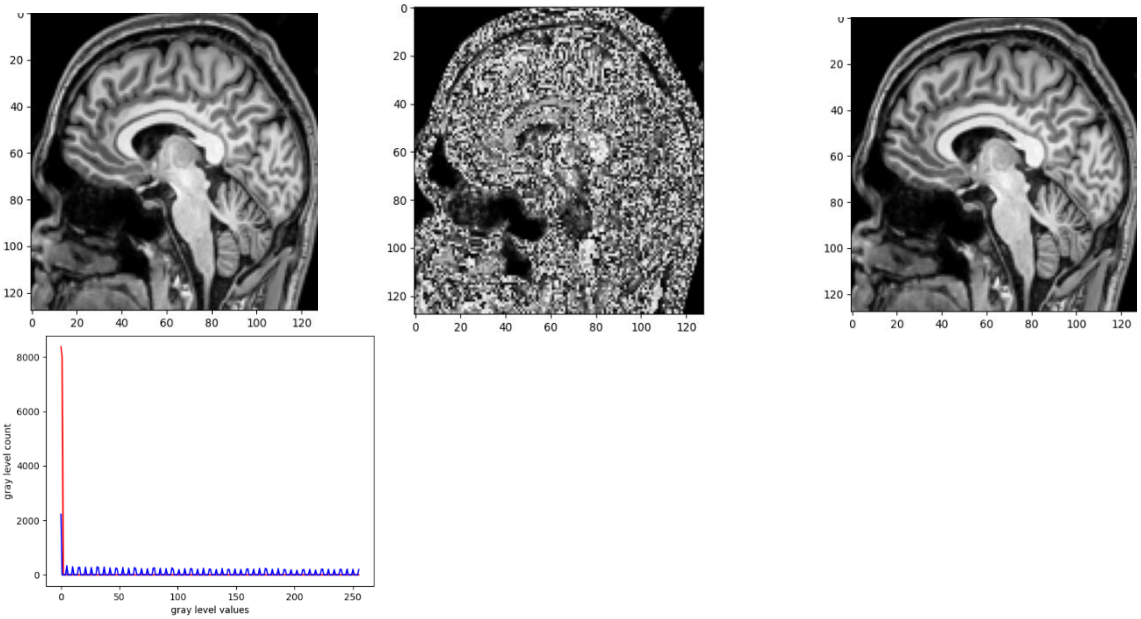
$$\text{Soksneath1} = \frac{a}{(a+2*(b+c))}$$

$$\text{Soksneath2} = 0.25 * \left(\frac{a}{(a+b)} + \frac{a}{(a+c)} + \frac{d}{(b+d)} + \frac{d}{(c+d)}\right)$$

Parameters	Fib-cypher	Golden RT-DNA Cipher
Jaccord	61.18	50.34
kulczynski1	157.62	101.37
kulczynski2	76.79	67.04
dice	75.91807487908282	66.96870846925215
ochiai	76.35	67.0
sokmich	75.38	66.63
rogers	60	50
soksneath1	86	80
soksneath2	44	34

4.2. Time complexity

Size of image	Fib cipher time	Golden RT-DNA Cipher
255X255	103.07418918609619	50.27222967147827



5. Comparison with Existing Encryption Schemes

Feature / Criteria	Fibonacci-Q Matrix Cipher	AES-DNA Hybrid	Chaos-Based Only	Proposed Method (Golden Matrix + Reverse T-DNA + Logistic Map)

Framework Type	Mathematical matrix-based	Symmetric + Bio	Nonlinear chaotic	Hybrid (Algebraic + Chaotic + Bio-inspired)
Key Sensitivity	Moderate	High	High	Very High (Logistic + Lucas Numbers)
Entropy (Typical Values)	7.4 – 7.8	~7.9	~7.8	~7.99
Pixel Correlation (Encrypted Image)	Higher (0.15 – 0.25)	0.01 – 0.04	~0.03	< 0.01
Reversibility	Yes	Partial	Yes	Fully Reversible (RT-DNA CA)
DNA Layer Integration	No	Yes	No	Yes (Dynamic Rule + XOR + T-DNA)
Execution Time (for 255×255 Image)	~103 ms	~70 ms	~85 ms	~50 ms
Resistance to Statistical Attacks	Medium	High	High	Very High
Differential Attack Resistance	Moderate	High	Moderate	High (Due to reverse T-DNA structure)
Flexibility to Image Format and Size	Limited	Moderate	High	High (DNA + Matrix scaling + chaos adaptability)
Novelty of Approach	Well-known method	Moderate	Common	Unique 3-layer encryption scheme

6. CONCLUSION AND FUTURE ENHANCEMENTS

A breakthrough technique for protecting image data is shown by combining the Golden Matrix with Reverse T-DNA image encryption. An organized, mathematical framework for creating pseudo-random sequences that improve encryption is introduced by the Golden Matrix. This is combined with Reverse T-DNA, which employs an encryption technique inspired by biology, to create a system that is more sophisticated and secure. Finally, we achieved enhanced security with greater efficiency and flexibility. Although, Algorithm Optimization and Integration with other security protocols could be improved in the future to increase the encryption scheme's usefulness and efficacy.

REFERENCES

[1] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A modified AES based algorithm for image encryption," World Academy of Science, Engineering and Technology, vol. 3, pp. 526–531, 2007.
[2] N. A. Abbas, "Image encryption based on independent com- ponent analysis and arnold's cat map," Egyptian Informatics Journal, vol. 17, no. 1, pp. 139–146, 2016.
[3] M. Mudia and P. Chavan, "Fuzzy logic based image encryption for confidential data transfer using (2,2) secret sharing scheme," Procedia Computer Science, vol. 78, pp. 632–639, 2016.
[4] L. Li, A. EL-Latif, and X. Niu, "Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images," Signal Processing, vol. 92, no. 4, pp. 1069–1078, 2012.
[5] M. Kumar and A. Vaish, "Encryption of color images using MSVD in DCST domain," Optics and Lasers in Engineering, vol. 88, pp. 51–59, 2017.
[6] J. B. Lima and L. F. G. Novaes, "Image encryption based on the fractional Fourier transform over finite fields," Signal Processing, vol. 94, no. 1, pp. 521–530, 2014.
[7] R.-J. Chen and S.-J. Horng, "Novel SCAN-CA-based image security system using SCAN and 2-D von Neumann cellular automata," Signal Processing: Image Communication, vol. 25, no. 6, pp. 413–426, 2010.
[8] A. Alghafis, F. Firdousi, M. Khan, S.I. Batool, M. Amin, "An efficient image encryption scheme based on chaotic and deoxyribonucleic acid sequencing", Math. Comput. Simulat. 177 pp. 441–466, 2020.

[9] N. Munir, M. Khan, Z. Wei, A. Akgul, M. Amin, I. Hussain, "Circuit Implementation of 3D Chaotic Self-Exciting Single-Disk Homopolar Dynamo and its Application in Digital Image Confidentiality", Wireless Networks, pp. 1–18, 2020.
[10] M. Khan, N. Munir, "A novel image encryption technique based on generalized advanced encryption standard based on field of any characteristic", Wireless Pers. Commun. 109 2, pp. 849–867, 2019.
[11] L. Teng and X. Wang, "A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive," Optics Communications, vol. 285, no. 20, pp. 4048–4054, 2012.
[12] R. Ye, "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism," Optics Communi- cations, vol. 284, no. 22, pp. 5290–5298, 2011.
[13] A. Kumar and M. K. Ghose, "Extended substitution-diffusion based image cipher using chaotic standard map," Communica-tions in Nonlinear Science and Numerical Simulation, vol. 16, no. 1, pp. 372–382, 2011.
[14] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic- adjusted-Sine map," Information Sciences, vol. 339, pp. 237–253, 2016.
[15] C. T. Clelland, V. Risca, and C. Bancroft, "Hiding messages in DNA microdots," Nature, vol. 399, no. 6736, pp. 533–534, 1999.
[16] M. Arita and Y. Ohashi, "Secret signatures inside genomic DNA," Biotechnology Progress, vol. 20, no. 5, pp. 1605–1607, 2004.
[17] M. Lu, X. Lai, G. Xiao, and L. Qin, "Symmetric encryption method based on DNA technique," Science in China E, vol. 37, no. 2, pp. 175–182, 2007 (Chinese).
[18] A. Gehani, T. LaBean, and J. Reif, "DNA-based cryptography," in Aspects of Molecular Computing, vol. 2950 of Lecture Notes in Computer Science, pp. 167–188, Springer, 2004.
[19] A. Leier, C. Richter, W. Banzhaf, and H. Rauhe, "Cryptography with DNA binary strands," BioSystems, vol. 57, no. 1, pp. 13–22, 2000.
[20] K. Halvorsen and W. P. Wong, "Binary DNA nanostructures for data encryption," PLoS ONE, vol. 7, no. 9, Article ID e44212, 2012.
[21] D. Tulpan, C. Regoui, G. Durand, L. Belliveau, and S. Le´ger, "HyDEn: a hybrid steganocryptographic approach for data encryption using randomized error-correcting DNA codes," BioMed Research International, vol. 2013, Article ID 634832, 11 pages, 2013.
[22] L. Qi, X. Wang, B. Ma, X. Wang, C. Wang, S. Gao, Y. Shi, Concealed attack for robust watermarking based on generative model and perceptual loss, IEEE Trans. Circ. Syst. Video Technol. 32 8 pp. 5695–5706, 2021.
[23] M. Alshehri, S. Almakdi, M.A. Qathrady, J. Ahmad, Cryptanalysis of 2D-SCMCI hyperchaotic map based image encryption algorithm, Comput. Syst. Sci. Eng. 46 2 pp. 2401–2414, 2023.