Securing while Sampling in WBAN using Compressive Sensing

Ravishankar Holla[1], Sukeshini Doddamani[2]

[1]Assistant. Professor, Dept. of E&CE, R.V. College of Engineering Bengaluru, Karnataka, India
[2]PG Student Dept. of E&CE, R.V. College of Engineering Bengaluru, Karnataka, India

---***---

Abstract - *In today's digital world, efficient data compression is required to transfer the long range of date over communication channel and data security is a serious concern in biomedical applications. There are several methods to address these problems separately i.e. first data compression is performed on source data based on Shanon-Nyquist theorem and then compressed data is encrypted. Traditional data compression methods requires more number of samples to reconstruct the signal back and security methods are based on public or private key both process requires computational memory and computational resources. This paper provides Compressed Sensing theory which performs compression and encryption simultaneously and avoids personnel key distribution, generating sensing matrix.*

Key Words: **Compressed sensing, Electrocardiography, Linear feedback shift register, Discrete wavelet transform, Orthogonal matching pursuit algorithm.**

1. INTRODUCTION

Diagnosis of heart diseases can be done effectively on long term recordings of ECG signals which keeps the signals morphologies. In such cases, the volume of ECG data produced by the monitoring system increases significantly. This leads to unnecessarily large requirements on storage, throughput and processing capabilities when transmitting samples wirelessly[1]. And also broadcast transmission. Is prone to interception and eavesdroppers hence arises serious security concerns. In order to overcome these issues normally we follow sampling the signal at Nyquist rate, compression and encryption. The existing security systems provides password or secret key to authorized users. Both sampling at Nyquist rate and secret key distribution consumes considerable memory and present an implementation in compact sensor nodes.

In order to solve this issue many researchers introduced new technique called compressed sensing to secure information which is based on the use of measurement matrix as encryption key. It not only provides security but also compresses the data. But the problem of key distribution is not addressed and remains unsettled.

In this paper we propose secure CS framework which includes generation of sensing matrix using linear feedback shift register. Which not only compresses the signal also provides security.

In our proposed model, we have applied various wavelet transform [6]-[7] to ECG signal in order to make signal sparse; a necessary condition for CS theory. For reconstruction we have used Orthogonal Matching Pursuit (OMP) algorithm. To check the quality of the reconstructed signal we assess widely used similarity metrics of Percentage Root Mean Square Difference (PRD), Structural Similarity Index Metric (SSIM), Correlation Coefficient (COC) and time required for encryption and decryption.

1.1 Motivation

The motivation behind this project are:

- To replace existing conventional sampling theory by low sampling algorithms based on CS theory.
- CS theory generates compressed sensing matrix which compresses the signal and also provides security.
- CS theory suggests that we can measure compressed representation directly rather than measuring every sample and then computing a compressed representation.

1.2 Goals and objectives

- To generate secure sensing matrix using LFSR which not only provides security but also compresses the cardiac signal.
- Make ECG signal sparse using various types of wavelets and select better wavelet transform for error free reconstruction of the signal.

2. COMPRESSED SENSING

The idea of "Compressed or Compressive sensing" got a new life in 2004 when David Donoho, Emmanuel Candes, gave important results regarding the mathematical foundation of compressive sensing [2]-[4]. Donoho have made a significant contribution to the body of signal processing literature, by giving sampling theory a new dimension i.e. sampling as well as compression. This method is different from traditional method as it sampled the signal below the Nyquist rate and it permits to exploit the sparse property at the signal acquisition stage of compression.

The basic principle of CS theory is that compressible signals or sparse signals can be reconstructed from a surprisingly fewer number of linear measurements i.e. signal is sampled without any information loss at a rate closer to its information content and still be effectively reconstructed.

The CS theory depends on following key concepts: incoherence and signal sparsity. Incoherence implies that the value of coherence must be very small. Sparsity reflects the inherent ability to be compressed. Most of the biomedical signals are sparse when projected in their suitable basis such as wavelet transform. Sparse is a term used to indicate that the signal has more number of zero values i.e. the information rate is much lower than indicated by its entire bandwidth. Hence zero value coefficients can be ignored or compressed keeping only information carrying coefficients.

Let x be a signal of interest, having a sparse representation in some basis $\Psi = [\Psi_1\ \Psi_2 ... \Psi_L]$ such that

$$x = \sum_{i=1}^{L} \Psi_i s_i \quad \text{or} \quad x=\Psi s \qquad (1)$$

Where 'x' is sparse under the basis $\Psi \in R^{NXN}$ and's' indicates the coefficient vector for x. The most of the coefficients, must be zero or insignificant to discard without loss of information in order to make 'x' to be sparse in Ψ. If has most compact representation in basis Ψ then it is said to be compressible. Hence sparseness also implies that the signal is compressible and vice versa.

The generalised sampling procedure for N dimensional input signal x is compressed to M dimensional set of measurements y, through a linear transformation by taking M linear random projections shown in fig (1) i.e.

$$y = \Phi x \qquad (2)$$

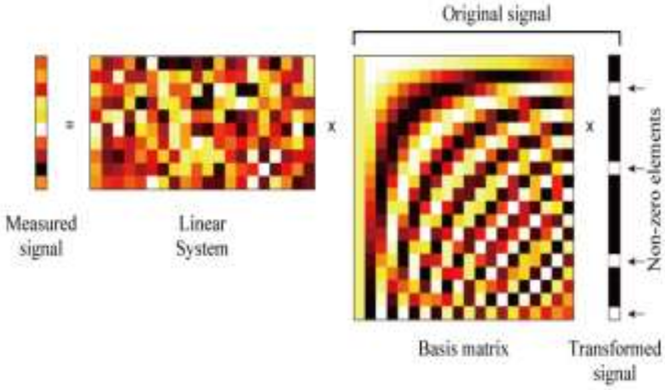

Fig 1: CS Encryption Framework

Where Φ is am MXN (M<N) matrix called the sensing or measurement matrix and y is a sensed signal of size MX1. CS is capable of finding a solution for problem (2) when the sensing matrix Φ satisfies the Restricted Isometric Property (RIP):

$$(1-\delta_k)\|\ x\ \|_2^2 \leq \|\ \ \|_2^2 \leq (1+\delta_k)\|\ x\ \|_2^2 \qquad (3)$$

for all k-sparse vectors x and some constant $0< \delta_k<1$.

Knowledge of sensing modality Φ and the compressed measurements y gives the original signal x in sparse domain Ψ after solving the optimization problem:

$$\min \|\ \hat{S}\ \|_{l_1} \qquad \text{subject to} \quad y = \Phi\Psi s \qquad (4)$$

that finds vector Ŝ with the lowest L1 norm, which solves reconstruction problem.

3. PROPOSED FRAMEWORK

A block diagram of the proposed encryption and decryption framework is shown in fig (2). It defines principle components namely peak detection, LFSR, Sensing matrix generation, CS encryption and reconstruction using OMP algorithm [5]. A detailed description of each block is discussed below.

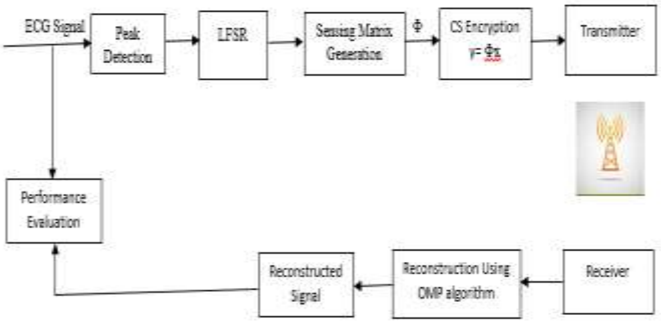

Fig2: Block diagram of proposed system

3.1 Peak Detection

To detect peak values of the ECG signal we take first order difference and calculate the Hilbert transform of the resultant from there we get magnitude by setting threshold value. These peak values are seeded to the LFSR as the input.

3.2 LFSR

The LFSR is a shift register whose input is a linear function of register's previous state. The m-stage LFSR takes a binary sequence of length m, called a seed, shifts it into adjacent positions producing a single output bit and fills the empty position on the other end according to linear feedback. The most commonly used feedback function is exclusive-or (XOR) of some bits in the register. Due to finite number of possible states the LFSR output sequence is also finite and after some point replicates itself. The carefully chosen linear feedback based on primitive polynomial allows generating a so-called maximal length sequence or m-sequence. m-sequence has the longest possible repeating cycle of (2^m-1) and features statistical properties that resemble a truly random binary sequence. This fact is crucial for our purposes since we use LFSR for spreading the distilled secret across a longer bit sequence. A set of m-sequences is used to generate a sensing matrix Φ.

3.3 Sensing Matrix Generation

To balance the number of zeros and ones the input m sequence is augmented with additional zero. Then the elements of a new sequence (0,1) are mapped to (-1,1) and reorganized to form a matrix. The process is repeated L times for different m-sequences and results in a set of matrices Φ_1 ,Φ_2 ,.... $\Phi_{L.}$ Arithmetic sum of Φ_i gives the sensing matrix as

$$\Phi = \sum_{i=1}^{L} \Phi_i$$

It follows that each entry of the sensing matrix converges to random variable with Gaussian distribution as L increases by the central limit theorem. Note that larger values of parameter L require more bits to be extracted from the channel and thus L defines the amount of randomness in the system.

3.4 CS Encryption

This block is the only part of the framework that differs for transmitter and receiver. The CS Encryption Block encrypts and compresses data *x* using the sensing matrix Φ. Transmitter follows equation (1) and performs secure compressed sampling of the original signal x with matrix Φ. The sensed version y is now safe for transmitting to a receiver over an insecure broadcast channel. On the other end, the receiver solves optimization problem in order to recover the desired signal x.

3.5 Reconstruction Using OMP Algorithm

In this work we have used Orthogonal Matching Pursuit (OMP) algorithm [8, 10] for signal recovery. It is an iterative greedy algorithm that finds the sparse solution x subject to y = ΦΨx,, Where Ψ is the basis matrix, Φ is the sampling matrix, and y is measurements. OMP reconstruction algorithm is explained in the following flow diagram.

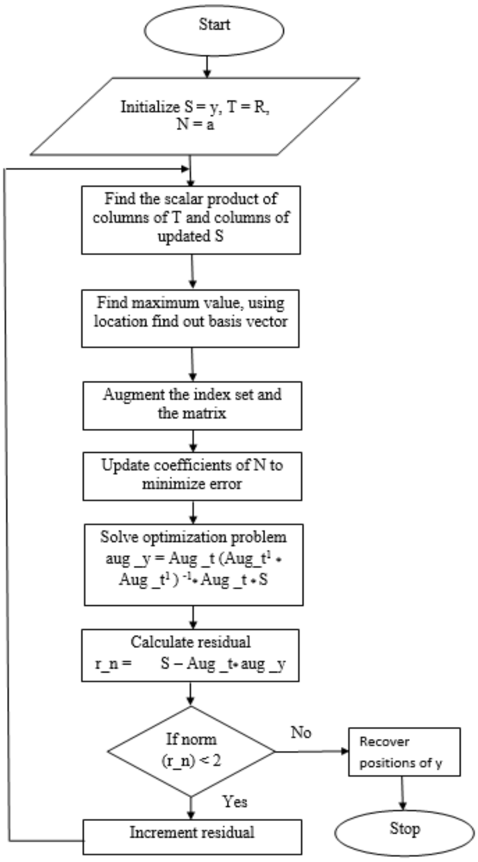
Start
Initialize S = y, T = R, N = a
Find the scalar product of columns of T and columns of updated S
Find maximum value, using location find out basis vector
Augment the index set and the matrix
Update coefficients of N to minimize error
Solve optimization problem aug _y = Aug _t (Aug_t¹ ∗ Aug _t¹) ⁻¹∗ Aug _t ∗ S
Calculate residual r_n = S – Aug _t∗ aug _y
If norm (r_n) < 2
No
Recover positions of y
Yes
Increment residual
Stop

Fig 3: Flow diagram of OMP recovery algorithm

4. PERFORMANCE EVALUATION AND RESULT ANALYSIS

The simulation of implementing the concept of insertion of security while the sampling in the WBAN signals is done using MATLAB in this work. The result analysis for both encryption and decryption is done based on the parameters like PRD, COC for different compression percentage values. We have used different wavelet transform to check better reconstruction quality.

The ECG signal taken for the analysis in this work consists of 512 samples which is sampled at the rate of 128Hz. This is considered as the input for the further processing.

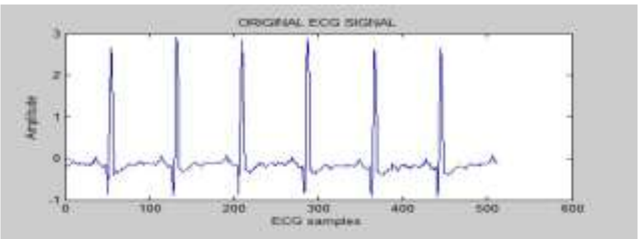

Fig 4.1 Input ECG signal

The R-Peak values of the ECG signal is detected using Hilbert transform. And the peak values are highlighted.

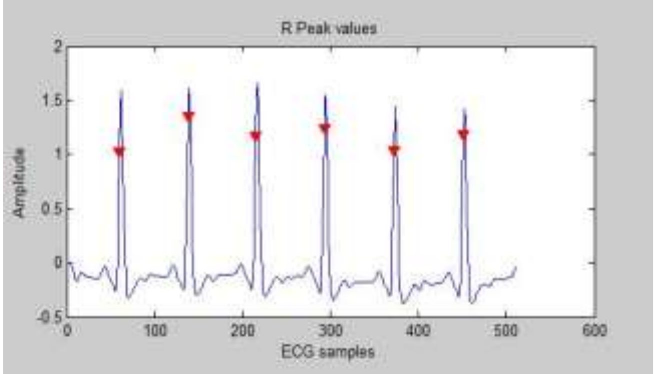

Fig 4.2 R-Peak Detection using Hilbert Transform

The encrypted signal is generated by multiplying Compressed Sensing matrix with the input. Linear feedback shift register (LFSR) is used to generate compressed sensing matrix and LFSR, which takes R-Peak values as input which is fed as binary values. The output of LFSR is later rearranged based on Gaussian distribution to get secure sensing matrix.

The ECG signal at the receiving end is reconstructed using Orthogonal Matching Pursuit (OMP) algorithm, based on ℓ1 minimization. This algorithm recovers original ECG signal with acceptable quality. Reconstruction with Coiflet wavelet after 40 percent compression and the reconstruction is done by using OMP recovery algorithm. Following fig shows original, encrypted and reconstructed ECG signal.

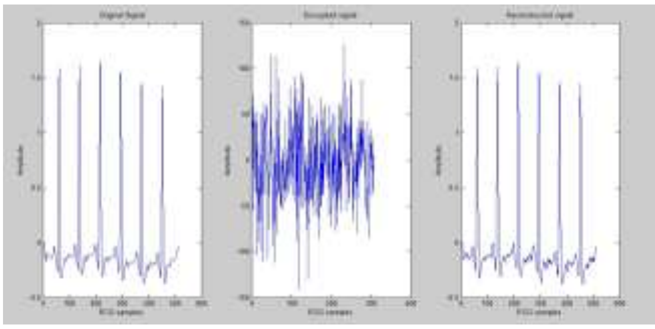

Fig 4.3 Original, Encrypted and Reconstructed signal.

To evaluate the reconstruction quality we have measured PRD values and COC values in order to check error in the signal. And the graph is plotted (4.4 and 4.5) by varying compression percentage values for considering various wavelets.

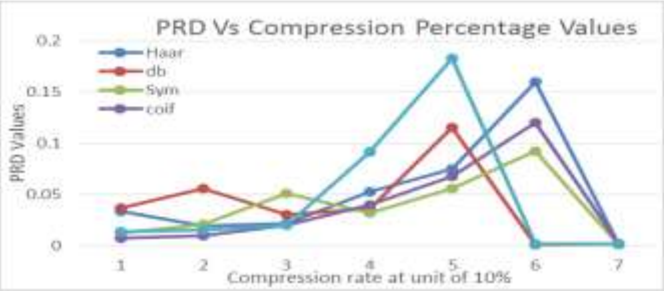

Fig 4.4 Comparison of PRD with Compression Percentage

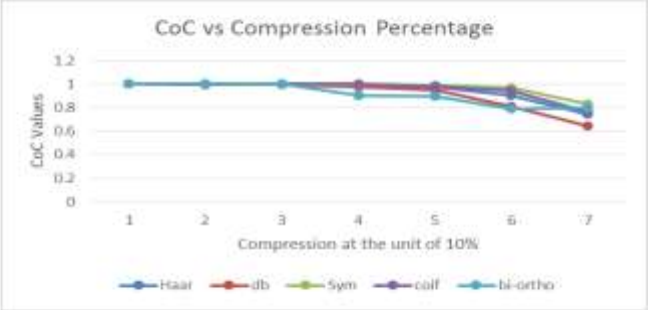

Fig 4.5 Comparison of CoC with Compression Percentage

From the above two graphs it can be inferred that symlets and coiflet wavelets recover the compressed signal with minimum error and Correlation coefficient almost 1.

4. CONCLUSION

Analysis of reconstructed signal is done using various wavelets namely Haar, symlets, Daubechies, Coiflets and Biorthogonal wavelets applied to ECG records extracted from physionet database. It is inferred that the reconstruction pattern varies with the wavelet used. Perfect reconstruction of cardiac signal is obtained using coiflet window at the decryption end with the compression percentage of 40 percent with the correlation coefficient equal to 1 and PRD value of 0.053. Moreover the advantage of the proposed method is that the quality of the received signal is guaranteed. Simulation results suggest that Compressive Sensing should be considered as an acceptable methodology for ECG compression and encryption.

ACKNOWLEDGEMENT

I would like to express my heartfelt gratitude to my project guide Mr. Ravishankar Holla, Assistant Professor, Department of E&CE, R.V. College of Engineering, Bengaluru. For his committed guidance, valuable suggestions, and sustained help from the very early stage of this project work.

REFERENCES

[1] J Daemen, V. Rijmen, The Design of Rijndael: AES-The Advanced Encryption Standard, Springer-Verlag.2002

[2] David L. Donoho. 2004. Compressive sensing. Department of statistics, Stanford University.

[3] E. J. Candes, J. Romberg, and T. Tao, ”Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information”, IEEE Trans. Inf. Theor., vol. 52, no. 2. Pp. 489-509. Feb. 2006

[4] E. J. Candes and T. Tao, “Near-optimal signal recovery from random projections: universal encoding strategies,” IEEE Trans. Inf. Theory, vol. 52, no. 12, pp. 5406-5425, Dec. 2006.

[5] R. Dautov and G. R. Tsouri, “Establishing secure measurement matrix for compressed sensing using wireless physical layer security,” in Computing, Networking and Communications (ICNC), 2013 International Conference on. IEEE, 2013, pp. 354–358.

[6] M.L. Hilton. “Wavelet and Wavelet packet compression of Electrocardiograms”. IEEE Transactions on Biomedical Engineering, 44(5):394-402,1997.

[7] Ibaida and I. Khalil. “Wavelet based ECG steganography for protecting patient confidential information in point-of-care systems.”IEEE transactions on bio-medical engineering, 2013.

[8] T. Tony Cai and Lie Wang, “Orthogonal Matching Pursuit for Sparse Signal Recovery With Noise”, IEEE Transactions On Information Theory, Vol. 57, No. 7, July 2011.

[9]]. Y. Cen, X. Chen, L. Cen, and S. Chen, “Compressed sensing based on the single layer wavelet transform for image processing,” Journal on Communications, vol. 31, no. 8, pp. 53–55, 2010.

[10] M. Figueiredo, R. Nowak, and S. Wright, “Gradient projection for sparse reconstruction: Application to compressed sensing and other inverse problems,” Selected Topics in Signal Processing, IEEE Journal of, vol. 1, no. 4, pp. 586-597, 2008.

BIOGRAPHIES

Mr. Ravishanka Holla,
Assistant Professor, Department of E&CE,
R.V. College of Engineering, Bengaluru, India.

Sukeshini Doddamani
PG Student, Department of E&CE,
R.V. College of Engineering, Bengaluru, India.