On the Individuality of Fingerprints

Sharath Pankanti, *Senior Member*, *IEEE*, Salil Prabhakar, *Member*, *IEEE*, and Anil K. Jain, *Fellow*, *IEEE*

Abstract—Fingerprint identification is based on two basic premises: 1) persistence: the basic characteristics of fingerprints do not change with time and 2) individuality: the fingerprint is unique to an individual. The validity of the first premise has been established by the anatomy and morphogenesis of friction ridge skin. While the second premise has been generally accepted to be true based on empirical results, the underlying scientific basis of fingerprint individuality has not been formally established. As a result, the validity of fingerprint evidence is now being challenged in several court cases. A scientific basis for establishing fingerprint individuality will not only result in the admissibility of fingerprint identification in the courts of law, but will also establish an upper bound on the performance of an automatic fingerprint verification system. We address the problem of fingerprint individuality by quantifying the amount of information available in minutiae features to establish a correspondence between two fingerprint images. We derive an expression which estimates the probability of a false correspondence between minutiae-based representations from two arbitrary fingerprints belonging to different fingers. For example, the probability that a fingerprint with 36 minutiae points will share 12 minutiae points with another arbitrarily chosen fingerprint with 36 minutiae points is 6.10×10^{-8}. These probability estimates are compared with typical fingerprint matcher accuracy results. Our results show that 1) contrary to the popular belief, fingerprint matching is not infallible and leads to some false associations, 2) while there is an overwhelming amount of discriminatory information present in the fingerprints, the strength of the evidence degrades drastically with noise in the sensed fingerprint images, 3) the performance of the state-of-the-art automatic fingerprint matchers is not even close to the theoretical limit, and 4) because automatic fingerprint verification systems based on minutia use only a part of the discriminatory information present in the fingerprints, it may be desirable to explore additional complementary representations of fingerprints for automatic matching.

Index Terms—Fingerprints, individuality, identification, minutiae, probability of correspondence, biometric authentication.

1 Introduction

Fingerprint-based personal identification is routinely used in forensic laboratories and identification units around the world [1] and it has been accepted in the courts of law for nearly a century [2]. Until recently, the testimony of latent fingerprint examiners was admitted in courts without much scrutiny and challenges. However, in the 1993 case of Daubert vs. Merrell Dow Pharmaceuticals, Inc. [3], the US Supreme Court ruled that the reliability of an expert scientific testimony must be established. Additionally, the Court stated that when assessing reliability, the following five factors should be considered:

1. whether the particular technique or methodology in question has been subject to a statistical hypothesis testing,
2. whether its error rate has been established,
3. whether the standards controlling the technique's operations exist and have been maintained,
4. whether it has been peer reviewed and published, and
5. whether it has a general widespread acceptance.

Subsequently, handwriting identification was challenged under *Daubert* (it was claimed that handwriting identification does not meet the scientific evidence criteria established in the Daubert case) in several cases between the years 1995 and 2001. For a recent empirical study on the individuality of handwriting, see [4].

Several courts have now ruled that handwriting identification does not meet the *Daubert* criteria. Fingerprint identification was first challenged by the defense lawyers under *Daubert* in the 1999 case of USA vs. Byron Mitchell [5] on the basis that the fundamental premise of fingerprint *uniqueness* has not been objectively tested and the potential error rate in fingerprint matching is unknown. The defense motion to exclude fingerprint evidence and testimony was denied. The outcome of the USA vs. Byron Mitchell case is still pending. Fingerprint identification has been challenged under *Daubert* in more than 20 court cases to date since the USA vs. Byron Mitchell case in 1999. More recently, a federal court judge has ruled that, without the credible (peer-reviewed) published estimates of matcher accuracies, fingerprint experts cannot testify with certainty whether two fingerprint impressions originated from the same finger [6].

The two fundamental premises on which fingerprint identification is based are: 1) Fingerprint details are permanent and 2) fingerprints of an individual are unique. The validity of the first premise has been established by empirical observations as well as based on the anatomy and morphogenesis of friction ridge skin. It is the second premise which is being challenged in recent court cases. The notion of fingerprint individuality has been widely

- *S. Pankanti is with the IBM T.J. Watson Research Center, Yorktown Heights, NY 10598. E-mail: sharat@watson.ibm.com.*
- *S. Prabhakar is with DigitalPersona Inc., 805 Veterans Blvd., #301, Redwood City, CA 94063. E-mail: salilp@digitalpersona.com.*
- *A.K. Jain is with the Department of Computer Science and Engineering, Michigan State University, East Lansing, MI 48824. E-mail: jain@cse.msu.edu.*

Manuscript received 10 Oct. 2001; revised 22 Jan. 2002; accepted 12 Feb. 2002.
Recommended for acceptance by M. Pietikainen.
For information on obtaining reprints of this article, please send e-mail to: tpami@computer.org, and reference IEEECS Log Number 115168.

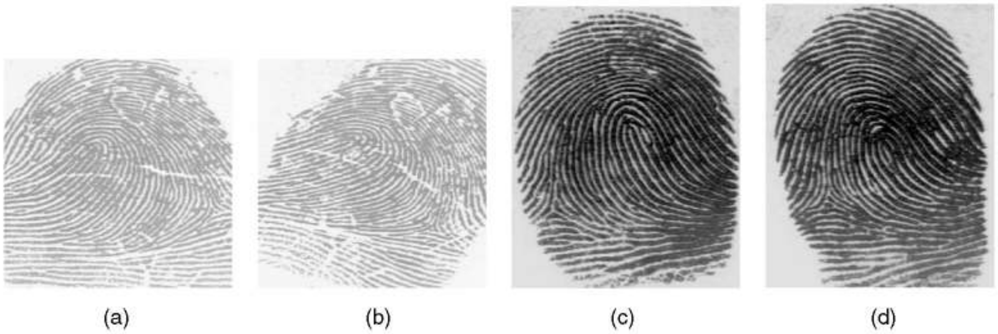


Fig. 1. Two fingerprint impressions ((a) and (b)) from the same finger may look significantly different (large intraclass variation); impressions ((c) and (d)) from different fingers may look similar to an untrained eye (small interclass variation). The fingerprint similarity metric must be designed such that impressions from the same finger are recognized as similar without erroneously associating impressions from different fingers with each other.

accepted based on a manual inspection (by experts) of millions of fingerprints. However, the underlying scientific basis of fingerprint individuality has not been rigorously studied or tested. In March 2000, the US Department of Justice admitted that no such testing has been done and acknowledged the need for such a study [7]. In response to this, the National Institute of Justice issued a formal solicitation for "Forensic Friction Ridge (Fingerprint) Examination Validation Studies" whose goal was to conduct "basic research to determine the scientific validity of individuality in friction ridge examination based on measurement of features, quantification, and statistical analysis" [7]. The two main topics of basic research under this solicitation included: 1) measure the amount of detail in a single fingerprint that is available for comparison and 2) measure the amount of detail in correspondence between two fingerprints.

What do we mean by fingerprint individuality [8]? If two fingerprints originating from two different fingers are examined at a very high level of detail (resolution), we may find that the fingerprints are indeed different. However, most human experts and automatic fingerprint identification systems (AFIS) declare that the fingerprints originate from the same source if they are "sufficiently" similar. How similar should the two fingerprints be before we can claim that they are from the same finger? This notion of similarity depends on the typical (intraclass) variations observed in the multiple impressions of a finger (See, Fig. 1). The fingerprint individuality problem can be formulated in many different ways, depending on which one of the following aspects of the problem is under examination: 1) The individuality problem may be cast as determining the probability that any two or more individuals may have sufficiently similar fingerprints in a given target population, 2) given a sample fingerprint, determine the probability of finding a sufficiently similar fingerprint in a target population, and 3) given two fingerprints from two different fingers, determine the probability that they are sufficiently similar. In this study, we solve for formulation 3 as solutions to formulations 1 and 2 can be derived from the solution to formulation 3 [9].

Our interest in the fingerprint individuality problem is twofold. First, a scientific basis (a reliable statistical estimate of the matching error) for fingerprint comparison can determine the admissibility of fingerprint identification in courts of law as evidence of identity. Secondly, it can establish an upper bound on the performance of automatic fingerprint verification systems. Here, we develop a fingerprint individuality model that attempts to estimate the probability of a false correspondence. We use this model to establish an upper bound on the performance of a fingerprint verification system [10].

In order to solve the individuality problem, we need to first define a priori the representation of fingerprint (*pattern*) and the metric for the similarity. Fingerprints can be represented by a large number of features, including the overall ridge flow pattern, ridge frequency, location and position of singular points (core(s) and delta(s)), type, direction, and location of minutiae points, ridge counts between pairs of minutiae, and location of pores (see Fig. 2). All these features contribute to fingerprint individuality. In this study, we have chosen minutiae representation of the fingerprints because it is utilized by forensic experts, it has been demonstrated to be relatively stable, and it has been adopted by most of the commercially available automatic fingerprint matching systems. Note that forensic experts use several other features in addition to minutiae when matching fingerprints. However, our adoption of minutiae feature is supported by the fact

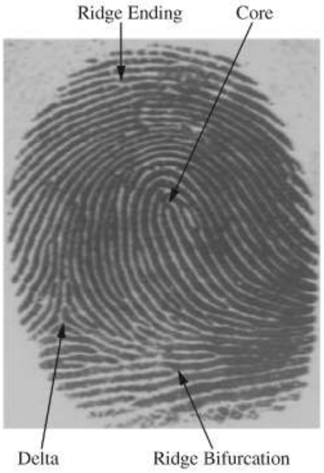


Fig. 2. A fingerprint image of type "right loop." The overall ridge structure, core, delta, a ridge ending, and a ridge bifurcation are marked.

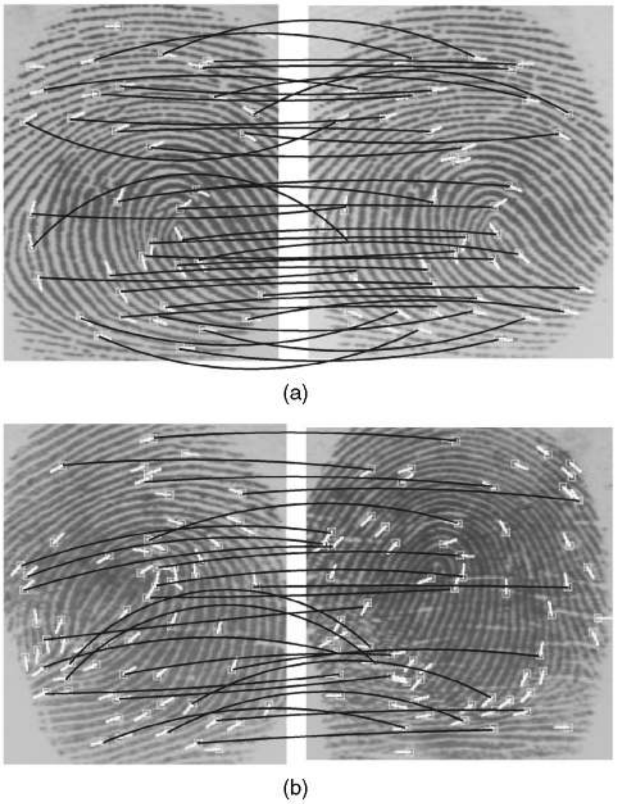


Fig. 3. Automatic minutiae matching. (a) Two impressions of the same finger are matched; 39 minutiae were detected in input (left), 42 in template (right), and 36 "true" correspondences were found. (b) Two different fingers are matched; 64 minutiae were detected in input (left), 65 in template (right), and 25 "false" correspondences were found.

that most of the automatic fingerprint matching systems are based on minutiae information alone (see Fig. 3). Our formulation can be extended to include other fingerprint representations as well.

Given a representation scheme and a similarity metric, there are two approaches for determining the individuality of the fingerprints. In the empirical approach, *representative* samples of fingerprints are collected and, using a *typical* fingerprint matcher, the accuracy of the matcher on the samples provides an indication of the uniqueness of the fingerprint with respect to the matcher. There are known problems (and costs) associated with collection of the *representative* samples. Additionally, even if a large database of fingerprints such as the FBI database, which contains over 200 million fingerprints [11], is used for an empirical evaluation of the fingerprint individuality, it would take approximately 127 years to match all the fingerprints in the database with each other using a processor with a speed of one million matches per second! In a theoretical approach to individuality estimation, one models all realistic phenomena affecting interclass and intraclass fingerprint pattern variations. Given the similarity metric, one could then theoretically estimate the probability of a false correspondence. Theoretical approaches are often limited by the extent to which the assumed model conforms to the reality. Here, we propose a fingerprint individuality model based on a number of parameters derived from a database of fingerprint images. We also juxtapose the probabilities obtained from our individuality model with the empirical results obtained using a state-of-the-art automatic fingerprint matcher.

The total number of degrees-of-freedom of the pattern space (e.g., minutiae configuration space) does not directly relate to the discriminability of the different patterns (e.g., minutiae from different fingers). The effective estimation of discriminatory information can only be achieved by taking into account intrapattern variations [12]. There are several sources of variability in the multiple impressions of a finger [10]: nonuniform contact (with the sensor), irreproducible contact, inconsistent contact, and imaging artifacts. This variability in multiple impressions of a finger manifests itself into 1) detection of spurious minutiae or missing genuine minutiae, 2) displacement/disorientation (also called deformation) of the genuine minutiae, and 3) transformation of the type of minutiae (connective ambiguity). This entails designing a similarity metric (matcher) that accommodates these intraclass variations. As a result, the probability of the false correspondence increases significantly.

Most of the earlier approaches to fingerprint individuality did not explicitly account for these (intraclass) variabilities into their models (see [13] for a critical review of several models) and, therefore, overestimated the fingerprint individuality (gave a smaller probability of false correspondence). Since most of the existing models of individuality do not address the problems associated with occurrence of spurious minutiae or missing genuine minutiae, they do not provide a systematic framework to address issues related to a partial representational match between two fingerprints (e.g., what is the probability of finding seven matched minutiae in two fingerprints with 18 and 37 minutiae, respectively?). This is very important in an automatic fingerprint matching system (feature extraction algorithms are not as accurate as a well-trained fingerprint expert in detecting minutiae) and in matching *latents* (where a print depicting a small portion of a finger is matched against a print depicting the full finger). Although, in a manual fingerprint matching procedure, the likelihood of *detecting* false minutiae is significantly smaller than that in an automatic system, the prints imaged from different portions of a finger may give rise to variability in the number of detected minutiae. Our approach not only explicitly models the situation of partial representational match, but also incorporates constraints on the configuration space due to intrapattern variations (e.g., number of minutia, minutia position/orientation, image area) based on empirical estimates derived from the ground truth data marked on fingerprints obtained in a realistic environment.

The rest of the paper is organized as follows: Section 2 presents a summary of major fingerprint individuality studies and compares the probability of a fingerprint configuration obtained by different models. Section 3 presents the proposed fingerprint individuality model and Section 4 presents the results. Summary and discussions are presented in Section 5.

TABLE 1
Fingerprint Features Used in Different Individuality Models

Author	Fingerprint features
Galton (1892)	ridges, minutiae types
Pcarson (1930)	ridgcs, minutiac typcs
Hcnry (1900)	minutiac locations, typcs, corc-to-dclta ridgc count
Balthazard (1911)	minutiae locations, two types, and two directions
Bose (1917)	minutiae locations and three types
Wentworth & Wilder (1918)	minutiae locations
Cummins & Midlo (1943)	minutiae locations and types, core-to-delta ridge count
Gupta (1968)	minutiac locations and typcs, fingcrprint typcs, ridgc count
Roxburgh (1933)	minutiae locations, two minutiae types, two orientations, fingerprint and core types, number of positionings, area, fingerprint quality
Amy (1948)	minutiae locations, number, types, and orientation
Trauring (1963)	minutiae locations, two types, and two orientations
Kingston (1964)	minutiae locations, number, and types
Osterburg et al. (1977)	minutiae locations and types
Stoney & Thornton (1986)	minutiae locations, distribution, orientation, and types, variation among prints from the same source, ridge counts, and number of alignments

2 Background

The early fingerprint individuality studies typically focused on minutiae-based representations; some studies explicitly factored in fingerprint class (e.g., right loop, left loop, whorl, arch, tented arch, etc.) information. The type, direction, and location of minutiae were the most commonly used features in these individuality studies. See Table 1 for a comparison of the features used in fingerprint individuality models. The types of minutiae used varies from one study to other: Some studies used two minutia types (ending and bifurcation), whereas others used as many as 13 types of events (e.g., empty cell, ridge ending, ridge fork, island, dot, broken ridge, bridge, spur, enclosure, delta, double fork, trifurcation, and multiple events) [14]. Later models considered additional features (e.g., ridge counts [13], sweat pores [15]) to determine the probability of occurrence of a particular fingerprint configuration.

Most of the early individuality studies examined the *distinctiveness* of a portion/feature of the fingerprint. Under simplifying assumptions (e.g., implicit assumptions about statistical independence of events and that the corresponding event distributions are identical), these studies estimated the distinctiveness of the entire fingerprint (total pattern variation) by collating the distinctiveness in the features extracted from fingerprints (total feature variation). We will refer to these total pattern variation-based fingerprint individuality estimates as the *probability of fingerprint configuration*. A summary of these studies is presented below.

The fingerprint individuality problem was first addressed by Galton in 1892 [16], who considered a square region spanning six-ridges in a given fingerprint. He assumed that, on average, a full fingerprint can be covered by 24 such six-ridge wide independent square regions. Galton estimated that he could correctly reconstruct any of the regions with a probability of $\frac{1}{2}$ by looking at the surrounding ridges. Accordingly, the probability of a specific fingerprint configuration, given the surrounding ridges, is $\left(\frac{1}{2}\right)^{24}$. He multiplied this conditional (on surrounding ridges) probability with the probability of finding the surrounding ridges to obtain the probability of occurrence of a fingerprint as

$$P(\text{Fingerprint Configuration}) = \frac{1}{16} \times \frac{1}{256} \times \left(\frac{1}{2}\right)^{24} = 1.45 \times 10^{-11}, \qquad (1)$$

where $\frac{1}{16}$ is the probability of occurrence of a specific fingerprint type (such as arch, tented arch, left loop, right loop, double loop, whorl, etc.) and $\frac{1}{256}$ is the probability of occurrence of the correct number of ridges entering and exiting each of the 24 regions. Equation (1) gives the probability that a particular fingerprint configuration in an average size fingerprint (containing 24 regions defined by Galton) will be observed in nature. Roxburgh [17], Pearson [18], and Kingston [19] objected to Galton's assumption that the probability of occurrence of any particular ridge configuration in a six-ridge square is $\frac{1}{2}$ and claimed that (1) grossly underestimates the fingerprint individuality (i.e., overestimates the probability of occurrence). Pearson [18] argued that there could be 36 (6×6) possible minutiae locations within one of Galton's six-ridge-square regions, leading to a probability of occurrence of a particular fingerprint configuration of

$$P(\text{Fingerprint Configuration}) = \frac{1}{16} \times \frac{1}{256} \times \left(\frac{1}{36}\right)^{24} = 1.09 \times 10^{-41}. \quad (2)$$

A number of subsequent models (Henry [20], Balthazard [21] (cf. [13]), Bose (cf. [13]), Wentworth and Wilder [22], Cummins and Midlo [23], and Gupta [24]) are interrelated and are based on a fixed probability, p, for the occurrence of a minutia. They compute the probability of a particular N-minutiae fingerprint configuration as

$$P(\text{Fingerprint Configuration}) = p^N. \quad (3)$$

In the following, we provide the values of p used in these studies. In most cases, the authors do not present any details on how they arrived at their choice of p. Henry [20] chose $p = \frac{1}{4}$ and added 2 to the number of minutiae, N, if the fingerprint type and core-to-delta ridge count could be determined from the given (latent) fingerprint. Balthazard [21], (cf. [13]) also set $p = \frac{1}{4}$ under the assumption that there are four types of equally likely minutiae events:

1. fork (bifurcation) to the right,
2. fork to the left,
3. ending to the right, and
4. ending to the left.

Bose (cf. [13]) adopted $p = \frac{1}{4}$, under the assumption that there are four possibilities in each square region of one ridge-interval width in a fingerprint:

1. a dot,
2. a fork,
3. an ending, and
4. a continuous ridge.

Wentworth and Wilder [22] chose $\frac{1}{50}$ as the value of p. Cummins and Midlo [23] adopted the same value of p as Wentworth and Wilder, but introduced a multiplicative constant of $\frac{1}{31}$ to account for the variation in fingerprint pattern type. Gupta [24] estimated the value of p as $\frac{1}{10}$ for forks and endings and $\frac{1}{100}$ for the less commonly occurring minutiae types, based on 1,000 fingerprints. He also used a fingerprint-type-factor of $\frac{1}{10}$ and correspondence-in-ridge-count-factor of $\frac{1}{10}$. Because of the widely varying values of p used in the above studies, the probability of a given fingerprint configuration also dramatically varies from one model to the other.

Roxburgh [17] proposed a more comprehensive analysis to compute the probability of a fingerprint configuration. His analysis was based on considering a fingerprint as a pattern with concentric circles, one ridge interval apart, in a polar coordinate system. Roxburgh also incorporated a quality measure of the fingerprint into his calculations. He computed the probability of a particular fingerprint configuration to be:

$$P(\text{Fingerprint Configuration}) = \left(\frac{C}{P}\right)\left(\frac{Q}{RT}\right)^N, \quad (4)$$

where P is the probability of encountering a particular fingerprint type and core type, Q is a measure of quality ($Q = 1.5$ for an average quality print and $Q = 3.0$ for a poor quality print), R is the number of semicircular ridges in a fingerprint ($R = 10$), T is the corrected number of minutiae types ($T = 2.412$), and C is the number of possible positions for the configuration ($C = 1$). Amy [25] (cf. [13]) considered the variability in minutiae type, number, and position in his model for computing the probability of a fingerprint configuration. He further recognized that K multiple comparisons of the fingerprint pair (e.g., each hypothesized orientation alignment, each reference point correspondence) increase the possibility of false association which is given by

$$P(\text{False Association}) = 1 - (1 - P(\text{Fingerprint Configuration}))^K. \quad (5)$$

Kingston's [19] model, which is very similar to Amy's model, computes the probability of a fingerprint configuration based on the probabilities of the observed number of minutiae, observed positions of minutiae, and observed minutiae types as follows:

$$P(\text{Fingerprint Configuration}) = (e^{-y})(y^N/N!)(P_1)\prod_{i=2}^{N}(P_i)\frac{(0.082)}{[S-(i-1)(0.082)]}, \quad (6)$$

where y is the expected number of minutiae in a region of given size S (in mm^2) and P_i is the probability of occurrence of a particular minutiae type in the ith minutia.

Most of the models discussed above implicitly assume that fingerprints are being matched manually. The probability of observing a given fingerprint feature is estimated by manually extracting the features from a small number of fingerprint images. Champod and Margot [26] used an AFIS to extract minutiae from 977 fingerprint images scanned at a relatively high resolution of 800 dpi. They generated frequencies of minutiae occurrence and minutiae densities after manually verifying the thinned ridges produced by the AFIS to ensure that the feature extraction algorithm did not introduce errors. They considered minutiae only in concentric bands (five ridges wide) above the core and acknowledged that their individuality estimates were conservative (i.e., provided an upper bound). As an example, they estimated the probability of occurrence of a seven-minutiae configuration (five endings and two bifurcations) as 2.25×10^{-5}.

Osterburg et al. [14] divided fingerprints into discrete cells of size $1\,mm \times 1\,mm$. They computed the frequencies of 13 types of minutiae events (including an empty cell) from 39 fingerprints (8,591 cells) and estimated the probability that 12 ridge endings will match between two fingerprints based on an average fingerprint area of $72\,mm^2$ as 1.25×10^{-20}. Sclove [27] modified Osterburg et al.'s model by incorporating the observed dependence of minutiae occurrence in cells and came up with an estimate of probability of fingerprint configuration that is slightly higher than that obtained by Osterburg et al. Stoney and Thornton [13] criticized Osterburg et al.'s and Sclove's models because these models did not consider the fingerprint ridge structure, distortions, and the uncertainty in the positioning of the grid. Stoney and Thornton [13] critically reviewed earlier fingerprint individuality models and proposed a detailed set of fingerprint features that should be taken into consideration. These features included ridge structure and description of minutiae location, ridge counts between pairs of minutiae, description of minutiae distribution, orientation of minutiae, variation in minutiae type, variation among fingerprints from the same source, number of positions (different translations and rotations of the input fingerprint to match with the template), and number of comparisons performed with other fingerprints for identification.

Stoney's [28] model is different from other models in that it attempts to characterize a significant component of pairwise minutiae dependence. Stoney [28] and Stoney and Thornton [13] studied probabilities of occurrences of various types of minutiae, their orientation, number of neighboring minutiae, and distances/ridge counts to the neighboring minutiae. Given a minutiae set, they calculated the probability of a minutiae configuration by conjoining the probabilities of the individual events in the configuration. For instance, they proposed a linear ordering of minutia in a minutiae configuration and recursively estimated the probability of a n-minutiae configuration from the probability of an $(n-1)$-minutiae configuration and the occurrence of a new minutia of certain type/orientation at a particular distance/ridge counts from its nearest minutia within the $(n-1)$-minutiae configuration. The model also incorporated constraints due to connective ambiguity and due to minutiae-free areas. The model corrected for the probability of false association by accounting for the various possible linear orderings which could initiate/drive the search for correspondence. A sample calculation for computing the probability of a false association using Stoney's model is given below.

$$P(\text{False Association}) = 1 - \left(1 - 0.6 * \left(0.5 \times 10^{-3}\right)^{(N-1)}\right)^{\lfloor \frac{N}{5} \rfloor}$$
$$\approx \frac{N}{5} \times 0.6 * \left(0.5 \times 10^{-3}\right)^{(N-1)}.$$

For the sake of simplicity, we have considered only a rudimentary version of Stoney's model for the above computation; it is arbitrarily assumed that the probability of a typical *starting* minutia is 0.6, a typical neighboring minutia places an additional constraint of 5×10^{-3} on the probability, and there are no constraints due to connective ambiguity, minutiae-free areas, or minutiae-free borders. Finally, it is (arbitrarily) assumed that one in every five minutia can potentially serve as a starting point for a new search. We believe that a more realistic estimation of the individuality based on Stoney's model would not deviate from the relatively simple model presented here by more than a couple of orders of magnitude.

Stoney and Thornton identified weaknesses in their model and acknowledged that one of the most critical requirements, i.e., consideration of variation among prints from the same source, was not sufficiently addressed. Their tolerances for minutiae position were derived from successive printings under ideal conditions and are far too low to be applicable in actual fingerprint comparisons.

The models discussed above (including Amy's model of false association due to multiple comparisons) focused mainly on measuring the amount of detail in a single fingerprint (i.e., estimation of the probability of a fingerprint configuration). These models did not emphasize the intraclass variations in multiple impressions of a finger. We will refer to the quantifications of fingerprint individuality which explicitly consider the intraclass variations as the *probability of correspondence*. Trauring [29] was the first to concentrate explicitly on measuring the amount of detail needed to establish a correspondence between two prints from the same finger (intraclass variation) using an AFIS and observing that corresponding fingerprint features in impressions of the same finger could be displaced from each other by as much as 1.5 times the interridge distance. He further assumed that

1. minutiae are distributed randomly,
2. there are only two types of minutiae (ending and bifurcation),
3. the two types of minutiae are equally likely,
4. the two possible orientations of minutiae are equally likely, and
5. minutiae type, orientation, and position are independent variables.

Trauring computed the probability of a coincidental correspondence of N minutiae between two fingerprints from different fingers to be:

$$P(\text{Fingerprint Correspondence}) = (0.1944)^N. \qquad (7)$$

Stoney and Thornton's [13] criticism of the Trauring model is that he did not consider ridge count, connective ambiguity, and correlation among minutiae location. Further, they claim that Trauring's assumption that the minutiae types and orientations are equally probable is not correct. The probabilities of observing a particular minutiae configuration from different models are compared in Table 2.

There have been few studies which empirically estimate the probability of finding a fingerprint in a large database that successfully matches the input fingerprint. Meagher et al. [30] (for more details, see Stiles [31]) matched about 50,000 rolled fingerprints belonging to the same fingerprint class (left loop) with each other to compute the impostor distribution. However, the genuine distribution was computed by matching each fingerprint image with itself; this ignores the variability present in different impressions of the same finger. Further, they assumed that the impostor and the genuine distributions follow a Gaussian distribution and computed the probability of a false correspondence to be 10^{-97}. This model grossly underestimates the probability of a false correspondence because it does not consider realistic intraclass variations in impressions of a

TABLE 2
Comparison of Probability of a Particular Fingerprint Configuration Using Different Models

Author	P(Fingerprint Configuration)	N=36,R=24,M=72 (N=12,R=8,M=24)
Galton (1892)	$\frac{1}{16} \times \frac{1}{256} \times \left(\frac{1}{2}\right)^R$	1.45×10^{-11} (9.54×10^{-7})
Pearson (1930)	$\frac{1}{16} \times \frac{1}{256} \times \left(\frac{1}{36}\right)^R$	1.09×10^{-41} (8.65×10^{-17})
Henry (1900)	$\left(\frac{1}{4}\right)^{N+2}$	1.32×10^{-23} (3.72×10^{-9})
Balthazard (1911)	$\left(\frac{1}{4}\right)^N$	2.12×10^{-22} (5.96×10^{-8})
Bose (1917)	$\left(\frac{1}{4}\right)^N$	2.12×10^{-22} (5.96×10^{-8})
Wentworth & Wilder (1918)	$\left(\frac{1}{50}\right)^N$	6.87×10^{-62} (4.10×10^{-21})
Cummins & Midlo (1943)	$\frac{1}{31} \times \left(\frac{1}{50}\right)^N$	2.22×10^{-63} (1.32×10^{-22})
Gupta (1968)	$\frac{1}{10} \times \frac{1}{10} \times \left(\frac{1}{10}\right)^N$	1.00×10^{-38} (1.00×10^{-14})
Roxburgh (1933)	$\frac{1}{1000} \times \left(\frac{1.5}{10 \times 2.412}\right)^N$	3.75×10^{-47} (3.35×10^{-18})
Trauring (1963)	$(0.1944)^N$	2.47×10^{-26} (2.91×10^{-9})
Osterburg et al. (1977)	$(0.766)^{M-N}(0.234)^N$	1.33×10^{-27} (1.10×10^{-9})
Stoney (1985)	$\frac{N}{5} \times 0.6 \times (0.5 \times 10^{-3})^{N-1}$	1.2×10^{-80} (3.5×10^{-26})

For a fair comparison, we do not distinguish between minutiae types. By assuming that an average size fingerprint has 24 regions ($R = 24$) as defined by Galton, 72 regions ($M = 72$) as defined by Osterburg et al., and has 36 minutiae on average ($N = 36$), we compute the probability of observing a given fingerprint configuration in the third column of the table.The probability of observing a fingerprint configuration with $N = 12$ and equivalently, $R = 8$ and $M = 24$ is given in braces in the third column. Note that all probabilities represent a full (N minutiae) match as opposed to a partial match (see Table 3).

finger (see also Stoney and Thornton [13] and Wayman [32]). Daugman [33] analyzed the probability of a false match in an iris recognition system based on an empirical impostor distribution of the IrisCode match scores from 340 irises. Under the assumption that the imposter and the genuine distributions are parametric (binomial), he concluded that irises are extremely individual (false correspondence error rate of 10^{-12} at a probability of a false rejection of 8.5×10^{-5}).

3 A Model of Fingerprint Individuality

We have developed a fingerprint individuality model in an attempt to obtain a realistic and more accurate probability of correspondence between fingerprints. The probabilities obtained using this model will be compared against empirical values using an *Automatic Fingerprint Matching System* (AFMS) [10] (an AFIS is used for identification; an AFMS is used for verification). To estimate the probability of correspondence, we make the following assumptions:

1. We consider only minutiae features since a) most of the discriminatory power of the AFMS is based on minutiae features and b) for an objective measurement of individuality, it is necessary that the representation be consistently reproducible, easily localized, and quantified. Minutiae features have been shown to be stable and practical systems have demonstrated a reliable extraction of minutiae representation from fingerprints of reasonable image quality. Only ridge endings and ridge bifurcations are considered because the occurrence of other minutiae types, such as islands, dots, enclosures, bridges, double bifurcations, trifurcations, etc. is relatively rare. Additionally, we do not distinguish between the two types of minutiae because ridge endings and ridge bifurcations cannot be discriminated with a high level of accuracy. Since minutiae can reside only on ridges which follow certain overall patterns in a fingerprint, the minutiae directions are not completely independent of the minutiae locations. We implicitly model the statistical dependence between minutiae directions and locations in our model. Finally, we have not considered the pairwise minutiae features such as ridge counts in the present analysis.
2. We assume a uniform distribution of minutiae in a fingerprint with the restriction that two minutiae cannot be very close to each other. While minutiae locations are not uniformly distributed, our assumption approximates the slightly overdispersed uniform distribution found by Stoney [34]. Sclove [27] showed that the minutiae tend to cluster. We have not explicitly modeled the clustering tendency of minutiae. Therefore, the assumption of independence of minutiae locations will bias the estimate of the probability of a false correspondence toward higher values. However, it is a common practice in fingerprint individuality studies to make conservative (higher) estimates of the probability of correspondence. Both Sclove [27] and Osterburg et al. [14] discuss how these conservative estimates favor a suspect in a criminal investigation in the sense that they give the suspect the benefit of the doubt by lowering the certainty attached with the fingerprint matching.
3. Correspondence of a minutiae pair is an independent event and each correspondence is equally important. Fingerprint matching systems weigh different correspondences based on their position

(e.g., correspondences involving minutiae from a peripheral pattern area are weighted less than those involving minutiae located in the center of the fingerprint). Similarly, it is possible to weigh spatially diverse correspondences more than all correspondences localized in a narrow spatial neighborhood. Our analysis currently ignores such dependencies among the minutiae correspondences.

4. We do not explicitly take into account fingerprint image quality in individuality determination. It is very difficult to reliably assign a quality index to a fingerprint because image quality is a subjective concept. Our approach to incorporating image quality in fingerprint matching assumes that only a subset of the true minutiae in a fingerprint will be detected. All correspondences are considered reliable and no certainty is associated with a correspondence based on the fingerprint image quality. In good quality fingerprints, one could use conflicting evidence (when a minutia in input does not match any minutiae in template) to reject the hypothesis that the input and the template fingerprints are the same. However, there will be some errors in identifying minutiae in fingerprints with poor quality. Therefore, we explicitly consider only the positive evidence from a minutiae correspondence; the negative information from the conflicting evidence (e.g., a minutia that does not match) is ignored.
5. Ridge widths are assumed to be the same across the population and spatially uniform in the same finger. This assumption is justified because the pressure variations could make nonuniform ridge variations uniform and vice versa. Further, there may be only limited discriminatory information in the ridge frequency.
6. The analysis of matchings of different impressions of the same finger binds the parameters of the probability of matching minutiae in two fingerprints from different fingers.
7. We assume that there exists one and only one (correct) alignment between the template and the input minutiae sets. The fingerprint correspondence problem involves matching two fingerprints; one is called the *template* (stored in the system) and the other is called the *input* (which needs to be identified). We assume that a reasonable *alignment* has been established between the template and the input. The alignment of the input minutiae set with the template minutiae set is done so that the minutiae correspondences can be determined with a small tolerance. In manual fingerprint matching, this alignment is typically based on utilizing the fingerprint singularities (core(s) and delta(s)) and ridges. An automatic system may seek an alignment that maximizes a given objective function (such as the number of matching minutiae). This assumption may not be valid when matching a partial (latent) fingerprint with a full print in the database, as there may be several "reasonable" alignments possible. When multiple alignments are indeed warranted by a situation, the probability of false correspondence increases (see (5)).

Given an input fingerprint containing n minutiae, our goal is to compute the probability that an arbitrary fingerprint (template in a database of fingerprints) containing m minutiae will have exactly q corresponding minutiae with the input. Since we only consider fingerprint minutiae which are defined by their location, (x, y) coordinates, and by the angle of the ridge on which it resides, θ, the input and the template minutiae sets, T and I, respectively, are defined as:

$$T = \{\{x_1, y_1, \theta_1\}, \{x_2, y_2, \theta_2\}, \ldots, \{x_m, y_m, \theta_m\}\}, \tag{8}$$
$$I = \{\{x'_1, y'_1, \theta'_1\}, \{x'_2, y'_2, \theta'_2\}, \ldots, \{x'_n, y'_n, \theta'_n\}\}. \tag{9}$$

Once an alignment between the input minutiae set and the template minutiae set is established, we develop our individuality model. A minutiae *j* in the input fingerprint is considered as "corresponding" or "matching" to the minutiae *i* in the template, if and only if

$$\sqrt{(x'_i - x_j)^2 + (y'_i - y_j)^2} \le r_0, \quad \text{and} \tag{10}$$
$$\min(|\theta'_i - \theta_j|, 360 - |\theta'_i - \theta_j|) \le \theta_0, \tag{11}$$

where r_0 is the tolerance in distance and θ_0 is the tolerance in angle. Both manual and automatic fingerprint matchings are based on some tolerance both in minutiae location and angle to account for the variations in different impressions of the same finger. Equation (11) computes the minimum of $|\theta'_i - \theta_j|$ and $360 - |\theta'_i - \theta_j|$ because the angles are $mod\ 360$ (the difference between angles of 2° and 358° is only 4°).

Let A be the total area of overlap between the input and the template fingerprints after a reasonable alignment has been achieved (see, Fig. 4). If a minutia in the template fingerprint falls within a distance r_0 from a minutia in the input, a minutia correspondence is declared. The probabilities that an arbitrary minutia in the input will match an arbitrary minutia in the template, only in terms of location, and only in terms of direction, are given by (12) and (13), respectively. Equation (12) assumes that (x, y) and (x', y') are independent and (13) assumes that θ and θ' are independent.

$$P\left(\sqrt{(x'_i - x_j)^2 + (y'_i - y_j)^2} \le r_0\right) = \frac{\text{area of tolerance}}{\text{total area of overlap}} = \frac{\pi r_0^2}{A} = \frac{C}{A}, \tag{12}$$
$$P(\min(|\theta'_i - \theta_j|, 360 - |\theta'_i - \theta_j|) \le \theta_0) = \frac{\text{angle of tolerance}}{\text{total angle}} = \frac{2\theta_0}{360}. \tag{13}$$

First, we will develop our fingerprint correspondence model when only minutiae locations are matched and later introduce the minutiae angles in the formulation. If the template contains m minutiae, the probability that only one minutia in the input will correspond to any of the m template minutiae is given by $\frac{mC}{A}$. Now, given two input

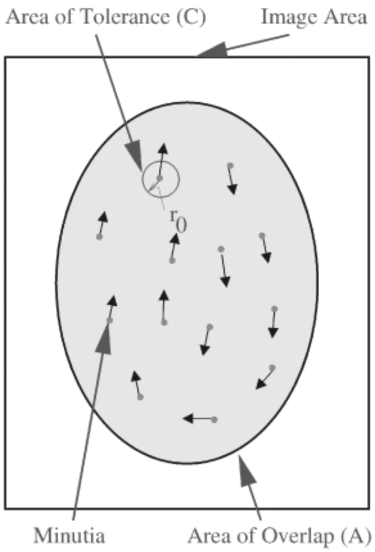


Fig. 4. When an input fingerprint is matched with a template, an alignment is first established. The area of the input fingerprint image that overlaps with the template and the input minutiae within the overlap area are shown. In addition, tolerance in area for minutiae matching for one particular minutia is also illustrated.

minutiae, the probability that only the first one corresponds to one of the m template minutiae is the product of the probabilities that the first input minutia has a correspondence ($\frac{mC}{A}$) and the second minutia does not have a correspondence ($\frac{A-mC}{A-C}$). Thus, the probability that exactly one of the two input minutiae matches any of the m template minutiae is $2 \times \frac{mC}{A} \times \frac{A-mC}{A-C}$ since either the first input minutia alone may have a correspondence or the second input minutia alone may have a correspondence. If the input fingerprint has n minutiae, the probability that exactly one input minutia matches one of the m template minutiae is

$$p(A, C, m, n) = \binom{n}{1}\left(\frac{mC}{A}\right)\left(\frac{A - mC}{A - C}\right). \qquad (14)$$

The probability that there are exactly ρ corresponding minutiae between the n input minutiae and m template minutiae is then given by:

$$\begin{aligned} &p(A, C, m, n, \rho) = \\ &\binom{n}{\rho}\underbrace{\left(\frac{mC}{A}\right)\left(\frac{(m-1)C}{A-C}\right)\cdots\left(\frac{(m-\rho-1)C}{A-(\rho-1)C}\right)}_{\rho\text{ terms}} \times \\ &\underbrace{\left(\frac{A-mC}{A-\rho C}\right)\left(\frac{A-(m-1)C}{A-(\rho+1)C}\right)\cdots\left(\frac{(A-(m-(n-\rho+1))C}{A-(n-1)C}\right)}_{n-\rho\text{ terms}}. \end{aligned} \qquad (15)$$

The first ρ terms in (15) denote the probability of matching ρ minutiae between the template and the input and the remaining $(n-\rho)$ terms express the probability that $(n-\rho)$ minutiae in the input do not match any minutiae in the template. Dividing the numerator and denominator of each term in (15) by C, we obtain:

$$\begin{aligned} &p(A, C, m, n, \rho) = \\ &\binom{n}{\rho}\left(\frac{m}{\frac{A}{C}}\right)\left(\frac{(m-1)}{\frac{A}{C}-1}\right)\cdots\left(\frac{(m-\rho-1)}{\frac{A}{C}-(\rho-1)}\right) \times \\ &\left(\frac{\frac{A}{C}-m}{\frac{A}{C}-\rho}\right)\left(\frac{\frac{A}{C}-(m-1)}{\frac{A}{C}-(\rho+1)}\right)\cdots\left(\frac{(\frac{A}{C}-(m-(n-\rho+1))}{\frac{A}{C}-(n-1)}\right). \end{aligned} \qquad (16)$$

Letting $M = \frac{A}{C}$ and assuming that M is an integer (which is a realistic assumption because $A \gg C$), we can write the above equation in a compact form as:

$$\begin{aligned} p(M, m, n, \rho) = &\frac{n!}{\rho!(n-\rho)!} \times \\ &\frac{(M-n)!}{M!} \times \frac{m!}{(m-\rho)!} \times \frac{(M-m)!}{((M-m)-(n-\rho))!}, \end{aligned} \qquad (17)$$

which finally reduces to:

$$p(M, m, n, \rho) = \frac{\binom{m}{\rho}\binom{M-m}{n-\rho}}{\binom{M}{n}}. \qquad (18)$$

Equation (18) defines a hypergeometric distribution of ρ with parameters m, M, and n . To get an intuitive understanding of the probability model for the minutiae correspondence in two fingerprints, imagine that the overlapping area of the template and the input fingerprints is divided into M nonoverlapping cells. The shape of the individual cells does not matter, just the number of cells. Now, consider a deck of cards containing M distinct cards. Each card represents a cell in the overlapping area. There is one such deck for the template fingerprint and an identical deck for the input fingerprint. If m cards are drawn from the first (template) deck without replacement and n cards are drawn from the second (input) deck without replacement, the probability of matching exactly ρ cards among the cards drawn is given by the hypergeometric distribution in (18) [9].

The above analysis considers a minutia correspondence based solely on the minutiae location. Minutiae patterns are generated by the underlying fingerprints, which are smoothly flowing oriented textures. The orientations of nearby minutiae points are strongly correlated. The orientation of minutiae points are also correlated with the location of the minutiae point in the fingerprint, depending on the fingerprint type. Thus, the configuration space spanned by the minutiae pattern is smaller than that spanned by a pattern of (directed) random points. This typically implies that the probability of finding sufficiently similar prints from two different fingers is higher than that of finding sufficiently similar sets of random (directed) point patterns. Next, we consider a minutia correspondence that depends on minutiae directions in addition to the minutiae locations. For the sake of this analysis, let us assume that the minutiae directions are completely independent of the minutiae positions and matching minutiae position and minutiae direction are therefore independent events. To account for the dependence between θ and θ', let l be such that $P\left(\min\left(\left|\theta'_{\mathrm{i}} - \theta_{\mathrm{j}}\right|, 360 - \left|\theta'_{\mathrm{i}} - \theta_{\mathrm{j}}\right|\right) \le \theta_0\right) = l$ in (13). Given n

input and m template minutiae, the probability of ρ minutiae falling into the *similar* positions can be estimated by (18). Once ρ minutiae positions are matched, the probability that q ($q \leq \rho$) minutiae among them have similar directions is given by

$$\binom{\rho}{q}(l)^q(1-l)^{\rho-q},$$

where l is the probability of two position-matched minutiae having a similar direction and $1-l$ is the probability of two position-matched minutiae taking different directions. This analysis assumes that the ridge direction information/uncertainity can be completely captured by

$$P\big(\min\big(\left|\theta'_{\rm i}-\theta_{\rm j}\right|, 360-\left|\theta'_{\rm i}-\theta_{\rm j}\right|\big) \leq \theta_0\big).$$

Therefore, the probability of matching q minutiae in both position as well as direction is given by

$$p(M,m,n,q) = \sum_{\rho=q}^{\min(m,n)} \left(\frac{\binom{m}{\rho}\binom{M-m}{n-\rho}}{\binom{M}{n}} \times \binom{\rho}{q}(l)^q(1-l)^{\rho-q} \right). \tag{19}$$

Until now, we have assumed that the minutiae locations are uniformly distributed within the *entire* fingerprint area. Since A is the area of overlap between the template and the input fingerprints, the ridges occupy approximately $\frac{A}{2}$ of the area, with the other half being occupied by the valleys. We assume that the number (or the area) of ridges across all fingerprint types is the same. Since the minutiae can lie only on ridges, i.e., along a curve of length $\frac{A}{w}$, where w is the ridge period, the value of M in (19) should therefore be changed from $M = A/C$ to $M = \frac{A/w}{2r_0}$, where $2r_0$ is the length tolerance in minutiae location.

3.1 Parameter Estimation

Our individuality model has several parameters, namely, r_0, l, w, A, m, n, and q. The value of l further depends on θ_0. The values of r_0, θ_0, l, and w are estimated in this section for a given sensor resolution. To compare the probabilities obtained from the theoretical model with the empirical results, we will estimate the values of A, m, and n from two different databases in the next section.

The value of r_0 should be determined to account for the variations in different impressions of the same finger (intraclass variation). However, since the spatial tolerance is dependent upon the scale at which the fingerprint images are scanned, we need to calculate it for a specific sensor resolution. We used a database (called GT) consisting of 450 mated pairs of fingerprints acquired using a high quality (Identicator [35]) optical scanner at a resolution of 500 dpi. The second print in the mated pair was acquired at least a week after the first print. The minutiae were manually extracted from the prints by a fingerprint expert. The expert also determined the correspondence information for the detected minutiae. Using the ground truth correspondence information between duplex (two) pairs of corresponding minutiae, a rigid transformation between the mated pair was determined. The overall rigid transformation between the mated pair was determined using a least square approximation of the candidate rigid transformations estimated from each duplex pairs of the corresponding minutiae. After aligning a given mated pair of fingerprints using the overall transformation, the location difference $(x'-x, y'-y)$ for each corresponding minutia pair was computed; distance

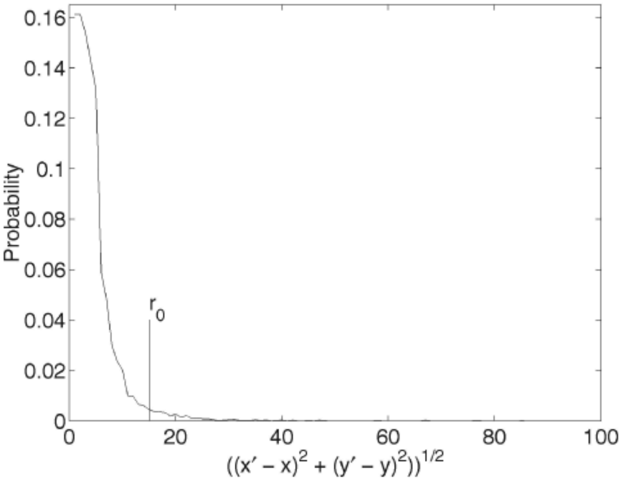


Fig. 5. Distribution of minutiae distance differences for the genuine fingerprint pairs in the GT database.

$$\left(\sqrt{(x'-x)^2 + (y'-y)^2}\right)$$

estimates for all minutiae pairs in all mated fingerprint pairs were pooled to obtain a distribution of the distance between the corresponding minutiae (see Fig. 5). We are seeking the smallest value of r_0 for which

$$P\left(\sqrt{(x'-x)^2 + (y'-y)^2} \leq r_0\right) \geq 0.975,$$

i.e., the value of r_0 which accounts for at least 97.5 percent of variation in the minutiae position of genuine fingerprint matchings. Thus, r_0 is determined from the distribution of

$$\sqrt{(x'-x)^2 + (y'-y)^2}$$

shown in Fig. 5 and is found to be 15 pixels for fingerprint images scanned at 500 dpi resolution.

To estimate the value of l, we first estimate the value of θ_0. The value of θ_0 can also be estimated using the database GT. After aligning a given mated pair of fingerprints using the overall transformation, we seek that value of θ_0 which accounts for 97.5 percent variation in the minutia angles in the genuine fingerprint matchings, i.e., we seek that value of θ_0 for which

$$P\big(\min\big(\left|\theta'_{\rm i}-\theta_{\rm j}\right|, 360-\left|\theta'_{\rm i}-\theta_{\rm j}\right|\big) \leq \theta_0\big) \geq 0.975.$$

The distribution, $P\big(\min\big(\left|\theta'-\theta\right|, 360-\left|\theta'_{\rm i}-\theta_{\rm j}\right|\big)\big)$, for the genuine fingerprint matchings in GT is shown in Fig. 6a. The smallest value of θ_0 for which $P(\min(|\theta'-\theta|, 360-|\theta'-\theta|) \leq \theta_0) \geq 0.975$ is found to be $\theta_0 = 22.5°$. In the second step, we determine the distribution $P(\min(|\theta'-\theta|, 360-|\theta'-\theta|))$ for the imposter fingerprint matchings. Since we do not have correspondences marked by an expert between

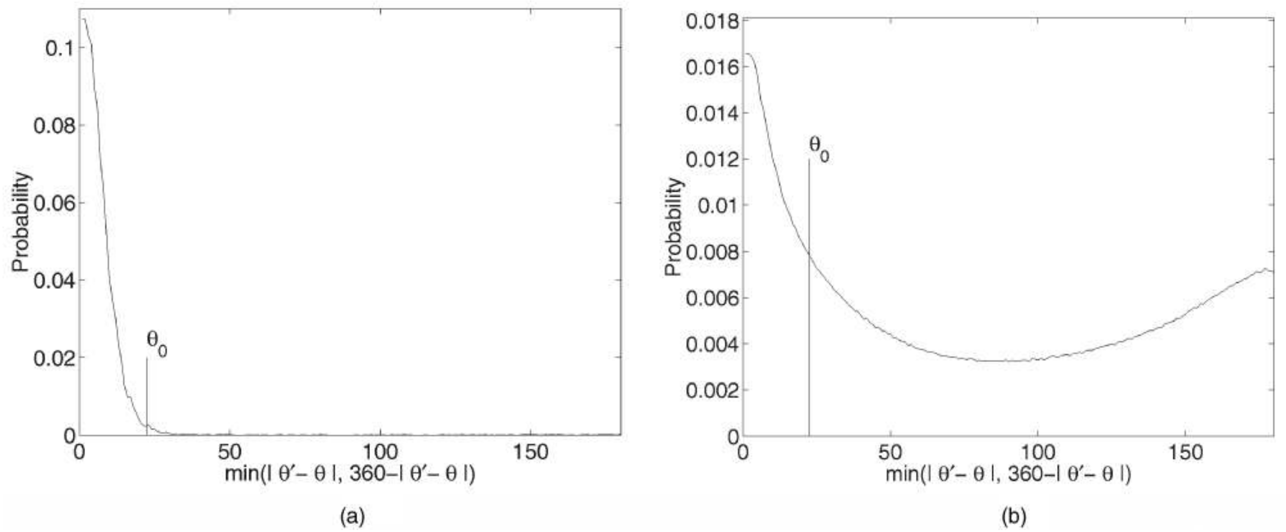


Fig. 6. Distributions for minutiae angle differences for the (a) genuine fingerprint pairs using the ground truth and (b) imposter matchings using the automatic fingerprint matching system.

imposter fingerprint pairs, we depend on our fingerprint matcher to establish correspondences between minutiae in imposter pairs. Thus, our estimation of l is slightly dependent on the automatic fingerprint matcher used. The distribution $P(\min(|\theta'_{\mathrm{i}} - \theta_{\mathrm{j}}|, 360 - |\theta'_{\mathrm{i}} - \theta_{\mathrm{j}}|))$ estimated by using our matcher on the GT database is shown in Fig. 6b from which we determined that

$$P(\min(|\theta'_i - \theta_j|, 360 - |\theta'_i - \theta_j|) \leq 22.5^\circ) = 0.267,$$

i.e., $l = 0.267$. Note that, under the assumption that minutiae directions are uniformly distributed and the directions for the minutiae that match in their location (θ and θ') are independent, we obtain $l = \frac{2\times 22.5}{360} = 0.125$. If minutiae orientations are considered instead of directions, the value for l determined from the experiments will be 0.417 as opposed to a value of $\frac{2\times 22.5}{180} = 0.25$ determined under the assumption stated above.

The value of w was taken as reported by Stoney [34]. Stoney estimated the value of ridge period as 0.463 mm/ridge from a database of 412 fingerprints. For fingerprint sensors with a resolution of $500\,\mathrm{dpi}$, the ridge period converts to ~ 9.1 pixels/ridge. Thus, $w \sim 9.1$. This value is also in close agreement with the values reported by Cummins and Midlo [23] and Kingston [19].

4 Experimental Results and Discussions

Fingerprint images were collected in our laboratory from 167 subjects using an optical sensor manufactured by Digital Biometrics, Inc. [36] (image size = 508×480, resolution = $500\,\mathrm{dpi}$). Single impressions of the right index, right middle, left index, and left middle fingers for each subject were taken in that order. This process was then repeated to acquire a second impression. The fingerprint images were collected again from the same subjects after an interval of six weeks in a similar fashion. Thus, we have four impressions for each of the four fingers of a subject. This resulted in a total of $2,672$ ($167 \times 4 \times 4$) fingerprint images. We call this database MSU_DBI. A live feedback of the acquired image was provided and the subjects were guided in placing their fingers in the center of the sensor in an upright orientation. Using the protocol described above, we also collected fingerprint images using a solid-state fingerprint sensor manufactured by Veridicom, Inc. [37] (image size = 300×300, resolution = $500\,\mathrm{dpi}$). We call this database MSU_VERIDICOM. A large number of impostor matchings (over 4,000,000) were generated using an automatic fingerprint matching system [10].

The mean values of m and n for impostor matchings were estimated as 46 for the MSU_DBI database and as 26 for the MSU_VERIDICOM database from the distributions of m and n (Figs. 7a and 7b). The average values of A for the MSU_DBI and the MSU_VERIDICOM databases are 67,415 pixels and 28,383 pixels, respectively. The value of the overall effective area A was estimated in the following fashion: After the template and the input fingerprints were aligned using the estimated transformation, a bounding box A_i, of all the corresponding minutiae in the input fingerprint was computed in the common coordinate system. Similarly, a bounding box, A_t, of all the corresponding minutiae in the template fingerprint was also computed in the common coordinate system. The intersection A of these two bounding boxes A_i and A_t for each matching was then estimated. The estimates of A for all the matchings performed in the database were pooled to obtain a distribution for A (see Figs. 8a and 8b). An arithmetic mean of the distribution was used to arrive at an estimate of A.

The probabilities of a fingerprint correspondence obtained for different values of M, m, n, and q are given in Table 3. The values obtained from our model shown in Table 3 can be compared with values obtained from the previous models in Table 2 for $m = 36$, $n = 36$, and $q = 36, 12$.

Typically, a match consisting of 12 minutiae points (*the 12-point guideline*) is considered as sufficient evidence in many courts of law. Assuming that an expert can correctly glean all the minutiae in a latent, a 12-point match with the full-print template (see the first row, last column entry in Table 4) is an overwhelming amount of evidence, *provided* that there is no contradictory minutia evidence in the overlapping area. The value of A was computed for $500\,\mathrm{dpi}$

TABLE 3
Fingerprint Correspondence Probabilities Obtained from the Proposed Individuality Model for Different Sizes of Fingerprint Images Containing 26, 36, or 46 Minutiae

M, m, n, q	P(Fingerprint Correspondence)
104, 26, 26, 26	5.27×10^{-40}
104, 26, 26, 12	3.87×10^{-9}
176, 36, 36, 36	5.47×10^{-59}
176, 36, 36, 12	6.10×10^{-8}
248, 46, 46, 46	$1.33 \times 10^{\ 77}$
248, 46, 46, 12	5.86×10^{-7}
70, 12; 12, 12	1.22×10^{-20}

The entry (70, 12, 12, 12) corresponds to the 12-point guideline. The value of M for this entry was computed by estimating typical print area manifesting 12 minutia in a 500 dpi optical fingerprint scan.

fingerprint images from the minutiae density of 0.246 minutiae/mm^2 estimated by Kingston (cf. [34]) from 100 fingerprints; thus, $M = 70$ was used for all the entries in Table 4. Since latent prints are typically of very poor quality, it is possible that there could be an error in judgment of the existence of minutiae in the latent or their possible match to the minutiae in the template print. The effect of such misjudgments on the probability of a false correspondence is rather dramatic. For instance, imposing two incorrect minutiae match judgments increases the probability of a false correspondence from 1.22×10^{-20} (entry $n = 12, q = 12$ in Table 4) to 1.96×10^{-14} (entry $n = 12, q = 10$ in Table 4) and ignoring two genuine minutiae present in the input (latent) print increases the probability from 1.22×10^{-20} (entry $n = 12, q = 12$ in Table 4) to 1.11×10^{-18} (entry $n = 14, q = 12$ in Table 4). Thus, the misjudgment of a false minutiae match has significantly more impact than that of missing genuine minutiae in the input latent print.

Figs. 9a and 9b show the distributions of the number of matching minutiae computed from the MSU_DBI and MSU_VERIDICOM databases using an automatic fingerprint matching system (AFMS) [10], respectively. These figures also show the theoretical distributions obtained from our model described in Section 3 for the average values of M, m, and n computed from the databases. The empirical distribution is to the right of the theoretical distribution, which can be explained by the following factors:

1. Some true minutiae are missed and some spurious minutiae are detected by the automatic system due to noise in the fingerprint images and the imperfect nature of the automatic algorithms. Spurious minutiae may also be detected because of cuts and bruises on the fingertips.
2. The automatic matching algorithm cannot completely recover the nonlinear deformation present in the fingerprint images, so the alignment between the input and template has some error.
3. Automatic feature extraction introduces error in minutiae location and orientations.
4. The matcher seeks that alignment which maximizes the number of minutiae correspondences. Consequently, the probability of a false correspondence increases.

Table 5 shows the empirical probability of matching 10 and 15 minutiae in, MSU_VERIDICOM and MSU_DBI databases, respectively. The typical values of m and n were estimated from their distributions by computing the arithmetic means. The probabilities of false correspondence for these values of m, n and q, are reported in the third column of Table 5. The probabilities for matching "q or more" minutiae are 3.0×10^{-2} and 3.2×10^{-2} for the MSU_VERIDICOM and MSU_DBI databases, respectively, i.e., of the same order. The probabilities of false correspondence (false acceptance rates) obtained on these databases are consistent with those obtained on similar databases by several other state-of-the-art automatic fingerprint verification systems reported in the FVC2000 fingerprint verification competition [38]. On the other hand, the performance claims by several fingerprint verification system vendors vary over a large range (a false acceptance rate of 10^{-9} to 10^{-3}) due to the absence of standardized testing protocols and databases. The probabilities of a false fingerprint correspondence from the proposed theoretical model obtained for different values of M, m, n, and q given in Table 3 are several order of magnitude lower than the corresponding empirical probabilities given in Table 5.

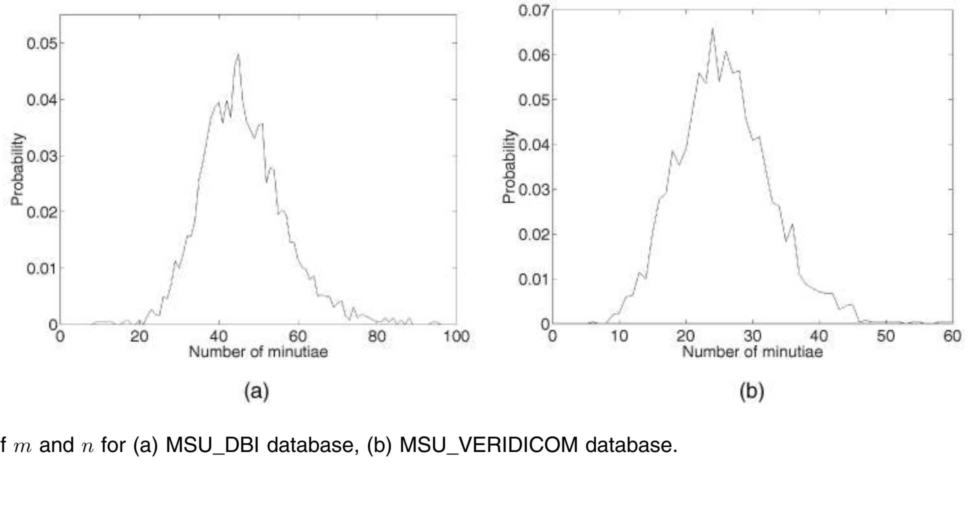
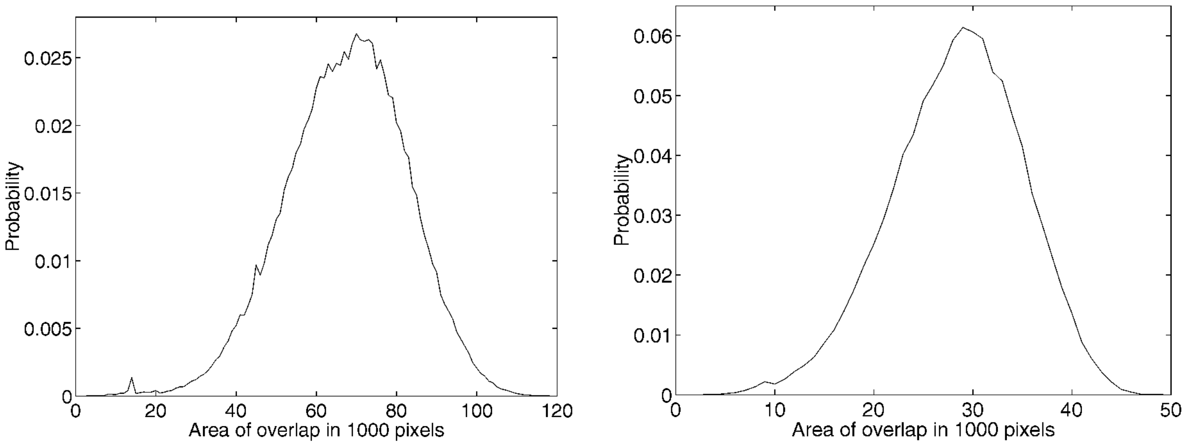


Fig. 7. Distributions of m and n for (a) MSU_DBI database, (b) MSU_VERIDICOM database.



(a) (b)

Fig. 8. Area of overlap between the two fingerprints that are matched based on the bounding boxes of the minutiae features for (a) MSU_DBI database, (b) MSU_VERIDICOM database.

5 Summary

One of the most fundamental questions one would like to ask about any *practical* biometric authentication system is: What is the inherent discriminable information available in the input signal? Unfortunately, this question, has been answered, if at all, in a very limited setting for most biometrics modalities, including fingerprints. The inherent signal capacity issue is of enormous complexity as it involves modeling both the composition of the population as well as the interaction between the behavioral and physiological attributes at different scales of time and space. Nevertheless, a first-order approximation to the answers to these questions will have significant bearing on the acceptance of fingerprint- (biometrics-) based personal identification systems into our society, as well as determining the upper bounds on scalability of deployments of such systems.

Estimating fingerprint individuality essentially involves determining the discriminatory information within the input measurements (fingerprint images) to resolve the identities of the people. The empirical and theoretical methods of estimating individuality serve complementary goals. Empirical observations lead us to characterize the constraints on the discriminatory information across different fingers as well as the invariant information among the different impressions of the same finger; the theoretical modeling/generalization of these constraints permits prediction of the bounds on the performance and facilitates development of constructive methods for an independent empirical validation. Historically, there has been a disconnect in the performance evaluations of practical fingerprint systems and theoretical performance predictions. Further, the results of the data-dependent empirical performance evaluations themselves have varied quite dramatically.

The pattern recognition theory prescribes that accurate characterization of the discriminatory power of a pattern needs measurement of not only the total variation present in the patterns, but also the variation of the patterns within each class (intraclass variations). As mentioned, most of the previous studies have focused their effort in modeling the total pattern variation. The existing studies of fingerprint individuality either grossly neglect to characterize the

TABLE 4
The Adverse Effects of Fingerprint Expert Misjudgments in Using the *12-Point Guideline*

q n	8	9	10	11	**12**
12	6.19×10^{-10}	4.88×10^{-12}	1.96×10^{-14}	3.21×10^{-17}	$\mathbf{1.22 \times 10^{-20}}$
13	1.58×10^{-9}	1.56×10^{-11}	8.42×10^{-14}	2.08×10^{-16}	1.58×10^{-19}
14	3.62×10^{-9}	4.32×10^{-11}	2.92×10^{-13}	9.66×10^{-16}	1.11×10^{-18}
15	7.63×10^{-9}	1.06×10^{-10}	8.68×10^{-13}	3.60×10^{-15}	5.53×10^{-18}
16	1.50×10^{-8}	2.40×10^{-10}	2.30×10^{-12}	1.45×10^{-14}	2.21×10^{-17}

The source of error could be in underestimating the number of actual minutiae in the latent print (n) *or overestimating the number of matched minutiae* (q)*. The value of* m *is* 12 *for all the entries in this table. The entry* $(n = 12, q = 12)$ *represents the probability of a false correspondence when the 12-point guideline is correctly applied by a fingerprint examiner. Except for the* $(n = 12, q = 12)$ *entry, all other entries represent incorrect judgments by the fingerprint expert to arrive at a decision that exactly 12 minutiae in the latent print matched 12 corresponding minutiae in the template print. For instance, the entry* $(n = 14, q = 8)$ *in the table represents an estimate of probability of a false correspondence due to two misjudgments by the examiner: First, the fingerprint examiner detected* 12 *minutiae in the latent print while there were in fact 14 minutiae in the latent print, i.e., the examiner overlooked two latent print minutiae. Further, while he associated all 12 minutiae he detected in the latent print to the 12 minutiae in the template print, only eight of those correspondences were indeed genuine correspondences (four incorrect minutiae match judgments).*

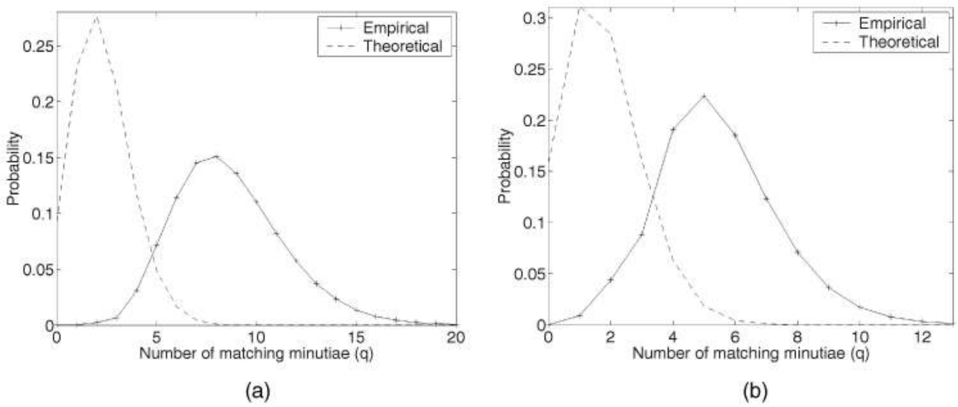


Fig. 9. Comparison of experimental and theoretical probabilities for the number of matching minutiae. (a) MSU_DBI database, (b) MSU_VERIDICOM database.

intraclass variations or restrict themselves to topological (ridge structure) representation which may be difficult to automatically extract, not available (e.g., latent prints), or unreliable (e.g., poor quality prints).

This study is an effort in statistical estimation of fingerprint individuality using a simple minutiae-based representation. The simplicity of the representation has allowed us to objectively and empirically quantify a number of constraints on the minutiae configurations, as well as intraclass variations, using a fingerprint matcher. The elastic string matching algorithm used in the estimation not only accomplishes the overall alignment of the two fingerprints being compared but also undistorts the prints to compensate for any elastic distortion they may have undergone.

The biometric signal capacity has direct implications to the system design. Inherent signal limitations may suggest a better sensor, temporal/spatial fusion of multiple sensors, or modalities. In some contexts, it may also indicate better system engineering to promote consistent acquisition through a constrained or user-friendly user interface. In other applications, when the validity of the biometric signal is suspect (e.g., due to circumvention issues), system design with integrity sensors (e.g., liveness detection for fingers) may be indicated. On the other hand, any excess signal capacity may suggest a method of delimiting the signal bandwidth for either individual privacy or efficiency reasons. More specifically, our results have direct implications for two fingerprint-based applications: automatic fingerprint verification systems and human expert visual fingerprint matching (forensic).

Let us first consider the automatic fingerprint verification systems. The model proposed here is relatively simple. It ignores most of the known (weak) dependencies among the minutiae features and does not directly include features such as ridge counts, fingerprint class, ridge frequencies, permanent scars, etc. For these reasons, we suspect that the proposed model does not yet compete in predicting the performance of human fingerprint expert matcher. Yet, we believe that the individuality estimates predicted by the present model are significantly closer to the performance of practical automatic fingerprint matchers on realistic data samples (images acquired under practical conditions; these images are typically not of very good quality and manifest typical problems related to acquisition) than other models reported in the literature.

TABLE 5
Fingerprint Correspondence Probabilities Obtained from Matching Imposter Fingerprints Using an AFMS [10] for the MSU_VERIDICOM and MSU_DBI Databases

Database	m,n,q	P(False Correspondence)
MSU_VERIDICOM	26, 26, 10	1.7×10^{-2}
MSU_DBI	46, 46, 15	1.4×10^{-2}

The probabilities given in the table are for matching "exactly q" minutiae. The average values for A, m, and n are 28,383, 26, and 26 for the MSU_VERIDICOM database and 67,415, 46, and 46 for the MSU_DBI database, respectively.

While the individuality of the minutiae-based fingerprint representation based on our model is lower than the previous estimates, our study indicates that the likelihood of an adversary guessing someone's fingerprint pattern (e.g., requiring matching 20 or more minutia from a total of 36) is significantly lower than a hacker being able to guess a six-character alpha-numerical case-sensitive (most probably weak) password by social engineering techniques (most common passwords are based on birthday, spouse's name, etc.) or by brute force. The probability of guessing such a password by brute force is

$$\left(\frac{1}{26+26+10}\right)^{6} = 1.76 \times 10^{-11}.$$

Obviously, more stringent conditions on matching will provide better cryptographic strength at the risk of increasing the false rejection error rate.

Although there is a huge amount of "inherent" discriminatory information available in minutiae representation, the observed matching performance of the state-of-the art automatic matching systems is several orders of magnitude lower than the theoretical performance because of the noise in sensing fingerprints, errors in locating minutiae, and fragility of the matching algorithms. Additionally, the present understanding of the fingerprint feature (minutia) detection and invariance as implemented in the automatic fingerprint matching system is too simplistic to accomplish significantly better accuracies. If a typical full dab fingerprint contains 46 minutiae, there is an overwhelming amount of information present in the minutiae representation of fingerprints for manual identification (the probability of a false correspondence between two fingerprints from different users containing 46 minutiae each is 1.33×10^{-77}). However, an automatic system that makes its decision based on 12 minutiae correspondences is utilizing only limited information (the probability of a false correspondence for matching 12 minutiae between two fingerprints from different users containing 46 minutiae each is 5.86×10^{-7}). Given this liberal operating point of an automatic matcher, it may be desirable to explore additional complementary representations of fingerprints for automatic matching. See, for example, [39].

Let us now consider the fingerprint matching scenarios for criminal applications. Neither the minutiae-based representation nor the simple similarity metric model proposed in our work completely captures the complexity of the fingerprint expert matching process. Perhaps, the proposed model is a reasonable first-order approximation of most of the discriminatory information that is consistently available to the expert across the impressions. Our model offers a systematic method of quantifying the likelihood of a false match. According to a recent fingerprint Daubert challenge verdict [3], the expert fingerprint matching error rates are not unequivocally zero. While the statement is technically correct, our model predicts that the chances of a false match are sufficiently small to be ignored. Based on our individuality model, when an expert strictly adheres to the "12-point" guideline, there is overwhelming identifying evidence to his testimony.

Fingerprint experts operate in two modalities. In one modality, fingerprint experts perform a 10-print comparison where 10 impressions scanned from a candidate under the supervision of a trained person are compared with the corresponding impressions gathered from known individuals (e.g., convicted criminals). This is referred to as (*10-print match*). The impressions involved in such a match are relatively clean and the possibility of error in analyzing the fingerprint impressions is minimal. Our model shows that a 12-point match between impressions from each finger (e.g., left index) in such a situation provides significant credible evidence that the two impressions originated from the same finger. Of course, a 12-point match on all fingers further bolsters the hypothesis that the same person made both sets of impressions and a lack thereof leaves some unanswered questions open for investigation (e.g., contamination).

In the other modality, fingerprint experts work by comparing latent impressions left by criminals at the scene of a crime (*latent match*), which are typically smudgy, distorted, indistinct, and/or fragmentary, to relatively good quality impressions taken from a suspect or from an individual on the police record. In such situations, it is likely that the fingerprint expert minutiae detection judgments may be contested by the defendant parties. In such situations, with each falsely detected minutia in the latent print or with each falsely imposed match, the strength of the evidence degrades rather dramatically. Given the number of undisputed matched minutia and the number of disputed minutia, our model provides quantitative estimates of theoretical tolerance bounds of the error rates. Perhaps, cross validation studies estimating consistency of the minutiae detection and matching capabilities of a large number of trained fingerprint experts can provide a baseline for confidence intervals on the error estimates.

The proposed model does not completely take into account the individuality of the fingerprints due to their different global ridge configurations. How to effectively incorporate fingerprint class information into the proposed model (3) needs further investigation. Additional work is also necessary to include the known dependencies among the minutiae features and other novel features to refine the fingerprint individuality estimation proposed here and its subsequent empirical validation. Further, since individuality is closely coupled with the composition of the target population, it is also important to know if and how the invariant fingerprint information is related to the genetic constitution of the individual [40]. How does the fingerprint individuality estimate suffer when the fingerprint is of exceptionally poor quality? What attributes of the applications (e.g., adversarial), of the subjects (e.g., European workers of advanced age prone to occupational injuries to their fingers), and of the imaging/environments (e.g., optical imaging in dry Arizona weather) significantly affect the uniqueness of the individuals in a given target population. The individuality problem in its present form is an ill-formulated problem in the information theoretic sense. For instance, it is not always possible to define what an *ideal* matcher ("Turing Test") should decide if presented with very obliterated biometric measurements from a single biometric entity. It is only to be expected that the fingerprint-based personal identification, being one of the most mature, most well-understood, with the strongest legitimate support from the biometrics community would be the first biometrics to be challenged for objective quantification of its distinctiveness. We believe that by objectively and quantitatively addressing individuality related issues, difficult as they may be, will force us to formalize the concepts of individuality. This eventually will lead us to establish the standards not only for other biometrics, but may also lay foundations for characterization/evaluation of complex pattern recognition systems.

Acknowledgments

The authors would like to thank Mário A.T. Figueiredo of I.S.T., Technical University of Lisbon, Portugal for his many useful comments and suggestions. An earlier version of this paper appeared in the *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 805-812, Hawaii, 11-13 December 2001.

References

[1] *Advances in Fingerprint Technology,* second ed., H.C. Lee and R.E. Gaensslen eds. New York: CRC Press, 2001.

[2] *Latent Print Examination,* http://onin.com/fp/, 2002.

[3] *Daubert v. Merrell Dow Pharmaceuticals.* 113 S. Ct. 2786, 1993.

[4] S.N. Srihari, S.-H. Cha, H. Arora, and S. Lee, "Individuality of Handwriting: A Validation Study," *Proc. Sixth Int'l Conf. Document Analysis and Recognition,* pp. 106-109, Sept. 2001.

[5] *US v Byron Mitchell,* Criminal Action No. 96-407, US District Court for the Eastern District of Pennsylvania. July 1999.

[6] A. Newman, "Judge Rules Fingerprints Cannot Be Called a Match," *New York Times,* Jan. 2002.

[7] US Dept. of Justice document SL000386, Online: http://www.forensic-evidence.com/site/ID/ID_fpValidation.html, Mar. 2000.

[8] S.A. Cole, *Suspect Identities: A History of Fingerprint and Criminal Identification.* Harvard Univ. Press, May 2001.

[9] J.A. Rice, *Mathematical Statistics and Data Analysis,* second ed., Duxbury Press, 1995.

[10] A.K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An Identity Authentication System Using Fingerprints," *Proc. IEEE,* vol. 85, no. 9, pp. 1365-1388, 1997.

[11] Federal Bureau of Investigation. www.fbi.gov, 2002.

[12] A.K. Jain and S. Pankanti, "Biometrics Systems: Anatomy of Performance," *IEICE Trans. Fundamentals,* special issue on Biometrics, vol. E84-D, no. 7, pp. 788-799, 2001.
[13] 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.
[14] J. Osterburg, T. Parthasarathy, T.E.S. Raghavan, and S. L. Sclove, "Development of a Mathematical Formula for the Calculation of Fingerprint Probabilities Based on Individual Characteristics," *J. Am. Statistical Assoc.,* vol 72, no. 360, pp. 772-778, 1977.
[15] A.R. Roddy and J.D. Stosz, "Fingerprint Features—Statistical Analysis and System Performance Estimates" *Proc. IEEE,* vol. 85, no. 9, pp. 1390-1421, 1997.
[16] F. Galton, *Finger Prints.* London: McMillan, 1892.
[17] T. Roxburgh, "On Evidential Value of Fingerprints," *Sankhya: Indian J. Statistics,* vol. 1, pp. 189-214, 1933.
[18] K. Pearson, *The Life and Letters of Francis Galton,* vol IIIA. Cambridge UK: Cambridge Univ. Press, 1930.
[19] C. Kingston, "Probabilistic Analysis of Partial Fingerprint Patterns," PhD thesis, Univ. of California, Berkeley, 1964.
[20] E.R. Henry, *Classification and Uses of Fingerprints.* pp. 54-58, London: Routledge, 1900.
[21] V. Balthazard, "De lìdentification par les Empreintes Ditalis," *Comptes Rendus, des Academies des Sciences,* vol. 1862, no. 152, 1911.
[22] B. Wentworth and H.H. Wilder, *Personal Identification.* Boston: R.G. Badger, 1918.
[23] H. Cummins and C. Midlo, *Fingerprints, Palms and Soles.* Philadelphia: Blakiston, 1943.
[24] S.R. Gupta, "Statistical Survey of Ridge Characteristics," *Int'l Criminal Police Rev.,* vol. 218, no. 130, 1968.
[25] L. Amy, "Recherches sur L'identification des Traces Papillaries," *Annales de Medecine Legale,* vol. 28, no. 2, pp. 96-101, 1948.
[26] C. Champod and P.A. Margot, "Computer Assisted Analysis of Minutiae Occurrences on Fingerprints," *Proc. Int'l Symp. Fingerprint Detection and Identification,* J. Almog and E. Spinger, eds., pp. 305, 1996.
[27] S.L. Sclove, "The Occurrence of Fingerprint Characteristics as a Two Dimensional Process," *J. Am. Statistical Assoc.,* vol. 74, no. 367, pp. 588-595, 1979.
[28] D.A. Stoney, "A Quantitative Assessment of Fingerprint Individuality," Ph. D. thesis, Univ. of California, Davis, 1985.
[29] M. Trauring, "Automatic Comparison of Finger-Ridge Patterns," *Nature,* pp. 938-940, 1963.
[30] S.B. Meagher, B. Buldowle, and D. Ziesig, "50K Fingerprint Comparison Test," USA vs. Byron Mitchell, US District Court Eastern District of Philadelphia. Government Exhibits 6-8 and 6-9 in Daubert Hearing before Judge J. Curtis Joyner, July 1999.
[31] M.R. Stiles, "Goverment's Post-Daubert Hearing Memorandum," US District Court for the Eastern District of Pennsylvania, USA vs. Mitchell, Criminal case No. 96-00407, http://www. usao-edpa.com/Invest/Mitchell/704postd.htm, 2000.
[32] J.L. Wayman, "Daubert Hearing on Fingerprinting: When Bad Science Leads to Good Law: The Disturbing Irony of the Daubert Hearing in the Case of US v Byron C. Mitchell," http://www.engr.sjsu.edu/biometrics/publications_daubert.html, 2002.
[33] J. Daugman, "Recognizing Persons by Their Iris Patterns," *Biometrics: Personal Identification in Networked Society,* A.K. Jain, R. Bolle, and S. Pankanti, eds., Kluwer Academic, 1999.
[34] D.A. Stoney, "Distribution of Epidermal Ridge Minutiae," *Am. J. Physical Anthropology,* vol. 77, pp. 367-376, 1988.
[35] Identix Incorporated, www.identix.com, 2002.
[36] Digital Biometrics, Inc., now Visionics Corporation, www.visionics.com, 2002.
[37] Veridicom Inc., www.veridicom.com, 2002.
[38] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, and A.K. Jain, "*FVC2000:* Fingerprint Verification Competition," *Proc. 15th IAPR Int'l Conf. Pattern Recognition,* Sept. 2000. http://bias.csr.unibo.it/fvc2000/.
[39] A.K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-Based Fingerprint Matching," *IEEE Trans. Image Processing,* vol. 9, no. 5, pp. 846-859, May 2000.
[40] A.K. Jain, S. Prabhakar, and S. Pankanti, "Twin Test: On Discriminability of Fingerprints," *Proc. Third Int'l Conf. Audio- and Video-Based Person Authentication,* pp. 211-216, June 2001.

Sharath Pankanti is with the Exploratory Computer Vision and Intelligent Robotics Group, IBM T.J. Watson Research Center, Yorktown Heights, New York. From 1995-1999, he worked on the Advanced Identification Solutions Project dealing with reliable and scalable fingerprint identification systems for civilian applications. For the past few years, he has been working on analysis and interpretation of video depicting human activities. His research interests include biometrics, pattern recognition, computer vision, and human perception. He is a senior member of the IEEE and a member of the IEEE Computer Society.

Salil Prabhakar received the BTech degree in computer science and engineering from Institute of Technology, Banaras Hindu University, Varanasi, India, in 1996. During 1996-1997, he worked with IBM Global Services India Pvt. Ltd., Bangalore, India, as a software engineer. He received the PhD degree in computer science and engineering from Michigan State University, East Lansing, in 2001. He currently leads the Algorithms Research Group at DigitalPersona Inc., Redwood City, California, where he works on fingerprint-based biometric solutions. Dr. Prabhakar's research interests include pattern recognition, image processing, computer vision, machine learning, biometrics, data mining, and multimedia applications. He is coauthor of more than 15 technical publications and has two patents pending. He is a member of the IEEE and the IEEE Computer Society.

Anil K. Jain is a University Distinguished Professor in the Department of Computer Science and Engineering at Michigan State University. He was the department chair between 1995-1999. He has made significant contributions and published a large number of papers on the following topics: statistical pattern recognition, exploratory pattern analysis, neural networks, Markov random fields, texture analysis, interpretation of range images, 3D object recognition, document image analysis, and biometric authentication. Several of his papers have been reprinted in edited volumes on image processing and pattern recognition. He received best paper awards in 1987 and 1991 and received certificates for outstanding contributions in 1976, 1979, 1992, 1997, and 1998 from the Pattern Recognition Society. He also received the 1996 *IEEE Transactions on Neural Networks* Outstanding Paper Award. He is a fellow of the IEEE and International Association of Pattern Recognition (IAPR). He received a Fulbright Research Award in 1998 and a Guggenheim fellowship in 2001.