International Journal of Students' Research in Technology & Management
eISSN: 2321-2543, Vol 5, No 1, April 2017, pg 05-08
https://doi.org/10.18510/ijsrtm.2017.512

DATA SECURITY USING 2D CELLULAR AUTOMATA RULES

Mohini
Department of Computer Science and Engineering, Sriram Engineering College, Chennai.
Email: mohinijha06@gmail.com

Article History: Received on 22nd Feb. 2017, Revised on 28th Feb. 2017, Published on 20th April 2017

***Abstract*- This paper deals with the secure transformation of text. Encryption is the most common method of hiding text from unauthorized access. Two popular ways of sending personal information in a secret way are Cryptography and Steganography. To hide the existence of the message as well as distorts the message itself using this method. LSB and ELSB are the advanced techniques used to hide text in the image. There are two levels to hide the secret information. In the first level of hiding text, data sent to images by using the password and in second level encryption of 2D Cellular Automata used to enhance more security. If one level of security technique is broken by third person then there will be one more level to provide security to that secret information. Encryption will do using 2 dimensional rules of Cellular Automata. The use of Cellular Automata rules is for the parallelism which provides high security during storing and communicating, higher compression ratio and higher encoding of data while comparing with the available security techniques.**

***Keywords*-**Cryptography; Steganography; LSB; ELSB; 2D Cellular Automata.

I. INTRODUCTION

The current improvements in technology, particularly in the computer industry and communications endorsed potentially huge market for sharing digital multimedia content over the internet. Nevertheless growing quantity of digital stuff, hypermedia processing tools, and the global availability of Internet has created an ideal way to sharing of multimedia (images, audio, and video). Because of huge quantity of sharing information, information security throughout storing and transmission has become a critical matter[1]. One of the main challenges now is to protect the confidential and critical information of multimedia content in multimedia linkages. In order to avoid the illegal information access, effective security measures, robust and consistent algorithms need to be applied. Safe and secure means of transmitting images like any other multimedia needs to be provided. Small encryptions were done over multimedia contents forsafe and secure transmission but with upgrading the speed of computer along with use of parallel processing they can be easily decoded by algorithms. Two usual methods of security implemented are to provide a user id and password for confirmation and to encodeinformation for concealment [3]. The most basic approach is to provide user-id and password to every user to authenticate the user. Authentication helps to establish trust by identifying the particular user/system. In another approach, the information stored in the database is in the form of encryption so that it is not visible to the third person to provide confidentiality. Steganography, cryptography are two different techniques for hiding the information but in a different way. In the present study both steganography, cryptography has been studied.

II. RELATED WORK CRYPTOGRAPHY

Cryptography is the approach to achieve safety by using encoding messages to make them non-recognizable language. On this, the structure of the message is encrypted to make it meaningless and unintelligible till the decryption key isn't available. The basic service delivered by cryptography is the capability to transmit information in such a way that unauthorized person can't understand it [2]. The original form of the message is known as plain text or clear text. Cryptography also can offer authentication for verifying the identification of something or a person. The process of creating a cipher text from plain text is known as Encryption and the reverse of encryption is decryption. The reverse engineering of cryptography is Cryptanalysis.

There are three types of cryptographic functions named as

- Symmetric Cryptography: In this type of cryptography single key is used for both encryption and decryption
- Asymmetric Cryptography: In this type of cryptographic function only one key is used for encryption and another fordecryption.
- Hash Functions: In this cryptography function mathematical transformation is used to irreversibly "encrypt" information.

A. Steganography

International Journal of Students' Research in Technology & Management
eISSN: 2321-2543, Vol 5, No 1, April 2017, pg 05-08
https://doi.org/10.18510/ijsrtm.2017.512

Steganography is the method to hide the original fact while communicating, with the help of hiding information in other data like images, audio or video. It is the method to cover the original fact without leaving any remarkable track [6]. Steganography is the concern with the hiding of text in another data like image, text, audio, and video.Steganography is derived from the Greek words "steganos" means hidden or secret and "grafia" means writing or sketch which defines steganography as "secret writing".

B. Steganography technique: Least Significant Bits

LSB is a simple and easy approach to hide information or data in the cover image. Steganography techniques are used to embed the bits of the message directly into least significant bit plane to cover image in a deterministic sequence. Because of the small change in amplitude the modulation of the least significant bit does not result in human-perceptible difference. Hiding mystery information inner a photograph, a proper cowl photo is required. Because of the use of every pixels bit in the picture, it is obligatory to apply a lossless compression layout, in any other case, the hidden facts will be misplaced within the alterations of a Lossy compression algorithm [10]. While using a 24-bit color picture, a chunk of each of the red, inexperienced and blue shade components are used to shop three bits in each pixel. For instance, the grid can be described as three pixels of a 24-bit coloration picture, using 9 bytes of reminiscence [10]:

(11100111 11101000 11001011)

(11100110 11001000 11101011)

(00001000 00100111 11101010)

When we are taking the character A, the binary

value A equals 10000001,is inserted, the following grid results [10]:

(11100111 11101000 11001011)

(11100110 11001000 11101011)

(00001000 00100111 11101010)

In this situation, only three bits are required to be modified to insert the individual efficiently. On average, best half of the bits in a photo need to be changed for hiding a secret message with the assist of the maximal cowl size. The end result changes that are made to the least great bits are too small to be recognized by way of the human visual gadget (HVS), so the message is efficaciously hidden As we noticed, the least tremendous bit of the 0.33 coloration remains without any modifications[7][10]. It is used to check the correctness of eight bits which can be embedded in those 3 pixels. In other words, it could be used as "parity bit".

Cellular Automata is extensively used in operations such as graphics (generated images and music), random number generation, pattern recognition, routing algorithm, and games.

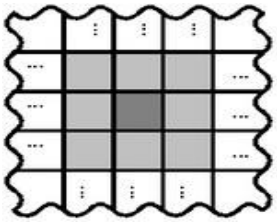

Fig. 1. Von Neumann Neighborhood

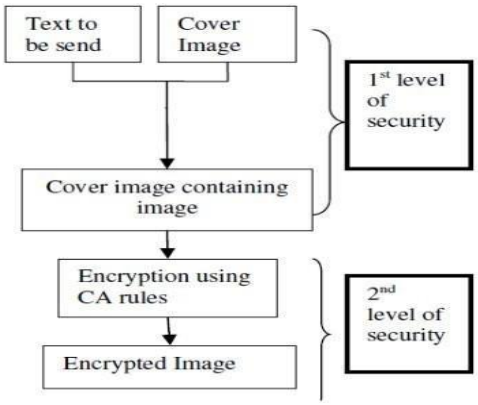

Fig. 2. Block diagram for encryption using CA

In the area of Digital image processing, the application of CA includes image enhancement, compression, encryption and watermarking. Stanislaw Ulam and John von Neumann in the 1940's proposed a self-producing organism model named as CA which is dynamic, complex space and time discrete systems. A Cellular Automata model consists of a regular grid of cells; each of them is a finite number of states. The grid can be in any finite number of dimensions. For each cell, a set of cells called its neighborhood is defined relative to the specified cell.

The basic principle of Cellular Automata:

- Spatial structure of cells
- Local Interaction among neighborhood cells
- Changing of state

Cellular Automata neighborhood:

There is a different kind of neighborhood interaction in CA. Some of them are [4]:

International Journal of Students' Research in Technology & Management
eISSN: 2321-2543, Vol 5, No 1, April 2017, pg 05-08
https://doi.org/10.18510/ijsrtm.2017.512

1. Von Neumann neighborhood
Its miles the smallest symmetric 2nd aligned community usually defined via guidelines at the compass [11]

$N = \{N, W, C, E, S\}$ Sometimes the central cell is omitted [11].

Formal definition
Officially the von Neumann neighborhood is the set of neighbors or a subset of the rectangular community size.

$$k_x = k_y = 3$$

With the output cell at the center.

$$k_0 x = k_0 y = 1$$

2. Moore neighborhood:

It is a simple square (usually 3×3 cells) in which the output cell used to present in the center. Usually, cells in the neighborhood

$$N = \{\{0,-1\},\{-1,0\},\{0,0\},\{+1,0\},\{0,+1\}\}$$

are described as directions on the compass

$$N = \{NW, N, NE, W, C, E, SW, S, SE\}$$

Sometimes the central cell may be omitted.

Formal definition
Formally the set of neighbors

$$k_x = k_y = 3$$

$$k_0 x = k_0 y = 1$$

or simply a square size with the output cell at the center.

II. Proposed System

Proposed System for the given security issue is designed separately for the RGB and gray level images using LSB and ELSB techniques [10]. Any message can be hidden in an image using 2 level securities with the help of following steps:

Step 1: Hide the text in an image using LSB and ELSB technique (this will provide the first level of Security)

Step 2: Image with the hidden message is encrypted using CA rules and generates a final Encrypted (this will provide thesecond level of security)

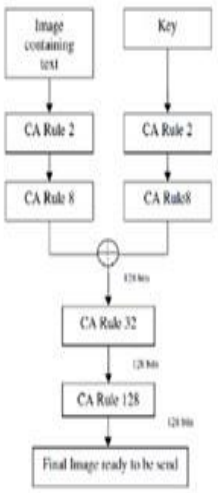

Fig. 3. Moore neighborhood

A. *Proposed Algorithm*:
Enhanced Least Significant Bits (ELSB)Algorithm
Least Significant Bits (LSB)Algorithm Encryption using Cellular Automata Algorithm

III. Conclusion

2D Cellular Automata is aninteresting 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 nano- seconds. On the same time, the proposed system can be used for safe and secure communication of data.

A. 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:

B. 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

.For instance, the construction of (8, -, -, 118) Boolean.

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 imagetypes.

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 Applications (0975-8887),

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

[8]. Pratibha Sharma, ManojDiwakar, NiranjanLal,"Edge Detection using Moore Neighborhood",InternationalJournal 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]. PradiptaMaji, Chandrama Shaw, NiloyGanguly,Biplab K. Sikdar and P. Pal Chaudhuri, "Theory and Application of Cellular Automata For Pattern Classification", IOS Press, FundamentalInformaticae 58 (2003), Pages 321–354.

[11]. http://www.iosrjournals.org/iosr-jce/full-issue/vol4-issue1.pdf

[12]. https://en.wikibooks.org/wiki/Cellular_Automata/Neighborhood