International Journal of Engineering Research & Management Technology ISSN: 2348-4039

January-2017 Volume 4, Issue-1

Email: editor@ijermt.org www.ijermt.org

STEGANOGRAPHY TECHNIQUE BASED ON IMAGE SECURITY USING CELLULAR AUTOMATA RULES

Ms. Ayushi Chaudhary
Department of Computer Science & Engineering
Marathwada Institute of Technology
Bulandshar

Mr. Manoj Kumar Sharma
Department of Computer Science & Engineering
Marathwada Institute of Technology
Bulandshar

ABSTRACT: This research article focuses on image processing and encryption techniques. 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. Decryption is done at the receiving end using inverse transformation, which operates on backtracking procedure. Such technique of dual encryption leads us in achieving enhanced security under space and time constraint.

Keywords: *Cellular Automata, Cell Neighbours, Random Number Generator, Encryption, Decryption*

I. INTRODUCTION

The concept of cellular automata gives the clear understanding about its label, which is "Game of life". A cellular automation is actually a discrete mathematical model representing the cell matrix which operates on the states and the rules are applicable to cells after transformation. The Information security carries much importance in very field of life. Especially the Military affairs and confidential business are very sensitive in this regard. To keep data away from the access of unauthorized users or to make it safe from being corrupted is called data security. Encryption is a very important security mechanism. The principle of its working is to scramble the information into unreadable information and then unscramble it for reading using a key. Encryption of the text is different from that of an image. Due to the intrinsic characters of images such as bulk data capacity and high redundancy, encryption on image or video objects has its own requirements. 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.

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 neighbouring 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.

II. LITERATURE REVIEW

In order to protect digital images from unauthorized users doing illegal reproduction and modifications, a variety of image encryption schemes have been proposed till now. The various ideas used in the existing image encryption techniques can be classified into three major categories: position permutation [4], value transformation [5] and the combination form [6]. The position permutation algorithms scramble the data position within the image itself and usually have low security. On the other hand, the value transformation algorithms transform the data value of the original signal and have the potential of low computational complexity and low hardware cost. Finally, the combination forms perform both position permutation and value transformation and usually have the potential of high security.

In recent years, a number of different image encryption schemes have been proposed in order to overcome image encryption problems. Various researchers have also used cellular automata concept for image encryption and decryption. A class of 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, evolving a complex chaotic system from this 'initial state' which cannot be predicted. Cryptographic techniques are very important in these times dominated by the growth of digital information storage and transmission. In fact, increasingly available communication networks and databases make the need for privacy and authentication a basic requirement in many areas, especially in electronic commerce transactions and for classified material. There exist many different cryptographic techniques.

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 is capable of emulating complex behaviour. Cell is the basic element of Cellular Automata. For each cell, a set of cells called its neighbourhood (usually including the cell itself) is defined relative to the specified cell. For example, the Moore neighbourhood of a cell is defined as the set of cells consisting of the cells itself and the top, bottom, left side and right side neighbours. And for instance, the rule might be that the cell is "On" in the next generation if exactly two of the cells in the neighbourhood 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

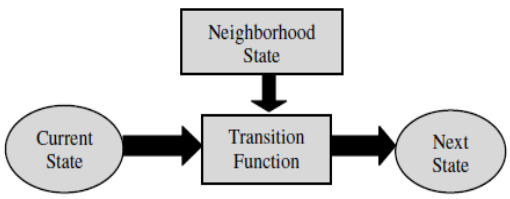

Fig. 1 Model of Cellular automata

Fig. 1. Cellular Automata

III. PROPOSED WORK

The techniques used for implementing the two levels of security are:

i. Hiding image to be send behind another image by password.
ii. Encryption of image using Cellular Automata rules.

First of all Steganography will be used for hiding image 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.

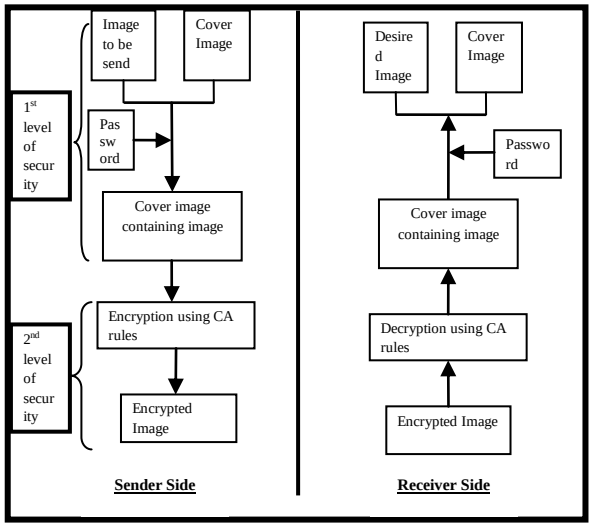

Fig. 2. Block Diagram showing the two levels of security

Using the concept of two levels of security, the system is more secure. In the 1st level, authentication is done by adding password and at the receiver side; the actual image can be retrieved if the password is correct. In the 2nd level, confidentiality is achieved by encryption method. If someone tries to break this level of security during transmission, then the image obtained will be cover image only and not the actual image. In this way, an efficient method providing security during transmission (confidentiality) and at the receiver side (authentication) can be achieved.

IMAGE HIDING BEHIND ANOTHER IMAGE

Suppose image shown in Fig. 1.2 having size 256 x 256 has to be send. Figure 5.2 having size 320 x 213 is to be used as cover image. Since the size of cover image and image to be sent are of different size, the cover image needs to be resized according to the image to be sent. This can be accomplished using the "resize" function of Matlab.

Fig. 3. Image to be sent

Fig. 4. Cover Image

First the sender is asked for a password. This password has to be kept secret among sender and receiver. After entering the password, the cover image needs to be resized. After resizing, the image to be sent is hidden behind the cover image using LSB technique. The last two least significant bits of the cover image are cleared and the two most significant bits of the image to be sent are moved to the cleared least significant bits. At the receiver side, first the receiver is asked for password. If the password entered is correct only then the image can be retrieved.

Fig. 5. User selecting the task

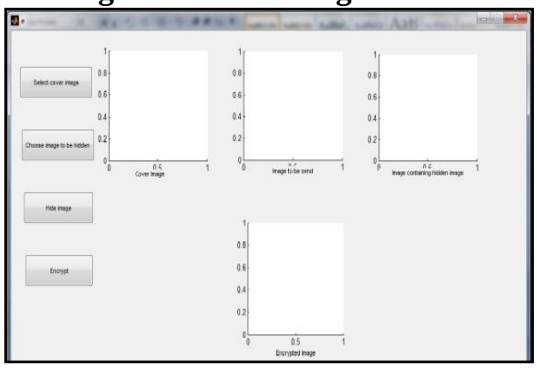

Fig. 6. Encryption window

Now the user is asked to select the cover image and the image to be sent. The images used here are same as shown in Fig. 5 and Fig. 6. After selecting the images, user click on the Hide Image button. After clicking on this button, a prompt window will ask 8 bit password from the user as shown in Fig. 7.

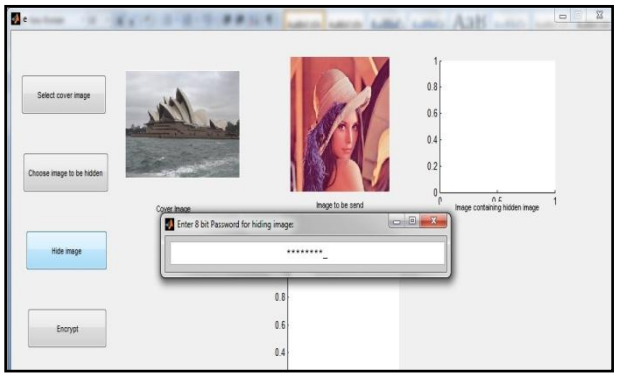

Fig. 7. Prompt window asking 8 bit password for hiding image.

After hiding the image, the user clicks on the encrypt button, the user is again asked for 8 bit key as shown in Fig. 8.

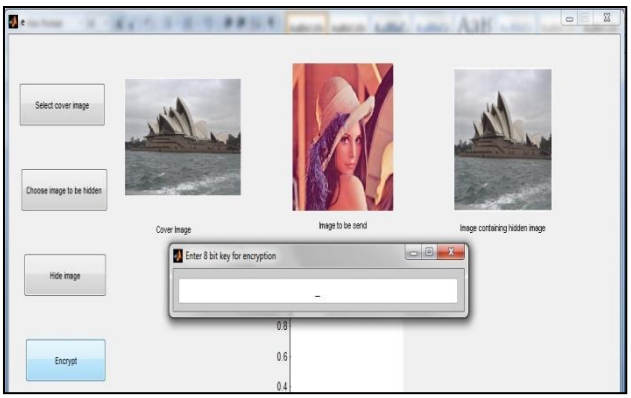

Fig 8 Prompt window asking 8 bit key for encryption

After entering the 8 bit key for encryption, the encryption process starts. User has to wait till encryption process is finished. This process is slightly time consuming because the encryption process

depends on the size of the image and the image containing hidden image is double of the size of the image to be send.

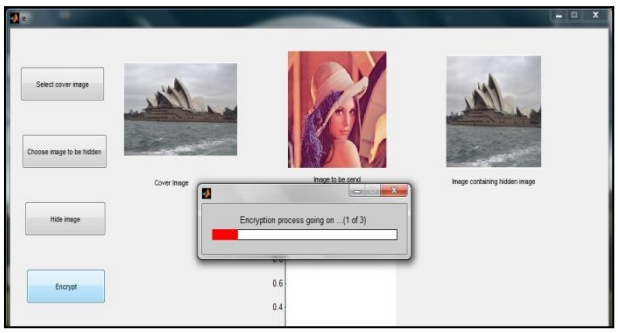

Fig .9 Prompt window showing progress of encryption

After the encryption process in finished, the output obtained is as shown in Fig. 10. The image obtained after encryption would be saved in the same path where the exe file is saved with image name as "output.bmp".

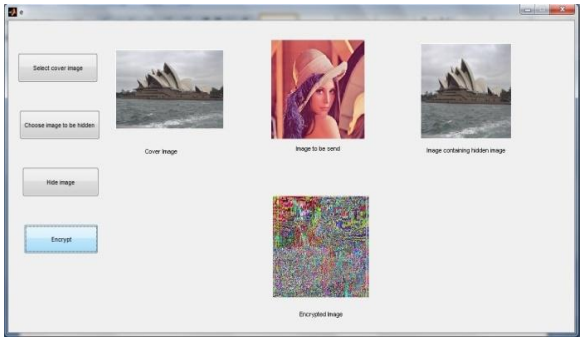

Fig. 10 Image obtained after encryption

This is the two level password protected image and can be decrypted on same or any other system only by entering correct passwords. Hence at the sender side, authenticity and confidentiality has been achieved. At the receiver side, the receiver will be first asked for the key and then for the password. If the receiver provides both the password correctly, only then the image can be retrieved, thereby providing two levels of security. The upcoming section explains the same. Now in order to retrieve the image at the receiver side, the same exe file should be available. After running the exe file, the window opened is same as shown in Fig. 11 and the receiver selects decryption task to be performed.

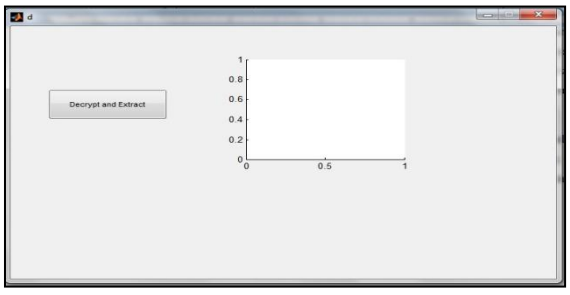

Fig 11. Decryption window

If the user is authorized, then correct key would be entered and the decryption process would start as shown in Fig.12. The decryption process would take the same time as taken by encryption process. Encryption and decryption process considers red, green and blue component separately and processes them separately.

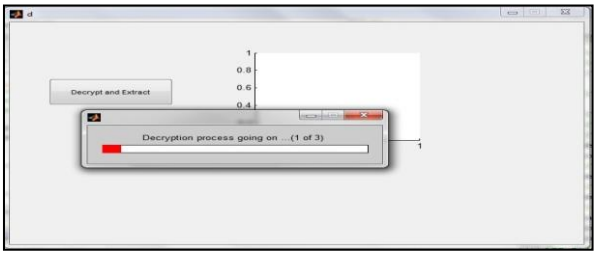

Fig 12. Window showing decryption progress

When the decryption process is finished, the user would be asked for the same password used for hiding the image.

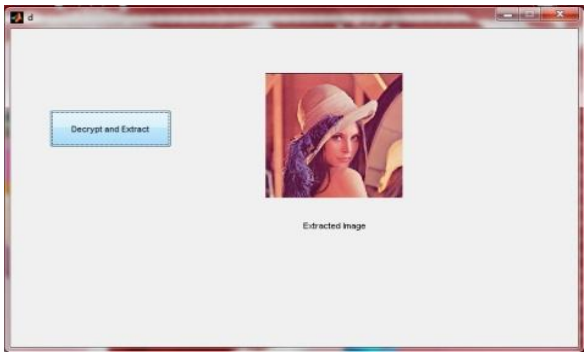

Fig.13. Finally Extracted Image

Hence as stated in the objective of the thesis, generalized fully functional software has been developed ensuring two level securities for secure transfer of images.

CONCLUSION AND FUTURE WORK

The proposed technique can be used to hide any format of image. The strength of the security can be greatly enhanced by combining Steganography and Cryptography concepts. For implementing Image Steganography concept, LSB (Least Significant Bit) technique has been used. The strength of the LSB technique used lies in the fact that it gives no idea that weather is something hidden inside it or not because the size of the cover image is doubled. The image obtained after hiding is encrypted and hence both authenticity and confidentiality are achieved. A two level security system for secure transfer of images has been developed and tested successfully. The exe file created by building complete package can run on any Windows platform. Matlab is not needed to be installed to run the exe file.

In future, the proposed method can be improved as follows: As the time taken for encryption is slightly more, it can be reduced by changing rule applied

For encryption using Cellular Automata, S box can be developed. Hybrid Cellular Automata rules can also be applied.

REFERENCES

1. 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.
2. 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.
3. 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.
4. M.A.B. Younes and A. Jantan, “An image encryption approach using a combination of permutation technique followed by encryption”, International Journal of Computer Science and Network Security, Volume 8, Pages 191-197, 2008.
5. X. Tong and M. Cui, “Image encryption with compound chaotic sequence cipher shifting dynamically”, Image and Vision Computing, Volume 26, Pages 843-850, 2008.
6. S. Behnia, A. Akhshani, H. Mahmodi and A. Akhavan, “A novel algorithm for image encryption based on mixture of chaotic maps”, Solitons and Fractals, Volume 35, Pages 408-419, 2008.
7. 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).
8. 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.

9. 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.
10. 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.
11. Debasis Das and Abhishek Ray "A Parallel Encryption Algorithm for Block Ciphers Based on Reversible Programmable Cellular Automata" , Journal of Computer Science and Engineering, Volume 1, Issue 1, Pages 82-90, May 2010.
12. 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.
13. Chinta Somswara Rao, Srinivasa Rao Attada "Implementation of Object Oriented Encryption System using Layered Cellular Automata", International Journal of Engineering Science and Technology (IJEST), Volume 3, No. 7, Pages 5786-5795, July 2011.
14. 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.
15. C.K. Chan, L.M. Cheng, Hiding data in images by simple LSB substitution, Pattern Recognition 37 (3) (2004) 469–474.
16. Marvel, L.M., 1999. Spread Spectrum Image Steganography. IEEE transactions on image processing 8(8), 1075-1083.
17. Khalaf, E.T., Sulaiman, N., 2011. Segmenting and Hiding Data Randomly Based on Index Channel. International Journal of Computer Science. 8(3), 522-529.
18. Wang, R.Z. Lin, C.F., Lin, J.C., 2001. Image hiding by optimal LSB Substitution and genetic algorithm. Pattern Recognition. 34, 671-683.
19. Marvel, L.M., 1999. Spread Spectrum Image Steganography. IEEE transactions on image processing 8(8), 1075-1083.
20. C.K. Chan, L.M. Cheng, Hiding data in images by simple LSB substitution, Pattern Recognition 37 (3) (2004) 469–474.
21. Marvel, L.M., 1999. Spread Spectrum Image Steganography. IEEE transactions on image processing 8(8), 1075-1083.
22. Khalaf, E.T., Sulaiman, N., 2011. Segmenting and Hiding Data Randomly Based on Index Channel. International Journal of Computer Science. 8(3), 522-529.
23. Wang, R.Z. Lin, C.F., Lin, J.C., 2001. Image hiding by optimal LSB Substitution and genetic algorithm. Pattern Recognition. 34, 671-683
24. Hussain, M., Hussain., M., 2010. Pixel Intensity Based High Capacity Data Embedding Method. International conference on Information and Emerging Technologies, 1-5.
25. C. Cachin, "An Information-Theoretic Model for Steganography", In Pro-ceedings nd of 2 Workshops on Information Hiding, MIT Laboratory for Computer Science, May 1998.
26. Wu., H.C., Wu., N.I., Tsai, C.S., Hwang, M.S., 2005. Image Steganographic scheme based on pixel value differencing and LSB replacement methods. IEE Proc. Vision Image Signal Process. 152, 611-615.
27. M. Niimi, H. Noda and E. Kawaguch, "An image embedding in image by a complexity W.N. Lie and L.C. Chang, "Data hiding in images with adaptive numbers of least significant bits based on the human visual system," In Proceedings of IEEE International Conference on Image Processing., vol. 1, pp. 286-290, 1999.