TWO-LEVEL DATA SECURITY USING STEGANOGRAPHY AND 2D CELLULAR AUTOMATA

S.Saraswathi[1], V.Santhosh Raj[2], S.Sethuraman[3], J.Saravanan[4]

[1]*Professor, Information Technology, Pondicherry Engineering College, Puducherry, India*
[2]*Student, Information Technology, Pondicherry Engineering College, Puducherry, India*
[3]*Student, Information Technology, Pondicherry Engineering College, Puducherry, India*
[4]*Student, Information Technology, Pondicherry Engineering College, Puducherry, India*

Abstract

An important amount of personal data concerning vital information of a person is in the form of documents such as the Client documents of a Lawyer, Patient Reports of a Psychiatrist, Auditor documents and so on. A secure method is needed to store and transmit these data when required. These data should be maintained confidential from third party since revealing of these data might seriously affect the privacy of the persons involved. Encryption is mostly used to hide data from unauthorized access. Steganography is used to provide the first level of security and 2-D Cellular Automata to provide the second level of security. In the first level, data is encoded in the image and in the second level the encoded image is encrypted using 2-D Cellular Automata rules. The use of Cellular Automata rules is for the parallelism it provides during generation. It also provides high security during storing and transmitting, higher compression ratio and higher encoding of data when compared with the existing security technique.

Keywords: *Cellular Automata; Security; Steganography.*

----------***----------

1. INTRODUCTION

The amount of information transmitted over the Internet has experienced an exponential growth over the last few years. Due to the increased amount of transmitting 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. For this different Steganography and Encryption algorithms are used. But, even the highly efficient encryption algorithms like AES, RSA, RC2, DES, 3DES, DSA are getting broken today. So, there comes the need for highly secure encryption method for the transmission of data through internet. A single level of security is not alone enough to handle security issues in today's world. Hence, a second level of security is needed to face the challenges during transmission of data.

1.1 Security and Steganography

The word steganography comes from the Greek *Steganos*, which means covered or secret and *graphy* means writing or drawing. Therefore, steganography means, literally, covered writing. The main goal or steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data.Digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information can be used as "covers" or carriers to hide secret messages. After embedding a secret message into the cover-image, a so-called *Stego-image* is obtained.

In this paper steganography is used in images since the hidden text doesn't stand out. It can be passed in innocuous content like an image. By making some slight changes to color values, for example, you can transmit the data by hiding in pixels that are practically undetectable. But in the previous works only 12.5 % of data sent through the Least Significant Bit (LSB) [1] method and 20.8% of data sent through the Enhanced LSB method [2]. To improve on this a method is proposed to exploit almost the entire size of the image to hide the transmitting data. The proposed method also explains the usage of second level of security using cellular automata since one level of security is not enough.

1.2 Crptography and Cellular Automata

Cryptography is an important element of any strategy to address message transmission security requirements. Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. It is the practical art of converting messages or data into a different form, such that no-one can read them without having access to the 'key'. The message may be converted using a 'code' (in which each character or group of characters is substituted by an alternative one), or a 'cypher' or 'cipher' (in

which case the message as a whole is converted, rather than individual characters).

Cellular Automata (CA) [3] 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 CA. CA 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.

The rest of the paper is organized as follows: Section 2 summarizes the work related to the fields (Steganography and CA) discussed. Section 3 proposes to study the issues in the existing system, the solutions to those issues by means of the approach based on the proposed model. Section 4 presents evaluation results for the proposed system performance. In Section 5 the research paper is concluded with the motivations that led us to merging of two different levels of security and finally and some ideas are presented for possible applications.

2. LITERATURE REVIEW

First level data security is provided by Steganography. Steganography can be carried out by various algorithms such as LSB and DCT. Throughout history, a multitude of methods have been used to hide information. David Kahn's "The Code breakers" provides an excellent accounting of this history. Bruce Norman has stated the usage of Steganography and Cryptography in "Secret Warfare: The Secrets of Codes and Ciphers".

Least Significant Bit (LSB) approach was basically carried out to hide text in images in which the last bit of every pixel of the image is replaced with the information. In the work carried out by Dr. Mazen M Al Hadidi et al. [4] LSB approach was carried out in which information was hidden in 4 least significant bits in 24 bit true colour image. Juan Jose Roque and Jesus Maria Minguet developed the SLSB (Selected LSB) approach [5] using filtering algorithm in which a default filter is used to cover the most significant bits of every pixel, leaving the least significant bits to carry the secret information. Mr. Vikas Tyagi, in his research, combined the basic LSB technique with cryptography. Shilpa Gupta, Geeta Gujral and Neha Aggarwal proposed the Enhanced Least Significant Algorithm in order to reduce the distortion level which is attained when using basic LSB algorithm. The work is proposed especially for carrying small information. It improves performance of LSB by hiding information in only one of the three colours that is blue colour of the carrier image. In Vipul Sharma's and Sunny Kumar's work [6], for each pixel, either red, green or blue of the RGB component is replaced fully with the information and a cover image is used to hide the distortion.

Cellular automata concept has been used by several researches for encryption and decryption of image. 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.CA have been previously suggested as a method in encrypting devices by Wolfram and by Nandi [7]. In the work carried out by Nandi, Cellular Automata (CA) was used for a class of block ciphers and stream ciphers.

In M. Phani Krishna Kishore's and S. Kanthi Kiran's proposal [8], a Layered Cellular Automata was considered in which an automata was viewed as a system consisting of layers where each layer consists of rows of 1D cellular automata. In their proposed system (LRCA), the symmetric key encryption and block encryption technique were carried out. Marcin Seredynski's and Pascal Bouvry's concept [9] were based on one dimensional, uniform and reversible CA. Sambhu Prasad Panda, Madhusmita Sahu [10] proposed an encryption and decryption algorithm for block cipher based on the linear (periodic boundary-PB) and nonlinear cellular (complements) automata rules. In the work carried out by Pratibha Sharma, Niranjan Lal and Manoj Diwakar the basic LSB algorithm and a Cellular Automata Model known as Moore neighbourhood model [11] have been combined to provide two level data security.

3. PROPOSED SYSTEM

The Overall Module Design shows the different levels of security used in both sender's side and the receiver's side. The Modules are divided as follows,

i. Image Steganography
ii. Cryptography using Cellular Automata
iii. Decryption and Decoding on Receiver's Side
iv. Secure Transfer of Files in e-mail

3.1 Image Steganography

In the proposed system, the first level of security starts with Image Steganography, where the image (*.jpg*) is used as the object to hide. In the previous works, different algorithms like LSB, Enhanced LSB and Replacement of 8 bits colour pixel were used. The works on Image Steganography has been declining due to the reason that a small amount of data only could be embedded and transmitted in a very large sized image. To overcome that, in the proposed work, we replace every bits of the image file by which about 80% of the image file can be used to hide the data. But this causes major distortion to the Image used, so as a security measure we place another cover image over the distorted image. This provides both security

against eavesdroppers and increases the storage amount capacity for the confidential data.

In this module, first the file to be sent is chosen by the user. Then, based on the size of the file chosen the image which is suitable for the data to hide is automatically selected from the database. The data file is converted into bit streams and each pixel in the image is replaced with the bit streams of the data file. Then, to reduce the size of the resulting steganographic image it is saved as *.png* (Portable Network Graphics) format which effectively handles the compression of the Steganographic Images by itself. At last, the resulting output is sent to the next module of cellular automata.

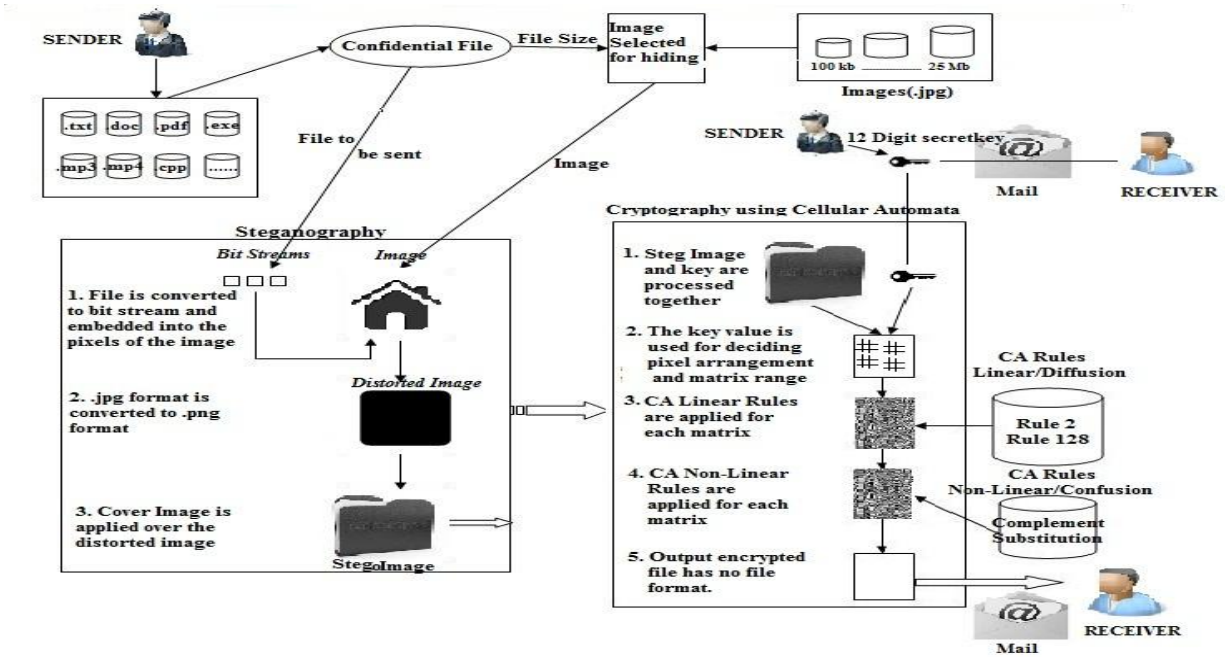

Fig-1: Overall System Architecture of proposed system

3.2 Cryptography using Cellular Automata

In the second level of security, we provide the cryptographic algorithm using the Cellular Automata (CA) technique to make the transmission more secure against some common Hackers attacks like Brute Force attack and Timing attack. The few well known cryptographic algorithms are AES, RSA, RC2, DES, 3DES, DSA. Most algorithms have major defect in the design of key used to pass along the file to be encrypted, since the key get trapped when the hackers use the Brute force attack. Even the complex way of designing the key using symmetric and asymmetric algorithms has been easily broken [12]. So, to handle this Cellular Automata provides a suitable solution because it has more advantage over other encryption algorithms. In the previous work, the encryption using CA of the images is handled in such a way that the image gets distorted using automata rules. But, the work has many major flaws. First, the cellular automata rules are applied to the key and processed along the image file and then the key is sent to the receiver, so there is a possibility to find the key value. Second, the file to be sent to the receiver is a highly distorted image format which has the high range of detection rate that an encrypted file is sent [13]. Third, the key doesn't have any direct impact in the process during encryption since it is mainly used like a password. Fourth, the key can be detected in no time using security attacks like brute force, since the operation stops as soon as the key value is wrong and asks for the re-entry of the password.

In the proposed work, the secret key is obtained by the user and the Linear Rules of CA (Diffusion) and Non-Linear Rules of CA (Confusion) are applied and the resulting highly secured output is sent to the receiver. Also, we came up with the solution for the above stated problems by follows methods respectively. The key value entered by the user is taken as the limit for the matrix range taken to apply CA rules for those blocks individually using a function to exact a specific value from the key. Hence the key value as the direct impact over the process of encryption and no longer it will act like a password rather a value which involves in the correct decryption of the original file. The output of the encryption will be distorted so to avoid it and to make it more complicated to determine the hackers about the presence, the end file is made in such a way that it has no file format to open and view it. It is sent as an unformatted file. To avoid the encrypted file from the brute force attack we used a key value of 12 digits. Along with it by using the random function, a 3 digit

range is framed from the key value. It is used to arrange the pixels in the Steg image in the order of the 3 digit value range and then the matrix computation is followed. From the Timing attack, it is protected since the main parameter considered by the Hackers in this attack is the program execution time module by module. But each rule applied to the individual matrix takes the same time to execute so there is no way to attack this using Timing Attack. Also since the key is not used like a password, even in the wrong attempt of key value the process continues till the decryption ends and the resulting output will be an invalid image. So, it consumes a complete process timing to find even a single wrong key. Thus, we provided a very high range of security measure to make transmission of the file in a secure manner to the receiver.

3.3 Decryption and Decoding on Receiver's side

The receiver uses the Hexadecimal value of the original key value provided by the user. By using Hex value the probability of finding the number still decreases. Then, the Hex value is converted to the original range since by using it the 3 digit number is obtained from the random function to arrange the pixels in the same pattern as the encryption is carried out. Also, the matrix range is obtained from the key value for the process of the reverse CA rules to be successful. After the successful attempt, Stego Image is obtained, and then it is sent to the steganography module again to extract the hidden confidential file.

3.4 Secure Transfer of Files in e-mail

The idea is to transmit the file safely by means of mail. The user has to mention his mail id and password and also the receiver's mail id in the user interface of the software which is designed based on the proposed method. Dynamically he has to choose the file to be transmitted. When the send command is given, the chosen file gets encoded in the auto chosen image and prompts the user to provide a secret key for encryption. When the image gets encrypted, it is sent to the receiver. The key is sent through proper channels. The receiver can view the file only if he provides the correct key for decryption and decoding. If wrong key is given, the resulting file would be an image which cannot be viewed (i.e. Invalid File).

4. PARAMETERS FOR TESTING

4.1 Performance Factors for Steganography

4.1.1 Embedding Ratio

$$\text{Embedding Ratio(ER)} = \frac{\text{Size of the Hiding Data}}{\text{Size of the Original Image}} \rightarrow (1)$$

The amount of data embedded in a file is calculated using Embedding Ratio. The size of the Hiding Data to the size of the Original Image gives the amount of data been embedded.

4.2 Performance Factors for Cryptography using CA

4.2.1 Computational Speed

In many real-time applications, it is important that the encryption and decryption algorithms are fast enough to meet real time requirements.

4.2.2 Security against Attack

The security has become a major concern since even the major encryption algorithms getting broken. So, to enhance the security level in this work, the solution has been provided for the Brute Force and Timing Attack.

5. Performance Evaluation for Proposed Work

5.1 Embedding Ratio

It can be inferred that the overall storage capacity of the proposed system has improved by storing about 73% of data to the image file where LSB contributes 12.5%, Enhanced LSB contributes 20.8% and the Replacement of Color Pixel method contributes 33.3% for the above file formats.

Table-1: Embedding Ratio

PROPOSED WORK	**EXISTING WORK**		
EMBEDDING RATIO	***EMBEDDING RATIO (LSB)***	***EMBEDDING RATIO (Enhanced LSB)***	***EMBEDDING RATIO (Replacement of Color Pixel Method)***
Text Document			
0.65	0.08	0.135	0.216
0.76	0.095	0.16	0.256
0.75	0.093	0.155	0.248
0.75	0.093	0.155	0.248
0.78	0.097	0.165	0.264
0.77	0.096	0.16	0.256
0.74	0.092	0.155	0.248
0.73	0.091	0.15	0.24
0.75	0.093	0.155	0.248
Word Document			
0.62	0.07	0.13	0.208
0.8	0.1	0.165	0.264
0.7	0.087	0.145	0.232
0.65	0.081	0.135	0.216
0.79	0.097	0.165	0.264
0.72	0.096	0.15	0.24
0.78	0.092	0.165	0.264
0.76	0.091	0.16	0.256
0.77	0.093	0.16	0.256

PDF Document			
0.6	0.075	0.125	0.2
0.7	0.087	0.145	0.232
0.75	0.093	0.155	0.248
0.71	0.088	0.15	0.24
0.72	0.09	0.15	0.24
0.78	0.097	0.165	0.264
0.76	0.095	0.16	0.256
0.79	0.098	0.165	0.264
0.79	0.098	0.165	0.264
EXE File			
0.6	NA	NA	NA
0.74	NA	NA	NA
0.69	NA	NA	NA
0.6	NA	NA	NA
0.66	NA	NA	NA
0.67	NA	NA	NA
0.73	NA	NA	NA
0.7	NA	NA	NA
0.7	NA	NA	NA

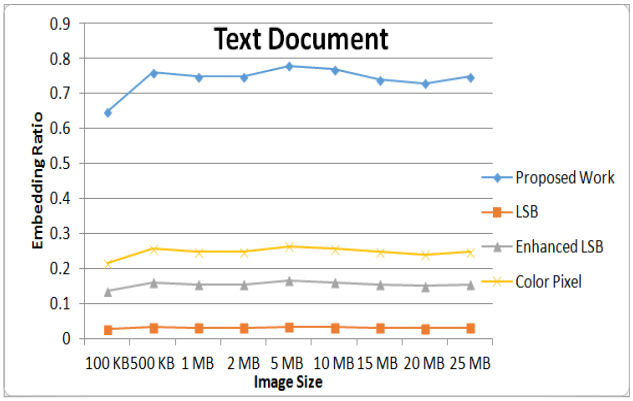

Chart-1: Embedding ratios of different algorithms for text document

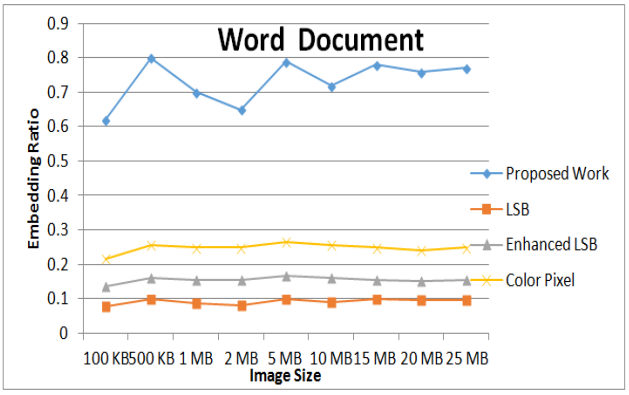

Chart-2: Embedding ratios of different algorithms for word document

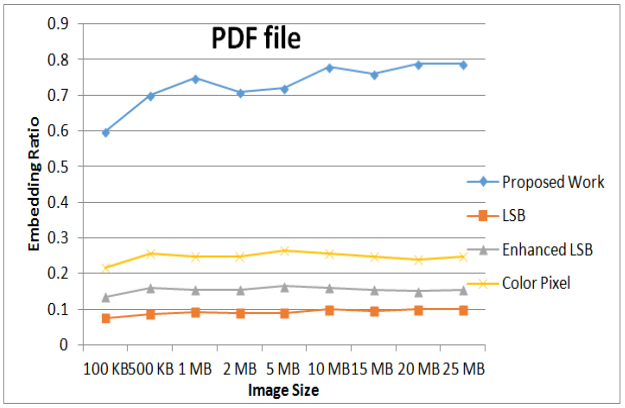

Chart-3: Embedding ratios of different algorithms for pdf document

5.2 Computational Speed

From the above graph, it clearly states that the computational speed of our proposed system of CA has increased by 2.5 times, 3 times, 6 times and 10 times when compared to Blow Fish, DES, AES and 3DES respectively.

Table-2: Computational Speed

Input Size (bytes)	DES	3DES	AES	BF	CA
20,527	24	72	39	19	10
36,002	48	123	74	35	14
45,911	57	158	94	46	19
59,852	74	202	125	58	25
69,545	83	243	143	67	32
137,325	160	461	285	136	54
158,959	190	543	324	158	56
166,364	198	569	355	162	58
191,383	227	655	378	176	65
232,398	276	799	460	219	73
Bytes/ sec	835	292	491	1036	2754

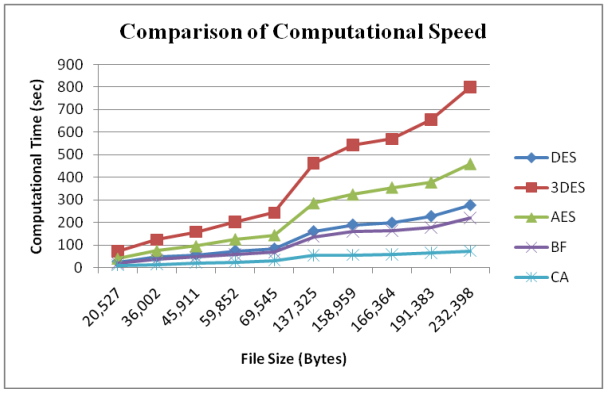

Chart-4: Comparison of Computational Speed

5.3 Security against Attacks

We have provided the solution for the brute force attack and Timing Attack in the paper by providing Hexadecimal secret key of size 10 since the time taken to crack this seems to be approx. 9 years and by providing security alert message to the user, once the key is provided wrongly it avoids the Brute Force Attack. The Timing Attack is handled effectively by using the key value to decide the arrangement of the matrix range. Thus, the execution speed of each and every matrix range gets similar. So, this avoids the timing attack to take effect.

6. CONCLUSIONS

From the above results it is clearly found that the embedding ratio, Computational speed and the Security against few Attacks have been enhanced. Thus the proposed work of joining the Steganography and Cellular Automata 2-D has desirably increased the security level of the hidden data. The proposed work can also be used in Bluetooth transfer application where the received software needs the secret key to decrypt and decode the encrypted file. The future works may involve by enhancing the Cellular Automata technique in 3-D form. Also we have used the symmetric encryption key method in the proposed work. So, the Asymmetric encryption key method can be carried out to enhance the proposed work.

REFERENCES

[1] V. Lokeswara Reddy, A.Subramanyam and P. Chenna Reddy, "Implementation of LSB Steganography and its Evaluation for Various File Formats", Int. J. Advanced Networking and Applications 868 Volume: 02, Issue: 05, Pages: 868-872 (2011).

[2] Shilpa Gupta, Geeta Gujral and Neha Aggarwal, "Enhanced Least Significant Bit algorithm For Image Steganography", IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012.

[3] Stephen Wolfram, "Cryptography with cellular automata". Lecture Notes in Computer Science, 218 (Springer-Verlag, 1986), pages 429-432, 1986.

[4] Mazen M Al Hadidi, Yasir Khalil Ibrahim and Haitham Karim Ali, "Data Hiding Using Least Significant Bit Approch", Recent Researches in System Science, ISBN: 978-1-61804-023-7, pp.238-240.

[5] Juan Jose Roque and Jesus Maria Minguet, " SLSB: Improving the Steganographic Algorithm LSB ", Universidad Nacional de Educación a Distancia (Spain).

[6] Vipul Sharma and Sunny Kumar , "A New Approach to Hide Text in Images Using Steganography", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 4, April 2013.

[7] 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.

[8] 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.

[9] 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.

[10] Sambhu Prasad Panda and 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.

[11] Pratibha Sharma, Niranjan Lal and Manoj Diwakar, "Text Security using 2D Cellular Automata Rules", Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013), Published by Atlantic Press.

[12] AL.Jeeva, Dr.V.Palanisamy and K.Kanagaram, "Comparative analysis of performance efficiency and security measures of some encryption Algorithms", ISSN: 2248-9622 ,Vol. 2, Issue 3, May-Jun 2012, pp.3033-3037.

[13] Vinay pandey, Angad Singh and Manish Shrivastava, "Medical Image Protection by Using Cryptography Data-Hiding and Steganography", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 1, January 2012.

BIOGRAPHIES

Dr. S. Saraswathi is the Professor, in the Department of Information Technology, Pondicherry Engineering College, Pondicherry, India. She is the Head of the Department. She completed her PhD, in the area of speech recognition for Tamil language. Her areas of interest include speech processing, artificial intelligence and expert systems

V. Santhosh Raj is final year student of Department of Information Technology, Pondicherry Engineering College, Pondicherry, India. His areas of interest are Artificial Intelligence, Computer Networks and Database Management.

S. Sethuraman is final year student of Department of Information Technology, Pondicherry Engineering College, Pondicherry, India. His areas of interest are Object Oriented Programming Concepts and Computer Networks.

J. Saravanan is final year student of Department of Information Technology, Pondicherry Engineering College, Pondicherry, India. His areas of interest are Artificial Intelligence and Data Structure.