

## International Conference on Emerging Innovation in Engineering and Technology

ICEIET-2017

## Image Encryption Using DNA Cryptography And Cellular Automata

Dr.S.Saraswathi<sup>1</sup>, Ch.Rushmitha<sup>2</sup>, S.Dhivya@Thirupurasundari<sup>3</sup>S.Nandhini Devi<sup>4</sup>,P.Revathi<sup>5</sup><sup>1</sup> Professor,<sup>2,3,4,5</sup> Student,Department of Information Technology,Pondicherry Engineering College,  
Kalapet, Puducherry.<sup>1</sup>swathi@pec.edu,<sup>2</sup>ch.rushmitha@gmail.com,<sup>3</sup>dhivyagaya3@gmail.com, <sup>4</sup>snandhinidevi20@gmail.com,  
<sup>5</sup>revathiparthiban@gmail.com**Abstract**

An image encryption scheme based on DNA cryptography and Cellular Automaton is presented. DNA Cryptography is a new technique in which DNA is used as an Information carrier. Cellular Automata in which patterns generally stabilize into homogeneity, in which patterns evolve into mostly stable or oscillating structures. In Cellular Automata, patterns evolve in a seemingly chaotic fashion, in which patterns become extremely complex and may last for a long time, with stable local structures. . These qualities are most impressive in these technology which help us to provide a highly secured security system for the users. There are limitations in most of the encryption techniques based on the cellular automata. To overcome this problem, we propose a DNA cryptography algorithm with cellular automata to make the system work in a more secured manner. First, a partially encrypted image is obtained by encrypting the pixels with DNA sequence such as adenine, guanine, cytosine, and thymine . At this stage the image is prone to attack. So to make the system more secure second level encryption is done. This is done by using the rules of Cellular Automata to get the more secure encrypted image.

**Keywords**— Cellular Automata, DNA, Adenine, Guanine, Cytosine, Thymine.

**I. INTRODUCTION**

Nowadays, Internet has become parts and parts of human life and it has emerged closely with human such that it is elevated as one of the basic needs of human life. The facility of using the Internet in mobile phones has increased its use among common man. Many sectors of business such as bank, travel, shopping etc., make use of Internet to reach many people and flourish their business by introducing their application (apps). Though there are many advantages of Internet, it has adverse effect such as security. Financial transactions, confidential government information, and medical records is transmitted through Internet which are sensitive. The protection of this sensitive information in the Internet is done by information security systems such as cryptography [2], steganography [3] [4] and combination of cryptography and steganography [5]. Security in Internet is provided by the information security systems. With the advancement in computational infrastructure and computer processing capacity, standard information security systems are no longer secure. As traditional cryptographic methods are based on mathematical and theoretical models, with the

recent advancements in computational techniques, cryptographic methods are vulnerable to attacks. Several protection method has been proposed to ensure the security and confidentiality of the information that is being transmitted. This paper effectively uses DNA cryptography and Cellular Automata to encrypt the images.

DNA computing is used to achieve massive parallelism, huge storage and ultra-low power consumption. From the research on DNA computing, DNA cryptography emerged as a new cryptographic field. Here DNA is used as an information carrier and modern biological technology is used as implementation tool. In this paper DNA sequence is effectively used of hiding the pixel information. For example, 00 is coded as A,01 is codes as T, 10 is coded as G and 11 is coded as C. This paper, try to utilize the power of DNA to hide the image[6].

Cellular automation is a system made up of many discrete cells, each of which may be in one of a finite number of states [7]. A cell or automaton may change state only at fixed, regular intervals, and only in accordance with fixed rules [16] that depend on cells own values and the values of

neighbours within certain proximity. The formal definition of Cellular Automata (CA) is one or two dimensional grid [8] of identical automata cells. Depending on its neighbourhood cells, each cell processes information and proceeds in its action .

**II. LITERATURE SURVEY**

This section defines the purpose of combining DNA computing and cellular automata methods .

DNA cryptography is a new technique for achieving parallelism, high density information carrier of DNA molecules and low power consumption, which challenges traditional cryptography. Guangzhao Cui et al [9], in his paper discussed about DNA computing and its application in information security field and reviews the principle of DNA computing

An analysis on DNA based cryptography to transfer the data securely and also discusses DNA technology used in the cryptographic methods was discussed by S.Jeevidha et al [10].

H.Z.Hsu [11] in his method exploits the several ways of DNA sequence to encrypt data. The author presents three methods namely, the insertion method, the complementary pair method and the substitution method. In [9] the paper analyze some schemes with secret key searching. Anupriya et.al [12] in her paper proposed an algorithm which is based on key sequence known only to two parties which is involved in communication. Since there are roughly 55 million publicly available DNA sequence it is virtually impossible to crack the sequence.

Rama R et al [13] proposed the Study of Data Encryption Standard (DES) Algorithm with Cellular Automata. In 1976 , the standard encryption algorithm was DES algorithm. The concept of Cellular Automata (CA) introduced by John von Neumann (1950s) exhibited the capability of producing complex and random behavior is the first model.

Cellular Automata is a parallel processor, which is dependent on the behavior of the cell at the time ‘t’[17]. The usage of Cellular Automata rules are simple in nature for the operation of DES and Advanced Encryption Standard (AES) algorithms.

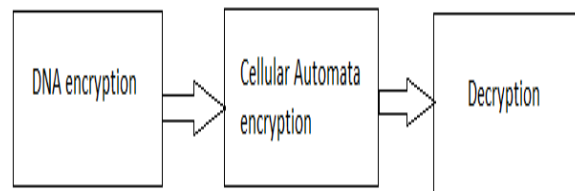
In smart devices, to provide security [14], pattern classification [15] and traffic modeling, cellular automata is applied. For the key generation in DES, Rama R et al [11] extend the usage of Cellular Automata (CA). In this, they have used rule 30 of cellular automata to achieve randomness. The minimal key size is the demerit in this approach.

**III. PROPOSED WORK**

This system is for encrypting the images based on the concepts of DNA cryptography and Cellular Automata. Image is broken down to binary pixel. The pixels are divided into sub matrices and the pixels are being encrypted with DNA sequence. Then this is again encrypted with the concept of cellular automata. The decryption happens to obtain the original image.

*A. Modules Involved*

We have proposed three modules in this system to achieve high parallelism and security in image encryption. Implementing only the first module will make the system prone to attacks such as pattern recognition. Merging the DNA encryption module with the rules of Cellular Automata high security of image is enabled. The Modules involved are DNA Encryption, Cellular Automata Encryption and decryption.



**Fig1. Overview of proposed system**

*B. DNA Encryption*

Original image is given as the input. The pixel information is first retrieved from the image. The sub matrix of pixels is obtained from the image. Pixel values of the sub matrix is then converted to binary sequence . DNA sequence is assigned to the elements in the array. i.e. encrypting the pixels with the DNA sequence. Temporary values are substituted in the obtained sequence. Then they are converted to the corresponding decimal values. Here the output is obtained is the partially DNA encrypted image.

All title and author details must be in single-column format and must be centered. Every word in a title must be capitalized. Email address is compulsory for the corresponding author.

*C. Cellular Automata Encryption*

The Cellular Automata Encryption involve the following steps . The Partially Encrypted Image is given as the input. The pixel information is first retrieved from the partially encrypted image. The sub matrix of pixels is obtained from the partially encrypted image. Pixel values of the sub matrix

is then converted to binary sequence . Cellular automata is then applied on binary sequence of each pixel. Rule 90 of cellular automata is used to apply on those pixels. Rule 90 is a Cellular Automata technique which changes the current state of the cell based on the neighbourhood cells. Thus the cellular automata is applied on each and every pixel of the image and thus encrypted. Here the output obtained is the fully encrypted image.

- Set of States  $S = \{S1, S2, S3, S4, \dots, SN\}$
- Transition Rules T
- Therefore  $A \sim (S, T, R)$  (R: neighboring automata)
- T:  $(St, It) \textcircled{R} St+1$

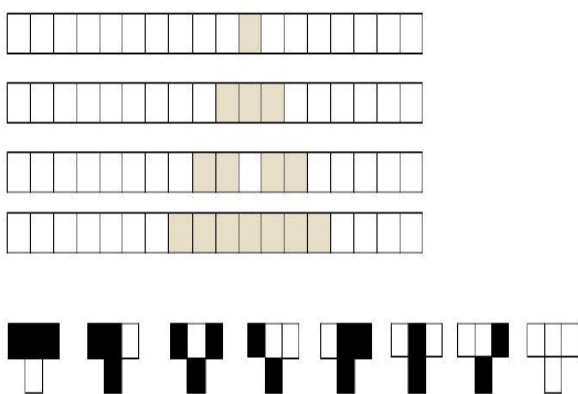


Fig2. Cell definition

D. Decryption

The encrypted image is given as input for decryption. From the encrypted image the temporary matrix is generated . Temporary matrix is broken into sub-block. In the each sub-block, reverse the cellular automata rule to obtain the partially encrypted image. The partially encrypted image is then decrypted by reversing the process of DNA Encryption. Thus a decrypted image is obtained.

E. Interaction Between The Modules

The DNA encrypted pixel information is retrieved from the DNA encryption module and then the output of the first module is used to apply cellular automata in the next module. Now the output of this operation forms the Encrypted Image. This Encrypted Image is decrypted in the decryption module.

F. Input And Output Description :

The Input is the secret image of jpg,tif,png,jpeg,bmp,pgm and gif format which has to be encrypted.

The output is the encrypted image by DNA sequence and cellular automata and the output also includes the image that is decrypted.

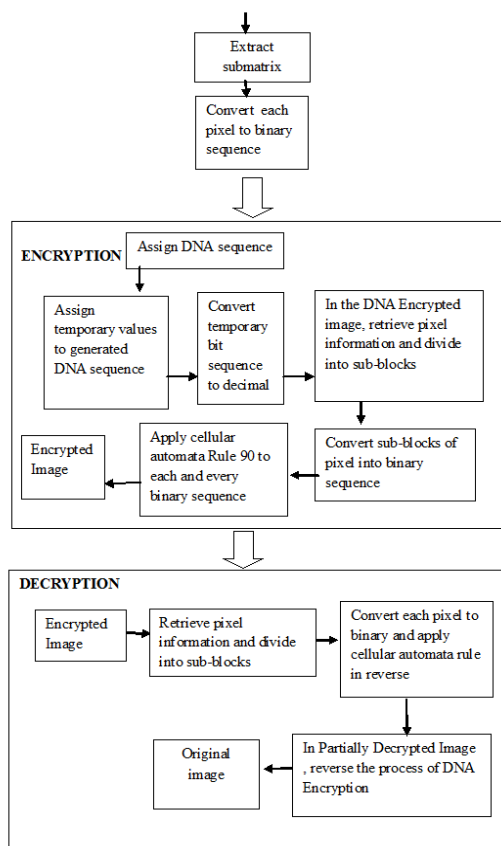


Fig3. System Architecture

TABLE Error! No sequence specified.

TYPE OF IMAGE	NUMBER OF IMAGE(S) TESTED	ATTACKES OVERCOMED
JPEG	4	Brute force and differential
PNG	3	Brute force and differential
TIFF	1	Brute force and differential

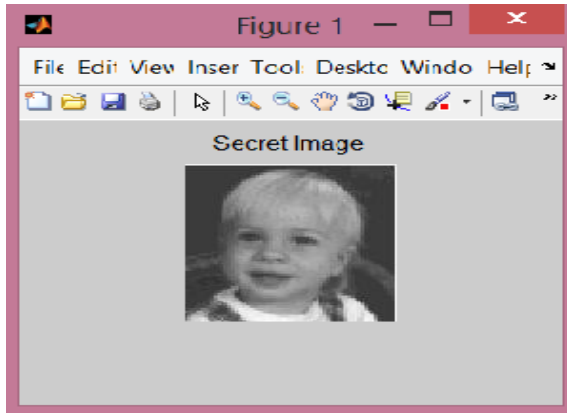


Fig4. The Image that is to be encrypted

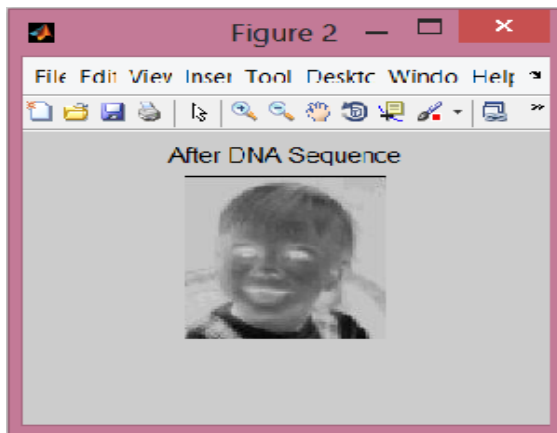


Fig5. Partially encrypted DNA image



Fig6. Image encrypted with Cellular Automata

#### IV. CONCLUSION

This paper explores the DNA cryptography along with the finite state machine. In the proposed algorithm, image is secured at 3 levels, using : conversion in DNA, DNA is converted in binary based sequence and it is subjected to rule 90 of cellular automata. By using this algorithm and mechanism the generated cipher image is quite difficult to crack. The proposed algorithm is powerful in terms of security features. Now we are working to increase the security by randomly applying the cellular automata rules to increase complexity, and then quality of the image will be calculated in future. Differential attack and brute force attack can be overcome by this further level of security.

#### REFERENCES

- [1] G.Shanmugasundaram, P.Thiyagarajan and S.Pavithra, "A Novel DNA Encryption system using Cellular Automata", International Journal of Security , Privacy and Trust Management (IJSPTM), vol.4, no.3/4, pp.39-49, November 2015.
- [2] Ferguson, N.,Schmier, B. and KonhoT, "Cryptography Engineering: Design principles and Practical applications", 2010.
- [3] Thiyagarajan P, Aghila G, Prasanna Venkatesan V, "Dynamic Pattern Based Image Steganography", Journal of Computing , vol.3, Issue 2 February 2011, pp.1-9, ISSN 2151-9617.
- [4] Thiyagarajan P, Natarajan V, Aghila G, Prasanna Venkatesan V, Anitha R, "Pattern based 3D Image Steganography", Springer 3D Research Journal, vol. 04, no.1, March 2013, pp.1-8, ISSN: 2092-6731.
- [5] Thiyagarajan P, Aghila G, Prasanna Venkatesan V, "Stepping up Internet Banking Security using Dynamic Pattern Based Image Steganography", Springer (LNCS) in Communications in Computer and Information Science Series(CCIS) , June 2011, ISSN: 1865:0929.
- [6] U.Noorul Hussain, T.Chithralekha, "Review of DNA cryptology", CiiT International Journal of Networking and Communication Engineering, vol.03, no.13, October 2011, pp.843-849.
- [7] Stephen Wolfram, "Random sequence generation by cellular automata", Advances in Applied Mathematics, 7:123,169, 1986.
- [8] Sambhu Prasad Panda, MadhusmitaSahu, Umesh Prasad Rout and Surendra Kumar Nanda, "Encryption

and Decryption algorithm using two dimensional cellular automata rules in Cryptography”, International Journal of Communication Network & Security, vol-1, Issue-1, 2011.

[9] Guangzhao Cui, Cuiling Li, Haobin Li and Xiaoguang Li, “DNA Computing and Its Application to Information Security Field”, Fifth international conference on natural computation, 2009.

[10]S.Jeevidha et.al , “Analysis on DNA based Cryptography to Secure Data Transmission”, International Journal of Computer Applications (0975 – 8887), vol.29– no.8, September 2011.

[11] H. Z. Hsu and R. C. T. Lee, “DNA Based Encryption Methods”, The 23rd workshop on combinatorial mathematics and computation theory.

[12] Anupriya Aggarwal and Praveen Kanth, "Secure Data Transmission Using DNA Encryption", Computer Engineering and Intelligent Systems, vol.5, no.7, 2014.

[13] Rama R, BalaSuyambu J, Andrew Arokiaraj, ShanmugamSaravanan, “A Study of DES Algorithm with cellular automata”, International Journal of Innovative Management, Information & Production ISME International , ISSN 2185-5439 vol.3, no.1,March 2012 , pp.10-16.


[14] M.Venugopal, Dr. E.G.Rajan and Dr. Sharma, “Security measures for Smart Devices through Cryptography Using Cellular Automaton”, International Journal of Computer Science and Information Technologies, vol. 4 (1), pp.129 – 133, 2013.



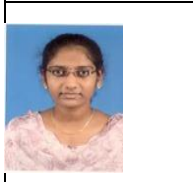

[15] PradiptaMaji and Chandrama Shaw, NiloyGanguly, Biplob K. Sikdar and P. Pal Chaudhuri, “Theory and Application of Cellular Automata For Pattern Classification”, FundamentaInformaticae 58 (2003) 321–354 321,IOS Press.

[16] Cellular Automata The 256 Rules (Stanford Encyclopedia of Philosophy)- url:http://www.roguebasin.com/index.php retrieved on september 16, 2013.

[17] Cellular automaton - Wikipedia, the free encyclopedia url:http://en.wikipedia.org/wiki/Cellular\_automaton retrieved on july 15, 2015.

**Author’s Biography**

	<p>Dr.S.Saraswathi is Professor in the Department of Information Technology, Pondicherry Engineering College, Pondicherry, India. She completed PhD,</p>
---	--

	<p>in the area of speech recognition for Tamil language. Her areas of interest include speech processing, artificial intelligence and expert systems.</p>
	<p>Ch.Rushmitha is the final year student of Department of Information Technology,Pondicherry Engineering College,Puducherry</p>
	<p>S.Dhivya Thirupurasundari is the final year student of Department of Information Technology,Pondicherry Engineering College,Puducherry</p>
	<p>S.Nandhini Devi is the final year student of Department of Information Technology,Pondicherry Engineering College,Puducherry</p>
	<p>P.Revathi is the final year student of Department of Information Technology, Pondicherry Engineering College, Puducherry</p>