Grenze International Journal of Computer Theory and Engineering , Special issue

Database Evaluation of ECG Fingerprint and Face Multimodal Biometric System

Raju A S[1] and V Udayashankara[2]
[1]Research Scholar, SJCE, Mysore, India
asraju74@gmail.com
[2]Professor, SJCE, Mysore, India
v_udayashankara@sjce.ac.in

***Abstract*—This paper is concerned with the effective evaluation of multimodal biometric database and discusses data collection method with testing protocols, for Electrocardiogram (ECG), face and fingerprint biometrics of 50 individuals. Database of biometric images, and the numerical modules or templates derived from them, are often encrypted with the intension of inhibiting their compromise in bulk. But compromise of individual measures cannot always be prevented by protecting database and transmission channels because biometric measures, although privately owned, are sometimes publicly observable (e.g. a photo of a person's face can be taken with a camera or downloaded from a web page.). In general, biometric measures are not secret, even if it might be quiet complicated to acquire usable copies (e.g. ECG map) without cooperation of the person when used for security and privacy, biometric characteristics are more like public keys than private keys. Unlike public keys, however, biometric measures cannot be revoked if stolen or mimicked. Hence Multi-modal biometrics has gained considerable attention because they enhance the accuracy of biometric person authentication as well as security against attack. Combinations of such multi-modal biometrics are diverse: fingerprint and iris; iris and face ; face and ocular ; face and gait ; gait and the height . In this research paper, we proposed an alternative method for database privacy to authenticate a person for live-ness testing using multimodal biometrics such as ECG-Finger Print-Face in a reliable way as compared to unimodal biometric traits.**

***Index Terms*— Multimodal Biometric, Electrocardiogram, Fingerprint, Evaluation, Privacy.**

I. INTRODUCTION

Biometric verification system used for authentication purpose is becoming very common in corporate security systems, public security systems, consumer electronics and point of sale (POS) applications. Unimodal Biometric authentication systems using internal body characteristics (Figure 1) such as electrocardiograms (ECGs) and finger print etc have attracted significant attention among researchers [1]. But unimodal biometric systems using a single source of biometric information are often affected by some problems [2]. These problems include noise in sensed data, non-universality, upper bound on identification accuracy, and spoof attacks [3]. They make the error rates quite high and consequently it makes them unacceptable for deployment in security critical applications. For example, ECG represents graphical electrical activity of the heart and is believed to be distinctive among individuals and stable for a long period

Grenze ID: 01.GIJCTE.3.4.22

of time. The uniqueness of ECG signals between individuals is based on the fact that the generated signals are related to the shape or condition of the heart, age, and sex of the person [4]. The main challenge in implementation of authentication system using ECG characteristic is very time dependent. This makes it difficult to extract the exact same ECG characteristic each time even from the same user. Therefore, some of the problems of unimodal biometric systems can be addressed by designing systems that used multiple sources of biometric information [5].

Automatic and accurate identity validation is becoming increasingly critical in several aspects of our everyday lives, such as in financial transactions, access control, traveling, healthcare and many others. Traditional strategies for automatic identity recognition include items such as PIN numbers, tokens, passwords and ID cards. Despite the wide deployment of such tactics, the means for authentication is either entity-based or knowledge-based which raises serious concerns with regard to the risk of identity theft. Identity theft can take different forms - credit card fraud (17%), falsification of government documents (16%), utilities fraud (15%), employment fraud (13%) and others. Among these cases, true-identity theft constitutes only a small portion of the complaints, while ID falsification appears to be the greatest threat [2]. Unfortunately, the technology for forgery advances without analogous improvements on the security side.

Every biometric feature has its own strengths and weaknesses and deployment choices are based on the characteristics of the envisioned application environment. There is a major drawback with biometric recognition - as opposed to static PIN numbers or passwords, biometric recognition may present false rejection since usually no two readings of the same biometric modality are identical. Anatomical, psychological or even environmental factors affect the appearance of the biometric modality at any particular instance. For instance, faces may be presented to the recognizers under various expressions, different lighting settings or with occlusion (glasses, hats etc). This may introduce significant variability (commonly referred to as intra-subject or intra-class variability), and the challenge is to design algorithms that are robust to it. Provided intra-subject variability can be addressed with appropriate feature extraction, another important consideration is the robustness to circumvention and replay attacks. Circumvention is a form of biometric forgery - for example, falsified fingerprints that are reproduced from an original fingerprint. A replay attack is the presentation to the system of the original biometric feature from an illegitimate subject, for example pre-recorded voice playbacks in speaker recognition systems.

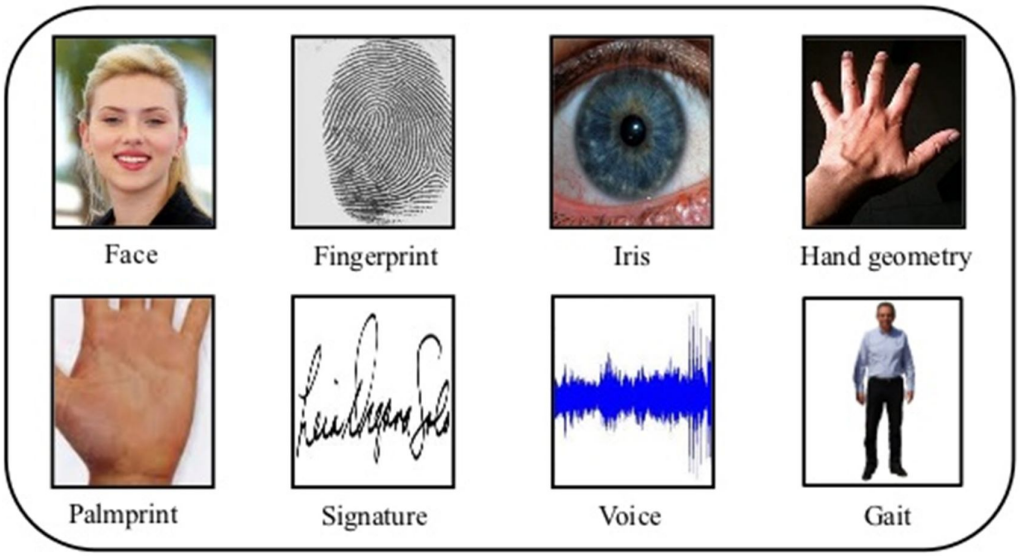

Figure 1. Characteristics Used For Biometric Recognition

II. Multimodal Biometric Database

This aims to provide a comprehensive study on the effectiveness of the proposed database of ECG, Face and Fingerprint multimodal biometric system.

Multimodal biometric systems are those which utilize, or are capability of utilizing, more than one physiological or behavioral characteristic for enrollment, verification, or identification. A biometric system is essentially a pattern recognition system. This system measure and analyzes human body Physiological characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements for authentication purposes or behavioral characteristics. The biometric identifiers cannot be misplaced. In spite of inherent advantages, unimodal biometric solutions also have limitations in terms of accuracy, enrolment rates, and susceptibility to spoofing. This limitation occurs in several applications domains, example is face recognition. The accuracy of face recognition is affected by illumination and facial expressions. The biometric system cannot eliminate spoof attacks. This new Multimodal biometric systems perform better than unimodal biometric systems and are complex even more popular also.

Most multimodal biometric studies assume different biometrics is independent therefore multiple biometric databases are combined in order to create virtual subjects instead of actually collecting multiple biometrics from each subject. However since in our work the ECG signals and fingerprint recordings are both collected from fingertips and face images for the same subjects, we will study the statistical dependency of ECG, fingerprint and face using a multibiometric database that we collected from 50 subjects. Furthermore we evaluate our proposed sequential ECG, fingerprint and face biometric system using our collected databases and in addition we evaluate the effectiveness of fusing the three biometric modalities under different variabilities, such as across-session, posture changes and heart rate variabilities. Finally the performance of the proposed system is compared with different commonly used score level fusion techniques namely the Weighted Sum Rule, SVM-based, Likelihood Ratio based.

Hence Multi-modal biometrics [6] has gained considerable attention because they enhance the accuracy of biometric person authentication as well as security against attack [7]. Combinations of such multi-modal biometrics are diverse: fingerprint and iris [8]; iris and face [9]; face and ocular [10]; face and gait [11, 12]; and face, gait, and the height [13][14]. In this research paper, we proposed an alternative method to authenticate a person using multimodal biometrics by using ECG-Finger Print-Face in a reliable way as compared to unimodal such as ECG, finger print and face.

III. MULTIMODAL ECG/FINGERPRINT/FACE DATABASE

ECG: The medical biometrics constitutes another category of new biometric modalities that encompasses signals which are typically used in clinical diagnostics [15]. Some examples of medical biometric signals are the electrocardiogram (ECG), phonocardiogram (PPG), electroencephalogram (EEG), blood volume pressure (BVP) and electromyogram (EMG). Medical biometrics has been actively investigated only within the last decade. Although the biometric property of these signals had been observed before, the complicated signal acquisition process and the waiting times were restrictive for application in access control. However, with the development of dry recoding sensors that are easy to attach even by non-trained personnel, the medical biometrics field flourished.

The rapid advancement over the last decade was supported by the fact that signal-processing tools had already been developed for diagnostic purposes. The main advantage of medical biometrics is the robustness to circumvention, replay and obfuscation attacks. If established as biometrics, then the respective systems are empowered with an inherent shield to such threats. Another advantage of medical biometrics is the possibility of utilizing them for continuous authentication, since they can provide a fresh biometric reading every couple of seconds. In addition, medical biometrics is one dimensional physiological signal, which ensures low computational effort. In this paper we present compact security scheme that provides the multilevel features which encompasses fingerprint and face fusing with the ECG in order to ensure the co-operation between the three concepts for the personal recognition and overcoming its individual limitations.

A. ECG Data Acquisition Materials and Methodology

The raw ECG signal acquired from different 50 individuals ITIE physiograph 2.0 manufactured bio-kit systems. The system includes data acquisition hardware with built-in universal amplifiers to record and condition electrical signals from the heart and other parts. the data acquisition system receives the signals from electrodes and transducers. The data acquisition system connects to a PC. The electrodes and transducers employ sensors that allow collecting good data. Software guides students by using onscreen. The sampling rate is set to 200Hz. A total of 30 subjects were considered for acquisition of ECG.

The model used in MP35, 4-Channel system. Four-channel data acquisition system with built-in universal amplifiers can record a wide range of physiological signals, plus current acknowledge 4 software (windows or Mac), which includes powerful automation and scoring tools.
The ECG is loaded, it is sampled and a part of it is considered. This is wavelet decomposed. This removes the noise in the ECG and improves it for better analysis of features. The Amplitude features are first extracted starting with R peak. The other peaks P, Q, S and T are determined using the time window. P and T will be the maximum value in the window taken for P and T respectively, while Q and S will be minimum in their own respective windows. Meanwhile, their locations are also found. All the peaks and marked on the original ECG plot.

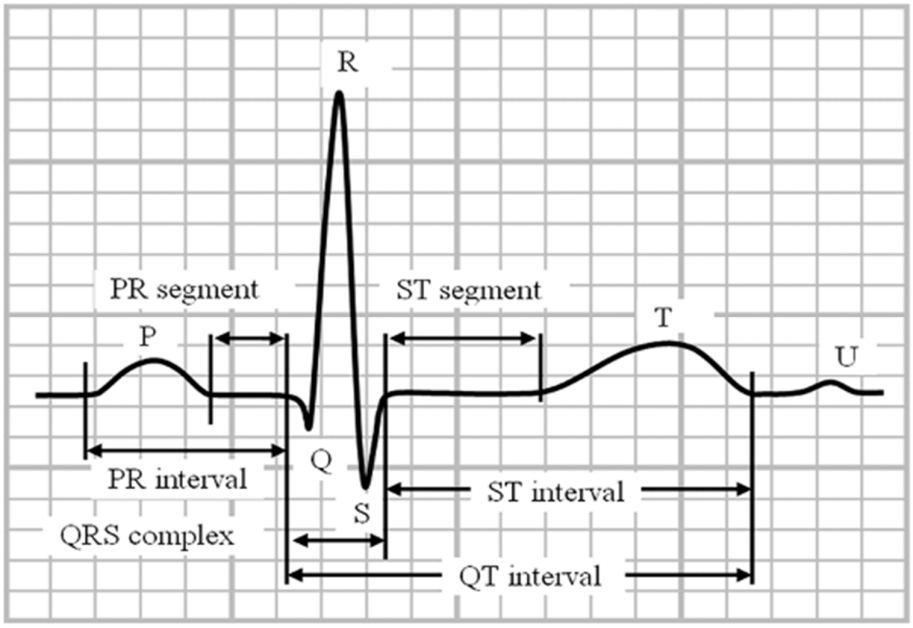

Figure 2. Sample ECG Recording of a Subject

Figure 3. ECG Physiograph 2.0 Version

Fingerprint

Fingerprint-based recognition has been the longest serving, most successful and popular method for person identification. There are numerous historical accounts which suggest that fingerprints have been used in business transactions as early as 500 B.C[16] in Babylon and later by Chinese officials to seal the official documents in the 3rd century B.C. Fingerprints consist of a regular texture pattern composed of ridges and valleys. These ridges are characterized by several landmark points, known as minutiae, which are mostly in the form of ridge endings and ridge bifurcations. The spatial distribution of these minutiae points is claimed to be unique to each finger; it is the collection of minutiae points in a fingerprint that is primarily employed for matching two fingerprints.

In addition to minutiae points, there are sweat pores and other details which can be acquired in high resolution (1000 ppi) fingerprint images. These extended features are receiving increased attention since forensics experts seem to utilize them particularly for latent and poor quality fingerprint images. Nearly all forensics and law enforcement agencies worldwide utilize Automatic Fingerprint Identification Systems (AFIS). Emergence of low cost and compact fingerprint readers has made fingerprint modality a preferred choice in many civil and commercial applications.

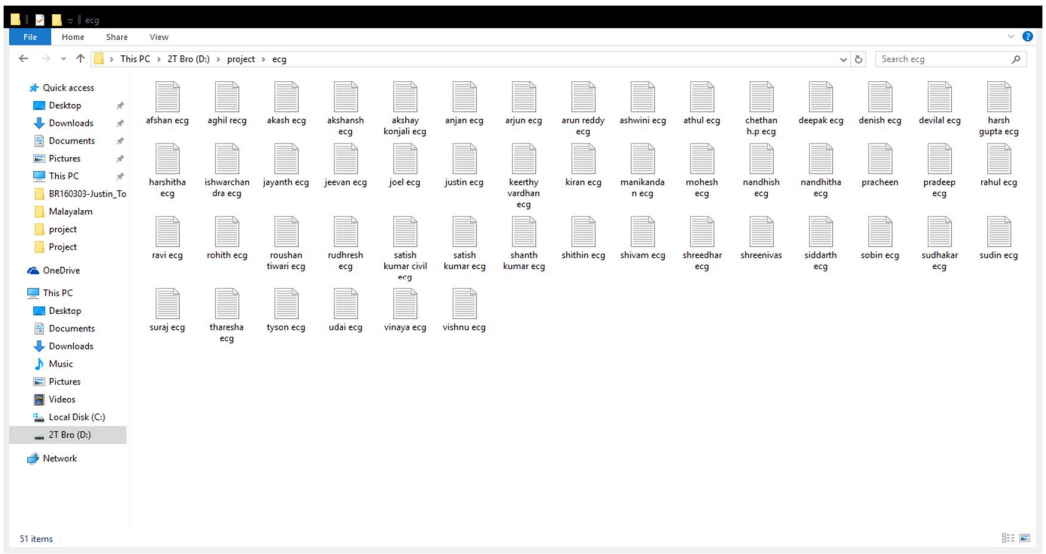

Figure 4. ECG database of 50 subjects

Figure 5. Sample Fingerprint

The fingerprint algorithm is tested on 2 databases. The first database is acquired directly using fingerprint sensor. The fingerprints of the thumb are acquired for a set of 50 individuals. 6 images are acquired per person. The other database is readily available database FVC 2002 from internet. The database comprised of different sets of fingerprints.

Figure 6. Fingerprint scanner

In the acquisition of the fingerprint, the user simply places their fingerprint on the glowing reader window, and the reader quickly and automatically scans the fingerprint. On-board electronics calibrate the reader and encrypt the scanned data before sending it over the USB interface. The sensor is composed with a combination of fast algorithms and high reliability, eSSL's fingerprint technology.

The second database used for the implementation of algorithm is FVC 2002. FVC2002 is the second international competition for fingerprint verification algorithms. The evaluation was held in april 2002 and the results of the 31 participants were presented at 16th ICPR. Three different databases (DB1, DB2 and DB4) were tested for the algorithm. 10 subjects, images were used with 8 images per subject. The fingerprint image preprocessing is accomplished by histogram equalization and fast Fourier transforms, these operations enhance image enhancement. The adaptive thresholding is used and the image is binarized. In segmentation process, the direction of the ridges is estimated and region of interest is extracted. The Binarized image is again considered. It is thinned, then the H-breaks and spikes in the thinned image are removed.

We used a fingerprint machine to create the database of fingerprint. For that we used employee fingerprint enrolment software Specifications: Resolution is 320*240, Image area 9.75mm*0.41mm/192*8 pixels, USB 2.0 Full Speed interface. We cropped the fingerprint image into 190*240.

Face: Humans have a remarkable ability to recognize fellow beings based on facial appearance. So, face is a natural human trait for automated biometric recognition. Face recognition systems typically utilize the spatial relationship among the locations of facial features such as eyes, nose, lips, chin, and the global appearance of a face. The forensic and civilian applications of face recognition technologies pose a number of technical challenges both for static mug-shot photograph matching (e.g., for ensuring that the same person is not requesting multiple passports) to unconstrained video streams acquired in visible or near-infrared illumination (e.g., in surveillance).

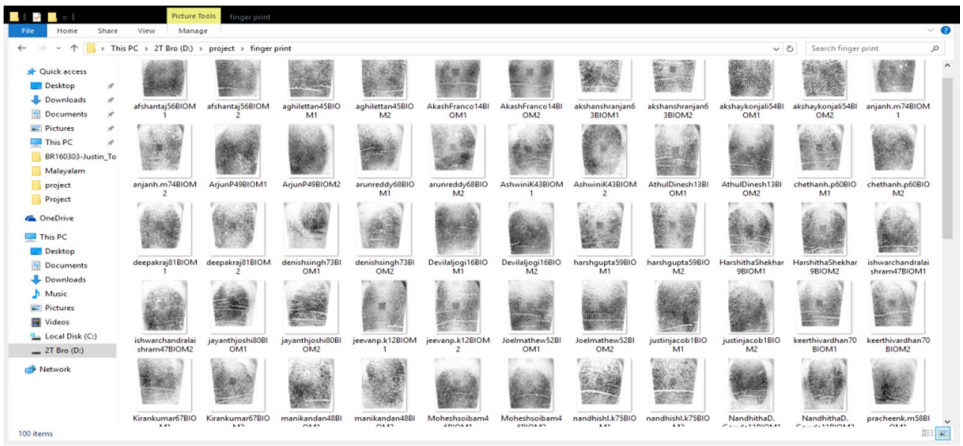

Figure 7. Fingerprint database of 50 subjects

The problems associated with illumination, gesture, facial makeup, occlusion, and pose variations adversely affect the face recognition performance. While face recognition is non-intrusive, has high user acceptance, and provides acceptable levels of recognition. Performance in controlled environments, robust face recognition in non-ideal situations continues to pose challenges. We used a webcam to capture the image for the database of face. A webcam is a video camera that feeds or streams its image in a real time to or through a computer to computer network. Webcams are known for their low manufacturing cost and their high flexibility. The facial features considered for facial recognition are distance between eyes, mouth, side of nose, entire face image, corner points, contours, gender, roundness of face, edge maps, pixel intensity, local and global curvatures. Here 50 induvial subjects faces are captured and preprocessed for a standard data size with resolution 320*240 interface type, and tested using standard recognition tech PCA, LDA, SOFM against to the standard database Yale face. These methods provide new research direction for potential solutions to face recognition under conditions of POSE and illumination and variation, which recent vendor test show are challenging issues for face recognition.

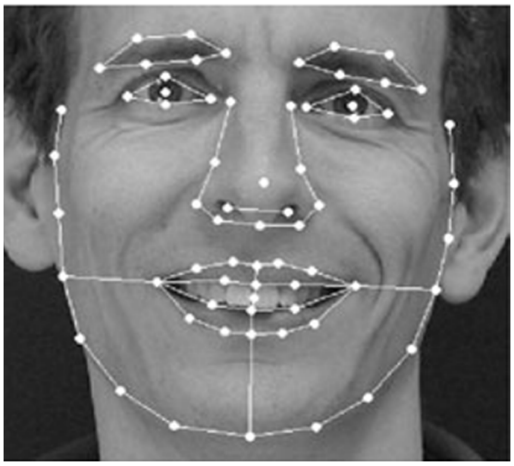

Figure 8: Sampled face

Figure 9. Web Cam

Here we created a database of 50 members face in an open area without any external lighting arrangements and cropped the face image into 170*230 grid size. The strength and weakness of an automated face recognition system are evaluated using standard databases and objective performances statistics. This method capable of detecting faces over a wide range of facial variations in color, position, scale, orientation, pose and expression.

IV. METHODOLOGY

An overview of the application of the work characterizes its divisions into three parts which comprises of the three individual modal which include face, fingerprint and ECG recognition. An overview of this work in brief is mandatory for the further implementation study of the work.

The fingerprint recognition passes through the histogram and FFT implementations so that the time division signals are converted to the frequency division signals followed by the face divisional features which are extracted by the Gabor filters and final stage is An ICA algorithm which is tested on 3−channel ECG recordings taken from human subjects, mostly in the ECG physiograph 2.0 version and main function of ICA is it can detect and remove a variety of noise and artifact sources in these ECGs, then the database that contains all the respective snaps are trained in the database with their extracted features which are the source for the SVM classification. Finally among the many images that are trained in the database, one image with specific features that matches the requirement is chosen by the SVM classifier.

The main objective of multi biometrics is to reduce one or more false accept rate, false reject rate and failure to enroll rate. Face Recognition (FR) is still considered as one of the most challenging problems in pattern recognition. The FR systems try to recognize the human face in video sequences as 3D object, in unconstrained conditions, in comparison to the early attempts of 2D frontal faces in controlled conditions. Despite the effort spent on research today there is not a single, clearly defined, solution to the problem of

Face Recognition, leaving it an open question. One of the key aspects of FR is its application, which also acts as the major driving force for research in that area. The applications range from law enforcement to human-computer interactions (HCI).

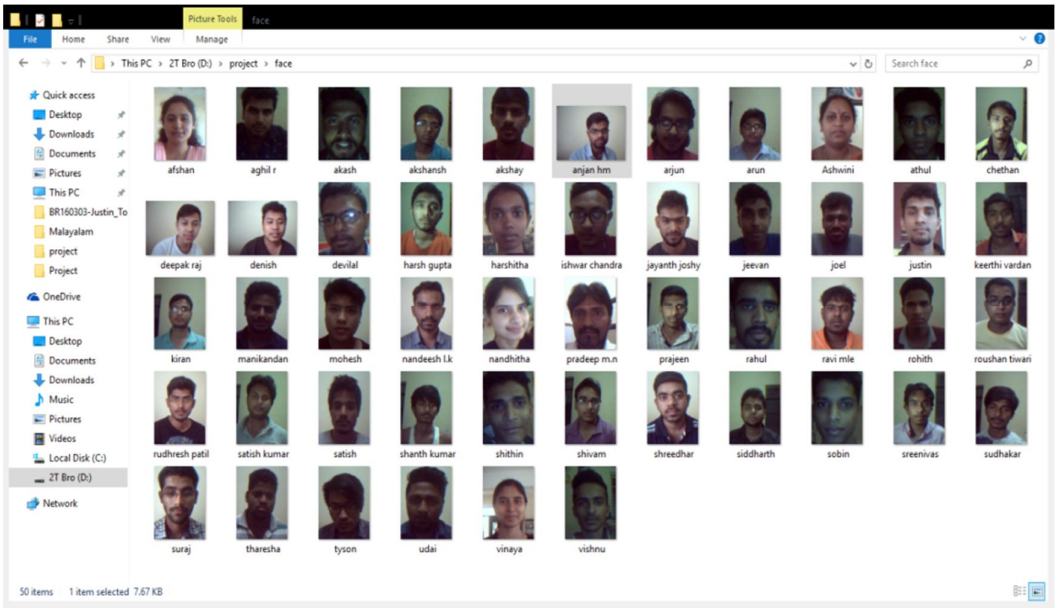

Figure 10. face database of 50 subjects

The systems used in these applications fall into two major categories: systems for identification and systems for verification. The first group attempts to identify the person in a database of faces, and extract personal information. These systems are widely used, for instance, in police departments for identifying people in criminal records. The second group finds its main application in security, for example to gain access to a building, where face is used as more convenient biometric. The more general HCI systems include not only identification or verification, but also tracking of a human in a complex environment, interpretation of human behavior and understanding of human emotions. Another biometric modality that we use in our approach is the electrocardiogram (ECG).

The modern concept for ECG personal identification is to extract the signal features using transform methods, rather than parameters in time domain (amplitudes, slopes, time intervals). The proper recognition of the extracted features and the problem of combining different biometric modalities in intelligent video surveillance systems are the novel steps that we introduce in this work i.e. To enhance the idea we combine the concept of the finger-print, face recognition, and ECG.

There are two psychological classification that we need to be associated with, one is behavioral approach and the other one is psychological based biometrics The physiological features based biometrics include iris image, finger prints, thumb print.

V. PROPOSED SYSTEM

Palm print, face, finger veins, hand geometry, DNA sequence, iris image, heartbeat, and palatesetc, on the other side, The behavioral features are the features which are extracted from day-to-day sociological behaviors of a person.

Each physiological and behavioral characteristic has its own limitations e.g. lip motion, body language, and voice of a person can be mimicked easily. The physiological features like palm prints, hand geoetry, finger veins, and heartbeats have very high false acceptance rate. Thus, a single biometric feature based approach is not reliable and secure. It cannot identify a particular person independently. Therefore, a single feature based biometric system will not be sufficient for fool proof identification of a person. Hence, we need to combine two or more physiological and behavioral characteristics for developing a foolproof multimodal identification system.

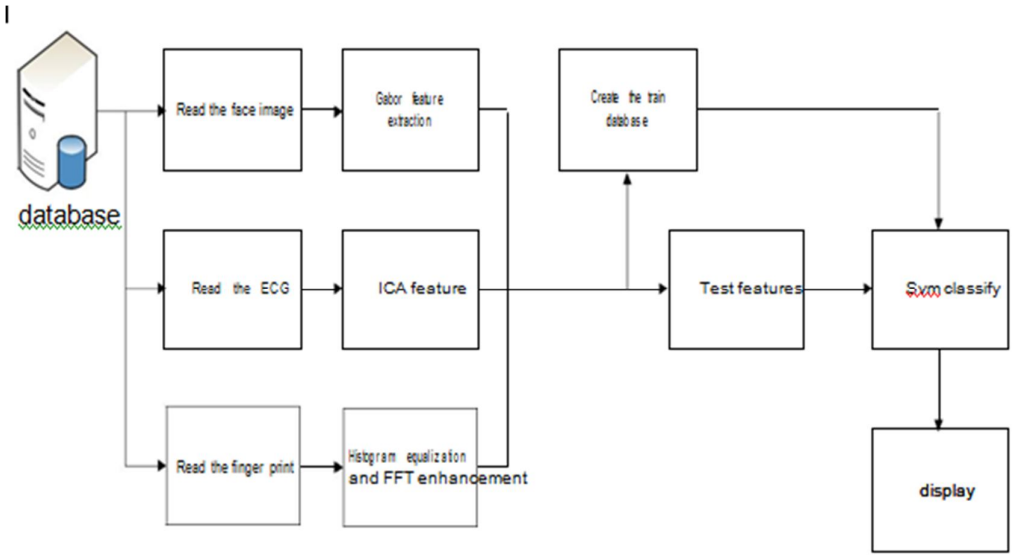

Figure 11. Block Diagram of Proposed Multimodal Biometric System

VI. Conclusion

Although Biometrics is becoming an integral part of the identity management systems, current biometric Systems do not have 100% accuracy. Some of the factors that impact the accuracy of biometric systems include noisy input, non-universality, lacks of invariant representation and non-distinctiveness. Further biometric systems are also vulnerable to security attacks. In case of multimodal biometric person authentication, typically more than one biometric feature is integrated this can overcome some of these limitations and Achieve better performance.

In this work we have discussed the analysis and improved framework of fingerprints, face image and ECG Signals Combined to multimodal system. Electrocardiogram [ECG] which is basically used for medical diagnosis, can also be used for person recognition, it is different even in identical twins, which means the uniqueness of ECG is very high Spoofing is another major issue faced by the existing biometric System.

Hence, by integrating the physiological signals with other biometrics like face & fingerprint results in employing liveliness detection along with person identification.

References

[1] Manjunathswamy, Appaji M A, Thriveni J, Venugopal K R, Patnaik L M, " Multimodal Biometric Authentication using ECG and Fingerprint" International Journal of Computer Applications, Volume 111 – No 13, February 2015, pp.33-39

[2] Bharathi, S., R. Sudhakar, and Valentina E. Balas, "Hand Vein-based Multimodal Biometric Recognition", Acta Polytechnica Hungarica, Vol.12.6, 2015.

[3] Ross, Arun, and Anil Jain, " Information fusion in biometrics ", Pattern recognition letters, Vol 24.13, pp. 2115-2125, 2003.

[4] R. Hoekema, G. J. H. Uijen, and A. van Oosterom, 'Geometrical aspects of the interindividual variability of multilead ECG recordings', IEEE Transaction on Biomedical Engineering, 2001, 48(5), pp. 551-559.

[5] S. Soviany and M. Jurian, "Multimodal biometric securing methods for informatic systems", Proceedings of the 34th International Spring Seminar on Electronic Technology, pp. 1214, Phoenix, Ariz, USA, May 2011.

[6] A. Ross, K. Nandakumar, and A. K. Jain, Handbook of Multibiometrics, ser. Int. Series on Biometrics. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2006.

[7] T. Murakami, K. Takahashi, and K. Matsuura, "Towards optimal countermeasures against wolves and lambs in biometrics," in Proc.of the 5th IEEE Int. Conf. on Biometrics: Theory, Applications and Systems (BTAS 2012), Sept 2012, pp. 69–76.

[8] F. Besbes, H. Trichili, and B. Solaiman, "Multimodal biometric system based on fingerprint identification and iris recognition," in Proc.of the 3rd Int. Conf. on Information and Communication Technologies:From Theory to Applications, April 2008, pp. 1–5.

[9] J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, and J. Bigun, Discriminative multimodal biometric authentication based on quality measures," Pattern Recognition, vol. 38, no. 5, pp. 777–779, May 2005.
[10] R. Jillela and A. Ross, "Mitigating effects of plastic surgery: Fusing face and ocular biometrics," in Proc. of the 5th IEEE Int. Conf. on Biometrics: Theory, Applications and Systems (BTAS 2012), Sept 2012, pp. 402–411.
[11] X. Zhou and B. Bhanu, "Feature fusion of side face and gait for video-based human identification," Pattern Recognition, vol. 41,no. 3, pp. 778–795, 2008.
[12] M. Hofmann, S. M. Schmidt, A. Rajagopalan, and G. Rigoll, "Combined face and gait recognition using alpha matte preprocessing," in Proc. of the 5th IAPR Int. Conf. on Biometrics, New Delhi, India,Mar. 2012, pp. 1–8.
[13] D. Muramatsu, H. Iwama, Y. Makihara, and Y. Yagi, "Multi-view multi-modal person authentication from a single walking image sequence," in Proc. of the 6th IAPR Int. Conf. on Biometrics, 2013, pp.1–8.
[14] "Soyuj Kumar Sahoo, TarunChoubsia, S.R.MahadevaPrasanna ",multimodal biometric person authentication, IETE Technical Review, Vol 29, Issue 1, jan-feb 2012
[15] Silva, H., Gamboa, H., Fred, A.: One lead ECG based personal identification with feature subspace ensembles. In: MLDM "07: Proceedings of the 5th international conference on Machine Learning and Data Mining in Pattern Recognition, Berlin, Heidelberg, Springer- Verlag (2007) 770–783.
[16] Ross, A.A., Nandakumar, K., Jain, A.K.: Handbook of Multibiometric (International Series on Biometrics). Springer-Verlag New York, Inc., Secaucus, NJ, USA (2006).