

# ECG COMPRESSION AND ENCRYPTION TECHNIQUES FOR DIAGNOSIS OF CARDIOVASCULAR DISEASE

This is a Diagnosis of Cardiovascular Disease

P.Santhi

Computer Science and Engineering  
Paavai Engineering College  
Namakkal,India

E-mail :mssanthiboopathicse@gmail.com

Dr.V.MuraliBhaskaran

Computer Science and Engineering  
Paavai College of Engineering  
Namakkal,India

E-mail:murali66@gmail.com

**Abstract**— The cardiovascular disease is number one killer of the world for both men and women. The ECG signal is mainly used to monitoring this type disease. In this paper proposes the compression of ECG signals and provide the encryption for that signals. The encryption technique of ECG signal is used to provide the security of the patient health information from the public media. This paper proposes the hybrid algorithms for the ECG signal compression and the combination of chaos key and polynomial based algorithm for ECG signal Encryption. The hybrid algorithms are Karhunen-Loeve Transform(KLT) and Wavelet Packet Transform on technique.

**Keywords**—*Compression, Encryption, Security, ECG, Hybrid algorithm.*

## I. Introduction

Today many people lost their life due to cardiovascular disease; this is the number one killer in the world for all men and women. The ECG signal is used by the cardiac specialists for diagnosis the cardiovascular disease. The cardiac specialists are using the tele cardiology to save the patient life from the death. In first the ECG signal sends from sensor to mobile. Then the ECG signals to be compressed to increasing the diagnosing accuracy of cardiovascular disease.

Effective compression of ECG signal is used for many applications are ECG Data Storage, ECG data transmission over the network. Data compression is the process of detecting and eliminating the redundancy of given data set. The techniques that is used for compressions are lossy data Compression and loss less data compression .

The loss less data compression allows the exact original data to be reconstructed from the compressed data. The loss less compression methods are Limbel Ziv Marcov chain algorithm, LZ77, LZWL. Another data compression technique is Lossy data compression technique is a data encoding method that compresses data by discarding some of it. The procedure aims to minimize the amount of data that need to be held, handled, and/or transmitted by a computer. The techniques are mainly used for the ECG

Compressions are discrete cosine Transform, Discrete Sine Transform, Wavelet transform and Fourier Transform.

In this paper proposes the new hybrid algorithm of Karhunen - Loeve Transform (KLT) and Wavelet Packet Transform compression techniques. The KLT is based on the discrete cosine Transform. The main advantage of KLT is the least number of orthogonal functions is needed to represent the input signal. The Wavelet Packet Transform compression technique is based on the wavelet transform. Wavelet packet decomposition (WPD) (sometimes known as just wavelet packets) is a wavelet transform where the signal is passed through more filters than the discrete wavelet transform (DWT). After that compression ECG signal will be Encrypted. The encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information. Many techniques are used to encrypt the ECG signals are Public Key Encryption and digital signatures. In this paper proposes the chaos key and polynomial based encryption techniques.

## II. Methodology

### A. Flowchart for Proposed Method

In this figure represent the steps for this proposed method. By using this flowchart users can easily understanding this Research in cardio vascular disease. This paper proposes the Wavelet and cosine transform for the ECG signal compression and Chaos and polynomial based method is used for ECG Encryption.

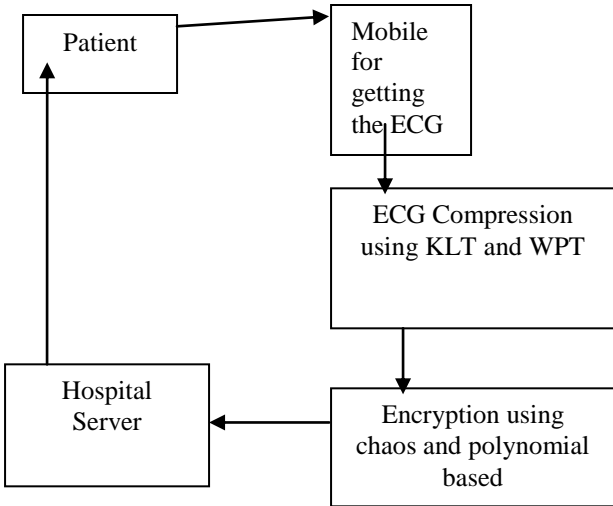


Fig.2.1.Flowchart

**B. ECG Compression Techniques**

The Compression technique is very important one to improving the Efficiency. It will reduce the space needed by the data. It contains two types of compression techniques are lossless compression and lossy compression. In ECG data compression the Discrete Cosine Transform is very better comparing to other techniques. In this paper proposes the KLT and WPT compression algorithm.

**a. Karhunen-Loeve Transform (KLT)**

So far no transformation has been found for images that completely removes statistical dependence between transformation coefficients. Suppose a reversible transformation is carried out on N-dimensional vector  $\vec{b}$  to produce N-dimensional vector  $\vec{c}$  of transform coefficients, denoted by,

$$\vec{c} = T\vec{b} \text{ -----(1)}$$

where T is a linear transformation matrix that is orthonormal or unitary;

The vectors  $\vec{t}_m$  are called orthonormal basis vectors for linear transform  $T$ .

The value of  $\vec{b}$  as,

$$\vec{b} = \sum_{m=1}^N \vec{c}_m \vec{t}_m \text{ -----(2)}$$

where  $\vec{c} = [c_1, \dots, c_N]$  are transform coefficients, and  $\vec{b}$  is represented as a weighted sum of basis vectors.

KLT transform is an orthogonal linear transformation that can remove pairwise statistical correlation between the transform coefficients; ie the KLT transform coefficients satisfy (for  $m \neq n$ )

$$\sum_{c_m, c_n} c_m, c_n P(c_m, c_n) = \sum_{c_m} c_m P(c_m) \cdot \sum_{c_n} c_n P(c_n)$$

where summation is over all possible values  $c_m$  and  $c_n$  and  $P()$  represents the probability.

The KLT can be derived by assuming

$$E(\vec{b}) = 0 \Rightarrow E[\vec{c}] = 0 \text{ ----- (3)}$$

The  $N \times N$  correlation matrix of  $\vec{b}$  then becomes

$$\underline{R} = E(\vec{b}\vec{b}^T) \text{ -----(4)}$$

**b. Wavelet Packet Transform (WPT)**

Wavelet packet transforms are also related to the discrete wavelet transform.

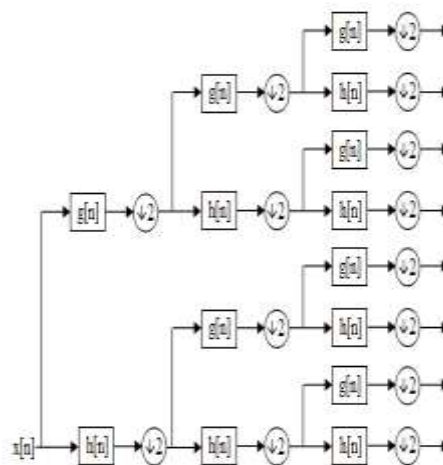


Fig.2.2.WPT Transform

(4.4.1)

**C. Encryption Techniques**

(4.4.2)

This technique is mainly used to providing the security to the patient data. To protect patient’s privacy and possible spoof attack, the ECG segments are required to be encrypted. In previous studies, we have used permutation cipher noised smearing technique , and wavelet based technique. However, all of these techniques are computationally expensive for mobile and embedded devices with low computational capacity. In this paper



proposes, a multi-scroll chaos cryptosystem and polynomial based method for ECG encryption.

**a. Chaos Crypto System**

The Patients mobile phone receives the ECG signal from the ECG acquisition device and also requests a chaos key from the chaos generation server. The chaos key is then XOR ed with the ECG packet, while both of them being the same size (length). After performing the XOR operation between the ECG packet and the chaos key, the resultant is encrypted ECG. Equation (1) represents the original ECG (unencrypted).  $\psi$  is the chaos key required to encrypt the unencrypted ECG,  $e(n)$ . Equation (2) shows the XOR operation for retrieving the encrypted ECG  $\tau$ .

$$e(n) = x(1), x(2), x(3), \dots, x(N) \text{---- (5)}$$

where,  $N$  is the length of the ECG packet.

$$\tau(n) = e(n) \oplus \psi \text{----- (6)}$$

**b. Polynomial Based Method**

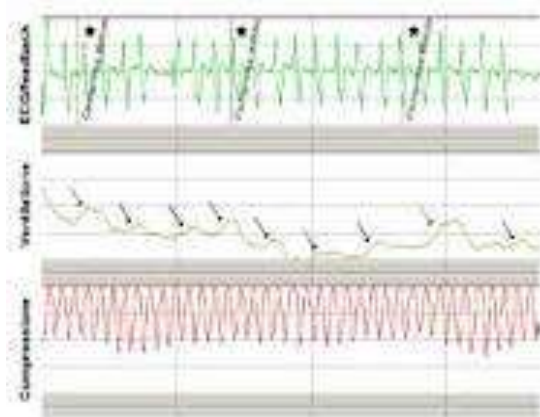
A polynomial was used to extract polynomial Coefficients from the ECG signal. These coefficients were then used as biometric templates for matching purposes. It uses a distance measurement technique, to ECG encryption. It will reduce the template size.

**III. Results and Discussion**

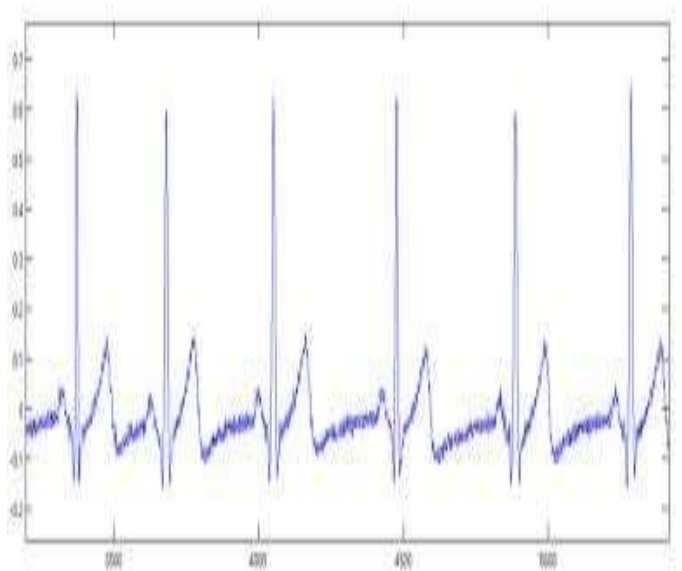
In this result show that ECG compression and Encryption of ECG signals.



**Fig.3.1.Original ECG Signal**



**Fig.3.2.Compressed ECG Signal**



**Fig.3.3.Encrypted ECG Signal**

**IV. Conclusion**

In this paper gives the compression and Encryption techniques for ECG signal. The Compression techniques are used to reduce the space for ECG signal. It contains the Loss Less and Lossy compression. In this paper proposes the KLT algorithm in DCT algorithm and WPT (Wavelet Packet Transform) for ECG Compression. In this Encryption techniques will reduces the template size and increasing the efficiency. The Encryption is used to provide the security of the patient data. Many Encryption techniques are there, but chaos is very flexible in mobile Environment. This Paper gives the chaos and polynomial based encryption for provide the security over the network.

**Acknowledgment**

I would thank my guide Dr.V.Murali Bhaskaran for giving innovative ideas for my research and also for my DC members and colleagues of CSE Department.

## References

- [1] F. Sufi\* , F. Han, I. Khalil and J. Hu,"A chaos-based encryption technique to protect ECG packets for time critical telecardiology applications," SECURITY AND COMMUNICATION NETWORKS *Security Comm. Networks* (2010).Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/sec.226.
- [2] Sufi F, Fang Q, Khalil I, Mahmoud SS,"Novel methods of faster cardiovascular diagnosis in wireless telecardiology,"*IEEE Journal on Selected Areas in Communications*2009; **27**(4): 537–552.
- [3] Khalil I, Sufi F. Legendre polynomials based biometric authentication using qrs complex of ECG. *International Conference on Intelligent Sensors, Sensor Networks and Information Processing, 2008 (ISSNIP 2008)*, December 2008; 297–302.
- [4] Robert S. H. Istepanian, Leontios J. Hadjileontiadis, *Member, IEEE*, and Stavros M. Panas, *Member, IEEE*, " ECG Data Compression Using Wavelets and Higher Order Statistics Methods," IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE, VOL. 5, NO. 2, JUNE 2001;108-116.
- [5] Fahim Sufi, Ibrahim Khalil, and Jiankun Hu," ECG-Based Authentication,"309-330.
- [6] Daniel Socek\_, Shujun Liy, Spyros S. Magliverasz and Borko Furhtx," Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption".