Two modal Biometrics System for Efficient Human Recognition

Somesh Yadav

Assistant Professor CSIT, Durg, Chhattisgarh
someshyadav@csitdurg.in

Abstract ***: This paper proposes the two different modal biometrics system for identity verification using two traits i.e., face and fingerprint. The proposed system is designed for applications where the training database contains a face and two fingerprint images. The final decision is made by fusion at "matching score level architecture" in which feature vectors are created independently for query images and are then compared to the enrollment templates which are stored during database preparation for each biometric trait. Based on the proximity of feature vector and template, each subsystem computes its own matching score. These individual scores are finally combined into a total score, which is passed to the decision module. Modal system is developed through fusion of face and fingerprint recognition.***

Key Words ***:*** Biometrics, Two modal, Face, Fingerprint, Fusion, Matching score**.**

1. Introduction

"Biometrics" means "life measurement", but the term is usually associated with the use of unique physiological characteristics to identify an individual. One of the applications which most people associate with biometrics is security. However, biometrics identification has eventually a much broader relevance as computer interface becomes more natural. It is an automated method of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are; face fingerprints, hand geometry, handwriting, iris, retinal, vein, voice etc. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions [1]. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent. In recent years, biometrics authentication has seen considerable improvements in reliability and accuracy, with some of the traits offering good performance. However, even the best biometric traits till date are facing numerous problems; some of them are inherent to the technology itself. In particular, biometric authentication systems generally suffer from enrollment problems due to non-universal biometric traits, susceptibility to biometric spoofing or insufficient accuracy caused by noisy data acquisition in certain environments.

One way to overcome these problems is the use of multi-biometrics. Driven by lower hardware costs, a multi biometric system uses multiple sensors for data acquisition. 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 two modal biometrics). This approach also enables a user who does not possess a particular biometric identifier to still enroll and authenticate using other traits, thus eliminating the enrollment problems and making it universal. A unimodal biometric system [2] consists of three major modules: sensor module, feature extraction module and matching module. The performance of a biometric system is largely affected by the reliability of the sensor used and the degrees of freedom offered by the features extracted from the sensed signal. Further, if the biometric trait being sensed or measured is noisy resultant matching score computed by the matching module may not be reliable. This problem can be solved by installing multiple sensors that capture different biometric traits. Such systems, known as two modal biometric systems [3], are expected to be more reliable due to the presence of multiple pieces of evidence. These systems are also able to meet the stringent performance requirements imposed by various applications. However, two modal systems address the problem of non-universality: it is possible for a subset of users who do not possess a particular biometric. For example, the feature extraction module of a fingerprint authentication system may be unable to extract features from fingerprints associated with specific individuals, due to the poor quality of the ridges. In such instances, it is useful to acquire multiple biometric traits for verifying the identity. Two modal systems also provide anti-spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously. By asking the user to present a random subset of biometric traits, the system ensures that a live user is indeed present at the point of acquisition. However, an integration scheme is required to fuse the information presented by the individual modalities.

This paper proposes an efficient two modal biometric system which can be used to reduce/remove the above mentioned limitations of unimodal systems. Next section presents an overview of two modal biometric system.

2. Two Modal Biometrics System

Two modal biometric systems are those that utilize more than one physiological or behavioral characteristic for enrollment, verification, or identification. In applications such as border entry/exit, access control, civil identification, and network security, two-modal biometric systems are looked to as a means of reducing false non-match and false match rates, providing a secondary means of enrollment, verification, and identification if sufficient data cannot be acquired from a given biometric sample, and combating attempts to fool biometric systems through fraudulent data sources such as fake fingers.

Ross and Jain (2003) have presented an overview of Two modal Biometrics and have proposed various levels of fusion, various possible scenarios, the different modes of operation, integration strategies and design issues. A two modal system can operate in one of three different modes: serial mode, parallel mode, or hierarchical mode. In the serial mode of operation, the output of one modality is typically used to narrow down the number of possible identities before the next modality is used. Therefore, multiple sources of information (e.g., multiple traits) do not have to be acquired simultaneously. Further, a decision could be made before acquiring all the traits. This can reduce the overall recognition time. In the parallel mode of operation, the information from multiple modalities is used simultaneously in order to perform recognition. The levels fusion proposed [2] for two modal systems are broadly categorized into three system architectures which are according to the strategies used for information fusion as shown in Figure 1:

- Fusion at the Feature Extraction Level
- Fusion at the Matching Score Level
- Fusion at the Decision Level

In *Fusion at the Feature Extraction Level*, information extracted from the different sensors is encoded into a joint feature vector, which is then compared to an enrollment template (which itself is a joint feature vector stored in a database) and assigned a matching score as in a single biometric system.

In *Fusion at the Matching Score Level***,** feature vectors are created independently for each sensor and are then compared to the enrollment templates which are stored separately for each biometric trait. Based on the proximity of feature vector and template, each subsystem computes its own matching score. These individual scores are finally combined into a total score which is passed to the decision module.

In *Fusion at the Decision Level*, a separate authentication decision is made for each biometric trait. These decisions are then combined into a final vote. This architecture is rather loosely coupled system architecture, with each subsystem performing like a single biometric system.

A substantial amount of work has been carried out on the combination of multiple classifiers. Most of such work focuses on fusing 'weak' classifiers for the purpose of increasing the overall performance (Tolba & Rezq, 2000) [3]. A hybrid fingerprint matcher [4] which fuses minutiae and reference point location classifiers has been proposed by Ross, Jain & Riesman (2003). It has been reported that the performance of the hybrid matcher is better than individual classifiers.
Apart from fusion of multi classifiers, much work has also been done to combine traits/different modalities at various levels. Yunhong, Tan & Jain (2003) proposed the fusion of iris and face modalities [5] and reported that besides improving verification performance, the fusion of these two has several other advantages. Dass, Nandakumar & Jain (2005) have proposed an approach to score level fusion in two modal biometrics systems [6]. Experimental results have been presented on face, fingerprint and hand geometry using product rule and coupla method. It is found that both fusion rules show better performance than individual recognizers. Common theoretical framework [7] for combining classifiers using sum rule, median rule, max and min rule are analyzed by Kittler et al. (1998) under the most restrictive assumptions and have observed that sum rule outperforms other classifiers combination schemes.

Guiyu Feng et. al. (2004) presents a novel fusion strategy for personal identification using face and palmprint biometrics [8]. The work considers the feature level fusion scheme. The purpose of the proposed paper is to investigate whether the integration of face and palmprint biometrics can achieve higher performance that may not be possible using a single biometric indicator alone. Both Principal Component Analysis (PCA) and Independent Component Analysis (ICA) are considered in this feature vector fusion context. It is found that the performance improved significantly.

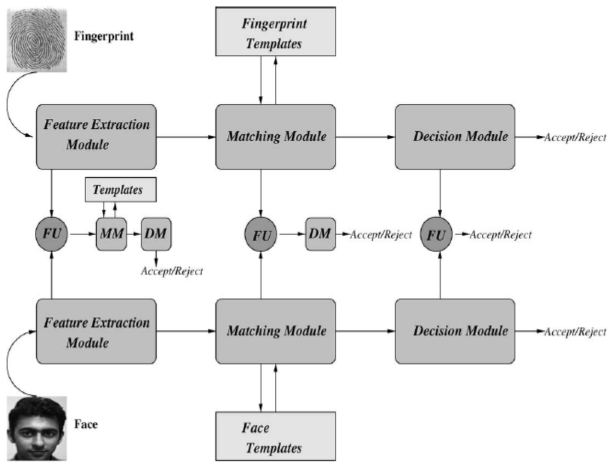

Figure 1**:** Two modal System using three levels of Fusion (taken from Ross & Jain, 2003)

3. Two Modal Biometrics System

Two modal biometric system using two traits i.e., face, fingerprint. In Face Recognition, the input face image is recognized using Elastic Bunch Graph matching algorithm. In Fingerprint Verification, the input image is enhanced to bring out obscure information based on Gabor filtering and matching is done by combination of Reference Point and Minutiae matching algorithms. The modules based on the individual traits returns an integer value after matching the database and query feature vectors. First of all the fusion is done at classifier level i.e., for face and fingerprint are combined at matching score level followed by fusion at multiple modalities level. The final score is generated by using sum of score technique at matching score level which is passed to the decision module. The brief description of various recognition algorithms are presented below:

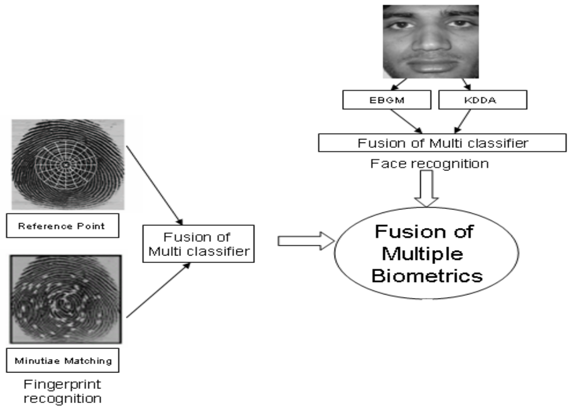

Figure 2 **:** Two modal Biometric System

3.1 Face Recognition

Face Recognition is a noninvasive process where a portion of the subject's face is photographed and the resulting image is reduced to a digital code. Facial recognition records the spatial geometry of distinguishing features of the face [9][10][11]. The recognition algorithm takes facial image, measures the unique characteristics and computes the template corresponding to each face. Using templates, the algorithm then compares that image with another image and produces a score that measures how similar the images are to each other.

Feature Extraction using EBGM and KDDA

Elastic Bunch Graph Matching (EBGM)

Face recognition using elastic bunch graph matching [12] is based on recognizing novel faces by estimating a set of novel features using a data structure called a bunch graph. Similarly for each query image, the landmarks are estimated and located using bunch graph. Then the features are extracted by convolution with the number of instances of Gabor filters followed by the creation of face graph. The matching score (MS_{EBGM}) is calculated on the basis of similarity between face graphs of database and query image. The diagrammatic representation of EBGM algorithm is shown in Figure 3.

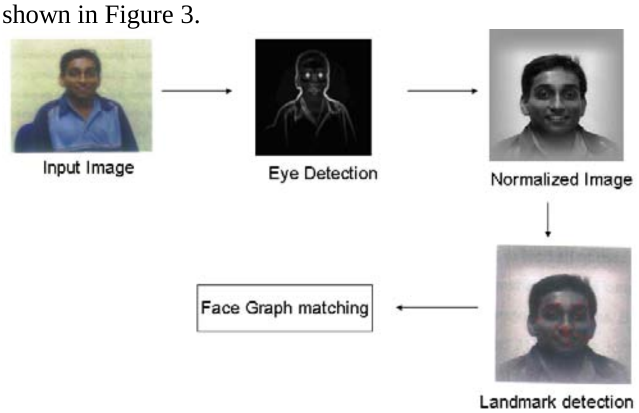

Figure 3 : Steps involved in face recognition

Kernel Direct Discriminant Analysis (KDDA)

Face recognition using KDDA [11] is based on computation of feature space F (from training set) and projection of input pattern into the feature space to calculate significant discriminant features. For each of the *m* features in the database and *n* features in the query image, reference features are chosen depending on the distance and rotation between the positions of features in the feature space. The matching score for each transformation of database and query feature vectors are calculated with respect to reference feature chosen using bounding box technique. MS_{KDDA} is defined by the maximum of all matching scores divided by the maximum number of features (among the query and the database).

Combination of EBGM and KDDA

The matching scores from the above two classifiers are converted from distance to similarity score and are combined at matching score level using sum of score technique which significantly increases the accuracy of the face recognition system.

3.2 Fingerprint Recognition

The fingerprint recognition system has been developed by the fusion of Reference Point and Minutiae Matching Techniques [13][14]. The key steps involved are fingerprint enhancement, feature extraction using Reference point Algorithm and Minutiae Matching approach and computation of matching score. The goal of fingerprint enhancement [15] is to increase the clarity of ridge structure so that minutiae and the reference points can be easily and correctly extracted.

Feature Extraction using Reference point and Minutiae matching approach

Reference Point Algorithm [4] gracefully handles local noise in a poor quality fingerprint. The detection should necessarily consider a large neighborhood in the fingerprint image. For an accurate localization of the reference point, the input image is segmented to remove any kind of noise present in the image. Further Sobel Operator is applied to obtain gradient of segmented image. The Orientation Field is estimated along with the Y component. A specific pattern in which the value of Y-Component is maximum is Reference point (the point of maximum curvature). The finger code is generated by drawing concentric circles of fixed radius centered at reference point (as shown in Figure 4). The image is segmented into 5 tracks and 16 sectors from the detected reference point. The size of the feature vector is 512 values. The distance (D_{Ref}) for the database and query feature vectors is calculated using Euclidean distance method.

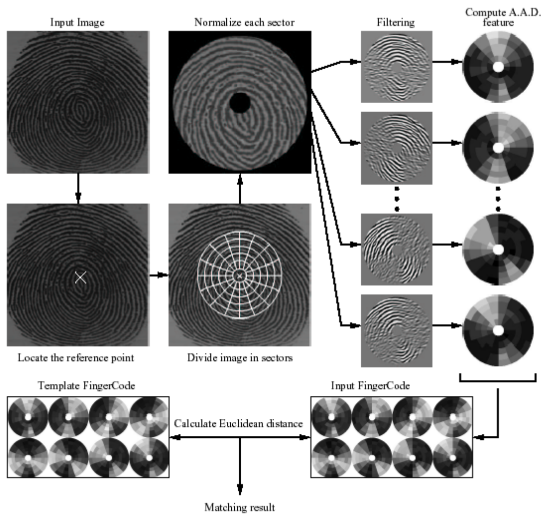

Figure 4 : Diagrammatic representation of Reference point Location algorithm

Minutiae Matching

The input fingerprint image is enhanced using Gabor Filters The enhanced image is further binarized and thinned using a morphological operation that successively erodes away the foreground pixels until they are one pixel wide. The thinned image is used to detect minutiae points [4] by locating ridge ending and bifurcations using Crossing Number (*CN*) method. The matching score MS_{MIN} between the database and query image is computed using Elastic matching approach [13].

Combination of Reference Point and Minutiae Matching Algorithm

The matching scores from the above two classifiers are converted from distance to similarity score and are combined at matching score level using sum of score technique which significantly increases the accuracy of the fingerprint system.

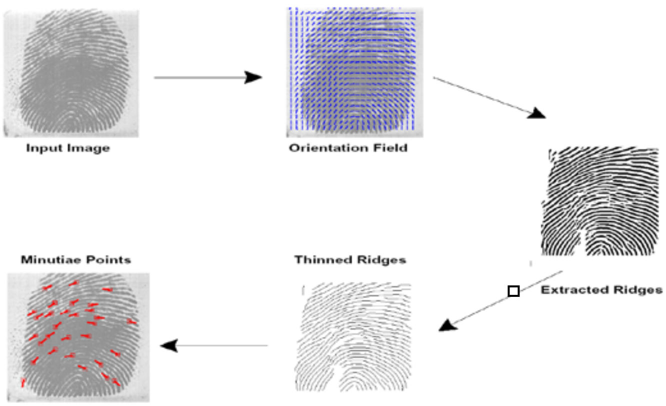

Figure 5 Steps involved in minutiae extraction

3.3 Fusion

The different biometrics systems can be integrated at multi-classifier and multi-modality level to improve the performance of the verification system. However, it can be thought as a conventional fusion problem i.e. can be thought to combine evidence provided by different biometrics [16] to improve the overall decision accuracy.

The two modal biometric system at multi-classifier and multi-modalities level. At multi- classifier level, multiple algorithms are developed and combined these traits like face and fingerprint. The following steps are performed for fusion at classifier level:

S1: Given a query image as input, features are extracted by the individual recognizers and then an individual comparison algorithm for each recognizer compares the set of features and calculates the matching scores or distances corresponding to each recognizer for various traits.

S2: The scores/distances obtained in S1 are normalized to a common range between 0 to 1.

S3: These scores are then converted from distance to similarity score by subtraction from 1 if it is a dissimilarity score. For example the dissimilarity scores, in case of face recognition using reference point algorithm (D_{Ref}).

S4: The matching scores are further rescaled so that threshold value becomes same for each recognizer.

S5: Then the combined matching score is calculated by fusion of the matching scores of multiple classifiers using sum rule technique.

$$MS_{Face} = \frac{\alpha \times MS_{EBGM} + \beta \times MS_{KDDA}}{2},$$

$$MS_{Finger} = \frac{\alpha \times MS_{Ref} + \beta \times MS_{MIN}}{2}$$

where α and β are the weights assigned to individual classifiers. Currently equal weightage is given to each classifiers and the value of α and β is one.

The two modal biometric system by integrating these traits i.e., face and fingerprint at matching score level. Based on the proximity of feature vector and template, each subsystem computes its own matching score. These individual scores are finally combined into a total score, which is passed to the decision module. The same steps for fusion at classifiers level are followed for multiple modalities level i.e., matching scores are computed for each trait followed by normalization the common scale and distance to similarity score ınversion for all the traits. The matching scores are further scaled so that the threshold value becomes common for all e subsystems. Finally, the sum of score technique is applied r combining the matching scores of traitsre. Thus the final ore MS_{Final} is given by,

$$MS_{Final} = \frac{1}{4} (\alpha \times MS_{Face} + b \times MS_{Sign})$$

here MS_{Face} = matching score of face, MS_{Finger} = matching ore of fingerprint and MS_{Sign} = matching score of signature ıd a and b are the weights assigned to the various traits. ırrently, equal weightage is assigned to each trait so the ılue of a and b is one. The final matching score (MS_{Final}) is compared against a certain threshold value to recognize the person as genuine or an imposter.

4. Conclusion

Biometrics systems are widely used to overcome the traditional methods of authentication. But the unimodal biometric system fails in case of lack of biometric data for particular trait. Thus the individual scores of two traits (face and signature) are combined at classifier level and trait level to develop a two modal biometric system. The performance and accuracy of two modal system performs better as compared to unimodal biometrics with accuracy of more than 90%. However, it is worth studying the results by assigning different weightage to different traits. At present equal weightage is assigned to each trait.

References

[1] L. Hong, A. Jain & S. Pankanti, Can Multibiometrics Improve performance, Proceedings of AutoID 99, pp. 59-64, 1999.

[2] A. Ross & A. K. Jain, Information Fusion in Biometrics, Pattern Recognition Letters, 24 (13), pp. 2115-2125, 2003.

[3] A.S. Tolba & A. A. Rezq, Combined Classifier for Invariant Face Recognition, Pattern Analysis and Applications, 3(4), pp. 289-302, 2000

[4] A. Ross, A. K. Jain & J.A. Riesman, Hybrid fingerprint matcher, Pattern Recognition, 36, pp. 1661–1673, 2003

[5] W. Yunhong, T. Tan & A. K. Jain, Combining Face and Iris Biometrics for Identity Verification, Proceedings of Fourth International Conference on AVBPA, pp. 805-813, 2003

[6] S. C. Dass, K. Nandakumar & A. K. Jain, A principal approach to score level fusion in Two modal Biometrics System, Proceedings of ABVPA, 2005

[7] J. Kittler, M. Hatef, R. P. W. Duin, & J. Mates, On combining classifiers, IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(3), pp. 226–239, 1998

[8] G. Feng, K. Dong, D. Hu & D. Zhang, When Faces Are Combined with Palmprints: A Novel Biometric Fusion Strategy, ICBA, pp. 701-707, 2004

[9] I. Craw, D. Tock & A. Bennett, Finding Face Features, Proceedings Second European Conference Computer Vision, pp. 92-96, 1992.

[10] C. Lin & Kuo-Chin Fan, Triangle-based approach to the detection of human face, Pattern Recognition, 34, pp. 1271-1284, 2001.

[11] Juwei Lu, K. N. Plataniotis & A. N. Venetsanopoulos, Face Recognition Using Kernel Direct Discriminant Analysis Algorithms, IEEE Transactions on Neural Networks, 14 (1), pp. 117-126, 2003.

[12] D. S. Bolme, J. R. Beveridge, M. L. Teixeira & B. A. Draper, The CSU Face Identification Evaluation System: Its Purpose, Features and Structure, Proceedings 3rd International Conference on Computer Vision Systems, 2003.

[13] N.K.Ratha, K.Karu, S.Chen & A.K.Jain, A Real-time Matching System for Large Fingerprint Database, IEEE Transactions on Pattern Analysis and Machine Intelligence, 18 (8), pp. 799-813, 1996

[14] A.K.Jain, L.Hong & R.M.Bolle, On-line Fingerprint Verification, IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(4), pp. 302-313, 1997

[15] L. Hong, Y. Wan & A. Jain, Fingerprint Image Enhancement: Algorithm and Performance Evaluation, IEEE Transcations on Pattern Analysis and Machine Intelligence, 20(8), pp. 777-789, 1998

[16] J. G. Daugman, High confidence visual recognition of persons by a test of statistical independence, IEEE Transactions on Pattern Analysis and Machine Intelligence Vol. 15, pp. 1148–1161, 1993

[17] C. H. Daouk, L. A. El-Esber, F. D. Kammoun & M. A. Al-Alaoui, Iris Recognition, Proceedings of the 2nd IEEE International Symposium on Signal Processing and Information Technology, pp. 558-562, 2002

[18] G. Ravichandran & M. M. Trivedi, Circular-Mellin Features for Texture Segmentation, IEEE Transactions on Image Processing Vol. 4, pp. 1629-1640, 1995

[19] J. J.Brault & R. Plamondon, Segmenting Handwritten Signatures at Their Perceptually Important Points, IEEE Transactions on Pattern Analysis and Machine Intelligence, 15

[20] M. Ammar, T. Fukumura, & Y. Yoshida, A new effective approach for off-line verification of signature by using pressure features. 8th International Conference on Pattern Recognition, pp. 566-569, 1986

[21] M. A. Ismail, S. Gad, Off-line Arabic signature recognition and verification, Pattern Recognition, 33 pp. 1727-1740, 2000