ELECTROCARDIOGRAM FOR BIOMETRIC VERIFICATION

Shweta[1], Puneet Mishra[2], Ravish Garg[3]
Department of Biomedical Engineering, Guru Jambheshwar University of Science & Technology, Hisar, Haryana, India-125001

Abstract: Biometric is a technique of identifying/verifying the subject based on their physiological and behavioral characteristics, being used extensively for security purpose in modern technological era. The limitation of conventional biometrics is that they can be challenged via exploiting use of gummy fingers, artificial iris, voice mimicking etc. These vulnerable practices make the system approachable for spoof attacks, and this motivates for the development of novel full-proof biometrics such as Electrocardiogram, Electroencephalogram, Electromyogram etc., because of universality, measurability, uniqueness and unfeasibility to mimic. In the present work, Electrocardiogram has been attempted to be used as biometric taking recorded Electrocardiogram database of 25 subjects, and different features like fiducial and non-fiducial points are extracted. Fiducial features extracted are Average Heart Rate, Average Peak Distance and Extreme Distance Points, and Non-fiducial features extracted are Activity, Mobility, and Complexity. Error rates, False Acceptance Rate (FAR) and False Rejection Rate (FRR) and Genuine Acceptance rate (GAR), were derived from extracted features and used as probability to verify the subject. Results illustrate that a probable accuracy of verification of 97.60% is achieved in fiducial features and probable accuracy of verification of 96% is achieved using non-fiducial features. From which, it can be concluded that ECG based biometric can be used as stand alone or can be easily cascaded with other biometric to enhance the reliability and security of the system in futuristic application.

Keywords: Biometric, Electrocardiogram, Fiducial Points, Non-Fiducial Points, False Acceptance Rate, False Rejection Rate.

I. INTRODUCTION

Recently, Biometric technology has attracted the attention of researchers as this is a fast developing field of information security, gradually entering into all spheres of human activity [1]. Biometrics provides an automatic method for the authentication of a person based upon his physical or behavioral features, such as voice, face, retina, gait, iris or fingerprint. Automated human authentication system has promising applications in many different areas where the identification of a person needs to be determined [2]. Greek words "Bio" means life and "metric" means measure is the origin of term Biometric [3, 4]. Measurement and statistical analysis of person's characteristics is called Biometrics [5]. Biometric system said to be perfect if the system is universal, easily measurable and permanent, depending on purpose and application of biometric. The various physiological/ behavioral characteristics of a person are shown in Fig.1.

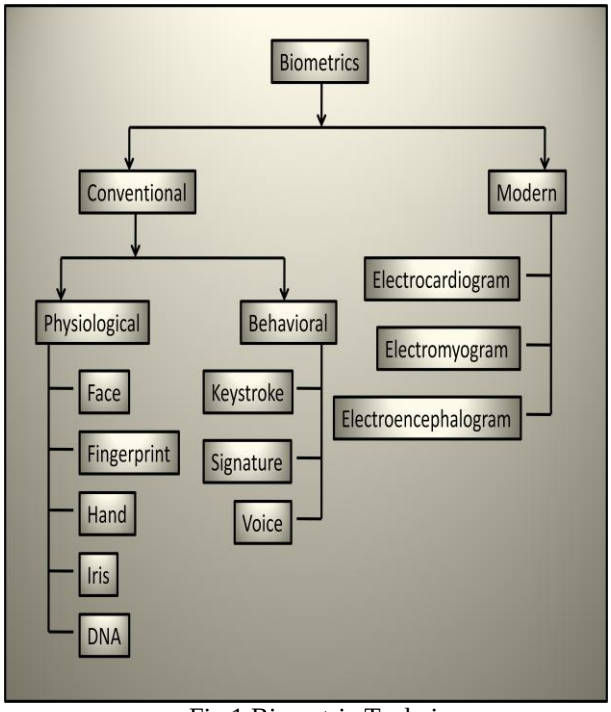

Fig.1 Biometric Techniques

Conventional biometrics like fingerprint has a unique pattern of ridges and furrows on fingertip surface [6]. However, fingerprint can be spoofed using gummy finger, also, skin problem or scar/cuts or any heredity problem related to skin may cause errors in measurement of fingerprint scan [7]. Whereas, ECG cannot be mimicked and remain same in different situations except diseased ones.

Ear biometric can be used as biometric by matching certain point's distance on pinna from designated landmarks located on ear [8]. Cumming et.al. [9] discovered ear matching biometric with 99.6% accuracy. Limitations of this system is that a person without ear cannot be enrolled. Whereas, using ECG the system adapts only for liveness detection of living subjects.

DNA (Deoxi ribonucleic acid) is also used as Biometric because DNA carries genetic information and is unique to every individual. It has certain limitations where twins share the identical DNA. Whereas, ECG can be used because no two persons have same ECG pattern [10].

Table 1 demonstrates the comparison between few existing biometric techniques on the basis of three parameters of evaluation (based on characteristic evaluation) i.e. High (H), Medium (M) and Low (L) [8, 10].

Table 1 Comparison of Conventional Biometric Techniques [8, 10, 11, 12]

Modality	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability
Fingerprint	M	H	H	M	H	M
Voice	M	L	L	H	L	M
Hand Geometry	M	M	M	H	M	M
Palmprint	M	H	H	M	H	M
Face	H	L	M	H	L	H
Iris	H	H	H	M	H	L
Signature	L	L	L	H	L	H

From Table 1, it can be seen that mentioned biometrics have a medium level of universality except iris and face however, iris and face biometric can be spoofed using superior quality image of iris; also, it employs expensive measurement device [8, 10]. As the acceptability of face and signature biometrics is high compared to remaining biometrics, but it has limitations of image resolution, illumination during capture, data storage, and interference due to glasses [8] but there is no such limitation in modern biometrics which are based on biosignals. Overall acceptability is also medium except signature and face. Face can be mimicked using mask, signature can be copied, but ECG can neither be copied nor can it be simulated. Howsoever, the individuality of above biometrics has been challenged [13] with recording units versus proportion of the population. Such circumvented incidence gives birth to the development of newer biometric techniques such as Electrocardiogram (ECG), Electromyogram (EMG), and Electroencephalogram (EEG) etc. ECG biometrics gives liveliness detection [14], however, techniques based on biosignals are possible to falsify theoretically [15] by simulating ECG signal but it may be difficult to replicate ECG at sensor level. There are certain limitations of biometric based on biosignals as they varies in cardiac conditions like hypertension, arrhythmia [16].

Electrocardiogram (ECG) as Biometric

Electrocardiogram is a graphical representation of electrical activity of the heart [17]. A typical waveform of an ECG has P wave, QRS complex, T wave and U waves as shown in Fig.2.

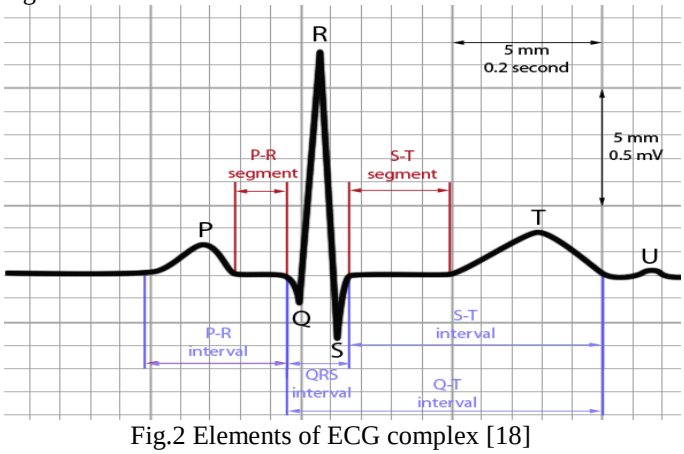

Fig.2 Elements of ECG complex [18]

The main advantages of ECG as biometric are liveliness detection, unique ECG pattern and structure of ECG complex [19]. ECG as biometric has been investigated with varying database and subject size. The signals were acquired and processed to extract the vital features from it. The attributable features could be fiducial or non-fiducial. The extracted features are fed to the classifier for person authentication by matching the query sample with the database. ECG's QRS complex doesn't vary with time even with varying heart beat [20]. It was found that there was no change observed in person's ECG especially QRS complex over the time or long duration gap (one hour and six months duration) [21].

II. METHODOLOGY

The methodology for "ECG for Biometric Verification" adopted in present work is to create an ECG database, extraction of features from ECG database and development of Biometric verification.

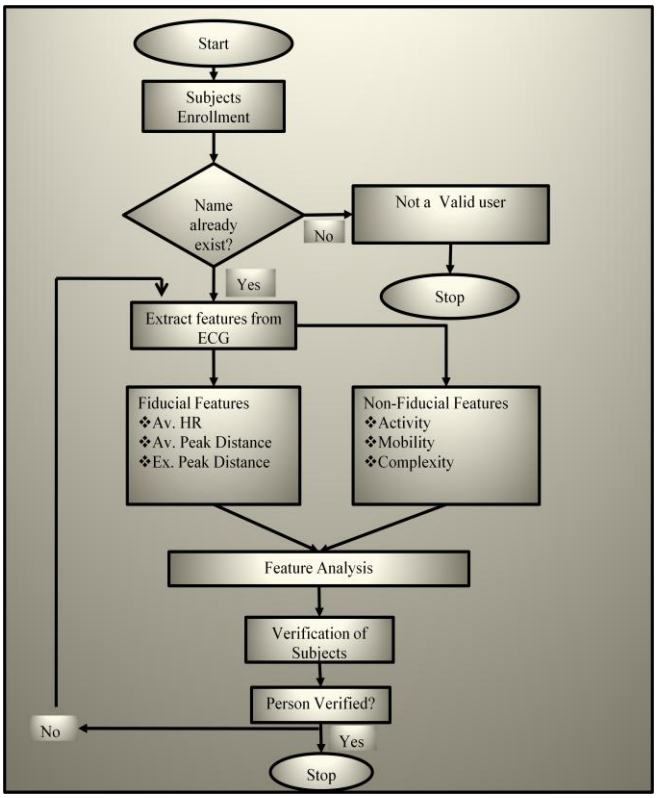

Fig.3 Flowchart of Verification system

Fig.3 shows the flowchart of verification system, where, first of all enrollment of subject is done, from there enrollment status of subjects is obtained. If subject enrollment status is not available, then process stops automatically and it asks for re-enrollment. Once the subject is enrolled the process of features extraction starts.

The features are extracted from fiducial and non-fiducial points. Fiducial features are Average Heart Rate, Average Peak Distance and Extreme Distance Points whereas; non-fiducial features are Activity, Mobility and Complexity (Hjort Parameters). Vigorous analysis of features is done to carry out verification process. Once the subject is verified

then the process completes otherwise, the process of feature extraction repeated once again.

ECG Data Acquisition

In this work, ECG standard database has been used for feature extraction and feature evaluation. The database is available as free source from internet [22]. Each ECG signal comprised of 20 second long epoch which is sampled at a sampling frequency of 500 Hz with 12-bit precision. The minimal waveform range was ±10 mV. In the present work, 25 subjects have been selected for the person verification with 05 trials per subjects with an epoch length of 10 seconds; thus, producing the sample length of 10000. Thus, the total ECG sample size comprised 25 × 5 i.e. 125 for person verification.

Feature Extraction

The features were extracted using MATLAB software tool, a MATLAB 2009b (version 7.9.0), a propriety of Mathworks Laboratory, USA. In this work, the features with hybrid feature model i.e. considering fiducial as well as non-fiducial features from ECG have been selected. The Fiducial features are Average Heart Rate, Average Peak Distance and Extreme Peak distance points. The Non-Fiducial features are Activity, Mobility and Complexity i.e. Hjorth parameters [23].

Performance of Verification

The performance of any biometric is measured in terms of error rates i.e. False Rejection Rate (FRR) and False Acceptance Rate (FAR) [24]. FAR is the positive claim of enrollment by the biometric system that a template stored in its database is from the same person that has just presented a sample, when in fact it is not [25]. FRR is the positive conclusion by the biometric system that a template stored in its database is not from the same person that has just presented a sample, when in fact, it is [25].

Calculation of False Rejection Rate (FRR)

Selected first 05 samples for training and testing whose Mean is calculated and stored in database. In order to test the 1st trial, Percentage Deviation (range) calculated from the Mean value i.e.

$$PD = \frac{M-T}{M} * 100 \qquad (1)$$

Here, PD is Percentage Deviation, M is Mean Value, T is Test value

Repeat the steps for Percentage Deviation calculation for remaining trials. The values which lie above or below the range of variation is rejected by the system; which gives the FRR rate.

Calculation of False Acceptance Rate (FAR)

Selected first 05 samples for training and testing whose Mean is calculated, then a variation of 10% of mean (named it as X) has been considered. Calculated the lower variation value (Mean – X) and higher variation value (Mean + X).

$$Total\ number\ of\ cells\ (T) = Total\ trials - Trials\ of\ 1\ subject \qquad (2)$$

Compare and count the observation that lie between the lower and upper variation and name it as 'Y'.

$$FAR = \frac{Y}{T} * 100 \qquad (3)$$

Where, Y is counted observation that lies between the lower and upper variation, T is total number of cells.

Performance Evaluation of Features

The performance of each feature is calculated in terms of error rates (FAR and FRR) and GAR (Genuine Acceptance Rate). They are measured with the standard variation of 10% (operator's

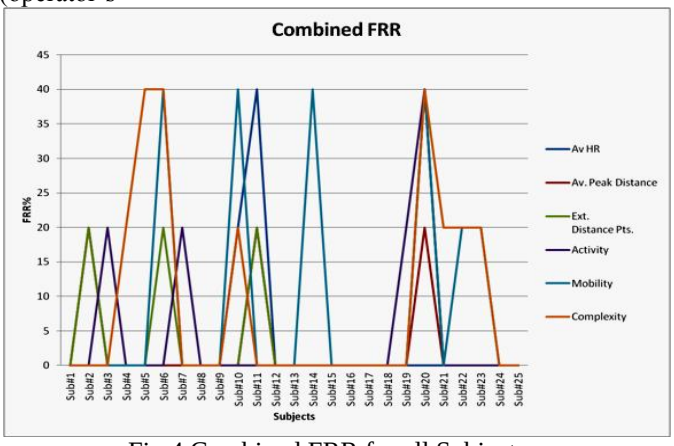

Fig.4 Combined FRR for all Subjects

Selection), which could be varied with the demand and security needs of the biometric purpose. The computation of error rates have been made in Microsoft Excel.

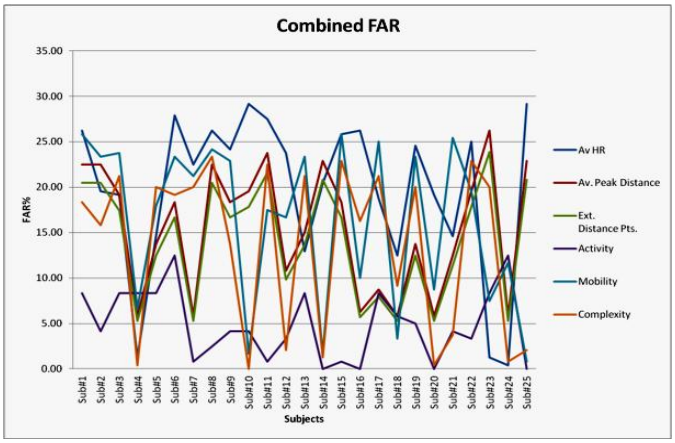

Fig.5 Combined FAR for all Subjects

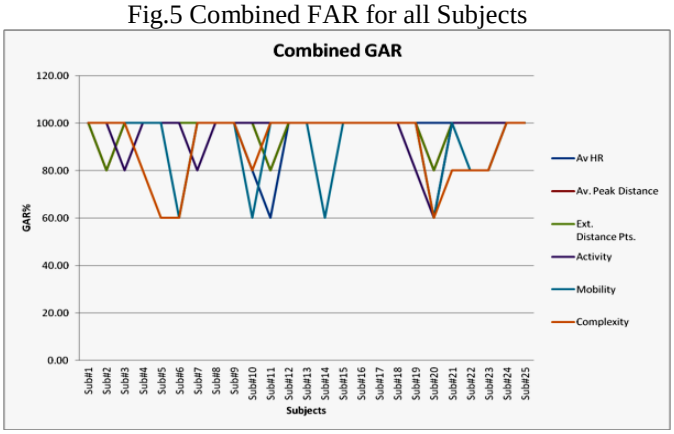

Fig. 6 Combined GAR for all Subjects

While, comparing the system accuracy (as shown in Fig. 4, 5 and 6), it can be seen that lower mean FRR (i.e. 2.40 to 8.80) has been obtained which is ideal to use for person verification. However, this costs in higher FAR (i.e. 4.90 to 19.72). The probable mean FAR & FRR from all the 25 subjects has been shown in Table 2.

Table 2 Mean FAR, FRR and GAR of Combined Feature set

Features	Mean FAR%	Mean FRR %	Mean GAR%
Av. Heart Rate	19.72	2.40	97.60
Av. Peak Distance	15.47	2.40	97.60
Ex. Distance Pts.	14.06	4.00	97.60
Activity	4.90	4.00	96.00
Mobility	16.45	8.00	92.00
Complexity	13.55	8.80	91.20

It can be seen from Table 2, maximum Genuine Acceptance Rate (GAR) of 97.60 (with FRR of 2.4%) achieved using fiducial features such as Average heart rate, Average peak distance and Extreme distance points. Whereas, GAR of 96% is achieved using activity parameter of Hjorth with FRR of 4% and FAR of 4.90%. charactistics.

III. CONCLUSION

In this paper, Electrocardiogram based approach for the biometric verification has been presented. For verification, few fiducial and non-fiducial features were extracted and the probable accuracy of verification has been found to be 97.60% and 96% respectively. This illustrate, ECG can be used for biometric verification/identification and the system could be used as standalone or multi-modal for authentication; Where, ECG biometric can also be used with other biometric modalities (fingerprint, iris, palmprint, facial, ear biometric etc.) to increase the reliability, robustness and anti circumvention to the system.

REFERENCE

[1] Saechia S., Koseeyaporn J. and Wardkein P., "Human Identification System Based ECG Signal", Proc. TENCON IEEE Region 10, 2005, 1-4p.

[2] Biel L., Pettersson O., Philipson L. and Wide P., "ECG Analysis: A New Approach in Human Identification", IEEE Trans. Instrum. Meas., 50(3), 1999, 557–561p.

[3] "Biometric Technology Application Manual Volume 1: Biometric Basis", National Biometric Security Project, 1, 2008.

[4] Waymanin L. James, "Biometrics Now and Then: The Development of Biometrics Over the Last 40 Years", New York Times Article: "Technology, Recognizing the Real You", 1981.

[5] Chaudhari D. Rahul, Pawar A. Ashok and Deore S. Rakesh, "The Historical Development of Biometric Authentication Technique: A Recent Overview", International Journal of Engineering Research and Technology, 2 (10), 2013.

[6] Jain Anil, Ross Arun and Karthik Nandhakumar, "An Introduction to Biometric Recognition", Springer Science and Business Media, 2011.

[7] Fernando L. Podio, "Personal authentication through biometric technologies", IEEE Fourth International Workshop on Networked Appliances, 2002.

[8] Klokova A., "Comparison of Various Biometric Methods", 2011.

[9] Cummings A, Nixon M. and Carter J., "A Novel Ray Analogy for Enrolment of Ear Biometrics", IEEE Fourth Conference on Biometrics: Theory, Applications and Systems, 2010.

[10] Saini R. and Rana N., "Comparison of Various Biometric Methods", International Journal of Emerging Technologies in Computational and Applied Sciences, 2, 2014.

[11] Tatepamulwar C. B. and Pawar V. P., "Comparison of Biometric Trends Based on Different Criteria", Swami Ramanand Teerth Marathwada University, Nanded (M.S.) India.

[12] Tripathi K. P., "A Comparative Study of Biometric Technologies with Reference to Human Computer Interface", International Journal of Computer Application, 14, 2011, 10-15p.

[13] Pankanti S., Prabhakar S. and Jain A. K., "On the Individuality of Fingerprints", IEEE Trans. Pattern Anal. Machine Intell., 24(8), 2002, 1010-1025p.

[14] Foteini Afrafioti, "ECG in Biometric Recognition: Time Dependency & Application Challenges, 2011, 20-24p.

[15] Tsao Y. T., Shen T. W., Ko T. F. and Lin T. H., "The morphology of the electrocardiogram for evaluating ECG biometrics", Proc. 9th Int. Conf. e-Health Networking, Application and Services, Taipei, Taiwan, 2007.

[16] Smallwood Brown and Barber Layford Hose, "Medical Physics and Biomedical Engineering", 1, 2005, 521-540p.

[17] Goldberger A.L. and Goldberger E., "Clinical Electrocardiography: A Simplified Approach", 5 (1), 1994.

[18] Guyton and Hall, "Textbook of Medical Physiology", Harcourt India pvt., 10, 2000, 96-132p.

[19] Gutta S. and Cheng Q., "Joint Feature Extraction and Classifier Design for ECG Based Biometric Recognition", IEEE Journal of Biomedical and Health Informatics, 2015, 1-9p.

[20] Nemirko A.P. and Lugovaya T.S., "Biometric Human Identification based on Electrocardiogram", proc. of 12th Russian Conference on Mathematical Methods of Pattern Recognition, Moscow, 2005.

[21] Tatiana S. Lugovaya, "Biometric Human Identification based on ECG".

[22] ECG-ID Database, URL: https://physionet.org/physiobank/database/ecgiddb/;

DOA: 12 April 2016

[23] Hjorth, B., "EEG Analysis based on Time Domain Properties", Electroencephalogram Clin Neurophysioly, 29, 1970, 306-310p.

[24] Jain, A. K., Flynn, P. and Arun, A., "Handbook of Biometrics, 1st Edition", Springer, 2007.

[25] Simon Liu and Mark Silverman, "A Practical Guide to Biometric Security Technology", IEEE Computer Society, 2002, 27-32p.

