# Chaos-based Encryption of Biomedical EEG Signals using Random Quantization Technique

Musheer Ahmad
Department of Computer Engineering,
JMI, New Delhi-110025, INDIA

Shahab Saquib Sohail
Department of Computer Science,
AMU, Aligarh-202002, INDIA

Omar Farooq
Department of Electronics Engineering,
AMU, Aligarh-202002, INDIA

Anoop L Vyas
Instrument Design Development Centre,
IIT, New Delhi-110016, INDIA

Sekharjit Datta
Department of Electronic and Electrical Engg.,
Loughborough University, Loughborough, UK

David Mulvaney
Department of Electronic and Electrical Engg.,
Loughborough University, Loughborough, UK

***Abstract*—As electroencephalography (EEG) signals contain sensitive personal health information, it is generally a legal requirement to prevent their unauthorized access. For example, the HIPAA in the US requires that access to personal health information is limited to properly authorized individuals. In this paper, a chaos-based encryption method is proposed to secure patients' EEG data before transmission over an insecure channel. The proposed method employs a multiplexer to dynamically select between two randomly quantized bitstreams for secure key generation. This method is simulated to encrypt the EEG datasets and the statistical properties such as signal distribution, auto and cross-correlation, power spectral density and the residual deviation of the encrypted/original EEG signals are evaluated. The experimental results verify that the proposed method has high security and is suitable for the protection of sensitive EEG data.**

***Keywords-lorenz chaos system; EEG signals; encryption; security; random quantization.***

## I. INTRODUCTION

With the advancement of wired and wireless telecommunication technologies, both m-healthcare and e-healthcare have become integral components of biomedical science. Telemedicine is now poised to take an important role in healthcare; in fact, according to a study by N. Lasierra *et al.* [1], 98% of patients using a telemedicine solution introduced in Spain were satisfied with the system, while 75% also preferred it to a conventional approach. The biomedical EEG signals have been used since the 1950s to monitor patients with coma, dementia and long-term memory problems. It is also used to assess brain death to legally prove that a patient on life-support equipment will not recover. The EEG data are private to the patient, but when obtained in a hospital they are routinely transmitted using an insecure channel prior to diagnosis. When the same data are obtained for telemedicine purposes, it becomes legally mandatory to protect the biomedical health information of patient from unauthorized access before it can be transmitted over the insecure channel. It is equally important that the protection approach taken does not modify the patients' data in any way that would influence any later diagnoses. Further, the protection must be sufficiently secure to give reasonable defense against unauthorized attempts to gain access. Any insecure acquisition and diagnosis system is likely to violate a country's regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the US [2]. The consequences of illegal access or modification of information are many, particularly perhaps in cases relating to insurance claims or when considering brain death. To adhere to these regulations, there is a profound need to implement a strong encryption method to protect the patient's health information prior to transmission.

In recent years, there has been substantial progress in the application of chaos theory to cryptography. A chaotic system has several cryptographically desirable features that make it ideal for secure communication; the most important being sensitivity to initial conditions, non-periodicity and randomness. Moreover, due to the similarity of the characteristics of the chaotic and cryptography methods, they have been shown to work well in harmony in delivering strong chaos-based security solutions [4,5] and they have been used to protect images, speech, voice and video signals [6-11]. In this paper, an encryption method based on a Lorenz chaotic map is proposed for the protection of patients' EEG data. To enhance the security of the proposed method, the discrete system variables of the Lorenz map are quantized randomly and two cryptographic Boolean functions are evaluated using the quantized Boolean variables. In addition, the key generation process is made random by employing a multiplexer that unpredictably switches between values that have been obtained using Boolean functions. The whole process generates highly random keys, which are employed to encrypt the patient's EEG signals. The simulation results verify that the proposed scheme provides high security for patients' EEG data, minimizing the possibility of unauthorized access.

978-1-4244-9352-4/11/$26.00 ©2011 IEEE

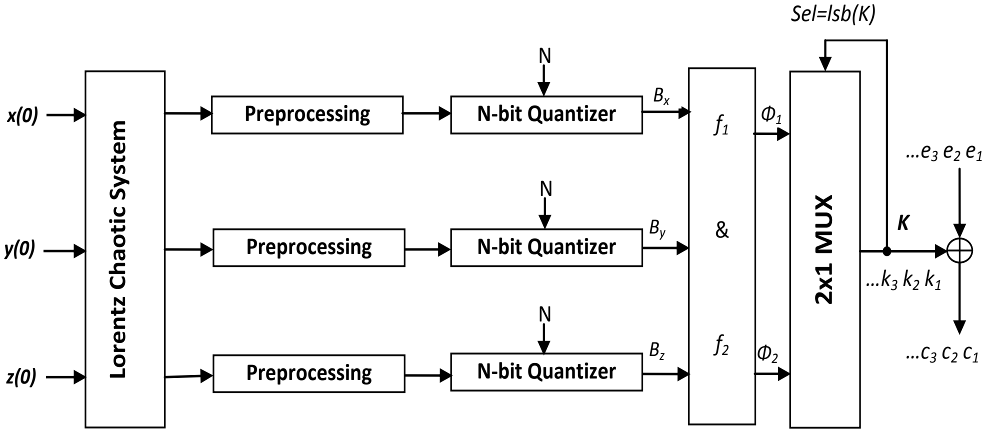

Figure 1. Schematic diagram of the proposed chaos-based EEG data encryption method

## II. PROPOSED CHAOS BASED EEG SIGNALS ENCRYPTION METHOD

A schematic diagram of the new method is shown in Figure 1. The three dimensional Lorenz system is used as a basis for the proposed scheme. Its governing equation is:

$$\begin{aligned} \frac{dx}{dt} &= \sigma(y-x) \\ \frac{dy}{dt} &= rx - xz - y \\ \frac{dz}{dt} &= xy - bz \end{aligned} \qquad (1)$$

Where $x$, $y$, and $z$ are real valued state variables of the Lorenz system, $\sigma$, $r$, $b$ are positive control parameters of the system. The parameter $\sigma$ is the Prandtl number and $r$ is the Rayleigh number. For $\sigma = 10$, $b = 8/3$, the dynamic orbits of Lorenz system are in chaotic state for $r > 24.74$. Due to the complex dynamic orbit of the Lorenz system, the chaotic sequences generated are more unpredictable than sequences obtained from one-dimensional chaotic systems. Moreover, a single iteration of the Lorenz system produces three distinct uncorrelated real-valued sequences, each with random-like and unpredictable characteristics. The Lorenz chaotic system makes use of numerical integration to obtain real-valued chaotic sequences and a Runge-Kutta-4 method can be applied to solve the Lorenz 3D differential equations. Following each iteration of the Runge-Kutta-4 method, preprocessing of the real-valued state variables obtained is carried out and includes the following steps

1. For each variable, right shift the radix point by a small number of places and extract the decimal part to provide a new member of the pseudo-random sequence. This can be achieved by following formulation

$$\begin{aligned} dx &= 10^6(x) - (floor\ [10^6\,(x)]\ ) \\ dy &= 10^6(y) - (floor\ [10^6\,(y)]\ ) \\ dz &= 10^6(z) - (floor\ [10^6\,(z)]\ ) \end{aligned} \qquad (2)$$

The pseudo-random values of $dx$, $dy$ and $dz$ will now lie in (0, 1).

2. The pseudorandom fractional values $dx$, $dy$ and $dz$ are multiplied by a factor of $10^{14}$ to obtain the corresponding pseudo-random integer numbers $ix$, $iy$ and $iz$ respectively.

$$\begin{aligned} ix &= floor\ [10^{14}(dx)] \\ iy &= floor\ [10^{14}(dy)] \\ iz &= floor\ [10^{14}(dz)] \end{aligned} \qquad (3)$$

3. These pseudo-random integer numbers are quantized with randomly generated quantization parameter $N$ during each iteration, to obtain the pseudo-random binary sequences $Bx$, $By$ and $Bz$ each of $N$-bits corresponding to real-valued state variables $x$, $y$ and $z$ of Lorenz system.

$$\begin{aligned} Bx &= DectoBin\{(ix)mod(L)\} \\ By &= DectoBin\{(iy)mod(L)\} \\ Bz &= DectoBin\{(iz)mod(L)\} \end{aligned} \qquad (4)$$

Where $L = 2^N$ denotes the number of quantization levels in the current iteration. The value of $N$ will vary from 1 to10 and can be dynamically evaluated from the pseudo-random fraction values $x$, $y$ and $z$ obtained using the following equation.

$$\begin{aligned} \xi &= floor[10^8(x)] + ceil[10^6(y)] + round[10^{11}(z)] \\ N &= (\xi)mod(10) + 1 \end{aligned} \qquad (5)$$

The outputs of the random quantization process are three blocks $Bx$, $By$ and $Bz$ of length $N$-bits. In each iteration, new value of $N$ is derived, thereby adding randomness to the encryption process which substantially improves the security and robustness of encryption method. The blocks of pseudo-random binary streams $Bx$, $By$ and $Bz$ are used to evaluate $\Phi_1$ and $\Phi_2$ using two balanced Boolean functions $f_1()$ and $f_2()$ as shown below

$$\Phi_1 = f_1(B_x,B_y,B_z) = B_y \oplus B_z \oplus (B_y.B_z) \oplus (B_x.B_z) \qquad (6a)$$

$$\Phi_2 = f_2(B_x,B_y,B_z) = B_x \oplus B_z \oplus (B_x.B_z) \oplus (B_y.B_z) \qquad (6b)$$

Where '⊕' and '.' denote the logical XOR and AND operations. The Boolean functions $f_1()$ and $f_2()$ provide input streams $\Phi_1$ and $\Phi_2$ to '2 to 1' multiplexer that generates member stream of final encryption keystream ***K***. The least significant bit of the stream output from the multiplexer is taken as select line *Sel*. Initially, *Sel* is set to 0; when *Sel* is 0, the output of multiplexer is $\Phi_1$ otherwise the output is $\Phi_2$. This means that on every iteration, the encryption system grows the size of the keystream ***K*** by *N* number of bits. The autocorrelation function of the keystream so obtained is shown in Figure 2, and the similarity of its shape to an impulse function indicates the high degree of randomness of the proposed generator. Let the generated keystream be denoted by $\boldsymbol{K} = k_n\ldots\ldots\ldots k_3\, k_2\, k_1$, the encrypted bit sequence ***C*** is given by

$$\boldsymbol{C(i)} = (k_n\ldots\ldots\ldots k_3\, k_2\, k_1) \oplus (e_n\ldots\ldots\ldots e_3\, e_2\, e_1) \qquad (7)$$

Where $\boldsymbol{E(i)} = e_n\ldots\ldots\ldots e_3\, e_2\, e_1$ is the original EEG signal to be encrypted and $\boldsymbol{C(i)} = c_n\ldots\ldots\ldots c_3\, c_2\, c_1$ is the encrypted EEG signal obtained using the proposed encryption method.

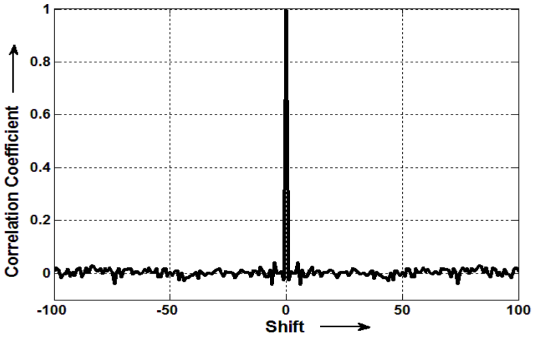

Figure 2. Auto-correlation of keystream

## III. Experimental Results

For the purposes of experimentation and simulation, the proposed encryption method is applied to the Bonn University EEG datasets [12,13]. The initial conditions and the control parameters adopted for the experiments are: $\sigma = 10$, $r = 28$, $b = 8/3$, $x(0) = 13.3604$, $y(0) = 7.2052$, $z(0) = 21.5026$, $h = 0.001$. To evaluate the performance of the proposed encryption method, randomness, signals distribution, correlation, power spectral density (PSD) and percentage residual deviation (PRD) analyses of the original and the corresponding encrypted EEG signals are performed in this section.

### A. Randomness Analysis

To assess the randomness of the bit sequence generated, statistical analysis of the output of the proposed random sequence was carried out using the National Institute of Standards and Technology (NIST) [14] test package. In the tests, the significance level, α, is set to 0.01, as required for cryptographic applications [14] and a p-value is produced that corresponds to the probability that the sequence under test is random. A test is considered as passed if the p-value obtained is greater than α. An α value of 0.01 indicates that one would expect 1 in every 100 sequences to be rejected and a p-value no less than 0.01 indicates that the sequence is considered to be random with a confidence of 99%. Statistical tests were carried out on sequences containing 50,000 consecutive bits and the results of the statistical testing are shown in Table 1. It can be seen that all but one of the tests was passed. It is important to note that good performance of the proposed approach in these tests is no guarantee of secure communications, but only an indicator of what can be expected in practice.

### B. EEG Signals Analysis

The data plots of original EEG signal of channel-1 and the corresponding encrypted EEG signals are shown in Figures 3 and 4, respectively. Subjectively, the encrypted EEG signal appears similar to a noise signal indicating its random nature.

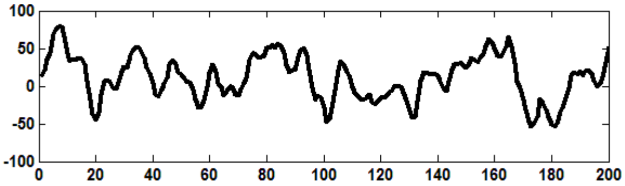

**Figure 3. Original EEG Signal**

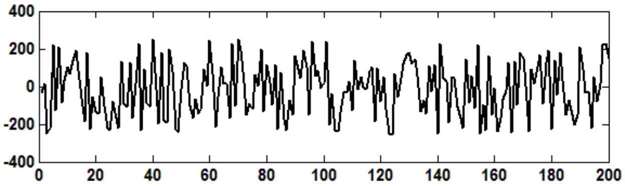

**Figure 4. Encrypted EEG signal**

TABLE I. NIST Randomness of Bits Generated From Proposed Method

| # | Test Type | p-value | Result |
|---|---|---|---|
| 1 | *Frequency Test* | 0.935841 | Success |
| 2 | *Block Frequency Test* | 0.005592 | Failure |
| 3 | *Cusum Forward Test* | 0.710813 | Success |
| 4 | *Cusum Reverse Test* | 0.785929 | Success |
| 5 | *Runs Test* | 0.622786 | Success |
| 6 | *Longest Runs Test* | 0.063048 | Success |
| 7 | *Rank Test* | 0.778634 | Success |
| 8 | *FFT Test* | 0.124046 | Success |
| 9 | *Linear Complexity Test* | 0.432161 | Success |
| 10 | *Serial Test* | 0.380394 | Success |
| 11 | *Approx Entropy Test* | 0.647816 | Success |
| 12 | *Overlapping Template Test* | 0.676712 | Success |

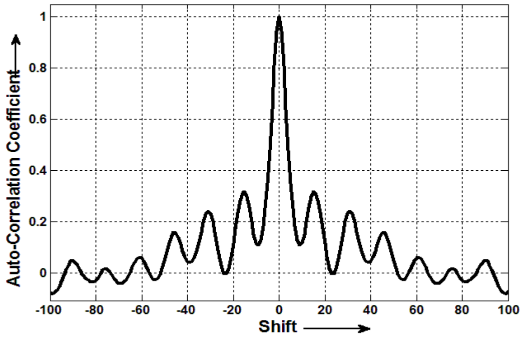

Figure 5. Auto-correlation of original EEG signal

### C. *Correlation Analysis*

The autocorrelation of a signal is a measure of similarity of the signal with its delayed version. The autocorrelation functions of the original and encrypted EEG signals are shown in Figures 5 and 6, respectively. For the original EEG signal, its autocorrelation shows considerable periodic content, whereas the autocorrelation function of the encrypted signal has small values other than at zero shift, demonstrating little correlation between values and a high degree of randomness.

The cross-correlation between the original and the encrypted EEG signals is shown in Figure 7. As the largest value in the cross-correlation is less than 0.05, the encrypted signal has no significant similarity with the original signal, which is an essential requirement of encryption.

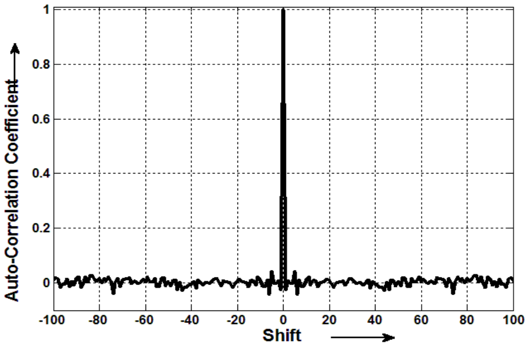

Figure 6. Auto-correlation of encrypted EEG signal

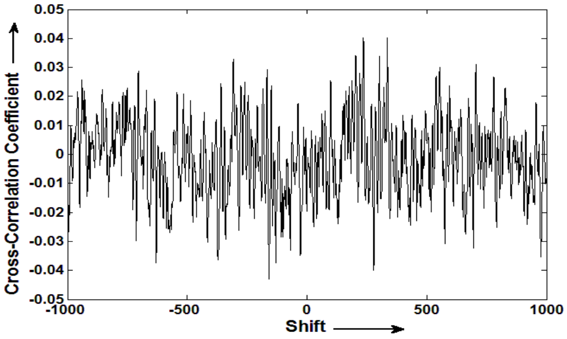

Figure 7. Cross-correlation of original and encrypted EEG signal

### D. *Power Spectral Density Analysis*

Power spectral density function (PSD) indicates the dominant frequencies present in the signal. For good quality encryption, the encrypted signal should have a similar content at all frequencies, somewhat akin to band-limited white noise. Figure 8 shows the PSD plots. For original signal which has dominant frequencies in the range of 0-20 Hz but less energy is present on the higher frequencies. The encrypted signal has a characteristic similar to white noise and has a flat PSD plot.

### E. *Percentage Residual Deviation Analysis*

To determine the extent to which the encrypted signal *C(i)* is different from the original signal *E(i)*, the percentage residual deviation (PRD) parameter is evaluated. It provides the measure of dissimilarity of original and encrypted EEG signals and is defined in Eqn. (8). The PRD values for the original and encrypted EEGs of first twenty channels EEG datasets of database are listed in Table II. Its values come out to be 0.0 for the original and decrypted EEG signals.

$$\rho = 100 \times \sqrt{\frac{\sum_{i=1}^{n}[E(i)-C(i)]^2}{\sum_{i=1}^{n}E^2(i)}} \qquad (8)$$

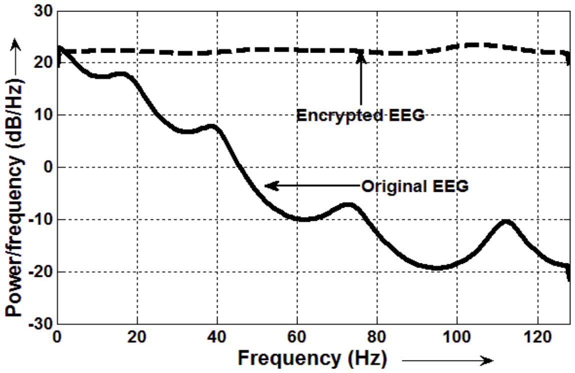

Figure 8. Power spectral density of EEG signals

TABLE II. PRD VALUES FOR DIFFERENT CHANNELS OF EEG SIGNALS

| EEG Dataset | PRD value | EEG Dataset | PRD value |
|---|---|---|---|
| Z001 | 360.919 | Z011 | 378.476 |
| Z002 | 229.760 | Z012 | 368.830 |
| Z003 | 321.005 | Z013 | 240.665 |
| Z004 | 330.502 | Z014 | 360.888 |
| Z005 | 323.183 | Z015 | 277.052 |
| Z006 | 300.661 | Z016 | 330.579 |
| Z007 | 325.612 | Z017 | 255.629 |
| Z008 | 464.484 | Z018 | 289.861 |
| Z009 | 242.282 | Z019 | 248.413 |
| Z010 | 305.705 | Z020 | 290.928 |

## IV. CONCLUSION

To provide suitable conditions for diagnosis in e-healthcare and m-healthcare environments, it is often mandatory to conceal patients' information from unauthorized and potentially illegal usage. In this work this is achieved by the implementation of an EEG signal encryption method that exploits the features of a 3D Lorenz chaotic system, whose state variables exhibit the characteristics of high randomness and unpredictability. The method also includes a random quantization technique, which adds further strength to the encryption system. The method has been tested with standard EEG datasets and experimental methods that include signal distribution, autocorrelation, cross-correlation, power spectral density and percentage residual deviation of the original and encrypted EEG signals. The results suggest that the proposed encryption method exhibits high security and is suitable for the protection of sensitive EEG data

## ACKNOWLEDGMENT

The authors would like to thank the British Council for providing partial support for the collaborative project under the UKIERI scheme.

## REFERENCES

[1] N. Lasierra, A. Alesanco, C. Campos, E. Caudevilla, J. Fernandez, J. Garcia, "Experience of a real-time tele-EEG service," *Annual International Conference of the IEEE Engineering in Medicine and Biology Society,* 2009, pp. 5211–5214.

[2] Health insurance portability accountability act of 1996 (HIPAA), centers for medicine and Medicaid services, 1996. available online at: http://www.cms.hhs.gov/hipaageninfo, [Accessed in 2011]

[3] T. H. Chen, G. Horng, and W. B. Lee, "A publicly verifiable copyright proving scheme resistant malicious attack," *IEEE Transaction on Industrial Electronics, 2005,* 52, pp. 327–334.

[4] F. Sufi, I. Khalil, "Enforcing secured ECG transmission for real-time telemonitoring: a joint encoding, compression, encryption mechanism," *Security and Communication Networks,* 2008, 1(5), pp. 389--405.

[5] F. Sufi, I. Khalil, "A new feature detection mechanism and its application in secured ECG transmission with noise masking," *Journal of Medical Systems,* 2009, 33(3), pp. 121-132.

[6] F. Daschselt, W. Schwarz, "Chaos and cryptography," *IEEE Transaction on Circuit System-1, 48(12), 2001,* pp. 1498-1509.

[7] J. Friedrich, "Image encryption based on chaotic maps," *International Conference on Computational Cybernetics and Simulation, 1997,* pp 1105-1110.

[8] L. Kocarev, "Chaos-based cryptograph: a brief overview," *IEEE Circuits System Magazine*, 2001, pp. 6-21.

[9] S. Li, X. Zheng, "The security of an image encryption method," *IEEE International Conference on Image Processing*, 2002, pp. 925-928.

[10] C. F. Lin, W. T. Chang, C. Y. Li, "A chaos-based visual encryption mechanism in JPEG medical images," *Journal of Medical and Biological Engineering,* 27(3), 2007, pp. 144-149.

[11] M. Yan, N. Bourbakis, S. Li, "Data-image-video encryption," *IEEE Potential*, 2004, pp 28-34.

[12] R. G. Andrzejak, K. Lehnertz, C. Rieke, F. Mormann, P. David, C. E. Elger, Indications of nonlinear deterministic and finite dimensional structures in time series of brain electrical activity: Dependence on recording region and brain state, *Physical Review E*, Vol. 64, 2001, pp. 061907-8.

[13] http://epileptologie-bonn.de/cms/front_content.php?idcat=193&lang=3&changelang=3 [last accessed on April 11, 2011].

[14] A. Rukhin, *et al*., "A Statistical Test Suite for Random and Pseudo-random Number Generators for Cryptographic Applications," NIST Special Publication, 2001, 800-22.