International Journal of Inventive Engineering and Sciences (IJIES)
ISSN: 2319–9598, Volume-3 Issue-8, July 2015

Analysis of Multimodal Biometric System Based on Level of Fusion

Mrunal Pathak, N. Srinivasu

Abstract - User authentication is essential to provide security that restricts access to system and data resources. Biometric system refers to an recognition of legitimate user based on a feature vector(s) derived from their distinguishing behavioral and/or physiological traits like face, finger, speech iris, gait, etc., Research on biometrics has distinctly increased for solving identification and authentication issues in forensics, physical and computer security , custom and immigration, However, unimodal biometric system is not able to satisfy acceptability, speed, and reliability constraints of authentication in real applications due to noise in sensed data, spoof attacks, data quality, lack of distinctiveness, restricted degree of freedom, non-universality and other factors. Therefore multimodal biometric systems are used to increase security as well as better performance. This paper presents overview of different multimodal biometric (multibiometric) systems and their fusion techniques with respective their performance.

Keywords: ***Biometrics, Unimodal, Multimodal, Fusion, Multibiometric Systems***

I. INTRODUCTION

Security is major concern for today's scenario. A high level industry uses biometric authentication systems based on evidence of single source of information called as Unimodal systems[1] which make use of physiological characteristics such as fingerprint, face, iris, ear, teeth,retina, palm print , veins or behavioral characteristics such as signature , voice, gait etc[2]. Each biometric has its own strength and weakness in terms of accuracy, user acceptance and applicability and accordingly each biometrics is used in authentication application. The advantage of biometric is that it doesn't change and misplaced. But no single biometric system is expected to effectively meet all requirements when deploying in real world application. The Unimodal biometric system have to contend with variety of problems like [3] .

(a) *Noisy sensor data*: for *example* fingerprint with a scar or voice sample altered by cold. Due to defective or improperly maintained sensor or ambient condition , noisy data leads to inaccurate matching or false rejection

(b) *Non universality*: Biometric system may not be able to acquire meaningful biometric data from subset of user, may be due to illness or disabilities.

(c) *Intra-class variation* :This variation caused by user who incorrectly interacting with sensor or when sensor characteristics are changed during authentication. For example incorrect facial pose. Large intra class variation increases false rejection rate (FRR) in biometric system.

(d) *Inter-class similarities*: It refers to overlap of feature space corresponding to multiple users. Large inter class similarities increases false acceptance rate (FAR) in biometric system

(e) *Failure-to-enroll*: attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.

(f) *Spoof attacks*: unimodal biometric is vulnerable to spoofing where data can be imitated. These type of attack occurs when behavioral traits such as signature or voice is used. For example face mask.

(g) *Restricted degree of freedom:* in Unimodal biometric system, we are using features from any single biometric traits like face, iris, palm, etc. which will restrict the performance of recognition

(h) *Unacceptable error rate:* FAR and FRR have the same value known as Equal Error Rate (EER). Lower the EER, system will be considered as more accurate. Otherwise error rate will be unacceptable

Some limitation of unimodal biometric systems can be alleviated by using multimodal biometric system. Multimodal biometric system utilizes information from multiple modalities or multiple processing techniques or both. Therefore, Multimodal biometric systems are those which integrates more than one physiological or/and behavioral characteristics for enrollment, verification, or identification to improve performance and reliability. Some common multimodal biometrics are :face and iris, iris and fingerprints, face and fingerprints, face and voice, face, fingerprints and iris, face, fingerprint and signature, etc.

The paper is divided into the following sections. In Section I, general biometric system will be discussed. Section II will be an introductory section on multimodal biometric systems. This section gives an overview of a selection of well known multimodal biometric systems and setups that are in used by researchers worldwide. Subsequently Section III, will be addressed on overview of methods of multimodal fusion. The paper is concluded in Section IV with a conclusion and discussion on the future directions of this project.

II. BIOMETRIC SYSTEM

Biometric systems have now been deployed in various forensic, commercial and civilian applications for person authentication. Traditional methods to secure such applications include magnetic and smart cards, tokens as well as passwords and PINs. However, when it comes to identity assurance, biometric technologies have an unsurpassed advantage: they are intrinsically linked to the person. Biometric system is an pattern recognition system that operates by acquiring biometric data from an individual. Generic biometric system has four phases[4]:(a)enrollment phase which captures the trait in the form of raw biometric data.(b) Feature extraction phase, processes data to remove artifacts from the sensor and use some kind of normalization, to build extracted feature set that is compact

Revised Version Manuscript Received on July 02, 2015.
Mrunal Pathak, Department of Information Technology, AISSMS Institute of Information Technology, Savitribai Phule Pune University, Pune (Maharashtra). India.
N. Srinivasu, Department of Computer Engineering, KL University, Guntur (Anndra Pradesh). India.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

representation of trait. A template is a synthesis of the relevant characteristics extracted from the trait (c) in matching phase ,the matching and comparing process creates ‘score’ based on how closely the sample matches with created templates which are stored in database.(d) decision making phase in which user is either accepted or rejected based on matching score in matching module. There are two modes of biometric recognition: verification and identification. Verification involves comparing acquired biometric information with only those templates corresponding to claimed identity and identification involves comparing acquired information against templates corresponding to all users in the database. Finally authentication occurs based on pattern matching

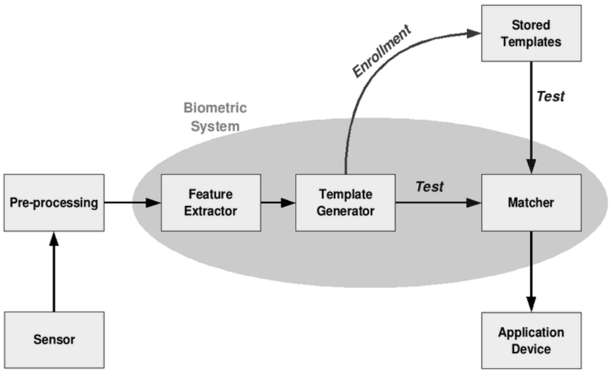

Figure 1: Block diagram of general biometric system

The performance of a biometric system can be measured by reporting its false accept rate (FAR) and false reject rate (FRR) at various thresholds.

a) *False acceptance rate (FAR)* : It is defined as the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts.
b) *False rejection rate (FRR)*: It is defined as the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. A system's FRR typically is stated as the ratio of the number of false rejections divided by the number of identification attempts.

The FAR and FRR are computed by generating all possible genuine and impostor matching scores and then setting a threshold for deciding whether to accept or reject a match. A genuine matching score is obtained when two feature vectors corresponding to the *same* individual are compared, and an impostor matching score is obtained when feature vectors from two *different* individuals are compared.

III. MULTIMODAL BIOMETRIC SYSTEM

Some of the limitations imposed by unimodal biometrics system like Noisy data, Intra-class Variation, Interclass Similarities, Non universality, Spoofing etc. can be overcome by including multiple source of information for establishing identity of person [5]. This allows capturing multiple samples of a single biometric trait (called multi-sample biometrics) and/or samples of multiple biometric traits (called multi source or multimodal biometrics). Multimodal biometric system take input from single or multiple sensors measuring two or more different modalities of biometric characteristics for the purpose of personal identification. Multi-modal biometric systems are more reliable because many independent biometric modalities are used which may result highly accurate and secure biometric identification system, as unimodal biometric system may not provide accurate identification due to non-universality. The reduction in failure to enroll (FTE) rate in multi-modal evaluation is very significant and which is one of major advantages of this system. Multimodal biometric system has the potential to be widely adopted in a very broad range of civilian applications: banking security such as ATM security, check cashing and credit card transactions, information system security like access to databases via login privileges. A decision made by a multimodal biometric system is either a “genuine individual" type of decision or an “imposter" type of decision. False Rejection Rate [FRR], False Acceptance Rate [FAR] and Equal Error Rate [ERR] is used to measure the accuracy of system [6]. Ross and Jain (2003) have proposed various levels of fusion, various possible scenarios, the different modes of operation, integration strategies and design issues for multimodal biometric system. A multimodal system can operate in one of three different modes: serial mode, parallel mode, or hierarchical mode. Serial mode forces the user to use the modalities one after another. Therefore, multiple sources of information (e.g., multiple traits) do not have to be acquired simultaneously and decision could be made before acquiring all the traits which reduce the overall recognition time. In the parallel mode of operation, the information from multiple modalities is used simultaneously in order to perform recognition. Multimodal biometric fusion combines measurements from different biometric traits to enhance the strengths. The block diagram for general multimodal biometrics system is as shown in figure 2.

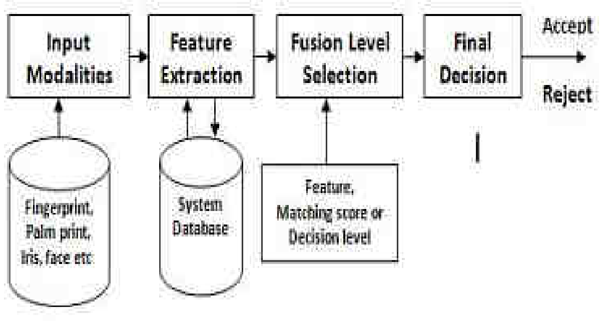

Figure 2: Block diagram of general multimodal biometric system.

Generally multimodal biometric system operates in two phases i.e. Enrollment phase and Authentication phase which are described as follows:

Enrollment phase: In enrollment phase, biometric traits of a user are captured and are stored as a template for that user in the system database which is further used for authentication phase.

Authentication phase: In authentication phase, once again traits of a user captured and system uses this to either identify or verify a person by comparing captured data with templates corresponding to all users in database. [7].

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

IV. LEVELS OF MULTIMODAL FUSION

Multimodal biometric fusion combines features from different biometric traits to enhance the strength and diminish the weakness of individual measurement. The goal of multimodal fusion is to extract meaning from a set of input modalities. Multimodal fusion in biometric system is classified into two broad categories [10]: *pre-classification* and *post classification*. In pre-classification fusion information is integrated before applying any classification method or matching algorithm. Information is integrated after decision of classifiers in post- classification method. Pre-classification fusion takes place either in data level (sensor level) or feature level (early fusion) as it uses raw input data from different biometric trait [8],[9]. Post-classification fusion categories into dynamic classifier selection, abstract level fusion, rank level fusion and matching score level fusion [10].

Data level fusion is the process of integration of multiple data and knowledge representing multiple signals from a very similar modality source (e.g. same scene recorded by two webcam from different viewpoint) without loss of information into a consistent, accurate, and useful representation. It is highly susceptible to noise and failures due to the absence of preprocessing. It is not commonly used because data required for fusion should be compatible which is rare in biometric sensors.

Feature level fusion: In feature level fusion, tightly coupled or time synchronized modalities are to be fused. Features extracted from different modalities are first combined and then analysis is to be performed. E.g. fusion of speech and lip movement in speaker recognition. Feature level fusion is at risk to time synchronization between multimodal features, low level information loss, although it handles noise and perform better task accomplishment.

A dynamic classifier selection scheme estimate accuracy of each classifier in local region surrounding input pattern to be classified and chooses classifier which is most likely to give the correct decision for the specific input pattern.[14,15]. Dynamic selection requires the large data sets for estimating local classifier accuracy.

Decision level fusion: In Decision level fusion, features are extracted from each biometric trait and these extracted features are then classified like accept or reject after matching module. The final output of multiple classifiers for different modalities is then combined. Methods like majority voting, AND rule and OR rule, weighted voting based on Dempster-Shafer theory of evidence behavior knowledge space is then used to arrive at final decision. Decision level fusion has some advantage over feature level fusion like scalability in terms of modalities used in fusion process, it also allows suitable method for analyzing each single modality such as support vector machine (SVM) for image and Hidden Markova Model (HMM) for audio. Disadvantage of decision level fusion is that learning process is tedious and more time consuming as it uses different method of classifier to obtain local decision for every modality used .Also Decision level fusion uses very abstract level of information which hold binary value so they are less preferred.

Rank level fusion: It is preferred in biometric identification system to improve performance. In rank level fusion, each classifier associates a rank with every enrolled identity. The output from each biometric matcher is subset of possible matches ranked in decreasing order of confidence values. Fusion can be done by consolidating more than two biometric matching score associated with an identity and determine new rank that would used in final decision.

Match score level fusion: Similarity between input biometric and template biometric is measure by 'match score'. Integration can be done at matching score level, when output from each biometric matching module is set of possible matches along with quality of each matching score associated with confidence values. Match score level fusion also known as measurement or confidence level fusion. Matching score level is most common approach in multimodal biometric because output of matching scores by matchers contain the richest information about input pattern which will gives more accurate decision. Also it is relatively easy to access and combine the scores generated by different matchers.

Integration of information in early stage (pre-classification fusion) is more effective than integration of information done in later stage (post-classification fusion) in multimodal biometric. So it is expected that feature level fusion gives better result of recognition but it difficult to integrate features at this level due to large feature set as well as incompatibility of features of different modality. Also most of the commercial biometric system don't provide access to feature set, which they use in their product. Integration of information at decision level fusion would inevitably lose useful detailed information as it uses abstract data. Match score level fusion is usually preferred because it easy to access and combine the scores of different modalities [1],[2],[11],[12].

V. METHODS FOR MULTIMODAL FUSION

Multimodal fusion is classified into following three categories: rule based methods, classification based methods, and estimation based methods based on nature of these methods and classification of problem space [10],[16].

a)Rule Based Fusion Methods : Basic rules of combing multimodal information are used in ruled based fusion methods. Linear weighted fusion (sum and product), majority voting, MAX, MIN , AND and OR are some statistical rule based methods. Custom defined rules can also be constructed depending on some specific application perspective. However these rules are domain specific and defining rules requires proper knowledge of the domain. In rule based method, Linear weighted fusion method is commonly used because it is simple and computationally less expensive and perform well if weight is different modalities are appropriately determined. This fusion method widely used in domain of multimodal dialog system and sports video analysis.

b)Classification Based Fusion Method : classification based fusion method includes range of classification techniques to classify multimodal observation into one of the predefined classes. The methods are support vector machine (SVM), Bayesian interface, Dynamic Bayesian Network (DBN), neural network (NN), Dempster Shafer theory and maximum entropy model. The Bayesian interface fusion works on probabilistic principals and use priori information to provide easy integration of new observation. However due to lack of appropriate priori information, it may provide inaccurate fusion results and not suitable for handling

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

mutually exclusive hypothesis. DBN in its different forms (e.g. HMM) have been commonly used to deal with time series data. However it is difficult to determine right DBN state. Hence NN method is generally used which is suitable to work in high dimensional problem space and generate high order nonlinear mapping. But due to complex nature of network, it suffers from slow training. SVM and DBN are widely preferred due to their improved classification performance.

c) Estimation Based Fusion Method: problem of estimating parameters is solved by estimation based fusion method. It uses Kalman Filter, extended Kalman filter and practical filter methods. These methods are primarily used to estimate and predict the fused observation over the period. These methods are suitable for object localization and tracking task. Kalman filter is suitable for linear model, extended Kalman filter suitable in non- linear model. However, practical filters method is robust in non-linear and non-Gaussian models.

VI. MODES OF OPERATION

Multimodal biometric system works in three modes of operation:

a. *Parallel Mode*: Multiple sources of information is acquired simultaneously to perform recognition [12].
b. *Serial Mode*: Multiple sources of information is not acquired simultaneously. The output of one biometric trait is used to reduce number of possible identities before getting next trait. So multiple source of information is not acquired simultaneously. This reduces the recognition time.[13]
c. *Hierarchical Mode:* Individual classifiers are combined in tree like structure in hierarchical mode. It will be used when there will be large number of classifiers.

Parallel fusion mode demands that in both enrollment and recognition stage, all type of required traits be always captured for each user. Because of this, parallel fusion will become inefficient and inconvenient due to redundant capturing and matching of all the traits. In serial fusion mode user checks authentication for individual biometric trait stage by stage. At each stage certain type of trait is sampled and matched against template, after valid authentication all later stages will be bypassed. As a result user efforts and time will be significantly saved and system efficiency significantly improved.

VII. ISSUES IN MULTIMODAL BIOMETRICS

- Optimal Modality selection
- Correlation between different modalities.
- Confidence level of different modalities based on learning weights assigned to individual biometric
- Fusion methodology
- Cost vs Performance trade off

VIII. APPLICATIONS

Today biometrics has been used in wide Varity of applications to provide security, convenience, privacy enhancement in much more commercial , criminal and civil application for e.g. personal information and business transactions requires fraud prevent solutions that increase security and cost effective and user friendly.

IX. CONCLUSION AND FUTURE DIRECTION

In this paper, we highlighted biometric system and limitations of individual biometric. Multimodal biometrics authentication process provide and maintain higher authentication security as strong as possible to provide more accuracy. We also discussed about various fusion levels and methods of multimodal system. For authentication of person, there are many multimodal biometric systems in existence but still selection of appropriate model, choice of optimal fusion level and redundancy in extracted features are some challenging issues in deigning multimodal biometric system needed to be solved

REFERENCES

1. A.K.Jain, A.Ross S. Prabhakar: An Introduction to biometric recognition, IEEE Trans., Circit systems and Video Technol., 14(1)(2004),pp 4-20
2. A.Ross, P.Flynn A.K.Jain : Handbook of Biometrics, New York, USA, Springer 2007
3. Ross , K. Nandkumar, A. Jain : Handbook of Multibiometrics, Springer international edition.
4. Mini Singh Ahuja, Sumit Chabbra: A survey of multimodal biometrics, International journal of computer science and its application, ISSN 2250-3765. pp 157-160
5. P.S. Sanjekar, J.B. patil : An Overview of Multimodal Biometrics, Signal and Image processing: an international journal(SIPIJ), vol.4, no.1, Feb 2013.
6. Ashish Mishra : Multimodal Biometrics it is: Need for Future Systems, International Journal of Computer Applications(0975-8887) vol 3,no.4, June 2010
7. M. Golfarelli, D. Maio and D. maltoni : On the error-reject tradeoff in biometric erification systems, IEE Trans on Pattern Analysis and Machine Intelligence, vol. 19, no.7, pp 786-796, July 1997.
8. Sharma ,R. Pavlovic, V. I. , Huang, T.S.: Towards multimodal Human computer interface. In Proceeding IEEE, 86(5),pp.853-860(1998).
9. Ross , A. Jain : Information fusion in biometrics, Journal of pattern recognition letters, vol 24, no.13,pp. 2115-2125,Sep 2003.
10. Pradeep Atrey, Anwar Houssain,Abdulmotaleb Saddik, Mohan kanakanhalli , Mutimodal fusion for multimedia analysis: A survey, Springer trans. multimedia systems (2010), 16: 345-379
11. A. Ross., R. Govindrajan: Feature level fusion using hand and face biometrics, Proc SPIE, Vol. 5779.,pp 196-204, Mar2005.
12. L. Hong, A.Jain : Integrating face and fingerprints for personal identification, IEEE Trans., Pattern Anal. Match. Intell, vol. 20, no. 1, pp. 1295-1307, Dec 1998
13. G. L. Marcialis, P. Mastinu and F. Roli:Serial fusion of multimodal biometric systems, in Proc BIOMS, Taranto, Italy, Spt. 2010, pp. 1-7
14. K Woods, W P Kegelmeyer Jr, K Bowyer :Combination of Multiple Classifiers Using Local Accuracy Estimates, IEEE Trans. Pattern Analysis and Machine Intelligence 19(4),405-410 (1997)
15. Giorgio Giacinto , Fabio Roli ,Et Dynamic Classifier Selection based on Multiple Classifier Behaviour. Pattern recognition. 34((),179-181(2001)
16. Aguilar, J.F., Garcia, J.O., Romero, D.G., Rodriguez, J.G.: A coparitive evaluation of fusion startegiesfor multimodal biometric verification. In International conference on video based biometric person authentication, pp., 830-837,Guildford(2003)

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.