BIOMET: A Multimodal Biometric Authentication System for Person Identification and Verification using Fingerprint and Face Recognition

Hiren D. Joshi
Phd, Dept. of Computer Science
Rollwala Computer Centre
Gujarat University, Ahmedabad

ABSTRACT

This paper suggests the multimodal biometrics system for identity verification using two traits: face and fingerprint. The proposed system is intended to use for the training database includes a face and four fingerprint images for each individual. The final decision is made by first individual score of face and fingerprint compares with enrolled templates and then makes fusion at matching score level architecture. The enrolled templates are stored in database. Each subsystem computes its own matching score by using closeness of feature vector and template. The decision module decides the final score by combining individual score of each trait. Multimodal system is developed through fusion of face and fingerprint recognition. The result is significantly improved by using multimodal biometric authentication.

General Terms

Biometrics, Multimodal, Fingerprint, Face

Keywords

Biometrics, Multimodal, Face, Fingerprint, Fusion, Matching score

1. INTRODUCTION

“Biometrics” means “life measurement”, but the term is generally related with the use of unique physiological characteristics to identify an individual. Biometric is mainly used for security. So, the biometric authentication application increases nowadays. Biometrics is an automated method of identify or verify a person based on his physiological and/or behavioral characteristics. The other traits of biometrics are: retinal, hand geometry, iris, handwriting, voice, gait etc.

Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions [1]. The need for highly secure identification and verification arise as the security breach and transaction fraud increases. Biometric authentication is considered reliable and secure in recent time, though it has some challenges. These challenges include enrollment problems – specially for elder and child - , spoofing of biometric trait or noisy data capture in certain operational environment. To overcome the limitations of single biometric trait, it may be feasible to deploy biometric system which uses more than one biometric characteristic. The combination can be either biometric characteristic with non-biometric characteristic or more than one different biometric characteristic. If the system uses more than one biometric trait, then the integrated system is known as multi-biometric system or multimodal biometric authentication system.

Multi-biometric system may be more reliable and provide higher verification rates as there are multiple independent biometric characteristics are used. Multi-biometric systems address the problem of non-universality, since multiple traits ensure sufficient population coverage, and provide anti-spoofing measures by making it difficult for an intruder to steal multiple biometric traits of a genuine user [2].

Sources of information in a multibiometric system may include
(i) multiple sensors to capture the same biometric trait (e.g., face captured using optical and range sensors),
(ii) multiple representations or multiple algorithms for the same biometric trait (e.g., texture and minutiae-based fingerprint matchers),
(iii) multiple instances of the same biometric trait (e.g., left and right iris),
(iv) multiple samples of the same biometric trait (e.g., two impressions of a person's right index finger), and
(v) multiple biometric traits (e.g., face and iris).[3]

The logic used in multi-biometrics system must be determined. There is logical integration of each individual biometric method in multi-biometric system.

The logic of the multi-biometric system may be implemented in an AND configuration or in an OR configuration [2]. The design of multi-biometric system has to determine the type of information which is used for fused. Depending on the type of information that is fused, the fusion scheme can be classified as sensor level, feature level, score level and decision level fusion. [4]

2. MULTIMODAL BIOMETRICS SYSTEM

The multimodal biometric system is developed using two character i.e., face and fingerprint (as shown in Figure 5). In Face Recognition, the input face image is recognized using Verilook 2.0 software. In Fingerprint Verification, the input image is recognized using FVS 4.2 software.
Each individual biometric trait returns an integer value after matching the database template and query feature vectors. The first fusion is done at classifier level i.e., for face, fingerprint are combined at matching score level. Then the second fusion is done at multiple modalities level. The final score is generated at matching score level. The matching score level use sum

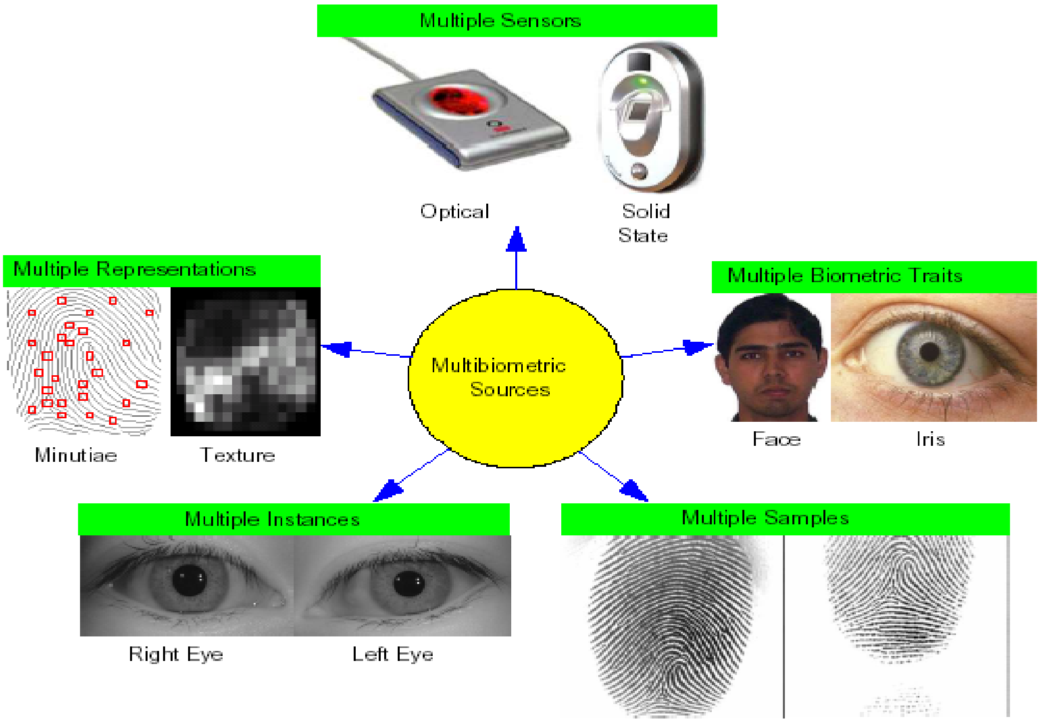

Fig 1: Various sources of information that can be fused in a multibiometric system. [3]

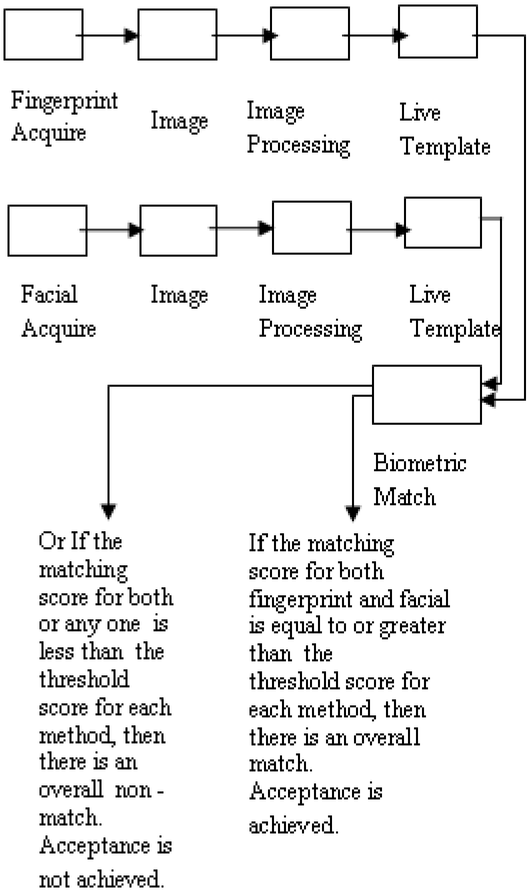
Fingerprint Acquire
Image
Image Processing
Live Template
Facial Acquire
Image
Image Processing
Live Template
Biometric Match
Or If the matching score for both or any one is less than the threshold score for each method, then there is an overall non - match. Acceptance is not achieved.
If the matching score for both fingerprint and facial is equal to or greater than the threshold score for each method, then there is an overall match. Acceptance is achieved.

Fig 2: Multibiometric System using AND Configuration.

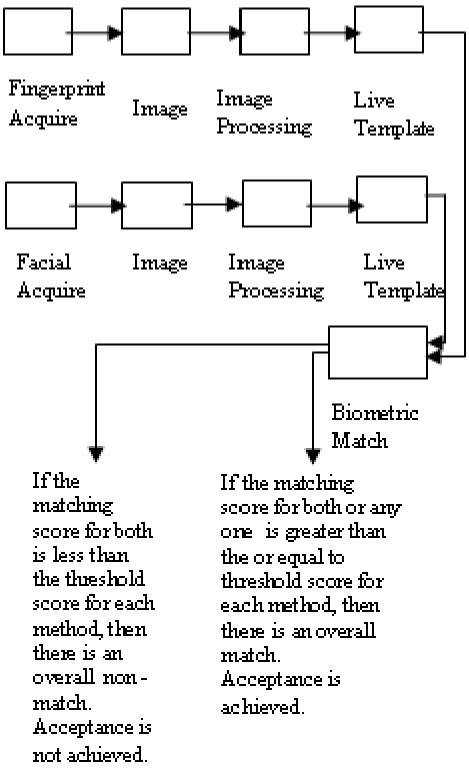
Fingerprint Acquire
Image
Image Processing
Live Template
Facial Acquire
Image
Image Processing
Live Template
Biometric Match
If the matching score for both is less than the threshold score for each method, then there is an overall non - match. Acceptance is not achieved.
If the matching score for both or any one is greater than the or equal to threshold score for each method, then there is an overall match. Acceptance is achieved.

Fig 3: Multibiometric System using OR Configuration.

of score technique. The final score is passed to the decision module.

To improve the performance of the verification system, the integration of different biometric system is done at multi-classifier and multi-modality level. Although, it is considered as a conventional fusion problem i.e. can be thought to combine evidence provided by different biometrics [5] to improve the overall decision accuracy.

The multimodal biometric system is developed at multi-classifier and multi-modalities level. In multi-classifier level, multiple algorithms are developed and combined for traits like face and fingerprint.

The following steps are performed for fusion at classifier level:[6]

Step 1: A query is given as input. The scanner/Camera extracts the features and individual comparison algorithm for each trait compares the features and calculates the matching scores or distance for the traits.

Step 2: Normalized the scores/distances get in step 1 are in a common range between 0 and 1.

Step 3: If these score are dissimilar, then the score is subtract from 1. Now the scores are represent similarity score for each trait.

Step 4: To make the threshold value same for each trait, the matching scores are further rescaled.

Step 5: Finally, the combined matching score is calculated using sum rule technique by fusion of the matching score of each trait.

The multimodal biometric system is developed by integrating two traits (face and fingerprint) at matching score level. Each subsystem calculates its own matching score based on the closeness of feature vector and database template matching. The decision module gets the total score. Total score is a combined score of individual score. The same steps are followed for fusion at classifier level for multiple traits level i.e. , Each trait matching score is computed, then normalize it common scale of 0 to 1. After normalize the score, if there is dissimilarity then the score subtracted from 1 so now it shows similarities score. To make the common threshold value for each subsystem, the scores are again rescaled. Finally the combined matching score is calculated by using the sum of score technique.

So, the final score , denoted as MSFinal is given by

$MS_{Final} = (a\times MS_{Face} + b\times MS_{Finger}) /2$ [7]

where MS_{Face} = matching score of face
MS_{Finger} = matching score of fingerprint and
a, b, are the weights assigned to the various traits.

Currently, each trait has equal weight age assigned.

So a = 1 and b = 1

To recognize the person, the final matching score (MS_{Final}) is compared against a precise threshold value. If the matching score is greater than or equal to threshold value then the person is genuine else an impostor.

3. Hardware and Software used for Multimodal Biometric Authentication System

Hardware used for Face Recognition

Logitech Camera 1.3 Mega pixel sensor with RightLight™ 2 technology

Software used for Face Recognition

VeriLook 2.0

Hardware used for Fingerprint Recognition

Digital Persona U.are.U. Fingerprint Reader

Software used for Fingerprint Recognition

Fingerprint Verification System (FVS) 4.2

Generation of the Multimodal Database

The multimodal database used in our experiments was constructed by merging two separate databases of 200 users each. 200 face images were acquired using a CCD camera (640 X 480). 200 fingerprint impressions (of the same finger) were obtained using a Digital Biometrics sensor (512 X 512). The random pair of each trait for the users is generated by mutual independence assumption of the biometric traits. Each user biometric data is compared with database. The database has all users' biometric data. The comparison recognizes the genuine user.

	Finger	**Face**
No. of users	200	200
No. of Impressions	4	1
Image Size	512 X 512	640 X 480
Template Size	256 – 1200 Bytes	84 – 2000 Bytes
Image Acquisition	Digital Persona U.are.U. (optical)	Logitech Camera (CCD)
Software	Finger Print Verification System (FVS) 4.2	Veri Look 2.0

Table 1: Database for face and fingerprint

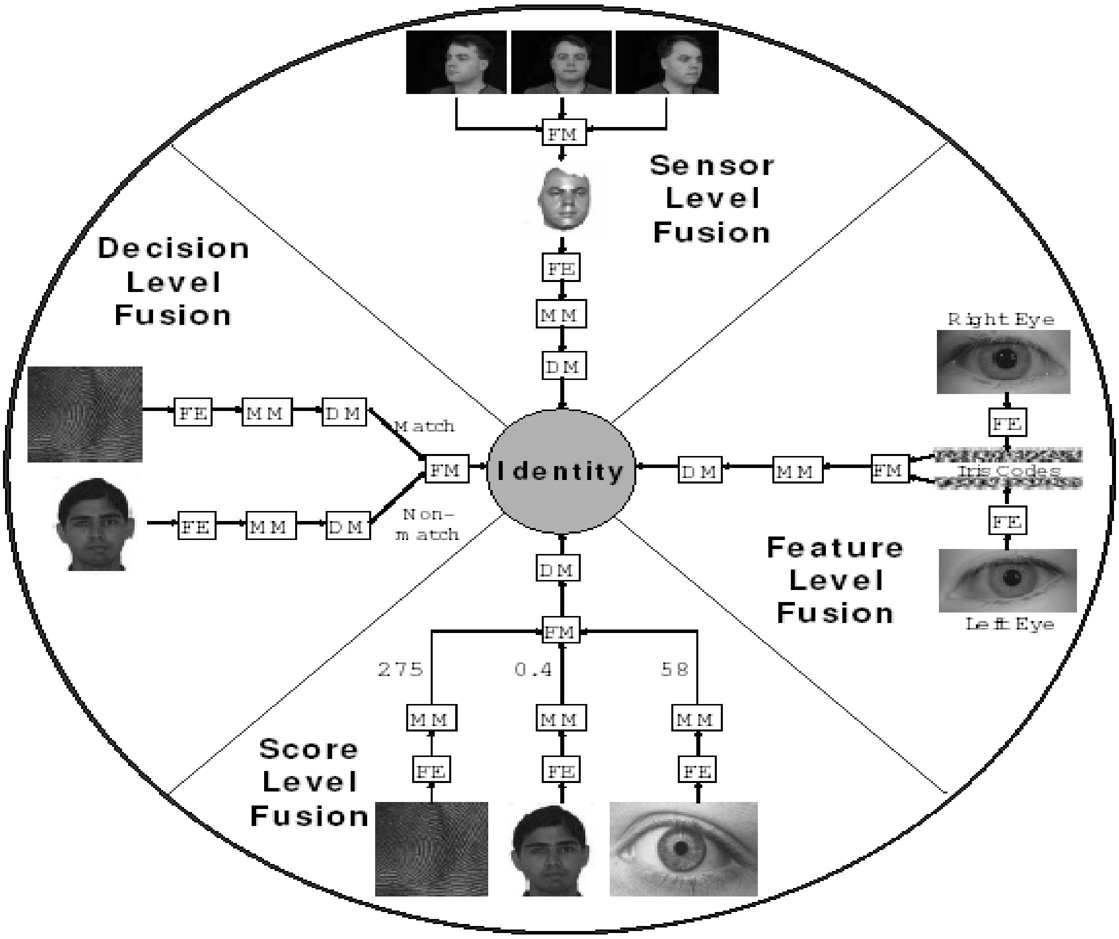

Fig 4: Fusion can be accomplished at various levels in a biometric system. [3]

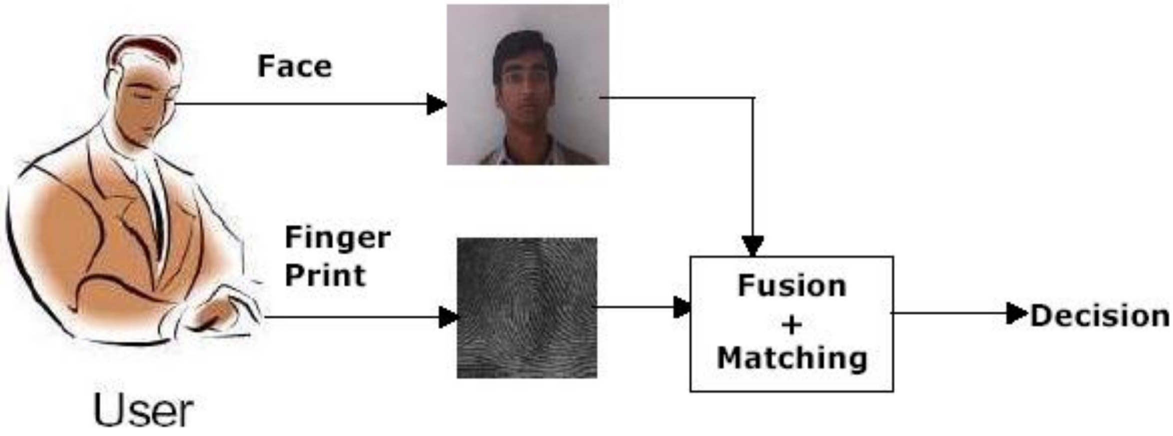

Figure 5: The multimodal biometric system is developed using two traits

4. Experimental Results of Multimodal Biometric System

The multimodal systems have been tested on databases containing 200 individuals. The multimodal biometric databases can be either true or virtual. True multimodal database is a database consists of different biometric traits obtained from the same person. Virtual multimodal database is a database consists of pairing a biometric trait from one unimodal database with another unimodel database. The virtual multimodal biometric database is based on the assumption that different biometric traits of the same person are independent. The data has taken from 200 different users vary from the ages 20-52 which includes both male and females. The data are taken at normal computer laboratory environment.

System	Failure to Enroll Rate
Face	0.0%
Fingerprint	1.0%

Table 2: Failure to Enroll Rate

FAR (t) = (1 – FTA) FMR (t)
FRR (t) = (1 – FTA) FNMR (t) + FTA

Where FTA is the failure to acquire rate, FNMR is the false non- match rate, and FMR is the false match rate. The false match and non- match rates are used to measure the accuracy of the matching process. t is used for the decision threshold. The decision threshold is the value which set initially to determine whether a user is accepted or rejected by the system according to his matching score.

The failure to acquire rate measures the ratio of attempts for which the system is unable to capture or locate a sufficient quality image. This may happen simply when the image that was captured doesn’t meet the quality requirements of the system.

System	Failure to Acquire Rate
Face	0.0%
Fingerprint	0.5%

Table 3: Failure to Acquire Rate

These tables exclude instances of user errors such as not correctly positioning fingers on the fingerprint device.

System	False Acceptance Rate
Face	2.5%
Fingerprint	1.5%

Table 4: False Acceptance Rate

System	False Rejection Rate
Face	6%
Fingerprint	2.5%

Table 5: False Rejection Rate

False Accept Rate (FAR)	False Reject Rate (FRR)		
	Face	Fingerprint	Multimodal
1%	14.45%	3.6%	1.53%
0.1%	41.32%	6.9%	4.30%
0.01%	62.5%	9.4%	6.6%
0.001%	66.27%	15.2%	10.33%

Table 6: FRR Vs FAR in a Multimodal Biometric Authentication System

The above table shows result for single biometric trait and then integration of these two single multiple biometric traits. As the data shows single biometric has a high False Rejection Rate (FRR) while the integration of fingerprint and face has low FRR for the same False Acceptance Rate (FAR). The following chart shows a comparison of the data presented in the table. As from the chart we can say that the multimodal (integration) of the biometric trait has significantly improved the performance.

5. CONCLUSION

Biometric systems are widely used for solving the problems of traditional methods of authentication. In spite of that, the unimodal biometric system may fails because lack of biometric data for particular trait. Multimodal biometric helps to solve the issue of unimodal biometric as there are more than one biometric data needed. The multimodal biometric takes the individual scores of two traits (face and fingerprint) which are combined at classifier level and trait level. The tables and comparison chart shows that multimodal system performs better as compared to unimodal biometrics. The result is significantly improved compare to unimodal biometric system. In this paper, equal weightage is assigned to each trait (face and fingerprint). The result might be vary if different weightage is assign to different trait.

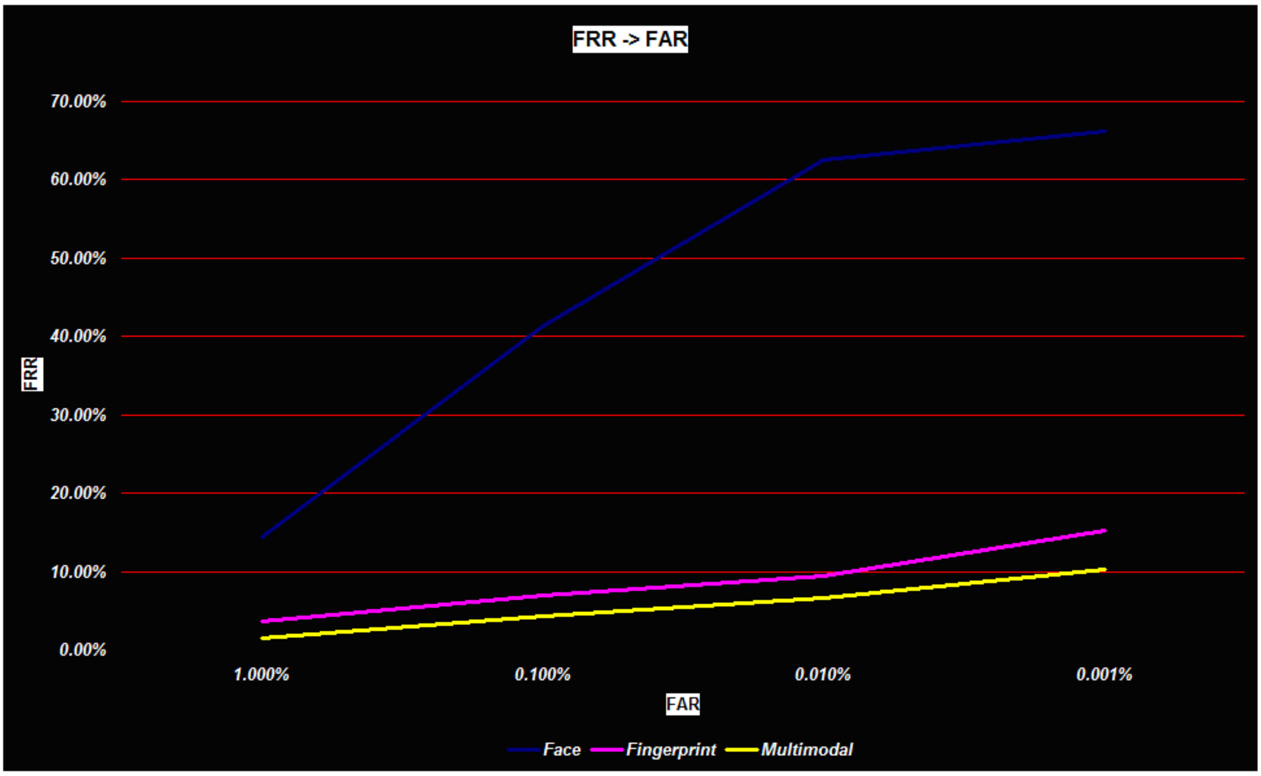

Fig 6: Comparison of FRR -> FAR for Face, Fingerprint and Multimodal biometric

REFERENCES

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

[2] Daugman J. “Combining Multiple Biometrics”, the Computer Laboratory at Cambridge University, 2000.

[3] Karthik Nandakumar, “Multibiometric Systems: Fusion Strategies and Template Security”, Michigan State University, 2008

[4]A. Ross, K. Nandakumar, and A. K. Jain. *Handbook of Multibiometrics*. Springer, 2006.

[5] 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 [original 16 , MMB]

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

[7] Phalguni Gupta, Ajita Rattani, Hunny Mehrotra, Anil Kumar Kaushik, “Multimodal Biometrics System for Efficient Human Recognition”, Proceedings -SPIE The international society for optical engineering, 2006 Vol. 6202 , Pages: 62020Y