ANALISIS 10(2), 139-150 (2003)

THE PERFORMANCE OF USER VERIFICATION USING TWO FINGERPRINTS BASED ON ERROR RATES

MOHAMAD AMIR ABU SEMAN
HATIM MOHAMAD TAHIR
ROSHIDI DIN
Faculty of Information Technology
Universiti Utara Malaysia

ABSTRACT

Biometric technologies, especially fingerprint verification, have started to attract users around the world to use it to secure their places or properties. The current implementation of a fingerprint verification system has faced several problems such as noisy finger and fingerprint misplacement by the user. To solve or minimise this kind of problem, the approach using two fingerprints on the verification process has been tried in this research. Two classifiers are used to study the performance level of the system, and compared to the current system that uses a single fingerprint. In this research, total error rate has been used as an indicator to the performance level of the system.

ABSTRAK

Teknologi biometrik terutamanya pengesahan cap jari telah menarik minat penggunaannya di seluruh dunia dalam memastikan keselamatan tempat atau harta benda. Pelaksanaan pengesahan cap jari kini menghadapi beberapa rintangan antaranya silap letak jari dan cap jari yang cemar. Bagi menyelesaikan atau mengurangkan masalah sedemikian, pendekatan menggunakan dua cap jari untuk proses pengesahan dilaksanakan untuk penyelidikan ini. Dua pengkelasan digunakan untuk mengkaji tahap prestasi sistem ini dan dibandingkan dengan sistem kini yang menggunakan satu cap jari saja. Dalam penyelidikan ini, jumlah kadar ralat digunakan sebagai penentu tahap prestasi sistem tersebut.

INTRODUCTION

User verification or identification has played a major role in our daily life. Since the earlier era of human kind, the technology to verify a

person for their authenticity has been rapidly moved. It was started from the system used by the Nile Valley villagers that identify people via their physiological parameter such as scar, eye colour, height, and so on (Visionic, 2000). Later, people move to use personal identification card that includes personal details and a thumbprint. Although the identification card provides a simple and reliable verification method, it is not a robust method because the people can simply make a fake copy of this identification card. Therefore, the other robust method is introduced to cater the problem of possession based on, verification process.

Increase computer capabilities make the verification technology take this opportunity for its automated system. In the late 1960's, Shearson Hamill, an investor at Wall Street had implemented a hand geometry recognition system called 'Identimat' to control access to their top secret applications (AIDC). This implementation started the new era of automated system for recognising a person based on their physical characteristics which is known as *Biometrics*. Physiological characteristics, which had been stated were the physical characteristic of the person such as the fingerprint, hand geometry and retinal pattern. In contrast, the behavioral characteristics refer to the specific behavior of a person that is different from other people such as, how they speak, sign, or use the keyboard.

The biometric verification system has faced many issues on its implementation such as performance level, which may refer to the accuracy, speed and robustness of the system (Hong, & Jain, 1998). These issues have emerged because of several factors, for example, in the case of fingerprint verification systems, poor quality image from the fingerprint sensor is caused by several factors or noises that have affected the fingerprint pattern. The major noises during the fingerprint acquiring process are improper placement of the finger on the fingerprint scanner and the finger cut (Jain, Prabhaker & Ross, 1999).

Multimodal is introduced to solve the problem with low performance of the biometric systems that used mono biometric modality. This approach uses a strong biometric modality, which has a higher reliability to support the weaker biometric modality. Even though this approach has increased the system performance, but there are still several drawbacks on its implementation (Daugman, 1999):

i. The cost for its implementation is higher compared to mono modality biometric implementation as a result of using several devices.

ii. It also compromises the performance level of strong biometrics that has been used with weak biometrics.

This research has tried to improve the performance of a fingerprint verification system by using the combining of two fingerprint verification decisions. Hopefully, the combination can decrease the total error rate of the single fingerprint verification system. When the total error rate is minimized, the performance level of the fingerprint verification system could also be increased.

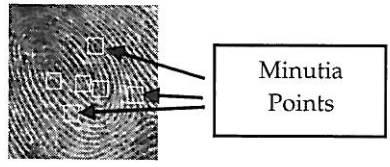
In this research, only two fingers, which are the middle and index finger from the left hand, are used. Two fingers were used because it could provide a better performance compared to the single fingerprint method, and it is hard for user to present more than two fingerprints. These fingers were used as a result of its performance, which is better than thumbs (Jain *et al.*, 1999). The fusion of the fingers are done at the decision level. It means that the decision (accept or reject) and verification scores from the verification processes are analysed to get the final decision for the system.

Only two simple classifiers have been used in this research to reduce the bias of the classifier on the system performance and to look at the performance of combining two fingerprints. Although the classifier can also played a major role in the system performance, but by using the simple classifier, the bias on the performance level can be minimised.

FINGERPRINT VERIFICATION SYSTEM

Fingerprint verification is one of the most reliable personal identification methods available nowadays (Lee & Gaensslen, 1991). The fingerprint verification system is based on ridge patterns that creates several unique fingerprint features such as minutia points (ridge ending and ridge bifurcation) (Figure 1).

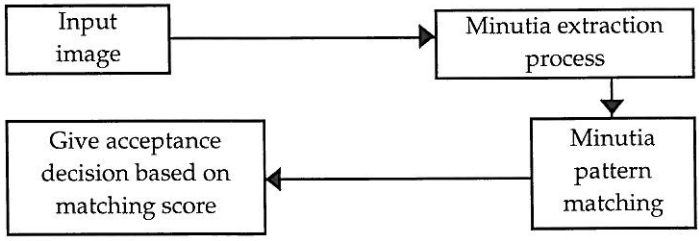
Figure 1
Location of Minutia Points



Traditional ink-based fingerprint verification technique is analysed for the relative position of minutia points (Jain, Hong, Pankanti & Bolle, 1997). This technique has been widely used in the personal identification method in most countries. While the automated fingerprint verification system nowadays is based more on the feature of the fingerprint such as ridge orientation and finger temperature.

The automated processes of fingerprint verification generally can be decomposed into two main fundamental tasks (Jain *et al.*, 1997; and Jain *et al.*, 1999): (i) minutia extraction, (ii) minutia pattern matching (Figure 2). In the first task, minutia points and the patterns of the ridges are extracted from the input fingerprint image captured by the fingerprint scanner. Then, the minutia pattern template is created to establish the identity of the person. The matching process between the live template with the one that is stored in database will produce the verification score which is used to give an acceptance decision for the user.

Figure 2
Fingerprint Recognition Process (Jain *et al.*, 1999)



For the time being, fingerprint verification is the most matured technique and the research that is involved with this technique is being extensively conducted. Because of its maturity, the validity of fingerprint identification has been well established (Jain *et al.*, 1997).

The presence of noises could decrease the quality of the fingerprint images. Although dirt and oil may have decreased the quality of the fingerprint image, other factors such as scars, bruises and misplacement of the finger can highly effect the quality of fingerprint image, which could lead to a lesser performance of the systems.

MULTIMODAL BIOMETRIC SYSTEM

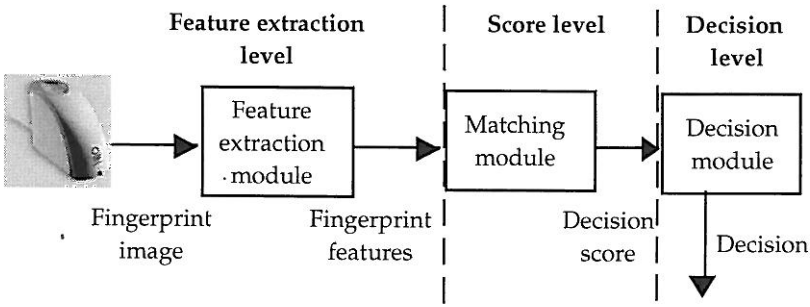
Verification cannot provide an adequate performance in the level of error rate such as false acceptance rate (FAR), false reject rate (FRR) or

total error rate (TER) on a single template of biometrics (Prabhakar, & Jain, 2002; Bigun, Bigun, Duc & Fisher, 1997; and Verlinde, Chollet & Acheroy, 2000). To address the problem, a biometric system needs to be combined with other a biometric identifiers, multiple sensors, multiple impressions, multiple prints, multiple matchers, or non-biometric attributes (Hong & Jain, 1999).

Most of the research in the performance enhancement being done by a number of researchers involve the method of combining several modality of biometrics (Ross, Jain & Jian-Zhong, 2000; and Verlinde *et al.*, 2000). There are also approaches that use multiple expressions of a single modality such as multiple face expressions or multiple attempts on a single fingerprint. Besides that, the verification of two different fingerprints could also be used for realising a multi-modal biometric verification system.

There are several levels of fusion to fuse or combine the biometrics such as at the feature extraction level, score (confidence) level, or decision (abstract) level. Figure 3 shows the fusion level of the fingerprint verification process.

Figure 3
Fusion Level Diagram



A strong biometric which is more reliable such as the fingerprint is better used alone than in combination with a weaker one, which is less reliable such as voice recognition (Daugman, 1999). The error probabilities using 'OR' and 'AND' rules have been proved that the hypothesis of combining weak and strong modality (test 1 and test 2) would decrease the performance of the strong biometric (Daugman, 1999). The explanation is given below.

Rule A: Disjunction (OR rule) – accept if either test 1 or test 2 is passed.
Rule B: Conjunction (AND rule) – accept if both tests are passed.

The error probabilities have been looked for the combined biometrics. These error probabilities will be the probability of false accept (FA) and probability of false reject (FR). So, for two biometric tests (1 and 2), there are four possible errors:

$P_1(FA)$ = probability of false accept using biometric 1 only.
$P_1(FR)$ = probability of false reject using biometric 1 only.
$P_2(FA)$ = probability of false accept using biometric 2 only.
$P_2(FR)$ = probability of false reject using biometric 2 only.

For the "OR rule", there is a false reject (FR) only if both tests produce false reject on the verifications. As a result, the combined probability of these two tests, $P_A(FR)$ is the product of probabilities for false reject on test 1 and test 2 has a false accept (Equation 3.1).

$$P_A(FR) = P_1(FR)P_2(FR) \tag{3.1}$$

The false accept for the combined biometric test is the complements of the probability that neither test 1 nor test 2 has a false accept (Equation 3.2).

$$\begin{aligned} P_A(FA) &= 1 - [1- P_1(FA)][1 - P_2(FA)] \\ &= P_1(FA) + (P_1(FA)P_2(FA)) \end{aligned} \tag{3.2}$$

For the second rule "AND rule", if false accept (FA) occurs in both test, then the combined biometric could be a false accept. As a result, the probability that the combined biometric to have a false accept, $P_B(FA)$, is the product of the false accept probability for both tests (Equation 3.3).

$$P_B(FA) = P_1(FA)P_2(FA) \tag{3.3}$$

As a result from the OR rule, we can see that the false reject for the combined biometric, $P_A(FR)$, is smaller than the single biometric $P_1(FR)$ or $P_2(FR)$. The probability for the false accept on the combined biometric, $P_A(FA)$, is bigger than the probability of each test alone $P_1(FR)$ or $(P_2(FR)$. The false reject for the combined biometric will occur, only if test 1 or test 2 has the false reject. So, the false reject probability, $P_B(FR)$, would be the complements of the probability that neither test 1 nor test 2 has a false reject (Equation 3.4).

$$\begin{aligned} P_B(FR) &= 1 - [1 - P_1(FR)][1 - P_2(FR)] \\ &= P_1(FR) + P_2(FR) - P1(FR)P_2(FR) \end{aligned} \tag{3.4}$$

For the AND rule, the probability for the combined biometric is opposite from the probability we get in OR rule. The false accept rates for the combined biometric, $P_2(FA)$, would be smaller than the false accept probability on each test $P_1(FA)$ or $P_2(FA)$ alone. In contrast, the probability of false reject for the combined biometric, $P_B(FR)$, would be bigger compared to the probability of false reject when each biometric is used alone $P_1(FR)$ or $P_2(FR)$.

As a conclusion, a strong biometric is better to be used alone rather than combined with a weaker one. To obtain any benefit from the combination of any strong biometric with the weaker one, the threshold value for the weaker one needs to be changed to suit each case (Daugman, 1999).

METHODOLOGY

There is no adequate number of respondents for a biometric test (Biometric Working Group, 2000). In this research, 33 respondents from Faculty of Information Technology, Universiti Utara Malaysia have been chosen (three male academic staff and the balance are students). The number of respondents were the average number used in Hong and Jain, 1998; Jain *et al.*, 1997; Jain *et al.*, 1999; Prabhakar and Jain, 2002; and Verlinde, 1999. From the student respondents, 10 of them were female and the others were male. In this research, there are two kinds of tests that have been done to collect the data:

i. True verification test.
ii. Impostor verification test.

The verification scores acquired from each respondent were used as data for this research. The verification process conducted is different from each other and it depends on the type of test involved. The data is in verification scores or soft decision form, which is a decimal value ranging from 0.00 to 1.00.

Both tests scores (true verification test and impostor test) have been used to study the error rate for the verification system. These scores were compared to several threshold values to get the decision for each finger on each user. Results from each finger then have been combined using 'OR' and 'AND' rule (Daugman, 1999; Verlinde, 1999) to get the user's authorisation.

a. True User Verification Test

In this test, all of the users need to verify their fingerprint that they had registered in the system. Normally, the users' fingers will have some noise such as fingerprint misplacement during the verification process. So, each user must clean their fingers to be free from noise. Scores obtained from this test were used to look at the false rejection rate of the system, which will indicate the error caused by the system. In this test, all respondents have been involved to collect the true verification scores and we found that four respondents have failed verification caused by humidity. So, the results gathered is based on the total data for 58 [(33 – 4) x 2] data.

b. Impostor Verification Test

In this research, the scores from the false or impostor verification have also been identified. From here, the range of the score for this type of verification has been known. The scores obtained from this test is used to look at the false accept rate for this system. Manual cross-match for the templates have been done to collect the data. For this test, only ten respondent templates have been cross-matched against the other 29 (33 – 4) respondents. For each respondent, they have tried to verify the other user using their own fingerprints. For this test, only two selected fingerprints have been used, which have been chosen from the process of selecting the best two fingers. As a result, 580 [(29 x 10) x 2] data scores were obtained from this data gathering process.

RESULTS

The performance rate is based on the error rate of the system. All the error rates are collected based on the scores of the true user and impostor verification test. There are two error rates (false acceptance rate and false rejection rate) that we get from the test and these two error rates have been combined into a single error rate called the *Total Error Rate (TER)*. The summary of TER collected from this research is shown in Table 1 and further depicted in Figure 4.

FAR = Number of False Accept / Total Trial (4.1)

FRR = Number of False Reject / Total Trial (4.2)

TER = FAR + FRR (4.3)

Table 1
Total Error Rate (TER) for Left Index, Left Middle, 'OR' Rule and 'AND' Rule

Threshold	TER Left Index	TER Left rule	TER 'AND' Middle	TER 'OR' rule
1E-30 to 1E-29	1.0000	1.0000	1.0000	1.0000
1E-28 to 1E-17	0.8421	1.0000	0.9744	0.8205
1E-16 to 1E-15	0.7105	1.0000	0.9744	0.6923
1E-14	0.5263	0.9211	0.9231	0.4872
1E-13	0.5000	0.7632	0.8205	0.4103
1E-12	0.4474	0.6579	0.7692	0.3077
1E-11	0.2632	0.5263	0.5897	0.1795
1E-10	0.1842	0.5000	0.5385	0.1282
1E-9	0.1316	0.3421	0.3846	0.0769
1E-8	0.0526	0.2368	0.2564	0.0256
1E-7	0.0263	0.0789	0.0769	0.0256
1E-6	0.0000	0.0526	0.0513	0.0000
1E-5	0.0000	0.0263	0.0256	0.0000
1E-4 to 1E-3	0.0000	0.0000	0.0000	0.0000
1E-2	0.0259	0.0776	0.0991	0.0043
1E-1	0.1164	0.2241	0.3017	0.0388
2E-1	0.1810	0.2759	0.3922	0.0647
3E-1	0.2284	0.3233	0.4526	0.0991
4E-1	0.2629	0.3621	0.5000	0.1250
5E-1	0.2931	0.4052	0.5345	0.1638
6E-1	0.4052	0.5086	0.6810	0.2328
7E-1	0.5345	0.6509	0.8147	0.3707
8E-1	0.6897	0.7414	0.8966	0.5345
9E-1	0.7328	0.8190	0.9267	0.6250

From Figure 4, we found that the result of the two fingerprint combination using 'OR' rule has a lower total error rate compared to the other methods which use the 'AND' rule and single fingerprint. Although the left index finger is better compared to the left middle finger, the combination scores of these two fingers will produce the better result for verification. The total error rate for 'OR' rule was lower than the one for single fingerprint verification approach because the system can still make a true decision on either left index or left middle fingers. So, if either one of the fingerprints have a problem, the true decision can still be made by the system.

thesis, Ecole Nationale Supérieure de Télécommunications, Paris, France: http://www.sic.rma.ac.be/Publications/index.html

Verlinde, P., Chollet, G., & Acheroy, M. (2000). Multi-modal identity verification using expert fusion. *Information Fusion* [Online], Vol. 1(1), page 17-33. Retrieved May 25, 2001 from http://www.sic.rma.ac.be/Publications/index.html

Visionic. (2000). *An overview of biometric technology* [Online]. Retrieved December 30, 2001 from Visionic Corporation: http://www.faceit.com/Newsroom/downloads.html