PERSONAL IDENTIFICATION USING MULTIBIOMETRICS SCORE-LEVEL FUSION

Amritha K.C[1], S.Velmurugan[2]

[1]*PG Scholar, EEE, K S R Institute for Engineering and Technology, Kerala, India*
[2]*Assistant Professor, EEE, K S R Institute for Engineering and Technology, Tamilnadu, India*

Abstract

A combination of more than one biometric is called multimodal biometric system. Here proposing an identification system by combining the feature of face and signature at matching score level. Thus, it is expected that spoofing two or more independent data would present more difficulty as compared to just one biometric data. With the hypothesis that impossible to spoof attack the physical quality and behavioral characteristic simultaneously, face and signature selected as the modalities of the biometric to be merged. The fusion, at the score level provides a matching score indicating the proximity of the feature vector with the template vector. These stacks can be blended with a simple sum rule. Storage of database in the form of these scores gives protection from hacking the databases. The results show that the error rates for this bimodal identification system is less than a single face identification system.GAR and FRR are used to evaluate the system performance.

Keywords: *Face, Signature, Genuine Acceptance Rate, False Rejection Rate.*

----------***----------

1. INTRODUCTION

Multibiometrics are a relatively new approach to overcome the problems of unibiometrics. Forced back by lower hardware costs, a multibiometric system uses multiple sensors for information acquisition. This leaves it to get multiple samples of a single biometric trait (called multi-sample biometrics) and/or samples of multiple biometric traits or multimodal biometrics). There are various different ways that multimodal systems can be made, based on the sources of the biometric information and the way the system is projected.

The term 'multimodal' sometimes refers specifically to the lawsuit where two or more different biometric modalities are in economic consumption (such as face and fingerprint), spell the term multi-biometrics are more generic [1].

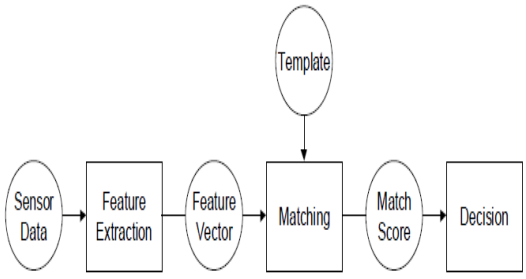

Fig-1: Biometric Authentication Process

Based on the combination techniques, the biometric fusion fall into three general categories, depending on the point at which the compounding is conducted: feature fusion combines low-level distinguishing features, score fusion makes use of multiple match scores, and decision level fusion logically combines accept/reject matching decisions. That is, classifying the systems depending on how early in the authentication process the data from the different sensors is combined as shown in the Fig.1.

1.1 Feature Level Fusion

In this architecture, the data extracted from the different sensors is encoded into a joint feature vector, which is then compared to an enrollment template (which itself is a joint feature vector stored in a database) and assigned a matching score as in a single biometric system

1.2 Score Level Fusion

There are two accesses to the compounding of the similarity score level: classification and grade combination

1.2.1 Classification

The idea of the classification approach is to consider verification as a classification problem with two classes: 'Accept' and 'Reject'. Each authentication is represented by a feature vector that is composed of similarity scores from the various sub-systems.

Training samples are collected, and machine learning or pattern recognition techniques (such as neural networks, support vector machines, decision trees, etc.) are used to build a model to distinguish the two classes. This classification model is applied to unseen data to make a verification decision.

1.2.2 Score Combination

Score combination involves taking several scores and applying a formula to combine them into a single score.

Some examples include adding the scores together, taking the average, or selecting the minimum or maximum score.

Such 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 [11]. Fusion at score level fusion is as shown in the Fig.2.

1.2.2.1 Simple Sum of Raw Scores

With no prior normalization matcher scores are simply added. Scores are neither rescaled, nor weighted to account for differences in matcher accuracy

1.2.2.2. Simple Sum of Z-Normalized Scores

This technique follows following steps:

- The estimation of the mean and standard deviation of imposter score distribution has been performed on the sample data.
- The mean of the imposter distribution is subtracted to normalize the scores and then are dividing by the standard deviation of the imposter distribution.
- Without weighting then the normalized scores are simply added. A normalized score is calculated by the equation:

$$s' = \frac{(s-\mu)}{\sigma} \quad (1)$$

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

1.2.2.3. 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.

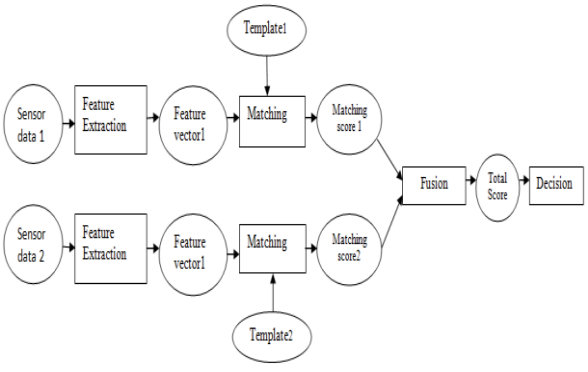

Fig-2: Fusion at Score Level

3. FUSION AT THE DECISION LEVEL

In this fusion strategy, a separate authentication decision is made for each biometric trait. These decisions are then combined into a final vote.

4. PERFORMANCE MEASURES

To judge the system performance of the scheme, the measurements used mainly are:

- Genuine acceptance rate (GAR), the rate of people genuinely accepted over the total number of enrolled people.
- False reject rate (FRR), the proportion of genuine transactions that are rejected by the system.
- False accepts rate (FAR), the proportion of impostor transactions that are assumed by the organization.

5. RELATED WORKS

Luca et al. used fingerprint and face to be fused at the score level [8]. PCA and LDA are used for the feature extraction and classification. Mean rule, product rule and Bayesian rule are used as the fusion techniques with FAR of 0% and FRR of 0.6% to 1.6%. Kartik et al. combined speech and signature by using sum rule as fusion technique after the min max normalization is applied [3]. Euclidean distance is used as the classification technique with 81.25% accuracy performance rate. Rodriguez et al. used signature as well with iris by using sum rule and product rule as the fusion techniques [5] Neural Network is used as the classification technique with EER below than 2.0%.

There are some related researches combined more than two biometrics as in [6] that combined hand geometry, fingerprint and voice by using global and local learning decision as fusion approach.

The accuracy performance is 85% to 95%.There are also some researches of multibiometric in which fusion is at decision level.Monwar and Gavrilova developed a multimodal biometrics system by using face, ear and signature. The features of the biometrics are extracted by using eigenface, engineer and eigensignature respectively and obtained a EER of 1.12% [12].Fusion at feature level, Feng et al. combined face and palmprint by concatenated the features extracted by using PCA and ICA with the nearest neighbor classifier (nnc) and SVM as the classifier [13].

From the related researches of the various multimodal biometric systems, at most of the cases the biometric features are stored in the database for the reference to the query inputs. It seems to be less secure, that is the spoofing of the biometry is possible. According to a multimodal biometry; fusion at score level with a simple sum rule gives good performance and easy implementation. Analyzed that multimodal biometry gives less error rates than a single biometry.

6. PROPOSED WORK

Biometrics, referred as the skill of distinguishing an individual based on his or her physical or behavioral traits, has been widely utilized as a security system in the aftermath of the latest security topics. Nevertheless, recent researches have indicated that many biometric traits are vulnerable to spoofing attacks. Here proposing a multimodal biometric identification system using face and signature as the modalities. The security of the system get enhanced due to the following reasons,

- Input face and signature are processed in the form of templates
- Face and Signature are the physical and behavioral characters of humans, which are difficult to spoof simultaneously.
- The database stored as the final scores of face and signature, which also enhances the security.

Step 1: Face and Signature are developed as templates-The part of biometric data common to all biometric systems is a template. A template is the refined, processed and stored representation of the distinguishing characteristics of a particular individual.

Step 2: Fusion of face and signature templates- Fusing face and signature templates and extracting features from that. Fusion has done by setting an alpha factor, which representing the depth of fusion. Based on these features the recognition is carrying out. Instead of considering the modality as image, template representation and feature extraction from that assumed to be easy for recognition. Fused Template of face and signature is as shown in Fig- 3.

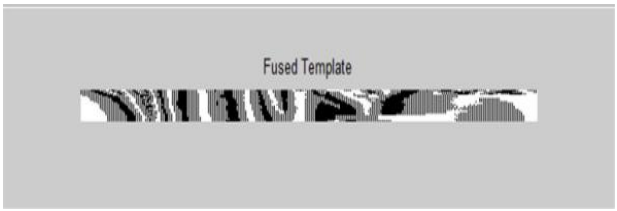

Fig- 3: Fused Template

Step 3: Feature extraction from the fused templates- Features extracting from the fused template are,

1. Fourier transform and spectrum
2. Phase angle
3. Real and imaginary part
4. PCA component
5. LDA component

Step 4: Recognition of face and signature and calculating the face and signature score has been carried out by Euclidian Distance as shown by the equation (2). This determines all nearest neighbors to each input feature vector and finds the smallest sum of distance chosen.

$$Ed = \sqrt{\sum_{i=1}^{p}(xi - yi)^2} \qquad (2)$$

Face recognition has been done by the template matching using the features extracted from the template. Signature recognition has been carried out by minutia extraction. The traditional method consists of the following steps. Binarization, thinning and minutiae detection

Binarization- This process consist in converting the gray scale image in binary image, i.e., the intensity of the image has only two values: black, representing the ridges, and white, representing the valleys and the background

Thinning- The objective of thinning is to notice the ridges of one pixel width. The process consists in performing successive erosions until a set of connected lines of unit-width is reached

Minutiae detection- From the binary thinned image, the minutia is detected by using pattern masks. After a successful extraction of minutiae, commonly they are stored in a template, which may contain the minutia position, minutia direction (angle), minutia type. Then it is compared with the query image. Ridge Segmentation and Orientation Field are used for finding the minutia position, angle and other parameters. Minutiae image of the signature is as shown in Fig-4.

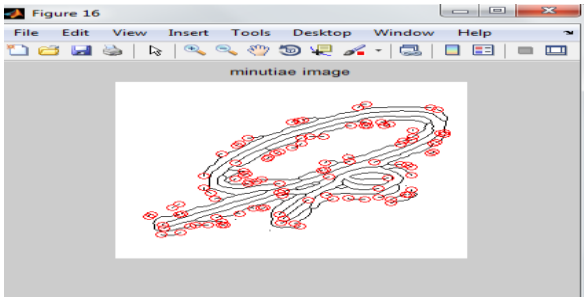

Fig- 4: Minutiae image of Signature

Step 5: Fusion of face and signature score and calculating the final score (Final score=Face score +Signature score) - The face score and signature combined by a simple sum rule and finding the final score. From the literature survey, found that the sum rule gives better results than other rules. Then these final scores are given to the neural network as inputs for the classification.

Step 6: Based on the final score, classifying the input images - The input to this classifier is the set of final scores; the output will be the final decision about the user claimed identity. In order to perform this task, the NN must be set by target. Fig-5 and 6 representing the Message Box Indicating the successful authentication and a failed one

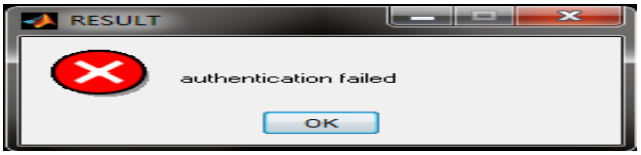

Fig-5: Message Box Indicating If the Face and Signature are not matched

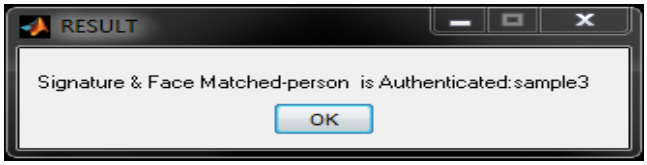

Fig-6: Message box indicating the face and signature matched to the person 1

7. EXPERIMENTAL RESULTS

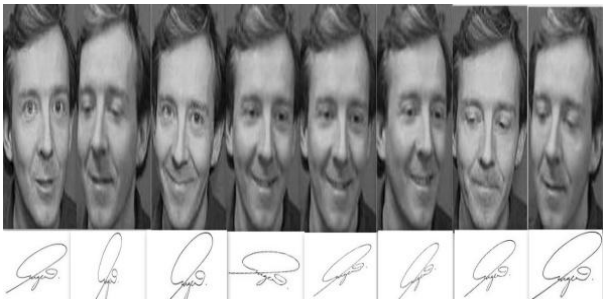

Fig- 7: Samples of face and signature

The experiments are carried out on the database of 40 users (ORL database). It contains the 8 different facial poses and 8 samples of the signature of each user. The model of the experimental setup has been shown in Fig 7.In this 3 face and 3 signature images are tested against 5 trained face and signature images. By considering the entire system, 12 imposters are identified from the total face and signature samples.

The equations (3), (4) are used for calculating the Genuine Acceptance Rate and False Rejection Rate are as shown below.

$$\text{GAR} = \frac{\text{No.of Genuine attempts accepted}}{\text{Total No.of genuine attempts}} \quad (3)$$

$$\text{FRR} = \frac{\text{No.of Genuine attempts rejected}}{\text{Total No.of genuine attempts}} \quad (4)$$

Table-1: Comparison of Error Rate and Accuracy Rates

Systems	**Biometric identifiers**	**Fusion level**	**GAR and Error rate**
Proposed System	Face, Signature	Score level (Sum rule)	94%, 6%
Proposed System	Face	-	90.5%,9 .5%
Suryanti Awang et al. [7]	Face, Signature	Feature level (Sum rule)	85.71%, 14.2-20%
Kazi M.M et al. [4]	Face	-	87%, 12%

From this calculation, 94% of GAR and 6% of error rate has been obtained. Comparing the proposed multibiometric face and signature system with single face identification system, the error rate is found to be less.

Table.1 shows the Comparison of Error Rate and Accuracy Rates .From the table it has been found that for a multibiometric system, the combination of score level with sum rule is better than feature level with sum rule. That is the acceptance rate is higher for score level with sum rule.

8. CONCLUSIONS AND FUTURE WORK

An identification system by the fusion of two modalities such as face and signature developed. For the score level fusion, the data can be easily accessed. By the analysis it has found that the error rate is less compared to a single biometric system with face. And also the score level fusion with sum rule is better than feature level with sum rule. By considering 40 persons, the genuine acceptance rate is found to be of 94% and the error rate is of 0.06 for a multibiometric system of face and signature. The future work can be done with other fusion levels, modalities, matching algorithm, fusion rules, classifier which can provide less error rates and more accuracy.

REFERENCES

[1] Frischholz.R.W and Dieckmann.U, (2000) 'BiolD: a multimodal biometric identification system,' Cover feature.

[2] Jain.A.K, Ross.A and Pankanti.S, (2006) 'Biometrics: a tool for information security,' IEEE Transactions on Information Forensics and Security, vol. 1, pp. 125-143.

[3] Kartik.P, S.R. Mahadeva Prasanna and Vara.R.P, (2008) 'Multimodal biometric person authentication system using speech and signature features,' in TENCON 2008 - 2008 IEEE Region 10 Conference, Ed, pp, 16.

[4] Kazi.M.M, Rode Y.S, Dab hade S.B, (2012), 'Multimodal Biometric System Using Face and Signature: A Score Level Fusion Approach'.

[5] Rodriguez.L.P, Crespo.A.G, Lara.M and Mezcua.M.R, (2008) 'Study of Different Fusion Techniques for Multimodal Biometric Authentication,' in Networking and Communications. IEEE International Conference on Wireless and Mobile Computing.

[6] Toh.K.A, J. Xudong and Y. Wei-Yun, (2004) 'Exploiting global and local decisions for multimodal biometrics verification,' Signal Processing, IEEE Transactions on, vol. 52, pp. 3059-3072.

[7] Suryanti Awang, Rubiyah Yusof, (2011) 'Fusion of Face and Signature at the Feature Level by using Correlation Pattern Recognition', World Academy of Science, Engineering and Technology 59.

[8] Gian Luca Marcialis and Fabio Roli, (2007) 'Serial Fusion of Fingerprint and Face Matchers' M. Haindl,© Springer-Verlag Berlin Heidelberg 2007.

[9] Shou-Der Wei, Shang-Hong Lai (2008) IEEE Transactions on Image Processing 17(11), 2227-2235.

[10] Abhishek Nagar, Karthik Nandakumar, Anil.K.Jain, (2012) 'Multibiometric Cryptosystems Based on Feature-Level Fusion,' IEEE transactions on information forensics and security, vol. 7, no.

[11] Ulery B., Fellner W., Hallinan P., Austin Hicklin, Watson C. (2006) Studies of Biometric Fusion report, National Institute of Standards and Technology, 1-14.

[12] M. M. Monwar and M. L. Gavrilova, (2009)"Multimodal Biometric System Using Rank-Level Fusion Approach," Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on, vol. 39, pp. 867-878.

[13] G. Feng, K. Dong, D. Hu and D. Zhang, (2004) "When Faces Are Combined with Palmprints: A Novel Biometric Fusion Strategy," in Biometric Authentication. vol. 307.

BIOGRAPHIE

Amritha.k.c was born in Kerala, India in 1990. She received B.E degree in Electronics and communication engineering from Anna University Chennai, tamilnadu,india in 2012 .She is currently working towards M.E degree in embedded system technologies at Anna University Chennai ,tamilnadu,india. Her research interests Digital Image processing, embedded system, digital electronics.