International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 14 Issue 2 –APRIL 2015.

Automatic System for Person Authentication by Multimodal Biometrics - A Survey

NAGAMMA ARAVALLI

PG student , Department of Computer Science and Engineering, BVBCET, Hubli, India

***Abstract*– Human authentication is very important in many application such as online banking, ATMs, airports, elections etc. Biometric system represents effective and reliable solution for human authentication. A biometric system operates by acquiring biometric data from an individual by extracting feature set, from the acquired data, and comparing this feature set against the template set in the database. A Multimodal Biometric system combines results obtained from two or more biometric traits. Typically each biometric trait processes its information independently and processed information is combined using an appropriate fusion method. In literature survey experimental studies show that the fusion of multiple biometrics minimizes the system error rates and increases accuracy of system. This paper presents overview of physiological and behavioral biometrics, different levels of fusion of multiple biometric traits, block diagram of multimodal biometric system and discussed different multimodal biometric systems.**

***Keywords*--- Authentication , Biometric trait , fusion , Multimodal , Template .**

I. INTRODUCTION

Biometric authentication refers to the automatic identification of living individuals by using their physiological and behavioural characteristics. Physiological characteristics are face ,finger print ,palm print , ear, iris ,retina ,hand geometry, finger vein, palm vein and behavioural characteristics are voice, gait and signature. Biometric Systems are of two kinds: Unimodal and Multimodal.

Unimodal Biometric system allow person recognition based on a single source of biometric information but cannot guaranty a perfect identification, because of noisy data , non-university and Unacceptable error rates. Multimodal systems consist of the fusion of two or more biometric traits ,such systems are more reliable due to the presence of multiple independent pieces of evidence as Biometric traits of an individual.

Multimodal biometrics are more important to fraudulent technologies, because forging multiple biometric characteristics is difficult than forging a single biometric characteristic thus provides higher accuracy rate and anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric traits of a legitimate user.

A typical multimodal biometric authentication system consists of five parts. Image capture, pre-processing, feature extraction, fusion and matching. Special biometric scanners are used for image capturing. It may vary depending on the type of biometric traits used . At the pre-processing stage the image is enhanced to remove noise and unwanted areas. Feature extraction gets effective features from the preprocessed biometric trait. After feature extraction fusion is carried out to combine different features and stored in the database as templates. A matching algorithm is used to compare it with the stored one in the database. In this paper we discuss some of such systems.

.

II. OVERVIEW OF COMMONLY USED BIOMECTRICS

A variety of factors should be considered when designing a multiple biometric system. These include the selection and number of biometric traits; the level in the biometric system at which information provided by multiple traits should be integrated; the methodology adopted to integrate the information; and the cost . Some of the biometrics discussed here are:

Face: Facial images are the most common biometric characteristic used by humans to make a personal recognition. Face verification involves extracting a feature set from a two-dimensional image of the user's face and matching it with the template stored in a database. Facial recognition system should be able to automatically detect a face from image, extract its

features and then recognize it from any pose which is a difficult task. One more problem is the fact that the face is a changeable social organ displaying a variety of expressions.

Iris: Iris biometrics involves analyzing features found in the colored ring of tissue that surrounds the pupil. Complex iris patterns can contain many distinctive features such as ridges, crypts, rings, and freckles. Undoubtedly, iris scanning is less intrusive than other eye-related biometrics. A careful balance of light, focus, resolution and contrast is necessary to extract a feature vector from localized image. While the iris seems to be consistent throughout adulthood, it varies somewhat up to adolescence.

FingerPrint: A fingerprint is a pattern of ridges and furrows located on the tip of each finger. Patterns have been extracted by compact sensors which provide digital images of these patterns or by creating an inked impression of the fingertip on paper. The feature values typically correspond to the position and orientation of certain critical points known as minutiae points. The matching process involves comparing the two-dimensional minutiae patterns extracted from the user's print with those in the template.

FalmPrint: Palms of the human hands contain unique pattern of ridges and valleys. Palmprint scanners need to capture larger area with similar quality as fingerprint scanners, so they are more expensive. Specific measurements include location of joints, shape and size of palm. Since Palm print geometry is not very distinctive, it cannot be used to identify a subject from a very large population.

Hand Geometry: It is claimed that individuals can be discriminated based on the shape of their hands. Person identification using hand geometry utilizes low resolution hand images to extract a number of geometrical features such as finger area , width ,finger length, thickness, perimeter.

Retina: Retinal recognition creates an "eye signature" from the vascular configuration of the retina which is supposed to be a characteristic of each individual and each eye, respectively. Since it is protected in an eye itself, and since it is not easy to change the retinal vasculature, this is one of the most secure biometric.

Ear: It has been suggested that the shape of the ear and the structure of the cartilaginous tissue of the pinna are distinctive. Matching the distance of salient points on the pinna from a landmark location of the ear is the method of recognition.

Voice: The features of an individual's voice are based on physical characteristics such as vocal tracts, mouth and lips that are used in creating a sound. These characteristics of human speech are invariant for an individual, but the behavioral part changes over time due to age, medical conditions and emotional state.

Signature. Signature is a simple, concrete expression of the unique variations in human hand geometry. The way a person signs their name is known to be characteristic of that individual. In addition to the general shape of the signed name, a signature recognition system can also measure pressure and velocity of the point of the stylus across the sensor pad.

Gait. This is one of the newer technologies and is yet to be researched in more detail. It is not supposed to be very distinctive but can be used in some low-security applications. Gait is a behavioral biometric and may not remain the same over a long period of time, due to change in body weight or serious brain damage. Since video-sequence is used to measure several different movements this method is computationally expensive.

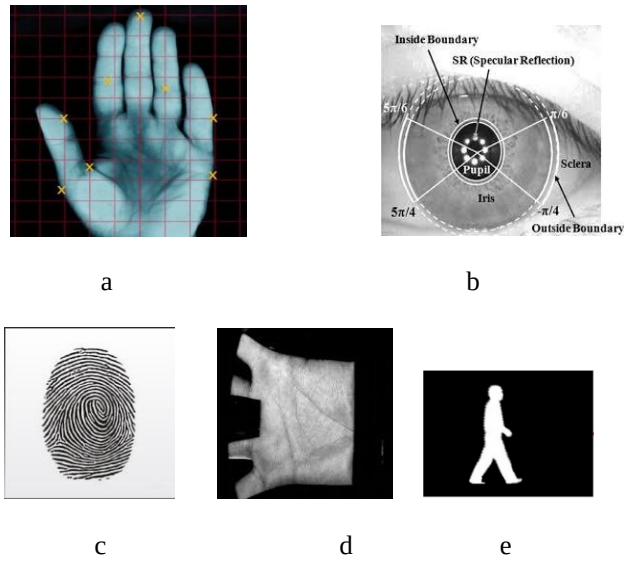

Figure 1: Samples of biometric traits a)Hand Geometry b)Iris c) Finger Print d) Palm Print e)Gait

III. MODULES AND BLOCK DIAGRAM OF MULTIMODAL BIOMETRIC SYSTEM

Modules of Multimodal biometric System

a) Sensor module

b) Pre-Processing module

c) Feature extraction module

d) Fusion module

e) Matching and Decision making module

a)Sensor module: This module is responsible for acquiring the biometric data of individual. For example palmprint sensor that captures palmprint impression of a user.

b)Pre-Processing: At this stage ,unwanted background of acquired image is removed and necessary enhancements are done to improve image quality.

c)Feature extraction : This acquired data is processed to extract feature values. For example geometry structure and principle line of palmprint image would be extracted in feature extraction module of palmprint system.

d)Fusion module: This combines features extracted from two or more biometrics. Fusion can be done at sensor level or at feature extraction level or at Matching level or at decision level.

e)Matching and Decision making module: In matching module extracted features are compared against the templates which are stored in database. And in Decision module user is either accepted or rejected based on the matching in the matching module

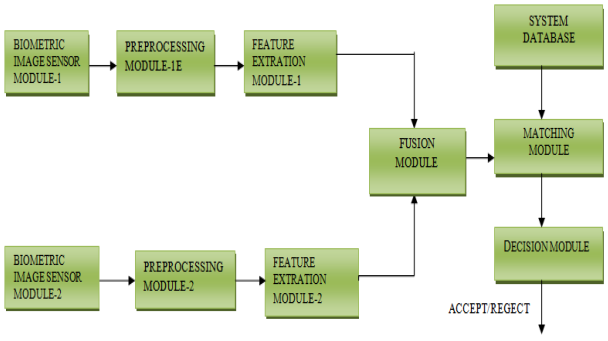

Figure 1. General Block diagram of multimodal biometric system

IV. DIFFERENT LEVELS OF FUSION FOR MULTIMODAL BIOMETRICS

As multimodal biometric systems uses multiple biometrics the system has to combine features of these biometrics extracted from their images called fusion. The goal is to identify or authenticate individuals more effectively than using a single sample. The fusion can be done at four levels: sensor level, feature level, match score level and decision level. Figure 2 illustrates the different levels of fusion for a multimodal biometric system using a fingerprint and a voice subsystem.

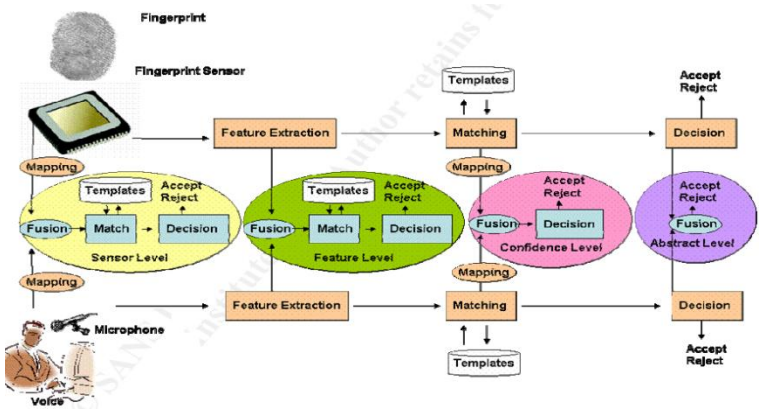

Figure 2. Levels of fusion for a multimodal biometric system

1. Sensor Level Fusion: In sensor level Fusion we combine the biometric traits coming from sensors like Thumbprint or Palmprint scanner, Video Camera, Iris or Face Scanner etc, to form a composite biometric trait and process.

2. Feature Level Fusion : In feature level fusion different samples coming from different sensors are preprocessed and feature vectors are extracted separately, using specific fusion algorithm we combine these feature vectors to form a composite feature vector. This composite feature vector is then used for classification process.

3. Matching Score Level: At this fusion method features of individual samples are compared with template stored in database and scores of individual matchers are combined and used for classification process.

4. Decision level Fusion: In decision level fusion each modality is first pre classified independently i.e. each biometric trait is captured then features are extracted from that captured trait, based on that extracted features these traits are classified like accept or reject. The final classification is based on fusion of the outputs of different modalities.

Table 1: Fusion Techniques

S.No.	Fusion Level	Refers To
1	Sensor Level	The raw data of the sensors are combined
2	Feature Extraction Level	The features extracted from the different sensors are concatenated to create a joint feature vector.
3	Matching Score Level	The matching scores of each subsystem are combined using techniques such as weighted sum rule, weighted product, linear discriminant, decision tree and the Bayesian Rule.
4	Decision Level	The decision of the subsystems are combined using techniques such as an AND rule, OR rule and Majority Voting.

K.Gunasekaran, P.Mahalakshmi [6] developed an authentication system that combines palm and fingerprint features . Histogram equalization is performed to enhance the clarity of the images. Feed Forward Neural Network which is classification method used to extract the features of palm and finger print images. For enrolling and storing images Ms-Access DataBase is used. Mohamed Soltane et al.,[7] proposed a system by combining face and speech biometrics. Principal Component Analysis algorithm is used to extract face features and nearest neighbor classifiers is used for classification. A text independent Gaussian Mixture Models (GMM) tool is used for speech verification, which is trained using the Expectation Maximization (EM) and Figueiredo-Jain (FJ) algorithms. Adaptive Bayesian Method Based Score Fusion is performed.

A Heterogeneous multimodal biometric system proposed by mukwinder singh and Tripatjot singh [8] with combination of Finger print and Iris and Fuzzy vault encryption scheme was used for template security. Iris features are extracted from iris image using Daugman‟s Integro differential operator and then the unique patterns of 1‟s are extracted from iris code. Fingerprint minutia points are extracted from fingerprint image using Crossing Number (CN) technique . The results are tested on Fingerprint FVC database and CASIA Iris database taking 100 samples from each.. The system was efficient with FAR of 2.3% and GAR of 92.4% .Padma polash paul et al .,[10] proposed a system with combination of signature, face and ear in which Fisher Linear Discriminant Analysis method is used for feature extraction and decision level fusion is performed to increase robustness of authentication system. This system is efficient in reducing the FAR 5% and increasing GAR 100%.

Muhammad Imran Ahmad *et al*.,[12] proposed a multimodal biometric system using face and palm print. A set of Gabor filter with different scales and orientations are used to extract the features of face and palm print images. To reduce the dimensionality Linear projection based on PCA and LDA method is used. Feature Fusion is constructed by concatenating low frequency components of the projected Gabor image. The experimental results are tested using AR and PolyU datasets. The system showed 97% recognition rate and 98% verification rate.

Ujwalla Gawande *et all*.,[14] proposed a system with combination of Iris, finger print ,face and palm geometry. Iris features are extracted using Blocksum method, Fingerprint features are extracted using Minutiae technique, Face features are extracted using skin mapped technique and Palm geometry features using principle line, strucal, edge mapping parameter are stored as feature vector. Feature level fusion is used to provide high accuracy rate. The system contains identification and verification phases. Probabilistic Neural Network and Radial Basis Function NN classifier used in Identification phase for obtaining precision in decision of adaptive and cascade classifier. The Back Propagation neural network classifier is used in Verification phase to classify user as genuine or imposter. The system given up to 98.8% of accuracy.

Eshwarappa M.N. *et all*.,[15] proposed a system by integrating signature , speech and handwriting biometrics. From each of the speech blocks Mel Frequency Cepstral Coefficients (MFCCs) are the features extracted. The MFCCs from the training or enrollment data are modeled using Vector Quantization (VQ) technique. The SSIT database is used to store the speech data of speakers. Features of signature are extracted by using Discrete Cosine Transform (DCT) analysis, Vertical Projection Profile (VPP) analysis and Horizontal Projection Profile (HPP) analysis. The features from the handwriting image

considered in their work are VPP vector and HPP (Horizontal Projection Profile)vector.

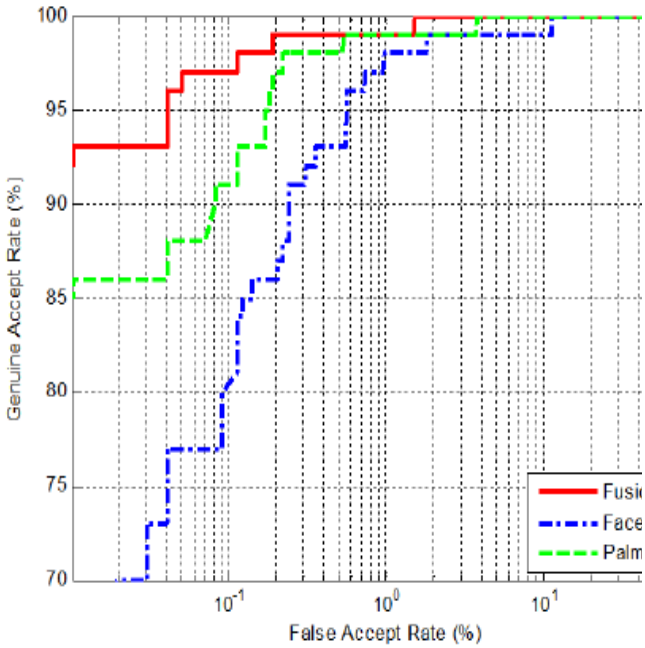

Figure 3. ROC curve [12]

V. CONCLUSION

Multimodal Biometrics using more than one physiological or behavioral characteristic for authentication or identification of human are more reliable due to the presence of multiple independent pieces of evidences. In this paper we have mentioned and discussed different levels of fusions and Various multimodal biometric systems proposed by various authors and observed that the biometrics fusion technology is considered to be an effective solution to improve the performances of single sample biometrics systems.

REFERENCES

[1] P. S. Sanjekar and J. B. Patil ,"*An Overview Of Multimodal Biometrics*", Signal & Image Processing : An International Journal (SIPIJ) Vol.4, No.1, February 2013.

[2] P. Prabhusundhar, V.K. Narendira Kumar, B. Srinivasan," *A Hybrid Model of Multimodal Approach for Multiple Biometrics Recognition*", International Journal of Computer Science and Business Informatics, pp 3-4,Vol. 3, No. 1. JULY 2013.

[3] Kande Archana, Dr.A .Govardhan ," *Enhace the Security in the ATM System with Multimodal Biometrics and Two-Tier Security*", International Journal of Advanced Research i Computer Science and Software Engineering, Volume 3, Issue 10, October 2013.

[4] Ashish Mishra," *Multimodal Biometrics it is: Need for Future Systems*", International Journal of Computer Applications (0975 – 8887) Volume 3 – No.4, June 2010.

[5] Cătălin LUPU, Vasile-Gheorghiță GĂITAN, Valeriu LUPU," *Security enhancement of internet banking applications by using multimodal biometrics*", IEEE 13th International Symposium on Applied Machine Intelligence and Informatics ,January 22-24, 2015.

[6] K.Gunasekaran, P.Mahalakshmi," *Implementation of Multimodal Biometric Authentication Using Soft Computing Techniques*", ICICES-2014.

[7] Mohamed Soltane, Noureddine Doghmane, Noureddine Guersi, " *Face and Speech Based Multi-Modal Biometric Authentication*" International Journal of Advanced Science and Technology Vol. 21, August, 2010.

[8] Komal Sondhi, Yogesh Bansal" *Concept of Unimodal and Multimodal Biometric System",* International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6, June 2014.

[9] Mukhwinder Singh, Tripatjot Singh Panag " *Heterogeneous Multimodal Biometric System with Fuzzy Vault Template Security*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 7, July 2014.

[10] Dr.Sudeep D.Thepade, Rupali K.Bhondave"*Bimodal Biometric Identification with Palmprint and Iris Traits using Fractional coefficients of Walsh, Haar and Kekre Transforms*", International Conference on Communication, Information & Computing Technology (ICCICT), Jan. 2015.

[11] Padma polash paul, Marina L.G and Reda Alhaj,"*Decision fusion for multimodal biometrics using social network Analysis",* IEEE transactions on systems, man, and cybernetics: systems, vol. 44, no. 11, november 2014.

[12] Dewi Yanti Liliana, Eries Tri Utaminingsih, "*The combination of palm print and hand geometry for biometrics palm recognition*", International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 12 No: 01, February 2012.

[13] Muhammad Imran Ahmad1, Mohd Zaizu Ilyas1,Mohd Nazrin Md Isa2, Ruzelita Ngadiran1, Abdul Majid Darsono," *Information Fusion of Face and Palmprint Multimodal Biometrics",* 2014 IEEE Region 10 Symposium.

[14] Ujwalla Gawande and Kamal Hajari , "*Adaptive Cascade Classifier based Multimodal Biometric Recognition and Identification System* "IJAIS, Foundation of Computer Science FCS, New York, USA Volume 6 – No.2, September 2013.

[15] Eshwarappa M.N. and Dr. Mrityunjaya V. Latte*,"Multimodal Biometric Person Authentication using Speech, Signature and Handwriting Features" ,IJACSA*