A Minutiae-based Fingerprint Individuality Model

Jiansheng Chen Yiu-Sang Moon
Department of Computer Science and Engineering,
The Chinese University of Hong Kong, Shatin N.T., Hong Kong
{jschen, ysmoon}@cse.cuhk.edu.hk

Abstract

Fingerprint individuality study deals with the crucial problem of the discriminative power of fingerprints for recognizing people. In this paper, we present a novel fingerprint individuality model based on minutiae, the most commonly used fingerprint feature. The probability of the false correspondence among fingerprints from different fingers is calculated by combining the distinctiveness of the spatial locations and directions of the minutiae. To validate our model, experiments were performed using different fingerprint databases. The matching score distribution predicted by our model actually fits the observed experimental results satisfactorily. Comparing to most previous fingerprint individuality models, our model makes more reasonably conservative estimate of the fingerprint discriminative power, making it a powerful tool for studying the fingerprint individuality as well as the performance evaluation of fingerprint verification systems.

1. Introduction

Fingerprint based personal authentication has been extensively used in security applications such as access control, e-commerce and surveillance. The wide social acceptance of the fingerprint in personal authentication mainly comes from its more than one hundred years of successful usage in forensic applications for recognizing people, although nowadays many fingerprint systems are used in daily lives beyond criminal domain. The basic foundation for using fingerprints is the three biological principles of universality, persistence and uniqueness that fingerprints are believed to follow [1]. The universality and persistence principles have been established by empirical observations as well as the anatomy and morphogenesis of friction ridge skin [2]. Nevertheless, challenges to the principle of uniqueness, or the fingerprint individuality, have never stopped [3].

In essence, fingerprint individuality refers to the distinctiveness of fingerprints originated from different fingertips. It is true that when examined at a very high level of details, two fingerprints from distinct fingertips will be different. However, considering the possible ambiguities and noises that could be introduced during fingerprint capturing, two fingerprints are usually declared to originate from the same fingertip if they are 'sufficiently' similar, as is practiced by most human fingerprint experts and automatic fingerprint authentication systems. Hence, the fingerprint individuality problem can be formulated as the answer to the following question: given two fingerprints from two different fingers, determine the probability that they are 'sufficiently' similar [3]. Galton is believed to be the first one who studied the fingerprint individuality problem [4]. After that, many models have been proposed for describing the fingerprint individuality [5, 6, 7]. Fingerprint individuality models have both theoretical and practical significances. Their critical role in legalizing fingerprint identification as an expert scientific testimony in lawsuits has been elaborated in [7]. In [8], a fingerprint individuality model is adopted as the foundation of a statistical evaluation model for fingerprint verification systems. Most existing fingerprint individuality models focus on fingerprint representations based on the minutia, which is defined as one of the various ways that the fingerprint ridge becomes discontinuous [3]. In this paper, we will propose a new minutiae-based fingerprint individuality model whose foundation is several simple assumptions on fingerprint minutiae properties. To validate our model, we have tested it through extensive experiments using different fingerprint databases and show that it is able to provide a satisfactory estimate on the discriminative power of fingerprints.

This paper is organized as follows. Section 2 introduces some major previous studies on the fingerprint individuality. A discussion on fingerprint minutiae properties is given in Section 3. In Section 4, we present our fingerprint individuality model. Experiments validating our model are explained and discussed in Section 5. The last section is a conclusion of our work.

1-4244-1180-7/07/$25.00 ©2007 IEEE

2. Background

A common practice in the fingerprint individuality study is to examine the distinctiveness of certain features of fingerprints so that the distinctiveness of whole fingerprints can be evaluated by combining all these features. Many fingerprint features have been used in previous fingerprint individuality studies. In his groundbreaking work in [4], Galton used ridge configurations and fingerprint types as features. He claimed that the probability of the occurrence of a certain fingerprint pattern equals *1.45e-11*.

In [5], Trauring computed that the probability of the existence of N minutia correspondences between two fingerprints from different fingers is 0.1944^N. The features Trauring used are minutiae types, locations and orientations. Stoney and Thornton studied the probabilities of occurrences of various types of minutiae, their orientations, number of neighboring minutiae and distances or ridge counts to the neighboring minutiae [6]. A sample calculation of the probability of the false matching of an N minutia fingerprint using a rudimental version of Stoney's model was given in [7] as $N*0.6*(0.5e\text{-}3)^{(N-1)}/5$. More recently, Pankanti et al. built a fingerprint individuality model by considering minutiae locations, number and directions [7]. By additionally assuming that fingerprint minutiae cannot be too close to each other, Pankanti et al. divided a fingerprint into cells containing no more than one minutia each so that the probability of minutia correspondence can be expressed using a hypergeometric distribution. Suppose that two fingerprints contain m and n minutiae respectively, then the probability that they have exactly q minutiae correspondences can be expressed by

$$P_{match} = \sum_{\rho=q}^{\min(m,n)} \left(\frac{\binom{m}{\rho} * \binom{M-m}{n-\rho}}{\binom{M}{n}} * \binom{\rho}{q} * l^q * (1-l)^{\rho-q} \right) \quad (1)$$

, in which M is the number of cells and l is the probability that two minutiae can be matched by their directions [7].

In [9], Zhu et al. addressed the fingerprint individuality problem in a different way. They created a stochastic model for fingerprint minutiae patterns. Fingerprint individuality under certain parameter settings were numerically estimated by performing fingerprint imposter matching experiments on the synthetic minutiae patterns generated from the model. Although Zhu et al. have not derived an explicit mathematic expression for fingerprint individuality, they did verify through matching experiments that Pankanti's model tends to significantly overestimate the discriminative power of fingerprints. Actually, Pankanti et al. have already revealed this problem of their model through empirical experiments in their own work [7]. A more thorough survey on fingerprint individuality studies can be found in [3].

As we can see, minutiae-based representations are most widely used in the fingerprint individuality study. This is natural since the minutia is believed to be the most discriminating and reliable fingerprint feature, and is used in almost all fingerprint authentication applications [3]. Generally speaking, more fingerprint features will lead to a higher estimate of the fingerprint discriminative power. However, a practical concern is that introducing more fingerprint features will increase the complexity of a fingerprint individuality model, especially when the correlations among these features are not negligible. What is more, some fingerprint features are not practically usable in automatic fingerprint authentication systems. One typical example is that the fingerprint type usually cannot be discriminated automatically with a high level of accuracy [7] and thus is not considered in most fingerprint authentication systems. Moreover, it is a common practice in fingerprint individuality studies to make conservative estimate of fingerprint discriminative power. Sclove explained how conservative estimates could benefit suspects in a criminal investigation by allowing them to doubt the certainty level of the fingerprint matching [10]. Therefore, we only use the minutiae number, locations and directions as features in our fingerprint individuality model. We will investigate the statistical properties of minutiae locations and directions in the following section.

3. Fingerprint minutiae properties

A fingerprint is the image of the finger tip epidermis. The most important and evident structural characteristics of fingerprint images are the ridges and valleys, which interleave with each other. Minutiae are spots of special local ridge patterns where ridges become discontinuous. The most commonly used attributes of a fingerprint minutia are its spatial location and its direction [3]. Most common fingerprint matching algorithms treat a fingerprint as a minutiae point pattern; and the fingerprint matching is performed using point pattern matching techniques.

The spatial distribution of fingerprint minutiae has been studied in [10, 11, 12]. It is believed that the fingerprint minutiae spatial distribution slightly deviates from a uniform distribution, or CSR (Complete Spatial Randomness). The specific way of the deviation is actually decided by the scale of the observation [12]. Nevertheless, the deviation has been proved to be so slight that by ignoring it in fingerprint individuality studies, as was practiced in [5, 7], the estimate of the fingerprint discriminative power will not be biased significantly.

Besides the location, another commonly used attribute for minutiae matching is the minutia direction ($0\sim2\pi$) which is defined according to the orientation ($0\sim\pi$) of the ridge along which the minutia resides; and the specific way the ridge becomes discontinuous [3]. Since fingerprint

ridges flow smoothly with very slow orientation changes, the directions of neighboring minutiae are strongly correlated. At the same time, fingerprint ridges follow certain global pattern determined by the fingerprint type so that the minutiae directions are not independent of the minutiae locations [7]. To model this dependency, let us study the statistical distribution of the direction difference in the imposter fingerprint matching, in which the two matching fingerprints come from different fingers. Suppose the directions of two minutiae are θ_1 and θ_2 respectively. Their direction difference can be defined by Equation (2) [3]. Hence, the value of θ_d ranges from *0* to π.

$$\theta_d = \min\left(\left|\theta_1 - \theta_2\right|, 2\pi - \left|\theta_1 - \theta_2\right|\right) \quad (2)$$

Jain suggested using the von-Mises distribution to model the probability distribution of θ_d [13]. To meet the data range requirement of the von-Mises distribution, we let $\theta_{2d}=2\theta_d$ and study the distribution of θ_{2d} instead. The data range of θ_{2d} is *[0, 2π)*. We performed a one-to-one imposter matching experiment [3] on all the *800* fingerprints in FVC2002 DB1_A [14] to get the empirical probability distribution of θ_{2d}. The parameters of the von-Mises distribution can then be estimated by calculating the circular variance of the empirical distribution. Equation (3) shows the estimated probability density function of the von-Mises distribution, where $I_0(\bullet)$ is a modified Bessel function of the first kind with order *0*. Figure 1 compares the empirical distribution to the estimated von-Mises distribution. The value of θ_{2d} apparently concentrates near *0* and 2π, indicating that two minutiae close in spatial locations tend to have similar orientations even if the two minutiae are actually from two different fingerprints.

$$P_\theta\left(\theta_{2d}\right) = \exp\left(-1.69 * \cos\left(\theta_{2d} - \pi\right)\right) \Big/ 2\pi I_0\left(-1.69\right) \quad (3)$$

We can also observe that the von-Mises distribution fits the empirical distribution quite well when $\theta_{2d} \leq 2\pi/3$, or $\theta_d \leq \pi/3$. This is promising considering the minutiae direction difference tolerances used in most common minutiae matching algorithms are smaller than $\pi/3$.

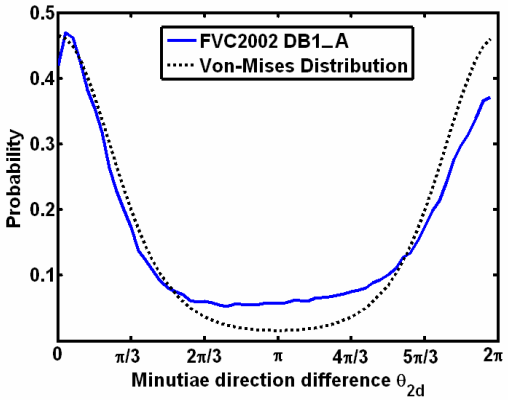


Figure 1. Modeling the minutiae direction difference distribution in imposter matching using the von-Mises distribution.

4. CSR based fingerprint individuality model

Based on the observations on the fingerprint minutiae properties described in the last section, we propose a fingerprint individuality model with the following assumptions.

- Fingerprint minutiae are used as features. Only two minutia types, terminations and bifurcations, are considered because the occurrence of other minutiae types is relatively rare [3]. Also, terminations and bifurcations are treated equally.
- When only the spatial location is considered, fingerprint minutiae form CSR patterns. In other words, fingerprint minutiae are uniformly distributed.
- Minutiae directions are not independent of their locations. This dependency can be modeled by a von-Mises distribution defined by Equation (3).
- Fingerprint image quality is not taken into account and there is one and only one 'correct' alignment between two fingerprints. In most pre-alignment based fingerprint matching algorithms, core points or delta points are used as references [3]. The overlapping area of the two fingerprints for matching equals A.
- Minutiae locations and directions are used for fingerprint matching. Two minutiae from two different fingerprints are matched if and only if the following three conditions are all fulfilled.
  1) The Euclidean distance between these two minutiae is smaller than or equal to d_0.
  2) The direction difference between these two minutiae is smaller than or equal to θ_0.
  3) One minutia cannot be matched more than once.
- The number of matched minutiae pairs, or minutiae correspondences, is directly used as the similarity measurement, or the matching score.

Quantitatively, the fingerprint individuality problem can be rephrased as a mathematical problem: given two fingerprints from different fingertips, what is the probability P_{match} that they have a given number q of minutiae correspondences? First we will examine the probability P_{SL} that the two fingerprints have ρ minutiae correspondences when only locations are used for the minutiae matching.

For convenience, we name one of the fingerprints the 'master fingerprint' and the other the 'live fingerprint'. Assume that the master fingerprint contains m minutiae and the live fingerprint contains n minutiae. Given a master fingerprint minutia p_i and a live fingerprint minutia q_j, the probability that the Euclidean distance between p_i and q_j is

smaller than or equal to d_0 is $\pi d_0^2/A$. As illustrated in Figure 2(a), this is exactly the probability that q_j falls into the disc centered at p_i with radius d_0 under the CSR assumption in our model. Let $C=1-\pi d_0^2/A$, which is the probability that q_j cannot be matched to p_i by its location. Therefore, the probability that p_i can be matched to at least one of the n live fingerprint minutiae becomes $1-C^n$. If p_i is matched to a live fingerprint minutia, then both p_i and the live fingerprint minutia will not be considered for any succeeding correspondences. Under the CSR assumption, removal of any single minutia will not affect the distribution of other minutiae. However, the order of the problem will be decremented by one when a minutia pair is removed so that a recursive relationship can be achieved as shown in Equation (4). To the right of the equation sign, the first term corresponds to the situation that the current master fingerprint minutia is matched and the second term is for the non-match case.

$$P_{SL}(m,n,\rho)=(1-C^n)P_{SL}(m-1,n-1,\rho-1)+C^nP_{SL}(m-1,n,\rho) \quad (4)$$

Equation (4) is a first-order linear homogeneous difference equation with three variables. In general, such a difference equation is difficult to solve and might have more than one solution. Nevertheless, according to the physical meaning of P_{SL}, we have two extra initial conditions as expressed by Equations (5) and (6). Equation (5) can be interpreted intuitively as: if the number of minutiae in any of the two fingerprints is smaller than ρ, then the probability of having ρ correspondences is definitely zero. Also, since the probability that a master fingerprint minutia fails to be matched to any live fingerprint minutia is C^n, the probability that none of the m master fingerprint minutiae can be matched is C^{mn} as expressed by Equation (6).

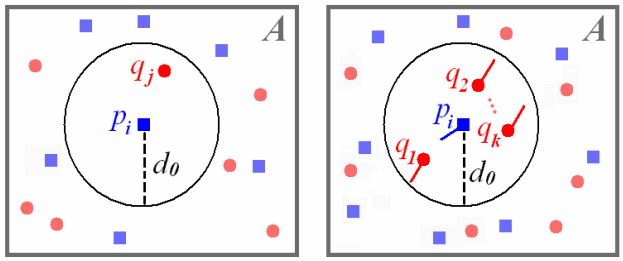
$$P_{SL}(m,n,\rho)=0, \quad (m<\rho \quad or \quad n<\rho) \quad (5)$$

$$P_{SL}(m,n,\rho)=C^{mn}, \quad (\rho=0) \quad (6)$$

A divide-and-conquer strategy is employed by us to solve Equation (4). First, we solve the simple cases when $\rho=1$ and $\rho=2$. Then we conjecture the possible form of the solution and apply the mathematical induction to prove our conjecture. For any $\rho>0$, the solution can be shown as:

$$P_{SL}(m,n,\rho)=\frac{C^{(m-\rho)(n-\rho)}\prod_{i=0}^{\rho-1}\left\{\left(1-C^{m-i}\right)\left(1-C^{n-i}\right)\right\}}{\prod_{i=1}^{\rho}\left(1-C^i\right)} \quad (7).$$

Next, we will consider both locations and directions for minutiae matching and deduce P_{match}. Suppose in a particular matching scenario, a master fingerprint minutia p_i can be matched to k live fingerprint minutiae $q_1, q_2, \ldots, q_k$ by their spatial locations. If there is at least one live fingerprint minutia q_j ($j \in [1, k]$) exists so that the direction difference between p_i and q_j is smaller than or equal to θ_0, then p_i and q_j can be matched. Since minutiae $q_1, q_2, \ldots, q_k$ come from the same fingerprint and are close to each other in terms of spatial locations, their directions are strongly correlated as explained in the last section. More specifically, they share approximately the same orientation, say equals Θ_q. Let the orientation of p_i be Θ_p. Similar to Equation (2), the orientation difference between minutiae can be defined as $\Theta_d=min(|\Theta_p-\Theta_q|, \pi-|\Theta_p-\Theta_q|)$. According to the symmetric property of Equation (3) as well as the circular nature of angles, the probability that Θ_d is smaller than or equal to θ_0 is 2γ, in which $\gamma=\int_0^{2\theta_0}P_\theta(x)dx$. However, only orientation matching alone is not enough. As illustrated in Figure 2(b), p_i will probably be matched to q_1, but can never be matched to q_2 and q_k. The chance that the direction difference between a live fingerprint minutia q_j ($j \in [1, k]$) and p_i is smaller than or equal to θ_0, given $\Theta_d \le \theta_0$, equals $1/2$. Therefore, the probability that p_i can be matched by the direction to at least one q_j ($j \in [1, k]$) is $2\gamma*(1-1/2^k)$.



(a) (b)

Figure 2. Illustration of minutiae matching. (a) minutiae matching by locations; (b) minutiae matching by both locations and directions.

From previous discussions, we know that $(1-C)$ is the probability that a live fingerprint minutia is within distance d_0 from p_i. Hence, the probability that there are exactly k minutiae located within distance d_0 from p_i should be $\binom{n}{k}*(1-C)^k*C^{n-k}$. By adding up these probability values for all the possible values of k, we have Equation (8), which is in fact the probability that a master fingerprint minutia can be matched to at least one live fingerprint minutia by both the location and the direction. Equation (8) can be simplified to Equation (9).

$$\eta(n,\gamma)=\sum_{k=1}^{n}\left\{\binom{n}{k}*(1-C)^k*C^{n-k}*2\gamma*\left(1-1/2^k\right)\right\} \quad (8)$$

$$\eta(n,\gamma)=2\gamma*\left(1-(1+C)^n/2^n\right) \quad (9)$$

In consequence, the term C^n in the difference equation (4) should now be replaced by $(1-\eta(n,\gamma))$ for the deduction of P_{match} instead of P_{SL}. Unfortunately, the outcome is a prohibitively complicated difference equation. As an alternative, we consider the conditional probability τ that a master fingerprint minutia can be matched by the direction given that it has already been matched by the location. According to the above discussions, we have $\tau(n,\gamma)=\eta(n,\gamma)/(1-C^n)$. It is not difficult to prove that $\tau(n,\gamma)$ is a monotonic increasing function of n. During the matching process, with the removal of matched live fingerprint minutiae, the value of τ decreases. The value of τ reaches its maximum when no live fingerprint minutiae have been removed, or $\tau_{max}=\tau(n,\gamma)$. Considering that the number of matched minutiae is generally small in an imposter matching, we use τ_{max} for a conservative estimate of fingerprint individuality (higher estimate of the number of minutiae correspondences). Thus, a conservative estimate of the probability that there are exactly q minutiae correspondences considering both minutiae locations and directions can be expressed by Equation (10). The right-hand side of Equation (10) is basically the summation of the probabilities of all the possible cases where exactly q minutiae pairs can be matched.

$$P_{match}(m,n,q)=\sum_{\rho=q}^{\min(m,n)}\left\{P_{SL}(m,n,\rho)*\binom{\rho}{q}*\tau_{\max}^{q}*(1-\tau_{\max})^{1-q}\right\} \tag{10}$$

Till now, we have presented our CSR based fingerprint individuality model. In the next section, we will validate this model by performing imposter matching experiments on several different fingerprint databases.

5. Experiments and discussions

Equations (7) and (10) are the two major outputs of our fingerprint individuality model. We tested the validity of these two equations by comparing the imposter matching score probability distribution deduced from these two equations with the corresponding empirical values calculated from one-to-one imposter matching experiments on different fingerprint databases.

$$I_{SL}(q)=\sum_{m=q}^{+\infty}\sum_{n=q}^{+\infty}\left(poiss(m,\lambda_0 A)*poiss(n,\lambda_0 A)*P_{SL}(m,n,q)\right) \tag{11}$$

First, we validate Equation (7). According to the CSR assumption, the number of minutiae in a given area follows a Poisson distribution. Therefore, the theoretical imposter matching score distribution under our model when only spatial locations are used for minutiae matching can be expressed by Equation (11), in which $poiss(\bullet)$ is the probability function of the Poisson distribution and λ_0 denotes the fingerprint minutiae density. The infinity signs in Equation (11) are only theoretically meaningful. Practically, when m or n gets fairly big, the corresponding value of the Poisson probability function will become extremely small and thus can be ignored. In our experiments, we chose $4\lambda_0 A$ as the common upper-limit for both m and n.

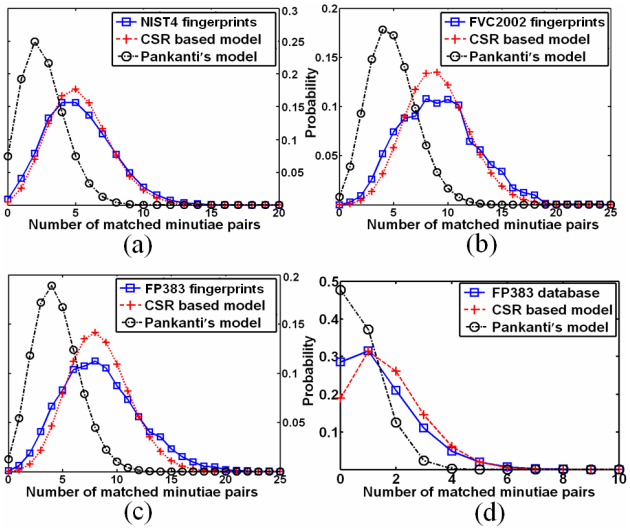


Figure 3. Imposter matching score probability distributions under the CSR based fingerprint individuality model compared to the empirical results on three databases. The corresponding distributions predicted by Pankanti's model are also shown for comparison. (a)-(c): only minutiae locations are considered for matching. (d): both minutiae locations and directions are considered for minutiae matching.

To get the corresponding empirical imposter matching score probability distribution, we carefully selected 113 fingerprints from the NIST4 database (512×512; ~500dpi) [15], 56 fingerprints from FVC2002 DB1 (388×374; 500dpi) [14], and 103 fingerprints from FP383 (256×256; 450dpi), a fingerprint database reported in [16]. In particular, all the selected fingerprints are from different fingers. To ensure that enough fingerprint minutiae could be extracted reliably, only fingerprints with high image quality and large ROI (Region of Interest) were selected. These fingerprints were first normalized to 500dpi. Then the minutiae positions of each fingerprint were manually marked by human experts. A square area of 220×220 pixel^2 was selected inside the ROI of each fingerprint. One-to-one matching experiments were performed on these square minutiae patterns. Only minutiae locations were considered for matching and $d_0=15$pixels. The experimental results are shown in Figure 3(a)-(c). The value of λ_0 for each database was calculated by averaging the minutiae number of all the selected fingerprints for that database. It can be seen that the imposter matching score probability distributions predicted by our model is close to the corresponding empirical results for most of the cases on all the three

fingerprint databases. While for Pankanti's model, the underestimate of imposter matching score, or overestimate of fingerprint individuality is obvious. Figure 3(a)-(c) do reveal that for relatively large number of matched minutiae pairs, or high matching scores, our model also slightly underestimates the probability, which is basically caused by the ignoring of the minutiae clustering tendency [12]. This issue is not the focus of this paper and will not be further discussed.

For validating Equation (10), we performed a different experiment. Still, the imposter matching score probability distribution was investigated and one-to-one matching was performed. The difference is that the whole FP383 database (1149 fingerprints from 383 users) was employed instead of selected high quality fingerprints. A minutiae-based fingerprint verification system proposed in [17] was applied to FP383 for minutiae extraction and matching. The matching module of this system was modified to behave exactly as described in our individuality model assumptions. Both locations and directions were used for minutiae matching and we set d_0 and θ_0 to *15*pixels and $\pi/8$ respectively. We further modified the matching module so that only minutiae whose distances from the core point lie between *77* pixels and *17* pixels inclusively are considered for matching. Thus, the area of the circular region between the two radii is $\pi*(77^2-16^2)\approx 17{,}000 pixel^2=A$.

The imposter matching score probability distribution reported by the fingerprint verification system is compared to the theoretical value under our fingerprint individuality model in Figure 3(d). The theoretical value was calculated by substituting all the occurrences of P_{SL} with P_{match} in Equation (11). It is natural that the matching score in Figure 3(d) is generally much lower than that in Figure 3(a)-(c), since the requirement on direction matching filters out many minutiae pairs which can be matched by their locations. Figure 3(d) indicates a satisfactory predicting power of our CSR based fingerprint individuality model. Still, Pankanti's model underestimates the matching scores. It should be emphasized here that FP383 consists of real life fingerprint images, indicating inevitable inaccuracy in minutiae extraction. Nevertheless, Figure 3(d) demonstrates the effectiveness of our model on noisy real life data.

We have listed some typical values of the fingerprint correspondence probability P_{match} predicted by different minutiae-based fingerprint individuality models in Table 1. We let $W=1/(1-C)$, where C is the probability value in our model used in Equations (4)–(9). For *500*dpi fingerprint images, the relationship between W and M, which is the number of cells in Pankanti's model, can be explicitly expressed by Equation (12). Still, $d_0=15$pixels and $\theta_0=\pi/8$.

$$W = 18.2 * M / \pi d_0 \qquad (12)$$

Among all the models, Trauring's model [5] makes the most conservative estimate of fingerprint individuality and is probably far too conservative. The fingerprint correspondence probability predicted by Stoney's model is obviously lower than the other models. This is due to the complicated fingerprint features used by Stoney as introduced in Section 2. Pankanti's model and our CSR based model are somewhat in the middle. This is not surprising since the same fingerprint features are used in these two models. Comparatively, our model gives more realistic estimates so that it might be a possible candidate for solving the problem of overestimating fingerprint discriminative power by Pankanti's model as revealed by the experiments reported in [7] and [9]. As mentioned before, Zhu et al. have not derived any explicit mathematic formula for calculating the minutiae correspondence probability from their stochastic model for minutiae patterns. Therefore, to compare Zhu's results with ours, we quote the experimental result for a specific case reported in [9] in the last row of Table 1. This is the only experimental case in [9] of which the parameters necessary for a fair probability calculation using other models are provided. Our theoretical result and Zhu's experimental result are of the same order of magnitude and are both orders of magnitude higher compared to that of Pankanti's model. It is not surprising that Zhu's result is larger than ours since non-linear deformation of fingerprints is allowed in the matching algorithm used in [9], leading to a higher probability of minutiae correspondences.

Table 1. Fingerprint correspondence probability predicted by different fingerprint individuality models.

(m, n, q) ;W, M	*CSR*	*Pankanti [7]*	*Stoney [6]*	*Trauring [5]*	*Zhu [9]*
(26, 26, 26) ;40.2, 104	5.0e-29	5.3e-40	9.3e-83	3.2e-19	--
(26, 26, 12) ;40.2, 104	3.8e-5	3.9e-9	--	--	--
(36, 36, 36) ;68.0, 176	2.3e-43	5.5e-59	1.3e-115	2.5e-26	--
(36, 36, 12) ;68.0, 176	4.1e-4	6.1e-8	--	--	--
(12, 12, 12) ;27.0, 70	**2.7e-15**	**1.2e-20**	**7.0e-37**	**2.9e-9**	--
(17, 17, 12) ;40.6, 105	**2.3e-10**	2.4e-15	--	--	**6.8e-10**

The last but one row of Table 1 corresponds to the famous 12-point guideline in forensic science. This guideline says that assuming an expert can correctly glean all the minutiae in a latent fingerprint, a 12-point match with the full-print master template can be considered as a sufficient evidence of fingerprint matching [3]. The values

listed in the second to the fifth columns of this row can be seen as the 'error rates' of this guideline under different individuality models. The value of *2.7e-15* predicted by our model is much larger than the value of *1.2e-20* under Pankanti's model. Nevertheless, both *1.2e-20* and *2.7e-15* are extremely small values so that such a 12-point match can be regarded as providing an overwhelming amount of evidence for the fingerprint correspondence in both models, considering the fact that there are now less than ten billion (*1e10*) people living on this planet.

For some other cases, the conclusions drawn from our model and Pankanti's model might be opposite. For example, the fifth row in Table 1 reflects the certainty level of a 12-point match out of 36 minutiae. Under Pankanti's model, such a fingerprint correspondence case might be considered as a quite reliable one (error rate = *6.1e-8*). However, our model tends to doubt the certainty of such a matching case (error rate = *4.1e-4*). One important reason why our model gives more realistic estimates on fingerprint individuality than Pankanti's model is that compared to Pankanti et al., we have made less assumptions on fingerprint minutiae properties.

6. Conclusions

In the proposed fingerprint individuality model, starting from several simple assumptions about the spatial location and direction distributions of fingerprint minutiae, we have deduced formulas describing the false correspondence probability of fingerprints. In our deduction, some approximations are made to drive our model towards a slightly conservative estimate of the fingerprint discriminative power. The model has also been validated using fingerprint data sourced from several different fingerprint databases. We demonstrate that the imposter matching score probability distribution predicted by our model can fit the corresponding empirical results calculated from one-to-one matching experiments quite satisfactorily. Compared to other previous fingerprint individuality models, our model is able to make more reasonably conservative estimates of fingerprint discriminative power. Thus, our model might be considered as a possible solution for solving the discrepancies between experimental results and theoretical predictions revealed in previous fingerprint individuality studies.

For the future work, it would be interesting to incorporate the clustering tendency of fingerprint minutiae spatial distribution into our model so as to eliminate the problem of underestimating fingerprint correspondence probability for the relatively high matching scores as revealed in Figure 3. Finally, we expect our fingerprint individuality model will be useful in enhancing the research in performance evaluation of automatic fingerprint verification systems as is practiced in [8].

Acknowledgements

This work was supported by the Hong Kong Research Grants Council Project 415106, "A Statistical Evaluation Model for Minutiae-based Automatic Fingerprint Verification Systems".

References

[1] A. Moenssnens, *Fingerprint Techniques*, Chilton, London, 1971.

[2] H.C. Lee and R.E. Gaensslen, *Advances in Fingerprint Technology*, New York: Elsevier, 1991.

[3] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer. 2003.

[4] F. Galton, *Finger Prints*, McMillan, London, 1892.

[5] M. Trauring, "Automatic Comparison of Finger-Ridge Patterns", Nature, pp. 938-940, 1963.

[6] D.A. Stoney and J.I. Thornton, "A Critical Analysis of Quantitative Fingerprint Individuality Models", J. Forensic Sciences, vol. 31, no. 4, pp. 1187-1216, Oct. 1986.

[7] S. Pankanti, S. Prabhakar, and A.K. Jain, "On the Individuality of Fingerprints", IEEE Trans. on Pattern Analysis and Machine Intelligence, vol.24, no. 8, pp. 1010-1025, 2002.

[8] J.S. Chen and Y.S. Moon, "A Statistical Evaluation Model for Minutiae-based Automatic Fingerprint Verification Systems", Proceedings of International Conference on Biometrics, pp. 236-243, Jan. 2006.

[9] Y. Zhu, S.C. Dass and A.K. Jain, "Compound Stochastic Models for Fingerprint Individuality", Proceedings of International Conference on Pattern Recognition, vol. 3, pp. 532-535, Aug. 2006.

[10] S.L. Sclove, "The Occurrence of Fingerprint Characteristics as a Two Dimensional Process", J. of American Statistical Association, vol. 74, no. 367, pp. 588-595, 1979.

[11] D.A. Stoney, "Distribution of Epidermal Ridge Minutiae", American J. of Physical Anthropology, vol. 77, pp. 367-376, 1988.

[12] J.S. Chen, Y.S. Moon, "A Statistical Study on the Fingerprint Minutiae Distribution", Proceeding of IEEE International Conference on Acoustics, Speech, and Signal Processing, pp. II169-II172, May 2006.

[13] A.K. Jain, "On the Uniqueness of Fingerprints", NAS Sackler Forensic Science Colloquium, Washington, DC, Nov. 18, 2005.

[14] Second International Competition for Fingerprint Verification Algorithms, http://bias.csr.unibo.it/fvc2002/.

[15] NIST 8-Bit Gray Scale Images of Fingerprint Image Groups (FIGS), http://www.nist.gov/srd/nistsd4.htm.

[16] K.C. Chan, Y.S. Moon, and P.S. Cheng, "Fast Fingerprint Verification Using Sub-regions of Fingerprint Images", IEEE Trans. On Circuits and Systems for Video Technology, pp. 95-101, vol. 14, issue 1, Jan. 2004.

[17] H.W. Yeung, Y.S. Moon, J.S. Chen, F. Chan, Y.M. Ng, and H.S.Chung, "A Comprehensive and Real-time Fingerprint Verification System for Embedded Devices", Proceedings of SPIE 5779, pp. 438-446, Mar. 2005.