Hybrid Primary and Secondary Biometric Fusion

Kiran Kulkarni
Department of Instrumentation
Hubli (Karnataka)
India

Raghavendra Shet
Department of Instrumentation
Hubli (Karnataka)
India

Nalini Iyer
Department of Instrumentation
Hubli (Karnataka)
India

ABSTRACT
Face and Fingerprint identifications are one of the basic forms of person's identification and they are well known for universality. They remain efficient and acceptable biometric trait in the society and hybrid fusion of these traits will increase a performance of one's system and also accuracy therefore ,this paper gives an idea about fusion of primary and secondary biometric information providing two levels of security which can be used in the field of criminal identification and prison security based application the most simple and yet strong fusion rules are used to combine these above data such that correct identification of person is authenticated. This paper also gives information on how system reliability can be increased.

Keywords
Secondary Biometric, Primary Biometric, Hybrid System.

1. INTRODUCTION
Identity recognition has become an important factor in the field of military and security applications from past few decades; demand is increasing for safe and reliable automatic user identification system. Biometric Identification [1] is the area related to person recognition by means of Physiological and behavioral features (fingerprints, iris, voice, face, etc.).

The following are the previous literary works in this field:

Subbarayudu *et al* [2] Presented experimental results of multi biometric system (Iris and palm print). The system fusion utilizes a matching score feature in which each system provides a matching score indicating the similarity of the feature vector with the template vector.

Multi biometric method using a combination of Fast Fourier Transform (FFT) and Gabor filters to enhance fingerprint imaging was proposed by Aguilar *et al.* [3] a novel stage for recognition using local features and statistical parameters were used.

Conti *et al.* [4] proposed a multimodal biometric system using two different Fingerprint acquisitions. The matching module integrates fuzzy logic methods for matching-score fusion.

From the survey made, it is evident that combining different biometric modalities enables to achieve better performances than techniques based on single modalities. Therefore in the proposed work we follow Hybrid fusion which not only saves systems time while recognition step but also aims at displaying genuine imposter. And these surveys just provideinformation about fusing two different modalities but the proposed methodology uses fusion at different level.

The organization of the paper is, section 1 describes the introduction with the highlighted view of an objective of the work which is carried out in this paper. Section 2 explains the methodology of this paper, also discussed the block diagram and describes the performance evaluation of the system. Section 3 deals with the experimental results and discussion. Section 4 deals with the conclusions and possible directions for future work.

2. PROPOSED METHODOLOGY
The proposed work consists of two biometric traits (Face and Fingerprint) and it aims at fusing these two biometric templates in building a hybrid recognition model (Figure 1). And it works in the form of if-else construct i.e. if the fingerprint module (Primary biometric system with threshold 0.98) fails to identify the correct identity then the values of this trait are stored into a database [5] and then the module scans for secondary biometric module which again comprises of score level fusion of two different face recognition system (Multi-algorithm system) as shown in Figure 1, at last matching rate of primary and secondary biometric systems are fused together using decision rule. [6]

Now let us look into these systems one by one:
Primary Biometric System: This system consists of a fingerprint recognition system. Here minutiae based feature extraction and CN number based matching algorithm is carried out to identify genuine imposter. To obtain accurate false rejection rate the primary system is maintained with the threshold of 0.98 (This increase in threshold is generally chosen for security based application to obtain accurate results).

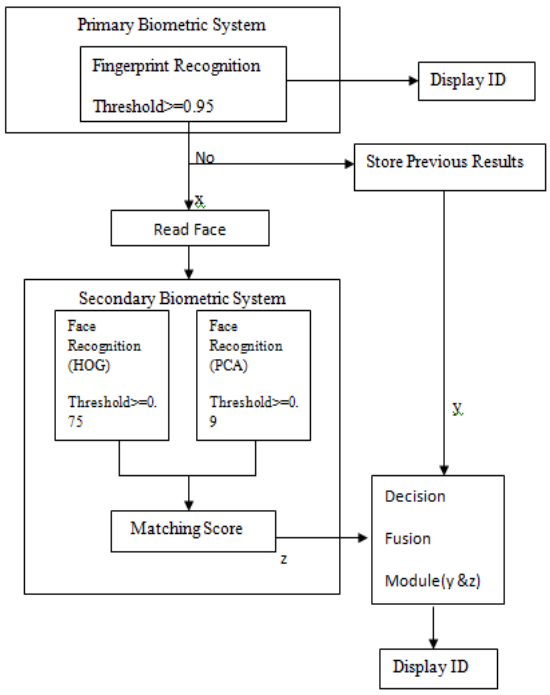

Fig 1: Block Diagram/Flow Chart

Secondary Biometric System: This is multi-algorithm system which fuses two different face recognition systems each having different extraction techniques wherein one uses HOG (Histogram Oriented Gradient) based feature extraction and other uses PCA (Principle Component Analysis)[7].Both of these systems use nearest neighbor technique to match the projected scores and identifies the genuine imposter.

These two systems are again fused at different levels as shown in Figure 1 and those fusion methodologies are briefly discussed below:

2.1 Score Level Fusion

The score level fusion approach is well known technique which can be used to fuse two different traits as shown in Figure 2.In this method each biometric matcher provides a similarity score indicating the proximity of the input feature vector with the template feature vector. These scores can be combined to claim an identity [8].

This step brings both matching scores between 0 and 1[9]. The normalization of both the scores is done by

$$N(F1) = \frac{MS(s) - \min(s)}{max(s) - \min(s)}$$

$$N(F2) = \frac{MS(f) - \min(f)}{max\,(f) - \min(f)} \qquad (1)$$

Where minimum and maximum scores for both face recognition system (F1 and F2) are substituted in the Eq. (1).

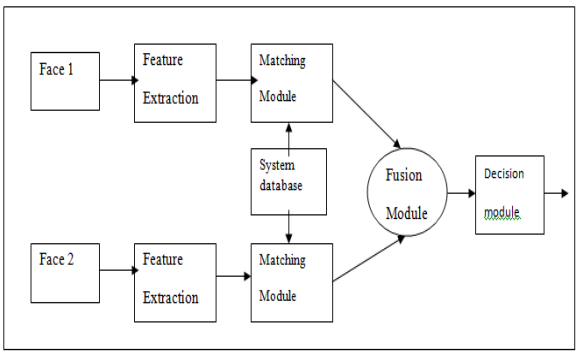

Fig 2: Score Level Fusion Block

And normalized values are determined to calculate the total matching score (MS) as in the Eq. (2) [10].

MS= a*$N(F1)$+b*$N(F2)$ (2)

Where 'a' and 'b' are two weight values. The value of weight is assigned linearly if the value of matching score is less than the threshold; otherwise exponential weightage is given to the score. The value of MS is used as the matching score [13].If the matching score obtained is more than the given threshold value the identity is accepted otherwise imposter is rejected.

2.2 Decision Level Fusion

In a Multibiometric system, fusion is done using abstract or decision methodology .The decision output by the individual matchers are available [14].Many commercial off-the shelf (COTS) biometric systems provide access to final results or recognition decision. When such a COTS systems are used to build a Hybrid multi biometric system, only decision level fusion is feasible [15]. Therefore the proposed work uses simple AND rule to combine both the primary and secondary system. When the AND rule is used the FAR (False Accept Rate) is extremely low while the FRR (False Rejection Rate) is high. This AND rule receives information from primary and secondary biometric system and then AND's the logic score to give the ID of imposter [15].

3. EXPERIMENTAL RESULTS

The results are tested on face and fingerprint samples collected. The database consists of 20 samples of faces with different gestures and fingerprint database with a total of 10 persons. The face database is obtained using camera and fingerprint images are acquired from optical fingerprint scanner. When the primary system fails, two different face recognition systems are fused and results are obtained and are fused against fingerprint data using decision fusion algorithm.

The below results were obtained when the threshold for fingerprint (primary system) was more than 0.98 as shown in Figure 3 and Figure 4. All these simulations were carried out in Matlab environment version 2014b also used parallel and computer vision tool boxes to obtain the results with greater accuracy and higher matching rate.

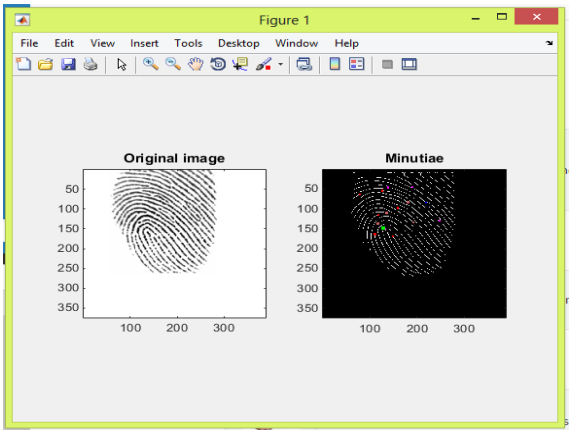

Fig 3: Feature Extraction Using Minutiae Method

Database was created to verify both the systems in simulation environment and to verify individual recognition system we used FVC2002 and AT&T databases for fingerprint and face recognition systems respectively.

Figure 3 shows the minutiae extraction from fingerprint image after performing series of steps like enhancement, filtering (Gabor filters) and thinning.

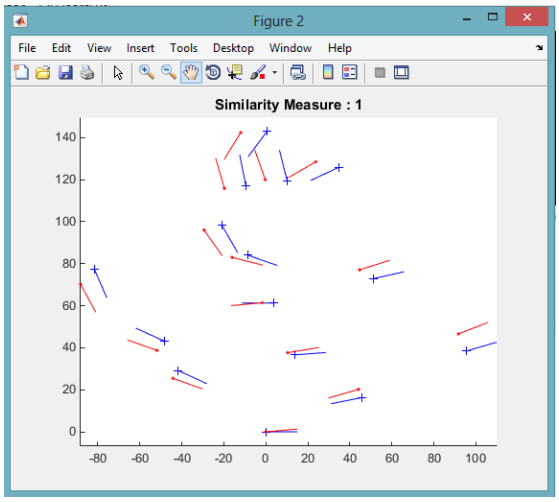

Fig 4: Similarity Measure for First Input Condition

Figure 4 shows the similarity score obtained such that the identity is declared by scanning primary system alone, below figure indicates that the trained vector and testing vector clusters are matched with 100 percent score such that the identity is declared in this module as depicted in Table 1.

Table 1: Results Obtained for various input condition

Sl.no	Input	Threshold	Obt threshold	Results
1.	Noiseless	0.98	1	100
2.	Noised	0.98	0.77	77.06

Now when the module is tested with fingerprint image for the same person with added noise the system did not meet the required threshold the similarity measure obtained was nearly 80 percent as depicted Figure 5 and Figure 6 indicating that testing vectors are not projected in the same direction as trained vector also the same is shown in Table 1.

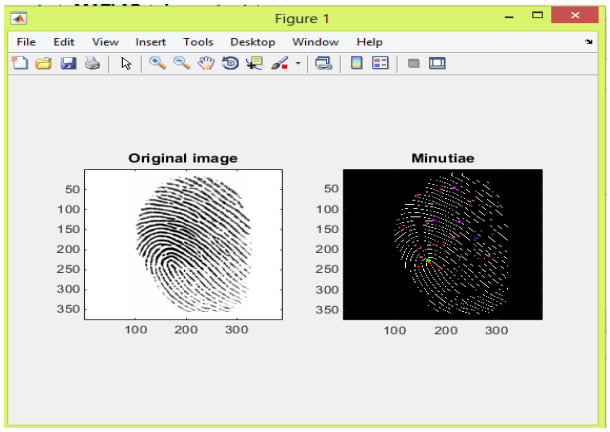

Fig 5: Feature Extraction for Second Case

After this step the secondary system will be scanned and the results obtained for both HOG based and PCA based Face Recognition as shown in Figure 7. Results for Principal component analysis showed better results when compared to Histogram Orientation Gradient(HOG) but fusion of both algorithm gave a good results as depicted from Table 1.

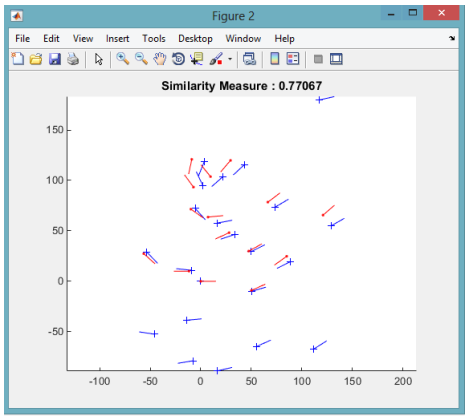

Fig 6: Similarity Measure for Second Case.

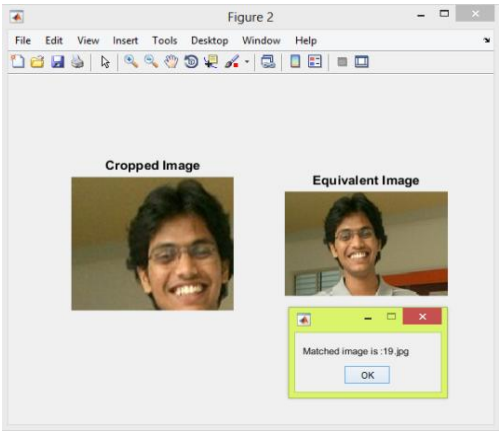

Fig 7: Face Recognition from Database

From the results obtained with the proposed system, it is evident that:

1. By testing genuine imposter the system saves lot of time by scanning only for primary recognition system.
2. Even when the system fails the previous results of an identification system are stored and then algorithm scans for secondary system.
3. The fusion of primary and secondary system can be more accurate if the modern fusion methodologies used.

4. CONCLUSION

The proposed work consists of the different traits of biometric identification systems and efforts towards the development of a common framework for hybrid biometric identification system. Summarizing we can say that the biometric systems are effective for human identification and authorization over various levels of implementation , for small to a large population, such systems are difficult to forge and can be made to secure by combining more than one biometric traits , that is multimodal biometric systems. Such systems will become ubiquitous and inevitable in the coming future.

5. ACKNOWLEDGMENTS

The authors would like to thank the B V Bhoomaraddi College, Hubli (Karnataka), India. Authorities for providing infrastructure to carry out experimental and research work required.

6. REFERENCES

[1] N. K. Ratha, R. M. Bolle, V. D. Pandit, and V. Vaish, ―Robust Fingerprint authentication using local structural similarity,‖ in Proc. 5th IEEE Workshop Appl. Comput. Vis., Dec. 4–6, 2000, pp. 29–34. DOI 10.1109/WACV.2000.895399.

[2] G. Aguilar, G. Sanchez, K. Toscano, M. Nakano, and H. Perez, ―Multimodal biometric system using Fingerprint,‖ in Proc. Int. Conf. Intell. Adv. Syst. 2007, pp. 145–150. DOI: 10.1109/ ICIAS.2007.4658364

[3] V. Conti, G. Milici, P. Ribino, S. Vitabile, and F. Sorbello, ―Fuzzy fusion in multimodal biometric systems,‖ in Proc. 11th LNAI Int. Conf. Knowl.- Based Intell. Inf. Eng. Syst. (KES 2007/WIRN 2007), Part I LNAI 4692. B. Apolloni et al., Eds. Berlin, Germany: Springer-Verlag, 2010, pp. 108–115.

[4] F. Besbes, H. Trichili, and B. Solaiman, ―Multimodal biometric system based on Fingerprint identification and Iris recognition,‖ in Proc. 3rd Int. IEEE Conf. Inf. Commun. Technol.: From Theory to Applications (ICTTA 2008), pp. 1–5. DOI: 10.1109/ ICTTA.2008.4530129.

[5] Igor B¨ohmAnd Florian Testor "Biometric Systems". IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 24,no. 5, pp. 696.706, May 2002.

[6] Arun Ross and Anil K. Jain "MULTIMODAL BIOMETRICS: AN OVERVIEW" Appeared in Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), pp. 1221-1224, September 2004.

[7] Prof. V. M. Mane and Prof. (Dr.) D. V. Jadhav" Review of Multimodal Biometrics: Applications, challenges and Research Areas". [8] W. Zhao, R. Chellapra, P.J. Phillips, A. Rosenfeld, "Face Recognition: A Literature Survey," ACM Computing Surveys, Vol. 35, No. 4, December 2003, pp. 399-458

[8] M.A. Turk, A.P. Pentland. "Face Recognition Using Eigenfaces," IEEE Conference on Computer Vision and Pattern Recognition, pp.586--591, 1998.

[9] P. N. Belhumeur, J. P. Hespanha, D. J. Kriegman, "Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection," IEEE Trans. Pattern Anal. Machine Intell., vol. 19, pp. 711–720, May 1997.

[10] M.S. Bartlett, J.R. Movellan, T.J. Sejnowski, "Face Recognition by Independent Component Analysis", IEEE Trans. on Neural Networks, Vol. 13, No. 6, November 2002, pp. 1450-1464 [10] X. Li and S. Areibi, "A Hardware/Software Co-design Approach for Face Recognition," Proc. 16th International Conference on Microelectronics, Tunis, Tunisia, Dec 2004.

[11] Moritoshi Yasunaga, Taro Nakamura, and Ikuo Yoshihara, "A Fault-tolerant Evolvable.

[12] Journal of Electronic Imaging/Mehmet Sezgin and Bulent Sankur; Survey over image thresholding techniques and quantitative

[13] https://books.google.co.in/books?id=JpUdlJnuE2MC&printsec=frontcover&dq=Handbook+of+multibiometrics&hl=en&sa=X&redir_esc=y#v=onepage&q=Handbook%20of%20multibiometrics&f=false

[14] Ms. Priya N. Ghotkar International Engineering Journal for Research & Development E-ISSN No: 2349-0721 Volume 1: Isuue 1