

## IMAGE ENCRYPTION USING NOVEL CHAOTIC MAP AND CELLULAR AUTOMATA DYNAMICS

M. MOHAMMED IBRAHIM AND R. VENKATESAN\* 

**Abstract.** The rapid growth of online information transmission has made the secure transmission and storage of sensitive visual information crucial, particularly in light of the continuous increase in cyber threats. Traditional encryption algorithms are not very effective on images due to their very high pixel correlation, larger file sizes, and intrinsic redundancy. This paper presents a new framework of secure image encryption that will make use of advanced chaotic maps and cellular automata dynamics. It creates deterministic randomness, high sensitivity to initial conditions, and unpredictability through chaotic maps. CA introduces a series of dynamic, rule-based transformations that ensure robust properties for diffusion and confusion. During encryption, chaotic maps create pseudo-random sequences that control both the CA-based pixel scrambling and value transformation. This provides a very secure encryption method with many layers. It ensures high entropy in key generation, resistance against brute-force attacks, and high sensitivity to initial parameters. The scheme works because it can withstand differential, statistical, and noise-based attacks and show performance metrics like entropy analysis, correlation coefficients, histogram uniformity, and robustness. The suggested method is characterized by large-scale use, adaptability, and safety from modern cryptographic threats.

**Mathematics Subject Classification.** 37B15, 68Q80, 68P25.

Received October 18, 2023. Accepted July 2, 2025.

### 1. INTRODUCTION

In the era of digital information proliferation, the security of sensitive data, particularly images, has become a paramount concern. Image encryption is pivotal in safeguarding these assets from unauthorized access, tampering, or interception. However, the evolving landscape of technology and increasing computational power has led to several challenges in the field of image encryption, necessitating innovative solutions to fortify the protection of visual data [1, 2]. Traditional encryption methods often struggle to meet the demands of modern security requirements. Many of these methods rely on conventional cryptographic algorithms, which have shown vulnerabilities when applied to image data. Challenges include maintaining image confidentiality, integrity, and authenticity while ensuring efficient encryption and decryption processes [3–9]. Additionally, with the advent of quantum computing, conventional encryption methods are at risk of being compromised, emphasizing the urgency of exploring novel approaches. Image encryption is vital in various domains, such as healthcare, finance, military, and communication. Protecting sensitive medical images, confidential financial documents, classified

---

*Keywords and phrases:* Cellular automata, cryptography, image encryption, decryption, chaotic map.

Department of Mathematics, College of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur 603203, India.

\* Corresponding author: [venkater1@srmist.edu.in](mailto:venkater1@srmist.edu.in)

military imagery, and private communications from unauthorized access is essential for safeguarding privacy and national security. Securely transmitting and storing images is pivotal in today's interconnected digital world [10].

Utilizing novel chaotic maps and cellular automata dynamics offers a unique and promising avenue for image encryption. Chaotic systems exhibit inherent unpredictability and sensitivity to initial conditions, making them ideal for generating complex cryptographic keys. Cellular automata, on the other hand, provide a framework for spatial transformations that can effectively scramble image pixels. By combining these dynamics, we aim to create a robust encryption scheme that guarantees the confidentiality and integrity of the image data [11–13]. Recently, several modern approaches have emerged for performing image encryption. A quadratic polynomial hyperchaotic map was used to enhance the randomness and diffusion properties, ensuring resistance against cryptographic attacks [14]. Fractional-order memristive cellular neural networks were found suitable for secure image processing featuring dynamic complexity and sensitivity on initial conditions [15]. In the same way, three-dimensional hyperchaotic maps with hidden attractors worked well for image encryption with a high key sensitivity and even better scrambling features [16]. Putting DNA computing together with chaotic systems has created strong hash functions for cryptography that make it safer by preventing collisions and responding quickly to changes in input [17]. Hybrid encryption schemes combining compressive sensing, elliptic curves, and novel multistable oscillators have demonstrated superior storage efficiency and encryption robustness [18]. The proposed [19] cryptosystem integrates chaotic maps, cellular automata, and a dynamically generated S-Box for effective image encryption. Strong S-box designs that use chaos, 2D cellular automata, and algebraic structures have also shown promise in making encryption algorithms stronger against cryptanalytic attacks [20].

Researchers have been encouraged to explore chaotic systems due to their inherent randomness and sensitivity to initial conditions, which makes them highly suitable for generating cryptographic keys. Similarly, cellular automata offer dynamic rule-based transformations that enhance data diffusion and confusion. The synergy between chaos theory and cellular automata will inspire and open up new ways towards advanced image encryption frameworks, enabling them to meet modern security challenges with greater efficiency and robustness. The Contribution to the paper is

- Creating Novel chaotic map for enhanced security.
- Hybrid approach on Chaotic map and cellular automata based Encryption/Decryption algorithm for cryptographic advances.
- Analysing and comparison of results from existing literature for readers understanding that how the system is capable of.

This paper addresses the abovementioned challenges by introducing a groundbreaking approach to image encryption, leveraging the power of novel chaotic maps and cellular automata dynamics. Our primary goal is to enhance the security of image data, making it resilient to attacks and suitable for secure transmission and storage. By harnessing the unpredictable and complex behaviour of chaotic systems and the computational capabilities of cellular automata, we seek to provide a robust framework for image encryption that surpasses the limitations of existing techniques. The following sections are structured as follows: Section 2 provides essential information about chaotic maps and evaluates its performance. In Section 3 we gave detailed explanation of cellular automata. In Section 4, we present the proposed encryption/decryption algorithm. Section 5 covers the discussion of simulation results and security performance analysis. Finally, Section 6 wraps up this paper with its conclusion.

## 2. TWO DIMENSIONAL EXPONENTIAL SINE MAP

In this section, we introduce an novel 2D chaotic map known as the Two Dimensional Exponential Sine Map(2D-ESM) and subsequently delve into an analysis of its chaotic complexity.

### 2.1. Definition of 2D-ESM

The 2D-ESM is the composition of exponential function and sine function, defined as follows

$$t(x) = e^{rx}, s(x) = \sin(1/x), (t \circ s)(x) = t(s(x)) = r(\sin(1/x)) = e^{r\sin(1/x)} \quad (2.1)$$

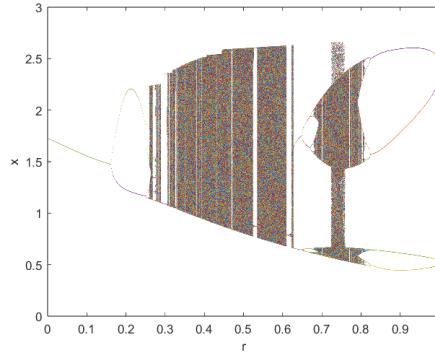


FIGURE 1. Bifurcation of 2D-ESM.

For the complexity of the chaotic map, we extended its dimension from one dimension to two dimension in the following way,

$$x_{i+1} = e^{r \sin(1/(1-x_i)) + (1-r) \sin(1/y_i)} \quad (2.2)$$

$$y_{i+1} = e^{r \sin(1/(1-y_i)) + (1-r) \sin(1/x_i)} \quad (2.3)$$

where the control parameter  $r \in [0.3, 1]$ .

## 2.2. Performance evaluation

Performance analysis for chaotic maps is essential for understanding and utilizing these mathematical systems in various applications, such as cryptography, data encryption, random number generation, and secure communications.

### 2.2.1. Bifurcation analysis

Bifurcation in chaotic maps refers to a phenomenon where a small change in a system's parameter values leads to a dramatic and unpredictable change in its behavior. During bifurcation, as a control parameter is varied, the system's behavior can transition from order to chaos or exhibit intricate patterns. These transitions are often represented graphically as bifurcation diagrams Figure 1, where the x-axis represents the parameter value, and the y-axis shows the behavior of the system, such as the values it takes or its stability. Bifurcation diagrams can reveal the underlying structure of chaotic systems [21].

### 2.2.2. Lyapunov experiment

The Lyapunov experiment is a fundamental concept in the study of chaos theory, which is used to analyze the chaotic behavior of dynamical systems, particularly chaotic maps. This experiment is named after Aleksandr Lyapunov, a Russian mathematician, and it plays a crucial role in understanding and quantifying chaos in nonlinear systems. To measure the chaotic behavior of the map, we compute the Lyapunov exponent, denoted as  $\lambda$  [22]. The Lyapunov exponent quantifies the exponential rate of divergence of nearby trajectories in the system. It is calculated as follows:

$$\lambda = \lim_{n \rightarrow \infty} \sum_0^{n-1} \ln \left| \frac{dx_{i+1}}{dx_i} \right| \quad (2.4)$$

TABLE 1. NIST Test Results for proposed method.

S. no.	Statistical test	Proportion	P-values	Results
1	Frequency test	0.5341	10/10	Pass
2	Block Frequency test	0.3439	10/10	Pass
3	Cumulative sums test	0.2133	10/10	Pass
4	Runs test	0.3949	10/10	Pass
5	Longest runs test	0.3421	10/10	Pass
6	Rank test	0.2133	10/10	Pass
7	FFT test	0.3504	10/10	Pass
8	Non overlapping template test	0.9114	8/10	Pass
9	Overlapping template test	0.3504	9/10	Pass
10	Universal	0.7399	10/10	Pass
11	Approximate Entropy	0.3504	8/10	Pass
12	Random Excursions	0.2232	9/10	Pass
13	Random Excursions Variant	0.3232	9/10	Pass
11	Serials test	0.7399	10/10	Pass
12	Linear Complexity test	0.9914	9/10	Pass

In this equation,  $dx_i$  represents the difference between two nearby trajectories at time step  $i$ , and the sum is taken over a sufficiently long trajectory. A positive Lyapunov exponent ( $\lambda > 0$ ) indicates chaotic behavior, as nearby trajectories diverge exponentially. Conversely, a negative Lyapunov exponent ( $\lambda < 0$ ) implies stability, where nearby trajectories converge. In this method the 2D-ESM exhibits a positive behaviour and also chaos when  $r \in [0.2, 0.29] \cup [0.7, 0.8] \cup [0.95, 1]$  and hyper-chaotic behaviour when  $r \in [0.3, 0.6]$  As a result, 2D-ESM is more sensitive to the initial conditions. It has a more intricate structure, making it more challenging to forecast its course.

### 2.2.3. NIST test analysis

The National Institute of Standards and Technology’s Special Publication (NIST SP 800-22) test suite is a specialized tool that rigorously evaluates the randomness of sequences based on several characteristics [23]. It offers a comprehensive evaluation comprising 15 distinct assessments. To evaluate the randomness of our data, we generated a 10 MB binary sequence randomly and tested it 10 times to get a 100 MB sequence, and Table 1 demonstrates the average value for (10\*10)100 MB sequences and that all sequences achieved near-perfect pass rates, surpassing their specified standards. The results demonstrate the ability of the generated fractional chaotic maps to reliably generate pseudo-random sequences that meet the stringent demands of actual applications.

## 3. CELLULAR AUTOMATA

Cellular automata (CA) are a class of mathematical models and computational systems that consist of a grid of cells, each of which can be in one of a finite number of states. These cells evolve over discrete time steps according to a set of simple rules based on the states of their neighboring cells(see Fig. 2). They were first introduced by Von Neumann and Ulam(under “cellular spaces” in 1950s) and popularized by mathematician named John Conway(under “Game of Life” in 1970) [24, 25].

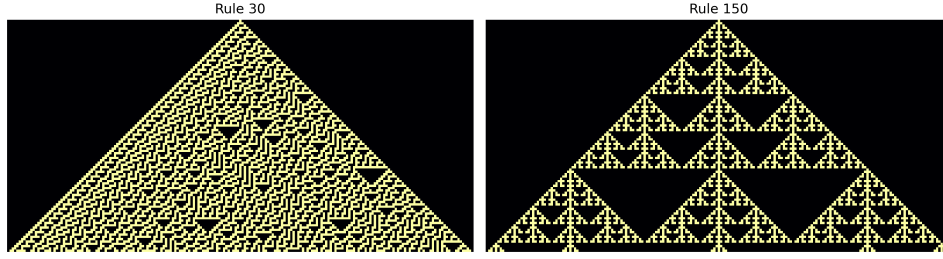


FIGURE 2. Cellular automata Rules.

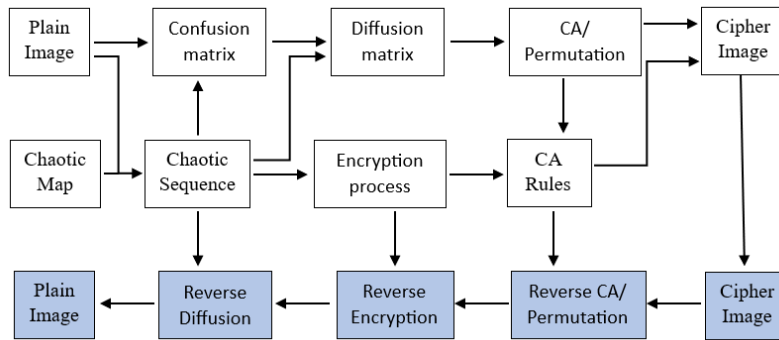


FIGURE 3. Flowchart for proposed Algorithm.

### 3.1. Neighborhood and transition function

Each cell has a neighborhood. The neighborhood can vary depending on the rules of the cellular automaton. Common neighborhood configurations include the Moore neighborhood (all adjacent cells) and the Von Neumann neighborhood (only the cardinal direction neighbors). The state of each cell is updated according to a transition function at each time step  $t$ , which takes the input of the current state of cell  $i$  and its two neighbours and outputs the new state of cell  $i$  at time step  $t + 1$ . Alternatively, the state of the cell at time  $t + 1$  is

$$C_{i(t+1)} = \delta(C_{[i-1](t)}, C_{i(t)}, C_{[i+1](t)}) \quad (3.1)$$

for example, the Rule 30 is selected from the Elementary cellular automata rules. The next state  $C_i$  is follows:  $g(111) = 0, g(110) = 0, g(101) = 0, g(100) = 1, g(011) = 1, g(010) = 1, g(001) = 1, g(000) = 0$ . So rule 30 is represented as  $(30)_{dec} = (00011110)_{bin}$ . Wolfram classified this rules of CA [26] into ordered, periodic, random or chaotic and complex behaviors.

## 4. ENCRYPTION ALGORITHM

The Proposed algorithm flowchart is showed in Figure 3 and the detailed steps are as follows and the algorithm example is shown in Figure 4 and overall encrypted/decrypted output is shown in Figure 5

### 4.1. Encryption process

**Step 1:** Convert the original image with dimension  $m * n$  into a matrix representation, it is denoted as  $I_{m*n}$ .

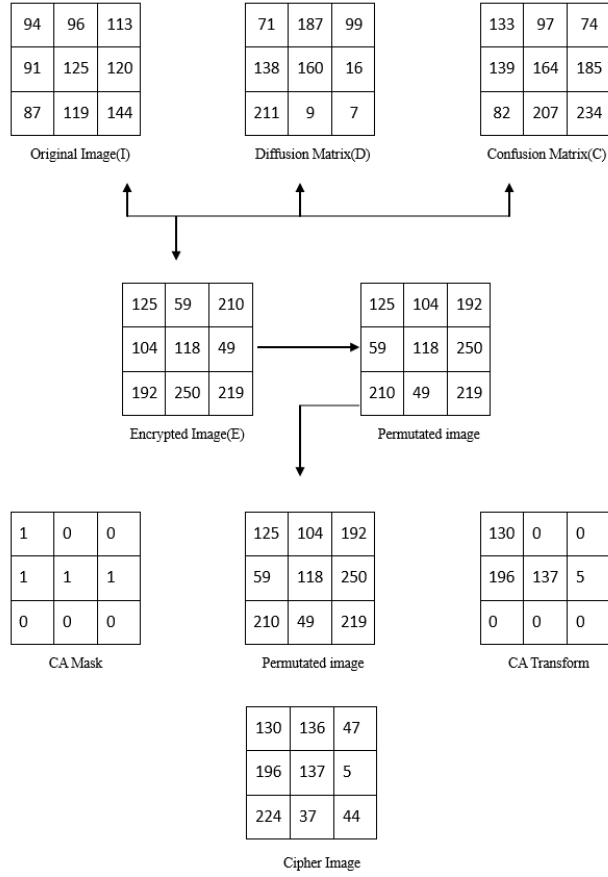


FIGURE 4. Process of algorithm.

**Step 2:** Define a chaotic map called 2D Exponential Sine Map and Initialize the map with specific initial conditions and a parameter  $r$ .

**Step 3:** Iterate the chaotic map for a total of  $m * n * 256$  (as image size) times to generate two chaotic sequences,  $x_i$  and  $y_i$ .

**Step 4:** Convert the chaotic sequences  $x_i$  and  $y_i$  into a matrix of the size of the original image, namely Confusion( $C_{m*n}$ ) and Diffusion matrix( $D_{m*n}$ ), where

$$C_{m*n} = \text{floor}(\text{mod}(x_i * 10^{15}, 257)) \quad (4.1)$$

$$D_{m*n} = \text{floor}(\text{mod}(y_i * 10^{15}, 257)) \quad (4.2)$$

**Step 5:** Encrypt the image using the equation:

$$E(a, b) = \text{mod}[\text{mod}(I(a, b) * D(a, b), 257) + C(a, b), 257] \quad (4.3)$$

where,  $a \in [1, m]$  and  $b \in [1, n]$ .

**Step 6:** Compute the custom SHA-256 hash of the encrypted matrix E, denoted as  $E_H$ . This hash value serves as an additional layer of security.



FIGURE 5. Encryption/Decryption.

**Step 7:** Permute the encrypted matrix from step 5 based on matrix transpose.

**Step 8:** Implement cellular automata rules by giving initial condition of automaton  $(1, 1 : 10 : end) = 1$ ; to produce the mask and implement this mask to the encrypted image to produce the cipher image( $E_C$ ).

**Step 9:** The matrix  $E_C$  represents the encrypted cipher image. The SHA-256 hash value( $E_H$ ) can be stored or transmitted alongside the encrypted image for verification during decryption.

#### 4.2. Decryption process

As showed in Figure 3 decryption process is the inverse process of encryption. The decryption as follows.

**Step 1:** Cipher image taken as a input.

**Step 2:** The Cellular Automata process is reversed and remove the mask and goto next step.

**Step 3:** Reversed permutation process of matrix transpose is processed.

**Step 4:** Decrypt the image using the equation:

$$E_D(a, b) = \text{mod}[\text{mod}(E(a, b) - C(a, b) + P_m, 257) * D^{-1}, 257] \quad (4.4)$$

where,  $a \in [1, m]$ ,  $b \in [1, n]$ ,  $P_m$  is prime nearer to size m and  $D^{-1}$  is inverse diffusion matrix.

**Step 5:** Calculate custom sha 256 hash for decrypted image.

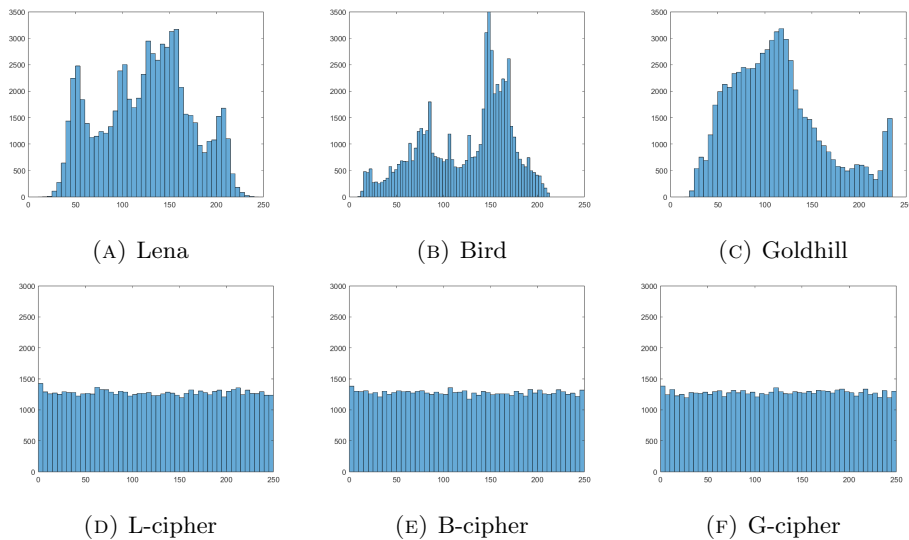


FIGURE 6. A-C Histogram of Original grayscale images. D-F Histogram of respective cipher images.

**Step 6:** Compare the hash value decrypted with the originally computed hash value. If they match, it indicates that the image hasn't been tampered with, during decryption.

**Step 7:**  $E_D$  is the Decrypted Image.

## 5. EXPERIMENTAL RESULTS AND COMPARISONS

### 5.1. Histogram analysis

The histogram analysis the distribution of image pixel values, and a uniform histogram indicates a balanced distribution of pixel intensities. In the context of encrypted images, a uniform histogram is desirable as it suggests that the encryption algorithm successfully conceals information, making it resistant to statistical attacks by attackers who may try to exploit non-uniform pixel distributions to extract sensitive data [12]. Therefore, the balanced histograms displayed in the Figures 6 and 7 demonstrate that the proposed encryption algorithm is effective in safeguarding the image content from such statistical attacks, enhancing its security.

### 5.2. Number of pixels change rate

NPCR measures the algorithm's effectiveness in terms of its ability to obscure the original content of an image during encryption and then accurately recover it during decryption. Specifically, NPCR quantifies the percentage of pixels that change between the original and encrypted images when a single-bit change in the input image [27]. It is calculated for original( $I_{m*n}$ ) and cipher image( $E_{m*n}$ ) using

$$NPCR = \frac{\sum_{i=1}^m \sum_{j=1}^n d(i, j)}{m * n} * 100 \quad (5.1)$$

subjected to

$$d(i, j) = \begin{cases} 1, & \text{if } I(i, j) = E'(i, j). \\ 0, & \text{if } I(i, j) \neq E'(i, j). \end{cases}$$

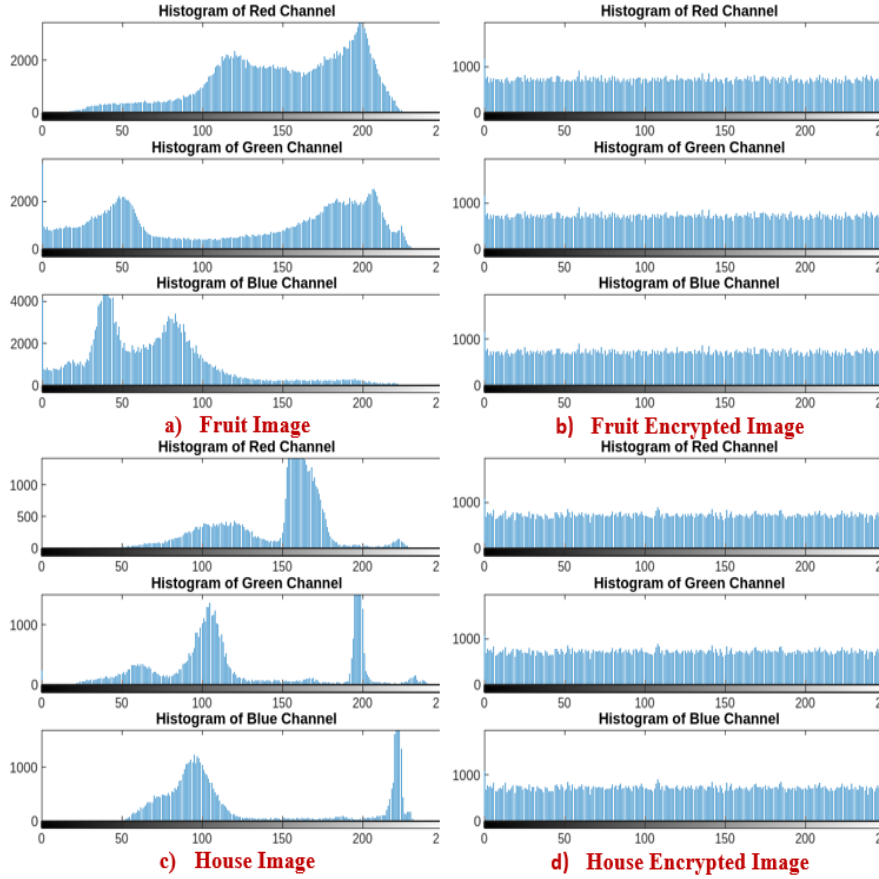


FIGURE 7. Histogram of original and encrypted images of fruit and house images.

A high NPCR value indicates that a minor alteration in the input image results in a significant change in the encrypted image, which is desirable for robust security. On the other hand, a low NPCR value implies that the encryption method might be weak and unable to mask the image effectively.

### 5.3. Peak signal to noise ratio

Peak Signal-to-Noise Ratio (PSNR) analysis is a widely used technique in image processing to quantify the quality of encrypted and decrypted images. When applied to encrypted images, PSNR measures the fidelity of the decryption process by comparing the decrypted image to the original unencrypted image. A higher PSNR value indicates a closer match between the original and decrypted images, implying better image quality and less information loss during encryption and decryption. PSNR analysis is essential for evaluating the effectiveness of encryption algorithms in preserving image quality while ensuring data security, making it a valuable tool in assessing the trade-off between security and image fidelity in image encryption systems.

$$PSNR = 10 * \log \left[ \frac{MAX^2}{MSE} \right] \quad (5.2)$$

where

TABLE 2. NPCR and PSNR analysis.

Test Image	NPCR	PSNR
Car	99.54%	26.46
Flight	99.61%	24.91
lena	99.70%	28.31
Bird	99.56%	25.92
Fruits	99.51%	27.58
Bridge	99.24%	28.00
House	99.50%	26.79
Camera	99.63%	27.70
Lake	99.59%	27.47
Goldhill	99.58%	27.37

- MAX: The maximum possible pixel value.
- MSE: Mean Squared Error, calculated as the average of the squared differences between corresponding pixels in the original and degraded (or decrypted) images.

The NPCR and PSNR analysis results is given in Table 2

#### 5.4. correlation

The correlation coefficient for encrypted and decrypted images is a measure of the similarity or consistency between the original unencrypted image and the image that results after decryption. This coefficient, typically ranging from -1 to 1, quantifies how well the decrypted image matches the original one. A value of 1 indicates a perfect match, meaning that the decryption process was highly accurate, while a value of -1 implies a perfect inverse relationship, suggesting that the decryption process has completely reversed the image's content. A coefficient close to 0 suggests little to no correlation, indicating that the decrypted image bears little resemblance to the original [28]. In image encryption and decryption applications, a high correlation coefficient is desirable, as it signifies that the decryption process successfully reconstructs the original image, preserving its integrity and visual quality. The pearson correlation coefficient is given by,

$$Cor_{u,v} = \frac{\sum_{i=1}^n (u_i - \bar{u})(v_i - \bar{v})}{\sqrt{\sum_{i=1}^n (u_i - \bar{u})^2 (v_i - \bar{v})^2}} \quad (5.3)$$

where  $\bar{u}$  and  $\bar{v}$  are mean values of  $u$  and  $v$  variables respectively and  $u, v$  is the neighboring pixel values of the image. The Horizontal, vertical and diagonal correlation of orginal and cipher images is given in Table 3.

#### 5.5. Entropy analysis

Entropy analysis is a valuable technique used to assess the randomness and information content within encrypted and decrypted images. In the context of image encryption, high entropy indicates that the image has undergone effective encryption, as the data appears random and unpredictable. Conversely, low entropy suggests that the image may not be adequately protected, as recognizable patterns or structures may remain [29]. It is calculated by

$$S = -\sum prob(i) * \log_2(prob(i)) \quad (5.4)$$

where

TABLE 3. Correlation analysis.

Image	Orginal			Cipher		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Car	0.9635	0.9364	0.9452	0.0032	0.0033	0.0042
Flight	0.9359	0.9456	0.9026	0.0072	0.0017	0.0029
Lena	0.9358	0.9346	0.9629	-0.0038	-0.0067	0.0033
Bird	0.9812	0.9899	0.9949	0.0016	-0.0008	-0.0538
Fruits	0.9753	0.9524	0.9635	0.0018	0.0039	0.0083
Bridge	0.9317	0.9068	0.9046	0.0091	-0.0034	0.0384
House	0.9744	0.9236	0.9056	0.0018	0.0052	0.0084
Camera	0.9335	0.9592	0.9296	-0.0056	-0.0010	0.0036
Lake	0.9677	0.9345	0.9622	0.0021	0.0042	0.0052
Goldhill	0.9425	0.9440	0.9255	-0.0062	0.0033	0.0069

TABLE 4. Entropy analysis.

Image	Original	Encrypted
Car	7.3601	7.9633
Flight	7.2979	7.9634
Lena	7.4572	7.9600
Bird	6.7743	7.9904
Fruits	7.2977	7.9915
Bridge	7.6685	7.9913
House	6.4000	7.9618
Camera	7.0090	7.9913
Lake	7.3896	7.9622
Goldhill	7.4715	7.9907

- S denotes the entropy of pixel values.
- $\text{prob}(i)$  denotes the probability of  $i^{\text{th}}$  pixel.

The Entropy analysis of the original and cipher images is given in Table 4.

## 5.6. Comparative analysis

It is a comprehensive way to evaluate the effectiveness and security of encryption algorithms. In this analysis, we will use Lena image as an example and compare several key metrics including Table 2 (NPCR and PSNR), Histogram Analysis, Table 3 (Correlation), and Table 4 (Entropy) with other papers for checking effectiveness of our encryption/decryption algorithm.

After conducting a comparative analysis of image encryption/decryption using a chaotic map-based algorithm on the overall image in Table 5, it is evident that the chosen encryption method demonstrates varying levels of effectiveness and security. The Peak Signal-to-Noise Ratio reveals the quality of the decrypted image in comparison to the original Lena image, while the Number of Pixel Change Rate indicates the extent of pixel alterations. Histogram analysis highlights differences in the distribution of pixel values, emphasizing the impact of encryption on image statistics. Additionally, the correlation coefficient between the original and decrypted images offers insights into their similarity, with lower values indicating stronger encryption. Lastly, entropy measurements quantify the randomness and information content in both images. These comprehensive evaluations serve as valuable metrics for assessing the performance and security of chaotic map-based image encryption algorithms.

TABLE 5. Comparative analysis.

Comparison	Correlation	PSNR	NPCR	Entropy	Encryp.time(s)
Bakhshandeh <i>et al.</i> [30]	-0.0063	27.42	99.460%	7.9696	4.37
Chai <i>et al.</i> [31]	0.0039	26.06	99.040%	5.5914	0.52
Gakam Tegue <i>et al.</i> [32]	-0.0040	–	99.61%	7.9991	3.15
Hu <i>et al.</i> [16]	0.0008	26.43	99.62%	7.9977	0.48
Ibrahim <i>et al.</i> [19]	-0.0002	28.21	99.61%	7.9961	1.25
Jeelani [33]	0.0491	28.03	99.402%	7.9767	6.03
Li <i>et al.</i> [6]	0.0051	27.03	99.610%	7.9927	1.35
Mondal <i>et al.</i> [11]	0.0043	28.28	99.688%	7.9993	4.05
Tegue <i>et al.</i> [18]	-0.0001	–	99.60%	7.9970	0.31
Zhou <i>et al.</i> [15]	-0.0001	–	99.74%	7.9980	7.99
Lena [proposed]	-0.0038	28.31	99.700%	7.9600	2.63

## 5.7. Data usage

This paper uses standard images from the repository [34, 35]. The system we are using holds 8GB RAM, AMD Ryzen 5, and MATLAB 2023a were used to carry out all the experiments in this paper.

## 6. CONCLUSION

The paper proposes a new encryption algorithm that uses chaotic maps and cellular automata for efficient and secure image transmissions. The encryption scheme starts by establishing initial conditions and parameters of chaotic maps, which generate pseudo-random sequences essential in driving the encryption dynamics. We then map the original image into a two-step transformation process, which involves a diffusion phase and a confusion phase. Diffusion changes the pixel values according to chaotic sequences, while confusion changes the position of pixels based on CA-based transformations. These steps guarantee a highly disordered structure in the encrypted image, preventing the attackers from inferring any meaningful information. The final encryption stage includes additional CA-driven permutation and value transformation operations for reinforcement. The suggested plan works well because it has a high level of entropy, low correlation between pixels next to each other, uniform histograms, and strong defence against common cryptographic attacks like statistical and differential analyses. The algorithm’s dynamic and rule-based approach allows robust security with computational efficiency. Future research will aim to enhance the algorithm through the exploration of higher-dimensional CA models for more intensive encryption and decryption mechanisms. We will extend the proposed algorithm to test its applicability on various multimedia data, real-time encryption situations, and even hardware-based implementation. Other potential extensions include adaptive CA rule selection, the integration of multiple chaotic systems, and optimization toward emerging cryptographic challenges that guarantee further relevance and robustness in secure image communication.

## REFERENCES

- [1] M. Cozzens, and S.J. Miller, The mathematics of encryption. *J. Am. Math. Soc.* **29** (2013).
- [2] H.C. Van Tilborg and S. Jajodia, *Encyclopedia of Cryptography and Security*. Springer Science and Business Media (2014).
- [3] Z. Hua, Y. Zhou and H. Huang, Cosine-transform-based chaotic system for image encryption. *J. Inf. Sci.* **480** (2019) 403–419.

- [4] Z. Hua, F. Jin, B. Xu and H. Huang, 2D logistic-sine-coupling map for image encryption. *J. Signal Process. Syst.* **149** (2018) 148–161.
- [5] Z. Hua, Y. Zhou, C.M. Pun and C.P. Chen, 2D sine logistic modulation map for image encryption. *J. Inf. Sci.* **297** (2015) 80–94.
- [6] L. Li, Y. Luo, S. Qiu, X. Ouyang, L. Cao and S. Tang, Image encryption using chaotic map and cellular automata. *Multimed. Tools Appl.* **81** (2022) 40755–40773.
- [7] W. Liu, K. Sun and C. Zhu, A fast image encryption algorithm based on chaotic map. *Opt. Lasers Eng.* **84** (2016) 26–36.
- [8] X. Wang and D. Xu, A novel image encryption scheme using chaos and Langton’s ant cellular automaton. *Nonlinear Dyn.* **79** (2015) 2449–2456.
- [9] Y. Zhou, L. Bao and C.P. Chen, A new 1D chaotic system for image encryption. *J. Signal Process. Syst.* **97** (2014) 172–182.
- [10] B.A. Forouzan and D. Mukhopadhyay, Cryptography and Network Security. McGraw Hill Education (India) Private Limited, New York, NY, USA **12** (2015).
- [11] B. Mondal, S. Singh and P. Kumar, A secure image encryption scheme based on cellular automata and chaotic skew tent map. *J. Inf. Secur. Appl.* **45** (2019) 117–130.
- [12] A.Y. Niyat, M.H. Moattar and M.N. Torshiz, Color image encryption based on hybrid hyper-chaotic system and cellular automata. *Opt Lasers Eng.* **90** (2017) 225–237.
- [13] P. Ping, J. Wu, Y. Mao, F. Xu and J. Fan, Design of image cipher using life-like cellular automata and chaotic map. *J. Signal Process. Syst.* **150** (2018) 233–247.
- [14] W. Feng, J. Zhang, Y. Chen, Z. Qin, Y. Zhang, M. Ahmad and M. Woźniak, Exploiting robust quadratic polynomial hyperchaotic map and pixel fusion strategy for efficient image encryption. *Expert Syst. Appl.* **246** (2024) 123190.
- [15] X. Zhou, D. Jiang, J.D.D. Nkpkop, M. Ahmad, J.T. Fossi, N. Tsafack and J. Wu, Dynamics analysis and cryptographic implementation of a fractional-order memristive cellular neural network model. *Chinese Phys. B* **33** (2024) 040506.
- [16] X. Hu, D. Jiang, M. Ahmad, N. Tsafack, L. Zhu and M. Zheng, Novel 3-D hyperchaotic map with hidden attractor and its application in meaningful image encryption. *Nonlinear Dynamics* **111** (2023) 19487–19512.
- [17] S.M.S. Eldin, A.A.A. El-Latif, S.A. Chelloug, M. Ahmad, A.H. Eldeeb, T.O. Diab and H.N. Zaky, Design and analysis of new version of cryptographic hash function based on improved chaotic maps with induced DNA sequences. *IEEE Access* **11** (2023) 101694–101709.
- [18] G.G. Tegue, J.D.D. Nkpkop, N. Tsafack, M.A. Abdel, J. Kengne, M. Ahmad and J.G. Tamba, A novel image encryption scheme based on compressive sensing, elliptic curves and a new jerk oscillator with multistability. *Physica Scripta* **97** (2022) 125215.
- [19] M. Ibrahim, R. Venkatesan and M. Ahmad, A hybrid approach of substitution and permutation techniques for modern image-cryptosystem. *Physica Scripta* **99** (2024) 125279.
- [20] A. Haque, T.A. Abdulhussein, M. Ahmad, M.W. Falah and A.A. Abd El-Latif, A strong hybrid S-box scheme based on chaos, 2D cellular automata and algebraic structure. *IEEE Access* **10** (2022) 116167–116181.
- [21] C.C. Karaaslanli, Bifurcation Analysis and its Applications. InTech, London, UK (2012).
- [22] C. Shen, S. Yu, J. Lü and G. Chen, Designing hyperchaotic systems with any desired number of positive Lyapunov exponents via a simple model. *IEEE Trans. Circuits Syst. I Regul. Pap.* **61** (2014) 2380–2389.
- [23] NIST SP 800-22. Available online: <https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software> (accessed on 30-09-2024)
- [24] A. Adamatzky, Game of Life Cellular Automata. Springer, London **1** (2010).
- [25] S. Wolfram, Cellular Automata and Complexity: Collected Papers. CRC Press (2018).
- [26] S. Wolfram, A new kind of science. *ASME. Appl. Mech. Rev.* **56** (2003) 18–19.
- [27] Z. Jeelani and F. Qadir, A comparative study of cellular automata-based digital image scrambling techniques. *Evol. Syst.* **12** (2021) 359–375.
- [28] A.K. Sharma, Text Book of Correlations and Regression. Discovery Publishing House (2005).
- [29] V.P. Singh, Entropy Theory and its Application in Environmental and Water Engineering. John Wiley and Sons (2013).
- [30] A. Bakhshandeh and Z. Eslami, An authenticated image encryption scheme based on chaotic maps and memory cellular automata. *Opt. Lasers Eng.* **51** (2013) 665–673.

- [31] X. Chai, X. Fu, Z. Gan, Y. Zhang, Y. Lu and Y. Chen, An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata. *Neural. Comput. Appl.* **32** (2020) 4961-4988.
- [32] G.A. Gakam Tegue, J.D.D. Nkpkop, M.A. Abdel, N. Tsafack, A. Musheer, F.V. Signing and J.G. Tamba, A novel image encryption scheme combining a dynamic S-Box generator and a new chaotic oscillator with hidden behavior, *Arabian J. Sci. Eng.* **48** (2023) 10653-10672.
- [33] Z. Jeelani, Digital image encryption based on chaotic cellular automata. *Int. J. Comput. Vis. Image Process.* **10** (2020) 29-42.
- [34] The USC-SIPI Image Database available on <https://sipi.usc.edu/database>
- [35] University of Waterloo, the waterloo fractal coding and analysis group image repository available on <https://links.uwaterloo.ca/Repository.html>



**Please help to maintain this journal in open access!**

This journal is currently published in open access under the Subscribe to Open model (S2O). We are thankful to our subscribers and supporters for making it possible to publish this journal in open access in the current year, free of charge for authors and readers.

Check with your library that it subscribes to the journal, or consider making a personal donation to the S2O programme by contacting [subscribers@edpsciences.org](mailto:subscribers@edpsciences.org).

More information, including a list of supporters and financial transparency reports, is available at <https://edpsciences.org/en/subscribe-to-open-s2o>.