An innovative image encryption scheme integrating chaotic maps, DNA encoding and cellular automata

Gaverchand Kukaram, Venkatesan Ramasamy, Yasmin Abdul
Department of Mathematics, College of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur, India

Article Info

Article history:

Received Aug 29, 2024
Revised Mar 14, 2025
Accepted Mar 26, 2025

Keywords:

Cellular automata
Chaotic map
DNA cryptography
Image encryption
Statistical analysis

ABSTRACT

In the current digital era, securing image transmission is crucial to ensure data integrity, prevent tampering, and preserve confidentiality as images traverse unsecured channels. This paper presents an innovative encryption scheme that synergistically combines a two-dimensional (2-D) logistic map, deoxyribonucleic acid (DNA) encoding, and 1-D cellular automata (CA) rules to significantly bolster encryption robustness. The proposed model initiates with the generation of a key image via the 2-D logistic map, yielding intricate chaotic sequences that fortify the encryption mechanism. DNA cryptography is employed to amplify randomness through diffusion properties, providing robust defense against various cryptographic attacks. The integration of 1-D CA rules further intensifies encryption complexity by iteratively processing DNA-encoded sequences. Experimental results substantiate that the proposed encryption scheme demonstrates exceptional endurance against a vast spectrum of attacks, affirming its superior security.

Corresponding Author:

Venkatesan Ramasamy
Department of Mathematics, College of Engineering and Technology
SRM Institute of Science and Technology
Kattankulathur 603203, Tamil Nadu, India
Email: venkater1@srmist.edu.in

1. INTRODUCTION

In the digital age, securing sensitive information transmitted over the internet is critical, especially for digital images that are vulnerable to unauthorized access. The risk of interception and exploitation during transmission underscores the need for effective image encryption [1]-[3]. Traditional encryption methods such as advanced encryption standard (AES), data encryption standard (DES), and Rivest-Shamir-Adleman (RSA) often fail to maintain critical properties of encrypted images, including low pixel correlation and high randomness, and may not fully address various security threats and robustness requirements [4]. To address these limitations, the proposed research introduces a novel encryption scheme that integrates chaotic maps, deoxyribonucleic acid (DNA) cryptography, and cellular automata (CA). This innovative approach aims to significantly enhance the robustness and effectiveness of image encryption, addressing contemporary security challenges with novel strategies.

Chaos theory has recently emerged as a powerful method for secure image encryption [5], [6], due to its sensitivity to initial conditions, deterministic behavior, and ergodicity [7]. These traits make chaos-based cryptosystems highly resistant to attacks. Multi-dimensional chaotic maps are preferred for their complex architectures and numerous parameters, which enhance encryption strength by complicating prediction and reverse-engineering [8]. However, this increased security brings greater computational complexity, requiring a balance between security and practical implementation. The proposed methodology employs the two-dimensional (2-D) logistic map to generate highly unpredictable sequences through chaotic dynamics, significantly bolstering encryption robustness and resisting unauthorized decryption attempts.

The advent of DNA computing has led to the emergence of DNA cryptography, utilizing DNA for information storage and biological technologies for its implementation [9], [10]. Adleman’s 1994 experiment laid the foundation for this approach, marking a pivotal advancement in information technology. DNA computing's exceptional capabilities, including extensive parallelism, vast storage potential, and low energy consumption, have inspired DNA-based image encryption methods [11]-[13]. In the proposed scheme, DNA cryptography bolsters encryption by leveraging DNA's high information density and biochemical complexity, significantly enhancing randomness and providing robust protection against brute-force and statistical attacks.

In the 1950s, John von Neumann and Stanislaw Ulam developed CA as mathematical models to explore complex systems through simple, local interactions. Despite their simplicity, CA exhibits remarkable complexity, making them effective tools for simulating natural processes and enhancing cryptographic security [14]. Jin *et al.* [15] proposed an image encryption scheme using an 8-length CA and state attractors, achieving effective confusion and diffusion with minimal computational resources. CA has become instrumental in generating random sequences for image encryption, with two primary methods: one uses CA to produce pseudo-random numbers, while the other encrypts images at the bit level, leveraging CA's chaotic behavior [16]. In the proposed scheme, CA iteratively processes DNA-encoded binary sequences, amplifying encryption complexity. Extensive research continues to advance image encryption using techniques like chaotic systems, quantum logistic maps, DNA computing, and CA. The subsequent review offers an analysis of innovative approaches in this field.

Li *et al.* [17] developed an encryption method using chaotic maps and CA to enhance security through diffusion, permutation, and scrambling, but it may suffer from high computational demands. Chai *et al.* [18] proposed a scheme integrating a memristive hyperchaotic system, CA, and DNA, driven by the plain image, achieving strong security with dynamic DNA encoding and block diffusion. However, its dependence on unique DNA rules may limit adaptability to various image types. Nandi *et al.* [19] designed an image encryption method with 1-D CA in a symmetric key framework, leveraging cyclic properties for efficiency, though its simplicity might make it vulnerable to advanced attacks.

Mondal *et al.* [20] developed a robust image encryption method using a chaotic skew tent map and CA, ensuring secure communication and storage with a large key space and effective pseudo-random sequences. However, managing extensive key spaces and key management may limit its effectiveness. Niyat *et al.* [21] created a novel strategy combining DNA, CA, and chaotic systems for pixel encryption using DNA rules, XOR operations, and CA rules. Although it provides a substantial key space and low pixel correlation, its complexity may hinder practical implementation. Liu *et al.* [22] proposed an advanced encryption scheme using DNA encoding and chaotic maps for pixel confusion and diffusion. Despite its strong encryption performance and large key space, practical implementation is complicated by multiple transformations. Li *et al.* [23] proposed a technique using a 5-D multi-wing hyper-chaotic system for enhanced security through pixel-level and bit-level permutations and diffusion. However, reliance on hyper-chaotic systems and permutations may introduce complexities and limitations in robustness.

Lone *et al.* [24] developed an image encryption procedure integrating DNA methods with three-dimensional chaos maps, employing complex diffusion and scrambling techniques. It demonstrates superior encryption performance and enhanced key sensitivity through extensive validation. Alkhonaini *et al.* [25] created a technique combining two-way chaotic maps with reversible CA, improving key space and sensitivity. Their approach uses spatiotemporal chaos for pixel permutation and reversible CA for bit-level modification, showing strong resistance to various attacks. Zhang *et al.* [26] developed an encryption technique combining DNA sequences with chaotic maps for pixel diffusion and confusion through iterative transformations. Despite its efficacy, the method faces challenges due to complexity, computational demands, and potential vulnerabilities. Samiullah *et al.* [27] introduced a symmetric encryption algorithm for color images using three chaotic systems, a secure hash algorithm, and a DNA sequence-based linear feedback shift register to enhance diffusion and confusion.

The preceding analysis assessed the pros and cons of image encryption techniques utilizing chaotic maps, CA, and DNA computing. Existing methods face challenges such as susceptibility to statistical attacks, high pixel correlation, low entropy, inadequate avalanche resistance, large key spaces, weak transmission security, and insufficient error handling. This paper presents a sophisticated encryption strategy integrating a 2-D logistic map, DNA encoding, and 1-D CA rules to address these limitations and bolster robustness. The 2-D logistic map strengthens key image generation with complex chaotic sequences, enhancing encryption efficacy. DNA cryptography boosts randomness and resists statistical and avalanche attacks. Additionally, 1-D CA rules increase encryption complexity and pixel disparity, making unauthorized decryption more difficult. Finally, error correction is implemented through forward error correction (FEC) for both key and encrypted images, while security is ensured via the receiver's public key, guaranteeing that only the intended recipient can decrypt the data. This model directly mitigates susceptibility to statistical attacks and high pixel correlation through chaotic sequences and DNA encoding, while 1-D CA rules enhance entropy and avalanche resistance. Moreover, FEC improves error handling, and secure transmission is ensured by the receiver's public key.

This paper is structured as follows: section 2 delivers an extensive review of chaos theory, DNA cryptography, 1-D CA, and FEC. Section 3 delineates the proposed image encryption methodology and associated algorithms. Section 4 offers a thorough evaluation and analysis of the outcomes derived from the proposed scheme. Section 5 provides a conclusive summary, encapsulating the core contributions of the study.

2. PRELIMINARIES

2.1. Chaotic maps

Chaos theory [28], [29] emphasizes two essential properties: nonlinearity and dynamical behavior. In the logistic map, nonlinearity arises from feedback mechanisms, while dynamical behavior signifies the system's evolution. The 1-D logistic map, expressed as,

$$x_{n+1} = r \cdot x_n \cdot (1 - x_n)$$

where $r \in (0,4]$ is the control parameter, and x_n represents the system state at iteration n. While this map generates sequences within $[0,1]$ and exhibits chaotic behavior for $r > 3.57$, its simplicity limits its suitability for cryptographic applications requiring greater complexity.

The 2-D logistic map addresses these limitations by introducing additional complexity via coupled equations and a perturbation factor. It is defined by:

$$x_{\{n+1\}} = r \cdot x_n \cdot (1 - x_n) + z_0$$

$$y_{\{n+1\}} = r \cdot y_n \cdot (1 - y_n) + z_0$$

in the 2-D logistic map, x_n and y_n represent the system's states at iteration n, with r as the control parameter and z_0 functioning as a perturbation factor. The incorporation of y_n, along with the perturbation z_0, introduces greater complexity by continually altering the trajectories of both variables, preventing stabilization into fixed points or periodic orbits and promoting chaotic behavior.

Though derived from the 1-D model, the interaction between the two dimensions and the perturbation factor substantially enhances the system's dynamical properties, resulting in more intricate and unpredictable behavior. The 2-D logistic map exhibits bifurcation patterns, with fixed points for $r \in (0,3]$, periodic attractors for $r \in (3,3.57]$, and chaos for $r > 3.57$. Figure 1 depict the bifurcation diagram of 2-D logistic map. The proposed scheme employs $r = 3.999$ for secure key image generation, leveraging its increased complexity and chaotic characteristics.

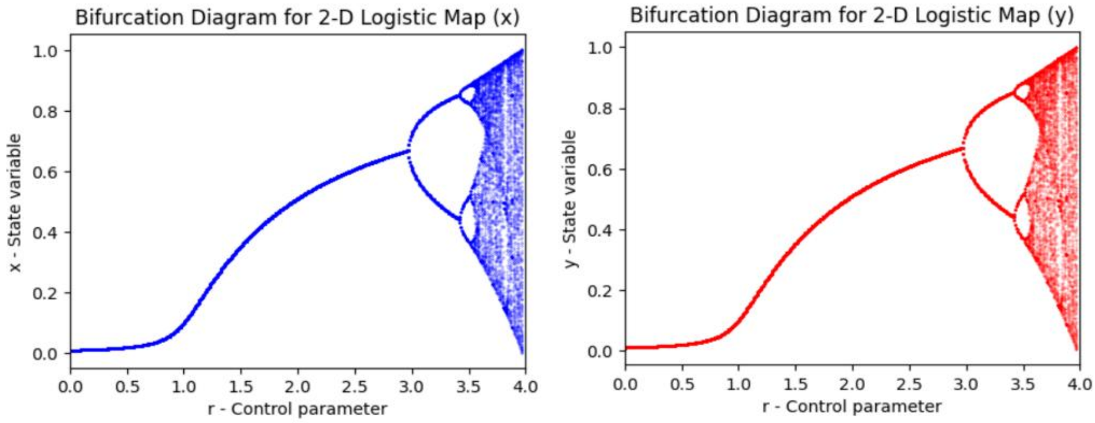


Figure 1. Bifurcation diagram for 2-D logistic map

2.2. DNA cryptography

DNA cryptography leverages the inherent properties of DNA sequences to bolster data security [30], [31]. A DNA sequence consists of four nucleic acid bases, adenine (A), guanine (G), cytosine (C), and thymine (T). In DNA, adenine bonds with thymine (A-T), while guanine bonds with cytosine (G-C), reflecting a complementary relationship analogous to binary digits (0 and 1). In the proposed scheme, binary pixel values from both the plain and key images are encoded into DNA nucleotides, with mappings defined as: 00 to A, 01 to C, 10 to G, and 11 to T. The fusion of these images is achieved using the XOR table presented in Table 1, resulting in a unified image. Utilizing DNA encoding, coupled with the XOR operation, introduces a higher level of complexity and obfuscation, enhancing resistance to cryptanalysis techniques. This method not only diversifies the encoding approach but also strengthens encryption, significantly bolstering resistance to decryption efforts. Consequently, integrating DNA encoding with XOR significantly augments security, robustness, and the overall integrity and confidentiality of the data through intricate transformation processes.

Table 1. DNA XOR table

XOR	A (00)	C (01)	G (10)	T (11)
A (00)	A	C	G	T
C (01)	C	A	T	G
G (10)	G	T	A	C
T (11)	T	G	C	A

2.3. Cellular automata

CA are mathematical models distinguished by discrete, quantized time, states, and space, with cells organized in a regular, finite lattice [32], [33]. Formally, CA are described by the five-tuple (L, Q, N, δ, I), where L is the lattice, Q represents the finite set of states, N denotes the neighbors, δ is the transition function, and I indicates the initial state. In elementary CA, or 1-D CA, cells are arranged linearly, with each cell updating its state according to local rules determined by its present state and the states of its neighboring cells. Every cell has two distinct states (0 or 1), results in $2^3 = 8$ unique neighborhood configurations and $2^8 = 256$ distinct transition rules. The CA model can incorporate different boundary conditions, such as periodic boundaries, where the lattice edges connect seamlessly to form a continuous grid, and null boundaries, where edge cells are fixed to simplify boundary interactions. The transition function of CA is determined by:

$$S_{t+1}^{(x)} = f\left(S_t^{(x-1)}, S_t^{(x)}, S_t^{(x+1)}\right)$$

where, $S_{t+1}^{(x)}$ represents the state of cell x at the subsequent time step $t+1$. At present time step $t,$ the cell x is represented by $S_t^{(x)}$, while $S_t^{(x-1)}$ and $S_t^{(x+1)}$ correspond to the states of the neighbouring cells to the left and right respectively. In the proposed scheme, a 1-D CA with periodic boundary conditions is utilized to process binary values through eight specific rules: 30, 86, 90, 101, 105, 150, 153, and 165, as detailed in Table 2. These rules have been demonstrated to enhance essential evaluative metrics such as entropy, pixel disparity, and Diehard test results, thereby increasing the complexity and chaotic nature of the encryption process [34]. The varied transition behaviors of these rules improve unpredictability and diffusion, which strengthens the system's defense against cryptanalytic attacks.

Table 2. Boolean expression of CA rules

No	Rule	Logical operations
1	30	$S_{t+1}^{(x)} = S_t^{(x-1)} + \left[S_t^{(x)} \vee S_t^{(x+1)}\right]$
2	86	$S_{t+1}^{(x)} = S_t^{(x+1)} + \left[S_t^{(x-1)} \vee S_t^{(x)}\right]$
3	90	$S_{t+1}^{(x)} = S_t^{(x-1)} + S_t^{(x+1)}$
4	101	$S_{t+1}^{(x)} = \left[\overline{S_t^{(x-1)}} \vee S_t^{(x)}\right] + S_t^{(x+1)}$
5	105	$S_{t+1}^{(x)} = \overline{S_t^{(x-1)} + S_t^{(x)} + S_t^{(x+1)}}$
6	150	$S_{t+1}^{(x)} = S_t^{(x-1)} + S_t^{(x)} + S_t^{(x+1)}$
7	153	$S_{t+1}^{(x)} = \overline{S_t^{(\mathrm{x})} + S_t^{(x+1)}}$
8	165	$S_{t+1}^{(x)} = \overline{S_t^{(x-1)} + S_t^{(x+1)}}$

2.4. Forward error correction

FEC [35], [36] is a robust error control technique that integrates redundant error-correcting codes into transmitted data, allowing the receiver to detect and correct errors without retransmission. This method enhances transmission reliability by minimizing the need for receiver feedback while preserving data integrity in high-error environments. FEC techniques are classified into two categories. Block codes, which partition data into fixed-size blocks and add redundant bits for error correction, and convolutional codes, which encode data streams using memory-based techniques.

In the proposed model, Reed-Solomon codes from block codes are applied to the key image and encrypted image to bolster its resilience against errors. These codes are crucial for correcting burst errors that may arise during transmission or storage, thereby ensuring the integrity of the key image. By protecting the key image from potential corruption, Reed-Solomon codes [37] enhance the reliability of both encryption and decryption processes, as inaccuracies in the key could jeopardize the system's security. This integration ensures a robust cryptographic scheme by maintaining the accuracy and stability of the key image.

3. PROPOSED METHOD

This section elucidates a sophisticated approach that integrates a 2-D logistic map, DNA encoding, and 1-D CA rules to significantly bolster image encryption. The model is comprised of three core components: the plain image, a key image, and the resulting encrypted image. In this model, the original image, with dimensions $m \times n$ (where m and n may either be equivalent or distinct), is initially processed to generate a key image through a 2-D logistic map. The key image is then transformed into DNA codons and used to scramble the original image by exploiting the confusion property during the initial phase. To further intensify randomness and security, 1-D CA rules are applied to iterate the image pixels during the encryption process. To ensure the integrity of both the key image and the encrypted image during transmission, Reed-Solomon codes are meticulously integrated. These codes effectively detect and rectify transmission errors, thereby safeguarding the data's reliability. After Reed-Solomon codes is applied, both the key image and the encrypted image are encrypted using the receiver's public key, ensuring robust confidentiality throughout the transmission. This encryption strategy guarantees superior security and significantly enhances the resilience of the proposed model throughout the process.

3.1. Key generation process

The key image generation process employs both the SHA-256 hash function and the 2-D logistic map to ensure robust security throughout [38]. By leveraging the cryptographic strength of SHA-256 and the unpredictability of chaotic systems, the generated key image is obfuscated and protected against unauthorized access. The process commences with a plain image of dimensions $m \times n$. The SHA-256 hash function [39], renowned for its cryptographic resilience and consistent output size, is exploited to derive a 256-bit hash from the plain image. This hash is transmuted into a binary string and segmented into four 64-bit portions, denoted as $B = (b_1, b_2, b_3, b_4)$. The binary string segments undergo additional obfuscation through key expansion, dispersing entropy across the key image to fortify its randomness. The initial parameters for the 2-D logistic map are determined as follows, x_0 is acquired by converting b_1 from binary to decimal and subsequently scaling it by 10^{-64}; y_0 is similarly derived from b_2 and z_0 is ascertained as the mean of the decimal conversions of b_3 and b_4, also scaled by 10^{-64}. To ensure an optimally complex chaotic sequence, the 2-D logistic map is iterated up to $[(m \times n) \, mod \, 13 + 10]$ times. This dynamic iteration count, based on the image size, balances chaotic intricacy with computational efficiency. The resulting chaotic sequence is mapped to pixel values, culminating in a key image that precisely aligns with the dimensions of the original image. This key image is pivotal to the encryption process, offering robust security and resilience against attacks while ensuring the data's protection in Algorithm 1.

Algorithm 1. Key image generation

```
Input: Original Images $I$ with dimensions $m \times n$
Output: Key Image $K$ with dimensions $m \times n$
1. Consider the image $I$ as input
2. Compute SHA-256 hash
        • Hash =SHA-256 $(I)$, where Hash is a 256-bit binary sequence
3. Extract Hash Segments
        • $B = (b_1, b_2, b_3, b_4)$, where $b_i$ are the 64-bit segments of Hash
4. Initialize 2-D Logistic Map Parameters
        • $x_0 = Dec(b_1) \times 10^{-64}$
        • $y_0 = Dec(b_2) \times 10^{-64}$
        • $z_0 = \left(\frac{Dec(b_3)+Dec(b_4)}{2}\right) \times 10^{-64}$
```

```
5.  Determine Iteration Count
        •  To ensure chaotic behavior, the number of iterations $i$ is
             ❖  $i = [(m \times n) mod 13] + 10$
6.  Iterate 2D Logistic Map
        •  For $n = 0\ to\ i$
             ❖  $x_{n+1} = r \cdot x_n \cdot (1 - x_n) + z_0$
             ❖  $y_{n+1} = r \cdot y_n \cdot (1 - y_n) + z_0$
Where, $r = 3.999$ is the logistic map parameter and $z_0$ is the perturbation factor

7.  Map Chaotic Sequence to pixel values
      •  For pixel $(i,j)$
           ❖  $K(i,j) = [255 \times (x_n mod 1)]$
8.  Resultant key image $K$ of size $m \times n$
```

3.2. Encryption and decryption

The encryption procedure initiates with the plain image I and the key image K, both of dimensions $m \times n$. Each pixel is transformed into binary sequences I_b and K_b, which are then encoded into DNA sequences I_{DNA} and K_{DNA} using a sophisticated DNA mapping. This encoding process provides a further level of complexity and randomness by translating each 2-bit binary data into nucleotide sequences. An XOR operation is subsequently performed between I_{DNA} and K_{DNA}, resulting in the fused DNA sequence E_{DNA} by employing the XOR table from Table 1, which merges data from both images to enhance security. The sequence E_{DNA} is then decoded back into binary form as E_b and partitioned into eight segments. Each segment undergoes processing through CA rules (30, 153, 90, 165, 86, 105, 101, and 150) for $[(m \times n) mod 13 + 10]$ iterations, introducing significant complexity and chaotic behavior that strengthen the encryption. This iterative CA processing ensures that even minor variations in the input result in substantial alterations in the output, thus enhancing the encryption's robustness. Finally, the processed binary sequence E_{CA} is converted back into pixel values, resulting in the encrypted image E with dimensions $m \times n$. To reverse the process, the encrypted image E is decoded by applying the inverse CA rules, followed by performing an XOR with the key image K. The final output is then decoded from DNA sequences back to binary form, accurately reconstructing the original image I of size $m \times n$. This multi-faceted encryption strategy comprising binary conversion, DNA encoding, XOR operation, and CA processing ensures a high degree of resilience and security in Algorithm 2. Figure 2 outlines the workflow of the proposed method.

Algorithm 2. Encryption algorithm

```
**Input:** Plain Image $I$ with dimension $m \times n$; Key Image $K$ with dimension $m \times n$
**Output:** Encrypted Image $E$ with dimensions $m \times n$
1.  Consider the images $I$ and $K$ as input
2.  Convert each pixel in $I$ and $K$ to their binary representations $I_b$ and $K_b$
3.  Encode $I_b$ and $K_b$ into DNA sequences $I_{DNA}$ and $K_{DNA}$
4.  Compute the XOR operation of $I_{DNA}$ and $K_{DNA}$ to obtain $E_{DNA}$ using Table 1
5.  Decode the DNA sequence $E_{DNA}$ back to binary sequence $E_b$ by inverse DNA encoding
6.  CA Processing
      •  Divide $E_b$ into eight segments $n_1, n_2, \ldots, n_s$each containing $\frac{|E_b|}{8}$bits
      •  Iterate each segment $n_1$ through $n_8$ using CA Rules 30, 86, 90, 101, 105, 150, 153 and
         165 respectively for $[(m \times n) mod 13 + 10]$ iterations.
      •  Combine the processed segments to form the refined binary sequence $E_{CA}$
7.  Transform $E_{CA}$ into pixel values to generate the encrypted image $E$
8.  Resultant encrypted image $E$ of size $m \times n$
```

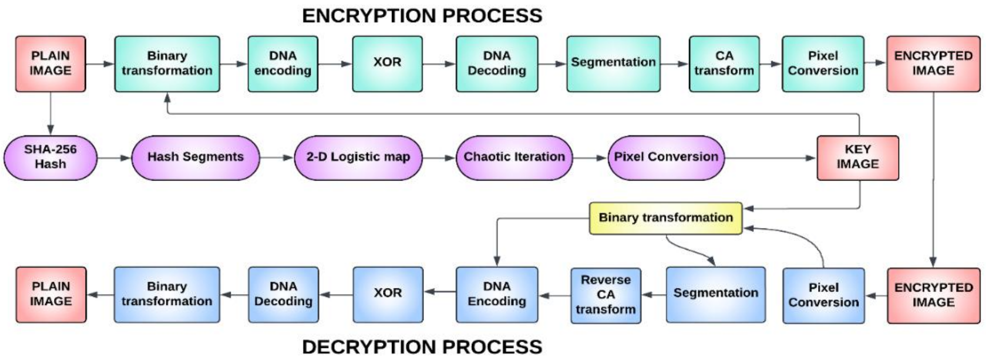


Figure 2. Workflow of the proposed scheme

4. RESULTS AND DISCUSSIONS

This section outlines a series of experiments to evaluate the performance metrics of the proposed encryption approach using high-resolution RGB images. Three different images were utilized: (a) Lena, (b) Airplane, and (c) Splash, each measuring 512×512 pixels. These images were sourced from the University of Waterloo Image Repository [40], and the evaluations were conducted using MATLAB on a Dell laptop equipped with a 12th-generation Intel Core i5 processor and a 128 GB SSD. The outcomes of the experiments will be presented in the following sections.

a) Statistical analysis: an ideal encryption method should resist statistical attacks by maintaining an even distribution of grayscale values in histograms and ensuring low correlations among neighboring pixels. Table 3 shows that the encrypted images of the proposed scheme display smoother and more evenly distributed patterns, enhancing the robustness of the proposed technique, and Table 4 assesses the correlation in the proposed model by randomly considering 3,000 pairs of neighboring pixels in the encrypted images. The results show that the values are approximately zero, indicating minimal relationship between the plain and encrypted images and demonstrating the model's effectiveness.

b) Analysis of information entropy: entropy analysis evaluates the randomness of pixel values in an encrypted image, with a value approaching 8 indicating superior encryption and reflecting maximal uncertainty.

c) Analysis of avalanche effect: the avalanche effect in image encryption ensures that minor modifications in the original or key image cause extensive, unpredictable changes in the encrypted image, enhancing security. NPCR measures the proportion of pixel changes, while UACI evaluates the mean intensity variation between two cipher images due to slight modifications.

d) Analysis of pixel disparity: pixel disparity analysis evaluates discrepancies between plain and cipher images, which is crucial for assessing encryption efficacy and is measured using two metrics: mean squared error (MSE), which quantifies the average squared differences between corresponding pixels, and peak signal-to-noise ratio (PSNR), which measures the ratio of the optimal pixel value to the MSE.

The evaluations for tests 2 to 4, encompassing entropy, NPCR, UACI, MSE, and PSNR for the proposed model, have been rigorously compared against existing image encryption techniques, as detailed in Table 5. The proposed model exhibits exceptionally high entropy, indicative of robust encryption randomness, while its UACI and NPCR metrics reflect a strong avalanche effect. Furthermore, the model's MSE and PSNR values demonstrate a balance between encryption strength and minimal degradation in image quality. Consequently, Table 5 highlights that the proposed scheme excels across all these metrics, surpassing the performance of other models.

Table 3. Histogram analysis of the proposed scheme

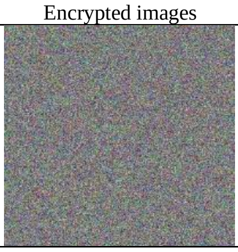
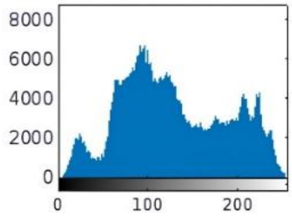
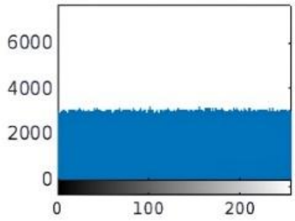
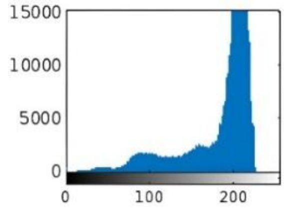
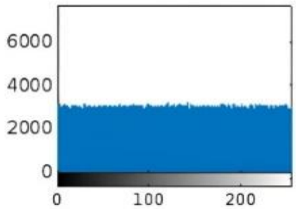
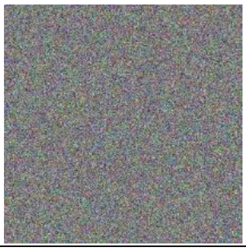
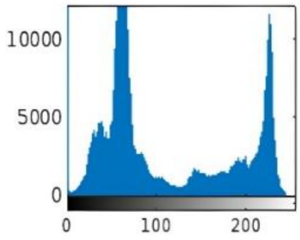
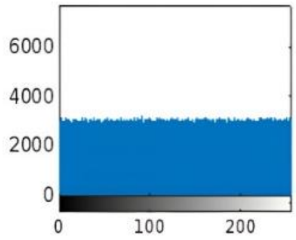
Original images	Encrypted images	Histogram of original images	Histogram of encrypted images
			
			
			

Table 4. Analysis of correlation coefficient among adjacent pixels

Image	Horizontal	Vertical	Diagonal
Lena	0.0063	0.0051	-0.0005
Airplane	0.0017	-0.0024	0.0009
Splash	0.0049	0.0034	-0.0021

Table 5. Comparative analysis of entropy, NPCR, UACI, MSE, and PSNR

Test	Images	Proposed	Ref [20]	Ref [27]	Ref [24]	Ref [21]	Ref [28]
Entropy	Lena	7.9987	7.9858	7.9875	7.8457	7.9964	7.9913
	Airplane	7.9991	7.9702	7.9736	7.7965	7.9979	7.9935
	Splash	7.9983	7.9494	7.8923	7.6820	7.9975	7.9921
NPCR	Lena	99.5285	97.5261	98.2731	99.2197	98.5326	98.4663
	Airplane	99.3694	96.4862	99.1564	98.0382	98.9258	99.1435
	Splash	99.5987	96.9136	99.2955	98.7936	98.3260	99.5347
UACI	Lena	37.7956	34.9351	29.4738	33.9375	36.5789	34.6453
	Airplane	36.8363	35.2673	32.7957	39.9824	35.8221	34.8235
	Splash	39.3737	35.9368	33.9614	35.5683	37.2615	35.2867
MSE	Lena	90.95	84.91	87.37	89.12	88.28	87.26
	Airplane	95.78	89.38	94.91	92.48	91.79	86.33
	Splash	93.93	92.17	92.52	97.31	91.42	85.78
PSNR	Lena	34.58	27.38	33.72	30.22	28.54	29.37
	Airplane	33.93	32.17	28.35	29.93	26.30	31.84
	Splash	34.81	28.49	35.84	32.16	27.47	32.93

5. CONCLUSION

Based on the experimental results, the proposed scheme demonstrates promising outcomes through the integration of DNA cryptography, a 2-D logistic map, and CA rules for real-time image encryption and decryption. The analysis of three distinct images revealed robust performance across statistical, entropy, avalanche, and pixel disparity metrics, with optimal entropy results near 7.99, an average NPCR of 99.49, UACI of 38.00, PSNR of 25.57, and MSE of 81.58, underscoring its strength and effectiveness. To ensure data integrity, Reed-Solomon codes were applied to both the key and cipher images, preventing retransmission and maintaining confidentiality through encryption using the receiver's public key. However, while the proposed model demonstrates superior efficacy in encrypting RGB images, future work will aim to adapt it for the simultaneous encryption of multiple images, assess its resilience against noise perturbations, and integrate quantum cryptography to further enhance security.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Gaverchand Kukaram	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Venkatesan Ramasamy		✓			✓	✓		✓	✓	✓	✓	✓	✓	
Yasmin Abdul	✓		✓	✓		✓	✓		✓	✓	✓		✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis

I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting

Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, upon reasonable request.

REFERENCE

[1] Y. Wang, Y. Zhao, Q. Zhou, and Z. Lin, "Image encryption using partitioned cellular automata," *Neurocomputing*, vol. 275, pp. 1318–1332, Jan. 2018, doi: 10.1016/j.neucom.2017.09.068.

[2] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an elliptic curve," *Signal Processing*, vol. 155, pp. 391–402, Feb. 2019, doi: 10.1016/j.sigpro.2018.10.011.

[3] M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," *Archives of Computational Methods in Engineering*, vol. 27, no. 1, pp. 15–43, Nov. 2018, doi: 10.1007/s11831-018-9298-8.

[4] X. Wang, L. Feng, and H. Zhao, "Fast image encryption algorithm based on parallel computing system," *Information Sciences*, vol. 486, pp. 340–358, Jun. 2019, doi: 10.1016/j.ins.2019.02.049.

[5] Y. Luo, R. Zhou, J. Liu, S. Qiu, and Y. Cao, "An efficient and self-adapting colour-image encryption algorithm based on chaos and interactions among multiple layers," *Multimedia Tools and Applications*, vol. 77, no. 20, pp. 26191–26217, Mar. 2018, doi: 10.1007/s11042-018-5844-5.

[6] Y. Zhang and Y. Tang, "A plaintext-related image encryption algorithm based on chaos," *Multimedia Tools and Applications*, vol. 77, no. 6, pp. 6647–6669, Apr. 2017, doi: 10.1007/s11042-017-4577-1.

[7] G. Maddodi, A. Awad, D. Awad, M. Awad, and B. Lee, "A new image encryption algorithm based on heterogeneous chaotic neural network generator and DNA encoding," *Multimedia Tools and Applications*, vol. 77, no. 19, pp. 24701–24725, Feb. 2018, doi: 10.1007/s11042-018-5669-2.

[8] A. H. Alrubaie, M. A. A. Khodher, and A. T. Abdulameer, "Image encryption based on 2DNA encoding and chaotic 2D logistic map," *Journal of Engineering and Applied Science*, vol. 70, no. 1, Jun. 2023, doi: 10.1186/s44147-023-00228-2.

[9] E. Z. Zefreh, "An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions," *Multimedia Tools and Applications*, vol. 79, no. 33–34, pp. 24993–25022, Jun. 2020, doi: 10.1007/s11042-020-09111-1.

[10] P. T. Akkasaligar and S. Biradar, "Selective medical image encryption using DNA cryptography," *Information Security Journal a Global Perspective*, vol. 29, no. 2, pp. 91–101, Feb. 2020, doi: 10.1080/19393555.2020.1718248.

[11] A. Theramban and R. V. Ravi, *Colour image encryption using DNA coding and logistic diffusion*. IEEE Fourth International Conference on Microelectronics, Signals and Systems (ICMSS), 2021. Doi: 10.1109/icmss53060.2021.9673628.

[12] Q. Zhang, L. Guo, and X. Wei, "Image encryption using DNA addition combining with chaotic maps," *Mathematical and Computer Modelling*, vol. 52, no. 11–12, pp. 2028–2035, Dec. 2010, doi: 10.1016/j.mcm.2010.06.005.

[13] B. Rahul, K. Kuppusamy, and A. Senthilrajan, "Dynamic DNA cryptography-based image encryption scheme using multiple chaotic maps and SHA-256 hash function," *Optik*, vol. 289, p. 171253, Oct. 2023, doi: 10.1016/j.ijleo.2023.171253.

[14] J. -l. Beuchat and J. O. Haenni, "Von Neumann's 29-state cellular automaton: a hardware implementation," *IEEE Transactions on Education*, vol. 43, no. 3, pp. 300–308, Jan. 2000, doi: 10.1109/13.865205.

[15] J. Jin, "An image encryption based on elementary cellular automata," *Optics and Lasers in Engineering*, vol. 50, no. 12, pp. 1836–1843, Dec. 2012, doi: 10.1016/j.optlaseng.2012.06.002.

[16] S. Roy, M. Shrivastava, U. Rawat, C. V. Pandey, and S. K. Nayak, "IESCA: an efficient image encryption scheme using 2-D cellular automata," *Journal of Information Security and Applications*, vol. 61, p. 102919, Sep. 2021, doi: 10.1016/j.jisa.2021.102919.

[17] L. Li, Y. Luo, S. Qiu, X. Ouyang, L. Cao, and S. Tang, "Image encryption using chaotic map and cellular automata," *Multimedia Tools and Applications*, vol. 81, no. 28, pp. 40755–40773, May 2022, doi: 10.1007/s11042-022-12621-9.

[18] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," *Signal Processing Image Communication*, vol. 52, pp. 6–19, Mar. 2017, doi: 10.1016/j.image.2016.12.007.

[19] S. Nandi, S. Roy, S. Nath, S. Chakraborty, W. B. A. Karaa, and N. Dey, "1-D Group Cellular Automata based Image Encryption technique," *IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies*, 2014. doi: 10.1109/iccicct.2014.6993017.

[20] B. Mondal, S. Singh, and P. Kumar, "A secure image encryption scheme based on cellular automata and chaotic skew tent map," *Journal of Information Security and Applications*, vol. 45, pp. 117–130, Apr. 2019, doi: 10.1016/j.jisa.2019.01.010.

[21] A. Y. Niyat, R. M. H. Hei, and M. V. Jahan, "Chaos-based image encryption using a hybrid cellular automata and a DNA sequence," *IEEE International Congress on Technology, Communication and Knowledge*, 2015. doi: 10.1109/ictck.2015.7582678.

[22] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Applied Soft Computing*, vol. 12, no. 5, pp. 1457–1466, May 2012, doi: 10.1016/j.asoc.2012.01.016.

[23] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Optics and Lasers in Engineering*, vol. 90, pp. 238–246, Mar. 2017, doi: 10.1016/j.optlaseng.2016.10.020.

[24] P. N. Lone, D. Singh, and U. H. Mir, "Image encryption using DNA coding and three-dimensional chaotic systems," *Multimedia Tools and Applications*, vol. 81, no. 4, pp. 5669–5693, Dec. 2021, doi: 10.1007/s11042-021-11802-2.

[25] M. A. Alkhonaini, E. Gemeay, F. M. Z. Mahmood, M. Ayari, F. A. Alenizi, and S. Lee, "A new encryption algorithm for image data based on two-way chaotic maps and iterative cellular automata," *Scientific Reports*, vol. 14, no. 1, Jul. 2024, doi: 10.1038/s41598-024-64741-x.

[26] J. Zhang, D. Fang, and H. Ren, "Image encryption algorithm based on DNA encoding and chaotic maps," *Mathematical Problems in Engineering*, vol. 2014, pp. 1–10, Jan. 2014, doi: 10.1155/2014/917147.

[27] M. Samiullah *et al.*, "An image encryption scheme based on DNA computing and multiple chaotic systems," *IEEE Access*, vol. 8, pp. 25650–25663, Jan. 2020, doi: 10.1109/access.2020.2970981.

[28] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Optics and Lasers in Engineering*, vol. 78, pp. 17–25, Mar. 2016, doi: 10.1016/j.optlaseng.2015.09.007.

[29] H. Tabti *et al.*, "Novel cryptosystem integrating the Vigenere cipher and one Feistel round for color image encryption," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 5, 5701, 2024, doi: 10.11591/ijece.v14i5.pp5701-5714

[30] S. Paul, P. Dasgupta, P. Naskar, and A. Chaudhuri, "Secured image encryption scheme based on DNA encoding and chaotic map," *Review of Computer Engineering*, vol. 4, no. 2, pp. 70–75, doi: 10.18280/rces.040206.

[31] J. G. Sekar, E. Periyathambi, and A. Chokkalingam, "Hybrid chaos-based image encryption algorithm using Chebyshev chaotic map with deoxyribonucleic acid sequence and its performance evaluation," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 6, p. 6952, 2023, doi: 10.11591/ijece.v13i6.pp6952-6963.

[32] J. Kari, "Theory of cellular automata: A survey," *Theoretical Computer Science*, vol. 334, no. 1–3, pp. 3–33, Apr. 2005, doi: 10.1016/j.tcs.2004.11.021.

[33] G. Kukaram and V. Ramasamy, "A novel approach of 1-D cellular automata in Cryptosystem," *Mathematical Modelling and Engineering Problems*, vol. 10, no. 6, pp. 2121–2126, Dec. 2023, doi: 10.18280/mmep.100623.

[34] F. Seredynski, P. Bouvry, and A. Y. Zomaya, "Cellular automata computations and secret key cryptography," *Parallel Computing*, vol. 30, no. 5–6, pp. 753–766, May 2004, doi: 10.1016/j.parco.2003.12.014.

[35] Z. Yuan and X. Zhao, "Introduction of forward error correction and its application," *2012 2nd International Conference on Consumer Electronics, Communications and Networks*, 2012, pp. 3288-3291, doi: 10.1109/CECNet.2012.6201904.

[36] S. L. S. Narayanan, B. C. D. Devappa, K. Pawar, S. Jain, and A. V. R. Murthy, "Implementation of forward error correction for improved performance of free space optical communication channel in adverse atmospheric conditions," *Results in Optics*, vol. 16, 2024, 100689, doi: 10.1016/j.rio.2024.100689.

[37] T. Kim and S. Kim, "Efficient transmission of reversible data hiding in encryption images by using reed-solomon codes," *2015 3rd International Conference on Future Internet of Things and Cloud*, Rome, 2015, pp. 765-769, doi: 10.1109/FiCloud.2015.31

[38] K. Panwar, R. K. Purwar and A. Jain, "Design of a SHA-2 hash based image encryption scheme using 1D chaotic systems and DNA sequences," *International Conference on Computing, Power and Communication Technologies*, pp. 769-773, 2019.

[39] S. Zhu, C. Zhu, and W. Wang, "A new image encryption algorithm based on chaos and secure hash SHA-256," *Entropy*, vol. 20, no. 9, p. 716, Sep. 2018, doi: 10.3390/e20090716.

[40] *University of Waterloo, Image Repository*. [Online]. Available: https://links.uwaterloo.ca/Repository.html. (accessed on 15 July 2024).

BIOGRAPHIES OF AUTHORS

Gaverchand Kukaram graduated from the Department of Mathematics in 2019 and received master's degree in mathematics from SRM Institute of Science and Technology in 2021. Currently he pursuing his Ph.D. degree in the same institution. His current area of research includes automata theory, cryptography, DNA computing and image processing. He can be contacted at email: gk1617@srmist.edu.in.

Venkatesan Ramasamy working as an assistant professor in the Department of Mathematics, SRM Institute of Science and Technology, India. His current area of research includes formal languages and automata theory, algebraic automata theory, image processing, and cryptography. He can be contacted at email: venkater1@srmist.edu.in.

Yasmin Abdul graduated from the Department of Mathematics in 2019 and received master's degree in mathematics from SRM Institute of Science and Technology in 2021. Currently she pursuing her Ph.D. degree in the same institution. Her current area of research includes automata theory, cryptography, and image processing. She can be contacted at email: ya5805@srmist.edu.in.