Text Security using 2D Cellular Automata Rules

Pratibha Sharma
Department of CSE, Mody Institute of Technology & Science,
Lakshmangarh, Rajasthan, India
pratibha49@gmail.com
www.mitsuniversity.ac.in

Niranjan Lal
Department of CSE, Mody Institute of Technology & Science,
Lakshmangarh, Rajasthan, India
niranjan_verma51@yahoo.com
www.mitsuniversity.ac.in

Manoj Diwakar
Department of CSE, DIT Dehradun, Uttarakhand, India
manoj.diwakar@gmail.com
www.dit.edu.in

Abstract

This paper deals with the secure transmission of text. Encryption is the most common method for hiding text from unauthorized access. Encryption provides only one level of security during transmission over the channel. The aim of this paper would be to provide 2 levels of security. First level comprises of hiding text to be sent behind some image using password and the second level comprises of encryption using 2D Cellular rules. If one level of security is broken then the other level would provide security thereby ensuring more security to the transmitted message. Encryption would be done using 2 dimensional rules of Cellular Automata.

Keywords: Cellular Automata, Encryption, Steganography.

1. Introduction

The amount of information shared over the Internet has experienced an exponential growth over the last few years. Due to this increased amount of information, security has become a vital issue. Stronger and reliable methodologies are required in order to handle the threats and vulnerabilities imposed by this increased information. The data shared over the internet includes the text, images, audio, video, etc. Data security is one of the critical issue amongst image, video, audio security etc. In order to prevent the illegal data access, efficient security measures need to be applied.

1.1 Need of Security

Most initial computer applications had either no or very less security. When the computer applications were developed to handle financial and personal data, the need for security was truly realized. Therefore, various areas in security began to gain prominence. Two typical measures of security implemented are:

- Provide a user id and password for **authentication**
- Encode information for **confidentiality**

Providing user id and password to every user is the most basic approach for authenticating the users. Authentication helps establish trust by identifying the particular user/system. In another approach, the information stored in the database is encoded so that it is not visible to the users providing confidentiality.

1.2 Cryptography and Cellular Automata

Cellular Automata is a discrete model which consists of grids of cells in which each cell exists in finite state i.e. either 0 or 1. Every cell changes its state based on the states of neighboring cells by following a prescribed rule. These rules are different in 1D and 2D Cellular Automata. Cellular Automata has following inherent properties:

- Parallelism
- Homogeneity
- Unpredictability
- Easily implementable in both software and hardware systems

Due to these inherent properties, Cellular Automata has become an important tool to develop cryptographic methods.

This paper is organized as section 2 contains literature review, section 3 contains brief introduction of cellular automata, section 4 contains the proposed methodology, section 5 contains the results and finally section 6 and section 7 contains conclusion and references respectively.

2. Literature Review

Various researchers have used cellular automata concept for image encryption and decryption. Cellular Automata (CA) based encryption algorithms presents a promising approach to cryptography, since the initial state of the CA is the key to the encryption, and thereby evolving a complex system from this 'initial state' which cannot be predicted. There exist many different cryptographic techniques. CA have been previously been suggested as encrypting devices by Wolfram [1] and by Nandi [2]. In the work carried out by Nandi, Cellular Automata (CA) was used for a class of block ciphers and stream ciphers.

In the work carried out by M. Phani Krishna Kishore and S. Kanthi Kiran [3], a Layered Cellular Automata was taken in consideration where the automata can be viewed as a system consisting of layers, and each layer consists of rows of 1D cellular automata. Each cell except the boundary cells has 8 neighbors in its plane and the cells that lie on the planes other than the top and bottom have 26 neighbors. In their proposed system (LRCA), the block encryption technique was used along with the symmetric key encryption. Rong-Jian Chen and Jui-Lin Lai [4] presented a novel image security system based on the replacement of the pixel values using recursive cellular automata (CA) substitution. The proposed image encryption method exhibits the properties of confusion and diffusion. Marcin Seredynski and Pascal Bouvry [5] proposed an encryption concept based on one dimensional, uniform and reversible CA. A class of CA with rules specifically constructed to be reversible was used. The reversible CA-based algorithm worked in a mode that was similar to CBC mode in terms of achieved result.

Sambhu Prasad Panda, Madhusmita Sahu [6] proposed an encryption and decryption algorithm for block cipher based on the linear (periodic boundary-PB) and nonlinear cellular automata rules. First they applied non linear CA rules (complements) to both plain text and key. Then PB CA rule was applied to the above results separately followed by the XOR operation of above results. After that the result of XOR operation is fed to substitution box(S-box) and again PB CA rules were applied followed by S Box. The decryption process was carried out just similar to that of encryption but in the reverse way.

In addition to encryption Cellular Automata finds its application in various fields like edge detection, pattern classification, error correction coding etc. For instance, in the work carried out by Pratibha Sharma, Manoj Diwakar, Niranjan Lal [7], Moore neighborhood model of Cellular Automata was used for edge detection. In the work carried out by Pratibha Sharma, Manoj Diwakar, Sangam Choudhary [8], Cellular Automata was used for brain tumor detections. Pradipta Maji and Chandrama Shaw et al. [9] presented the theory and application of a high speed, low cost pattern classifier. The proposed classifier was built around a special class of sparse network referred to as Cellular Automata (CA). Hence Cellular Automata is widely used for various applications.

3. Cellular Automata

The cellular automata (CA) have been used since the forties of last century. It was used in many physical applications. The applications of Cellular Automata extended to fields such as biological models, image processing, language recognition, simulation, computer architecture, cryptography etc. The Cellular Automata is also one of the modern methods used to generate binary pseudo–random a sequences using registers.

The concept of CA was initiated by J. Von Neumann and Stan Ulam in the early 1940's. He devised a CA in which each cell has a state space of 29 states, and showed that the devised CA can execute any computable operation. He studied the 1 dimensional rules of Cellular Automata. However, due to its complexity, in the 1970, the mathematician John Conway proposed his now famous game of life which received widespread interest among researchers. His research was based on 2D Cellular Automata rules. Stephen Wolfram studied in much detail and showed that a family of simple one-dimensional cellular automata rules (now famous Wolfram rules) and are capable of emulating complex behavior.

Cell is the basic element of Cellular Automata. For each cell, a set of cells called its neighborhood (usually including the cell itself) is defined relative to the specified cell. For example, the Moore neighborhood of a cell is defined as the set of cells consisting of the cells itself and the top, bottom, left side and right side neighbors. And for instance, the rule might be that the cell is "On" in the next generation if exactly two of the cells in the neighborhood are "On" in the current generation; otherwise the cell is "Off" in the next generation. In this way there are different rules for 1D and 2D Cellular Automata. Figure 1 shows the basic model of Cellular Automata.

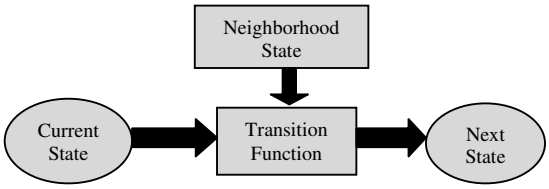

Fig. 1 Model of Cellular automata

In the model adopted in this project, each cell can have the binary states either 1 or 0. As shown in the figure 1, Cellular Automata changes their state synchronously, according to a local update rule that specifies the new state of each cell based on the old states and its neighbors gives the global change of CA. After each iteration, the next state is calculated according to some rules. These rules are different in 1D and 2D cellular automata.

4. Proposed Methodology

The objective of this paper is to develop a method providing security to the transfer of text messages over the network. The objective of this paper is to provide security at two levels:

- Security at one level assures **authenticity** (at sender and receiver side)
- Security at second level ensures **confidentiality** (during transmission over the network).

Providing security at two different levels at both sender and receiver side will result in more secure system. If the unauthorized person breaks one level of security then the second level will provide security. Different techniques are available to achieve authenticity and confidentiality. The techniques used for implementing the two levels of security are:

- Hiding text to be sent behind some image by password.
- Encryption of image obtained using Cellular Automata rules.

First of all Steganography will be used for hiding text to be send behind the cover image. The image obtained from this step will be then encrypted for making the content invisible. Encryption will be done by applying Cellular Automata rules. The block diagram showing the methodology is shown in figure 2.

4.1 Hiding Text using Password

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the

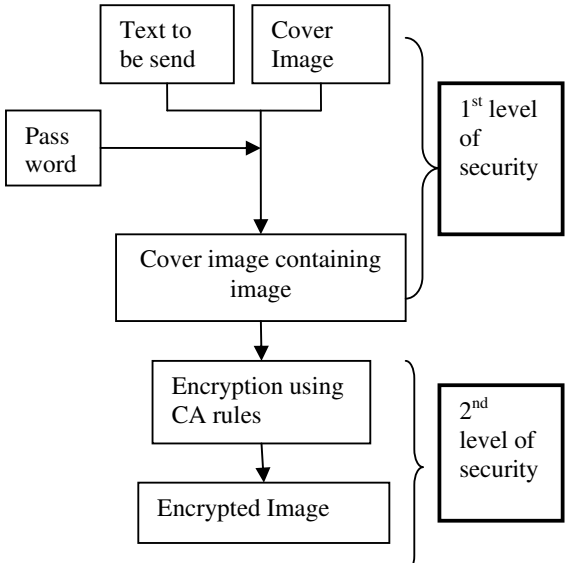

Fig 2. Proposed Method

existence of the communicated information. Steganography is the first step of the method which ensures authenticity. Steganography allows a user to hide large amounts of information within image and audio files. The text to be send is hidden behind the cover image and this will be password protected. For hiding the text LSB substitution method have been used here. LSB (Least Significant Bit) substitution is the process of modifying the least significant bit of the pixels of the cover image. By doing so, the value of each pixel is changed slightly, but the changes are not reflected physically in the cover image. In a 24-bit image, 3 bytes are used for each pixel, so each pixel could encode 3 bits of a secret message. The altered image would look identical to the human eye, even when compared to the original.

The receiver will be able to recover the message only when the correct password is be entered. So this step ensures security at one level.

4.2 Encryption using Cellular Automata

Moore neighborhood model have been used as Cellular Automata model. In Moore neighborhood model 9 cells are considered at a time including the cell itself. The value of current cell (i.e. central cell) depends on its 8 neighbors. Table 1 shows all the rules of two dimensional CA. These rules are called as the linear rules of Cellular Automata.

Table 1: 8 Neighborhood CA Rules

64	128	256
32	1	2
16	8	4

In 2-D eight neighborhood CA the next state of a particular cell is affected by the current state of itself and eight cells in its nearest neighborhood (Table 1). Such dependencies are accounted by various rules. These 8 rules are called the fundamental rules of cellular automata and are known as linear rules of cellular automata. In case the cell has dependency on two or more neighboring cells, the rule number will be the arithmetic sum of the numbers of the relevant cells, which gives the non linear rules of cellular automata.

The rules used in the proposed method are Rule2, Rule 8, Rule 32 and Rule 128. The steps involved are shown in figure 3.

According to rule number 2, the central cell will be alive in next generation only when its right side cell is alive in present generation. According to rule number 8, the central cell will be alive in next generation only when its bottom side cell is alive in present generation. According to rule number 32, the central cell will be alive in next generation only when its left side cell is alive in present generation. According to rule number 128, the central cell will be alive in next generation only when its upper side cell is alive in present generation. Fox example, the rule number 8 can be illustrated as:

0	1	1	0		0	0	1	1
0	0	1	1	Applying CA Rule 8	0	1	0	0
0	1	0	0		1	1	0	0
1	1	0	0		0	0	0	0

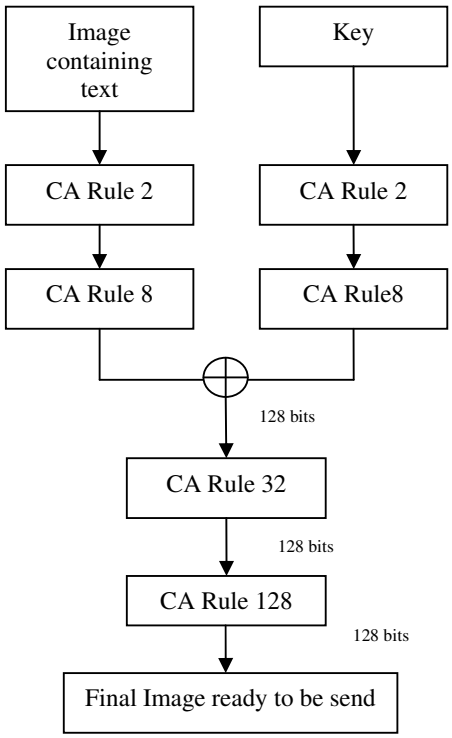

Fig 3. Encryption steps

Hence different rules were applied to obtain much security. The decryption process was carried out in similar way in reverse fashion.

5. Results

For hiding text behind an image, the text needs to be written in text file (.txt). User is asked for an input image to be used as cover image. After that a password would be asked for hiding the text in the image. Finally the image will be provided. Figure 4 shows the image to be used as cover image. Suppose that the text to be hidden behind cover image is “Computer Science”. The text is saved in sample.txt file. User is asked for password. This is shown in figure 5.

Fig. 4: Cover Image

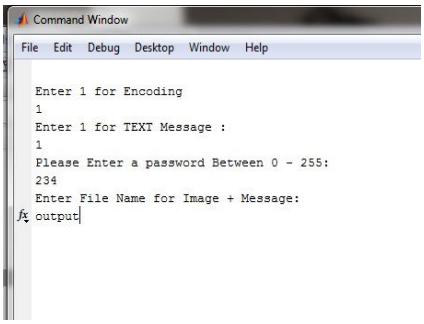

Fig. 5: Information required from user

Fig. 6: Output image containing hidden text

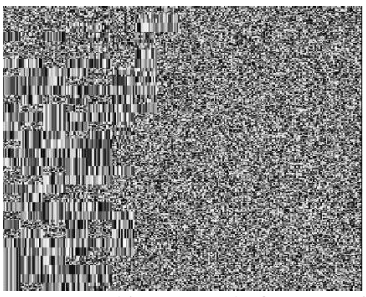

Fig. 7: Encrypted image ready for transmission

Next step is the encryption of the image obtained in figure 6 using CA rules. The image obtained after applying the encryption algorithm is shown in figure 7.

Now this is the secure image ready for transmission. At the receiver side, first the image received will be decoded and then the password will be required to extract desired text. The extracted text will be saved in a txt file.

The decrypted image is obtained as shown in figure 8. Finally the text will be extracted by entering the password used at time of hiding by the sender. The output is saved in txt file as shown in figure 9.

Figure 8: Decrypted Image

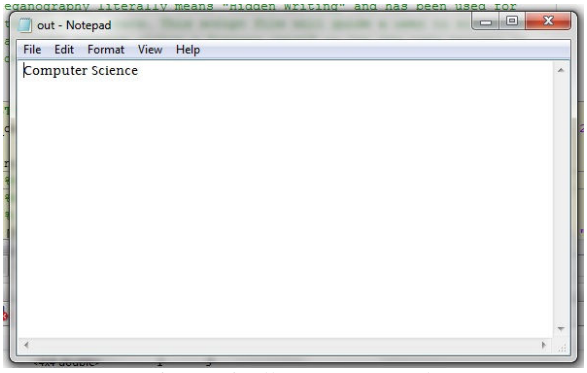

Fig. 9: Finally text extracted

6. Conclusion

By using two different levels of security, the transmitted message is much secure as compared to simple encryption method. Using different CA rules provides the confusion and diffusion property of encryption. The proposed algorithm, being based on concept of CA, helps parallel processing of text. Besides, due to availability of chip level design cellular automata machine (CAM), the algorithm can encrypt and decrypt the text at very high speed in the order of nano seconds. Also the algorithm can be used for secure transmission of images.

7. 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 Kanthi Kiran “A Novel Encryption System using Layered Cellular Automata”, Proceedings of the World Congress on Engineering, Volume 1, July 6 - 8, 2011.

[4] Rong-Jian Chen, Jui-Lin Lai “Image security system using recursive cellular automata substitution” Pattern Recognition Society, Published by Elsevier Ltd., Volume 40, Pages 1621 – 1631, 2007.

[5] Marcin Seredynski and Pascal Bouvry “Block Encryption Using Reversible Cellular Automata”, 6th International Conference on Cellular Automata for Research and Industry, Volume 3305, Pages 785-792, 2004.

[6] Sambhu Prasad Panda, Madhusmita Sahu “Encryption and Decryption algorithm using two dimensional cellular automata rules in Cryptography”, International Journal of Communication Network & Security, Volume-1, Issue-1, Pages 18-23, 2011.

[7] Pratibha Sharma, Manoj Diwakar, Niranjan Lal, “Edge Detection using Moore Neighborhood”, International Journal Of Computer Applications, Volume 61– No.3, January 2013, Pages 26-30.

[8] Pratibha Sharma, Manoj Diwakar, Sangam Choudhary, “Application of Edge Detection in Brain Tumor Detection”, International Journal Of Computer Applications, Volume 58– No.16, November 2012, Pages 21-25.

[9] Pradipta Maji, Chandrama Shaw, Niloy Ganguly, Biplab K. Sikdar and P. Pal Chaudhuri, “Theory and Application of Cellular Automata For Pattern Classification”, IOS Press, Fundamenta Informaticae 58 (2003), Pages 321–354.