Improving Biometric Identification through Score Level Face Fingerprint Fusion

Mrs. Smita Kulkarni

Abstract— Multi-modal biometric fusion is more accurate and reliable compared to recognition using a single biometric modality. However, most existing fusion approaches neglect the influence of the qualities of the biometric samples in information fusion. Our goal is to advance the state-of-the-art in biometric fusion technology by providing a more universal and more accurate solution for personal identification and verification with predictive quality metrics. In this work, we developed score-level multi-modal fusion algorithms based on predictive quality metrics and employed them for the task of face and fingerprint biometric fusion In this paper the performance of sum rule-based score level fusion are examined. Before fusion of sum rule, normalization is done by using any one technique like min-max normalization, z score normalization and tanh estimator's normalization. In this paper min max normalization is used for normalization.

Index Terms— Multimodal biometrics, score level fusion, verification, normalization, sum rule, Support Vector Machines.

1. INTRODUCTION

In recent years, biometric-based authentication systems have been widely used in many applications which require reliable verification/identification scheme. A biometric system is essentially a pattern-recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic the person possesses [1]. It differs from classical user authentication system which is based on something that one has (e.g., identification card, key) and/or something that one knows (e.g., password, PIN). Biometric-based authentication system is based on something that one is, such as fingerprints and face, or something that one produces, such as voice and signature. Depending on the application context , a biometric system may operate in two modes [2, 3] verification or identification. Biometric verification is the task of authenticating that a test biometric sample matches the pattern or model of a specific user. Biometric identification is the task of associating a test biometric sample with one of N patterns or models that are available from a set of known or registered individuals. Unibiometric systems (based on single biometric trait) suffer from several practical problems like noisy sensor data, non-universality or lack of distinctiveness of the biometric trait, unacceptable error rates, and spoof attacks [4]. Multimodal biometric systems which combine multiple bio metric samples, or characteristics derived from samples, have been developed in order to overcome those problems.

Several studies have suggested that by consolidating information from multiple Biometric traits, better performance can be achieved to meet tight requirement of real-world applications. The key to multimodal biometric system is the fusion of various biometric modality data. The system requires an integration scheme to fuse the information obtained from the individual modalities. In a multimodal biometric system that uses different biometric traits, fusion can be done at four different levels of information [4] and these levels correspond to four important components of a biometric system. Those four important modules are: (1) Sensor module, (2) Feature extraction module, (3) Matching module, and (4) Decision making module [5]. The fusion thus can take place at the sensor level, feature extraction level, matching score level, or decision level. This paper will first observe the advantage of multimodal biometric system over unimodal biometric system. We examine how the accuracy will improve as several biometric data are integrated in a verification system. Furthermore, performance evaluation on two common score level fusion techniques: sum rule based fusion and Support Vector Machines (SVM)-based fusion are conducted. In the sum rule technique, if the match scores being combined come from different ranges, they need to be transformed (normalized) to a common range before fusion can take place. In this paper three well known normalization methods are considered, namely, min-max normalization, z-score normalization, and tanh estimators normalization [6]. They are chosen since they appear frequently in the literature and generally attained good performance. Besides these, a new transformation method which is derived from minmax normalization is proposed here. The proposed method is more robust because it takes account on outliers, while normalization step is often necessary and cannot be avoided in sum rule based fusion.

Mrs. Smita Kulkarni working as Asst. Prof in MAE Alandi Pune.
Email: sksmita.mail@gmail.com

2. SCORE LEVEL FUSION

Score level fusion is commonly preferred in multimodal biometric systems because matching scores contain sufficient information to make genuine and impostor case distinguishable and they are relatively easy to obtain. Given a number of biometric systems, matching scores for a pre specified number of users can be generated even with no knowledge of the underlying feature extraction and matching algorithms of each system. Therefore, combining information obtained from individual modalities using score level fusion seems both feasible and practical [7]. Since the scores generated by a biometric system can be either similarity scores or distance scores, one needs to convert these scores into a same nature. The common practice, which is followed in this paper, is to convert all the scores into similarity scores. In general, score level fusion techniques can be divided into three categories as follows : (a) transformation-based score level fusion (e.g., sum-rule based fusion preceded by min-max normalization), (b) classifier-based score level fusion (e.g., SVM-based fusion), and (c) density-based score level fusion (e.g., likelihood ratio test with Gaussian Mixture Model). In this paper only transformation based technique (sum rule based fusion) is used for fusion.

3. MIN-MAX NORMALIZATION SCHEME

Let X denote the set of raw matching scores from a specific matcher, and let $x \in X$. The normalized score of x is then denoted by x'. This normalization maps the raw matching scores to interval [0, 1] and retains the original distribution of matching scores except for a scaling factor. Given that max(X) and min(X) are the maximum and minimum values of the raw matching scores, respectively, the normalized score is calculated as

$$X ' = X - Min(X) / Max(X) - Min(X)$$

This method is highly sensitive to outliers in the data used for estimation and therefore it is not robust. The presence of, even only one, outliers will make most of the data concentrate only in a small range. This case will be explained clearly by an illustration. Suppose that one has a set of matching scores as listed below

Genuine	7	11	17	30	40	42	51	95	120
Imposter	5	5	6	7	10	12	13	15	29

It can be clearly seen that there are two outliers in the genuine matching scores distribution, which are, the scores 95 and 120. In the real world this situation is not unlikely to happen, because some genuine users may get very high score when their present biometric data are compared to the data in the database. However, most of users will not reach that high score for several reasons:

- A little/significant change of the biometric trait itself, such as cut/scratch on fingerprint and face/voice variations by age.
- The level of subject's cooperation degree [8]. Some users may exhibit non-cooperative behavior in the sampling process.
- Alteration of condition between enrollment phase and testing phase. There may be presence of noise in either process, or in some biometric systems like fingerprint and finger vein recognition systems, the finger position in sampling process may be significantly different between enrollment phase and testing phase. After above table is applied to the matching scores in the list, one will get this result:

Genuine	0.017	.052	.104	.217	.27	.304	.322	.4	.783
Imposter	0	0	.09	.017	.017	.043	.061	.07	.o87

The result shows that most of genuine scores concentrate in the small range [0.017, 0.4], while the impostor scores lie between [0, 0.13]. Now let us make a little change on the dataset by replacing the outliers (scores 95 and 120) with the maximum score before them (i.e. score 51). After that min-max normalization is conducted on this dataset. Distribution of scores after normalization is listed as follows:

Genuine	.043	.130	.260	.543	.674	.761	.804	1	1	1
Imposter	0	0	.022	.043	.043	.109	.152	.174	.217	.326

As the outliers have been removed, the genuine scores now are distributed more evenly in the entire range [0,1],while the impostor scores concentrate only in the restricted range [0, 0.326]. From this illustration it can be observed that, while performing min-max normalization, the presence of outliers in the dataset reduces separation degree between genuine and impostor scores.

4. EXAMPLE OF SCORE LEVEL FUSION

This example shows a fusion of left fingerprint and right fingerprint scores. Suppose that there are 5 persons, and we have captured the images of their left fingerprint and right fingerprint (2 images per finger per person). After that their images are compared and the genuine and impostor scores are shown in Tables given below

Table 1 Genuine and impostor scores of 5 persons for the left fingerprint

Left Fingerprint

Image I						
	Person	A	B	C	D	E
	A	29	4	6	4	4

Left Fingerprint						
Image I						
Image I	Person	A	B	C	D	E
	A	.7647	.0294	.0882	.0294	.0294
	B	0	.3823	0	.882	.1764
	C	.58824	.0294	.1764	.294	.0882
	D	.205882	.0882	.1764	1	.0588
	E	.29412	.1470	.8823	.882	.0294

Table 2 Genuine and impostor scores of 5 persons for the right fingerprint

Right Fingerprint						
Image1						
Image 2	Person	A	B	C	D	E
	A	84	5	5	4	8
	B	4	5	3	7	4
	C	15	8	10	7	5
	D	3	4	4	4	10
	E	6	9	7	3	4

In Tables given above, the scores that are located at diagonal are the genuine scores, since they are the result of comparing two images that belong to the same person. The scores in others are the impostor scores because they are the result of comparing two images that belong to different persons. For simplicity, we will use all the scores as the training set and also as the testing set. Since we use the min max normalization method, the parameters that we need is the maximum and minimum scores. The training set is used to determine these parameters. For the left fingerprint, the maximum score is 37, and the minimum score is 3. For the right fingerprint, the maximum score is 84 and the minimum score is 3. Now we use the formula for minmax normalization. After the fusion, there are 5 genuine scores and 20impostor scores. In order to calculate the FAR and GAR, a threshold is needed. The falsely accepted impostor scores are the impostor scores which are larger than the threshold, while the correctly accepted genuine scores are the genuine scores which are larger than the threshold. Suppose that the threshold is equal to 0.26, then the number of falsely accepted impostor scores is 0, because there is no impostor score which has the value greater than 0.26. Therefore, FAR = 0/20 = 0. The number of correctly accepted genuine scores is 4, because there are 4 genuine scores which have the value greater than 0.26. Therefore, GAR = 4/5 = 0.8. Suppose that it is desired to have GAR = 1 = 100%, so the threshold is set to 0.041, such that all the genuine scores are greater than the threshold. However this will make FAR greater than before. There are 18 impostor scores which are larger than 0.041, and therefore FAR = 18/20 = 0.9 = 90%. In most cases we will prefer to use the threshold which causes the FAR to be as smaller as possible.

5. CONCLUSION

This paper basically explains one of the normalization schemes of Score Level Fusion with some examples and after normalization is carried out fusion is done by Sum Rule based fusion[9] and in example it shows that after considering some threshold value GAR should be greater than FAR because we consider FAR should be as small as possible.

REFERENCES

[1] Prabhakar, S. Pankanti, and A. K. Jain, *Biometric Recognition: Security and Privacy Concerns*, IEEE Security & Privacy, March/April 2003, pp. 33-42.

[2] J. Ortega-Garcia, J. Bigun, D. Reynolds, and J. Gonzalez-Rodriguez, *Authentication Gets Personal with Biometrics*,IEEE Signal Processing Magazine, Vol. 21, March 2004, pp. 50-62.

[3] A. K. Jain, A. Ross, and S. Prabhakar, *An Introduction to Biometric Recognition*, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, January 2004, pp. 4-20.

[4] K. Nandakumar, Y. Chen, S. C. Dass, and A. K. Jain, *Likelihood Ratio-Based Biometric Score Fusion*, IEEE Transactions on Pattern Analysis and Machine Intelligence,Vol. 30, No. 2, February 2008, pp. 342- 347.

[5] A. Ross and A. Jain, *Information Fusion in Biometrics*, Pattern Recognition Letters 24 (2003), pp. 2115-2125.

[6] S. Ribaric and I. Fratric, *Experimental Evaluation of Matching- Score Normalization Techniques on DifferentMultimodalBiometric Systems*, IEEE Mediterranean Electro technical Conference 2006, May 2006, pp. 498-501.

[7] S. C. Dass, K. Nandakumar, and A. K. Jain, *A Principled Approach to Score Level Fusion in Multimodal BiometricSystems*, Proceedings of AVBPA, Rye Brook, July 2005, pp.1049-1058.

[[8] G. L. Marcialis and F. Roli, *Score-level Fusion of Fingerprint and Face Matchers for Personal Verification Under "Stress" Conditions*, 14th Int. Conf. on Image Analysis and Processing, 2007, pp. 259- 264.

[9] A. K. Jain and A. Ross, "*Multibiometric Systems*," Communications of the ACM 47(1), 34-40 (2004).

[10] Rowshan BR, Khalid MK, Yusof R (2008). Multi-level Fuzzy Score Fusion for Client Specific Linear Discriminant Analysis based FaceAuthentication System, IEEE International Conference on Signal

[11] Zhou J, Su G, Jiang C, Deng Y, Li C (2007). A face and fingerprint identity authentication system based on multi-route detection, Neurocomputing, 70: 922-931.

[12] E. Tabassi, C. L.Wilson, and C. I.Watson. Fingerprint image quality. Technical report, NIST, 2004.

[13] B. Ulery, W. Fellner, P. Hallinan, A. Hicklin, And C. Watson. Studies of biometric fusion appendixc evaluation of selected biometric fusion techniques. Technical Report IR 7346 NIST, 2006.

[14] P. Wang, Q. Ji, and J. L. Wayman. Modeling

And predicting face recognition system performance based on analysis of similarity scores. IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(4):665–670, 2007.

[15] W. J. Scheirer, A. Bendale, and T. E. Boult. Predicting biometric facial recognition failure with similarity surfaces and support vector machines. In IEEE Computer Society Workshop on Biometrics (in association with CVPR 2008), 2008.