Comparative Analysis of distinct Fusion levels in Multimodal Biometrics

Vinay Kumar M.S.
M.Tech Student, Signal Processing,
Siddaganga Institute of Technology,
Tumakuru, Karnataka (India).

R.Srikantaswamy, PhD
Professor, Dept. of ECE,
Siddaganga Institute of Technology,
Tumakuru, Karnataka (India).

ABSTRACT
Nowadays, Multimodal biometrics has created a substantial interest in the field of identification management due to higher recognition performance. This paper presents a comparative analysis of different fusion levels like feature level, score level and decision level in multimodal biometrics using fingerprint and face. Histogram of Oriented Gradients (HOG) descriptor has been used for fingerprint recognition, Linear Discriminant analysis (LDA) along with Principal component analysis (PCA) for feature reduction and face recognition. These modalities are combined at different fusion levels and the results have shown that biometric fusion at feature level gives superior performance when compared to score level and decision level.

General Terms
Pattern Recognition, Computer Vision, Identity management, Histogram of Oriented Gradients, Linear Discriminant Analysis.

Keywords
Multimodal Biometrics, Feature level, Score level, Decision level.

1. INTRODUCTION
Biometric Technology is an automatic technique of recognizing a person based of one (Unimodal) or more (Multimodal) behavioral or physiological characteristics. An authentication system is now a part of almost every major information technology. Biometric technology has become the foundation for highly secure person verification and identification. The global-state of information security survey reveals that the security breaches are on rise. Unimodal biometric systems can be hacked easily and it suffers from the problems like noisy sensor data, non-universality, intra-class variation, lack of individuality and spoofing attacks. Multimodal biometrics has additional information regarding various discreet modalities which in turn increases the recognition performance in terms of accuracy and also to overcome the drawbacks associated with unimodal biometrics. A combination technique is necessary which fuses information from diverse modalities so as to have a multimodal biometric system. There are four levels of fusion techniques viz., fusion at sensor level, fusion at feature level, fusion at matching score level and fusion at decision level[1][2]. But the fusion at sensor level is used very rarely and also not compatible in most of the applications.

Fusion levels are broadly classified as,

i) Fusion before matching [3]

Prior to matching, information can be combined either at sensor level or feature level. Raw data obtained from the different sensors are combined in *sensor level fusion* [4]. The fusion at this level is possible only if the multiple cues are either instances of same biometric modality using different compatible sensors or multiple instances of same biometric modality with single sensor.

Feature level fusion [5] combines the different features obtained from different sources like, multiple sensors, multiple units, multiple snapshots and multiple biometrics. If the features are homogeneous, the final fused vector can be computed as a weighted sum of individual features. If the features are non-homogeneous, they are concatenated to form a final vector. It can be noted that fusion prior to matching is more effective than fusion after matching [6], since the features contain richer information.

ii) Fusion after matching [3]
Information fusion at *decision level* [7] can takes place when each unimodal biometric decides on the best match for the input given to it. Many methods [8] are available to arrive at final decision viz., majority voting, AND rule, OR rule etc.

Each biometric matcher output a set of possible scores along with the confidence score for each match, can be fused at *matching score level* [9]. Next to features, matching scores obtained from each of the matchers contain richer information and also easy to access and combine the scores. There are two approaches for consolidating the scores, one is to formulate it as a classification problem, where a feature vector is constructed using the scores obtained from different matchers; this feature vector is then classified as either "Genuine" or "Imposter". Other approach is to formulate it as combination problem, where the scores from different matchers are combined using various fusion rules to make the decision[10].

The Multimodal biometric system showing three levels of fusion is as shown in Figure 1. Many authors have proposed various fusion strategies at different fusion level using different biometric modalities.

Multimodal biometric system consists of sensor module, feature extraction module, matching module, decision module and fusion module. Sensor module is used to capture the biometric traits and these biometric traits are given as input to the feature extraction module. Features are extracted from the different modalities using suitable feature extraction algorithms in feature extraction module. These extracted feature yields the compact representation of the modalities and these features are forward to matching module for comparison. In matching module, extracted features are

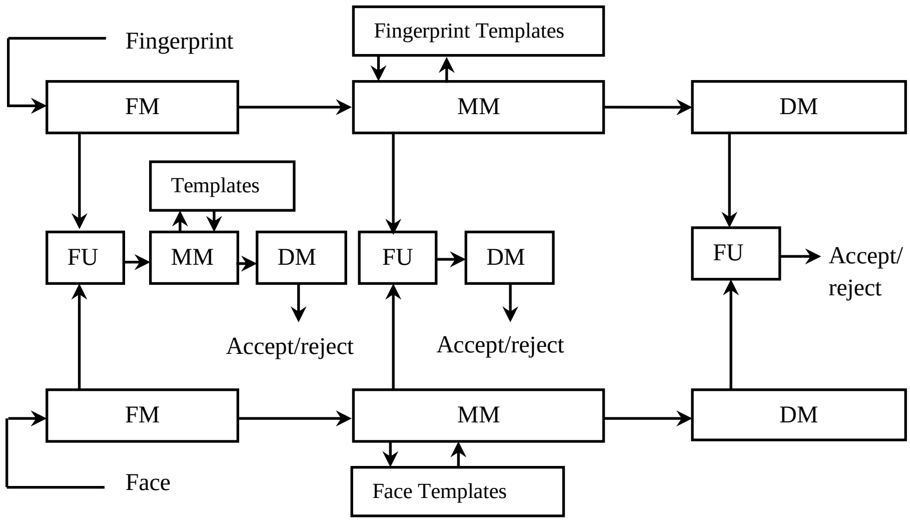

Fig 1: Multimodal Biometric system showing three levels of fusion (FM: Feature extraction Module, MM= Matching module, DM=Decision Module, FU=Fusion Module)

compared with the templates which are stored in the database. Decision is made by the decision module (either accepted or rejected) based on the comparison made in the matching module.

2. FEATURE LEVEL FUSION

The face and fingerprint biometric modalities are used to make decision. The feature extraction algorithms used for face is Linear Discriminant Analysis (LDA) along with Principal Component Analysis (PCA) for feature reduction; and for fingerprint, Histogram of Oriented Gradient (HOG) descriptor has been used.

Here, the features obtained from the face and fingerprint modalities are non-homogenous in nature hence concatenation method has been used to fuse the vectors to form a final fused vector. These fused vectors are given to Support Vector Machine (SVM) for Classification.

Let Y_{face} be the face feature vector extracted by LDA given by $[w_{face_1}, w_{face_2} ..., w_{face_n}]$ and Y_{finger} be the feature vector of fingerprint extracted using HOG given by $[w_{finger_1}, w_{finger_2} ..., w_{finger_n}]$ where n is the number of training samples or test samples. A new feature vector is generated by serially concatenating face feature, Y_{face} and its corresponding fingerprint feature,Y_{finger}. The final feature vector becomes $[w_{face_1}, w_{face_2} ..., w_{face_n}, w_{finger_1}, w_{finger_2} ..., w_{finger_n}]$. Support Vector Machine is trained using the fused feature vectors.

SVM's are based on the structural risk minimization principle. The quality and complexity of the SVM solution does not depend directly on the dimensionality of the input space. The derivation of SVM's is based on constructing an optimal separating hyperplane after linearly or non-linearly mapping the input space into a higher dimensional space.

2.1 Multi-class Classification

There are two basic strategies for solving multiclass problems, say k-class, with SVMs:

- In One-Against-All (OAA) approach, *M* SVMs is trained. Each of the SVMs separates single class from all remaining classes.
- In One-Against-One (OAO) approach, *M(M-1)/2* machines are trained. Each SVM separates a pair of classes.

The Multiclass SVM [11] is to construct a decision function given N samples: where, is a vector of length n and represents the class for set of samples. The classical approach to solving Multiclass SVM classification problems is to consider the problem as a collection of binary classification problems. In OAA method, *M* classifiers are constructed one for each class. The m^{th} classifier constructs a hyperplane between class *m* and the *M-1* remaining classes. A new test sample is allocated to the class that the distance from the margin in the positive direction is maximal. The decision boundary is given by,

$$f(x) = \arg\max_m [(w_m^T x) + b_m]$$

3. SCORE LEVEL FUSION

The similarity scores are generated for fingerprint using the concept of feature matching i.e., given a feature of one image, finds the best matching feature in one or more images and for face, Euclidean distances are calculated, and these are considered as distance scores. Scores obtained from fingerprint and face may not lie in same numerical range. Hence, there is need to transform the scores into same numerical range before combining using normalization techniques viz., min-max, z-score, tanh etc. Min-max normalization has been used which is best suitable for the case where the bounds of the scores are known. Let v_i be a vector which contains the scores. Let v_{ik} and v_{ik}' be the unnormalized and normalized score using min-max normalization which is defined as,

$$v_{ik}' = \frac{v_{ik} - min(\{v_i\})}{max(\{v_i\}) - min(\{v_i\})} \quad (1)$$

The normalized scores of face and fingerprint are combined using different fusion rules viz., weighted sum rule, product rule, min rule, max rule etc. Weighted sum rule has been used for fusion.

$$\text{Final score} = \alpha * \text{face score} + \beta * \text{finger score} \quad (2)$$

Threshold is set based on genuine and imposter distribution. The accuracy can be computed as follows,

$$\text{Accuracy} = 100 - \frac{(\text{FAR+FRR})}{2} \qquad (3)$$

4. DECISION LEVEL FUSION

Decision level fusion consolidates the final decision of unimodal biometric matchers to arrive at the final decision. Each unimodal biometric matcher outputs its own class label saying accept/reject in verification system or identity of user in identification system. Final decision can be made using different techniques, such as, AND rule, OR rule, Majority voting, decision table, Bayesian decision etc. Majority voting method is most suitable for most of the decision level based fusion systems. Since only two biometric modalities were used, logical AND rule was the best suitable method to make the decision. The available information for this fusion method is binary, which allows very simple operations for fusion.

5. EXPERIMENTAL RESULTS

This section compares the accuracies and describes the analysis of different fusion levels.

5.1 Feature level fusion

The Support Vector Machine (SVM) is trained using the concatenated features of both face and fingerprint. Individual modalities like face and fingerprint results in 84.6% and 86% respectively. For training, 10 samples/ subject of both face and fingerprint from 20 subjects (total of 200 samples) were used. For testing, 5 samples/ subject of both face and fingerprint from the 20 subjects were used. This fusion level yields an identification rate of 94%.

$$Identification\,rate = \frac{No.of\ samples\ identified\ correctly}{Total\ no.of\ samples}$$

5.2 Score level fusion

The matching scores obtained from face and fingerprints are normalized using min-max normalization and combined using weighted sum rule. The distributions of both genuine and imposter are computed for 100 samples of genuine user and 100 samples of imposter. The probability distribution plot of both genuine and imposter for fingerprint and face are as shown in Figure 2 (a) & Figure 2 (b).

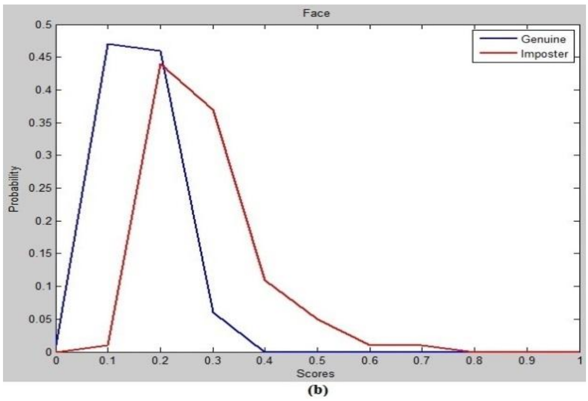

Fig 2(a). Probability distribution of genuine and imposter for fingerprint modality

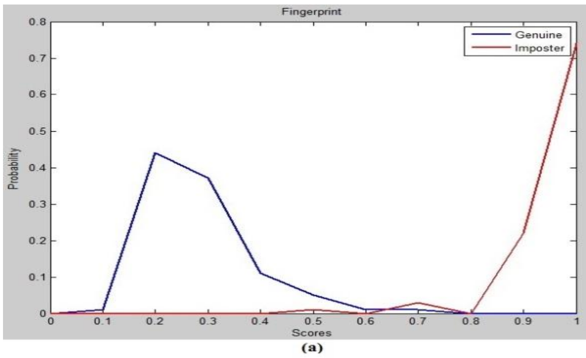

Fig 2(b). Probability distribution of genuine and imposter for face modality

The probability distribution of genuine and imposter for both face and fingerprint modalities fused at matching score level is as shown in Figure 3.

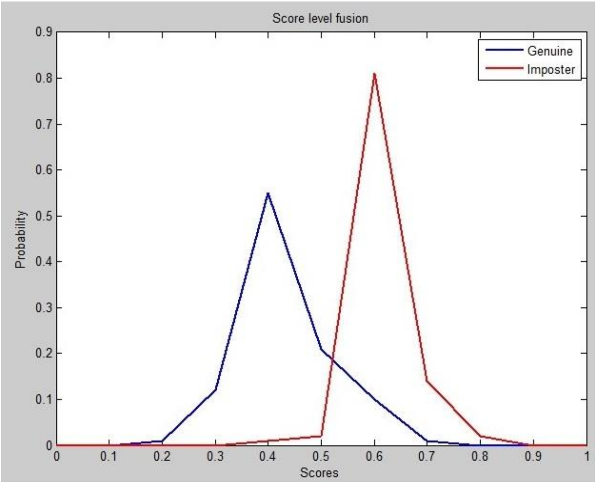

Fig 3. Probability distribution of genuine and imposter using fused scores

The False acceptance rate (FAR), false reject rate (FRR) and accuracies of the individual and fusion biometrics is as shown in Table 1. (verification scenario)

Table 1. Performance of individual and fused biometrics

Biometric Modalities	FRR	FAR	Accuracy
Face	23%	16%	80.5%
Fingerprint	8%	25%	83.5%
Face + Fingerprint	9%	19%	86%

5.3 Decision level fusion

Each individual biometric algorithm gives its own decision (i.e., a binary decision, yes/no). Logical AND rule has been used to combine the decisions as only two modalities are present. The individual decisions are merged from different matchers using AND rule to make the final decision. Again it is tested on 100 genuine and 100 imposter samples which yield an accuracy of 75%.

Accuracy comparison of all three levels has been carried out accordingly and it is shown in Figure 4.

Table 2. Accuracy comparison of different fusion levels

Fusion Levels	Accuracy
Decision level	75%
Matching score level	86%
Feature level	94%

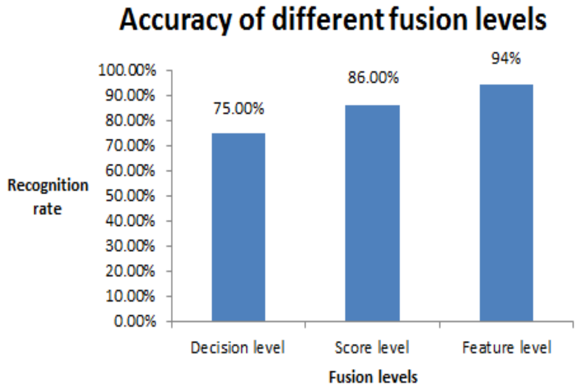

Fig 4. Accuracy comparison of three fusion levels

6. CONCLUSION

In this paper, a research on various multimodal biometric fusion techniques has been carried out. Biometrics considered are face and fingerprint. The features of face and fingerprint are extracted from different feature extraction algorithms. Comparative analysis of feature level fusion, matching score level fusion and decision level fusion in terms of recognition accuracy is performed. The experimental results have shown that fusion before matching approach (feature level fusion) yields better recognition performance compared to fusion after matching approach. As a future work, other biometric modalities can be integrated into the system in order to improve the verification/identification performance.

7. 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] Arun Ross and Anil K. Jain, "Multimodal Biometrics: An Overview", *Proc. Of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria)*, pp. 1221-1224, September 2004.

[3] Arun Ross and Anil. K. Jain, "Information fusion in biometrics", *Elsevier, Pattern Recognition Letters,* vol.24, pp: 2115-2125, 2003.

[4] Raghavendra. R , Rao. A. and Kumar. G.H, "Multisensor biometric evidence fusion of face and palmprint for person authentication using Particle Swarm Optimization (PSO)", *International Journal of Biometrics (IJBM),* Vol. 2, No. 1, 2010.

[5] Hassan Soliman, "Feature level fusion of Palm veins and Signature Biometrics", *International Journal of video & Image Processing and Network Security (IJVIPNS-IJENS)*, vol:12, no.01,2006.

[6] Rattani.A, Kisku.D.R, Bicego.M, and Tistarelli.M, "Feature level fusion of face and fingerprint biometrics", *In proc. Of 1st IEEE international conference on biometrics: Theory, applications and systems*, pp. 1-6, Washington DC, USA.

[7] Yu. P, Xu. D, Zhou. H and Li. H, "Decision fusion for hand biometric authentication", *In proc. of IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS)*, vol. 4, pp. 486-490, Shanghai, China, 2009.

[8] Anil. K. Jain, Lin Hong and Yatin Kulkarni, "A Multimodal biometric system using Face, Fingerprint and Speech", *IEEE Transactions on Pattern Analysis And Machine Intelligence*, Vol. 21, No. 06, December 2000.

[9] Priyanka S. Patil and A. S. Abhyankar, "Multimodal Biometric Identification System Based on Iris & Fingerprint", *IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)*, Volume 1, Issue 6 (Mar.-Apr. 2013), pp: 76-83, 2013.

[10] Lin Hong and Anil. K. Jain, "Integrating faces and fingerprints for personal identification", *IEEE Transactions on pattern analysis and machine intelligence*, vol. 20, no. 12, pp.1295-1307, Dec. 1998.

[11] Fereshteh Falah Chamasemani and Yashwant Prasad Singh, "Multi-class Support Vector Machine (SVM) classifiers: An Application in Hypothyroid detection and Classification", *International conference on Bio-Inspired computing: Theories and Applications*, pp: 352-356, 2011.