JNNCE Journal of Engineering & Management, Volume 6, No.1, Jan – June 2022 ISSN 2582-0079
This paper is presented at National Workshop on Cryptology NWC 2021, held at JNN College of Engineering, Shimoga during 18-20 Nov 2021

Available online @ https://jjem.jnnce.ac.in
https:www.doi.org/10.37314/JJEM.2022.060112
Indexed in International Scientific Indexing (ISI)
Impact factor: 1.395 for 2021-22
Published on: 31July 2022

# Securing the Information Contents in Images based on Cellular Automata and Genetic Operations – a Parallel Approach

[1*]Jalesh kumar [2]Chakrapani D S

[1,2] Department of Computer Science and Engineering

JNN College of Engineering, Shivamogga- 577 204

jaleshkumar@jnnce.ac.in, chakrads@jnnce.ac.in

***Abstract***

*In this paper, a parallel encryption approach is proposed based on cellular automata and genetic operations to secure image at different levels. The proposed method comprises of three stages. In the first stage, rules of cellular automata are selected based on pseudo random number generator to generate the key sequence. Among the key sequence generated crossover operation is applied in the second stage. The input image is decomposed into different blocks of uniform size which are processed in parallel. Encryption process is carried out by varying the position for crossover operation of genetic algorithm. The performance analyses of the proposed methods are measured in terms of Structural Similarity Index, entropy and Peak Signal to Noise Ratio. The analysis carried out reveals that the proposed methods work efficiently to secure the multimedia information.*

**Keywords:** *Digital image; Security; Crossover; Cellular automata*

## 1. Introduction

Secure storage and transmission of information is a challenging task in today's highly computerized world. Ancient methods available in Sanskrit literature [1] to conventional methods available in today's world versatile techniques are available for securing the information.

Communications in modern technology takes place through internet with information. Information contains not only textual, even images and videos. Sharing of such information in less time also needs protecting from hackers. Many approaches have been proposed based on standard methods, chaos, or SCAN patterns [2]. Most of the approaches are compromising between computational complexity and speed to process large multimedia information. It is difficult to secure large size satellite images, text document images or medical images with reduced computation time. By taking the advantage of today's multi core processors a parallel approach is proposed to encrypt images of large size.

A recent past many cryptographic techniques were proposed to secure image contents. Many of the techniques are on serial approach rather than a parallel approach. In this work a parallel approach is also carried out for encryption. The rest of this paper is organized as follows.

Literature survey is carried out in section 2. The operations of cellular automata are discussed in section 3. Section 4 discusses the proposed approach. In section 5, experimental results are explained. Section 6 analyses the results obtained. Section 7 summarizes with conclusions.

## 2. Literature Survey

To secure the information contents different types of cryptographic schemes are needed. In recent literature various techniques are available to protect the information in images. Image security can be applied on frequency domain or spatial domain. Further, the methods are categorized either full or partial encryption according to need of the security. Many cryptographic methods were proposed to secure information of an image [2]. Most of the techniques are on serial approach with single core rather than multicore architecture. In [3], encryption technique using parallel chaos has been discussed. Chaotic sequence is generated using Piecewise linear map. In [4], encryption operation is performed in parallel based on RGB colors. Encryption operation is performed based on Lorenz chaotic sequences. Image encryption algorithm using discrete chaotic map is discussed in [5]. Input image is decomposed into sub images in the proposed work. Advanced encryption standards algorithm is used to secure each sub images. Mirzaei discusses a parallel image encryption approach with chaos method [6]. Four sub images are created from the input image. Each sub images are scrambled based on permutation. Logistic sequence also applied for scrambling. Cipher Block Chaining is implemented in the proposed work. Cellular automata based parallel encryption techniques are discussed in [7,8]. Rules of Cellular automata are used to generate the sequence in the proposed work. Behavior of cellular sequence is utilized for parallel operation. RSA encryption algorithm using parallel platform (Compute Unified Device Architecture) is carried out in [9]. But analysis is not discussed to prove the efficiency of the method. Self adaptive parallel encryption algorithm based on discrete 2D-Logistic map is described in [10]. Binary sequences obtained from the logistic map are used to distribute mode of processors.

It is revealed from the survey that different techniques are available for image encryption. A new dimension in the field of encryption is provided by Evolution algorithms. In this paper, an encryption approach is proposed for securing the contents of an image using genetic algorithm and cellular automata. According to the required security level block are selected and crossover operation is performed.

## 3. Cellular Automata

It is a grid of cells with different number of states which are finite. The behavior of each cell is associated with its adjacent cells. Wolfram cellular automata consists of 256 different rules. Rules are classified into one among four classifications namely, uniformity, repetition, random, and complexity.

For three bit numbers different combinations are

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |

For example, rule 70 is represented as 01010000 which is binary equivalent of 70.For rule 70 if the adjacent value is ‘0’ and middle value is ‘0’, the output bit is ‘0’. As a result, relying on the neighbour values next output bit is generated.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
| 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 |

Consider the initial value “10101100”. When rule 70 is applied to the initial bits, next sequence generated is “00001111”. Circular bits are selected for last and first bits when neighbors are considered.

Initial bits: 1 0 1 0 1 1 0 0
Next sequence: 0 0 0 0 1 0 0 1

The sequence obtained after applying the rule 30 with initial bits “10101100” are as shown below

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
| 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 |

Initial bits: 1 0 1 0 1 1 0 0
Next sequence: 0 1 0 1 1 1 1 0

## 4. Proposed Approach

In the proposed approach cellular automata sequence is combined with crossover operation of genetic algorithm for encryption operation. Different levels of operation is carried out based on number of blocks which process in parallel. Figure 2 shows the proposed approach. The input image is divided into different blocks of size 4,16,64 and 256. Each block is processed in parallel. For the key sequence cellular automata is used. Based on pseudo random number generator cellular automata rule is selected.

Depending on the rule selected next sequence is generated until the sequence is repeated. Among the $K_n$ sequence generated crossover operation is performed between $K_1$ & $K_{2,\ldots}$ $K_{n-1}$ & $K_n$. Among 'n/2' crossover operations one is selected based on more number of 1s in the sequence for encryption operation.

Example for crossover operation :

Consider two initial values which considered as parents P1: 01010101 & P2 : 11001010

By considering crossover point as 5, new offspring's generated are Offspring 1: 01001010 & Offspring2: 11010101

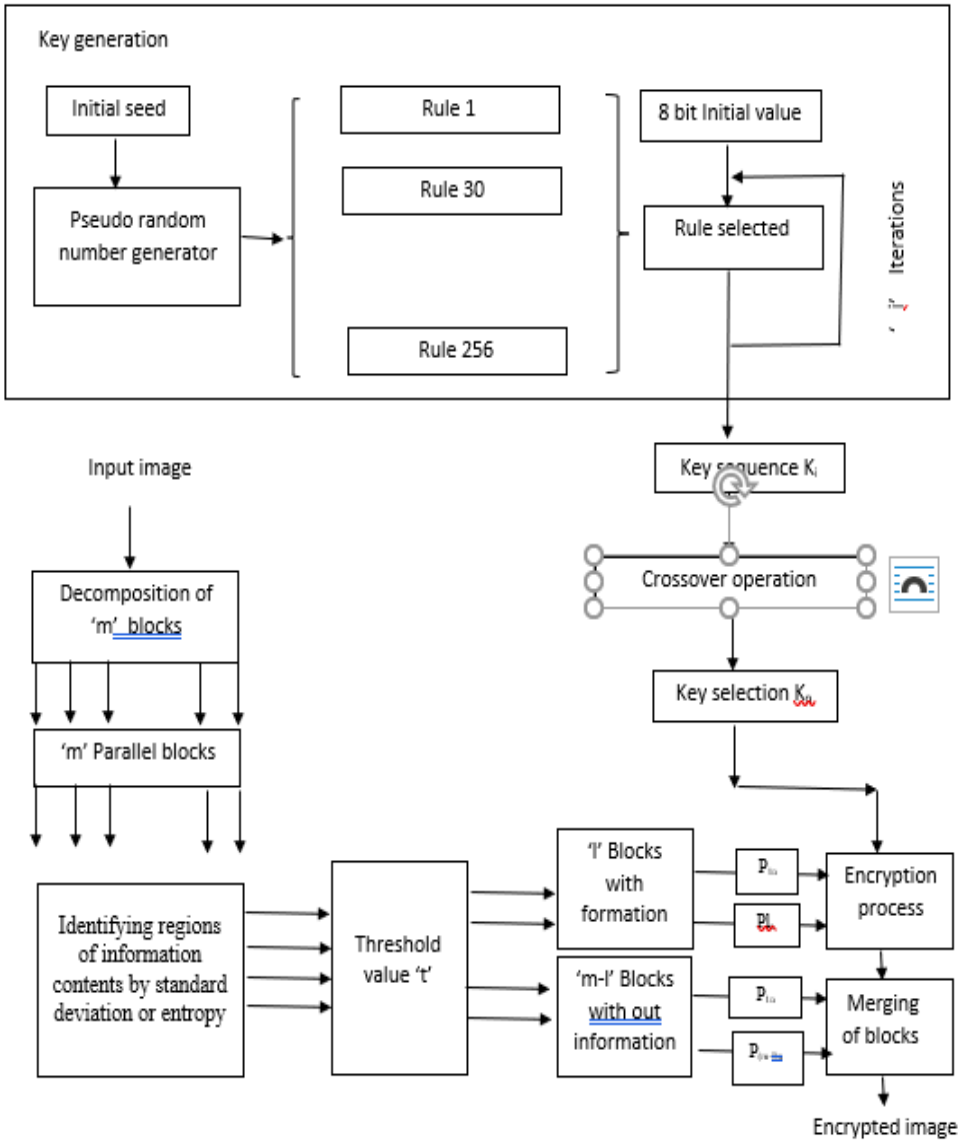


Figure 2: Block diagram of proposed approach

## 5. Results

The experiments are conducted on the sample color images. Corpus used for experiments contain 250 color images of 256 X 256 size. Different level of encryption is performed based on the number of blocks which is processed in parallel. The experiments are conducted by considering the number of blocks of size 4, 16, 64 and 256. Figure 3 (a) show the sample input color image. The encrypted images based on the proposed approach for the block size 4 is shown in Figure 3(b). The decryption process is the reverse of encryption process. Figure 3 (c) show the decrypted images. It is observed from the result obtained that the cipher image will not give any clue about the original input image.

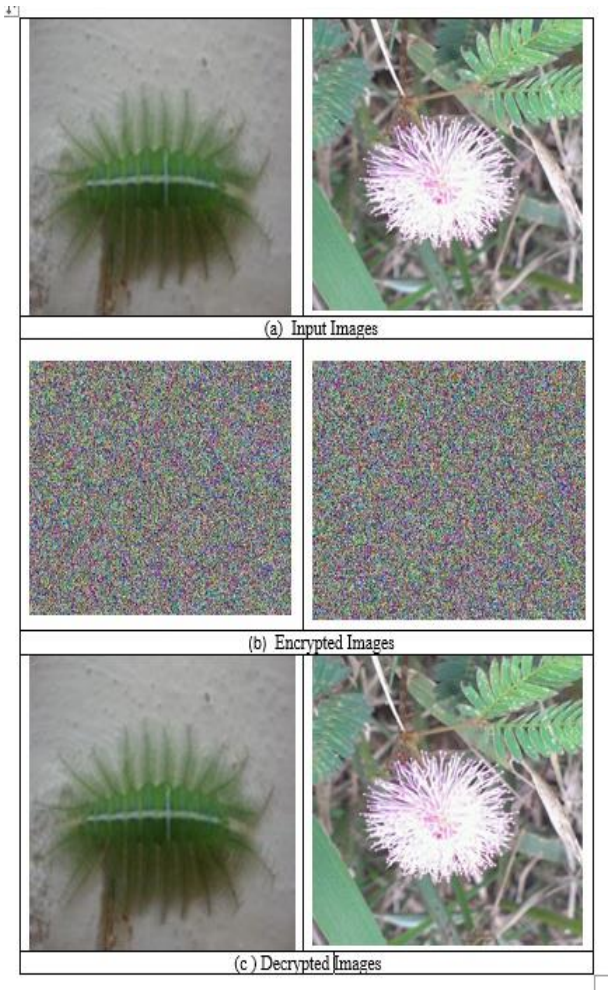


Figure 3: Experimental results for sample images for blocks of size 4.

It is also observed that the decrypted image obtained is without loss of any information contents. The sample results for parallel blocks of size 16 are in Figure 4.

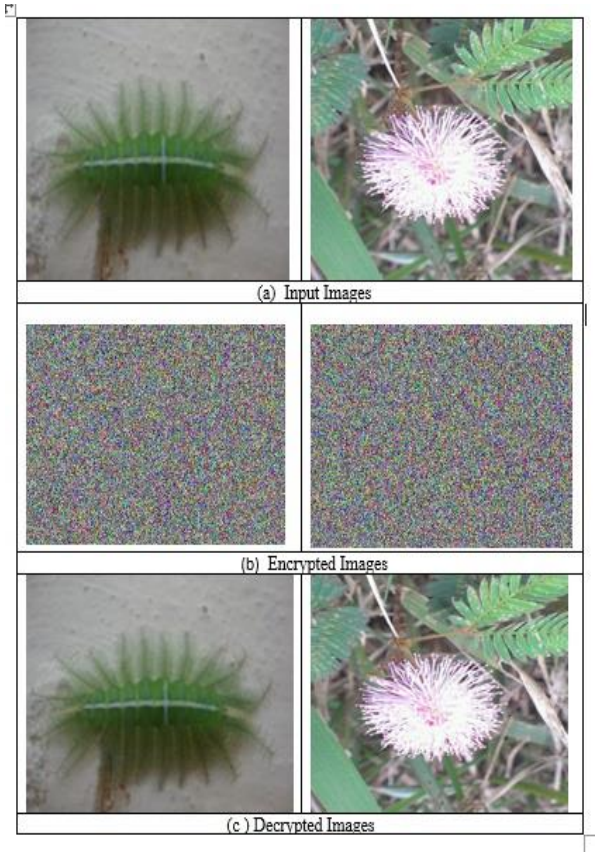


Figure 4: Experimental results for sample images for blocks of size 16.

## 6. Result Analysis

To evaluate the performance of the proposed method, statistical analysis is carried in terms of structural similarity index, peak Signal to noise ratio and entropy [11,12].

Similarity between two images is computed based on Structural Similarity Index (SSI). It is found to be 1 if images are similar and 0 if no similarity. The value of SSI computed between input and encrypted image is tabulated in Table 1. Similarly, the SSI calculated between input image and decrypted image is in Table 2. It is evident from values in Table 2 that the

decrypted image is same as input image without any loss of information

Table 1: Avg. SSI between input image and Cipher

| SSI | | | |
|---|---|---|---|
| Parallel Operation (No. of blocks) | | | |
| 4 | 16 | 64 | 256 |
| 0.019 | 0.0174 | 0.0137 | 0.0244 |

Table 2: Avg. SSI between input image and decrypted image

| SSI | | | |
|---|---|---|---|
| Parallel Operation (No. of blocks) | | | |
| 4 | 16 | 64 | 256 |
| 1 | 1 | 1 | 1 |

The Peak Signal to Noise Ratio (PSNR) is calculated between input image and encrypted image. PSNR between two identical images are equal to infinity. Hence, low value of PSNR indicates that the encrypted image will not reveal any clue about the input image. It is evident from the Table 3 that the encrypted image does not provide any residuals about input image.

Table 3: Avg. PSNR between input image and cipher

| PSNR Values | | | | |
|---|---|---|---|---|
| Parallel Operation (No. of blocks) | | | | Serial Operation |
| 4 | 16 | 64 | 256 | |
| 10.51 | 10.49 | 10.48 | 10.46 | 10.47 |

Entropy is used to find the measure of randomness in the encrypted image. Standard value for entropy is 8. Table 4 shows the value of entropy computed on the encrypted images. It is observed from the entropy value computed that the encrypted image is completely scrabbled.

Table 4: Avg. Entropy values

| Entropy Values | | | | |
|---|---|---|---|---|
| Parallel Operation (No. of blocks) | | | | Serial Operation |
| 4 | 16 | 64 | 256 | |
| 7.79 | 7.84 | 7.89 | 7.92 | 7.90 |

## 7. Conclusion

In this work, parallel encryption process is designed and implemented. Key sequence is generated based on the cellular automata. Based on pseudo random number generator, rules of cellular automata is selected. Key sequence generated is selected by performing crossover operation of the genetic algorithm on the sequence. In the proposed approach genetic process is combined with cellular automata rules. To decrease the processing time, parallel operations are carried out by dividing the image in terms of various blocks. Depending on the number of blocks different level of encryption is achieved. The experiment results and analysis carried out reveals that the proposed design is suitable for securing multimedia information's.

## References

1. Subhash C. Kak, Some early codes and ciphers, Indian J. of History of Science, Vol.24, No.1, 1989. pp.1-7.

2. Marwa Abd El-Wahed et al.,Efficiency and Security of Some Image Encryption Algorithms, in Proc. World Congress on Engineering 2008, Vol 1, 2008, pp. 822-1706.

3. Xizhong Wang and Deyun Chen, A Parallel Encryption Algorithm Based on Piecewise Linear Chaotic Map, Mathematical Problems in Engineering, Vol. 2013. 2013.

4. Y. Wang and C. Y. Han, A Parallel Encryption Algorithm for Color Images Based on Lorenz Chaotic Sequences, Conference Proceedings on 6th World Congress on Intel- ligent Control and Automation, Dalian, 21-23 June 2006, pp. 9744-9747.

5. Zhou, K. W. Wong and X. F. Liao, Parallel Image En- cryption Algorithm Based on Discretized Chaotic Map, Chaos Soliton & Fractals, Vol. 29, No. 11, 2008, pp. 1081-1092.

6. O. Mirzaei, M. Yaghoobi and H. Irani, A New Image En- cryption Method: Parallel

Sub-Image Encryption with Hyper Chaos, Nonlinear Dynamics, Vol. 67, No. 1, 2012, pp. 557-566.

7. Faraoun Kamel Mohamed, A parallel block-based encryption schema for digital images using reversible cellular automata, Engineering Science and Technology, an International Journal 17, 2014, pp. 85-94.

8. Debasis Das and Abhishek Ray, A Parallel Encryption Algorithm for Block Ciphers Based on Reversible Programmable Cellular Automata, Journal Of Computer Science And Engineering, Vol. 1, No. 1, May 2010.

9. Vaibhav Tuteja, Image Encryption Using Parallel RSA Algorithm on CUDA, International Journal of Computer Networks and Communications Security, Vol. 2, No. 7, July 2014, pp.232–235.

10. Jing Wang and Guoping Jiang, A Self-Adaptive Parallel Encryption Algorithm Based on Discrete 2D-Logistic Map, International Journal of Modern Nonlinear Theory and Application, 2013, 2, pp.89-96.

11. Jalesh Kumar and S. Nirmala, A Hybrid Approach for Enhancing the Security of Information Content of an Image, Multimedia Processing, Communication and Computing Applications, Lecture Notes in Electrical Engineering 213, DOI: 10.1007/978-81-322-1143-3_14, _ Springer India 2013.

12. Kumar, J., Nirmala, S., A new light weight encryption approach to secure the contents of image,International Conference on Advances in Computing, Communications and Informatics ICACCI, 2014, pp. 1309–1315. IEEE (2014)