MVA2002 IAPR Workshop on Machine Vision Applications, Dec. 11 - 13, 2002, Nara - ken New Public Hall, Nara, Japan

3—21

Fingerprint Identification Using the Accidental Coincidence Probability

Akira Monden [†] and Seiji Yoshimoto [‡]
Multimedia Research Laboratories, NEC Corporation

Abstract

A method of comparing and identifying two patterns is proposed based on the accidental coincidence probability of the patterns' features. The probability is calculated under the assumption that there is no correlation between the patterns. This approach makes it possible to overcome the difficult problem of estimating the probabilities of features missing and spurious features occurring. Applying this method to fingerprint identification, we show that it can be used to control the probability of imposter acceptance. Therefore, this method is suitable for security applications.

1 Introduction

In this paper, we propose a method of identify two patterns to be identical. This method employs the accidental coincidence probability of the patterns' features. The probability is calculated under the assumption that the patterns have no correlation.

If we start from the hypothesis that two patterns are the same, there are some problems to overcome. Under this hypothesis, the similarity is estimated from the observed probability distribution of the features. The probability distribution of the individual features should be known in advance. If there are missing features or there are spurious features, there will be no one-to-one correspondence between the two sets of features. In such a case, it is necessary but difficult, in general, to estimate the probabilities that some features are missing and that spurious features have appeared. The proposed method makes it possible to overcome this difficulty in estimating such probabilities.

Here, we apply the method to fingerprint identification. We show that our proposed criterion enables the identification of two fingerprints with the required false match rate.

A fingerprint is a pattern of ridges and valleys on a fingertip. It can be used for personal identification because of the pattern's uniqueness and invariance. Recently, fingerprint identification technologies have found broad application not only in criminal investigation, but also in fields such as e-commerce, network access, and security checkpoints. A fingerprint can be identified by comparing its minutiae, which include ridge endings and bifurcations[1, 2]. In this paper, the methods of comparing and identifying two fingerprints are discussed under the assumption that the candidates for the corresponding minutiae have already been detected. Many kinds of features are associated with minutiae, such as the direction or curvature of contacting or adjoining ridges, the number of ridges between minutiae, and so on. In the following discussion, for simplicity we only consider the positions of the minutiae.

Pankanti, et al.[3] addressed the boundaries of minutia-based fingerprint identification. It is impossible to completely avoid imposter acceptance, in which a fingerprint from a different finger is determined to be identical. A fingerprint is recognized as identical if a given measure, like similarity, is greater than a threshold. The threshold should be set so that the false match rate is lower than the required level. In the general approach to fingerprint identification, however, there is no theoretical relationship between the criterion and the imposter acceptance rate. Therefore, it is necessary to determine the threshold experimentally. The probability that some imposter fingers are accepted may be larger than the required level, even if, on average, the imposter acceptance probability is sufficiently small. Because our proposed method uses the probability that fingerprints with no correlation are accidentally matched, there is a strong relationship between the measure we use and the imposter acceptance rate. Therefore, it is possible to evaluate the false match rate theoretically, rather than experimentally.

2 Difficulties in Fingerprint Identification

Because of finger deformation, the positions of minutiae change whenever fingerprints are acquired with a live scanner or similar device. They may also change during the process of feature extraction. Thus, there will be position gaps between corresponding minutiae if two fingerprints overlap. These positional errors between corresponding minutiae are distributed as a normal distribution with a mean of 0. Figure 1 shows $P(X)$: the distribution of the positional differences in corresponding minutiae extracted from mated fingerprints in the NIST14 database (500 dpi)[6]. The graph shows that $P(X)$ (the solid line) is similar to a normal distribution with a mean of 0 and standard deviation of 8.2 (the dashed line).

[†] Address: Miyazaki 4-1-1, Miyamaeku, Kawasaki Kanagawa 216-8555 Japan. E-mail: a-modnen@bk.jp.nec.com

[‡] E-mail: s-yoshimoto@bq.jp.nec.com

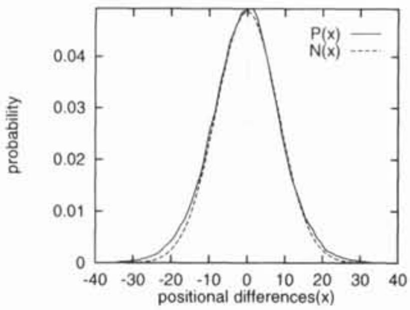

Figure 1: Distribution of positional differences in minutiae (measured in units of pixels, where the resolution is 500 dpi)

Consider the case of determining that fingerprint A and fingerprint B are the same. Suppose M pairs of corresponding minutiae are found, and the differences in their positions are $e_i(i = 1 \cdots M)$. The event X represents such a state. The probability that event X occurs in comparing the same finger is denoted as $P(X|A = B)$. If the differences for each pair are independent, $P(X|A = B)$ can be represented by

$$P(X|A = B) = \prod_{i=1}^{M} P(e_i). \tag{1}$$

Based on the Bayesian theorem, the posterior probability that $A = B$ when X occurs can be represented by

$$P(A = B|X) = \frac{P(X|A = B) \cdot P(A = B)}{P(X)}, \tag{2}$$

where $P(A = B)$ is the probability that fingerprints A and B originate from the same finger. Suppose that there is no distinction between the occurrences of each finger. Then, $P(A = B)$ is equal for each finger. Suppose as well that each event X occurs with the same probability. Then, $P(X)$ is the same for each event X. Therefore, as $P(X|A = B)$ becomes higher, so does $P(A = B|X)$, which is the probability that fingerprints A and B come from the same finger when event X occurs. As a result, it is possible to conclude that fingerprints A and B are the same if $P(X|A = B)$ is high.

Poor-quality fingerprint images and incorrect ridge structures detected during the process of feature extraction may cause some minutiae to be missing or spurious minutia to be detected. Because of these possibilities, there are, in general, no one-to-one correspondences between two sets of minutiae. In these cases, it is necessary to estimate the probabilities that some minutiae have disappeared and that spurious minutiae have appeared. These probabilities depend on the feature extraction process. Moreover, it is difficult to determine that for a minutia that does not correspond with any other minutia, the corresponding minutia is missing or spurious. Ignoring these probabilities, in Equation 1 the calculated value obviously decreases as the number of corresponding minutiae increases. This is not a desirable behavior for determining similarity.

3 Accidental Coincidence Probability

As mentioned in section 2, it is difficult to calculate the probability that some minutiae are missing or that spurious minutiae have appeared. To overcome this difficulty, the methods of identifying fingerprints were proposed in previous works[4, 5]. These methods employ the accidental coincidence probability. In this paper, we propose a modified method to control the imposter acceptance rate. The same equation we use here was derived by Pankanti, et al. from the viewpoint of the individuality of fingerprints[3].

Our proposed method starts from the hypothesis that two fingerprints originate from different fingers. The accidental coincidence probability is thus calculated under the assumption that the fingerprints have no correlation. If this probability is small enough, the hypothesis is rejected, and we conclude that the two fingerprints come from the same finger.

The accidental coincidence probability is calculated as follows. Let C be a sub-region of fingerprint A, which is common with that of another fingerprint B. Let S be the area of region C. We assume that fingerprints A and B are reasonably aligned. Fingerprint A contains N_1 minutiae in region C and fingerprint B contains N_2 minutiae in region C. Suppose there are M corresponding minutia pairs between of the two fingerprints. Minutiae a_i of fingerprint A and b_j of fingerprint B are considered a corresponding minutia pair if and only if the positional difference between a_i and b_j is smaller than a threshold E. Given that fingerprints A and B have no correlation, we assume that the N_1 minutiae of fingerprint A are randomly distributed in region C (as shown in Figure 2).

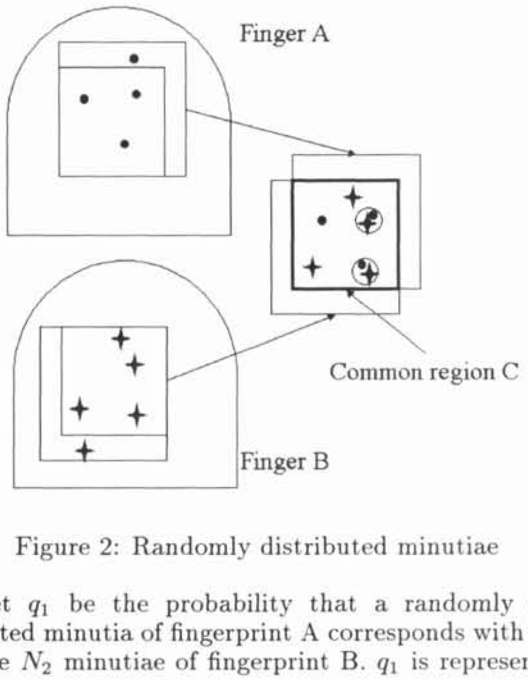

Figure 2: Randomly distributed minutiae

Let q_1 be the probability that a randomly distributed minutia of fingerprint A corresponds with one of the N_2 minutiae of fingerprint B. q_1 is represented by

$$q_1 = \frac{m \cdot \pi E^2}{S}. \tag{3}$$

Suppose that $(i - 1)$ minutiae of fingerprint A are arranged at random in region C and all of them correspond with minutiae of fingerprint B. The area of the region in which they are not distributed is $(S-(i-1)T)$, so the number of minutiae of fingerprint B that do not correspond with any randomly distributed minutiae in region C is $(N_2-(i-1))$. After the $(i-1)$ minutiae are distributed, we randomly place an i-th minutia in the region. Let q_i be the probability that the i-th minutia corresponds to one of the $(N_2-(i-1))$ minutiae. q_i is represented by

$$q_i = \frac{(m-i)\cdot\pi E^2}{S-(i-1)\cdot\pi E^2}(i=1\cdots M). \qquad (4)$$

As the number of corresponding minutia pairs is M, the $(M+1)$-th minutia does not correspond to any minutiae of fingerprint B. Let r_1 be the probability that the $(M+1)$-th randomly distributed minutia does not correspond to any minutia of fingerprint B. r_1 is given by

$$r_1 = \frac{S-\pi E^2\cdot N_2}{S-M\cdot\pi E^2}, \qquad (5)$$

assuming that the minutiae of fingerprint B are sparse and the tolerance area of a minutia does not overlap that of another minutia. Let r_i be the probability that the $(M+i)$-th minutia is randomly distributed somewhere in the rest of region C and does not correspond to any minutia of fingerprint B. In the same way, r_i is given by

$$r_i = \frac{S-\pi E^2\cdot(N_2+i)}{S-(M+i)\cdot\pi E^2}. \qquad (6)$$

Q_M is the probability that N_1 minutiae are randomly distributed in region C and M minutiae correspond to minutiae of fingerprint B. The number of cases in which M corresponding minutiae can be selected from the N_1 minutiae of fingerprint A is represented as ${}_{N_1}C_M$. Thus, Q_M is given by

$$Q_M = {}_{N_1}C_M\cdot\prod_{i=1}^{M}\cdot q_i\cdot\prod_{i=1}^{N_1-M} r_i, \qquad (7)$$

assuming that the minutiae of fingerprint A are sparse, and that the probability that two randomly distributed minutiae correspond to the same minutia of fingerprint B is small enough to be ignored. Q is the probability that more than M minutiae correspond with the N_2 minutiae of fingerprint B, assuming that the N_1 minutiae of fingerprint A are randomly distributed in region C. Q is given by

$$Q = \sum_{m=M}^{N_1} {}_{N_1}C_m\cdot\prod_{i=1}^{m}\cdot q_i\cdot\prod_{i=1}^{N_1-m} r_i. \qquad (8)$$

If Q is small enough, the hypothesis that fingerprint A and fingerprint B have no correlation is rejected. Therefore, we can conclude that fingerprints A and B originate from the same finger.

As mentioned above, this method estimates the effects of missing and spurious minutiae by considering corresponding minutiae to be distributed randomly. Therefore, with this method we can avoid calculating the probability that minutiae are missing or that spurious minutiae have appeared.

4 Experimental Results

In this section, we present our experimental results, demonstrating that the proposed method controls the imposter acceptance rate. Figure 3 shows the distribution function of the accidental coincidence probability for imposter fingerprint pairs. The minutiae were extracted from fingerprint images in the NIST 14 database. The images were cut to 300 × 300 pixels. The solid line in Figure 3 shows the distribution function of Q, the measure used in the proposed method. The dashed line shows that the value of the distribution function is equal to our measure. Because Q is defined as the accidental coincidence probability, it represents the probability of a false match. Thus, the threshold for sufficiently small Q can be determined based on the security level required for the application.

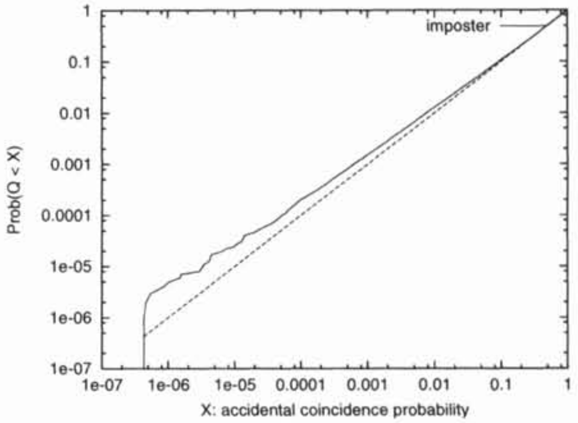

Figure 3: Distribution function of the proposed measure for imposter fingerprint pairs

Figure 4 shows the distribution functions of the proposed measure for fingerprints containing few (10 ~ 40) minutiae (solid line) and many (40 ~ 80) minutiae (dashed line). The figure shows that the distribution function of the measure is not related to the number of minutiae. If the threshold for identification is set experimentally, each fingerprint may have various imposter acceptance rates. For example, consider a system that recognizes fingerprints based on the number of corresponding minutiae. A fingerprint containing many minutiae may be matched more often with an imposter fingerprint than one containing few minutiae. The security level may be lower than the required level for some fingerprints, even if the required level is achieved on average. Because the measure Q in the proposed method is the probability of accidental coincidence, and it gives the distribution function, all fingerprints should have the same security level for false matches.

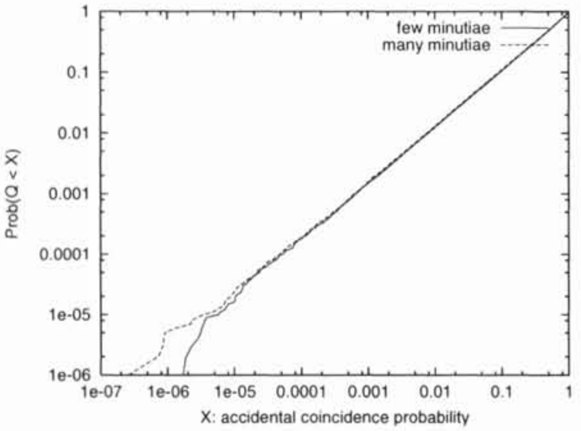

Figure 4: Distribution functions of the proposed measure for the cases of few and many minutiae

Figure 5 shows the distribution function of the proposed measure when applied to 1000 genuine fingerprint pairs from the NIST 14 database. The images were again cut to 300 × 300 pixels. The positions of the fingerprints were reasonably aligned, and their deformations were corrected to make them overlap with their corresponding fingerprints. Comparing Figure 3 and Figure 5 demonstrates that the range of the proposed measure for the genuine fingerprints and that for the imposter fingerprints have little overlap. Therefore, this measure can enable us to determine whether a fingerprint pair under comparison is genuine or not.

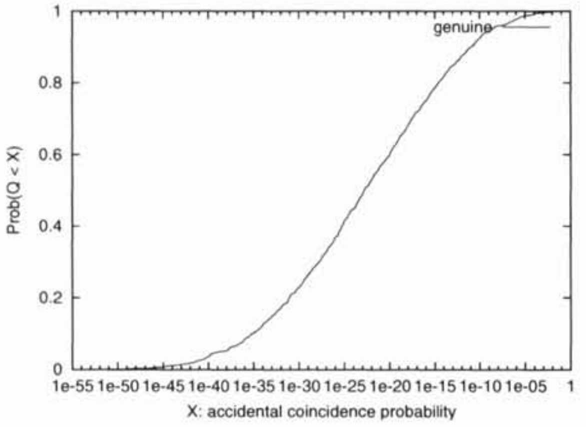

Figure 5: Distribution function of the proposed measure for genuine fingerprint pairs

5 Conclusion

We have proposed a method of identifying two patterns as identical, which makes it possible to avoid the difficult problem of estimating the probabilities of features missing and spurious features occurring. This method also controls the imposter acceptance rate. It employs the probability that two patterns' features coincide accidentally under the assumption that they have no correlation. Experimental results using actual fingerprints showed that the proposed method makes it possible to estimate the imposter acceptance rate theoretically. If the security level is estimated experimentally, it may not be satisfied for some fingerprints, even if the level is achieved on average. Because this method can be used to control the imposter acceptance rate theoretically, it is suitable for security applications.

References

[1] A. Jain, L. Hong and R. Bolle, "On-Line Fingerprint Verification," IEEE Trans. Pattern Anal. Mach. Intell., Vol. 19, No. 4, Apr. 1997.

[2] K. Asai, Y. Hoshino and K. Kiji, "Automated Fingerprint Identification by Minutia-Network Feature — Matching Processes —," IEICE Trans. Inf. & Syst.(Japanese Edition), Vol. J72-D-II, No. 5, pp. 733-740, May 1989. (in Japanese)

[3] S. Pankanti, S. Prabhakar and A. K. Jain, "On the Individuality of Fingerprints," IEEE Trans. Pattern Anal. Mach. Intell., Vol. 24, No. 8, pp. 1010-1025, August 2002.

[4] A. Monden and S. Yoshimoto, "Fingerprint Verification Method Using Unrelated Probability Model," Proc. IEICE-ESS Conf. IEICE '2001, p. 178, Sep 2001. (in Japanese)

[5] A. Monden and S. Yoshimoto, "Similarity Based on Probability that Two Fingers Have No Correlation," IEICE Technical Report, PRMU 2001-161, pp. 53-58, Dec 2001. (in Japanese)

[6] NIST Special Database 14, NIST Mated Fingerprint Card Pairs 2(MFCP2), Advanced System Division, Computer System Laboratory, Nat'l Inst. Standards and Technology, 1993.