Improved Image Encryption Algorithm Based on Reversible Cellular Automata

Zhihua Feng, *Member, IAENG,* Dayong Zhou

***Abstract*—As the demand for image transmission and storage is increasing in multimedia technology and on the Internet, image security and encryption has become a critical research area. This paper presents a novel image encryption algorithm based on several evolved rules of reversible cellular automata. Considering the reversible nature of reversible cellular automata, the proposed approach employs a sequence of reversible cellular automaton rules and pseudo-random data to enhance image security by improving both confusion and diffusion properties. The encryption process converts the original images to highly secure versions, while the decryption process accurately restores the original images using the same reversible cellular automaton rules. Experimental results demonstrate that the improved method effectively achieves uniform pixel distribution in encrypted images, ensuring strong confusion property. Additionally, encrypting the same image with different initial random sequences of data results in completely different encrypted versions, confirming the high diffusion property. The proposed method achieves strong computational performance, rendering it appropriate for use in real-time scenarios.**

***Index Terms*—Image encryption, reversible cellular automata, confusion and diffusion, security, real-time encryption**

I. Introduction

THE security of information transmission and storage has become an increasingly critical concern for society, with the rapid advancements in network and multimedia technologies [1]-[3]. Digital images, playing a significant role in modern information systems, have revolutionized various sectors by offering a more convenient means of communication, entertainment, and storage. However, the proliferation of digital images in personal and professional settings has also raised pressing concerns regarding privacy, copyright protection, and data security. As such, safeguarding the confidentiality of image data has emerged as a vital problem, with image encryption technology becoming indispensable in addressing these challenges [4]. The application of image encryption spans a wide array of fields, including Internet communication, telemedicine, medical imaging, multimedia systems, and military communication [5], [6].

Several image encryption methods have been developed to address the unique security requirements of digital images. These include Switched Coupled Network (SCAN)-based methods, chaos-based methods, and deep learning-based approaches, each with its strengths and limitations [7]-[11]. Despite the variety of existing encryption techniques, there remains a need for methods that can provide both high security and efficient performance, particularly for applications where real-time encryption and decryption are essential.

Reversible cellular automata (RCA) have gained significant attention in the field of image encryption due to their ability to achieve both confusion and diffusion, which are two essential properties for secure encryption [12], [13]. Specifically, one-dimensional RCA (1D RCA) have been widely explored for image encryption due to its relatively low computational complexity and minimal storage requirements, making it suitable for real-time applications[14]. The flexibility and reliability of 1D RCA-based encryption methods have been demonstrated in various studies, with the ability to maintain security while being computationally efficient [15], [16]. However, while 1D RCA offers advantages such as fast processing time and low memory usages, its encryption strength is often limited when using a single rule for encryption, as this may leave the system vulnerable to attacks [17].

To address these limitations and improve the security of RCA-based encryption methods, this paper presents a new encryption algorithm that leverages several evolved rules of reversible cellular automata. By integrating several evolved rules, the proposed algorithm enhances both the security and performance of the encryption process, making it suitable for high-security applications. This method aims to strike a balance between high security and efficient real-time performance, ensuring that both properties are optimum for encrypting the given digital image.The simulation results of the algorithm demonstrate that the image encryption scheme based on several RCA rules achieves excellent encryption performance. Specifically, the algorithm satisfies the key requirements of confusion and diffusion, which are fundamental to ensuring robust security in encrypted images. The effectiveness shows that this encryption method not only provides strong security but also operates with minimal computational overhead.

The structure of this paper is organized as follows: Section II provides a brief overview of reversible cellular automata, highlighting their role in image encryption. Section III details the proposed image encryption algorithm with several RCA rules. Section IV presents the simulation results to demonstrate performances of the improved RCA-based

Manuscript received March 20, 2025; revised July 18, 2025.

This work was supported in part by the Applied Basic Research Program Foundation of Department of Science & Technology of Liaoning Province, China, under Grant 2023JH2/101300221.

Zhihua Feng is a researcher of School of Science, Dalian Jiaotong University, Dalian, Liaoning 116028 China (corresponding author to provide phone: +86-155-0408-6650; e-mail: fzh@djtu.edu.cn).

Dayong Zhou is an associate professor of the School of Science, Dalian Jiaotong University, Dalian, Liaoning 116028 China (e-mail: zhoudy102@163.com).

image encryption method. Finally, section V provides a summary of the study's main findings and outlines possible directions for future research.

II. Reversible Cellular Automata

A. Cellular automata

A one-dimensional cellular automaton (CA) consists of a line of cells, each holding a value of either 0 or 1. The value α_i of cell at each position i is updated according to a deterministic rule, which depends on the state of its neighboring cells [18]-[20]

$$\alpha_i^{(t+1)} = \phi(\alpha_{i-r}^{(t)}, \alpha_{i-r+1}^{(t)}, ..., \alpha_{i-1}^{(t)}, \alpha_i^{(t)}, \alpha_{i+1}^{(t)}, ..., \alpha_{i+r}^{(t)}). \quad (1)$$

where $\alpha_i^{(t)}$ is the value of the i-th cell in step t; r is a radius of the neighborhood, and the neighborhood size is $2r+1$; there are 2^{2r+1} possible configurations of the neighborhood; φ is the evolution rule of the CA. This means that the total number of rules with the neighborhood of radius r is $2^{2^{2r+1}}$. So there are $2^{2^3} = 256$ rules for CA that radius equals one. The naming of the rules follows the standard convention introduced by Wolfram. The rule definition is shown

$$(\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6, \beta_7, \beta_8)_{bin} = (\sum_{i=1}^{8} \beta_i 2^{8-i})_{dec}. \quad (2)$$

An example of the CA that radius is one is shown on Fig. 1.

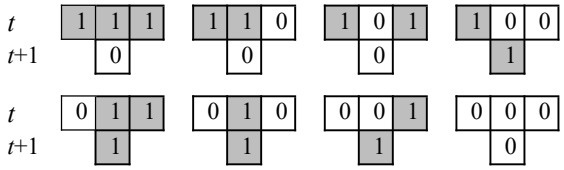


Fig. 1. A CA rule

According to (2), the rule definition is

$$0\times2^7+0\times2^6+0\times2^5+1\times2^4+1\times2^3+1\times2^2+1\times2+0\times2^0=30. \quad (3)$$

The next state values defined for each possible configuration of the neighborhood form a binary number 00011110 (decimal 30). Therefore, the decimal rule number is 30.

In the case of finite CA, cyclic boundary conditions are typically applied, effectively treating the CA as a ring. Given an initial configuration, the CA evolves by updating the values of all cells simultaneously, resulting in a new configuration based on a predefined CA rule. The process of repeatedly applying this rule to update all cell values step by step is referred to as CA iterations.

B. Reversible cellular automata

A CA is deemed reversible if its global transition function is bijective. Every possible configuration maps to a unique successor and, conversely, has a unique predecessor. This property ensures that the system's evolution is fully traceable in both forward and backward directions [21]. When analyzing the original CAs, only a small subset of rules possess reversible property. Out of the 256 possible CA rules with a radius of one, only six rules are reversible, namely, rule 30, 60, 90, 102, 150, and 195. This means that classic CA rules is specifically selected to ensure reversibility.

In reversible cellular automata, the new state of a cell is determined not only by its own state and the states of its neighbors from the previous step but also by its state from two steps back. In a CA, the value $\alpha_i^{(t+1)}$ of the i-th cell in configuration t+1 depends on its own state and the states of its r radius neighbors in configuration t. However, in RCA, the state of the central cell from step t-1 is also taken into account. Although these RCA rules are named after their corresponding original CA rules, they are not simply the inverse rules of the original ones. Instead, RCA represents a distinct class of cellular automaton where the state of a cell from two steps back acts as an additional neighbor, influencing its current state. The RCAs exhibit reversal invariance, meaning their rules inherently ensure invertibility. An example of such a rule is shown in Fig. 2, where the decimal rule number is 30R.

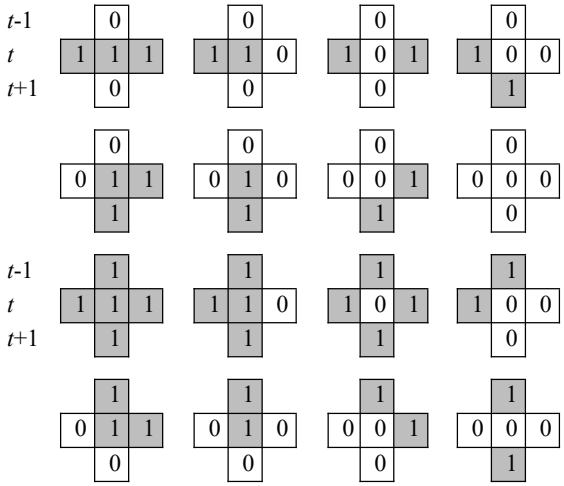


Fig. 2 RCA rule 30R

The rule 30R behaves the same as rule 30 when the cell was 0 two time steps earlier (t-1). However, if the cell was 1 at t-1, the new state at t+1 is flipped. Since a RCA rule now depends on the state from two steps back, the initial configuration must consist of two consecutive configurations. To run a RCA in reverse, it suffices to copy the states from one step prior to the next step. As illustrated in Fig. 3, the reversible cellular automaton reconstructs the initial data.

0	0	0	0	0	1	0	0	0	0	0	0
0	0	0	0	0	1	1	0	0	0	0	0
0	0	0	0	1	0	0	1	0	0	0	0
0	0	0	1	1	0	0	1	1	0	0	0
0	0	1	1	1	1	1	0	0	1	0	0
0	1	1	1	1	0	0	0	0	1	1	0

(a) Rule 30R forward

0	1	1	1	1	0	0	0	0	1	1	0
0	0	1	1	1	1	1	0	0	1	0	0
0	0	0	1	1	0	0	1	1	0	0	0
0	0	0	0	1	0	0	1	0	0	0	0
0	0	0	0	0	1	1	0	0	0	0	0
0	0	0	0	0	1	0	0	0	0	0	0

(b) Rule 30R in reverse

Fig. 3 Running rule 30R

III. Image Encryption Based on Several RCA Rules

A. Principle of several RCA rules for encryption

Reversible cellular automata are frequently employed due to their complex behavior, making them suitable for encryption applications[22]-[25]. Image encryption using several evolved RCA rules demonstrates more intricate behavior compared to encryption with a single RCA rule. In the RCA-based encryption process, a block of pseudo-random data is initialized as configuration C_{00}, while the data to be encrypted is set as configuration C_{11}. C_{00} and C_{11} form the initial configuration of the RCAs encryption system together.

The encryption process involves multiple stages. The same RCA rule can be repeatedly employed. First, RCA evolves forward for n_1-1 iterations according to the first RCA rule, producing the first encrypted configuration $C1_{n_1}$. Subsequently, n_1-1 ciphertext and $C1_{n_1}$ serve as the new initial configuration for the next encryption phase, where RCA evolves forward for n_2-1 iterations under the second RCA rule, yielding the second encrypted configuration $C2_{n_2}$, and so forth. The final encrypted data, denoted as CNn_N, is obtained after completing all iterations. This process is illustrated in Fig. 4.

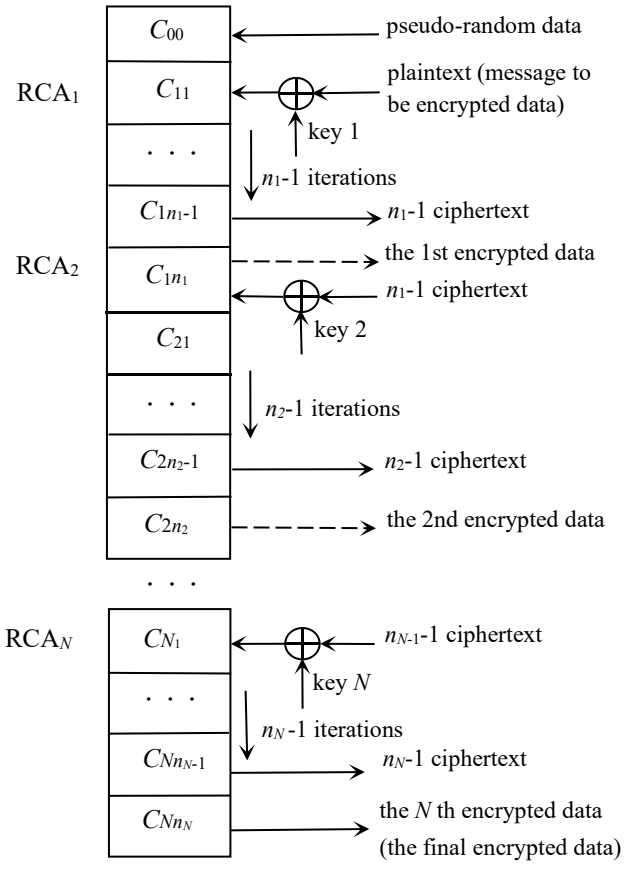


Fig. 4 Encryption based on RCA rules

The decryption process is essentially the reverse of the encryption process, involving backward iterations of RCA. The initial configuration consists of C_{00} and C_{11}, reconstructed from the previously obtained the final encrypted data CNn_N and n_N-1 ciphertext CNn_N-1 in the encryption process. Decryption begins by applying RCA forward for n_N-1 iterations according to the N-th RCA rule, yielding the first decrypted data. This process is then repeated iteratively, following the corresponding RCA rules in reverse order, until the original plaintext and pseudo-random data are fully recovered. The decryption process is shown in Fig. 5.

The same set of N RCA rules is used for both encryption and decryption, forming secret keys. To maintain the algorithm's security, the block of pseudo-random data is employed. The random configuration serves as part of the initial RCA configuration, ensuring that even when the same messages are encrypted with the same rules, different ciphertexts and final encrypted data are generated. A crucial property of using RCAs for encryption is its high sensitivity to small changes: modifying a single randomly chosen bit in either the plaintext or one of RCA rules results in approximately half of the final ciphertext and encrypted data being altered after a certain number of iterations. The encryption process further demonstrates that employing several evolved RCA rules for data encryption enhances security significantly compared to using a single RCA rule.

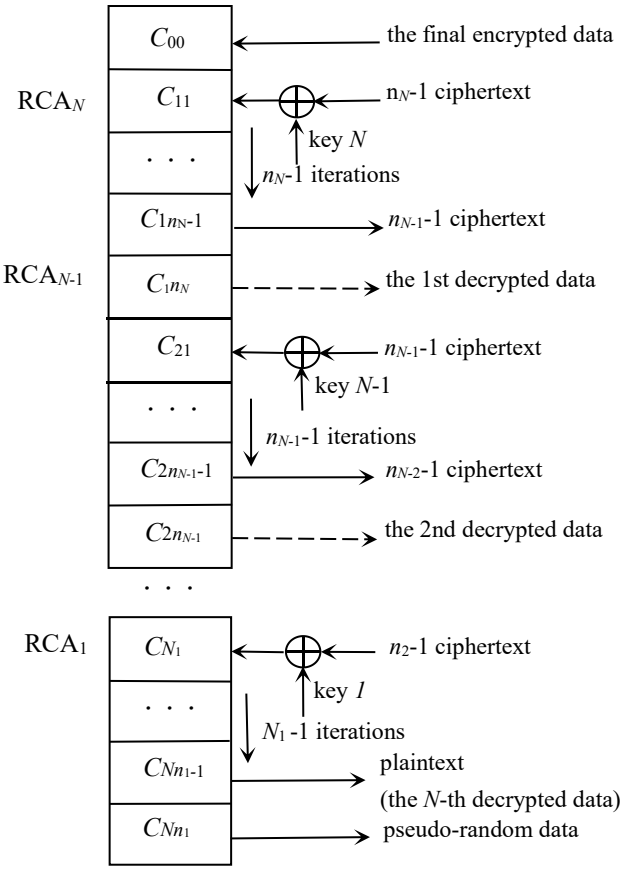


Fig. 5 Decryption based on RCA rules

B. Image encryption with several RCA rules

Assuming a gray level image to be encrypted and decrypted, its data can be denoted by a $n \times n$ matrix:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1j} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2j} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ij} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nj} & \cdots & a_{nn} \end{pmatrix} \tag{4}$$

The value of a_{ij} is between decimal 0-255, and can be expressed by 8 bit binary. In order to use one dimensional RCA, (4) is converted into one $1 \times n^2$ matrix:

$$(a_{11}\ a_{21} \cdots a_{n1}\ a_{12}\ a_{22} \cdots a_{n2} \cdots a_{1n}\ a_{2n} \cdots a_{nn}) \quad (5)$$

The RCA-based image encryption is shown in Fig. 6.

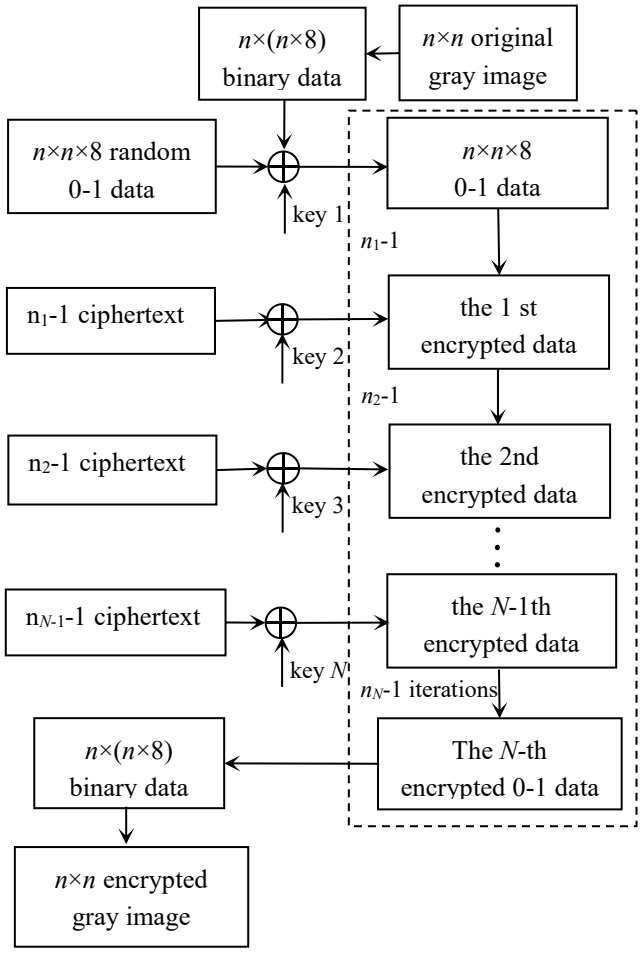


Fig. 6 Image encryption based on RCA rules

As illustrated in Fig. 6, the image encryption algorithm operates as follows. Given an $n \times n$ original grayscale image for encryption, first each pixel's decimal value is converted into its binary representation. These binary values are then rearranged into a string of 0s and 1s, with a total length of $n \times n \times 8$. This string is denoted as C_{11}. Simultaneously, a sequence of random binary data is generated, forming a string of the same length as C_{11}, which is denoted as C_{00}. Both C_{00} and C_{11} serve as the initial configuration of the RCA. The encryption process begins with n_1-1 forward iterations using the first RCA rule, producing the first encrypted data. Next, n_1-1 ciphertext and the first encrypted data are used as the new initial configuration, and another encryption step is performed by iterating forward for n_2-1 iterations according to the second RCA rule, generating the second encrypted data. This process is repeated iteratively with RCA rules until the final encrypted data is obtained.

Finally, the final encrypted data, composed of 0s and 1s, is converted back into an $n \times (n \times 8)$ binary matrix. This matrix is then transformed into an $n \times n$ decimal representation, resulting in the encrypted image.

Fig. 7 shows the process of the image decryption with RCA rules. The decryption procedure is essentially the reverse of the encryption process, achieved through backward iterations. The final encrypted data and n_N-1 ciphertext from the encryption stage serve as the initial input for decryption. By applying the same RCA rules used during encryption in reverse order, the original images can be accurately reconstructed from the decrypted data.

The rules applied in both encryption and decryption function as secret keys. One of the prominent advantages of this algorithm is their high level of security. However, a significant drawback is that if the sender and receiver lose or forget the secret keys, the encrypted image cannot be recovered, not even partially.

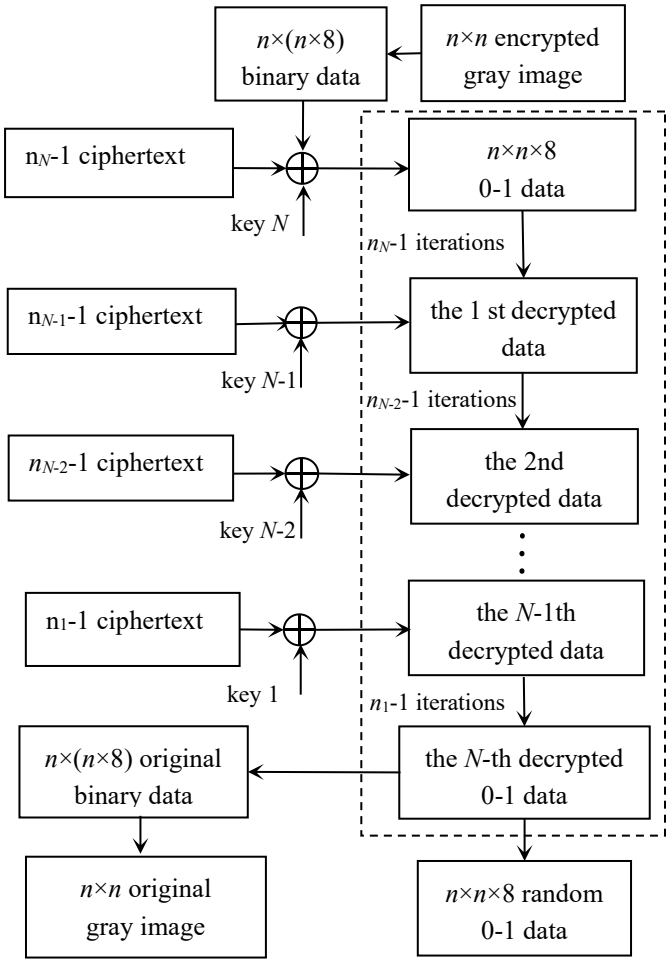
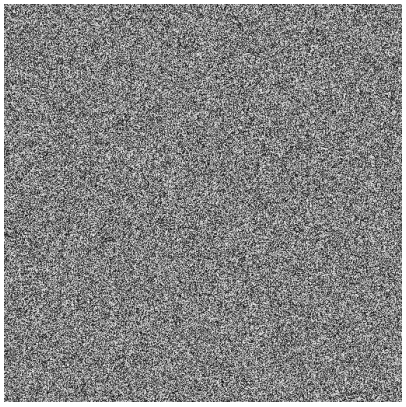


Fig. 7 Image decryption based on RCA rules

IV. Simulation Results

In all the simulation experiments, the images are of size 256×256. The confusion and diffusion properties of the proposed RCA-based image encryption method are evaluated. Fig. 8(a) presents the "Lake" image, which is used to assess the performances of the improved RCA-based encryption algorithm. To generate the encrypted images, a sequence of random 0-1 data was first generated as the initial input. Then, RCA rules 30R, 150R, and 60R were sequentially applied as encryption keys. Each RCA rule underwent 13 iterative evolution steps, after which the final binary data was converted into decimal form. As a result, the encrypted version of the "Lake" image was obtained, as shown in Fig. 8(b). It represents the final encrypted image.

(a) “Lake” image

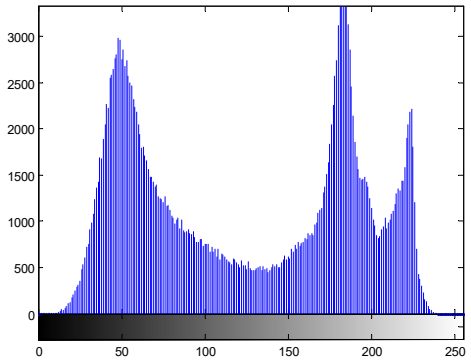


(b) the final encryption image

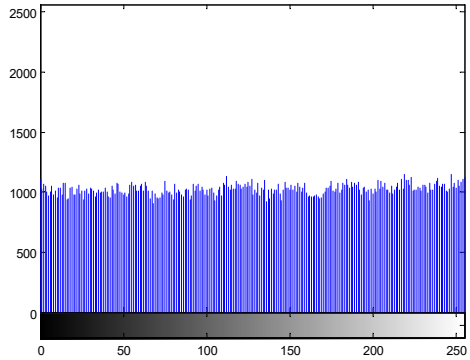
Fig. 8 “Lake” image and its encrypted version

The histograms of the "Lake" image (Fig. 9(a)) and its final encrypted version (Fig. 9(b)) demonstrate that the encrypted image exhibits an uniformly distributed pixel distribution. This result indicates that the proposed RCA-based image encryption algorithm effectively satisfies the confusion property. Furthermore, when the encrypted image undergoes the decryption process, the recovered image is identical to the original "Lake" image, verifying the reversibility and accuracy of the encryption algorithm.

To further demonstrate the security of the RCA-based image encryption algorithm, another sequence of random 0-1 data was generated and applied the same keys to encrypt the "Lake" image. Despite originating from the same source image, the two final encrypted images exhibit no similarities. This result confirms that the RCA-based encryption method satisfies the diffusion property, ensuring that minor changes in the initial data can produce significantly different encrypted outputs.



(a) Histogram of the “Lake” image



(b) Histogram of the final encrypted version

Fig. 9 Histogram of “Lake” image and its encrypted version

V. Conclusions

This paper proposes a novel image encryption algorithm considering several evolved rules of reversible cellular automata. By sequentially applying several distinct RCA rules during the encryption process, the proposed method significantly strengthens both the confusion and diffusion characteristics essential for robust image security. Compared to traditional approaches relying on a single RCA rule, this method offers a considerable improvement in resistance to cryptographic attacks while maintaining computational efficiency.

The proposed algorithm takes full advantage of the reversible nature of RCA, ensuring that the original images can be accurately and completely reconstructed during decryption without any loss of information. Experimental results confirm the method’s strong confusion capability, as the histograms of the encrypted images are uniformly distributed, showing no trace of the original image patterns. Moreover, when identical images are encrypted using different pseudo-random initial conditions, the resulting ciphertexts are highly uncorrelated. This demonstrates the excellent diffusion property of the scheme, effectively minimizing statistical similarities and enhancing overall security. These findings highlight the robustness and reliability of the encryption approach.

The improved RCA-based encryption method offers a balance between computational efficiency and robust security, thus enabling its use in real-time scenarios. However, the algorithm relies on the precise retention of encryption secret keys; losing the keys renders decryption impossible. Future studies will aim to enhance the efficiency of image management strategies and exploring the integration of RCA encryption with other cryptographic techniques to further improve security and adaptability in practical applications.

References

[1] R. K. Paul, A. Vishwakarma, and S. Chandran, "An aquatic image compression scheme based on optimized deep convolutional autoencoder," *IAENG International Journal of Computer Science*, vol. 51, no. 2, pp. 83-90, 2024

[2] H. M. Ghadirli, A. Nodehi, and R. Enayatifar, “An overview of encryption algorithms in color images,” *Signal Processing*, vol. 164, pp. 163–185, 2019.

[3] J. Sun, S. Xu, D. Liu, and J. He, "Design of belt no-load detection system based on image processing technology," *IAENG International Journal of Computer Science*, vol. 51, no. 11, pp. 1731-1739, 2024

[4] B. N. Al, "Image encryption methodology based on cellular automaton," *Journal of Theoretical and Applied Information Technology*, vol. 100, no. 23, pp. 6998–7004, 2022.
[5] Z. Hua, Z. Zhu, Y. Chen, and Y. Li, "Color image encryption using orthogonal latin squares and a new 2D chaotic system," *Nonlinear Dynamics*, vol. 104, pp. 4505–4522, 2021.
[6] G. Ye, K. Jiao, X. Huang, B. M. Goi, and W. S. Yap, "An image encryption scheme based on public key cryptosystem and quantum logistic map," *Scientific Reports*, vol. 10, 21044, 2020.
[7] T. Sivakumar and R. Venkatesan, "A novel approach for image encryption using dynamic SCAN pattern," *IAENG International Journal of Computer Science*, vol. 41, no. 2, pp. 91–101, 2014.
[8] S. F. Yousif, A. J. Abboud, and H. Y. Radhi, "Robust image encryption with scanning technology, the el-gamal algorithm and chaos theory," *IEEE Access*, vol. 8, pp. 155184–155209, 2020.
[9] Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, "A new algorithm for digital image encryption based on chaos theory," *Entropy*, vol. 23, no. 3, 341, 2021.
[10] W. Alexan, M. Elkandoz, M. Mashaly, E. Azab, and A. Aboshousha, "Color image encryption through chaos and kaa map," *IEEE Access*, vol. 11, pp. 11541–11554, 2023.
[11] M. Kumar, A. S. Chivukula, and G. Barua, "Deep learning-based encryption scheme for medical images using DCGAN and virtual planet domain," *Scientific Reports*, vol. 15, 1211, 2025.
[12] K. Morita, "Reversible computing and cellular automaton—A survey," *Theoretical Computer Science*, vol. 395, no. 1, pp. 101–131, 2008.
[13] P. L. Rosin, "Training cellular automaton for image processing," *IEEE Transactions on Image Processing*, vol. 15, no. 7, pp. 2076–2087, 2006.
[14] S. K. Nanda, S. Mohanty, P. K. Pattnaik, and M. Sain, "Throughput optimized reversible cellular automaton based security algorithm," *Electronics*, vol. 11, no. 19, 3190, 2022.
[15] G. C. Stănică and P. Anghelescu, "Reversible cellular automaton based cryptosystem," *Electronics*, vol. 13, 2515, 2024.
[16] L. Mariot, S. Picek, D. Jakobovic, and A. Leporati, "Evolutionary algorithms for designing reversible cellular automaton," *Genetic Programming and Evolvable Machines*, vol. 22, pp. 429–461, 2021.
[17] S. Bouchkaren and S. Lazaar, "A fast cryptosystem using reversible cellular automaton," *International Journal of Advanced Computer Science and Applications*, vol. 5, no. 5, pp. 207–210, 2014.
[18] S. Wolfram, "Cellular automaton as models of complexity," *Nature*, vol. 311, no. 5985, pp. 419–424, 1984.
[19] J. Kari, "Theory of cellular automaton: A survey," *Theoretical Computer Science*, vol. 334, no. 1–3, pp. 3–33, 2005.
[20] F. Seredynski, P. Bouvry, and A. Y. Zomaya, "Cellular automaton computations and secret key cryptography," *Parallel Computing*, vol. 30, no. 5–6, pp. 753–766, 2004.
[21] J. Kari, "Reversible cellular automaton: from fundamental classical results to recent developments," *New Generation Computing*, vol. 36, pp. 145–172, 2018.
[22] N. Abbassi, M. Gafsi, R. Amdouni, M. A. Hajjaji, and A. Mtibaa, "Hardware implementation of a robust image cryptosystem using reversible cellular-automaton rules and 3-D chaotic systems," *Integration*, vol. 87, pp. 49–66, 2022.
[23] Y. Su, Y. Wo, and G. Han, "Reversible cellular automaton image encryption for similarity search," *Signal Processing: Image Communication*, vol. 72, pp. 134–147, 2019.
[24] A. M. Latif and Z. Mehrnahad, "A novel image encryption scheme based on reversible cellular automaton," *Journal of Electronic & Information Systems*, vol. 1, no. 1, pp. 18-25, 2019.
[25] R. Dehghani and H. Kheiri, "Chaotic-based color image encryption using a hybrid method of reversible cellular automaton and DNA sequences," *Multimedia Tools and Applications*, vol. 83, pp. 17429–17450, 2024.

Zhihua Feng is currently a researcher at the School of Science, Dalian Jiaotong University, China. She received her B.S. degree in Applied Mathematics from Liaoning University, China, in 2001, and her M.S. degree in Applied Mathematics from Dalian Maritime University, China, in 2008. Her research interests focus on image encryption and compression.