International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 16
June 2018

Data Security Using 2d Cellular Automata Rules

Roshani Lata
Kanpur Institute of Technology
Roshnichandra04@gmail.com

Abstract- *This paper deals with secure transmission of text. Since we are moving towards complete online era so it is important to encrypt sensitive information before transmission. This paper introduces two levels of encrypting text in image. In first level, ELSB & LSB techniques are used to hide plain text in cover image using password. In second level 2D- Cellular Automata rules are applied to generate final encrypted image.*

1. INTRODUCTION

Cryptography & Steganography plays important and vital application in security, defense, medical, business and many other application areas. Steganography is hiding information in plain sight and Cryptography is the approach to achieve safety by using encoding messages to make them non-recognizable language. Here steganography is used to hide text in image and 2D CA rules are applied to encrypt the image.

2. BACKGROUND

2.1 Cellular Automata

A Cellular Automata (CA) is defined by the 4 tuple: (D, S, N, and R) Where, D is the dimension of CA

S is the set of the finite states

N is the neighborhood vector=(x_1, x2, x3, x4,……..,x_n)

R is the set of local rules.

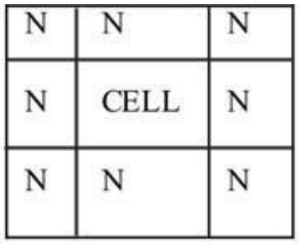
This is an idealized parallel processing machine, which is an array (1-D, 2-D, 3-D or nD) of numbers or symbols called cell values together with an updating rule. A cell value is updated according to the cell value as well as other cell values in a particular neighborhood.

A. Neighborhood

If we consider d-dimensional grid it is possible to define different kinds of neighborhood. In particular if we consider two-dimension CA then the most common neighborhoods is:

1. VonNeumann:Only North, South, West and East neighborhood.(Four neighborhoods)
2. Moore: One adds the diagonals to Von Neumann to form nine neighborhoods.
3. Extended Moore: One extends the distance of neighborhood beyond one.

Figure 1 shows the structure of two dimensional cellular automata neighborhood cells respectively. In both of these figures, central cell is denoted by CELL and all of its 9 neighborhood are denoted by N.



N	N	N
N	CELL	N
N	N	N

Figure 1: 2D Moore neighborhood

B. *Two-dimensional cellular automata*

Two-dimensional cellular automaton consists of an infinite (or finite) grid of cells, each in one of a finite number of states. Time is discrete and the state of a cell at time t is a function of the states of its neighbors at time t-1.For two-dimensional cellular automata two types of cellular neighborhoods are usually considered .In Von Neumann neighborhood five cells are considered. That is Only North, South, East, West, and itself. In Moore neighborhood nine cells are considered (as shown in figure 1).

2D CA rules as Boolean functions

Table 1 shows all the rules of two dimensional cellular automata.

64	128	256
32	1	2
16	8	4

Table I: 8-neighborhood CA rules

2.2 *Encryption Degree Measurement Parameters*

1. MSE (Mean square Error)
2. PNSR (Peak Noise to Signal Ratio)
3. Correlation
4. GDD (Gray Difference & Degree)
5. Entropy Encrypted

3. PROPOSED SYSTEM

Block diagram shows the method used in this paper. It is done in two levels.

1st level: In first level of security, two most famous techniques LSB(Least significant bit) and ELSB(enhanced least significant bit)[10] are used to insert text in cover image.

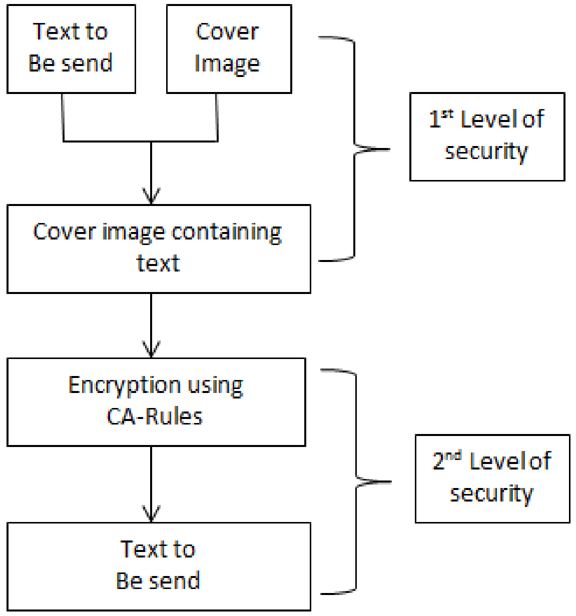


Fig. 2. Block Diagram of proposed Algorithm.

2nd Level: In second level 2-D CA rules are applied to cover image containing text to get final encrypted image which is safe for transmission.

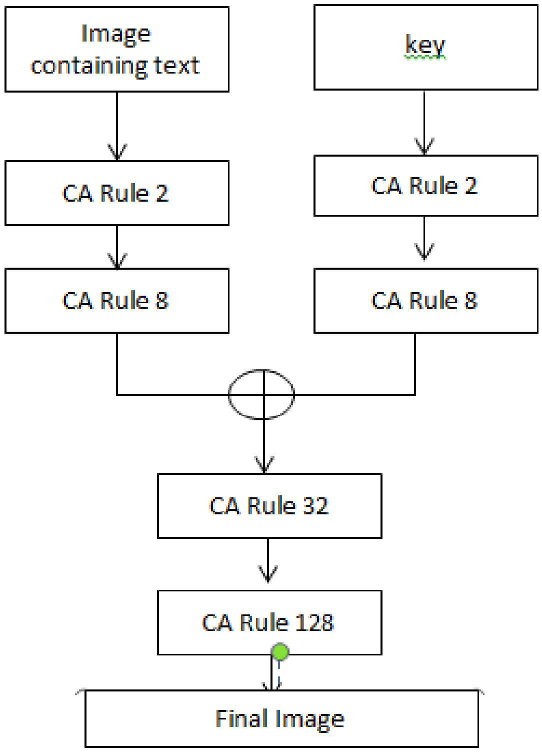


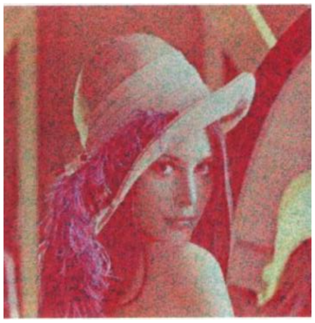
Fig. 3. Block Diagram for encryption using cellular automata.

4. RESULTS

I. Result using ELSB for RGB Image

Cover image

Image containing text

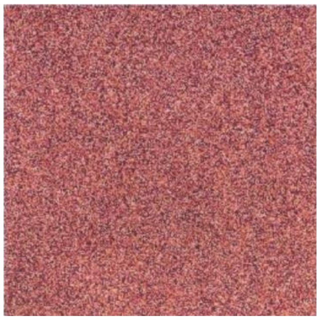

Scrambled image

Descrambled image

II. Result using LSB for RGB Image

Cover image

Image containing text


Scrambled image

Descrambled image

III. Result using LSB for Gray Image

Cover image

Image containing text

Scrambled image

Descrambled image

IV. Table showing comparison of different encryption degree measurement parameters.

	MSE	PNSR	GDD	CORELATION	E.E
ELSB_RGB	0.0013	77.0014	0.0057	0.4060	7.3060
LSB_RGB	0.0013	77.0014	0.00032	0.4078	6.7839
LSB_GRAY	0.0039	72.2302	0.0019	0.4088	7.4913

5. Conclusion and Future scope

2D Cellular Automata is an interesting and clever way of solving problems associated, unlike Arnold transform it doesn't possess periodic nature and can work upon quadrilateral images too. Using two dissimilar levels of security, the communicated message is much more protected in comparison with normal encryption techniques. [8] Using various CA Rules offers the confusion and dispersal properties of encryption. The proposed algorithm being based on combination of Cryptography, steganography and Cellular Automata, which assistance the text in parallel processing way. Because of the availability of the chip level design cellular automata machine (CAM), the encryption and decryption can be done at very high speed in the order of nanoseconds. On the same time, the proposed system can be used for safe and secure communication of data.

Future Scope

Several interesting research directions are inspired by this research solution are discussed next. In addition to constructing and analyzing the Cryptographic Boolean function and their generalization over various finite fields, following projects in the near future can be accomplished:

A. *Cryptographic Boolean Function:*

Exploring the application of off-the- self SAT solvers as the tool to answer some of the interesting open problems is designing Boolean function

B. Secret Sharing scheme for 3D models:

Another possible future research path is the procedure of in the low frequency coefficients. The advantage of integrating mesh compression techniques for 3D secret distribution is mainly due to the large reduction of the resulting 3D model shares. Moreover, faster algorithms for computation can be developed with the different image types.

6. REFERENCES

[1]. S. Wolfram, "Cryptography with Cellular Automata in Advances in Cryptology", Crypto '85 Proceedings, Volume 218 of Lecture Notes in Computer Science, Pages 429–432 (Springer-Verlag, Heidelberg, 1986).

[2]. S. Nandi, B. K. Kar, and P. P. Chaudhuri, "Theory and Applications of Cellular Automata in Cryptography," IEEE Transactions on Computers,Volume 43(12), Pages 1346–1357, December,1994.

[3]. M Phani Krishna Kishore and S KanthiKiran "A Novel Encryption System using Layered Cellular Automata", Proceedings of the World Congress on Engineering, Volume 1,July 6 - 8, 2011

[4]. K.Hemachandran, "Study of Image Steganography using LSB, DFT and DWT", International Journal of Computers & Technology, vol 11, oct.25 2013, pp. 2618-2627

[5]. Zin.w, soe. N "Implementation and Analysis of three Steganographic Approaches", University of Computer Studies, Mandalay, 2011, pp. 456-460

[6]. Manoj.S, " Cryptography and Steganography", International Journal of Computer Applicati ons (0975-8887),

[7]. 2010, vo1-no.12, pp.63-68

[8]. Pratibha Sharma, Manoj Diwakar, NiranjanLal, "Edge Detection using Moore Neighborhood", International Journal Of Computer Applications, Volume 61– No.3, January 2013, Pages26-30.

[9]. Pratibha Sharma, ManojDiwakar, SangamChoudhary, "Application of Edge Detection in Brain Tumor Detection", International Journal Of Computer Applications, Volume 58– No.16,November 2012, Pages21-25.

[10]. Pradipta Maji, ChandramaShaw, NiloyGanguly,Biplab K. Sikdar and P. Pal Chaudhuri, "Theory and Application of Cellular Automata For Pattern Classification", IOS Press, Fundamental Informaticae 58 (2003), Pages 321–354.