International Journal of Power Control Signal and Computation (IJPCSC)
Vol. 5. No.1. pp.23-27,Jan-March 2013 ISSN: 0976-268X
www.ijcns.com

# A Novel Approach For Data Encryption Using EEG, SPIHT and Genetic Algorithm For Secured Applications

**G. Lokeshwari, Dr.S. Udaya & G.Aparna**
**gandrakoti@yahoo.com, Kumar uksusarla@gmail.com & G.Aparnagiraaparna@gmail.com**

**Abstract**

**In today's computer world secured digital images are vulnerable to unauthorized access while in storage and during transmission over a network. Streaming digital images also requires high network bandwidth for transmission. In this paper we propose a new approach for data security using the concept of genetic algorithm and EEG with pseudo random binary sequence to encrypt and decrypt the data. To effectively utilize the bandwidth of the network image compression algorithm SPIHT is employed. The scope of this approach provides high data security and feasibility for practical implementation.**

**KEYWORDS: Image compression, image encryption, data encryption , SPIHT, EEG, genetic algorithm, pseudo random binary sequence, cross over operator.**

## I. INTRODUCTION

In present day situations, network users demand audio, images and video along with the text. This necessity has become the convergence of computers, networks, communications, and multimedia applications. The information revolution is projecting a new area where medical aspects will combine the functions of data encryption and confidentiality [1].The presence of a network has prompted new problems with security and privacy. The main requirement in order to communicate with images and video is a secured and reliable means. Present situation demands highly secured details of an individual. In recent developments network security and data encryption have become vital and high profile issues [2]. 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 [8].

In this paper we propose a new approach for encrypting real time data transmission. Firstly pseudo random sequence is generated using non-linear forward feedback shift register (NLFFSR). The NLFFSR is a mechanism for generating extremely well pseudo random binary sequence, that can be used as a key [3]. Secondly this pseudo random sequence is used along with cross over operator for encrypting the data. For key generation logic EEG features are extracted compressed using SPIHT for effective utilization of bandwidth. The obtained compressed details are given as input for pseudo random sequence generator [2].

### 1.1 Genetic Algorithm

The genetic algorithm is employed for providing optimization solution. This is a search algorithm based on the mechanics of natural selection and natural genetics. The genetic algorithm belongs to the family of evolutionary algorithms, along with genetic programming, evolution strategies and evolutionary programming [4]. Evolutionary algorithms can be considered as a broad cast of stochastic optimization techniques. An evolutionary algorithm maintains a population of candidate's solutions for the problem at hand. The population is then evolved by the iterative application of a set of stochastic operators. The set of operators usually consists of mutation, recombination, and selection or something very similar.

### 1.2 SPIHT

Set Partitioning in Hierarchical Trees (SPIHT) algorithm [8] displays exceptional characteristics over several properties all at once including steps that can be summarized as follows:
*Good image quality with a high peak signal to noise ratio (PSNR).
*Fast coding and decoding
* Fully progressive bit stream
*Can be used for loss less compression.
*May be combined with error protection
*Ability to quote for exact bit rate or PSNR.

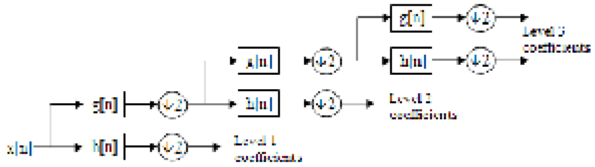

**Figure 1: 3- level decomposition of the coefficients.**

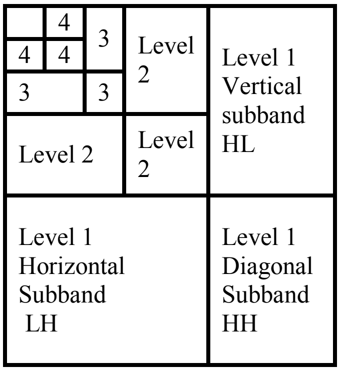
4
4
4
3
3
3
Level 2
Level 1 Vertical subband HL
Level 2
Level 2
Level 1 Horizontal Subband LH
Level 1 Diagonal Subband HH

**Figure 2 Levels of the decomposition in SPIHT**

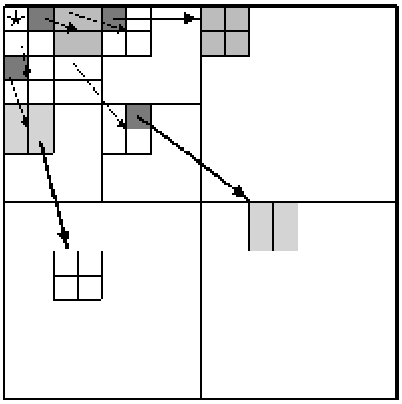

**Figure. 3.The process of compression**

Figure 1 represents the 3 level decomposition of the coefficients using SPIHT algorithm. Figure 2 represents the 2 levels of decomposition in SPIHT. Figure 3 indicates the process of compression involved respectively.

### 1.3 EEG FEATURES EXTRACTION

Electroencephalography deals with the recording and study of electrical activity of the brain. By means of electrodes attached to the skull of a patient, the brain waves can be picked up and recorded. the brain waves are the summation of neural depolarization’s in the brain due to stimuli from the senses as well as from the thought process. On the surface of the brain, these voltages are about 10mV. Due to propagation through skull bone, they are attenuated to levels from 1 to 100 micro volts which are picked up by EEG electrodes. They are in frequency range 0.5 to 3000Hz. These potentials vary with respect to position of the electrode on the surface of skull. Therefore during recording, the electrodes are placed around the frontal, parietal, temporal and occipital lobes of the brain.

Electroencephalogram is the record of the brain waves by an electroencephalograph. Brains waves represent a summation of the action potentials of neurons in the brain. Electrical patterns obtained on the surface of the skull are result of the graded potentials on the dendrites of neurons in the cerebral cortex and other parts of the brain. Graded potentials are variations around the average value of the resting potential. Electric charges are transferred between one nerve fiber and the other through a dendrite of a post synaptic neuron during the release of acetylcholine. A large number of these potentials are then summed to produce EEG rhythms [7]. It is difficult to record the discharge of a single neuron or single nerve fiber from the surface of the head. Large portions of nervous tissue must emit electrical current simultaneously to handle this difficulty. The electrical current emits in two ways firstly tremendous number of nerve fibers can discharge in synchronous with each other there by generating very strong electrical currents. Secondly, large number of neurons can partially discharge, though not emit action potentials. Furthermore, these partially discharge neurons can give periods of current flow which is undulate with changing degrees of excitability of the neurons.

The surface of the cerebral cortex is composed almost entirely of a mat of dendrites extending to the surface from neuron cells in the lower layers of the cortex. When signals impinge on these dendrites, the dendrites become partially discharged. This partially discharged state makes the neurons of the cortex highly excitable. One of the important sources of the signal to excite the other dendrite layer of the cerebral cortex is the ascending reticular activating system.

## II. WAVE PATTERNS

| Type | Frequency(Hz) | Location | Normally | Pathologically |
|---|---|---|---|---|
| Delta | Up to 4 | frontally in adults, posterior in children; high amplitude waves | Adults slow wave sleep in babies Has been found during some continuous attention tasks | • sub cortical lesions<br>• diffuse lesions<br>• metabolic encephalopathy hydrocephalus |

| Type | Frequency(Hz) | Location | Normally | Pathologically |
|---|---|---|---|---|
| | | | | deep midline lesions |
| Theta | 4-8 | Found in locations not related to task at hand | • young children<br>• drowsiness or arousal in older children and adults<br>• idling<br>• Associated with inhibition of elicited responses (has been found to spike in situations where a person is actively trying to repress a response or action) | • focal sub cortical lesions<br>• metabolic encephalopathy<br>• deep midline disorders some instances of hydrocephalus |
| Alpha | 8-13 | posterior regions of head, both sides, higher in amplitude on dominant side. Central sites (c3-c4) at rest | • young children<br>• relaxed/reflecting<br>• closing the eyes<br>• Also associated with inhibition control, seemingly with the purpose of timing inhibitory activity in different locations across the brain. Drowsiness or arousal in older children and adults<br>• idling | Coma |
| | | | • Associated with inhibition of elicited responses (has been found to spike in situations where a person is actively trying to repress a response or action). | |
| **Beta** | >13 – 30 | both sides, symmetrical distribution, most evident frontally; low amplitude waves | • alert/working<br>• active, busy or anxious thinking, active concentration | Benzodiazepines |
| Gamma | 30 – 100+ | Somato sensory cortex | • Displays during cross-modal sensory processing (perception that combines two different senses, such as sound and sight)<br>• Also is shown during short term memory matching of recognized objects, sounds, or tactile sensations | • A decrease in gamma band activity may be associated with cognitive decline, especially when related the theta band; however, this has not been proven for use as a clinical diagnostic measurement yet |
| **Mu** | 8 – 13 | Sensor motor cortex | • Shows rest state motor | • Mu suppression could be |

| Type | Frequency(Hz) | Location | Normally | Pathologically |
|---|---|---|---|---|
| | | | neurons. | indicative for motor mirror neurons working, and deficits in Mu suppression, and thus in mirror neurons, might play a role in autism |

## III. PROPOSED METHOD

The proposed method block diagram is shown below. It consists of key generation logic, encryption and decryption modules, which are explained in following subsections.

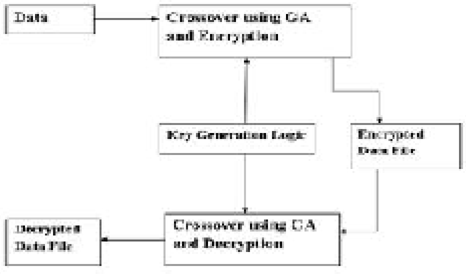
Data
Crossover using GA and Encryption
Key Generation Logic
Encrypted Data File
Decrypted Data File
Crossover using GA and Decryption

**Figure 7 Block Diagram of Proposed Method.**

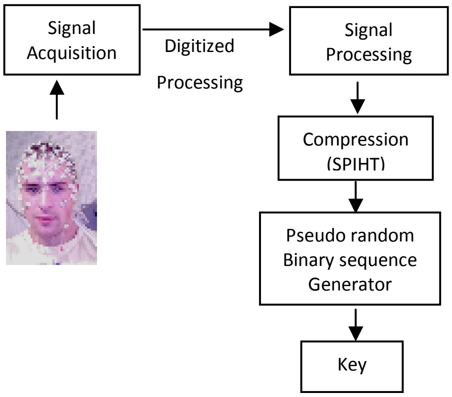

**Figure 4 The model of key generation logic.**

### 3.1 Pseudorandom Binary Sequence Generator

Figure 9 shows a general model of PRBSG Pseudo random Binary Sequence Generator [3]. It is a non linear forward feedback shift register (NLFFSR) with a feedback function 'f' and non linear function 'g'.

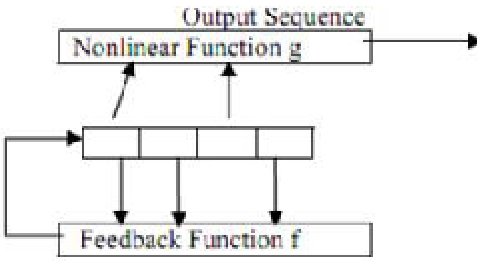

**Figure 5. A General Model Of 4 bit NLFFSR**

When register is loaded with a non-zero value, a pseudo random sequence with very good randomness and statistical properties is generated. The only signal required for the operation of this module is clock pulse. The balance, run and correlation properties of the sequence generated make it more useful for generating the private key. When the register is loaded with any given initial value (except zero which will generate a pseudo random binary sequence of all zeros), then pseudo binary sequence is generated with very good randomness and statistical properties.

### 3.2 Crossover Operator

Crossover in simple words is a process in which two strings are mixed such that they match their desirable qualities in a random fashion [10]. Figure 10 illustrates the crossover operation and its procedure. Crossover operator proceeds in three steps as given below:

1. Two new strings are selected.
2. A random location from strings is selected.
3. The portions of strings on right side are swapped together.

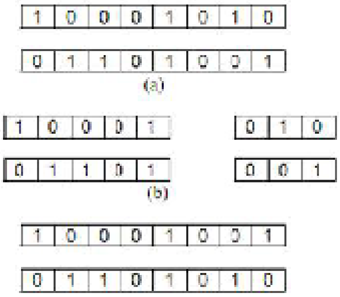

**Figure 6: Illustration of crossover operator**

### 3.3 Key Generation Process

The key generation algorithm used here produces a very strong key which is very difficult to guess even with exhaustive search. The process of key generation is as given below:

1. Extract the main features of EEG wave.
3. To reduce the bandwidth compress the EEG wave using SPIHT algorithm.
4. Pass the non zero output of this block to the pseudo random binary sequence generator.
4. The output of PRBSG is the key kn.
5. Take mod 8 of the key generated to get a decimal value ranging from 0 to 7.

### 3.4 The Encryption Process

The encryption process emulates the operation of key generator and crossover operator. The encryption process comprises of following steps:

1. Generate the key using the key generator logic as Kn.
2. Take mod 8 of the key generated to get decimal value ranging from 0 to 7.
3. Kn =mod (Kn, 8)
4. Initialize i=0
5. Take two consecutive bytes of the data file as A1 and A2
6. Crossover the two consecutive bytes of the data file as B1 and B 2 Using the number Ki.
7. Encrypt data as C1 and C2 .This is done as follows:

Xi=Ki XOR Ki << 4
Xi+1=ki+1 XOR ki+1 <<4
C1=Bi XOR X1
C2=B2 XOR Xi+1
And i=i+2
Repeat steps 4 to 6 until end of the file.

### 3.5 The Decryption Process

The steps for decryption are just reversal of the encryption . First extract the features from sensory output, pass the nonzero data to PRBS, the output of the PRBS is the key. Apply the process using crossover operator to decrypt the data.

## IV. PERFORMANCE ANALYSIS

It should be checked that, if a data is encrypted by the proposed technique whether it can be easily decrypted or not. Since there are M combinations to encrypt 2 consecutive data bytes, thus the number of possible encryption results is M (N/2), where N is the total number of bytes in data to be encrypted and M is the length of one data byte.

## V. CONCLUSION

In this paper a new approach for data security is proposed. The concept of EEG, genetic algorithms and pseudorandom binary sequence are applied. This methodology of scurrying the confidential data is highly safe and reliable. In the future work, we plan to implement a system implementing this methodology and provide security to a level of highly confidential and secret data in defense and other institutions.

## ACKNOWLEDGMENT

We thank our guide Dr. S. Udaya Kumar and Dean Research and Development of our college for their support. And also would like to thank all the anonymous of this constructive comments.

## REFERENCES

[1] Douglas, R. Stinson, "Cryptography - Theory and Practice",CRC Press, 1995.

[2] Menzes A. J., Paul, C., Van Dorschot, V., anstone, S. A.,
"Handbook of Applied Cryptography", CRS press 5th Printing; 2001.

[3] Ahmad A., Al-Musharafi M. J., Al-Busaidi S., Al-Naamany A.and Jervase J. A., "An NLFSR Based Sequence Generation for Stream Ciphers", Proceedings of International Conference on Sequences and their Applications, pp. 11-12, 2001.

[4] Tragha A., Omary F., and A. Kriouile, "Genetic Algorithms Inspired Cryptography" A.M.S.E Association for the Advancement of Modeling & Simulation Techniques in Enterprises, Series D: Computer Science and Statistics, 2005.

[5] Tragha A., Omary F., Mouloudi A.,"ICIGA: Improved
Cryptography Inspired by Genetic Algorithms", Proceedings of the International Conference on Hybrid Information Technology (ICHIT'06), pp. 335-341, 2006.

[6] A New Approach for Data Encryption using Genetic Algorithms and Brain Mu Waves by Gove Nitinkumar Rajendra, Bedi Rajneesh kaur International Journal Of Scientific And Engineering Research Volume 2, Issue 5, May-2011 ISSN 2229-5518

[7]Medline Plus A service of U.S National Library of Medicine
And National Institutes of Health

[8] Digital Image Processing by Jayaraman, Esakkirajan and Veerakumar Tata Mc Graw Hill.

[9] Bio-medical Instrumentation by Dr. M. Arumugam Anuradha Publications.

[10] Goldberg D.E., "Genetic algorithms in search optimization & Machine learning", Addison-Wesley,1989.