PROTECTION TECHNIQUES FOR TRANSFORMED EEG SIGNALS

Ankita Varshney[1],Abdul Khalid [2], Shaziya Parveen[3]

Department of Computer Science and Engineering,

Noida Institute of Engineering & Technology Greater Noida India , AMU University Aligarh India

ABSTRACT: **In recent developments network security and data encryption have become vital and high profile issues. New approaches in encryption techniques are required to be developed for effective data encryption and multimedia applications.**
For future internet applications on wireless networks, besides source coding and channel coding techniques, cryptographic coding techniques for multimedia applications need to be developed.
Telemedicine changes the way patients are treated, from the traditional methods of a person care to remote care; The concept of Telemedicine is totally depending on the wireless network. i.e. Internet which is public network anyone can access the confidential medical data or modify it and use it for their personal use so to avoid these situation, a concept of Cryptography to provide the security against unauthorized use of medical data.
Telemedicine may also improve healthcare access to areas where it was essentially not available in the past.

Telemedicine is a confluence of Communication Technology, Information Technology, Biomedical Engineering and Medical Science. Telemedicine is an effective solution for providing healthcare in the form of improved access and reduced cost to the rural patients. Telemedicine can enable ordinary doctors to perform extra-ordinary tasks.
Telemedicine allows for a virtual communication, using real–time audiovisual information transmitted over, between a patient and a physician at two different sites. Use of this technology has the potential to reduce the cost of providing healthcare.

To provide the privacy or security to the information the various encryption techniques have been developed. In this paper the two encryption techniques LFSR - based and chaos-based security technique for transformed EEG signals are discussed. Our techniques provide all QOS features like key sensitivity, encryption decryption time, network latency etc. those are essential for the quality of medical data in telemedicine system.

KEYWORDS:
Telemedicine, Transformation Signals, Secure EEG ,Chaos & LFSR (Linear feedback shift register)

I. INTRODUCTION

With the Advent of Information Technology in the medical world, various radiological modalities produce a variety of digital medical files most often datasets and images. The surge of digital radiological modalities in modern hospitals and research institutes around the world, has led to the creation of a vast amount of medical digital assets, like signals and images. These files as any digital asset should be protected from unwanted modification of their contents, especially as they contain vital medical information. Thus their protection and authentication seems of great importance and this need will rise along with the future standardization of exchange of data between hospitals or between patients and doctors[1].
Telemedicine enable patients to communicate through video conferencing, audio, images and data. The presence of a network has prompted new problems with security and privacy..
. The Telemedicine system consists of customized hardware and software at both the Patient and Specialist doctor ends with some of the Diagnostic Equipments like ECG, X-ray and pathology Microscope/Camera provided at the patient end. A Telemedicine system consists of simple computer with

ISSN: 2278 – 1323

communication systems, the medical images/signals and other information pertaining to the patients can be sent to the specialist doctors, either in advance or on a real time basis through the satellite link or WiFi system in the form of Digital Data Packets. These packets are received at the specialist centre, the images and the signal data along with the other information is reconstructed so that the specialist doctor can study the data, perform diagnosis, interact with the patient and suggest the appropriate treatment during a Video Conference with the patient end. Telemedicine facility thus enables the specialist doctor and the patient separated by thousands of kilometers to see visually and talk to each other. This enables the specialist doctor to assess the physical and psychological state of the patient and suggest treatment.

For future internet applications on wireless networks, besides source coding and channel coding techniques, cryptographic coding techniques for multimedia applications need to be developed.

Therefore in this paper, we proposed two encryption techniques, First is LFSR based security technique for Transformed EEG signals and second is chaos based security technique for Transformed EEG signals. Key is used for encrypting the data in cryptography. So we are generating the key based on the concept of Gold sequence generator. The Gold Sequence Generator is a well known pseudorandom sequence generator that generates the key with the help of pseudorandom numbers.

This gold sequence will be used as a key for encrypting the 16-channel data of EEG signal i.e. medical signal. Our proposed technique will increase the speed for encryption and also provide good security against unauthorized access.

II. BACKGROUND

PSEUDORANDOM SEQUENCE GENERATORS

(i) LFSR-based pseudorandom number Generator:

Linear feedback shift register (LFSR) is a shift register whose input bit is a linear function of its previous state. It is one of the most important technique that provide pseudorandom numbers. Feedback shift register sequences have been widely used as synchronization codes, masking or

Scrambling codes, and for white noise signals in communication systems.

We are using the XOR function with the single bit of feedback registers.

In short, an LFSR takes a series of bits from a long shift register, XORs them together to come up with a resultant bit, shifts the register along one bit, and then sticks the new bit back into the beginning of the register. 'Tapping' technique provides the highly secure random numbers.

If the positions of the bits (the "taps") are chosen carefully, this produces a maximal-length string of bits which is as damn near random as makes no odds to anyone other than mathematicians and cryptographers [4].

LFSR technique is highly supportable to all types of hardware. LFSR can produce sequences of large period and it can also be used for sequences with good statistical properties.

(ii) Chaos-based random number Generator:

Chaos-based cryptosystems are secure communication schemes designed for noisy channels. Chaos technique can provide high level of security due to the excellent unpredictability of chaotic sequence.

Chaos is a pseudo-random process produced in nonlinear dynamical systems. It is non-periodic in nature, non-convergent and extremely sensitive to the initial condition.

There exists relationship between the chaos and cryptography [7-8] such as Ergodicity and confusion, Sensitivity to initial condition and diffusion with a small change in the secret key or plain text, Mixing property and diffusion, Deterministic dynamics and deterministic pseudo-randomness, Structure complexity and Algorithm complexity.

There are two basic approaches to the design of chaos-based cryptosystems: analog and digital. The first one is generally based on chaos synchronization, and the associated chaotic systems are implemented in analog form. The second one is independent of chaos synchronization and the chaotic systems are completely implemented in digital form.

Recall that traditional cryptographic schemes mainly rely on complicated algebraic operations. Interestingly, chaotic systems exhibit attractive complex dynamics but exist in a relatively simple form. In this sense, it is feasible to employ chaos theory in cryptographic aspect. Over the past decades, the field of chaos-based cryptography has become more and more popular in the research literature.

One dimensional and two dimensional chaotic maps have been used for pseudorandom generation. The simplest class of chaotic dynamic system is one-dimensional chaotic map which is a difference equation of the form

$$x_{n+1} = f(x_n, \lambda), \qquad n = 0, 1, 2, 3, \ldots$$

where the state variable $\boldsymbol{x}$ and the system parameter $\boldsymbol{\lambda}$ are scalars, i.e., $x, \lambda \in \boldsymbol{R}$, and f is a mapping function defined in the real domain $\boldsymbol{R} \rightarrow \boldsymbol{R}$. As for an introductory purpose from here on, only one- and two-dimensional chaotic maps are briefly discussed.

ISSN: 2278 – 1323

One Dimensional chaotic maps those are widely used are tent map and logistic map. We are using logistic map in our proposed technique. logistic map which is originally proposed to describe population growth model [9]. The map is quadratic and thus nonlinear with the following expression: $x_{n+1} = bx_n(1-x_n)$,

Where ***b*** is the control parameter governing the chaotic behavior. To ensure ***xn*** in the range [0,1], parameter b has to be in the range [0,4]. Figure 1. shows the trajectory of the map with b = 3.999. Both the tent and the logistic maps exhibit a maximum at xn = ½. In the next section, the logistic map is explicitly chosen as a typical study case of chaotic behavior.

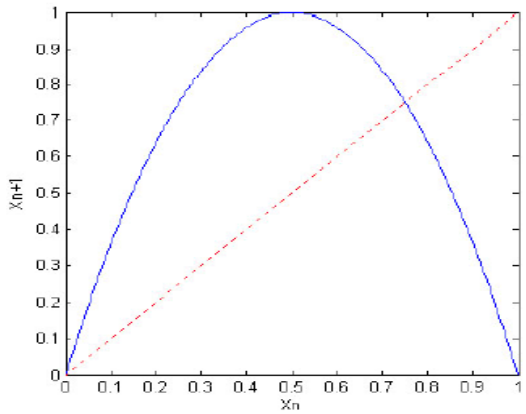

Fig1: The Acknowledgement mechanism works like a chain

TRANSFORMATION TECHNIQUE

(iii) Lifting Wavelet Transformation:

This framework was introduced by Sweldens and is known as the lifting scheme or simply lifting. Using the lifting scheme the end arrive at a universal discrete wavelet transform which yields only integer wavelet- and scaling coefficients instead of the usual floating point coefficients[6]. As mentioned before, a wavelet transform (or subband coding or multiresolution analysis) cam be perform using a filter bank. A simple one-stage filter bank is shown in figure 1 and it can be made using FIR filters. Although IIR filters can also be used, they have the disadvantage that their infinite response leads to infinite data expansion.

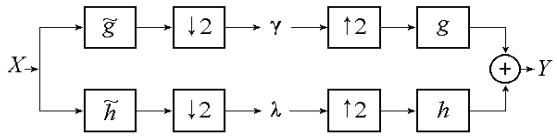

Figure 6.1: A one-stage filter bank for signal analysis and reconstruction.

III. PROPOSED TECHNIQUES

(i) LFSR-based Security Technique for Transformed EEG Signals:

This technique is carried out on 16-channel/reference electrodes of EEG signal. The two LFSR pseudorandom number generators with different parameter will be used to generate the gold sequence which is used as key for encryption/decryption process.

The basic idea of generating the gold sequence is that the random sequence generated by Generator1 and random sequence generated by Geneator 2 are EXORed together. After this gold sequence/number EXORed with the transform EEG signal to get the encrypted EEG signal. Transform EEG signal contain the approximate values of original signal on which we will apply encryption this may result in decreases both encryption and decryption time.

(ii)Chaos-based Security Technique for Transformed EEG signals:

This technique is carried out on 16-channel/reference Electrodes of EEG signal. The two chaos pseudorandom number generators with different parameter will be used to generate the gold sequence which is used as key for encryption/decryption process.

The basic idea of generating the gold sequence is that the random sequence generated by Generator1 and random sequence generated by Generator 2 are EXORed together. After this gold sequence/number EXORed with the transform EEG signal to get the encrypted EEG signal. Transform EEG signal contain the approximate values of original signal on which we will apply encryption this may result in decreases both encryption and decryption time. But still chaos-based technique in transform domain will required the more time than LFSR-based technique due to computational complexity.

ISSN: 2278 – 1323

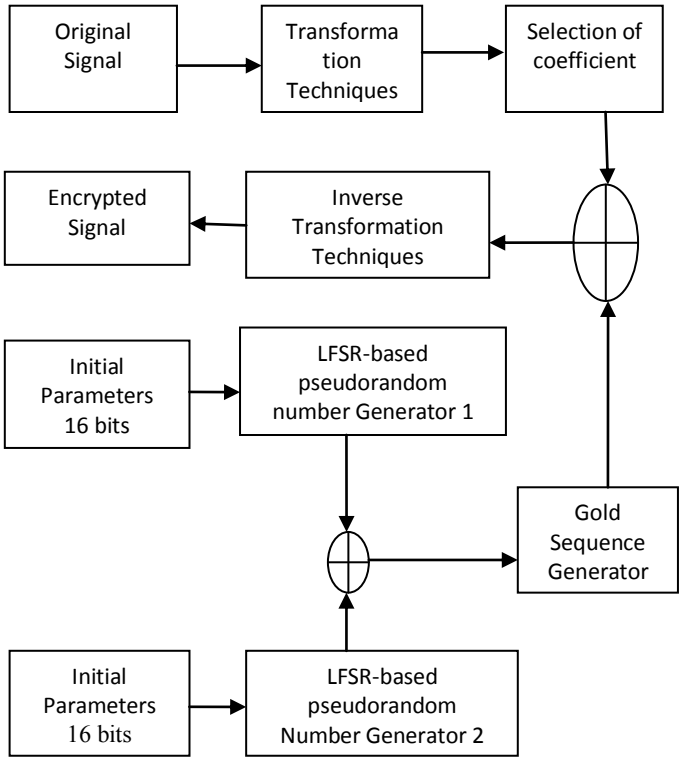

Fig2. Graphical View of LFSR-based technique for Transformed EEG signals

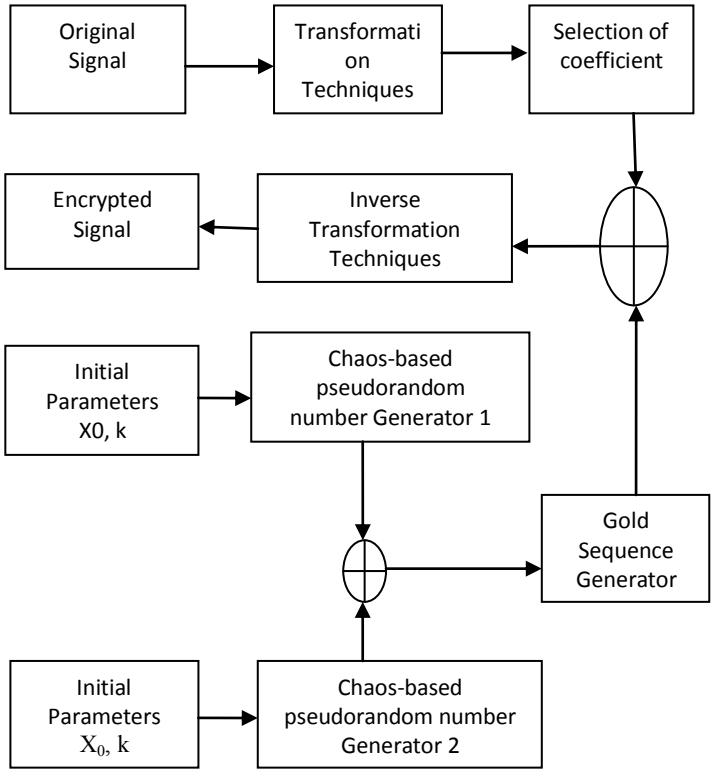

Fig3: Graphical view of Chaos based technique for Transformed EEG signals

IV. PERFORMANCE MEASURES

(i) Time Analysis (Encryption-Decryption Time)

Encryption time is required to encrypt the EEG signal at sender end and decryption time is required to decrypt the EEG signal at the receiving end.

(ii)Key Sensitivity

An efficient encryption algorithm should be key sensitive. Key sensitivity means a small change in secret key during decryption process results into completely different decrypted image.

(iii)MSE(Mean Squared Error)

MSE measures the average of the squares of the 'errors'. The error is the amount by which the valued implied by the estimator differs from the quantity to be estimated.

(iv)PSNR(Peak signal to noise ratio)

It is the ratio between the maximum possible power of a signal and the power of corrupting noise that effects on the value of its representation.Signal is the original data & the noise is the error. PSNR is expressed in terms of decibel scale. Values over 40db in PSNR are acceptable in terms of degradation.

(v) NIST TEST

NIST of the United states is statistical package [12] used for testing the randomness of binary sequences produced by either hardware or software based pseudorandom number generators. The NIST 800-22 test suite consists of a set of 16 tests focusing on a variety of different types of non-randomness that could exist in a sequence. Some tests may be decomposed into a variety of sub-tests. Therefore total 189 items exist in the test suite. For each type of test, after complex statistical analysis provided by the NIST 800-22 suite was performed, a percentage called P-value can be derived from the test data.
The test whose P-value falls in the confidence interval succeed[12].

ISSN: 2278 – 1323

V.CONCLUSION / FUTURE WORK

In this paper, we are proposing two techniques one as a LFSR based and other as chaos based for providing security for medical signals i.e. EEG data. If we send these data to other places then nobody can access or modify these data.

We have studied a lot about the telemedicine networks and all other techniques those have been developed. These existing techniques are not good enough in the area of speed and security. So, we are trying to simulate our proposed techniques that can provide higher security and also good in encryption decryption speed .We will analyze them on the basis of quality of service parameters and also analyze on the basis of NIST test to find out the randomness of our chaotic sequence bits.

Telemedicine and Cryptography is an emerging field, which is capturing the imagination of all the researchers worldwide. Thus the scope of enhancements and improvements is enormous. We will try to simulate these techniques via using some simulator like MATLAB and analyze the performance on the basis of quality of service parameters.

For these techniques we can create an interactive GUI so that they can be used for commercial purpose. We can use other 1D and 2D chaotic equation[5] for generating the pseudorandom numbers for better results.

VI.REFERENCES

[1] K.V.R. Ravi, R. Palaniappan, C. Eswaran and S. Phon-Amnuaisuk. "Data encryption using event-related brain signals" International Conference on Computational Intelligence and Multimedia Applications 2007.

[2] http://www.garykessler.net/library/crypto.html.

[3]http://en.wikipedia.org/wiki/Symmetric-key_algorithm.

[4]http://www.cs.cornell.edu/courses/cs513/2007fa/TL04.asymmetric.html.

[5] Chin-Feng Lin and Cheng-Hsing Chung. "A Fast Chaos-based Visual Encryption Mechanism for Integrated ECG/EEG Medical Signals with Transmission Error". 12th WSEAS International Conference on SYSTEMS, Heraklion, Greece, July 22-24, 2008.

[6] Lala krikor, sami baba at al , "Image Encryption Using DCT and Stream Cipher", European Journal of Scientific Research ISSN 1450-216X Vol.32 No.1 (2009), pp.47-57.

[7] Gr¨undlingh, W. & van Vuuren, J. H. (Using Genetic Algorithms to Break a Simple Cryptographic Cipher. Retrieved March 31, 2003 from http://dip.sun.ac.za/˜vuuren/abstracts/abstr genetic.htm

[8] R. Brown, L. O. Chua, Clarifying chaos: Examples and counterexamples, Int. J. Bifurcation and Chaos 6 (2) (1996) 219–249.

[9] Ismet Ozturk, Ibrahim Sogukpinar, "Analysis and Comparison of Image Encryption Algorithms", World Academy of Science, Engineering and Technology 3 2005.

[10]http://en.wikipedia.org/wiki/Linear_feedback_shift_register.

[11] G. ´Alvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis of a chaotic secure communication system, Phys. Lett. A 306 (4) (2003) 200–205.

[12]Rashidah Kadir, Mohd Aizaini Maarof,"A Comparative Statistical Analysis of Pseudorandom Bit Sequences", 2009 Fifth International Conference on Information Assurance and Security.

ISSN: 2278 – 1323