Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1639–1648
DOI : 10.47974/JDMSC-2164

1-D group cellular automata based image encryption scheme : A lightweight approach for IoT devices

B. Vijaya Bhaskara Rao [§]
Umashankar Rawat [†]
Satyabrata Roy *
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Utsav Upadhyay [‡]
Department of Computer Science & Engineering
Sir Padampat Singhania University
Udaipur 313601
Rajasthan
India

Abstract

In the era of IoT, ensuring data security and privacy is crucial given the limited computational resources of IoT devices. This article presents an image encryption scheme utilizing one-dimensional group cellular automata (1-D GCA) to offer a lightweight and robust solution for image security. The method leverages the parallelism and simplicity provided by cellular automata for efficient encryption and decryption and leverages 1-D GCA to produce pseudo-random sequences for pixel-permutation and substitution, thereby strengthening security by altering spatial and statistical characteristics. Experiments and analyses demonstrate its effectiveness against various attacks and show significant performance improvements over traditional methods, making it suitable for real-time IoT applications.

Subject Classification: *Primary 94A60, Secondary 68P25.*

Keywords: *Image encryption, Cellular automata, Security, Lightweight.*

[§] *E-mail:* **bvb.rao@gmail.com**
[†] *E-mail:* **umashankar.rawat@jaipur.manipal.edu**
* *E-mail:* **satyabrata.roy@jaipur.manipal.edu (Corresponding Author)**
[‡] *E-mail:* **upadhyay.utsav@gmail.com**

© Taru Publications

1. Introduction

The extensive use of "Internet of Things (IoT)" devices has brought a substantial revolution in several industries, such as healthcare, smart homes, and industrial automation. These devices, which range from sensors and actuators to smart appliances, produce and transmit massive quantities of data that are often sensitive and critical. Consequently, ensuring the protection of this data's security and privacy is of utmost importance. However, the intrinsic limitations of IoT devices, including restricted processor capabilities, memory capacity, and energy supply, provide considerable obstacles to the implementation of conventional cryptographic methods.

Image encryption is a critical area of focus within IoT security, particularly for applications involving surveillance, medical imaging, and personal media. Long-established algorithms like "Advanced Encryption Standard (AES)" [1] and "Rivest-Shamir-Adleman (RSA)" [2], while secure, are computationally intensive and may not be feasible for real-time applications on resource-constrained IoT devices [3]. Therefore, there is a pressing need for lightweight encryption schemes that can provide robust security without overwhelming the limited resources of these devices.

"Cellular Automata (CA)" [4], a category of dynamic discrete systems, have gained attention in recent years as a promising tool for designing lightweight cryptographic algorithms. CA comprise a grid of cells, with each cell capable of being in one of a limited number of states. The state of every cell progresses over discrete steps as per a local rule that varies on the statuses of adjacent cells. This simple, yet powerful, structure allows CAs to exhibit complex and unpredictable behaviour, making them suitable for cryptographic applications.

This article introduces an innovative image encryption scheme utilizing one-dimensional (1-D) "Group Cellular Automata (GCA) [5], aimed at providing a lightweight yet secure solution for IoT devices. The use of 1-D GCA is motivated by their simplicity and efficiency, which are crucial for resource-constrained environments. Our proposed scheme leverages the pseudo-random sequence generation capabilities of 1-D GCA to perform pixel value permutation and substitution operations on images, thereby achieving high levels of security with minimal computational overhead. The principle findings of this article are outlined below:

1. Design of a 1-D GCA-based image encryption scheme: We develop a novel encryption algorithm that utilizes the pseudo-random sequences generated by 1-D GCA for pixel permutation and substitution, increasing the protection of the generated image.
2. Performance evaluation: Comprehensive experiments were performed to assess the strength of the proposed algorithm through statistical and key sensitivity analyses, showcasing its effectiveness for real-time applications on IoT devices.

2. Related works

Cellular automata (CA), introduced by S. Ulam in the 1940s [6], are discrete computational systems that have found applications in various fields, including cryptography. The grid of cells in a CA has a finite number of states. At each discrete step, every cell's state is updated according to a predefined rule that depends on the states of its neighboring cells. The simplicity, parallelism, and local interaction properties of CA make them suitable for cryptographic applications, particularly in scenarios requiring lightweight and efficient algorithms.

In recent years, cellular automata have been extensively studied for their potential in cryptographic schemes. Researchers have explored both one-dimensional (1-D) [3][7] and two-dimensional (2-D) CA for encryption [8] [9][10] and pseudorandom number creation. Wolfram's pioneering work in the 1980s demonstrated the suitability of elementary CA for cryptographic purposes, showing that simple rules could generate complex and unpredictable behavior, a desirable property for encryption.

The use of 1-D CA in image encryption has gained attention due to its simplicity and low computational overhead [8][11]. Group cellular automata (GCA), a generalization of classical CA, operate on groups rather than individual cell states, enabling more complex and flexible rule definitions. GCA can enhance the security of CA-based cryptographic schemes by increasing the complexity of the state transition rules and providing a larger key space.

Several studies have demonstrated the effectiveness of 1-D GCA in image encryption. For instance, a 1-D CA-based image encryption scheme that utilized a combination of permutation and substitution operations were proposed in [12]. Their methodology has attained an optimal equilibrium between security and computational performance, rendering it well-suited for real-time applications.

Recent research has focused on developing encryption algorithms specifically tailored for IoT environments. Lightweight cryptographic primitives, such as PRESENT [13] and SPECK [14], have been designed to provide adequate security with minimal resource consumption. However, these algorithms still face challenges in balancing security, efficiency, and ease of implementation.

3. Group Cellular Automata Rule vector generation

GCA rules are special types of CA rules having a cyclic property i.e., if we apply a rule vector [8] in an initial binary bit-stream, then after certain iterations, say n, the bit-stream is regenerated. This n is called the order of the group. The characteristic matrix, T can be used to determine whether a particular CA is GCA using the following equation (1) [5].

$$[T]^n = I \tag{1}$$

were, n is the group order and I is the identity matrix of the same size as of T. For a 2-state 3 neighborhood CA, some of the GCA rules are listed below whose group order is 8:

{51,198,51,51,53,195,195,150},

{102,43,195,195,51,156,51,51},

{106,15,153,153,153,51,51,51}.

Here each number represents the CA-rule number. Since each configuration consists of more than one CA rule, these GCA rule vectors are hybrid rule vectors.

4. Proposed Model

The proposed image encryption scheme leverages the properties of 1-D Group Cellular Automata (GCA) to provide a lightweight and secure method suitable for IoT devices. The scheme involves a series of stages, each designed to improve the security of the image while preserving computational efficiency. The following Figure 1 depicts the main components and workflow of the proposed encryption scheme. The following are the detailed steps involved:

Image Preprocessing: The input image is initially changed to a gray-scale image and then normalized. This step simplifies the encryption process by reducing the complexity of the image data.

Initial Key Generation: A random initial key is generated. This key serves as the seed for the subsequent key expansion process.

Key Expansion using Group Cellular Automata: The initial key is expanded using 1-D Group Cellular Automata rules. The GCA rules are applied iteratively to generate a pseudorandom sequence of keys that will be used in the permutation and substitution processes. This step ensures a high level of security by creating a complex and unpredictable key stream.

Permutation Process: The pixel positions of the image are shuffled based on the keys generated in the previous step. This scrambling of pixel positions ensures that the spatial relationships between pixels are obfuscated, making it hard for anyone to reconstruct the actual image.

Substitution Process: The pixel-values of the permuted figure are then modified using the keys generated by the GCA. The substitution process involves changing the pixel values according to the GCA rules, further strengthening the security.

Algorithm 1: GCA-Based Image Encryption

Input: Original Image (I), Initial Key (K), Number of rounds (n)
Output: Encrypted Image (E)

1. Preprocess the Image:
   a. Convert the input image I to a grayscale image G.
   b. Normalize the grayscale image G to have pixel values in the range [0, 255].
2. Generate Initial Key:
   a. Generate a random initial key K of length equal to the width of the image.
3. Key Expansion using GCA:
   a. Initialize the key array with the initial key K.
   b. For each iteration from 1 to n:
      i. Apply GCA rules to the key array to generate a new key sequence.
      ii. Store the new key sequence.
4. Permutation Process:
   a. Flatten the grayscale image G into a 1-D array P.
   b. For each pixel position i in P:
      i. Determine the new position using the key sequence generated from GCA.
      ii. Swap the pixel at index i with the new position.

5. Substitution Process:
   a. For each pixel value i in the permuted array P:
      i. Modify the pixel value using the corresponding value from the GCA key sequence.
      ii. Apply the GCA rules to alter the pixel value based on its neighbors.
6. Reshape the 1-D array back to the actual image dimensions to form E.
7. Return E.

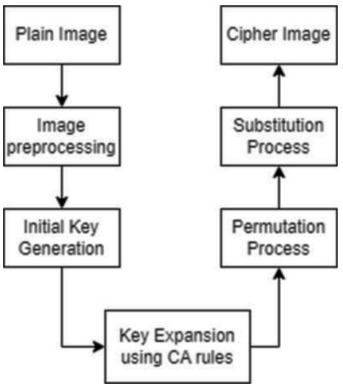

Figure 1

Proposed Encryption Strategy

Encrypted Image: The final output is the encrypted image, which can be transmitted securely over insecure channels. The decryption process reverses the encoding steps, employing the same initial key.

The encryption scheme has been represented in the form of an algorithm in Algorithm 1. It should be noted that the image cipher is a symmetric cipher and the decipherment of the generated cipher-image could be done using exactly the inverse steps of the encryption scheme. All the operations involved consumed very low space, i.e. in the order of the image size. The CA operations were performed through XOR and as a result it was lightweight in nature.

5. Results and Discussion

In this section the result of the encryption has been presented along with the detailed performance and security analysis. The test images

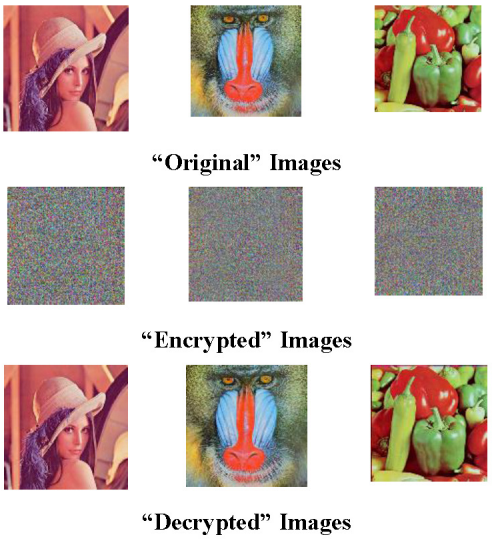

Figure 2

Result of the proposed scheme

considered were Lena, Baboon and Peppers. Fig. 2 shows the original, scrambled and deciphered images.

4.1 *Performance Analysis*

Examination of the performance of the proposed 1-D GCA-based encryption scheme, we performed a series of experiments using test images. The following metrics and criteria were used for the evaluation:

- **Key Sensitivity**: Assessed by decrypting the same cipher image with slightly varied keys and analyzing the resultant decrypted images. The result is shown in Fig. 3.

Decrypted Images with minor change in key

Figure 3

Result of Key Sensitivity Analysis

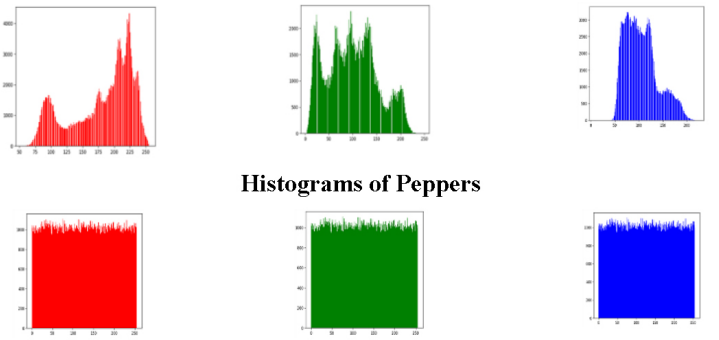

Figure 4

Result of histogram analysis

- **Statistical Analysis**: Experimented to assess the randomness and uniformity of the generated cipher-images, with histogram-analysis and information-entropy values serving as assessment metrics, alongside "Mean Squared Error (MSE)" and "Peak Signal-to-Noise Ratio (PSNR)" [15]. The result of histogram analysis is shown in Fig. 4. The comparative results of MSE, PSNR and corresponding "Correlation Coefficient (CC)" values are presented in Table 1 from where it highlights that the proposed method outperforms other existent techniques. The comparative results of MSE, PSNR, Entropy, NPCR and UACI values are presented in Table 1 from where it highlights that the proposed method outperforms other existent techniques.

Table 1

Outcome of Statistical Analyses

	Proposed Method	Ref. [16]	Ref. [10]	Ref. [11]
MSE	82.45	72.73	82.38	74.18
PSNR	28.94	29.54	28.95	29.46
Entropy	7.9995	7.9993	7.9895	7.9934
NPCR	99.7974	99.6967	99.7412	94.9703
UACI	33.5423	32.2956	33.4033	31.5159

6. Conclusion

This article presents a 1-D Group Cellular Automata-based image encryption scheme designed for lightweight, secure encryption in IoT devices. The proposed method leverages group algebra to achieve robust encryption with linear scalability, ensuring efficient performance even in resource-constrained environments. Performance analysis demonstrates manageable encryption and decryption times, while security tests confirm high key sensitivity and effective disruption of pixel correlations. Overall, the scheme offers a practical solution for secure image encryption, balancing efficiency and security for modern IoT applications. Future work will focus on enhancing security features and optimizing performance.

References

[1] A. M. Abdullah, "Advanced encryption standard (AES) algorithm to encrypt and decrypt data," *Cryptography and Network Security*, vol. 16, no. 1, p. 11 (2017).

[2] P. Mahajan and A. Sachdeva, "A study of encryption algorithms AES, DES and RSA for security," *Global Journal of Computer Science and Technology*, vol. 13, no. 15, pp. 15–22 (2013).

[3] S. Roy, U. Rawat, and J. Karjee, "A lightweight cellular automata based encryption technique for IoT applications," *IEEE Access*, vol. 7, pp. 39782–39793 (2019).

[4] T. A. Dhopavkar, S. K. Nayak, and S. Roy, "IETD: a novel image encryption technique using Tinkerbell map and Duffing map for IoT applications," *Multimedia Tools and Applications*, vol. 81, no. 30, pp. 43189–43228 (2022).

[5] S. Nandi, B. K. Kar, and P. P. Chaudhuri, "Theory and applications of cellular automata in cryptography," *IEEE Transactions on Computers*, vol. 43, no. 12, pp. 1346–1357 (1994).

[6] K. C. Clarke, "Cellular automata and agent-based models," in *Handbook of Regional Science*, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 1751–1766 (2021).

[7] S. Nandi, S. Roy, S. Nath, S. Chakraborty, W. B. A. Karaa, and N. Dey, "1-D group cellular automata based image encryption technique," in *Proc. 2014 Int. Conf. Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, pp. 521–526 (July 2014).

[8] K. Kumar, S. Roy, U. Rawat, and A. Shandilya, "SOCIET: Second-order cellular automata and chaotic map-based hybrid image encryption technique," *Multimedia Tools and Applications*, vol. 83, no. 10, pp. 29455–29484 (2024).

[9] 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 (2021).

[10] S. Roy, M. Shrivastava, C. V. Pandey, S. K. Nayak, and U. Rawat, "IEVCA: An efficient image encryption technique for IoT applications using 2-D Von-Neumann cellular automata," *Multimedia Tools and Applications*, vol. 80, pp. 31529–31567 (2021).

[11] J. Jin, "An image encryption based on elementary cellular automata," *Optics and Lasers in Engineering*, vol. 50, no. 12, pp. 1836–1843, 2012.

[12] S. W. Kang, U. S. Choi, and S. J. Cho, "Fast image encryption algorithm based on (n, m, k)-PCMLCA," *Multimedia Tools and Applications*, pp. 1–27 (2022).

[13] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An ultra-lightweight block cipher," in *Proc. 9th Int. Workshop Cryptographic Hardware and Embedded Systems (CHES)*, Vienna, Austria, Sep. 10–13, 2007, pp. 450–466. Berlin, Germany: Springer (2007).

[14] A. Biryukov, A. Roy, and V. Velichkov, "Differential analysis of block ciphers SIMON and SPECK," in *Proc. 21st Int. Workshop Fast Software Encryption (FSE)*, London, U.K., Mar. 3–5, 2014, Revised Selected Papers, vol. 21, pp. 546–570. Berlin, Germany: Springer (2015).

[15] S. Roy, U. Rawat, H. A. Sareen, and S. K. Nayak, "IECA: an efficient IoT friendly image encryption technique using programmable cellular automata," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, pp. 5083–5102 (2020).

[16] 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 (2019).

Received November, 2024