Advances in Computational Research
ISSN: 0975-3273 & E-ISSN: 0975-9085, Volume 4, Issue 1, 2012, pp.-99-103
Available online at http://www.bioinfo.in/contents.php?id=33

MULTIMODAL BIOMETRIC SYSTEM USING FACE AND SIGNATURE: A SCORE LEVEL FUSION APPROACH

KAZI M.M.[1]*, RODE Y.S.[1], DABHADE S.B.[1], AL-DAWLA N.N.H.[1], MANE A.V.[2], MANZA R.R.[1] AND KALE K.V.[1]

[1]Department of Computer Science and IT, Dr. B.A.M. University, Aurangabad, MS, India.
[2]Department of Digital & Cyber Forensic, Government Institute of Forensic Science, Aurangabad, MS, India.
*Corresponding Author: Email- mazhar940@gmail.com

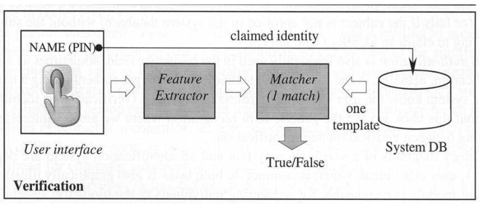
Received: February 21, 2012; Accepted: March 06, 2012

Abstract- A multimodal biometric system combines the different biometric traits and provides better recognition performance as compared to the systems based on single biometric trait or modality. In multimodal biometric system the fusion of the information can be done at various levels, but due to the ease in combining and accessing the scores generated by different matchers, the most common approach is the integration at the matching score level. Before combining, the scores should alter into a common domain, since different matchers generate heterogeneous scores. In this paper, we have studied performance of a single fast normalized cross-correlation matcher and simple sum-rule fusion technique based on face and signature traits of a user. The experiments conducted on a database of 17 users indicate that simple sum of score fusion method results in better recognition performance than using single face or single signature based biometric system. However, experiments also reveal that the normalized cross-correlation based matcher gives better results, highlighting the need for a robust and efficient feature extraction technique.
Keywords- biometric systems, multi-biometric system, face, signature, score level fusion

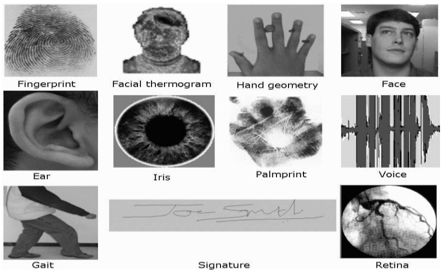
Citation: Kazi M.M., et al (2012) Multimodal Biometric System Using Face and Signature: A Score Level Fusion Approach. Advances in Computational Research, ISSN: 0975-3273 & E-ISSN: 0975-9085, Volume 4, Issue 1, pp.-99-103.

Introduction

Biometrics refers to the physiological or behavioral characteristics of a person to authenticate his/her identity [1]. Due to the increasing demand of enhanced security systems biometric based person authentication system has led to an unprecedented interest of the researchers world-wide. Biometric systems based on single source of information are called unimodal systems. Although some unimodal systems (e.g. Face, Iris, Palm, Fingerprint) [2], (Figure 1 shows a typical fingerprint biometric system and popular biometric traits) have got considerable improvement in reliability and accuracy, they have suffered from enrollment problems due to non-universality of biometrics traits, susceptibility to biometric spoofing or insufficient accuracy caused by noisy data [3], Figure 2 shows the sample images of such affected traits. Hence, single biometric may not be able to achieve the desired performance requirement in real world applications. One of the methods to overcome these problems is to make use of multimodal biometric authentication systems, which combine information from multiple modalities to arrive at a decision. Studies have demonstrated that multimodal biometric systems can achieve better performance compared with unimodal systems. This paper presents score level fusion approach to multimodal biometrics using face and signature modalities. The paper is organized as follows. Approaches to multi-biometric system is discussed in Section 2 whereas different fusion levels and score level fusion techniques to multi-biometric system is illustrated in Section 3, Normalized cross correlation matching technique and simple sum based score level fusion are given in Section 4 and Section 5 respectively. Experimental results and conclusions to the work are presented in the last section of the paper.

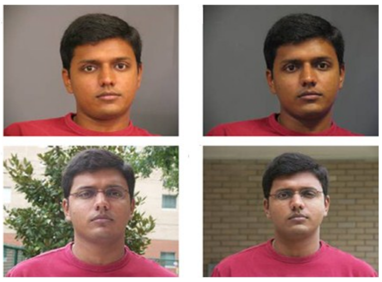


(a)



(b)

Fig. 1- Simple model and traits in biometric system (a) Unimodal (fingerprint) biometric system and (b) some popular biometric traits



(a)

(b)

Fig. 2- Different conditions that affect the performance of unimodal biometric systems (a) Face images in different scenario (illumination) and (b) Noisy Fingerprint images

Approaches in Designing Multi-Biometric System

There are six different approaches to design the multi-biometric system depending upon the type of the incorporation of the sources of the biometric traits. The Multi-biometric systems can incorporate information from multiple modalities, instances, sensors, samples, or any combination of the five sources of the evidences shown in Figure 3.

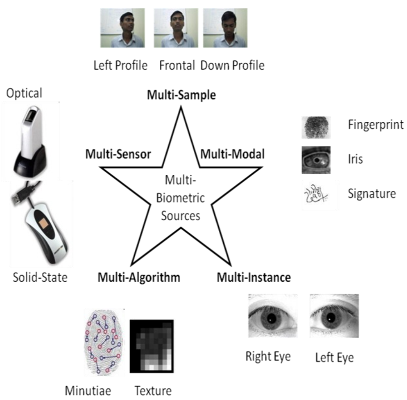


Fig. 3- Sources of Multi-Biometric System

a. **Multi Sensor Biometric System:** Multi sensor biometric system consists of multiple sensors to capture the one biometric trait data more than just once and combine them at different levels to deliver accurate data matching process. For example, a 2D camera can be joined with infrared/multispectral sensors to capture images of an individual under different illuminations/ conditions.
b. **Multi Algorithm Biometric System:** Algorithms are an integral part of biometric systems to carry out sampling and identification. In this case, multiple algorithms are used for heightened security. Though this security system is economical it can be quite complex.
c. **Multi Sample Biometric System:** Multiple samples of the same physical trait are captured to produce samples that are highly accurate and ensure better security. For instance, apart from taking the person's face, different profiles are also recorded [4].
d. **Multi Instance Biometric System:** This system captures impressions of all 10 fingers and both irises during different instances and combines them to form specific biometric samples. The multi instance biometric system provides better access control.
e. **Multimodal Biometric System:** This system uses a simple method. The security system combines samples from 2 physically uncorrelated features of an individual and is thus given the name, multimodal biometric system. For example, palmprint patterns can be combined with face recognition or iris patterns with fingerprints, etc. This hybrid biometric system has been devised to combine, 2 fingerprint samples with 3 face patterns etc.

The multi-biometric systems are definitely a gift for better security. These systems keep evolving with different types thus making it a popular technology for identification.

Levels of Fusion in Multi-biometric system

The fundamental issue in the information fusion system is to identify the type of the information before it get consolidate. The information can be consolidating at different levels in biometric system, starting from the acquisition of the data to the decision making module. The layout of a bimodal multi-biometric system is shown in Figure. 4. Figure 4 illustrates the various levels of fusion for combining two (or more) biometric systems. There are four different possible levels of fusion viz. (i) sensor level fusion (ii) fusion at the feature extraction level, (iii) fusion at the matching score level, (iv) fusion at the decision level.

1. **Fusion at the sensor level** (at acquisition time of raw data or before feature extraction module)**:** 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. The new feature vector now has a higher dimensionality and represents a person's identity in a different (and hopefully more discriminating) hyperspace. Feature reduction techniques may be employed to extract useful features from the larger set of features [5].

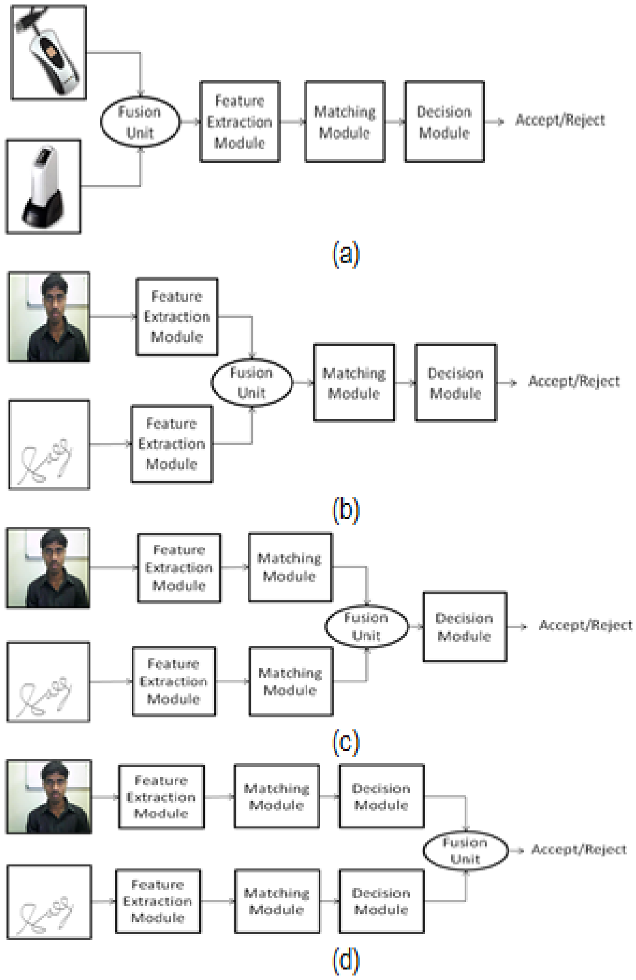


Fig. 4- Levels of fusion in bimodal multi-biometric system (a) Sensor Level, (b) Feature Level, (c) Matching Score Level, and (d) Decision Level

2. **Fusion at the feature extraction level** (after feature extraction module)**:** 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. The new feature vector now has a higher dimensionality and represents a person's identity in a different (and hopefully more discriminating) hyperspace. Feature reduction techniques may be employed to extract useful features from the larger set of features [6].
3. **Fusion at the matching score level** (after match score estimation module)**:** 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. These techniques attempt to minimize the FRR for a given FAR.
4. **Fusion at the decision level** (after the decision module)**:** 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 can be used to make the final decision.

Score level fusion techniques

Various score level fusion techniques have been proposed by the researchers to normalize the matching scores, to be used in decision module of the multi-biometric system [7].

i. **Simple Sum of Raw Scores**

Matcher scores are simply added, with no prior normalization. Scores are neither rescaled, nor weighted to account for differences in matcher accuracy. Included largely to demonstrate its limited applicability, which includes situations where scores have comparable distributions, such as two fingers scored by one matcher [8].

ii. **Simple Sum of Z-normalized Scores [9]**

This technique follows following steps:

a. The estimation of the mean and standard deviation of imposter score distribution has been performed on the sample data.

b. The mean of the imposter distribution is subtracted to normalize the scores and then are dividing by the standard deviation of the imposter distribution.

c. Without weighting then the normalized scores are simply added.

A normalized score is calculated by the equation:

$$s' = \frac{(s-\mu)}{\sigma}$$

Where μ is the mean and σ is the standard deviation of the matching score distribution.

iii. **Product of Likelihood Ratios**

This technique works with following steps:

- In the first step probability density functions are modeled separately for genuine and impostor distribution by each.
- For each matcher the Likelihood ratios are computed from these models.
- Transformation is performed to their likelihood ratios to normalize scores.
- Lastly, Normalized scores are simply multiplied.

Normalized Cross-Correlation and simple sum based fusion [10-12]

For image-processing applications in which the brightness of the image and template can vary due to lighting and exposure conditions, the images can be first normalized. This is typically done at every step by subtracting the mean and dividing by the standard deviation. That is, the cross-correlation of a template, $(t(x,y)$ with a sub-image $f(x,y)$ is

$$\frac{1}{n-1}\sum_{x,y}\frac{(f(x,y)-\bar{f})(t(x,y)-\bar{t})}{\sigma_f \sigma_t}$$

Where n is the number of pixels in $t(x,y)$ and $f(x,y)$,

$\bar{f}$ is the average of f and σ_f is standard deviation of f. In functional analysis terms, this can be thought of as the dot product of two normalized vectors. That is, if

$$F(x,y) = f(x,y) - \bar{f}$$

and

$$T(x,y) = t(x,y) - \bar{t}$$

Then the above sum is equal to

$$\left\langle \frac{F}{\|F\|}, \frac{T}{\|T\|} \right\rangle$$

Where $\langle \cdot , \cdot \rangle$ is the inner product and $\| \cdot \|$ is the L^2 norm,

Thus, if f and t are real matrices, their normalized cross-correlation equals the cosine of the angle between the unit vectors F and T, being thus 1 if and only if F equals T multiplied by a positive scalar. Normalized correlation is one of the methods used for template matching, a process used for finding incidences of a pattern or object within an image.

Simple Sum of Raw Scores

Matcher scores are simply added, with no prior normalization. Scores are neither rescaled, nor weighted to account for differences in matcher accuracy. Included largely to demonstrate its limited applicability, which includes situations where scores have comparable distributions, such as two fingers scored by one matcher [8].

Experimental Results

The experiments are carried out on the database of 17 users (the data captured by Multimodal Biometric Research Lab, Department of Computer Science and Information Technology, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad (MS) - India. It contains the 10 different facial poses and 10 samples of the signature of each subject. The model of the experimental setup has been shown in Figure 5.

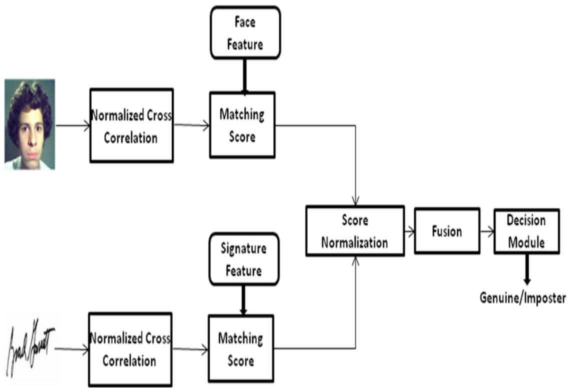


Fig. 5- Experimental setup

The frontal face of a subject has been processed under normalized cross correlation section of the model with the other 9 images. This block gives the matching score in the form of 0 or 1, (1 indicates match where 0 indicates non-match). Similarly, a signature of a subject has been processed under the same block with the other 9 images. Using same procedure the genuine score and imposter score has been calculated. Figure 6 shows false positive and false negative plot of the BAMU face database while Figure 7 shows false positive and false negative plot on BAMU signature database.

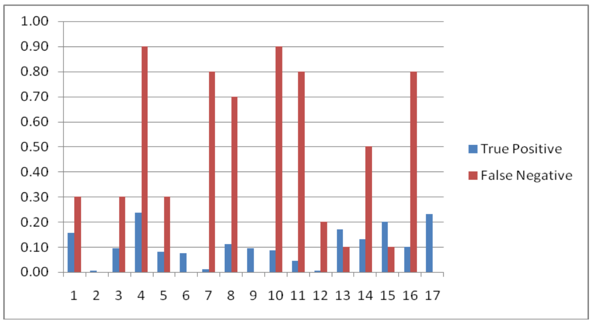


Fig. 6- Plot of False Rejection rate and True acceptance rate on BAMU face single modality.

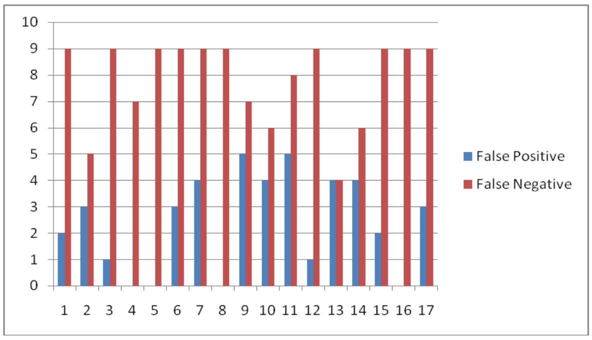


Fig. 7- Plot of False Acceptance rate and False Rejection rate on BAMU signature single modality.

The score of BAMU face and BAMU signature are fused using simple sum fusion method to build the bimodal biometric recognition system. In this system as normalized cross-correlation matching is used to calculate match score for both face and signature modalities, there is no need of score normalization. The Table 1 shows the accuracy rate and error rate of single face madality (BAMU and face94 database), single signature based system and biomodal biometric system using face and signature. Figure 8 shows the plot of the bimodal (face+signature) biometric system.

Table1 - Total Error Rate and Total Accuracy Rate

	BAMU Face	face 94	BAMU Signature	BAMU Face + Signature
Correct Predictions	2529	6640	2499	2826
Incorrect Predictions	361	580	391	64
Total Scored Cases	2890	7220	2890	2890
Error rate	0.12	0.08	0.15	0.02
Accuracy Rate	0.87	0.91	0.86	0.97

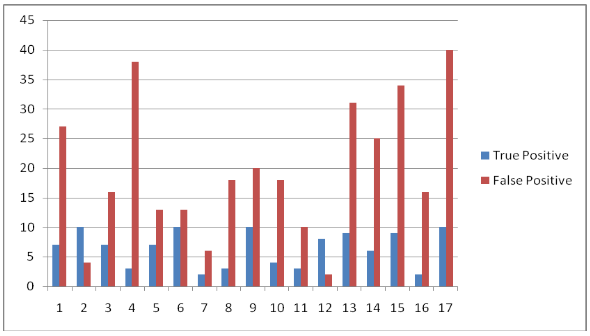


Fig. 8- Plot of False Acceptance rate and True Acceptance rate on BAMU (face + signature) fused modalities.

Conclusion

The performance of single modality based biometric recognition has been suffering from the different noisy data, non-universality of biometric data, and susceptibility of spoofing. The multimodal biometric system can improve the performance of the system. In this paper shows that face and signature based bimodal biometric system can improve the accuracy rate about 10%, than single face/signature based biometric system. The rate can also be improved using advanced pattern recognition techniques, which will be studied in future.

Acknowledgment

The authors wish to acknowledge the financial support of UGC in Special Assistance Program (SAP) DRS Phase-I for research work on the theme “Biometrics: Multimodal System Development”. The authors also thank delegates of the department and various institutes, who have donated their biometrics for the Multimodal Biometric Research Lab.

References

[1] Jain A.K., Ross A. and Prabhakar S. (2009) *IEEE Transactions on Circuits and Systems for Video Technology*,14, 4-20.
[2] Chander Kant, Rajender Nath (2009) *International Journals of Biometric and Bioinformatics*, 3(1), 1- 9.
[3] Jain A.K., Ross A. (2004) *Communications of the ACM,* 47, 34 -40.
[4] Mane A.V., Rode Y.S. and Kale K.V. (2011) *International Journal of Computer Applications* 27(8), 26-31.
[5] Mitchell H.B. (2007) *Multi--Sensor Data Fusion*, *Springer,* 281.
[6] Ross A. and Govindarajan R. (2005) *SPIE Conference on Biometric Technology for Human Identification*, 5779,196-204.
[7] Ulery B., Fellner W., Hallinan P., Austin Hicklin, Watson C. (2006) *Studies of Biometric Fusion report, National Institute of Standards and Technology*, 1-14.
[8] Watson C., Wilson C., Indovina M., Cochran B. (2005) *NIST Interagency Report* 7249.
[9] Jain A.K., Nandakumar K. and Ross A. (2005) *Pattern Recognition*.
[10]Shou-Der Wei, Shang-Hong Lai (2008) *IEEE Transactions on Image Processing* 17(11), 2227-2235.
[11]Karna D.K., Agarwal S., Nikam S. (2008) *Fifth International Conference on Computer Graphics Imaging and Visualization*.
[12]Zhao F., Huang Q. and Gao W. (2006) *IEEE Int. Conference on Acoustics, Speech and Signal Processing* 2, 14-19.