RESEARCH ARTICLE OPEN ACCESS

Improving the accuracy of fingerprinting system using multibiometric approach

Safa M. AL-Taie
Electrical and computer engineering, Florida Institute of Technology, Melbourne, Fl, USA

ABSTRACT
Biometric technology is a science that used to verify or identify the individual based on physical and/or behavioral traits. Although biometric systems are considered more secure than other traditional methods such as password, or key, they also have many limitations such as noisy image, or spoof attack. One of the solutions to overcome these limitations, is by applying a multibiometric system. Multibiometric system has a significant effect in improving the performance of both security and accuracy of the system. It also can alleviate the spoof attacks and reduce the fail to enroll error. A multi-sample is one implementations of the multibiometric systems. In this study, a new algorithm is suggested to provide a second chance for the genuine user who is rejected, to compare his/her provided finger with the other samples of the same finger. Multisampling fingerprint is used to implement this new algorithm. The algorithm is activated when the match score of the user is not equal to a threshold but close to it, then the system provides another chance to compare the finger with another sample of the same trait. Using multi-sample biometric system improved the performance of the system by reducing the False Reject Rate (FRR). Applying the original matching algorithm on the presented database produced 3 genuine users, and 5 imposters for the same fingerprint. While after implementing the suggested condition, the system performance is enhanced by producing 6 genuine users, and 2 imposters for the same fingerprint. This work was built and executed depending on a previous Matlab code presented by Zhi Li Wu. Thresholds and Receiver Operating Characteristic (ROC) curves computed before and after implementing the suggested multibiometric algorithm. Both ROC curves compared. A final decision and recommendations are provided depending on the results obtained from this project.

***Keywords*:** Biometrics, Multibiometrics, Multi-sample, FRR, FAR, ROC curves.

I. INTRODUCTION

A biometric system determines one or more physical or behavioral traits, including fingerprint, face, iris, voice, signature, gait, hand vein, odor, and DNA. The set of attributes that is related to a specific person represents his\her identity, and gives the system the ability to identify the uniqueness of that individual.

There is no doubt that a multibiometric system plays a critical role in most applications and it receives a lot of attention due to their advantages in overcoming limitations in unibiometric systems. Applying multibiometric system can improve the accuracy of authentication system rather than single biometric system. Using multi algorithm to process the same biometric traits can minimize the cost, because it does not require an additional sensor to capture those traits. (Gokberk et al., 2005) combined multiple algorithms for 3D face recognition.

In order to recognize the individual, the most important task: is to establish the relation between the individual and his identity. Person identity refers to the ability of verifying the claim of the user. (Todorov, 2007) To verify the identity of any individual, three fundamental methods can be used: (a) "what he knows": this method depends on the fact that the person has a special knowledge of a secret information (e.g., password, personal ID number, cryptographic key), (2) "what he possess extrinsically": this method relies on the fact that the person has exclusive possession of the external token (e.g., passport, driver license, personal device as mobile phone), (3) "Who he is intrinsically"(biometric recognition): this method establish the association between the individual and his/her identity based on his/her physical inherent or behavioral traits.

In general, biometric recognition is defined as the science that establish the identity of the individual based on his/her physical or behavioral traits. Biometric recognition can be either fully automated (i.e. without human intervention) or semi-automated (i.e. with human intervention).

II. METHODOLOGY

While a biometric system with the single biometric trait (unibiometric) can improve the security of an application in a significant way, it can also be the weakest point in this system. Usually when a biometric is chosen to be the trait that will determine users' originality, because of the unique properties for this trait. Unibiometric systems can be exposed to many limitations in the different

biometric system levels figure (1). On the other hand implementing multibiometrics can insure both security and accuracy in the authentication system. Combining multiple techniques can improve the performance of the authentication system [1].

A. Biometric Used In The Project

In this project Fingerprint Minutiae were chosen to be the Biometric traits. It has been chosen because it presents the most Biometric trait adopted by commercial applications among other traits, especially with facilities that require speed more than accuracy [2]. Fingerprints can exhibit sufficient uniqueness, also fingerprint can be considered Immutable biometrics [3].

B. Data Base implemented in the project

The first phase of this project was choosing the DataBase. This is an important step to make sure that all fingerprints included in this project are obtained under the same conditions, which is an important factor in the experimental work. In this project the FVC2004 DataBase was chosen, it was obtained from thermal sweeping sensor "FingerChip FCD4B14CB" by Atmel. All fingerprints images are of 300x480 (144 K pixels) with 512 dpi resolution [4]. This fingerprint DataBase contains (80) samples as each finger of the two hands has (8) samples.

Application used to implement the project

The fingerprint reader and minutiae extractor implemented by Zhi Li Wu (2003) was chosen to implement this project. Zhi Li Wu software was coded in the Matlab platform, including all functions required to read fingerprint scans to the real minutiae extractor phase, and getting matching score results [5]. This software was originally designed to provide only match scores after comparing two minutiae properties files. In our project we added extra stages in the matching process. These additional stages followed specific conditions, where these conditions reflected the proposed algorithm to enhance the performance of the system in the False Reject Rate (FRR).

C. The Receiver Operating Characteristic (ROC) curve

The Receiver Operating Characteristic (ROC) curve, is a graphical presentation of the system performance. In biometric science the ROC curve will represent the false rates of the system, including both False Reject Rate (FRR), and False Accept Rate (FAR) [6]. The main question in this experiment was: Can the False Reject Rate (FRR) be enhanced if the system algorithm was modified at the matching phase? First to answer this question we draw the ROC curve for the fingerprint recognition system before modifying the match process. The second step was to modify the algorithm by considering a second chance for scores of match process which are close to the threshold. So instead of providing final decision (reject) for scores which are close to the threshold, a suggestion for the user asking him/her to provide his/her fingerprint again to be compared it with another sample which is stored in the template in the database. This second chance provided the user an opportunity to overcome some physical problems that can affect the recognition process. These problems led to provide less information to the sensor so the sensor refused the genuine user, and caused in a False negative (FN). In this project we proposed to use a multi-sampling biometric system as a second chance in case of having close but not the requested matching score algorithm as shown in figure (2). According to [7], the following terms are defined as:

$$Th_{mean}=(Match\ score1+Match\ score2+\ldots+Match\ score8)/8$$

$$Th_j = Smin + (j-1)*p$$

$$P = (Smax-Smin) / (T-1)$$

$$FAR(Thj) = 1/L0 \sum_{Li+1}^{L} I(Si \geq Thj)$$

$$FRR(Thj) = 1/L1 \sum_{i=1}^{Li} I(Si < Thj)$$

Where:

$$I(x) = \begin{cases} 1, \text{ if } x \text{ is true,} \\ 0, \text{ otherwise.} \end{cases}$$

Th_{mean}: refers to Th of the system.
Th_j : refers to Th value at each sample of the finger.
Smin: refers to the minimum matching score.
Smax: refers to the maximum mathing score.
T: refers to the total number of the samples for the same finger.
L0: refers to the match score of imposter class.
L1: refers to the match score of genuine class.
L= (L0+L1) the total number of the scores.
Si: refers to the score at each sample.

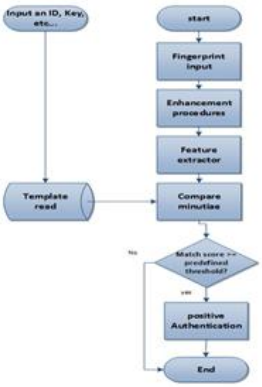

Figure (1) the original algorithm

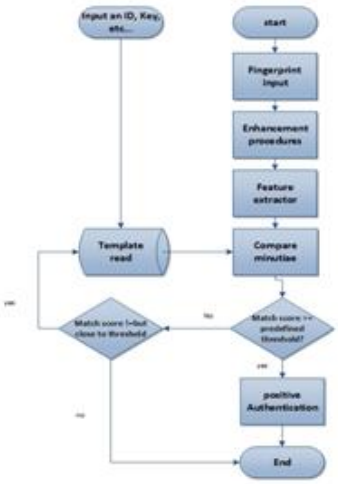

Figure (2) the proposed algorithm

Before implementing the proposed algorithm

- The first set of fingerprints with 8 image samples were all read, enhanced, features were extracted, and stored in a*.m file for further matching.
- Calculating the threshold of the system by implementing the mean deviation equation for all matching scores obtained during the matching phase, using equation (1).
- Classifying both genuine L1 match scores (L1=3) and L0 imposter match score (L0=5), with a total number of match score L=L0+L1=8.
- Generating a set of thresholds (thj) j=1-T as shown in table 1, where Smax> (thj)>Smin, where Smax is the maximum matching score, and Smin is the minimum matching score. All thresholds were equally placed by implementing both equation (2) and equation (3).
- Both FAR and FRR were calculated at each threshold, using equation (4) and equation (5) respectively, as shown in table 2 and table 3.
- Connecting the set points of FAR and FRR, to obtain the ROC curve, as shown in figure (3).
- Determining the best operating point for such system, with the lowest FRR and FAR. Which produced FAR and FRR (0.2, 0.33).

Table I

Thj	Equation	Th
Th1	**38.3+(1-1)*1.9**	**38.3**
Th2	**38.3+(2-1)*1.9**	**40.2**
Th3	**38.3+(3-1)*1.9**	**42.1**
Th4	**38.3+(4-1)*1.9**	**44**
Th5	**38.3+(5-1)*1.9**	**45.9**
Th6	**38.3+(6-1)*1.9**	**47.8**
Th7	**38.3+(7-1)*1.9**	**49.9**
Th8	**38.3+(8-1)*1.9**	**51.6**

Table II

Thj		FAR
1	Th(30)	1
2	Th(37.85)	0.5
3	Th(45.7)	0
4	Th(53.55)	0
5	Th(61.4)	0
6	Th(69.25)	0
7	Th(77.1)	0
8	Th(84.95)	0

Table III

Thj		**FAR**
1	Th(38.3)	1
2	Th(40.2)	0.2
3	Th(42.1)	0
4	Th(44)	0
5	Th(45.9)	0
6	Th(47.8)	0
7	Th(49.9)	0
8	Th(51.6)	0

After implementing the suggested algorithm The second set of fingerprints with 8 image samples, and all images were read, enhanced, features were extracted and stored in a*.m file for the further matching process.
Calculating the threshold of the system by implementing the mean deviation equation for all matching scores which are obtained during the matching phase, using equation (1), and adding the new condition of matching scores that are near to threshold and not equal to it.

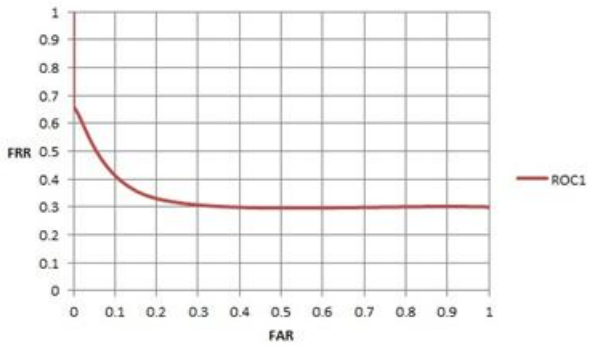

Figure (3)

Table IV

	Thj	FRR
1	Th(30)	0.16
2	Th(37.85)	0.16
3	Th(45.7)	0.5
4	Th(53.55)	0.83
5	Th(61.4)	0.83
6	Th(69.25)	0.83
7	Th(77.1)	0.83
8	Th(84.95)	0.83

- Classifying both genuine L1 match scores L1=6, and L0 imposter match scores L0=2, with a total number of match scores L=L0+L1=8.
- After implementing the proposed algorithm, both FAR and FRR were calculated at each threshold using equation (4) and (5) respectively, as shown in table 4 and table 5.
- Connecting the set points of FAR and FRR to obtain the ROC curve after implementing the suggested algorithm, as shown in figure (4).
- Determining the best operating point for the system, with the lowest FAR and FRR. In this case, the best point of the system represented by FAR and FRR (0.5, 0.16).

Table V

	Thj	FRR
1	Th(38.3)	0.33
2	Th(40.2)	0.33
3	Th(42.1)	0.66
4	Th(44)	0.66
5	Th(45.9)	0.66
6	Th(47.8)	0.66
7	Th(49.9)	0.66
8	Th(51.6)	1

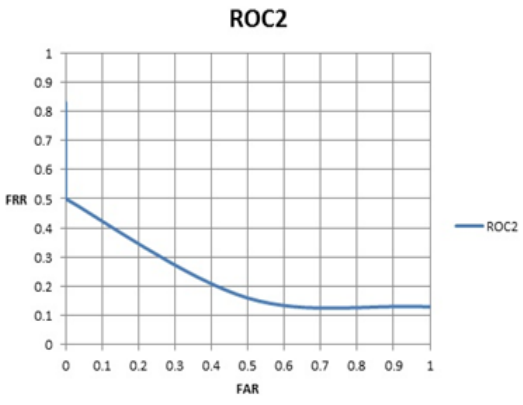

Figure (4)

III. Results And Discussion

While it is important for some environments to have a high security level, it also can produce positive and negative results. Positive results, will ensure that only genuine users allowed to pass the biometric authentication test. On the other hand, the negative results will increase the potential of refusing the genuine users. The suggestion of modifying the original algorithm and adding a new condition, enhanced the performance of the system by reducing the FRR errors. The new proposed condition, tends to provide a second chance to the genuine user who was falsely rejected, by comparing his/her fingerprint with other samples of the same fingerprint. This condition is implemented when the match score of any individual is not equal to a threshold value but close to it. Using multibiometric system is better than using single biometric, because the individual can have more samples or more traits to use, in case of any error occurred. This provided another chance to the user instead of rejecting him/her at first time. The results show that applying the presented database to the original algorithm (before modification) provided 3 genuine users, and 5 imposters for the same fingerprint. While after modifying the algorithm and implementing the suggested condition, then the system obtained 6 genuine users, and 2 imposters for the same fingerprint. This is a good evidence that the performance of the biometric system is improved and enhanced.

Both systems are examined with the ROC curve, by plotting FAR and FRR before and after the suggested condition. The observed figure (5) shows that the value of FRR is improved after implementing the condition. The area under the curve for ROC2 is closer to the (x-axes) compared to ROC1. So the performance of system 2 with (ROC2) is better than system1 with (ROC1).

This additional stage decreased the FRR value from 0.33 to 0.16, and the authentication system is improved by reducing the number of False Negative (FN) cases. These results can be applied to the authentication systems that do not need a high security level, where the time factor is more important than the security level for the system. A system having this performance is recommended for facilities that will have a large input number of people to authenticate, where time becomes more precious than results. Administrator for such systems would prefer to have such performance and such error handling, to overcome more complicated problems in the future. On the other hand, users that will enroll in such authentication systems will have additional chances to compare the same provided fingerprint with other samples (in case of verifying the proposed condition) before they are considered as imposters.

Enrollment time will be a critical phase in such system, usually in a normal circumstances, users have to provide the biometric once or twice to enroll in the system. In this project, an additional time required during the enrollment phase. Depending on results, the more samples that users

provided in the enrollment phase, provide the best results to the recognition system, especially in the case of the user is not rejected at the first time.

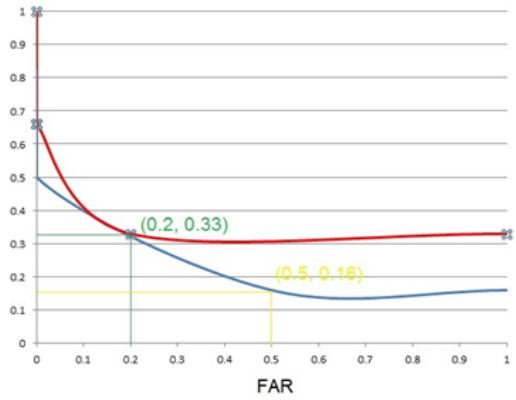

Figure (5)

References

[1]. Norman Poh, Samy Bengio and Jerzy Korczak, "A multi-sample multi-source model for biometric authentication" IEEE International Workshop on Neural Networks for Signal Processing (NNSP), 2002.

[2]. Arun Ross, Norman Poh, "Multibiometric systems: overview, case studies, and open issues" 273- 292. In *Handbook of remote biometrics*, 2009.

[3]. Anil K. Jain, Arun A. Ross, Karthik Nandakumar, "Introduction to biometrics" 52-53. Springer Science+Business Media, LLC, 2011.

[4]. Fingerprint verification competition, (2004). Available: http://bias.csr.unibo.it/fvc2004/default.asp

[5]. Zhi li wu, "Fingerprint recognition", Available: http://www.comp.hkbu.edu.hk/~vincent/resPaper.htm

[6]. Kar-Ann Toh∗, Jaihie Kim, Sangyoun Lee, "Maximizing area under ROC curve for biometric scores fusion" Pattern Recognition, 2008.

[7]. Giorgio Giacinto, Fabio oli, Roberto Tronci, "Score Selection Techniques for fingerprint Multi- modal Biometric Authentication" (2005).