International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161
©2014 INPRESSCO®, All Rights Reserved
Available at http://inpressco.com/category/ijcet

General Article

Multimodal Biometric Systems: Study to Improve Accuracy and Performance

Almas M. N. Siddiqui[A*], Rupali Telgad[A] and Prapti D. Deshmukh[B]

[A]Dr. Babasaheb Ambedkar Marathwada University, A'bad, India
[B]MGM's G. Y. Pathrikar College, Aurangabad, India.

Accepted 10 January 2014, Available online 01 February 2014, **Vol.4, No.1 (February 2014)**

Abstract

Biometrics is the science and technology of measuring and analyzing biological data of human body, extracting a feature set from the acquired data, and comparing this set against to the template set in the database. In literature survey experimental studies show that Unimodal biometric systems had many disadvantages regarding performance and accuracy. Multimodal biometric systems perform better than unimodal biometric systems. In biometric system physical or behavioral traits are used. A multimodal biometric identification system aims to fuse two or more physical or behavioral traits. It is used in order to improve the accuracy. The fusion of multiple biometrics helps to minimize the system error rates. This paper presents an overview of multimodal biometrics. This includes block diagram of multimodal biometrics, module of multimodal biometric system, different levels of fusion in multimodal biometrics.

Keywords: *Biometrics, Multimodal Biometrics, unimodal, Fusion, Authentication*

1. Introduction

Biometrics refers to automatic identification of people based on their distinctive physiological (e.g., face, fingerprint, iris, retina, hand geometry) and behavioral (e.g., voice, gait) characteristics, should be an essential component of any effective person identification solution because biometric identifiers cannot be shared, misplaced, and they intrinsically represent the individual's identity (A. K. Jain, et al 2004). A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Unimodal biometric systems allow person recognition based on a single source of biometric information but cannot guaranty a perfect identification. Multimodal biometric systems have been widely used to overcome the limitations of unimodal biometric systems and to achieve high recognition accuracy. The remainder of the paper is organized as follows: section 2 presents an overview of Biometrics, section 3 presents overview of Multimodal biometric recognition system, section 4 represents modules of multimodal biometric, section 5 presents different levels of fusion in multimodal biometrics, section 6 presents different levels of fusion in multimodal biometrics, section 5 concludes the paper with some suggestions for further investigations.

2. Overview of Biometrics

Biometrics as a branch of industry, science and technology exists since about 20 years. Problems and questions having to do with automatic people recognition are attracting more and more scientists and technician. A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in verification mode or identification mode (M. Golfarelli, D. Maio, and D. Maltoni, July et al ,1997).

In the verification mode, the system validates a person's identity by comparing the captured biometric data with his own biometric templates stored in the system database. Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity (A. Ross and A. K. Jain et al 2003).

In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (S. Prabhakar and A. K. Jain et al 2002). Identification is a critical component in negative recognition applications where the system establishes whether the person is who he denies to be.

A simple biometric system has four important components:

(1) Sensor module: This acquires the biometric data of an individual. An example is a fingerprint sensor that captures fingerprint impressions of a user.

*Corresponding author: **Almas M. N. Siddiqui**

(2) Feature extraction module: This acquired data is processed to extract feature values. For example, the position and orientation of minutiae points in a fingerprint image would be extracted in the feature extraction module of a fingerprint system.
(3) Matching module: In which the feature values are compared against those in the template by generating a matching score. For example, in this module, the number of matching minutiae points between the query and the template will be computed and treated as a matching score.
(4) Decision-making module: In which the user's identity is established or a claimed identity is either accepted or rejected based on the matching score generated in the matching module.

3. Overview of Multimodal biometric system

A biometric system which relies on presence of multiple pieces of evidence for personal identification is called multimodal biometric system. A multimodal system can combine any number of independent biometrics and overcome some of the limitations presented by using just one biometric as your verification tool. Multimodal are generally much more vital to fraudulent technologies, because it is more difficult to forge multiple biometric characteristics than to forge a single biometric characteristic thus provide higher accuracy rate and higher protection from spoofing. Some of the limitations of a unibiometric system can be addressed by designing a system that consolidates multiple sources of biometric information. This can be accomplished by fusing, for example, multiple traits of an individual, or multiple feature extraction and matching algorithms operating on the same biometric. Such systems, known as multibiometric systems (K.A. Toh, X. Jiang and W.Y. Yau et al, 2004; M. Faundez-Zanuy et al, 2004) can improve the matching accuracy of a biometric system while increasing population coverage and deterring spoof attacks. This paper presents an overview of multibiometric systems. There are several multimodal biometric person authentication systems developed in the literature.

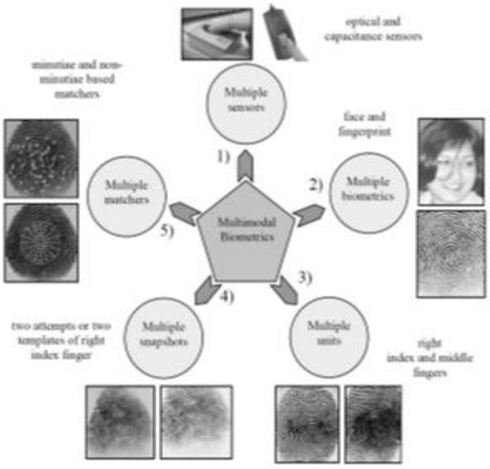
optical and capacitance sensors
minutiae and non-minutiae based matchers
Multiple sensors
face and fingerprint
1)
Multiple matchers
2)
Multiple biometrics
5)
Multimodal Biometrics
3)
4)
two attempts or two templates of right index finger
Multiple snapshots
Multiple units
right index and middle fingers

Fig. 1: Scenarios in a multimodal biometric system (R. Bruneelli and D.Falavigna et al oct.1995).

Advantages of Multibiometric Systems

Besides enhancing matching accuracy, the other advantages of multibiometric systems over traditional unibiometric systems are enumerated below (A.K. Jain and Ross et al, 2002).
1. Multibiometric systems address the issue of non-universality encountered by unibiometric systems.
2. Multibiometric systems can facilitate the filtering or indexing of large-scale biometric databases.
3. It becomes increasingly difficult for an impostor
to spoof multiple biometric traits of a legitimately enrolled individual. If each sub-system indicates the probability that a particular trait is a 'spoof', then appropriate fusion schemes can be employed to determine if the user, in fact, is an impostor.
4. Multibiometric systems also effectively address the problem of noisy data. When the biometric signal acquired from a single trait is corrupted with noise, the availability of other traits may aid in the reliable determination of identity.
5. These systems also help in the continuous monitoring or tracking of an individual in situations when a single trait is not sufficient.
6. A multibiometric system may also be viewed as a fault tolerant system which continues to operate even when certain biometric sources become unreliable due to sensor or software malfunction, or deliberate user manipulation.

Multimodal Biometric Technologies

In order for the biometrics to be ultra-secure and to provide more-than-average accuracy, more than one form of biometric identification is required. This uses a combination of different biometric recognition technologies (A.K. Jain, A Ross and S. Prabhaker, et al 2004). A pattern / template that are going to be identified are going to be matched against every known template, yielding either a score or distance describing the similarity between the pattern and the template. The system assigns the pattern to the person with the most similar biometric template. To prevent impostor patterns (in this case all patterns of persons not known by the system) from being correctly identified, the similarity has to exceed a certain level. If this level is not reached, the pattern is rejected (S. Prabhakar and A. K. Jain et al 2002). With verification, a person's identity is known and therefore claimed a priority to search against. The pattern that is being verified is compared with the person's individual template only. Similar to identification, it is checked whether the similarity between pattern and template is sufficient enough to provide access to the secured system or area.

4. Modules of multimodal biometrics

Multimodal biometric system has four modules:
1. Sensor module,
2. Feature extraction module,
3. Matching module,
4. Decision making module respectively.

Sensor module: - At sensor module biometric modalities are captured and these modalities are given as inputs for feature extraction module.

Feature extraction module: - At feature extraction module features are extracted from different modalities after preprocessing. These features yields a compact representation of these traits or modalities and these extracted features are then further given to the matching module for comparison.

Matching module: - In matching module extracted features are compared against the templates which are stored in database.

Decision making module: - In this module user is either accepted or rejected based on the matching in the matching module.

Multimodal biometric system can operate in serial mode or parallel mode. In serial mode of operation, the output of one modality is used to narrow down the number of possible identities before the next modality is used (R. Bruneelli and D. Falavigna, et al, 1995). This can reduce the overall recognition time. In parallel mode of operation, information from different modalities is used simultaneously. In case of multimodal biometric system decision can be made at various levels of fusion like Feature level fusion, Matching score level fusion and Decision level fusion. The block diagram for general multimodal biometric system is as shown in Figure 2.

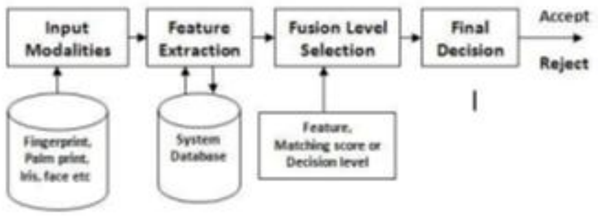

Fig. 2. Block diagram of general multimodal biometrics

5. Different levels of fusion in multimodal biometrics:

Fusion in the context of biometrics can take the following forms:

(1) Single biometric multiple representation.
(2) Single biometric multiple matchers.
(3) Multiple biometric fusions.

1. Single biometric multiple representation

This type of fusion involves using multiple representations on a single biometric indicator. Typically, each representation has its own classifier. The similarity scores reported by these classifiers are then consolidated. Cappelli et al. (2000) describe a fingerprint classification system 1 that combines a structural classifier with a KL transform- based classifier by integrating the scores generated by the two classifiers. This is done by first mapping the scores (which are distance measures) into a common domain via a double sigmoid function and then taking a weighted average in the new domain. Jain et al. (1999) also use multiple classifiers for fingerprint indexing. Their technique uses a K nearest neighbor classifier and a set of 10 neural network classifiers to classify fingerprints. General strategies for combining multiple classifiers have been suggested in (Ho et al., 1994). All the approaches presented there (the highest rank method, the Borda count method and logistic regression) attempt to reduce or rerank a given set of classes. These techniques are thus relevant to the identification problem in which a large number of classes (identities) are present. The fusion in this approach takes place at the matching stage, after the classifiers report a similarity score for each class. Prabhakar and Jain (2002) show that selecting classifiers based on some ‘‘goodness’’ statistic may be necessary to avoid performance degradation when using classifier combination techniques. It should also be possible to combine (concatenate) the feature vectors extracted by the individual classifiers.

2. Single biometric multiple matcher

It is also possible to incorporate multiple matching strategies in the matching module of a biometric system and combine the scores generated by these strategies. Jain et al. (1999b) use the logistic function to map the matching scores obtained from two different fingerprint matching algorithms into a single score. The authors demonstrate that such an integration strategy improves the overall performance of a fingerprint verification system. This type of fusion also takes place at the matching stage of a biometric system. Although there are multiple matchers in this case, all matchers operate on the same representation of the biometric data.

3. Multiple biometric fusions

Multibiometric fusion refers to the fusion of multiple biometric indicators. Such systems seek to improve the speed and reliability (accuracy) of a biometric system (Hong and Jain, 1998) by integrating matching scores obtained from multiple biometric sources. A variety of fusion schemes have been described in the literature to combine these various scores. These include majority voting, sum and product rules, k-NN classifiers, SVMs, decision trees, Bayesian methods, etc. (see for example Ben-Yacoub et al., 1999; Bigun et al., 1997; Dieckmann et al., 1997; Jain et al., 1999d; Kittler et al, 1998; Verlinde and Cholet et al, 1999). An important aspect that has to be addressed in fusion at the matching score level is the normalization of the scores obtained from the different domain experts (Brunelli and Falavigna, 1995). Normalization typically involves mapping the scores obtained from multiple domains into a common domain before combining them. This could be viewed as a two-step process in which the distributions of scores for each domain is first estimated using robust statistical techniques (Hampel et al., 1986) and these distributions are then scaled or translated into a common domain. Besides the techniques described above, other types of fusion are also possible in biometrics:

1. A fingerprint biometric system may store multiple templates of a user_s fingerprint (same finger) in its

database. When a fingerprint impression is presented to the system for verification, it is compared against each of the templates, and the matching score generated by these multiple matchings are integrated.

2. A system may store a single template of a user finger, but acquire multiple impressions of the finger during verification.

3. Another possibility would be to acquire and use impressions of multiple fingers for every user. These possibilities have been discussed in (Jain et al., 1999e).

The layout of a bimodal system is shown in Fig.3. The purpose of this diagram is to illustrate the various levels of fusion for combining two (or more) biometric systems.

According to Jain and Ross (R. Bruneelli and D.Falavigna et al, 1995), there are three fusion levels in multimodal biometrics:

The three possible levels of fusion are:

(a) Fusion at the feature extraction level,
(b) Fusion at the matching score level,
(c) Fusion at the decision level.

It is generally believed that a combination scheme applied as early as possible in the recognition system is more effective (L. Hong and A.K. Jain et al, 1998). These three levels of fusion are described as follows:

1. Fusion at the feature extraction level: The data obtained from each sensor is used to compute a feature vector. As the features extracted from one biometric trait are independent of those extracted from the other, it is reasonable to concatenate the two vectors into a single new vector. Feature reduction techniques may be employed to extract useful features from the larger set of features. It normalizes features from multiple channels and includes all in one vector, and then it selects features using some specific mechanisms, such as sequential forward selection. It calculates distance scores between a query vector and one in the database based on a measure, such as Euclidean distance. Feature Fusion produced best results when modalities are related (e.g. LDA-Red, LDA-Green, LDA-Blue) than when they were unrelated.

*2. Fusion at the matching scores level***:** Each system provides a matching score indicating the proximity of the feature vector with the template vector. These scores can be combined to assert the veracity of the claimed identity. Techniques such as logistic regression may be used to combine the scores reported by the two sensors. Fusion at matching level normalizes scores of matchers to same domain using mechanisms such as Min Max, which maps score values to [0, 1], or Quadric-Line-Quadric function, which tries to separate the genuine and impostor score distributions. Then it may use one or more of following approaches for the actual classification (R. W. Frischholz and U. dieckmann et al, 2000). Fixed rules, such as simple sum, maximum unimodal score, and minimum unimodal score.Trained rules, such as Support Vector Machines, Fisher's Linear Discriminant, Bayesian Classifier, Multi-Layer Perceptron, and Decision Trees (A. Kumar et al, 2003). Adaptive rules, such as assigning less weight to modalities that are disadvantaged by the current environment.

3. Fusion at the decision level: Each sensor can capture multiple biometric data and the resulting feature vectors individually classified into the two classes—accept or reject. A majority vote scheme, such as that employed in (Zuev and Ivanon et al, 1996) can be used to make the final decision.

Fusion of multiple biometrics can be also done at the decision level where each classifier provides its decision as accept or reject. Then the Borda count method can be used for combining the classifiers' outputs. The Borda count is a winner election method in which voters rank candidates in order of preference. In a multi biometric system, fusion is carried out at this level when only the decisions output by the individual biometric matchers are available.

One problem that appears with decision level fusion is the possibility of having a tie. Therefore it is necessary to have more classifiers than classes. Hence, for verification applications, at least three classifiers are needed because only two classes exist in a verification process (yes or no). But for identification cases, it is not practical and even sometimes not feasible to have more classifiers than classes; this is why combination level is usually applied to verification scenarios. Important combination schemes at this level are the serial and parallel combination (AND and OR combinations); where AND combination improves the False Acceptance Ratio (FAR) while the OR combination improves the False Rejection Ratio (FRR), (S.Ribaric, D. Ribaric and N. Pavesic et al, 2003). Fusion at this level is considered to be rigid compared to the other fusion schemes due to the availability of limited information.

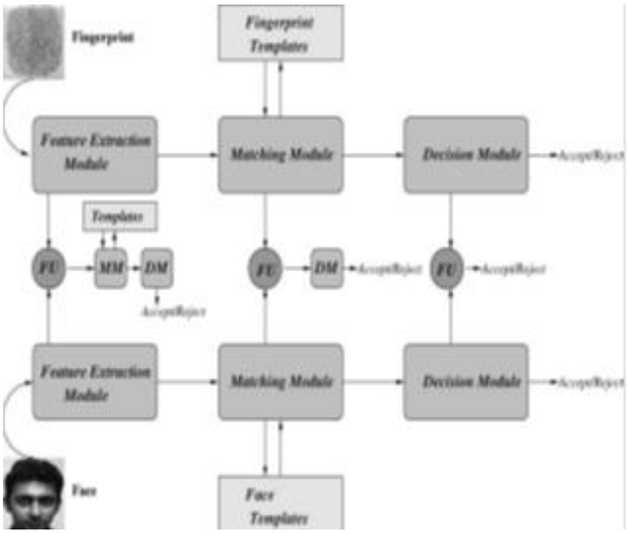

Fig.3: A bimodal biometric system showing the three levels of fusion (FU: fusion module, MM: matching module, DM: decision module).

Sanderson and Paliwal have classified information fusion in biometric systems into two broad categories: pre-classification fusion and post-classification fusion.

Pre-classification fusion refers to combining information prior to the application of any classifier or matching algorithm. In post-classification fusion, the information is combined after the decisions of the classifiers have been obtained.

A. Pre-classification fusion

Prior to classification/matching, integration of information can take place either at the sensor level or at the feature level. The raw data from the sensors are combined in sensor level fusion. For example, the face images obtained from several cameras can be combined to form a single face image. In sensor level fusion, the data obtained from the different sensors must be compatible, and this may not always be possible (e.g., it may not be possible to fuse face images obtained from cameras with different resolution). Feature level fusion refers to combining different feature vectors that are obtained by either using multiple sensors or employing multiple feature extraction algorithms on the same sensor data. When the feature vectors are homogeneous (e.g., multiple fingerprint impressions of a user‟s finger), a single resultant feature vector can be calculated as a weighted average of the individual feature vectors. When the feature vectors are non homogeneous (e.g., feature vectors obtained using different feature extraction techniques, or feature vectors of different biometric modalities like face and hand geometry), we can concatenate them to form a single feature vector. Concatenation is not possible when the feature sets are incompatible (e.g., fingerprint minutiae and Eigen face coefficients). Biometric systems that integrate information at an early stage of processing are believed to be more effective than those systems which perform integration at a later stage. Since the features contain richer information about the input biometric data than the matching score or the output decision of a classifier/matcher, integration at the feature level should provide better recognition results than other levels of integration. However, integration at the feature level is difficult to achieve in practice because of the following reasons:

1. The relationship between the feature spaces of different biometric systems may not be known. In the case where the relationship is known in advance, care needs to be taken to discard those features that are highly correlated. This requires the application of feature selection algorithms prior to classification.
2. Concatenating two feature vectors may result in a feature vector with very large dimensionality leading to the „curse of dimensionality‟ problem. Although, this is a general problem in most pattern recognition applications, it is more severe in biometric applications because of the time, effort and cost involved in collecting large amounts of biometric data.
3. Most commercial biometric systems do not provide access to the feature vectors which they use in their products. Hence, very few researchers have studied integration at the feature level and most of them generally prefer post-classification fusion schemes.

B. Post-classification fusion

Schemes for integration of information after the classification/ matcher stage can be divided into four categories: dynamic classifier selection, fusion at the abstract level, fusion at the rank level and fusion at the matching score level. A dynamic classifier selection scheme chooses the results of that classifier which is most likely to give the correct decision for the specific input pattern. This is also known as the winner-take-all approach and the device that performs this selection is known as an associative switch. Integration of information at the abstract or decision level can take place when each biometric matcher individually decides on the best match based on the input presented to it. Methods like majority voting, behaviour knowledge space, weighted voting based on the Dempster–Shafer theory of evidence, AND rule and OR rule, etc. can be used to arrive at the final decision. When the output of each biometric matcher is a subset of possible matches sorted in decreasing order of confidence, the fusion can be done at the rank level. Ho et al. describe three methods to combine the ranks assigned by the different matchers. In the highest rank method, each possible match is assigned the highest (minimum) rank as computed by different matchers. Ties are broken randomly to arrive at a strict ranking order and the final decision is made based on the combined ranks. The Borda count method uses the sum of the ranks assigned by the individual matchers to calculate the combined ranks.

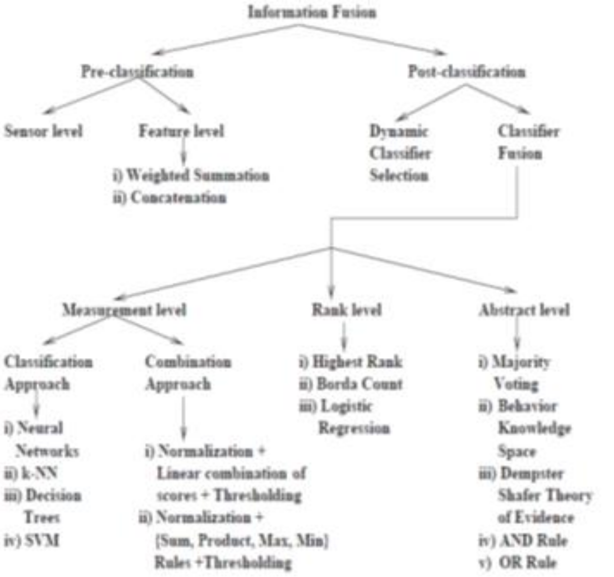

Fig. 2 Approaches to information fusion

The logistic regression method is a generalization of the Borda count method where the weighted sum of the individual ranks is calculated and the weights are determined by logistic regression. When the biometric matchers output a set of possible matches along with the quality of each match (matching score), integration can be done at the matching score level. This is also known as fusion at the measurement level or confidence level. Next to the feature vectors, the matching scores output by the matchers contain the richest information about the input pattern. Also, it is relatively easy to access and combine the scores generated by the different matchers. Consequently, integration of information at the matching score level is the most common approach in multimodal biometric systems.

In the context of verification, there are two approaches for consolidating the scores obtained from different matchers. One approach is to formulate it as a classification problem, while the other approach is to treat it as a combination problem. In the classification approach, a feature vector is constructed using the matching scores output by the individual matchers; this feature vector is then classified into one of two classes: Accept (genuine user) or Reject (impostor). Generally, the classifier used for this purpose is capable of learning the decision boundary irrespective of how the feature vector is generated. Hence, the output scores of the different modalities can be non-homogeneous (distance or similarity metric, different numerical ranges, etc.) and no processing is required prior to feeding them into the classifier. In the combination approach, the individual matching scores are combined to generate a single scalar score which is then used to make the final decision. To ensure a meaningful combination of the scores from the different modalities, the scores must be first transformed to a common domain.

6. Methods for Multimodal Fusion

The fusion methods are divided into the following three categories:

A. Rule-based methods,

B. Classification based methods,

C. Estimation-based methods.

This categorization is based on the basic nature of these methods and it inherently means the classification of the problem space, such as, a problem of estimating parameters is solved by estimation-based methods. Similarly the problem of obtaining a decision based on certain observation can be solved by classification-based or rule based methods. However, if the observation is obtained from different modalities, the method would require fusion of the observation scores before estimation or making a classification decision.

A. Rule-based fusion methods

The rule-based fusion method includes a variety of basic rules of combining multimodal information. These include statistical rule-based methods such as linear weighted fusion (sum and product), MAX, MIN, AND, OR, majority voting. There are custom-defined rules that are constructed for the specific application perspective. The rule-based schemes generally perform well if the quality of temporal alignment between different modalities is good.

B. Classification-based fusion methods

This category of methods includes a range of classification techniques that have been used to classify the multimodal observation into one of the pre-defined classes. The methods in this category are the support vector machine, Bayesian inference, Dempster–Shafer theory, dynamic Bayesian networks, neural networks and maximum entropy model. Note that we can further classify these methods as generative and discriminative models from the machine learning perspective. For example, Bayesian inference and dynamic Bayesian networks are generative models, while support vector machine and neural networks are discriminative models.

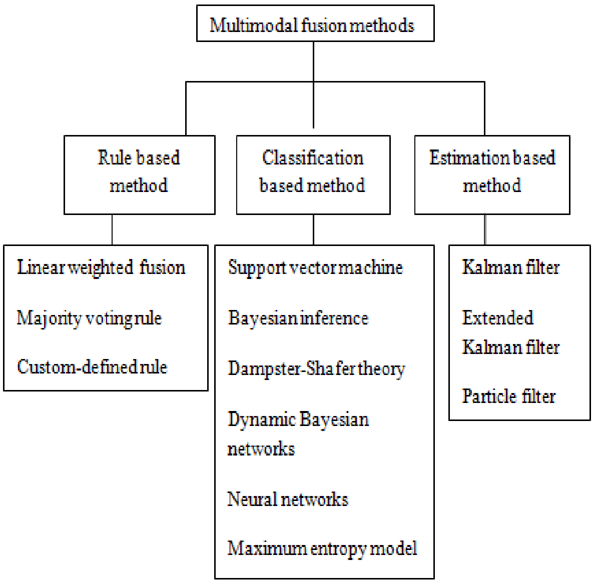

Fig. 3: A Categorization of the Fusion Methods

C. Estimation-based fusion methods

The estimation category includes the Kalman filter, extended Kalman filter and particle filter fusion methods. These methods have been primarily used to better estimate the state of a moving object based on multimodal data. For example, for the task of object tracking, multiple modalities such as audio and video are fused to estimate the position of the object.

6. Concludes the paper with some suggestions for further investigations.

We have observed that multimodal biometrics is frontier to the unimodal biometrics as itovercomes the problems related with unimodal biometrics like noisy data, interclass similarities, intra class variation, non universality and spoofing. There are many multimodal biometric systemsin existence for authentication of a person but still selection of appropriate modals, choice ofoptimal fusion level and redundancy in the extracted features are some challenges in designingmultimodal biometric system that needs to be solved This paper discusses the various scenarios that are possible in multimodal biometric systems, the levels of fusion that are plausible and the integration strategies that can be adopted to consolidate information. A lot of research work is still need in this area. In near future combination of more than two biometrics can apply to enhance the security of our system. By combining multiple biometric traits, the performance of biometric system can be improved. Various applications of multimodal biometrics system and different levels of fusion are discussed. The multimodal biometrics is very popular in these days due to its performance and advance level of security.

Acknowledgement

We are thankful to our Guide Dr. P. D. Deshmukh Principal of Dr. G.Y.P.C.C.S and I.T. for providing valuable guidance and technical support.

References

A. K. Jain, A. Ross, and S. Prabhakar, Jan 2004 An introduction to biometric recognition, *IEEE Trans. on Circuits and Systems for Video Technology,* vol. 14, pp. 4–20.

M. Golfarelli, D. Maio, and D. Maltoni, July 1997 On the error-reject tradeoff in biometric verification systems, *IEEE Trans. on Patt. Anal. and Mach. Intell.,* vol. 19, pp. 786–796.

A. Ross and A. K. Jain, Information fusion in biometrics, Sep 2003 *Pattern Recognition Letters,* vol. 24, pp. 2115– 2125

S. Prabhakar and A. K. Jain, 2002 Decision-level fusion in fingerprint verification, *Pattern Recognition,* vol. 35, no. 4, pp. 861–874.

A.K. Jain, A Ross and S. Prabhaker, Jan. 2004 An introduction to biometric recognition, *IEEE Trans. Circuits and Systems for Video Technology,* vol. 14, no. 1, pp, 4-20.

R. Bruneelli and D.Falavigna, oct.1995 Person identificationusing multiple cues, *IEEE Trans. PAMI, vol. 17, no.10, pp.955-96.*

L. Hong and A.K. Jain, Dec. 1998 Integrating faces and fingerprints for person identification, *IEEE PAMI,* vol. 20, no. 12, pp. 1295-1307.

V. Ghattis, A.G. Bors and I. Pitas, Nov. 1999 Multimodal decision level fusion for person authentication*, IEEE Trans. Systems, Man and Cybernatics,* vol. 29, no. 6, pp, 674-680.

R. W.. Frischholz and U. dieckmann, Feb.2000 Bioid: A multimodal biometric identification system, *IEEE Computer Society, pp. 64-68,. Name Stand. Abbrev., in press*.

A. Kumar et. al., 2003 Person verification using palmprint and handgeometry biometric, proc. *Fourth Int. Conf. AVBPA, pp.668-678*.

S.Ribaric, D. Ribaric and N. Pavesic, 2003. Multimodal biometric user identification system for network based applications, *IEEE Proc. Vision, Image and Signal Processing, vol. 150, no.6,* pp.409-416.

A.K. Jain and Ross, 2002 Learning user specific parameters in multibiometric system, *Proc. Int. Conf. Image Processing (ICIP),* pp. 57-60.

A. K.Jain, L.Hong and Y. Kulkarni, 1999 A multimodal biometric system using fingerprint, face and speech, *Proc. Second Int. Conf.* AVBPA, pp.182-187.

S.Ribaric, I. Fratic and K. Kris, 2005 A biometric verification system based on the fusion of palmprint and face features, *Proc.Fourth Int. Symposium Image and Signal Processing,* pp.12-17.

B.Duc et. al., 1997. Fusion of audio and video information for multimodal person authentication, *Pattern Recogntion Letters*, vol. 18, pp.835-845.

Jain, A.K., Hong, L., Kulkarni, Y., 1999. A multimodal biometric system using fingerprint, face and speech. *In: Second Internat. Conf. on AVBPA, Washington, DC, USA.* pp. 182–187.

Jain, A.K., Prabhakar, S., Ross, A., 1999. Fingerprint matching: Data acquisition and performance evaluation. *Technical Report MSU-TR:99-14, Michigan State University*.

Jain, A.K., Ross, A., Pankanti, S., 1999. *A prototype hand geometry-based verification system, in: Second Internat. Conf. on Audio and Video-based Biometric Person Authentication* (AVBPA), Washington, DC, USA. pp. 166– 171.

A. K. Jain, Arun Ross and U. Uludag, September 2005 *Biometrics Template Security: Challenges and Solutions*, In Proc. of European Signal Processing Conference.

N. Ratha, J. H. Connell, and R. M. Bolle, June 2001 An Analysis of Minutiae Matching Strength, *In Proc. Audio and Videobased Biometric Person Authentication (AVBPA), pp. 223–228, (Halmstad, Sweden),.*

A. Ross and R. Govindarajan, (2005). Feature level fusion using hand and face biometrics, *Proceedings of the SPIE Conference on Biometric Technology for Human Identification II, 5779, pp 196–204*.

K.A. Toh, X. Jiang and W.Y. Yau, (2004 Exploiting global and local decisions for multimodal biometrics verification, *IEEE Transactions on Signal Processing, 52(10),* pp 3059-3072).

M. Faundez-Zanuy, 2004, Data fusion in biometrics, *IEEE Aerospace and Electronic Systems Magazine*, 20(1), pp 34-38.