VIDEO-BASED FINGERPRINT VERIFICATION

Wei Qin, Yilong Yin, Chunxiao Ren, Lili Liu

Shandong University
School of Computer Science and Technology
Jinan, Shandong, China 250101

ABSTRACT

In this paper, fingerprint videos are used to improve the accuracy of a fingerprint verification system. We define the "inside-similarity" and "outside-similarity" to represent the similarity within a video and between two videos, respectively. A new method is proposed to define and calculate the matching score of two videos according to the similarity and the effect on the error probability of this method is analyzed theoretically. Experimental results confirm our arguments in the analysis and indicate that the proposed method can lead a much better performance than the method using a single impression. Therefore, we believe that video-based method is an effective approach to improve the accuracy of fingerprint system.

Index Terms— Fingerprint, Video, Fingerprint Verification, Similarity

1. INTRODUCTION

Fingerprint verification is a most popular and reliable biometric technique for automatic personal identification [1]. During the recent years, fingerprint verification has received more and more attention and been widely used in commercial applications. Despite the brilliant achievements it has made, its less than satisfactory accuracy is still a challenging problem which hindering its wide scale deployment.

To improve the accuracy of fingerprint systems, three aspects of work are undertaken. Firstly, researchers focus on improving the performance of one or more steps of automatic fingerprint verification system using a single impression. The steps include segmentation [2], enhancement [3], and matching [4], etc. Secondly, researchers try to use multiple sources of fingerprint to get a higher accuracy. These sources include multiple sensors [5], multiple features [6], multiple matchers [7], multiple fingers [7], multiple impressions of a same finger [7]. Thirdly, fingerprint together with other biometric traits

are considered to construct a more robust and effective biometric system [8]. Many industrious researchers' work within these three aspects can indeed access a better performance.

Dorai et al. [9, 10] have acquired fingerprint video while a finger is interacting with the sensor. Then they measure the distortions and dynamic behaviors from a video and also propose a new type of biometrics called the "resultant biometrics". This offers us an enlightenment that we can use videos for fingerprint verification to achieve a higher accuracy, which can be considered as a new idea different with the existing work.

With the advent of faster capture hardware and faster processors, newer systems can capture and exploit video signals for applications. There are two main advantages to use fingerprint videos for verification. Firstly, the user experience of capturing a video and sensing a single impression is completely the same. Secondly, a fingerprint video contains abundant information for verification. Therefore, investigating video-based fingerprint verification is a meaningful and interesting work.

In this paper, a new method is proposed to take advantage of fingerprint videos for a high accuracy. This method has been named Video Matching Score Calculation (VMSC), as it defines and calculates the matching score between fingerprint videos. The effect on error probability of this method will also be theoretically analyzed.

The rest of this paper is organized as follows: in section 2, a video-based method for fingerprint verification is proposed and its effectiveness is also illustrated in this section. Section 3 describes the experiment procedure and presents the experimental results. Finally, conclusions are given in section 4.

2. VIDEO-BASED METHOD FOR FINGERPRINT VERIFICATION

To use fingerprint videos for verification, we must define the similarity between two matching videos. The matching score is used to represent the similarity of two videos. There are two stages in our method: enrollment and verification. During the enrollment stage, fingerprint videos are captured and stored as templates. The "inside-similarity" of a video is calculated. During the verification stage, a new video is acquired

and compared to a stored template to verify the user's identity. In this stage, the "outside-similarity" is calculated and then the two kind of similarity are used to calculate the final matching score.

Before using a video, we have to preprocess it by eliminating adjacent frames with the same fingerprint foreground area and reserve only one of them. In the rest of this paper, when mentioning a video, we actually refer to the set of remaining frames left in the preprocessed video.

2.1. Inside and outside similarity

Suppose the set of frames in an enrolled fingerprint video is represented as

$$E = \{F_i^E | i = 1, 2, \ldots, n\} \tag{1}$$

where n is the number of the frames and F_i^E is the *ith* frame. After segmentation of a fingerprint frame, we can calculate the area of the fingerprint foreground by simply counting the number of pixels or blocks in this region. The frame with largest area of fingerprint foreground in E can be represented as F_{max}^E. In the enrollment stage, we can calculate the matching score $S_{i,j}^E$ of each pair of impressions F_i^E and F_j^E in the set E. Consequently there will be t such scores altogether, where $t = n * (n - 1)/2$. Then, their average score can be obtained by

$$\overline{S^E} = \frac{1}{t} \sum_{i=1}^{t-1} \sum_{j=i+1}^{t} S_{i,j}^E \tag{2}$$

We use S^E to represent the "inside-similarity". These computations are offline.

The set of frames in a claimed video is represented as

$$C = \{F_i^C | i = 1, 2, \ldots, k\} \tag{3}$$

Where k is the number of the frames and F_i^C is the *ith* frame. The frame with largest area of fingerprint foreground in the claimed video can be represented as F_{max}^C.

In the verification stage, for a pair of frames F_i^E and F_j^C from the sets E and C respectively, we can calculate their matching score $S_{i,j}$. Therefore, there will be r such scores, where $r = n * k$. Three strategies of score level fusion method can be adopted to use these r scores according to the quantity of the information being used:

● Strategy 1: all the n frames in the set E and the frame F_{max}^C in the set C are chosen for matching. So we can get n matching scores $S_{i,max}^1 (i = 1, 2, \ldots, n)$ and the final score $\overline{S^1}$ can be calculated by

$$\overline{S^1} = \frac{1}{n} \sum_{i=1}^{n} S_{i,max}^1 \tag{4}$$

● Strategy 2: we first follow the strategy 1 to get the n matching scores $S_{i,max}^1 (i = 1, 2, \ldots, n)$. Then the frame

F_{max}^E in the set E and all the k frames in the set C are chosen for matching and thus we get k matching scores $S_{max,j}^2 (j = 1, 2, \ldots, k)$. The final score $\overline{S^2}$ can be calculated by

$$\overline{S^2} = \frac{1}{n+k} (\sum_{i=1}^{n} S_{i,max}^1 + \sum_{j=1}^{k} S_{max,j}^2) \tag{5}$$

● Strategy 3: each frame from the set E is chosen to match against every frame in set C, so we can get $n*k$ matching scores $S_{i,j}^3 (i = 1, 2, \ldots, n; j = 1, 2, \ldots, k)$ and the final score $\overline{S^3}$ can be calculated by

$$\overline{S^3} = \frac{1}{n*k} \sum_{i=1}^{n} \sum_{j=1}^{k} S_{i,j}^3 \tag{6}$$

The final score of any strategy can be chosen to represent the "outside-similarity".

2.2. Proposed method

It's worth noting that all the impressions in a fingerprint video are homologous. So, the "inside-similarity" can be an approximate representation of the similarity between two homologous videos. The "outside-similarity", however, can represent the similarity between two matching videos that could either be homologous or be heterologous. We propose a method that uses the two kind of similarity to calculate the final matching score of two videos. The method has been named Video Matching Score Calculation (VMSC), as it defines and calculates the matching score between fingerprint videos.

Considering an enrolled fingerprint video V captured from an individual I, we can calculate $\overline{S^E}$ by formula (2) to represent the "inside-similarity" of V. Suppose $\overline{S_g^C}$ is the matching score between V and a genuine claimed video, then the mathematical expectation of $\overline{S^E}$ should be larger than that of $\overline{S_g^C}$ as there exist correlations in a fingerprint video.

Suppose V' is a claimed video and the matching score between V and V' is $\overline{S^C}$, which can be calculated by one of the three formulas (4-6). Let $\Delta S = \overline{S^C} - \overline{S^E}$, if $\Delta S \geq 0$, we argue that the larger ΔS is, the more V' is likely to be a genuine claimed video, relative to the "outside-similarity" represented by $\overline{S^C}$; if $\Delta S < 0$, we argue that the larger the absolute value ΔS is, the more V' is likely to be an impostor claimed video relative to the "outside-similarity". It's well known that for an impostor matching, the absolute value ΔS tends to be larger than a genuine matching. So, we propose to calculate the final matching score S as follows:

$$S = \overline{S^C} + f(\Delta S) = \overline{S^C} + f(\overline{S^C} - \overline{S^E}) \tag{7}$$

where $f(\bullet)$ is an increasing function. We can use the simplest form as follows:

$$S = \overline{S^C} + \omega * \Delta S = \overline{S^C} + \omega * (\overline{S^C} - \overline{S^E}) \tag{8}$$

where ω is the weight of ΔS and $\omega > 0$.

2.3. Effect of this method

We use $\overline{S_g^C}$ and S_g to replace $\overline{S^C}$ and S respectively if V' is genuine, and use $\overline{S_i^C}$ and S_i to replace if V' is an impostor. $E(\bullet)$ and $D(\bullet)$ are used to represent the mathematical expectation and variance, respectively. Then we can conclude that

$$E(\overline{S_i^C}) < E(\overline{S_g^C}) < E(\overline{S^E}) \qquad (9)$$

so,

$$E(\overline{S_i^C} - \overline{S^E}) = E(\overline{S_i^C}) - E(\overline{S^E})$$
$$< E(\overline{S_g^C}) - E(\overline{S^E}) = E(\overline{S_g^C} - \overline{S^E}) < 0 \qquad (10)$$

Further,

$$E(S_g) - E(S_i) = E(S_g - S_i)$$
$$= E\{[\overline{S_g^C} + \omega * (\overline{S_g^C} - \overline{S^E})] - [\overline{S_i^C} + \omega * (\overline{S_i^C} - \overline{S^E})]\}$$
$$= E(\overline{S_g^C} - \overline{S_i^C}) + \omega * \{E(\overline{S_g^C} - \overline{S^E}) - E(\overline{S_i^C} - \overline{S^E})\}$$
$$= (1 + \omega) * E(\overline{S_g^C} - \overline{S_i^C})$$
$$> E(\overline{S_g^C} - \overline{S_i^C}) = E(\overline{S_g^C}) - E(\overline{S_i^C}) \qquad (11)$$

and

$$D(S_g) = D(\overline{S_g^C} + \omega * (\overline{S_g^C} - \overline{S^E}))$$
$$= D\{(1 + \omega) * \overline{S_g^C} - \omega * \overline{S^E}\}$$
$$= (1 + \omega)^2 * D(\overline{S_g^C}) + \omega^2 * D(\overline{S^E}) > D(\overline{S_g^C}) \qquad (12)$$

where we note that $\overline{S_g^C}$ is independent of $\overline{S^E}$.

The proposed method enlarges the difference between the mathematical expectations of the genuine matching score and that of the impostor matching score, which is beneficial for reducing the error probability. But at the same time, the variances of both genuine matching score and impostor matching score become larger, which can lead a higher error probability. We argue that when ω is within a certain range, the expectation difference plays a leading role in changing the error rate and there must be a 'best' ω value that can minimize the error probability. The analysis is shown in Fig. 1.

3. EXPERIMENTAL RESULT

3.1. Database

We collected fingerprint videos from 50 individuals using an optical fingerprint capture device ($image\ size = 400 \times 400$, $frame\ rate = 25\ frames\ /\ sec$). The subjects mainly consisted of volunteers from the students and staff at Shandong University. All the subjects were not told the purpose of the capturing which guaranteed the capturing process of a video was the same as that of a single impression. This database was collected in two sessions, with an interval of one month. In each session, a subject was asked to provide 5 fingerprint
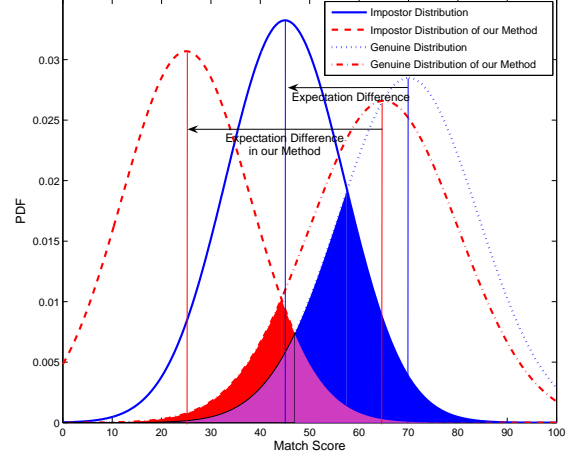

Fig. 1. The error rate will be reduced as the difference between the expectation of the genuine matching score and that of the impostor matching score is enlarged.

videos. Therefore, each person provided 10 videos and our database contained a total of 500 (50×10) videos. After preprocessing, the number of frames in a video is 9.6 on average. Six frames in a video are presented in Fig. 2.
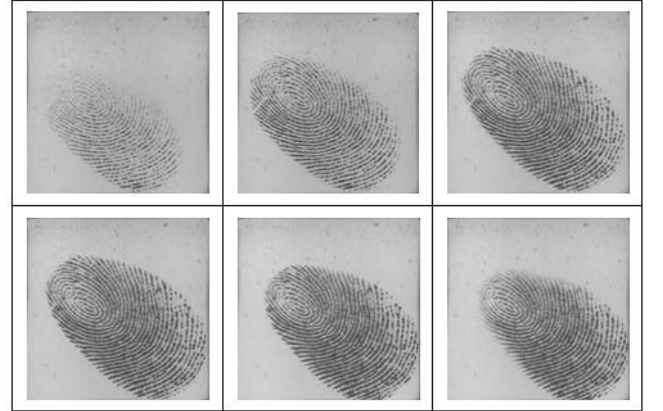

Fig. 2. Six frames in a fingerprint video.

3.2. Verification

For the 50×10 video sequences, there will be 2,250 genuine matchings. We select the 1st and 2nd videos of every subject for impostor matching and the number of matchings will be 2,450. So the total number of matchings is 4,700.

A minutiae-based matching method is used for completing one-on-one matching. For comparisons, the experiment using a single impression is also carried out. The impression with the largest area of fingerprint foreground in a video is chosen for single impression based matching. The receiver operating curves (ROC) depicting the performances of the

three strategies are shown in Fig. 3. The equal error rate (EER) of the strategy 1, 2 and 3 are 2.28%, 2.41% and 2.36%, respectively. We choose strategy 2 to represent the "outside-similarity" and use the average value of "inside-similarity" of both the enrolled and claimed videos.

Fig. 4 shows the ROC of single impression based method, strategy 2 and VMSC with four different ω values. From the ROC we can see when $\omega = 1$, the general performance of VMSC is best. With other ω values the performance get worse gradually, which verifies our argument. The EER of single impression based method, strategy 2 and VMSC with $\omega = 1$ are 3.02%, 2.41% and 1.24%, respectively.
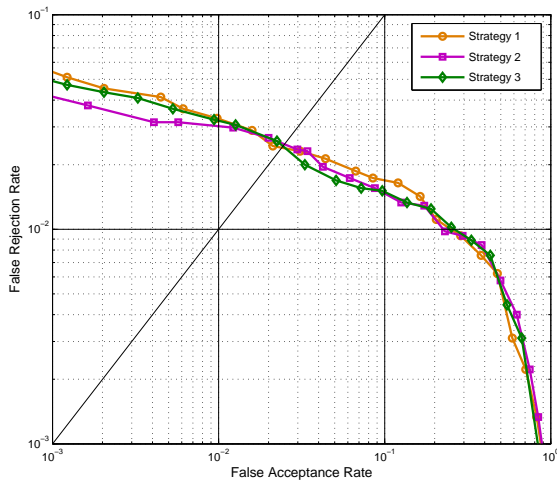

Fig. 4. ROC of single impression based method, strategy 2 and VMSC with four different ω values.

Fig. 3. ROC of the three strategies.

4. SUMMARY AND FUTURE WORK

In this paper, videos are used to improve the accuracy of a fingerprint verification system. The VMSC is proposed to define and calculate the matching score between two fingerprint videos and the effect on the error probability of this method is analyzed theoretically. Experimental results indicate that VMSC can get a higher accuracy than the single impression based fingerprint system. Therefore, we can conclude that the video-based method is a new aspect of the approaches that can improve the accuracy of fingerprint systems.

The future work will involve investigating the correlations within a video, improving the final score calculating method and try the feature level fusion strategy.

5. REFERENCES

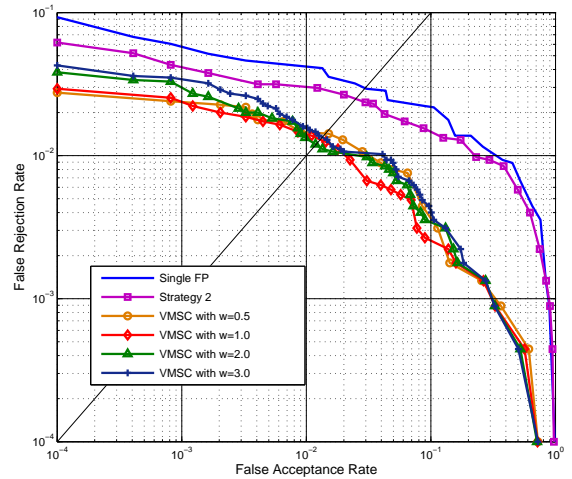[1] A.K. Jain, "Biometric recognition: Q & A," *Nature*, vol. 449, pp. 38–40, 2007.

[2] E. Zhu, J. Yin, C. Hu, and G. Zhang, "A systematic method for fingerprint ridge orientation estimation and image segmentation," *Pattern Recognition*, vol. 39, pp. 1452–1472, 2006.

[3] L. Hong, Y. Wan, and A.K. Jain, "Fingerprint image enhancement: Algorithms and performance evaluation," *IEEE Trans. PAMI*, vol. 20, pp. 777–789, 1998.

[4] X. Zheng, Y. Wang, and X. Zhao, "A robust matching method for distorted fingerprints," *Proc. ICIP*, vol. 2, pp. 377–380, 2007.

[5] G.L. Marcialis and F. Roli, "Fingerprint verification by fusion of optical and capacitive sensors," *Pattern Recognition Letters*, vol. 25, pp. 1315–1322, 2004.

[6] A.K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based fingerprint matching," *IEEE Trans. Image Process*, vol. 9, pp. 846–859, 2000.

[7] S. Parbhakar and A.K. Jain, "Decision-level fusion in fingerprint verification," *Pattern Recognition*, vol. 35, pp. 861–874, 2002.

[8] L. Hong, A.k. Jain, and S. Pankanti, "Can multibiometrics improve performance?," *Proc. AutoID*, vol. 2, pp. 59–64, 1999.

[9] C. Dorai, N. Ratha, and R. Bolle, "Detecting dynamic behavior in compressed fingerprint videos: Distortion," *Proc. CVPR*, vol. 2, pp. 320–326, 2000.

[10] C. Dorai, N. Ratha, and R. Bolle, "Dynamic behavior analysis in compressed fingerprint videos," *IEEE Trans. Circuits and Systems for Video Technology*, vol. 14, pp. 58–73, 2004.