Volume 3, Issue 7, July 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure and Reliable Multimodal Biometric Systems Using two and three Biometric Traits

Shekhar Karanwal*
Assistant Professor
Department of Computer Science
FET GKV Haridwar, INDIA

Abstract— this paper discusses about multimodal biometric systems using two biometric traits (Face and Palm Print) and three biometric traits (Face, Fingerprint and Palm Print). The results from both the systems are compared and it is proved that system with three traits is more secure and reliable as compared to the system with two traits. This concept can be generalized for a multimodal system with n biometric traits. Major emphasis in the work is given on wavelet decomposition of the images of the traits, fusion of the images and feature extractor algorithm SIFT. The proposed method for evidence fusion is presented which is based on the image decomposition into multiple channels depending on their local frequency. The wavelet transform provides a framework to decompose image into a number of new images, each of them having a different degree of resolution. The wavelet based image fusion would be applied to two dimensional multispectral face, palmprint and fingerprint images. When the fused image is ready for further processing SIFT is used for feature extraction and matching is performed by unit vectors.

Keywords— Wavelet decomposition, SIFT, Unibiometrics, Multibiometrics, Histogram Equalization.

I. INTRODUCTION

Biometrics refers to the automatic identification of an individual based on his/her physiological and behavioural traits [1]. Biometric systems based on a single source of information (unimodal systems) suffer from limitations like the lack of uniqueness, non-universality and noisy data and hence, may not be able to achieve the desired performance requirements of real-world applications. In contrast, multi-modal biometric systems combine information from its component modalities to arrive at a decision. Several studies have demonstrated that by consolidating information from multiple sources, better performance can be achieved compared to the individual unimodal systems. Multibiometric systems offer the following advantages over unibiometric systems.

1. Combining the evidence obtained from different sources using an effective fusion scheme can significantly improve the overall accuracy of the biometric system. The presence of multiple sources also effectively increases the dimensionality of the feature space and reduces the overlap between the feature spaces of different individuals.
2. Multimodal biometric systems can address the non-universality problem and reduce the FTER (Failure to Enroll Rate) and FTCR (Failure to Capture Rate). For example, if a person cannot be enrolled in a finger print system due to worn-out ridge details, he can still be identified using other biometric traits like face or iris.
3. Multimodal biometric systems can also provide a certain degree of flexibility in user authentication. Suppose a user enrols into the system using several different traits. Later, at the time of authentication, only a subset of these traits may be acquired based on the nature of the application under consideration and the convenience of the user. For example, consider a banking application where the user enrols into the system using face, voice and fingerprint. During authentication, the user can select which trait to present depending on his convenience. This document is a template. An electronic copy can be downloaded from the Journal website. For questions on paper guidelines, please contact the journal publications committee as indicated on the journal website. Information about final paper submission is available from the conference website. While the user can choose face or voice modality when he is attempting to access the application from his mobile phone equipped with a digital camera he can choose the fingerprint modality when accessing the same application from a public ATM or a network computer.
4. The availability of multiple sources of information considerably reduces the effect of noisy data. If the biometric sample obtained from one of the sources is not of sufficient quality during a particular acquisition, the samples from other sources may still provide sufficient discriminatory information to enable reliable decision-making.
5. Multimodal biometric systems [2] can provide the capability to search a large database in a computationally efficient manner. This can be achieved by first using a relatively simple but less accurate modality to prune the database before using the more complex and accurate modality on the remaining data to perform the final identification task. This will improve the throughput of a biometric identification system.
6. Multimodal biometric systems are more resistant to spoof attacks because it is difficult to simultaneously spoof multiple biometric sources. Further, a multibiometric system can easily incorporate a challenge-response mechanism during biometric acquisition by acquiring a subset of the traits in some random order (e.g., left index finger followed

by face and then right index finger). Such a mechanism will ensure that the system is interacting with a live user. Further, it is also possible to improve the template security by combining the feature sets from different biometric sources using an appropriate fusion scheme. This work discusses about two multimodal biometric systems. First comprises of two biometric traits which are face and palmprint and second has three biometric traits which are face, palmprint and fingerprint. In both the systems wavelets are used for decomposition and fusion and SIFT is used for feature extraction and lastly matching is performed by using unit vectors.

I section introduces some aspects of multibiometrics, in section II wavelet decomposition is described, section III explains conceptual description of SIFT, after explaining SIFT section IV describes steps for matching, V section evaluate results and conclusion is drawn on section VI

II. WAVELET DECOMPOSITION

The wavelet representation [3] of an image has the property that the image can be recovered without any information loss. Many researches showed that multi resolution transforms in wavelet are very useful for image fusion. First, the DWT of each of the two or more images is computed. Then, the wavelet coefficients are fused using the developed fusion rule in the wavelet transform domain. Specifically, the wavelet coefficients are fused using different combining rule for low frequency band and high frequency band respectively. Finally, the fused image is formed by using inverse DWT (IDWT) [4, 5, 6].A sample set of images considered are shown in Fig. 1, Fig. 2 and Fig. 3. The complete process of decomposition and fusion of face and palm print is shown in Fig. 4 and the process of decomposition and fusion process of face, palm print and fingerprint is described in Fig. 5.

Fig.1: Face

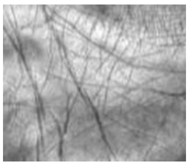

Fig. 2: Palm Print

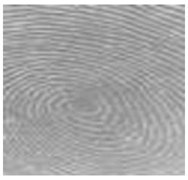

Fig. 3: Fingerprint

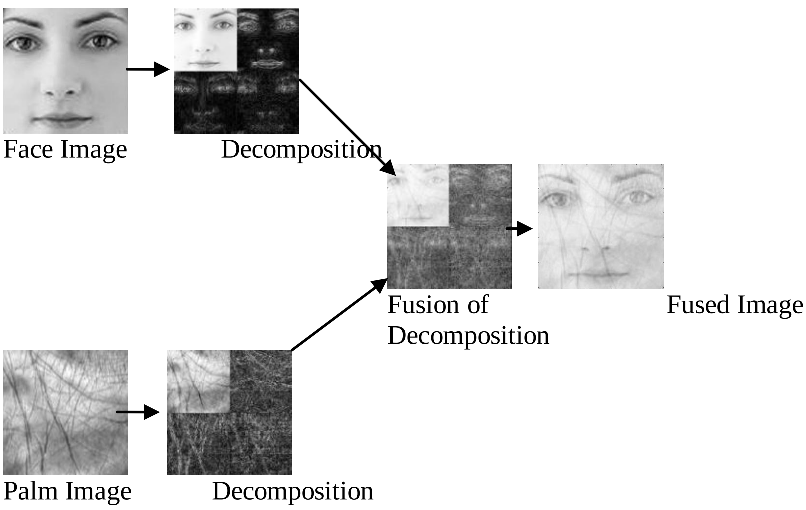

Fig.4 Wavelet decomposition and fusion of face and palmprint

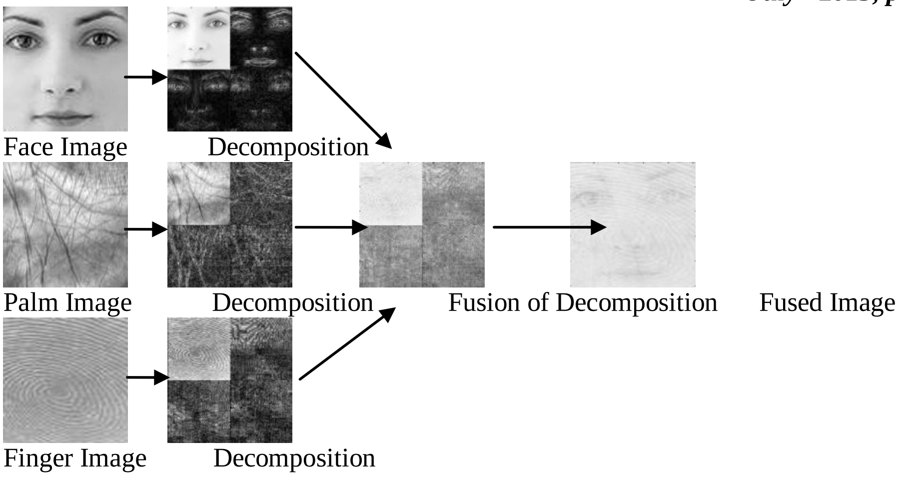

Fig.5 Wavelet decomposition and fusion of face, palmprint and fingerprint

The fused image and normalized image of face, palmprint and face, palmprint and fingerprint is shown on Fig. 6 and Fig. 7, Normalization is done by histogram equalization. Fig. 8 and Fig. 9 show the normalized images of fused images.

Fig.6 fusion of face and palmprint

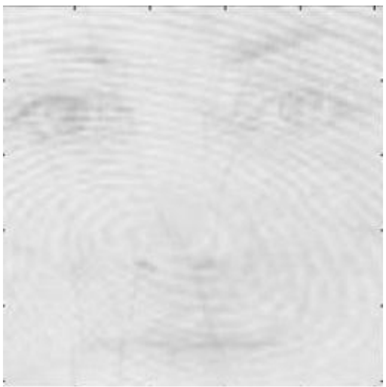

Fig.7 Fusion of face, palmprint and fingerprint

Fig.8 Histogram equalization of face and palmprint

Fig.9 Histogram equalization of face, palmprint and fingerprint

III. SIFT

The scale invariant feature transform, called SIFT [7] [8] [9] descriptor, has been proposed by and proved to be invariant to image rotation, scaling, translation, partly illumination changes. The investigation of SIFT features for biometric authentication has been explored in. The basic idea of the SIFT descriptor is detecting feature points efficiently through a staged filtering approach that identifies stable points in the scale-space. Local feature points are extracted through selecting the candidates for feature points by searching peaks in the scale-space from a difference of Gaussian (DoG) function. Then the feature points are localized using the measurement of their stability and assign orientations based on local image properties. Finally, the feature descriptors, which represent local shape distortions and illumination changes, are determined. As previously shown that fused image is normalized by histogram equalization. After histogram equalization key points are extracted from fused normalized image. SIFT consists of various parameters but only key points information is taken out from image. Fig. 10 shows the key point extraction of face and palmprint and key point extraction of face, palmprint and fingerprint is shown on Fig. 11.

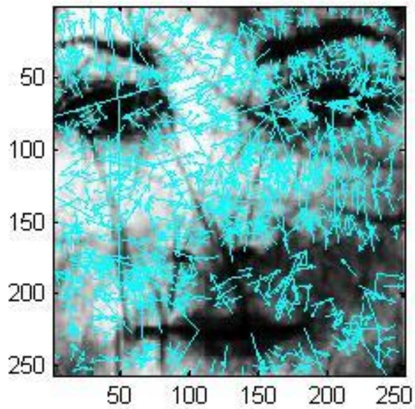

Fig.10 SIFT keypoint extraction of face and palmprint

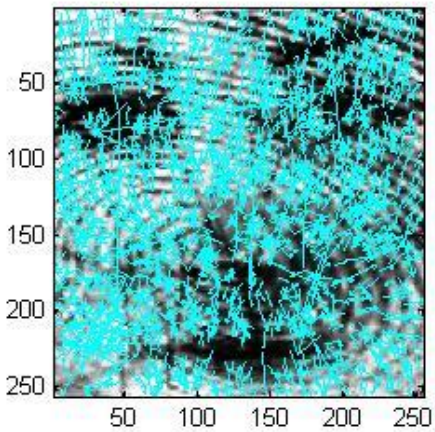

Fig.11 SIFT Keypoint extraction of face, palmprint and fingerprint

For image matching and recognition, SIFT features are first extracted from a set of reference images and stored in a database. A new image is matched by individually comparing each feature from the new image to this previous database and finding candidate matching features based on their feature vectors.

IV. STEPS OF MATCHING

1. SIFT (Scale Invariant Fourier Transform) Keypoints are calculated for each image.
2. Dot product is calculated between unit vectors. The ratio of angles, acos of dot products of unit vectors is a close approximation to the ratio of Euclidean distances for small angles.
3. Distance ratio of .6 is assumed, it means that it only keep matches in which the ratio of vector angles from the nearest to second nearest neighbor is less than distance Ratio.
4. Selection of matching is performed to second image for each descriptor in the first image
5. Matrix transpose is calculated, vector of dot products is calculated, inverse cosine is performed and results are sorted. Evaluate if nearest neighbor has angle less than dist ratio times second.

V. RESULT EVALUATION

For obtaining the results a database of 30 images consisting of face, palmprint and fingerprint are used. Images size is taken 256X256 and resolution is set to 72 dpi. First of all face and palmprint implementation is performed, then face, palmprint and fingerprint implementation is performed. In implementation of face and palmprint it is found that out of 30 iterations there are two FAR & FRR. FAR stands for false acceptance rate which defines number of false users who enters the system by trying various combinations and makes access to systems. FRR stands for false rejection rate which defines that there are some users which are unable to deal system accurately. For example there are some users whose finger is not in proper contact of the sensor or there are some users whose finger is wounded. So the accuracy or GAR (Genuine acceptance rate, defines the number of correct users) for two biometric traits is 28/30=.933=93.3% and (FAR & FRR) =2/30=.066=6.6%.

For implementation of face, palmprint and fingerprint it is found that there is only one FAR & FRR. So the accuracy or GAR for three biometric traits is 29/30=.966=96.6% and (FAR & FRR)=1/30=.033=3.3%.

Results shows that in three biometric traits GAR is 96.6%, FAR=3.3%, FRR=3.3%. However in case of two biometric traits GAR is 93.3%, FAR=6.6%, FRR=3.3%. So it is clear from these results that three biometric traits are more secure and reliable as compare to two biometric traits. Another reliable and security point is that it is impossible to reconstruct original images from the fused images. Further if the system is extended for more biometric traits then it provides more security and reliability to the system.

VI. CONCLUSION

This paper compares a result which is obtained from two biometric traits and three biometric traits by using one level 2d-discrete wavelet transform for decomposition and image fusion and SIFT for feature extraction. Images sizes are set to 256X256 and resolution is set to 72 dpi and distance ratio is set to 0.6. Firstly result is obtained from two biometric traits which are face and palmprints and then results are obtained from three biometric traits which are face, palmprints and fingerprints. Total of 30 iterations are performed between both for two biometric traits and three biometric traits. Three biometric traits produces accuracy of 96.6% and two biometric traits produces accuracy of 93.3%. It is also impossible to reconstruct original image from fused images which makes system more secure and reliable.

References

[1] S. C. Dass, K. Nandakumar, and A. K. Jain, (2005), A Principled Approach to Score Level Fusion in Multimodal Biometric Systems, In Proceedings of Fifth International Conference on Audio- and Video-based Biometric Person Authentication (AVBPA), pp. 1049–1058.

[2] A. K. Jain and A. Ross, (2004), Multibiometric Systems, Communications of the ACM, Special Issue on Multimodal Interfaces, 47(1), pp. 34–40.

[3] H. Wang, (2004), Multisensor Image-fusion by Using Discrete Multiwavelet Transform, In Proceedings of International Conference on Machine Learning and Cybernetics, vol.7, pp. 4331- 4336.

[4] S. M. Prasad, V. K. Govindan, P. S. Sathidevi, (2009), Palmprint Authentication Using Fusion of Wavelet Based Representations, IEEE World Congress on Nature and Biological Inspired Computing (NABIC 2009), Coimbatore, India, pp. 520-525.

[5] M. A. Berbar, S. F. Gahe, and N. A. Ismaill, (2003), Image fusion using multi decomposition levels of discrete wavelet transform, pp. 294-297.

[6] Rohini Asamwar, Kishor Bhurchandi, Abhay Gandhi, (2010), Interpolation of Images using Discrete Wavelet Transform to Simulate Image Resizing as in Human Vision, IJAC, pp.9-16.

[7] David G. Lowe, (1999), Object Recognition from Local Scale-Invariant Features, International Conference on Computer Vision, pp. 1150-1157.

[8] Lowe. D., (2004), Distinctive image features from scale-invariant key points, International Journal of Computer Vision vol. 60. no.2, pp.91-110.

[9] David G. Lowe, (2001), Local Feature View Clustering for 3D Object Recognition, Proc. of the IEEE Conference on Computer Vision and Pattern Recognition, Kauai, Hawaii vol.1, pp.682-688.

