ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 11, November 2018

A Hybrid DNA Based Cryptography Algorithm Using Chaos Method

Paulin Rachel C.[1], Dr. Sampath Kumar[2]

PG Scholar, Dept. of CS & SE, Andhra University College of Engineering, Visakhaptnam, India[1]

Professor, Dept. of CS & SE, Andhra University College of Engineering, Visakhaptnam, India[2]

ABSTRACT:The security of data is a crucial issue in our everyday life, especially when it comes to healthcare related data collected using wearable devices, the usage of which is becoming widespread. DNA based cryptography is a new promising direction in this field of security. Additionally, Chaos theory is another paradigm which seems promising. In this paper, a hybrid cryptography algorithm is proposed keeping in mind the limitations of the memory of the wearable health devices and the dire need for high level of security. The proposed algorithm makes use of the genomic encryptions and the deterministic chaos method resulting in a hybrid DNA based cryptography algorithm using chaos method that provides a high level of security.

KEYWORDS: Genomic encryptions, DNA cryptography, Chaos function, Security.

I. INTRODUCTION

With the increase in the usage of mobile devices by the healthcare organizations with various storage options, cloud computing security is soon becoming a top healthcare industry concern. The key intent of this paper is to present a nee algorithm for security to ensure confidentiality, integrity and authentication. Cryptography is the science of protecting the privacy of information during communication under hostile conditions. The healthcare related data that is collected using wearable devices must be ensured that it is not manipulated in the course of communication as that could lead to fatal issues. Cryptography is now routinely used to protect data, which must be communicated or saved over long periods. Among the present cryptographic methods under research, Chaos is another paradigm. It is an offshoot from the field of nonlinear dynamics. The chaotic behavior has the major characteristics such as its high sensitivity to the initial conditions thereby exhibiting a fine behavior of a nonlinear system.

Along with the various cryptographic systems that were developed in the past years, the recent development in this field is the DNA Cryptography which has emerged after the disclosure of computational ability of the DNA (Deoxyribo Nucleic Acid). DNA can be used in cryptography as well as for computation [1].

II. RELATED WORK

Being an emerging technology, a lot of research has been done in the field of DNA cryptography. As many modern cryptography algorithms have been broken, new ways of encryption are being sought to secure data. The earliest involvement of DNA in computing was introduced by Adleman [2] where real world computation problems were solved using DNA computing. This paved the way for DNA to be used in the field of cryptography for the generation of ciphers that would be unbreakable. It was examined by [3] that Data Encryption Standard (DES) can be broken using the DNA computing. It also paved the way for DNA steganography in which DNA encoded message was hidden and compressed in the complexity of human genomic DNA [4]. DNA cryptography further advanced to the formation of a one time pad using DNA strands [5]. In yet another advancement, instead of using actual DNA computing, the principal ideas of molecular biology were applied in encryption [6]. In [7], a simple substitution cipher based on the structure of DNA and its sequence was proposed.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 11, November 2018

Chaos based cryptography has also been given more attention over the past years. Among the early works [8] and [9], Chaos based cryptography has been used on cryptosystems in cellular automation. The properties of cryptography occur normally in chaotic system, therefore chaos based cryptography is on the rise [10]. Using both genomics and chaos theory, [11] designed an image encryption algorithm. [12] has proposed a genomics computing algorithm that aims to perform computations with adaptive parameters. Further, an algorithm that encrypts a color image using DNA encoding and chaos theory was designed by [13]. In this paper, an algorithm based on genomic encryption and chaos theory has been implemented to protect physiological signals such as ECG. The rest of the paper is organized into: Section III gives the background details of genomic based encryption and chaos function. Section IV explains the proposed algorithm used followed by results in Section V and conclusions in Section VI.

III. BACKGROUND

De-oxyribo Nucleic Acid (DNA)

The genetic material in humans and almost every other organism is known as the De-oxyribo Nucleic Acid or DNA. The information contained in the DNA is stored in the form of chemical bases. There are four chemical bases: adenine (A), guanine (G), cytosine (C) and thymine (T). These bases are arranged in an order which determines the information that is available to build and maintain an organism. This concept can also be used in many encryptions algorithms emulating the DNA structure. [14] The DNA bases pair up with each other in a manner such that adenine is conjoined with thymine while cytosine with guanine. Each base is attached to a sugar molecule and a phosphate molecule, this combination together is called a nucleotide [15]. These nucleotides are arranged in two long strands in the form of a double helical structure.

The cryptography based on genomics emerged as a new field in cryptography in the year 1994 and is being used as carrier of information and as implementation tool in biological technology. The process of computation using cryptography based on genomics produces a sequence of nucleotides in the form of the bases A, T, C and G as the encrypted data output. The DNA bases are encoded such that A=00; T=01; C=10; G=11 and addition and subtraction is performed on these values similar to binary addition and subtraction respectively, this is used to encode the data.

Chaotic Systems

Chaos or chaotic system is an intersection between fixed regularity and non-predictability based on probability [16]. They have been used in mathematical models of the nonlinear systems, attracting the attentions of many mathematicians owing to the extreme sensitivity of the chaos functions to the initial conditions of the system, as well as their enormous applicability to modelling complex problems of daily life. The nature of the sequences produced by such functions has good amount of randomness and complexity making it highly usable for cryptographic algorithms. The important advantage in using the Chaos functions is the observation that a chaotic signal in general looks like noise to unauthorized users. The added benefit is that generating chaotic values is often low cost with simple iterations making it suitable for construction of stream ciphers i.e. chaotic stream ciphers use the chaotic functions to generate random key streams for the encryption of data [17].

IV. PROPOSED SYSTEM

The proposed system implements a hybrid algorithm which uses genomic encryption and chaos function to encrypt data. The chaos function used is the optical logistic map built using Mach Zehnder interferometers. The proposed algorithm takes in the input of ECG digital signals and works in 8 simple steps for the encryption of the inputted data. These steps are as follows:

Step 1: Convert the signal samples into a sequence of binary values as a binary matrix.

Step 2: The binary sequence is then encoded into nucleotides matrix which is the DNA sequence matrix to the encoding matrix; such that A=00, T=01, C=10, G=11.

Step 3: The DNA sequence matrix is divided into 8 sub-matrices.

Step 4:A chaotic signal is generated through 1-D chaotic map with initial conditions x01 and constant parameter μ01. The chaotic sequence is then scaled to [0, 65536].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 11, November 2018

Step 5: The step 1 to step 3 are applied to the chaotic sequence generated in the previous step.
Step 6: The DNA sub-matrices of the original signal are then added to the DNA sub matrices of the chaotic sequence, according to the rules of binary addition.
Step 7: The sub-matrices are then recombined to form a new sequence matrix of binary values which is then communicated and/stored for later use.
Step 8: Applying the inverse of the steps 2 and 1 for the above obtained sequence matrix will give us the real value of the matric that would represent the encrypted data signal.
For the process of decryption, the steps are applied in the reverse manned from the step 8 to the step 1. Also, instead of addition, subtraction operation is used. The addition and the subtraction is the binary addition and the subtraction of the binary form of the DNA bases respectively.

V. RESULTS

For this algorithm, the data has been taken from the Physionet waveform database [18] and the algorithm was implemented in Matlab. This hybrid algorithm which has been proposed for the ECG signal encryption is designed to be an algorithm where all computations can be performed on the sensor node, with limited resources. The usage of the chaotic function to generate a key sequence is much more powerful than most other key generators. This algorithm requires minimum computations. It minimizes the required memory space making it useful to be used in wireless sensor network because of the nature of the one-time pad to encrypt each sample. The implementation results are obtained both on Matlab Command Window and Matlab GUI. The screenshot of the Graphical User Interface of the implemented algorithm in Matlab is as follows:

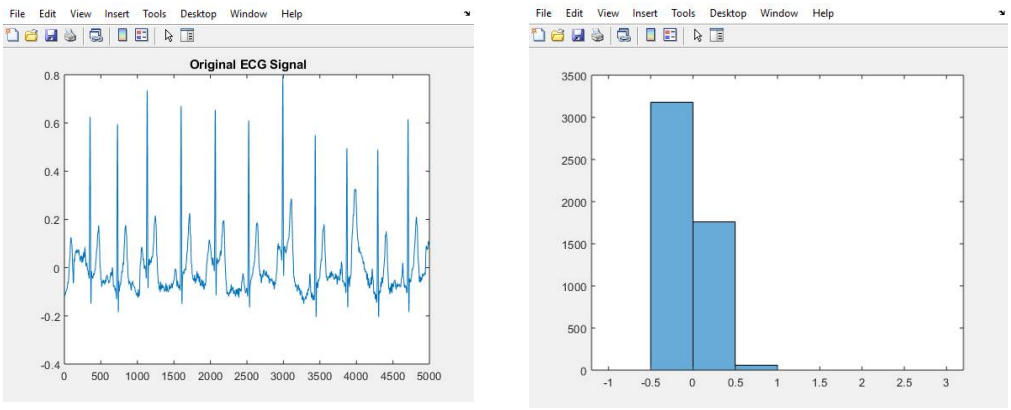

Fig. 1 Original ECG Signal and histogram of original ECG Signal

When a person's ECG signal is encrypted using the proposed encryption algorithm the following results are displayed. Fig. 1 shows the original ECG signal of the selected person before encryption and also the histogram of the original ECG signal prior to encryption.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 11, November 2018

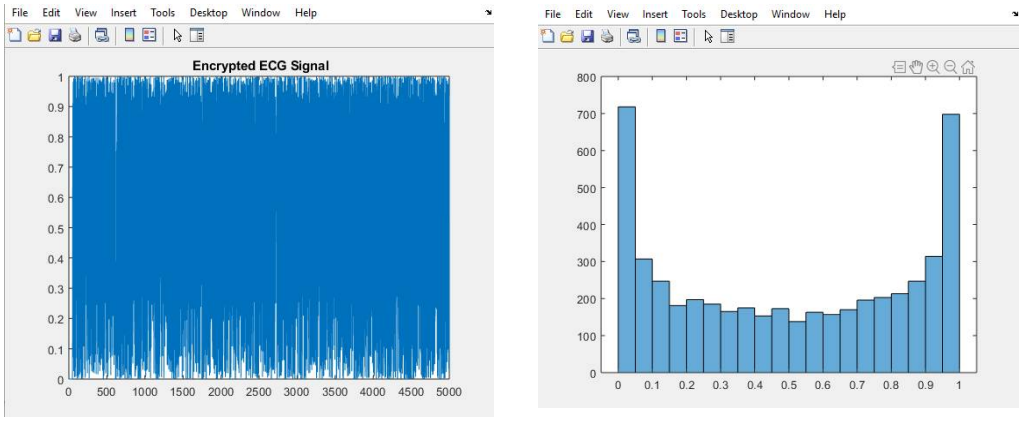

Fig. 2Encrypted ECG Signal and its histogram

The above images show the encrypted ECG signal after the proposed encryption algorithm has been applied on the original ECG signal. Fig. 2 shows the encrypted ECG signal that can be stored or communicated which seems as noise to an eavesdropper because of the chaotic behaviour of the system. Fig. 2 also shows the histogram of the encrypted ECG signal showing the distribution of the data.

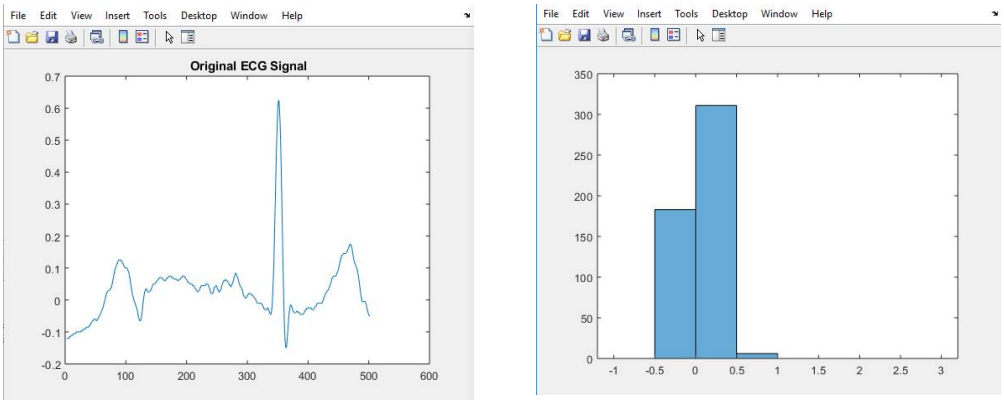

Fig. 3Original single beat ECG Signal and its histogram

Likewise, taking into consideration a single beat of an ECG signal to apply the proposed cryptography algorithm, the fig. 3 shows the original single beat of an ECG signal that is going to be encrypted and the histogram of the original single beat of the ECG signal prior to encryption.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 11, November 2018

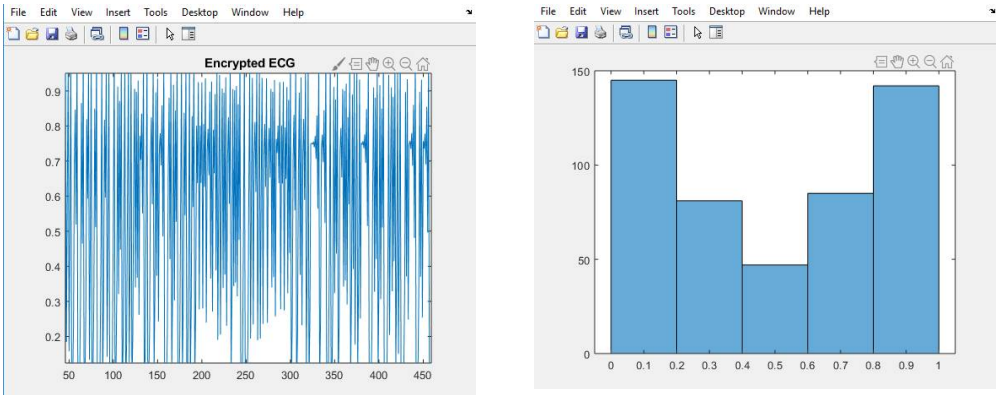

Fig. 4Encrypted single beat ECG Signal and its histogram

The result of encryption of the single beat of the ECG signal is shown in the images above. Fig. 4 shows the encrypted single beat ECG signal when the proposed hybrid cryptographic algorithm was applied on it. The histogram of that encrypted signal showing the distribution of the data after the algorithm was applied is also shown adjacent to the image of the encrypted signal.

VI. CONCLUSION

Since the usage of smart wearable devices in the field of medicine is becoming prominent for healthcare providers due to many advantages, the maintenance of security of data collected over these devices plays a vital role in its ultimate usage. Using the basic cryptography algorithms for those security issues does not protect health data over the network as the data can be transferred over multiple devices and various protocols. The hybrid algorithm that has been proposed and implemented in this paper is based on the genomics encryptions and the chaos theory for the protection of the health data from any attack namely, man-in-the-middle, brute force or even key theft attack. Also this algorithm considers the size limitations of the above mentioned devices and the limitation of other resources. The implementation and the results prove it to be ideal for such systems for the security of the data and their computations.

REFERENCES

1. Snehal Javheri, Rahul Kulkarni, “Secure Data communication and Cryptography based on DNA based Message Encoding”, International Journal of Computer Applications, Volume 98– No.16, July 2014.
2. Adleman L M, Molecular Computation of Solutions to Combinatorial Problems, Science, Vol 266, pp 1021-1024, November 1994.
3. Dan Boneh, Cristopher Dunworth, and Richard Lipton. "Breaking DES Using a Molecular Computer". Technical Report CS-TR-489-95, Department of Computer Science, Princeton University, USA, 1995.
4. TAYLOR Clelland Catherine, Viviana Risca, Carter Bancroft, 1999, "Hiding Messages in DNA Microdots". Nature Magazine Vol. 399, June 10, 1999.
5. Gehani, T. LaBean, and J. Reif, DNA-Based Cryptography, Lecture Notes in Computer Science, Springer, Vol 2950, pp 167-188 2004.
6. KANG Ning, "A Pseudo DNA Cryptography Method", Independent Research Study Project for CS5231, October 2004.
7. Bonny B Raj, J Frank Vijay, and T Mahalakshmi, “Secure Data Transfer through DNA Cryptography using Symmetric Algorithm”, International Journal of Computer Applications, Volume 133- No. 2, January 2016.
8. S. Wolfram, Cryptography with cellular automata, CRYPTO ’85 Advances in Cryptology, pp. 429–432, 1986.
9. P. Guan, Cellular automaton public-key cryptosystem, Complex Systems, 1, pp. 51–57, 1987.
10. P. Carmenand L. Ricardo, Notions of choatic cryptography: Sketch of a chaos based cryptosystem, Applied Cryptography and Network Security, pp. 267–294, 2012.
11. Q. Zhang, L. Guo, and X. Wei, “Image encryption using dna addition combining with chaotic maps,” Mathematical and Computer Modelling, vol. 52, no. 11, pp. 2028–2035, 2010.
12. M. Karakose and U. Cigdem, “Qpso-based adaptive dna computing algorithm,” The Scientific World Journal, vol. 2013, 2013.
13. M. A. Mokhtar, S. N. Gobran, and E.-S. A. El-Badawy, “Colored image encryption algorithm using dna code and chaos theory,” in Computer and Communication Engineering (ICCCE), 2014 International Conference on. IEEE, pp. 12–15, 2014.
14. Watson, J.D., & Crick, F.H.C., “A structure for deoxyribose nucleic acid. Nature 171, 737-738 , 1953.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 11, November 2018

15. M. E. Borda, O. Tornea, and T. Hodorogea, “secret writing by dna hybridization,” Acta Technica Napocensis-Electronica-Telecommunicatii (Electronics and Telecommunications), vol. 1, no. 50, pp. 21-24, 2009.
16. Q.V. Lawande and S.D. Dhodapkar, “Chaos based Cryptography: A new approach to secure communications”, BARC Newsletter 258, July 2005.
17. Winnie Sara Simon, Josy Elsa Varghese,”Chaotic based asymmetric and symmetric key encryption using augmented Lorenz Equations, International Journal of scientific research and management, Vol.3 Issue 11, pp. 3762-3769, 2015.
18. Lugovaya T.S. Biometric human identification based on electrocardiogram. [Master's thesis] Faculty of Computing Technologies and Informatics, Electrotechnical University "LETI", Saint-Petersburg, Russian Federation; June 2005.