International Journal of Computational Intelligence and Informatics, Vol. 4: No. 3, October - December 2014

Elliptic Curve Cryptography based key generation from the fusion of ECG and Fingerprint

M Sreemathi
Department of Computer Science
Periyar University
Salem, Tamailnadu
sreemathi23@gmail.com

K Thangavel
Department of Computer Science
Periyar University
Salem, Tamailnadu
drktvelu@yahoo.com

K Sasirekha
Department of Computer Science
Periyar University
Salem, Tamailnadu
ksasirekha7@gmail.com

***Abstract*-This article deals with the new innovative model for cryptographic key generation from the fusion of Electrocardiogram (ECG) and fingerprint using Elliptic Curve Cryptography (ECC). Among all the biometrics, ECG and Fingerprint is used to generate the key since ECG provides intrinsic liveliness detection and fingerprint based identification is highly scalable. After preprocessing the biometric traits, the features are extracted. Then the extracted features are fused to generate the cryptographic key. ECC is used as many mathematicians proved that elliptic curve gives the best solution for cryptography. The generated cryptographic key using the proposed method is smaller when compared with RSA.**

Keywords- ECG, Daubechies Wavelet, Fingerprint, Fusion, ECC, RSA

I. INTRODUCTION

Biometric is used to find the individuals in group. The identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition retina and odour. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice [1].More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information [2].

The ECG is quite appealing for biometrics in light of the seven factors defined in Jain et al [3]. the ECG modality is admissible given that it can be found in virtually all living humans (Universality), its authentication capabilities for circumscribed groups of individuals has been shown (Uniqueness), it can be easily acquired using suitable devices (Measurability), it has been shown to perform accurately for subsets of the population (Performance), the approach has made it acceptable (Acceptability), and it's not easily spoofed as it depends. Furthermore, ECG signals provide intrinsic liveliness detection and are continuously available, which are also highly desirable properties in biometrics. Fingerprint is a widely used form of biometric identification. It is a robust means of person identification.

Fingerprint recognition has forensic applications like criminal investigation, missing children etc., government applications like social security, border control, passport control, driving license etc., and commercial applications such as e-commerce, Internet access, ATM, credit card etc. [4][5]. Because of their uniqueness and consistency over the time, fingerprints have been used for identification and verification over a century. The process of fingerprint recognition is becoming automated and results in many Automatic Fingerprint Identification System (AFIS). Fingerprint usually appears as a series of dark lines that represent the ridges while the valleys between these ridges appear as white space.

Cryptography is a secured communication system through insecure channels. It is also expanding in application field. It is safe to send encrypted message without fear of interception, because an interceptor is unlikely to be able to decipher the message. A public key cryptography is important in the field of cryptography, provides answer to the problems for key management, authentication and digital signatures.

In this study, finger print and ECG signals are taken into consideration as biometrics for the security purpose. In most of the research papers unimodal procedure is adopted, but there are certain disadvantages. In order to overcome the problems faced in the existing methods, features extracted from the fingerprint and ECG signals are fused to generate key using cryptography key generation method. Figure 1 shows the process of key generation.

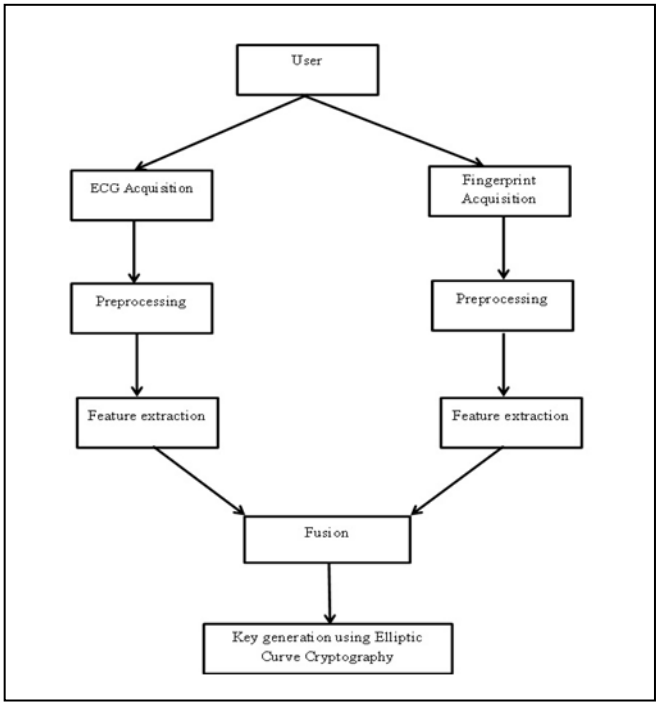


Figure 1. Key generation process

II. RELATED WORK

ECG signals are used in biometrics to identify the heartbeat of the individuals. It gives the authentic values.ECG signal should be preprocessed since it may have several noises due to breathing of identity and thus features can be absolutely extracted.

Biel et al. [6] demonstrated the possible use of ECG for biometric application. They conducted the biometric experiment on a group of 20 subjects where 30 features are extracted from each heartbeat. In order to reduce the amount of information the features with a relatively high correlation with other features are discarded and finally, 12 features are selected for classification. A multivariate analysis based method is used for classification; however Principle Component Analysis (PCA) score plot is utilized to interpret the similarities and differences of heartbeats among individuals.

Israel et al. [7] proposed to extract patterns from ECG they performed ECG processing for quality check. A quantifiable metrics is proposed for classifying heartbeats among individuals. A total of 15 intrabeat features based upon cardiac physiology is extracted from each heart- beat and the classification is performed using linear discriminant analysis. The tests show that the extracted features are independent to electrode positions (e.g., around chest and neck), invariant to the individuals state of anxiety and unique to an individual.

Mikhled Alfaouri et al. [8] suggested that ECG signal denoising is done based on wavelet transform thresholding, where relationship is established between threshold value obtained and the noisy signal using the wavelet transform.

Ayman Rabee et al. [9]suggested that ECG signal analysis using discrete wavelet transform multi resolution analysis and classification by support vector machine. Wavelet transform is used for signal preprocessing, denoising, and for extracting the coefficients of the transform as features of each ECG beat which are employed as inputs to the classifier. SVM is used to construct a classifier to categorize the input ECG beat.

S. Banerjee et al.[10] demonstrated the discrete wavelet transform (DWT) based feature extraction technique is proposed. The signal is denoised by decomposing it using DWT technique and discarding the coefficients corresponding to the noise components. A multi resolution approach along with an adaptive thresholding is used for the detection of peaks.

K.Sasirekha et al. [11] proposed the cryptographic key generation using fingerprints. In this paper binarization using threshold, normalization using min-max method, segmentation to extract ROI and thinning to reduce the ridge thickness has been discussed. After preprocessing, the minutiae points are extracted and using Crossing Number (CN) method.

Fu et al. [12] proposed a method of multibiometric cryptosystem, by binding the multiple features of biometrics to cryptography. There are two levels of combining, that is combining at the biometric level and combining at the cryptographic level. Shannon entropy is used to afford security. Accuracy and efficiency are also evaluated and it was compared with other systems.

In the proposed work, the fusion of the ECG and fingerprint has been performed and applied Elliptical Curve Cryptography method to generate key. ECG cannot be mimic as others. First we get ECG through fingers and then denoising the ECG as well as fingerprint and extract the features for biometric values. It is be used for key generation by adopting Elliptic curve Cryptography (ECC).The ECC method has not been used so far to generate key from the fusion of biometric features as per the literature.

III. PRELIMINARIES

ECG signal data has been taken from Physionet website ECGID database. The collected records of more than 50 different persons by digitized ECG signal are converted to ECG signal; Feature extraction can be taken place by preprocessing step and get the biometric value for key generation.

A. Daubechies wavelet

Wavelets are building blocks that can quickly decorrelate data. The signal can be decomposed into many frequency bands .A wavelet transform is multi-resolution analysis as it gives frequency and time representation at same time [8] by using Daubechies wavelet, we can identify wavelet decomposition of signal. Daubechies wavelet is chosen, since it has structure similar to waveform. As daubechies wavelet of higher orders has better frequency resolution than time resolution. To denoise the ECG signal ,daubechies wavelet of order 5 can be used to extract features of each signal. Wavelet transformation is convolution of mother wavelet function ψ (t) with signal x (t).

$$\gamma(s,\tau) = \int f(t)\psi^{*}_{s,\tau}(t)dt \tag{1}$$

$$f(t) = \int\int \gamma(s,\tau)\psi_{s,\tau}(t)d\tau ds \tag{2}$$

$$\psi_{s,\tau}(t) = \frac{1}{\sqrt{s}}\psi\left(\frac{t-\tau}{s}\right) \tag{3}$$

$\psi_{s,\tau}(t)$ is wavelet with scale, s and time, t, -Shift in time,S change in scale S means long wavelength,1/√s is used for normalization. The signal approximation of the original signal at scale index is the combination of approximation and detail signal at the next lower [8,13-14]. Figure 2 represents decomposition and reconstruction of ECG signal.

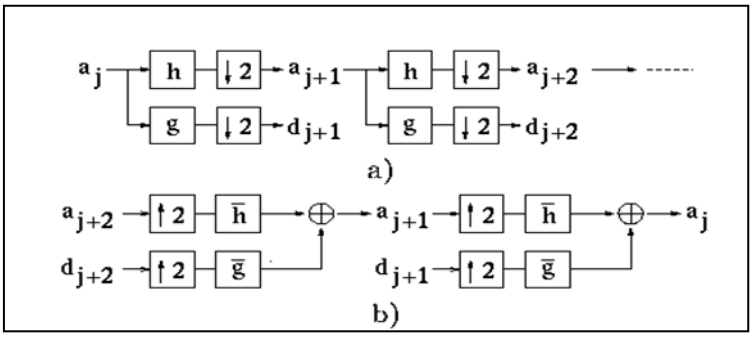


Figure 2. Decomposition and Reconstruction of ECG signal

$$a_{j+1}(p) = \sum_{n} h(n-2p)a_j(n) \tag{4}$$

$$\phi(x/2) = 2^{1/2}\sum_{n} h(n)\phi(x-n) \tag{5}$$

Where the set of numbers aj(n) represents the approximation of the signal at the resolution 2^{-j}

$$d_{j+1}(p) = \sum_{n} g(n-2p)a_j(n) \tag{6}$$

$$\psi(x/2) = 2^{1/2} \sum_{n} g(n)\phi(x-n) \tag{7}$$

Where the set of numbers $d_j(n)$ represents the details lost in approximating the signal at resolution $2^{-(j-1)}$

The method is based on taking the discrete wavelet transform (DWT) of a signal, passing this transform through a threshold, which removes the coefficients below a certain value .In this paper denoising is done by decomposing the signal into five levels of wavelet transform using daubechies wavelet(db5) [15]. The Percentage Root mean square Difference (PRD) and Signal to Noise Ratio (SNR) are calculated to verify the improvement in the reconstructed signal [8].

$$PRD = \sqrt{\frac{\sum_{n=0}^{N}\left(V(n) - V_R(n)\right)^2}{\sum_{n=0}^{N} V^2\ (n)}} * 100\% \tag{8}$$

V(n): original ECG signal.

$V_R(n)$: reconstructed ECG signal.

$$\text{SNR} = \log_{10} \frac{\sum_{n=0}^{N} {V_R}^2(n)}{\sum_{n=0}^{N} {S_R}^2(n)} \tag{9}$$

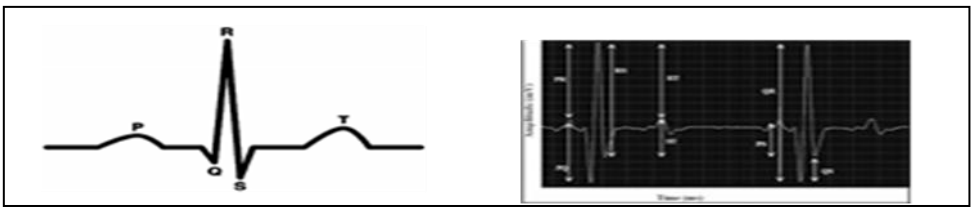
S_R (n): the deformation in reconstructed ECG signal.

Using SNR and PRD calculations from the decomposed ECG signals the feature has to be extracted for biometric value from the signal using Discrete wavelet Transform (DWT). The vital important task in all automated ECG analysis algorithms is ECG R-wave peak detection. Using MINPEAKHEIGHT THRESHOLD Value the Position of R-wave Peak [16] is found. The MINPEAKHEIGHT THRESHOLD is 0.1. The locations of other components of ECG signals such that Q, S and P and the T waves can be found by considering the relative position of R, Q, S respectively.

The three types of features are

1. Amplitude features.
2. Angle features.
3. Interval features.

The extraction of P amplitude feature from ECG signal has the characteristic of constant, based on position and age throughout the life. This can be identified through the difference between the waves or valleys. The latter is not constant, varies based on time. Hence former can be used as a biometric [17]. Figure 3 represents standard ECG waveform and amplitude features. Figure 4 represents feature extraction from ECG.



(a) (b)

Figure 3. a) Standard ECG waveform b) Amplitude features

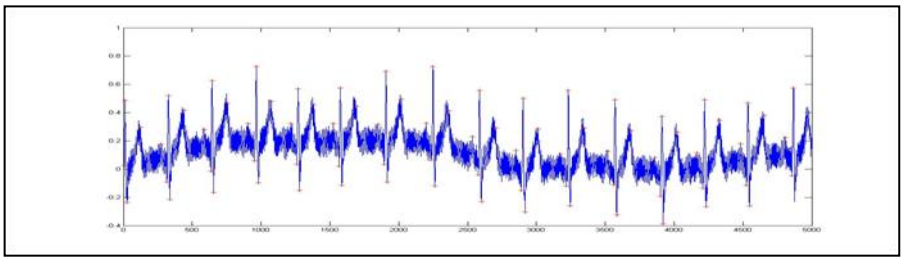


Figure 4. Feature Extraction from ECG

B. Fingerprint

Fingerprint is acquired from Fingerprint Verification Competition (FVC) database. An acquired images are preprocessed it includes Binarization using threshold, normalization using min-max method, segmentation to extract ROI and thinning to reduce the ridge thickness. After preprocessing, the minutiae points are extracted using Crossing Number (CN) method. Finally a cryptographic key is generated from the fused ECG and Fingerprint.

- *Binarization*

Based on the threshold the acquired grayscale image is converted to binary image. The input image is replaced by the output image with the value 1(white) for the image with luminance greater than threshold and other with the value 0 (black). Hence the threshold value is in the range (0, 1). We have used the function graythresh to compute the threshold [12].

$$pval[i] = \begin{cases} 1 & if \quad G[i] \geq threshold \\ 0 & otherwise \end{cases} \tag{10}$$

The intensity value of the gray scale image at the pixel I is G[i] and pval[i] is the grey value of the binarized image at the pixel i [15].

- *Normalization*

The process of changing the range of pixel intensity values is called Normalization. By using this required step, the fingerprint can be normalized by mapping the intensity levels into the range [gmin, gmax]. The formula for gray level normalization is given below

$$g(i,j) = g_{\min} + \frac{(g_{\max} - g_{\min}) X (g_o(i,j) - g_{o\min})}{(g_{o\max} - g_{o\min})} \tag{11}$$

- *Segmentation*

The process of separating the foreground regions in the image from the background regions is termed as Segmentation. The former correspond to the clear fingerprint area containing the ridges and valleys, which is the area of interest where the latter corresponds to the regions outside the borders of the fingerprint area, which do not contain any valid fingerprint information [18].

In a fingerprint image, the low grey scale variance was exhibited by the background region and high variance by foreground region respectively. Therefore a method with variance threshold is used to perform the Segmentation. First, the blocks can be made by dividing the image and each block in the image is calculated for the grey-scale variance. The less variance block is assigned to be a background region and the high is assigned to be part of the foreground. The grey-level variance for a block of size W x W is defined as:

$$V(k) = \frac{1}{W^2} \sum_{i=0}^{W-1} \sum_{j=0}^{W-1} \left(I(i,j) - M(k)\right)^2 \tag{12}$$

where V(k) is the variance for block k, I (i, j) is the grey-level value at pixel (i, j) and M(k) is the mean greylevel value for the block k.

- *Thinning*

To reduces the ridge thickness to one pixel wide the enhanced fingerprint is converted to thinned image. a morphological operation that is used to remove selected foreground pixels from enhanced images called Thinning . The result shows the well preservence of connectivity of the ridge structures, and that the skeleton is eight-connected throughout the image.

- *Minutiae Extraction from Fingerprint*

The minutiae points had been extracted after the enhancement of the fingerprint image. By examining the local neighborhood of each ridge pixel using a 3 × 3 window the ridge endings and bifurcations are acquired from the skeleton image. The Crossing Number (CN) is the most commonly employed method of minutiae extraction. A large number of techniques for minutiae extraction available in the literature belong to this category. The usage of the skeleton image where the ridge flow pattern is eight connected is involved in this method. By scanning the local neighborhood of each ridge pixel in the image using a 3 × 3 window minutiae points are extracted.

$$CN = 0.5\sum_{i=1}^{8}|p_i - p_{i+1}|, \qquad p_9 = p_1 \tag{13}$$

Where p is the pixel value in the neighborhood of p. Figure 5 represents minutiae extraction from fingerprint.

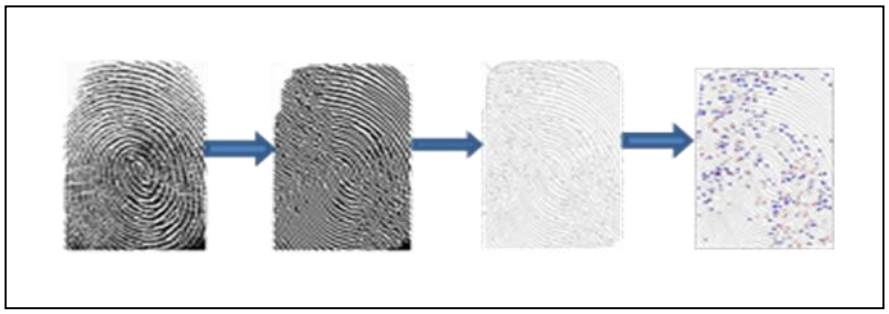


Figure 5. Minutiae Extraction from fingerprint

C. ECG with Fingerprint

The objective of the inclusion of ECG with fingerprint biometric is because; ECG is a physiological signal that has inherent real time vitality signs. In addition, the ECG information is intrinsic to an individual so it is hard to steal and impossible to mimic. Therefore, ECG as a biometric is robust enough against spoof attacks or falsification.ECG can be combined with fingerprint biometrics, effectively.

D. Elliptic Curve Key Generation for ECG and Fingerprint

Let p be a prime number, and let Fp denote the field of integers modulo p. An elliptic curve E over Fp is defined by an equation of the form

$$y^2=x^3+ax+b \tag{14}$$

where a, b ∈ Fp satisfy $4a^3+27b^2\equiv 0 \pmod p$.A pair(x,y),where x,y∈Fp, is a point on the curve if (x,y) satisfies the equation. The point at infinity, denoted by ∞, is also said to be on the curve. The set of all the points on E is denoted by E (Fp) Let E be an elliptic curve defined over a finite field Fp. Let P be a point in E(Fp),and suppose that P has prime order n. Then the cyclic subgroup of E(Fp) generated by P is

$$<P>=\{\infty,P,2P,3P,...,(n-1)P\} \tag{15}$$

The prime p, the equation of the elliptic curve E, and the point P and its order n,are the public domain parameters[19].

IV. Experimental Results And Comparative Analysis

Biometric individuality is a major concern to assess the performance of a biometric system. In real time application, it is applied in such a way in which the ECG and Fingerprint is given as input to the key generator. Which will generates the biometric based keys i.e., private key and public key.

In proposed work by using ECG and Fingerprint as a biometric component. Features are extracted and key is generated with the help of Elliptic Curve Cryptography.

Elliptic curves provide good security with smaller key sizes, something that is very useful in many applications. Smaller key sizes may result in faster execution timings for the schemes, which is beneficial to systems where real time performance is a critical factor. So we use ECC for key generation. The used input is fusion of ECG with Fingerprint, to generate secured key.

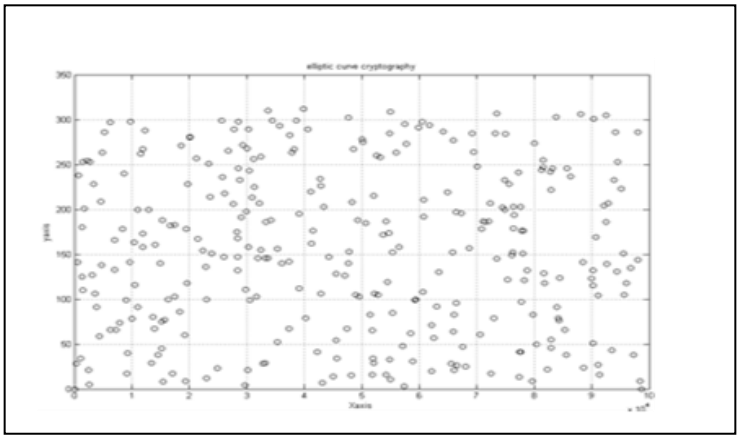


Figure 6. Elliptic Curve Cryptography

Algorithm: ECC

Step 1. A private key is an integer d that is selected uniformly at random from the interval[1,n−1], and the corresponding public key is Q=dP.
Where d is the private key and Q is public key.

Step 2. A Biometric values is first represented as a point M, and then encrypted by adding it to kQ
Where k is randomly selected integer and Q is intended recipient's public key

Step 3. The sender transmits the points and to the recipient who uses her private key d to compute.
dC1=d(kP)=k(dP)=kQ

Step 4. Thereafter recovers M=C2−kQ. An eavesdropper who wishes to recover M needs to compute kQ.

When ECC is compared with RSA, the key size is too smaller than RSA. It provides relatively small block size, high speed, and high security.

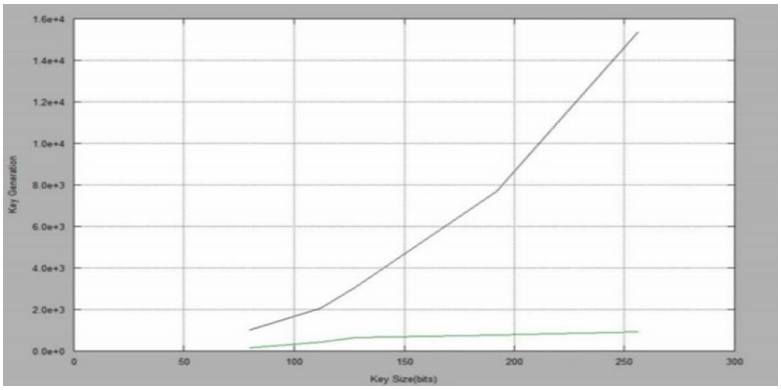


Figure 7. Key size comparision of ECC and RSA

V. CONCLUSION

In this work, a method for key generation from the fusion of ECG and fingerprint is proposed. The small key size of the ECC makes all to use in many application field. The usage of this method provides security with privacy. In the proposed method, the extracted features from biometric are used for key generation. The proposed method is compared with RSA and it proves that it has the characteristics of smaller key size, less storage and Communication and much efficient than RSA.

REFERENCES

[1] Jain,Anil,K,Ross andArun, "Introduction to Biometrics", Springer pp 1-22, 2005.

[2] Jain,A., Hong.L and Pankanti, "Biometric Identification", communications of the ACM, vol. 42(2), pp.91-98, 2000.

[3] A. K. Jain, R. M. Bolle, and S. Pankanti, "Biometrics: Personal Identification in Networked Society". Springer, 2005.

[4] Davide.M, Dario.M, Jain.A.K, Salil .P, "Handbook of Fingerprint Recognition", 2nd Ed. Springer, 2005.

[5] K. Sasirekha, and C. Immaculate Mary, "Biometric based Network Video Security System with RSA Implementation," CiiT International Journal of Biometrics and Bioinformatics, vol.4, no. 8, 2012.

[6] L. Biel, O. Peterson, L. Phillipson, and P. Wide " ECG analysis: A new approach in human identification", IEEE Transactions on Instrumentation and Measurement, 50(3) pp. 808–812, 2001

[7] S. Israel, J. Irvine, A. Cheng, M. Wiederhold, and B. Wiederhold "ECG to identify individuals. Pattern Recognition",38(1):133–142, 2005.

[8] Mikhled Alfaouri and Khaled Daqrouq, "ECG Signal Denoising By Wavelet Transform Thresholding" American Journal of Applied Sciences, pp: 276-281, 2008.

[9] Ayman Rabee And Imad Barhumi, "ECG Signal Classification Using Support Vector Machine Based On Wavelet Multiresolution Analysis", Information Science, Signal Processing And Their Applications (Isspa),11th International Conference pp: 1319 - 1323 , 2012.

[10] S. Banerjee, R. Gupta, M. Mitra, "Delineation of ECG characteristic features using multi resolution wavelet analysis method", Measurement, pp: 474–487, 2012.

[11] K.Sasirekha, K.Thangavel and K. Saranya, "Cryptographic key generation from multiple fingerprints", International Journal of computational intelligence and informatics,vol 2,issue 2, 2013.

[12] Fu B, Yang S, " Multibiometric cryptosystem: Model structure and performance analysis" IEEETransactions on Information Forensics Security, vol 4(4), 867–882, 2009.

[13] Rai, H.M. ; Trivedi, A. ; Shukla, S. ; Dubey, V. "ECG Arrhythmia Classification Using Daubechies Wavelet And Radial Basis Function Neural Network", Engineering ,pp: 1 – 6, 2012.

[14] Khanwahi, " Low Complexity Implementation Of Daubechies Wavelets For Medical Imaging Applications" Discrete wavelet Transforms -Algorithms And Application, 2012.

[15] Hyejung Kim ,Yazicioglu, R.F. , Merken, P. , Van Hoof, C.and Hoi -Jun Yooecg " Signal Compression And Classification Algorithm With Quad Level Vector For ECG Holter System" InformationTechnology In Biomedicine, IEEE Transactions On Volume: 14 , Issue: 1, pp: 93 – 100, 2010.

[16] Patil, P.B. , Chavan, M.S, "A Wavelet Based Method for Denoising Of Biomedical Signal Pattern Recognition" , Informatics And Medical Engineering (Prime), pp:278-283, 2012.

[17] Sunil kumar singhla and ankil sharma "ECG as bometric in the automated word" ,international journal of computer science and communication ,pp 291-283, 2012.

[18] R. Subash Chandra Boss, K. Thangavel and D. Arul Pon Daniel, "Automatic Mammogram image Breast Region Extraction and Removal of Pectoral Muscle", International Journal of Scientific & Engineering Research, vol. 4, issue 2, 2013.

[19] Hankerson D and Menezes A et al. .Guide to elliptic curve cryptography, Chapter 3, Springer, 75–95, 2004.