2nd Int'l Conf. on Electrical Engineering and Information & Communication Technology (ICEEICT) 2015
Jahangirnagar University, Dhaka-1342, Bangladesh, 21-23 May 2015

ECG Based Biometric Human Identification Using Chaotic Encryption

Md. Jahiruzzaman, A. B. M. Aowlad Hossain
Dept. of Electronics and Communication Engineering
Khulna University of Engineering and Technology, Khulna-9203, Bangladesh
mdjahiruzzaman@gmail.com, aowlad0403@ece.kuet.ac.bd

Abstract—**Biometric identification provides a reliable performance on recognition of identity for different security and authentication management problems. With the development of technology, the privacy and security is the main concern as technology can be falsified. In recent decades biometric traits are the trusted choice to the researchers and there are strong documentations on biometric traits like human electrocardiogram which is the time changing electrical impulse signal passing through heart is able to use for identity subject identification. In this work, an analytic and serviceable analysis of the ECG for human identification is presented. A new approach based on chaotic encryption (CE) of continuous wavelet transformed (CWT) ECG signal has been proposed. The CWT used here to obtain similarity pattern of each individual and CE of the CWT decomposed signal used for subject identification. The proposed approach has been tested using 11 different subjects ECG signal available at MIT-BIH arrhythmia database. The obtained results show that the identification rate is 96.82%. The findings of this study can be helpful to develop effective biometric human identification system.**

Keywords- Biometric identification; electrocardiogram; continious wavelet transform; chaotic encryptition.

I. INTRODUCTION

Human identification is platform where the identity of an individual need to be determined and has variety application areas in security management, medical records management, private document protection, mobile health monitoring, government and forensic applications etc. Besides biometric is the only authentic method that provides reliable performance over any conventional methods of individual identification based system like physical key, ID cards, secret password and code lock entrance system [1]-[6]. Biometric human identification process can be considered as a pattern recognition problem. Biometric traits are the physiological as well as geometrical or behavioral or both characteristics of an individual. In recent years, the uses of biometric modalities are gaining attraction to the researchers for security and authentication purpose because of its greater reliability against falsification. But most of the conventionally used biometric methods are not robust, some methods provides lower recognition accuracy and required high resolution computer vision system such as face is sensitive and requires high resolution computer vision, finger print can be recreated using latex etc. and in practice it is more difficult to identify a moving object [2]-[6].

ECG has been used for diagnosis and monitoring hearts all over a century. It is a time varying bioelectric quantity generated by the electrical activity of the heart. It is a fast growing choice to the researchers for biometric purposes because of its highly reliable fundamental characteristics such as it can be found in all living humans, has the inter-individual variability, has the authentication capabilities besides it can be recorded easily by attaching a group of electrodes on human body such as chest, arms, legs, fingers etc. The fundamental purposes of ECG is to recognize the biometric abnormality and the cardiac functionality of an individuals besides it can be easily extracted and can be implemented on biometric human identification [2]-[13]. Every individuals manifest unique characteristics patterns in their ECG which varies due to the different anatomy, physiology, geometrical condition, position and size of the heart that makes ECG to be considered as a biometric trait. Besides it is a live indicator object and provides heart rate, rhythm and morphology level of a subject [12]-[16].

Biometric human recognition is an active research work for last three decades. Several authors emphasizes ECG as biometric identification tool on the basis of two category of detection, the analytic based fiducial detection which considered as the regions of interest of detected points of heartbeat and the non-fiducial detection [2]-[6]. Agrafioti *et al.* [3] and Plataniotis *et al.* [4] demonstrated an autocorrelation with discrete cosine transformation based non-fiducial biometric human recognition system. Biel *et al*. [5] first demonstrated that ECG can be a useful tool for biometric identification. The system extracted a set of temporal and amplitude features. The limitation was the systems features extraction method is not automated. Isreal *et al.* [6] demonstrated a complete biometric identification system including the preprocessing, features extraction and classification. A decision based neural network approach for template matching applied in [7] for subject identification. A chaos based individual identification based on ECG was described in [8].

Biometric identification using ECG is a challenging task for recognition of same subject as human ECG signal inherently varies at different heartbeat due to cardiovascular condition of the heart [16]. Therefore, ECG based biometric identification study still demands lot of research works to do. In this work, we propose a non-fiducial based approach where there is no need to detect the fiducial point from the signal contents and no need to extract the analytical features of the ECG signal. The

978-1-4673-6676-2/15/$31.00 ©2015 IEEE

proposed approach lean on the chaotic encryption estimation derived from the continuous wavelet transformed ECG signal and comparing this estimated sequence with the CE identification systems database IDs. The experimentation outcome is expected as reliable and efficient.

II. METHODOLOGY

The proposed biometric system contains three major steps: the preprocessing, feature extraction and identification of subject. The preprocessing involves the de-noising and smoothing the raw ECG data. The features extraction CWT estimation, chaotic encryption estimation from CWT ECG signal and the CE length and identity bit sequence extraction. The identification of individual subjects are done by the CE identification system. Figure 1 shows the flow diagram of the proposed approach.

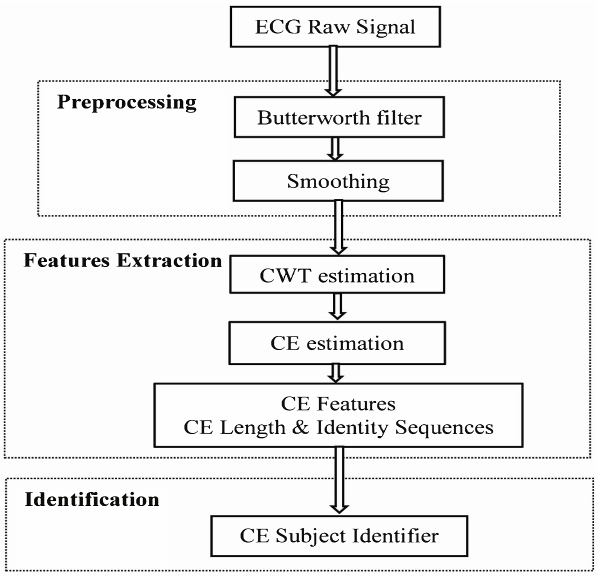


Figure 1. Flow diagram of the proposed system

A. *Overview of ECG Signal and its Preprocessing*

ECG is the electrical representation of cardiac activity. Each heart beat is triggered by an electrical impulse generated by a special sinus node in the atrium [17]. An ECG signal is composed of a group of amplitude and temporal components. Figure 2 describes the basic structure of a normal ECG heartbeat signal. A typical ECG of a healthy object consists of three main components the P components, the QRS complex and the T components. Each of these components has its own characteristic, behavior and origin. The P components a low frequency signal below 10-15 Hz, generated due to the sequential depolarization of the right and left atria and stability less than 120 milliseconds. The QRS complex is a largest amplitude component, frequency signal in the range 10-40 Hz, generated due to the depolarization right and left ventricles and stability in the range of 70-110 milliseconds. The T component is generated due to the repolarization of the ventricles and stability greater than 300 milliseconds. The heart rate variability is completely depends on the temporal component ST interval. The duration of ST is less if the heartbeat is fast and vice versa.

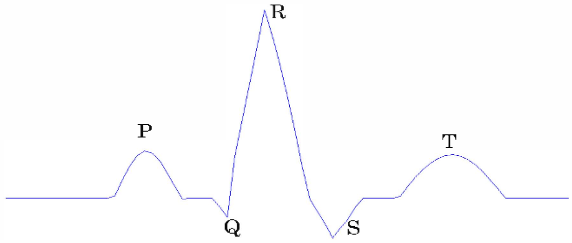


Figure 2. A typical ECG signal for one heartbeat

The raw ECG data consists of low frequency noise component like baseline drift due to respiration (less than .5Hz), high frequency noise component caused by power line interferences (not more than 50 to 60Hz), electromyographic and electrode motion artifacts noise component. Before features extraction and classification this noise components need to be removed for better performance of the proposed system. We plan to use a third order Butterworth filter for de-noising the noise corrupted ECG signal. The objective of this band pass filter is to allow signal in the range 0.5 to 45 Hz while the remaining noise component will be removed.

B. *Features Extraction Using CWT and Chaotic Encryption*

Wavelet transform is a time-domain representation which has a wide range of applications in signal processing such as data compression, de-noising, image compression and pattern recognition. In this work, we choose CWT for suitable features extraction.

CWT uses internal products to measure the similarity between a signal and a mother wavelet function ψ. It compares the signal to shifted, compressed or stretched versions of a wavelet at various scales parameter, a>0 and position b, the CWT coefficients are effected by the scale, position parameter and the wavelet which implied.

$$C(a,b;x(t),\psi(t)) = \frac{1}{\sqrt{a}}\int_{-\infty}^{\infty} x(t).\,\psi^{*}(\frac{t-b}{a})dt \tag{1}$$

Here, $\psi^{*}(t)$ is the complex conjugate of the wavelet function ψ(t), and $x(t)$ is the analyzed signal. We use morlet wavelet which is defined by the mother wavelet $\psi(t)$, provide better performance for extracting the CWT signal.

$$\psi\ (t) = \frac{1}{\sqrt[4]{\pi}}(e^{i\omega_0 t} - e^{-\frac{\omega_0{}^2}{2}})e^{-\frac{t^2}{2}} \tag{2}$$

Here, ω_0 is denoted as the central frequency of the mother wavelet. Using CWT signal to extract the following features.

The extracted CWT data execute an inter-individual repeatability of signal response for each subject. We apply a chaotic encryption technique on it to find a significant result on subject identification. This CE technique follows an algorithmic step on finding the chaotic information. This CE technique records the local maxima of a selected data as 0 or 1. It is found by observing the current positive/ negative peaks with the following positive/ negative peaks weather it is greater than or not. If found greater than then assign 0 otherwise it will assign 1. Let P(1), P(2), P(3), P(4), ... are positive peaks and N(1), N(2), N(3), N(4), ...are negatives peaks.

The chaotic encryption technique generally used in digital secure communication system [18] and there two threshold parameters are considered. In our implementation we neglect this consideration as the following

- If *P(i)>P(i+1)* or *N(i)>N(i+1)* then assign 0 in that *P(i)* or *N(i)* position of the sequence (here, *i*= 0, 1,…..,*Z*).
- If *P(i)=<P(i+1)* or *N(i)=<N(i+1)* then assign 1 in that *P(i)* or *N(i)* position of the sequence and so on.

We plan to use this estimated chaotic encryption information as a means for establishing a human identification system. From the extracted sequence we can be found two major features. One, the chaotic encrypted length of a certain duration which match with the CE length of that duration in different time interval for the same subject. Two, we can be established a unique bit sequence derived from the CE sequence for each individual, which repeats to the same subject but will not be presented in the CE sequence of different subjects.

C. Subject Identification

The chaotic encryption technique is independent to subject heartbeat analytical or fiducial detection requirements. In our study, the applied CE technique has two features as describe earlier in the above sub-section. Figure 3 shows the flow chart of the proposed CE based identification technique. Firstly, we insert a 5 seconds window of a subject. The window data generate a bit sequence by CE technique and store to the CE response block. This chaotic bit sequence is stored to the CE length block and directed to the database where individual information is stored. The database consist two information of an individuals, CE bit length range and corresponding subject ID's. The database provides those subjects ID which matches with the CE bit length range to the ID matching block. The ID matching blocks matches the ID with the chaotic encryption bit sequence provided by the CE response block. If the operation match with one of ID's then the corresponding ID will provide to the subject ID block. Otherwise, the system will ask for another window of that subject.

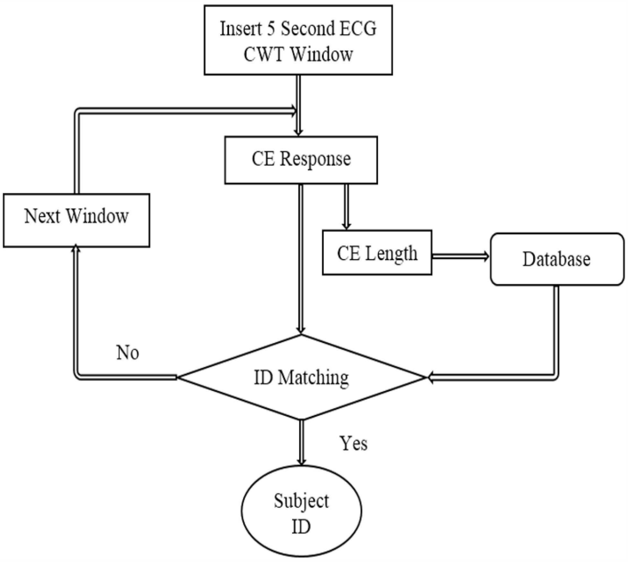
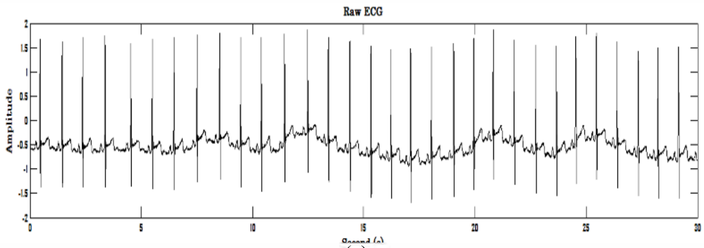


Figure 3. Flow chart of CE based identification system

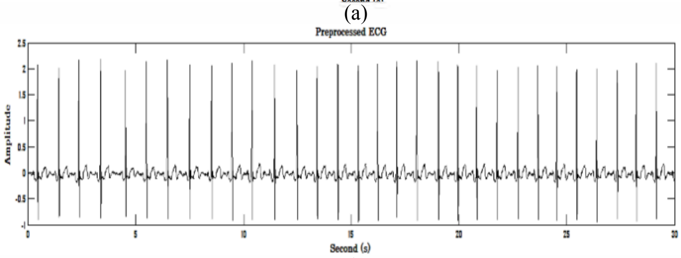
III. Result Analysis and Discussions

The MIT-BIH arrhythmia database has been used in this study. The database consists of two channel ambulatory ECG recording obtained from 47 subjects (25 man and 22 women) studied by the BIH arrhythmia laboratory. This database offer a record of 30 minute samples for each subject with a digitalized rate of 360 samples per second per channel [19]. In this paper, we work on 11 subject record for biometric identification and partition each record into 360 windows; each window contains 5 second data.

We have used the Butterworth filter for removing the low and high frequency noise components from the original data. The preprocessing was completed smoothing the data by taking an average of 200 samples window and add the new upcoming window. Figure 4 depicts a 30 second preprocessed ECG data of a subject.



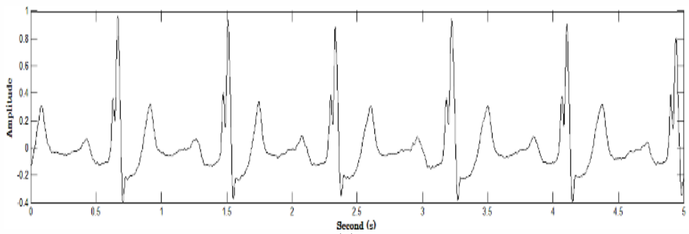
(a)



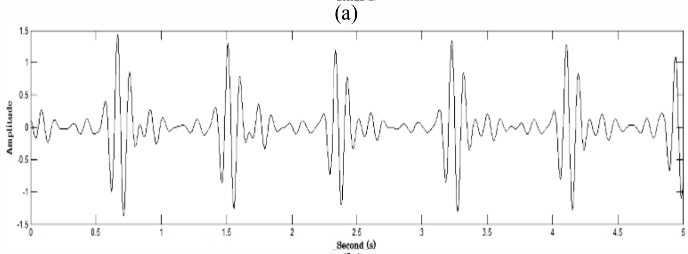
(b)

Figure 4. Preprocessing of signal (a) original signal, (b) preprocessed signal

Figure 5 shows the two different subjects 5 second window CWT data extraction from same database MIT-BIH arrhythmia. In this figure, we observe that the data set of same subject characteristic repeats due to their inter-individual behavior of electrocardiogram and this characteristic has been obtained due to the continuous wavelet transform analysis.



(a)



(b)

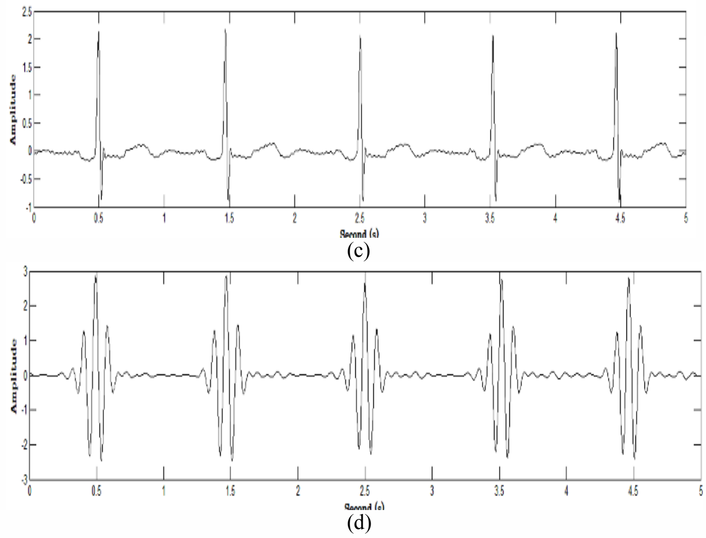


Figure 5. (a) and (c) 5 seconds preprocessed signal window of two different subject and (b) and (d) are their CWT reponse respectively

A 25 seconds CE bit sequence is derived and the selected orange block indicates a 5 seconds encrypted bit sequence in the Fig. 6. There are two observations on extracting the CE response. Firstly, considering a 5 second window it is observed that an approximately equal number of bits are generated by an individual in different time. For example, the selected block bit number will be almost the same for another window of same subject as shown in the Fig. 6. Then, a particular bit sequence is repeated (as indicated the blue color bit sequence) after some period of time for an individual.

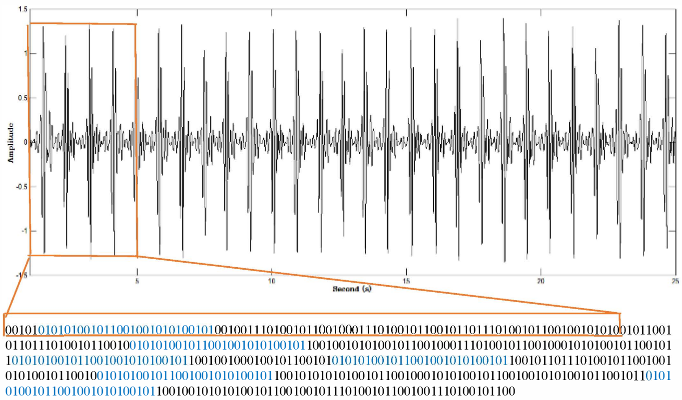


Figure 6. Chaotic encrypted (CE) bit sequence representation of a subject's 25 secondsCWT ECG data

Table. I describes a contingency matrix table where the CE technique features are used. We can found the rate of sensitivity, specificity and accuracy of the system by investigating this table. Though the CE length range may confuse with other subjects but the advantage of its, is it helps the identifier to check with those ID within the CE length range with the chaotic encrypted sequences. This makes this system more efficient, identical and less time consuming. By investigating this experiment we found a CE length range identification rate up to 100% and subject identification rate of 96.8%. Table. II depicts the performance of CE identifier.

TABLE I. PERFORMANCE OF CE TECHNIQUE

	Known Subject											
	Sub	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***
Detected Subject	***1***	20	0	0	0	0	0	0	0	0	0	0
	2	0	19	0	0	1	0	0	0	0	0	0
	3	0	0	20	0	0	2	0	0	0	0	0
	4	0	0	0	20	0	0	0	0	0	0	1
	5	0	0	0	0	18	0	0	0	0	0	0
	6	0	0	1	0	0	19	0	0	1	0	0
	7	0	1	0	0	0	0	19	0	0	0	0
	8	0	0	0	0	0	0	0	20	0	0	0
	9	0	0	0	0	0	0	0	0	20	0	2
	10	0	0	1	0	0	1	0	0	0	20	0
	11	0	0	0	0	0	0	0	0	0	0	18

The performance of this classification system can be evaluated in terms of sensitivity, specificity and accuracy.

- Sensitivity: It is the measurement of true positive ratio.

$$Sensitivity \;= \frac{True\ Positive}{True\ Positive + False\ Negative}$$

- Specificity: It is the measurement of true negative ratio.

$$Specifiity \;= \frac{True\ Negative}{True\ Negative + False\ Positive}$$

- Accuracy:It is the measurement of correct classification

$$Accuracy \;= \frac{TP\ +\ TN}{TP + FN + TN + FP}$$

TABLE II. PERFORMANCE OF CE IDENTIFIER

Sensitivity	Specificity	Accuracy
96.82%	96.18%	96.89%

IV. CONCLUSIONS

We have presented a new approach for ECG based biometric human identification system using chaotic encryption of continuous wavelet transformed ECG data. The self-similarity finding capability of CWT is used to find effective bit pattern for encryption. The chaotic encryption of CWT data gives a very small length bit pattern and uses of only two features shows an excellent result. Therefore, this simple technique can be realized in embedded system with reasonable cost. Whereas, most of the existing systems are image based and hence require high resolution computer vision system. The obtained results of the proposed technique show that subject identification rate is 96.8% for 11 subjects of MIT-BIH arrhythmia database. As our future work, we are trying to include more suitable feature to increase the performance of the proposed approach considering more subjects. Though the applied Butterworth filter perform well on the raw ECG signals of MIT-BIH arrhythmia database, we also plan to test the system using more noise incorporated signal as well as compare with other filters to choose the more effective filtering approach in support of the promising chaotic encryption part. We believe the findings of this study will be helpful to develop simple and effective biometric human identification system.

REFERENCES

[1] F. Agrafoiti, F. M. Bui, and D. Hatzinnakos, "Medical boimetrics in mobile health monitoring," Security and Communication Networks, vol. 4, no.5, pp. 525-539.

[2] Y. Wang, F. Agrafoiti, D. Hatzinnakos, and K. N. Plataniotis, "Analysis of human electrocardiogram for biometric Recognition," EURASIP Journal on Advances in signal processing, pp. 1 -11, 2008.

[3] F. Agrafoiti, and D. Hatzinakos, "ECG biometric analysic in cardiac irregularity conditions," Signal, Image and Video Processing, vol. 3, no. 4, pp 329-343, 2009

[4] K. N. Platantinos, D. Hatzinakos, and J. K. M. Lee, "ECG Boimetric Recognition Without Fiducial Detection," in Procedings of Biometric Symposium (BSYM '06), September 2006, USA.

[5] L. Biel, O. Pettersson, L. Phillipson, and P. Wide, "ECG Analysis: A New Approach in Human Identification," IEEE Transaction on Instrumentation and Measurement, vol. 50, no. 3, pp. 808-812, June 2001.

[6] S. A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold, and B. K. Wiederhold, "ECG to Identify Individuals," Pattern Recognition, vol. 38, no. 1, pp. 133-142, 2005.

[7] T. W. Shen, W. J. Tompkins, and Y. H. Hu, "One-Lead ECG for Identity Verification," in Proceeding of Second Joint EMBS/BMES Conference, pp. 62-63, 2002.

[8] C. K. Chen, C. L. Lin, and Y. M. Chiu, "Individual identification based on chaotic electrocardiogram signals," in Procedings of 6th International Conference on Industrial Electronics and Applications, pp. 1765-1770, 2011.

[9] H. P. Silva, A. Louren□o, A. Fred, and A. K. Jain, "Finger ECG Signal for User Authentication: Usability and Performance," in Proceedings of IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), pp. 1-8, 2013.

[10] R. Mizutani, and T. Matsumoto, "Evaluation security of a simple interactive human identification scheme," IEICE Transaction on Fundamental Electronics, Communication and Computer Science, col. E78A, no. 5, pp. 577-578, 1995

[11] N. Venkatesh, and S. Jayaraman, "Human Electrocardiogram for Biometric using DWT and FLDA," in Procedings of International Conference on Pattern Recognition, pp. 3838-3841, 2010.

[12] A. K. Jain, R. M. Bolle, and S. Pankanti, Biometric: Personal Identification in Networked Society, Kluwer Academic, 1999..

[13] Y. N. Singh, and P. Gupta, "ECG to Individual Identification," in Proceedings of 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS '08), pp. 1–8, October 2008.

[14] R. Hoekema, G. J. H. Uijen, and A. V. Oosterom, "Geometrical aspects of the individual variability of multilead ECG recording," IEEE Transaction on Biomedical Engineering, vol. 48, no. 5, pp. 551-559, 2001.

[15] A. K. Jain, A. Roos, and S. Prabhakar, "An introduction to biometric introduction," IEEE Transaction on Circuits and Systems, vol. 14, no. 1, pp. 4-20, 2004.

[16] M. Li, and X. Li, "Verification based ECG biometrics with cardiac irregular conditions using heartbeat level and segment level information fusion," in Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 3769 – 3773, May 2014.

[17] O. Sayedi, and M. B. Shamssollahi, "Multiadaptive Bionic Wavelet Transform: Application to ECG Denoising and Baseline Wandering Reduction," EURASIP Journal on Advances in Signal Processing, pp. 1-11, Volume 2007.

[18] T. I. Chien, and T. L. liao, "Design of secure digital communication systems using chaoyic modulation, cryptography and chaotic synchronization," Chaos, Solitons and Fractals, vol. 24, pp. 241-255, 2005.

[19] G. B. Moody, and R. G. Mark, "The impact of the MIT-BIH arrhythmia database," IEEE Engineering in Medicine and Biology, pp. 45-50, 2001.