Altered Fingerprints: Analysis and Detection

Soweon Yoon, *Student Member*, *IEEE*, Jianjiang Feng, *Member*, *IEEE*, and
Anil K. Jain, *Fellow*, *IEEE*

Abstract—The widespread deployment of Automated Fingerprint Identification Systems (AFIS) in law enforcement and border control applications has heightened the need for ensuring that these systems are not compromised. While several issues related to fingerprint system security have been investigated, including the use of fake fingerprints for masquerading identity, the problem of fingerprint alteration or obfuscation has received very little attention. Fingerprint obfuscation refers to the deliberate alteration of the fingerprint pattern by an individual for the purpose of masking his identity. Several cases of fingerprint obfuscation have been reported in the press. Fingerprint image quality assessment software (e.g., NFIQ) cannot always detect altered fingerprints since the implicit image quality due to alteration may not change significantly. The main contributions of this paper are: 1) compiling case studies of incidents where individuals were found to have altered their fingerprints for circumventing AFIS, 2) investigating the impact of fingerprint alteration on the accuracy of a commercial fingerprint matcher, 3) classifying the alterations into three major categories and suggesting possible countermeasures, 4) developing a technique to automatically detect altered fingerprints based on analyzing orientation field and minutiae distribution, and 5) evaluating the proposed technique and the NFIQ algorithm on a large database of altered fingerprints provided by a law enforcement agency. Experimental results show the feasibility of the proposed approach in detecting altered fingerprints and highlight the need to further pursue this problem.

Index Terms—Fingerprints, AFIS, obfuscation, alteration, ridge pattern, minutiae distribution, image quality, fingerprintness.

1 Introduction

Fingerprint recognition has been successfully used by law enforcement agencies to identify suspects and victims for almost 100 years. Recent advances in automated fingerprint identification technology, coupled with the growing need for reliable person identification, have resulted in an increased use of fingerprints in both government and civilian applications such as border control, employment background checks, and secure facility access [2]. Examples of large-scale fingerprint systems in the US government arena include the US-VISIT's IDENT program [3] and the FBI's IAFIS service [4].

The success of fingerprint recognition systems in accurately identifying individuals has prompted some individuals to engage in extreme measures for the purpose of circumventing these systems. The primary purpose of fingerprint alteration [5] is to evade identification using techniques varying from abrading, cutting, and burning fingers to performing plastic surgery (see Fig. 1). The use of altered fingerprints to mask one's identity constitutes a serious "attack" against a border control biometric system since it defeats the very purpose for which the system was deployed in the first place, i.e., to identify individuals in a watch list.

It should be noted that *altered* fingerprints are different from *fake* fingerprints. The use of fake fingers—made of glue, latex, or silicone—is a well-publicized method to circumvent fingerprint systems. Altered fingerprints, however, are real fingers that are used to conceal one's identity in order to evade identification by a biometric system. While fake fingers are typically used by individuals to adopt another person's identity, altered fingers are used to mask one's own identity. In order to detect attacks based on fake fingers, many software [10] and hardware [11] solutions have been proposed. However, the problem of altered fingerprints has hitherto not been studied in the literature and there are no reported techniques to identify them. Furthermore, the lack of public databases comprised of altered fingerprint images has stymied research in this area. One of the goals of this paper is to highlight the importance of the problem, analyze altered fingerprints, and propose an automatic detection algorithm for them.

The aforementioned problem involving altered fingerprints falls under a broader category of attacks known as *biometric obfuscation*. Obfuscation can be defined as a deliberate attempt by an individual to mask his identity from a biometric system by altering the biometric trait prior to its acquisition by the system. Examples include mutilating the ridges of one's fingerprint by using abrasive material, perturbing the texture of the iris by wearing theatrical lenses, or altering facial attributes such as nose and lips via surgical procedures. In this study, we will concern ourselves with the problem of fingerprint obfuscation for the following reasons: 1) Fingerprint-based biometric systems are much more widespread for large-scale identification than any other biometric modality; 2) it is relatively easy to alter one's fingerprints using chemicals and abrasives compared to, say, one's iris or face, where a more elaborate surgical procedure may be

- *S. Yoon and A.K. Jain are with the Department of Computer Science and Engineering, Michigan State University, East Lansing, MI 48824. E-mail: {yoonsowo, jain}@cse.msu.edu.*
- *J. Feng is with the Department of Automation, Tsinghua University, Beijing 100084, China. E-mail: jfeng@tsinghua.edu.cn.*

Manuscript received 29 Nov. 2010; revised 30 Mar. 2011; accepted 8 May 2011.
Recommended for acceptance by M. Tistarelli.
For information on obtaining reprints of this article, please send e-mail to: tpami@computer.org, and reference. IEEECS Log Number TPAMI-2010-11-0911.
Digital Object Identifier no. 10.1109/TPAMI.2011.161.

0162-8828/12/$31.00 © 2012 IEEE Published by the IEEE Computer Society

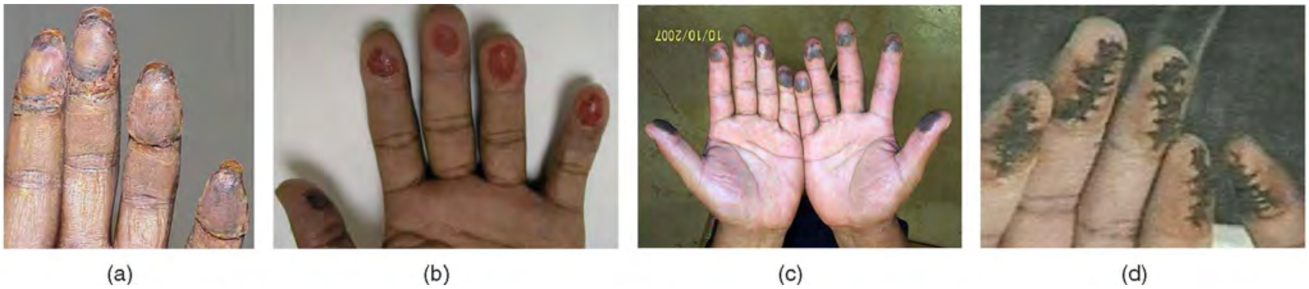


Fig. 1. Photographs of altered fingerprints. (a) Transplanted friction ridge skin from sole [6]. (b) Fingers that have been bitten [7]. (c) Fingers burnt by acid [8]. (d) Stitched fingers [9].

necessary; and 3) mutilated fingerprints are being routinely encountered by law enforcement and immigration officials in several countries, thereby underscoring the urgency of finding a solution to this problem.

Developing an automatic solution to detect altered fingerprints is the first step in defeating fingerprint alteration. Fingerprint quality assessment routines used in most fingerprint identification systems, such as the open source NFIQ (NIST Fingerprint Image Quality) software [12], may be useful in detecting altered fingerprints if the corresponding images are indeed of poor quality. But, not all altered fingerprint images have poor quality (see Figs. 10 and 11). Since existing fingerprint quality assessment algorithms [13] are designed to examine if an image contains sufficient information (say, minutiae) for matching, they have limited capability in determining if an image is a natural fingerprint or an altered fingerprint. For example, while the synthesized ridge pattern in Fig. 2 is not likely to appear on fingertips, it is declared to be of the best quality according to the NFIQ measure.[1]

Given that the altered fingerprints are likely to be encountered in large-scale national identification or border control systems, the automatic detector must satisfy the following three requirements:

1. Given the large throughput requirement of these systems, the algorithm must be extremely fast. In other words, it should not increase the computational burden of the matcher by any significant amount. State-of-the-art Automated Fingerprint Identification Systems (AFIS) can process fingerprints at the rate of about 1 million matches per second. This implies that the feature extraction and decision rule used to automatically detect altered fingerprints must be simple.
2. In operational scenarios, the number of individuals with altered fingerprints that will be encountered by AFIS will be very small. Keeping this in mind, the altered fingerprint detection algorithm should operate at a very small false positive rate, say 1 percent or lower. Subjects that are suspected to have altered fingerprints will go through a secondary inspection stage.
3. The altered fingerprint detector should be easily integrated into any AFIS.

The rest of the paper is organized as follows: Section 2 lists some of the cases where altered fingerprints were encountered by law enforcement agencies. In Section 3, the impact of the fingerprint alteration on the matching performance is investigated and three different categories of altered fingerprints and their potential countermeasures are described. The proposed approach for detecting altered fingerprints is presented in Section 4, and evaluated in Section 5. Finally, Section 6 proposes future directions for research on this topic.

2 Background

Fingerprint alteration has a long history. As early as 1933, Gus Winkler, a murderer and bank robber, was found to have altered the fingerprints of his left hand except for the thumb by slashing and tearing the flesh of the fingers [5]. Further, the pattern type of one finger was altered from double loop to left loop (see Fig. 3a).

In more recent cases, a man using the name Alexander Guzman, arrested by Florida officials in 1995 for possessing a false passport, was found to have obfuscated fingerprints (see Fig. 3b). After a two-week search based on manually reconstructing the damaged fingerprints and searching the FBI database containing 71 million records, the reconstructed fingerprints of Alexander Guzman were linked to the fingerprints of Jose Izquierdo who was an absconding drug criminal [15]. His fingerprint mutilation process consisted of three steps: Making a “Z” shaped cut on the fingertip, lifting and switching two triangular skin patches, and stitching them back. In September 2005, a drug dealer named Marc George was apprehended because his limping gait as a result of surgery caught the attention of border officials (see Fig. 1a) [16].

It is not just the criminals who have been found to alter their fingerprints. In December 2009, a woman successfully

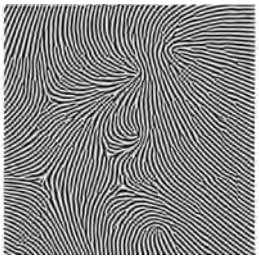


Fig. 2. NFIQ value for this synthetic ridge pattern (generated by iterative contextual filtering [14]) is 1, the highest quality level.

[1] NFIQ defines five quality levels in the range $[1, 5]$ with 1 indicating the highest quality.

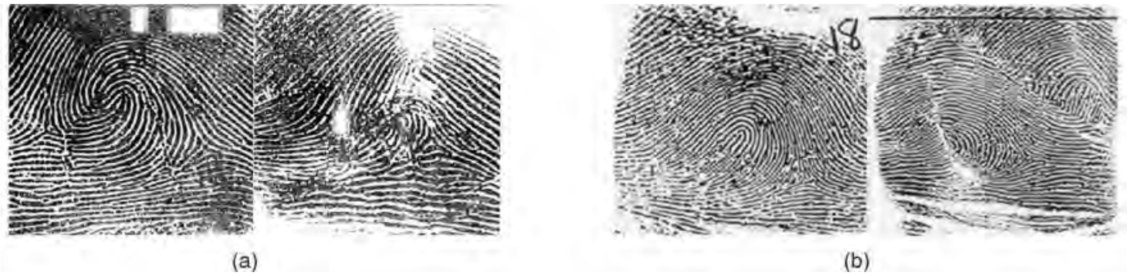


Fig. 3. Inked impressions before and after fingerprint alteration (a) of Gus Winkler [5] (pattern type is altered from double loop to left loop) and (b) of Jose Izquierdo [15] (altered by switching two parts of a "Z" shaped cut on the fingertip).

TABLE 1
High Profile Cases of Fingerprint Alteration

Case	Year	Alteration Type	Description
Criminal Cases			
Gus Winkler [5]	1933	Imitation	Pattern type was changed from double loop to left loop (Fig. 3a).
John Dillinger [16]	1934	Obliteration	Fingerprints were mutilated by applying acid.
Robert J. Philipps [16]	1941	Obliteration	Skin from the chest was transplanted to the fingertips.
Jose Izquierdo [15]	1997	Distortion	A fingerprint with strange pattern was formed by "Z" cut (Fig. 3b).
Marc George [16]	2005	Imitation	Friction ridge skin from sole was implanted to the fingertips (Fig. 1a).
A man arrested for vehicle theft [7]	2007	Obliteration	Fingers were bitten (Fig. 1b).
Mateo Cruz-Cruz [8]	2007	Obliteration	Fingerprints were blackened as a result of applying acid (Fig. 1c).
Gerald Perez [17]	2008	Obliteration	Fingertips with thick stitches (Fig. 1d).
Non-criminal Cases			
A woman at a border crossing [8]	2007	Obliteration	A surgery was performed on fingertips to generate strange fingerprint pattern.
A woman attempting to deceive the Taiwan border control system [18]	2008	Obliteration and Distortion	Thumbprints were altered by "Z" cuts and five other fingerprints were altered using a laser.
Asylum seekers to EU [19], [20]	2008	Obliteration	Fingertips were abraded and burned.
A woman attempting to evade the Japanese border control system [21]	2009	Imitation	Friction ridge skins from thumbs and index fingers were swapped between left and right hands.
Three people charged with conspiring to mutilate fingerprints [22]	2010	Obliteration	A physician, a broker, and a patient were involved in a scheme to mutilate or surgically remove the fingerprints to conceal illegal aliens from detection.

evaded the Japanese immigration AFIS by surgically swapping fingerprints of her left and right hands [21]. Although she was originally arrested for faking a marriage license, scars on her hands made the police suspicious.

Fingerprint alteration has even been performed at a much larger scale involving a group of individuals. It has been reported that hundreds of asylum seekers had cut, abraded, and burned their fingertips to prevent identification [19], [20] by EURODAC [23], a European Union-wide fingerprint system for identifying asylum seekers. Table 1 lists reported cases of fingerprint alteration.

Although the number of publicly disclosed cases of altered fingerprints is not very large, it is extremely difficult to estimate the actual number of individuals who have successfully evaded identification by fingerprint systems as a result of fingerprint alteration. Almost all the people identified as having altered their fingerprints were not detected by AFIS, but by some other means [16], [21].

3 Analysis of Altered Fingerprints

Based on a database of altered fingerprints made available to us by a law enforcement agency, we first 1) determine the impact of fingerprint alteration on the matching performance, 2) categorize altered fingerprints into three types[2]: *obliteration*, *distortion*, and *imitation* (see Figs. 9, 10, and 11), and 3) assess the utility of an existing fingerprint quality measure in terms of altered fingerprint detection.

3.1 Database

The database contains 4,433 altered fingerprints from 535 tenprint cards of 270 subjects.

- Not all of the 10 fingers in a tenprint card may have been altered. The distribution of the number of altered fingers in a card is shown in Fig. 4; in 57 percent of the tenprint cards all 10 fingerprints were altered; 85 percent of the tenprint cards have more than five altered fingerprints.
- The number of tenprint cards for a subject varies from 1 to 16; a total of 87 subjects out of the 270 subjects have multiple tenprint cards due to multiple arrests.
- For subjects with multiple tenprint cards, there exist 1,335 pairs of pre-altered (natural) and post-altered fingerprints. Fig. 5 shows an example of pre-altered and post-altered tenprint cards of a subject.

[2] While the categorization is exclusive, there is ambiguity in some cases.

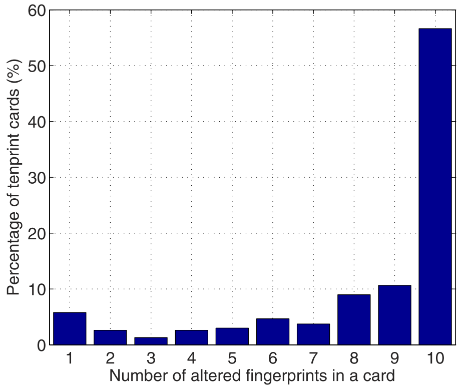


Fig. 4. Distribution of the number of altered fingerprints in tenprint cards in our database.

3.2 Vulnerability of Fingerprint Identification Systems

Fingerprint alteration is a serious threat to AFIS since it revokes one of the fundamental premise that fingerprint is persistent during one's lifetime. To understand the vulnerability of AFIS to fingerprint alteration, we used a commercial matcher, VeriFinger SDK 4.2 [24], to match 1,335 altered fingerprints to their mated pre-altered fingerprints. To establish a baseline, NIST SD4 database [25], which consists of 2,000 fingers with two impressions per finger, was used to obtain genuine and impostor match score distributions using VeriFinger SDK.[3]

Fig. 6 shows the score distributions for pre/post-altered fingerprint pair matches according to type and genuine and impostor matches in NIST SD4. The key observations here are:

1. The match score distributions of pre/post-altered fingerprint pairs for all alteration types follow the impostor score distribution.
2. Heavy tails in pre/post-altered match score distributions indicate that fingerprint alteration, as observed in our database, is not always successful in evading AFIS.
3. At a threshold of 41, which corresponds to 0 percent False Acceptance Rate (FAR) on NIST SD4, 83 percent of the pre/post-altered fingerprint pairs have genuine match scores below the threshold. This means that AFIS is unable to link most of the altered fingerprints to their true mates.

Fig. 7 shows examples where altering a fingerprint leads to failure in matching to its true mate. The process of fingerprint mutilation destroys the ridge structure itself so that minutiae extraction is not possible in this area (Fig. 7a). Also, severe ridge distortion, such as ridge structure transformation (Fig. 7b) or ridge deformation due to scars, alters the spatial distribution of the minutiae.

There is no guarantee that fingerprint alteration will always be successful in evading AFIS (see Fig. 8). As long as there are a sufficient number of minutiae that can be extracted in the unaltered area, pre/post-altered fingerprint mates can be successfully matched.

3.3 Types of Altered Fingerprints

We classify altered fingerprints into three categories based on the changes in ridge pattern due to alteration. This categorization will assist us in following manner: 1) Getting a better understanding of the nature of alterations that can be encountered, 2) detecting altered fingerprints by modeling well-defined subcategories, and 3) developing methods for altered fingerprint restoration.

Table 2 shows the exclusive categorization of 4,433 altered fingerprints in our database. Note that this classification is not based on the method of alteration, which is not known to us; it is subjective and is based on our examination of the ridge patterns in a large number of altered fingerprint images in the database.

3.3.1 Obliteration

Friction ridge patterns on fingertips can be obliterated by abrading [26], cutting [5], burning [18], [19], [20], [27], applying strong chemicals (Fig. 1c), and transplanting smooth skin [16]. Further factors such as skin disease (such as leprosy [28]) and side effects of a cancer drug [29] can also obliterate fingerprints. Friction ridge structure is barely visible within the obliterated region. According to Table 2, obliteration appears to be the most popular form of alteration. This may be because obliteration, which completely destroys ridge structures, is much simpler to perform than distortion/imitation, which requires a surgical procedure. Furthermore, detecting distorted or imitated fingerprints is much more difficult for human examiners than obliterated fingerprints.

Obliterated fingerprints can evade fingerprint quality control software, depending on the area of the damage. If the affected finger area is small, the existing fingerprint quality assessment softwares may fail to detect it as an altered fingerprint (the fingerprint in Fig. 9a has an acceptable NFIQ value of 3), but AFIS is likely to successfully match the damaged fingerprint to the original mated fingerprint (Fig. 8a). But, if the altered area is sufficiently large, fingerprint quality control software can easily detect the damage. For example, the obliterated fingerprint in Fig. 9b has the lowest NFIQ value of 5.

To identify individuals with severely obliterated fingerprints, it may be necessary to treat these fingerprints as latent images, perform AFIS search using manually marked features, and adopt an appropriate fusion scheme for tenprint search [30]. In rare cases, even if the finger surface is completely damaged, the dermal papillary surface, which contains the same pattern as the epidermal pattern, may be used for identification [31].

3.3.2 Distortion

Friction ridge patterns on fingertips can be turned into unnatural ridge patterns [9], [15], [32] by removing portions of skin from a fingertip and either grafting them back in different positions (Fig. 10a) or replacing them with friction ridge skin from the palm or sole (Fig. 10b). Distorted fingerprints have unusual ridge patterns which are not found in natural fingerprints. These abnormalities include

[3] Note that while the analysis is based on a specific fingerprint matcher, the results of fingerprint alteration are likely to affect all commercial matchers in a similar manner. VeriFinger, like other state-of-the-art fingerprint matchers, utilizes ridge pattern for matching, which is what the culprits are trying to change through fingerprint alteration.

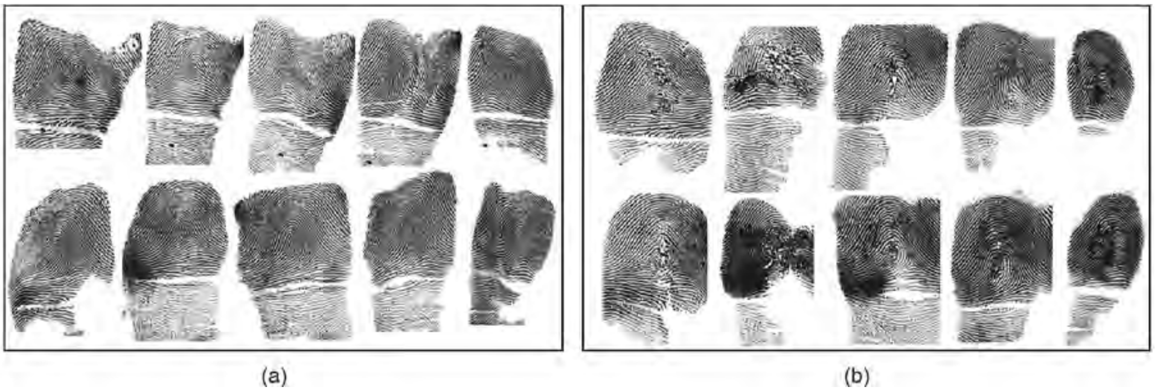


Fig. 5. Mated pre/post-altered tenprint cards from a subject. (a) Pre-altered fingerprints. (b) Post-altered fingerprints.

abnormal spatial distribution of singular points or abrupt changes in orientation field along the scars. Note that orientation field discontinuity in natural fingerprints is usually observed only at singular points.

Distorted fingerprints can also successfully pass the fingerprint quality test since their local ridge structure remains similar to natural fingerprints while their global ridge pattern is abnormal. For instance, a distorted fingerprint as a result of swapping skin patches within the same finger (e.g., Fig. 10a) retains the same ridge property (e.g., ridge frequency and width) over the entire fingerprint area. Fig. 10a is assigned the highest quality level, NFIQ of 1. Similarly, the altered fingerprint in Fig. 10b is assigned the second highest quality level, NFIQ $= 2$.

Fingerprints altered by "Z" cut are of special interest since they retain their original ridge structure, enabling reconstruction of the original fingerprint before alteration. Therefore, it is imperative to upgrade current fingerprint quality control software to detect the distorted fingerprints. Once detected, the following operations may be performed to assist AFIS: 1) identify unaltered regions of the fingerprint and manually mark the features (i.e., the minutiae) in these regions and 2) reconstruct the original fingerprint as in the "Z" cut case [15].

3.3.3 Imitation

Friction ridge patterns on fingertips can still preserve fingerprint-like pattern after an elaborate procedure of fingerprint alteration: 1) a portion of skin is removed and the remaining skin is pulled and stitched together (Fig. 11a), 2) friction ridge skin from other parts of the body is used to fill the removed part of the fingertip to reconcile with the remaining ridge structure (Fig. 11b), or 3) transplantation of the entire fingertip. As reported in [21], simply swapping the skin on fingertips between the left and right hands successfully evaded AFIS.

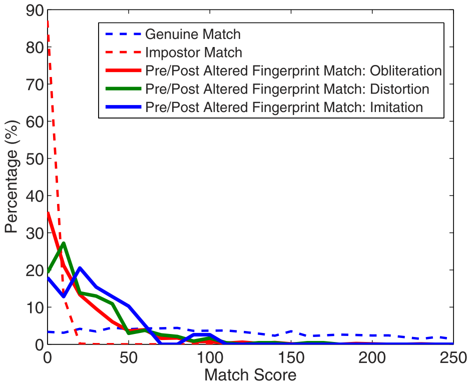


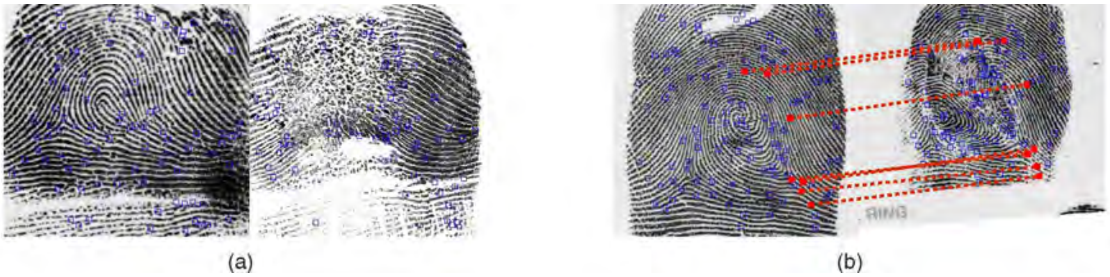
Fig. 6. Match score distributions of pre/post-alteration pairs according to type and genuine and impostor pairs in NIST SD4.

Imitated fingerprints can not only successfully pass the fingerprint quality assessment software, they can also confound human examiners. Fig. 11 shows pre-altered and post-altered fingerprint mates. The altered fingerprint in Fig. 11a has a very smooth orientation field over the entire fingerprint area (which looks like an arch-type fingerprint) and the only evidence of possible alteration is a thin scar. This fingerprint has the highest NFIQ value of 1. However, its pre-altered mate is indeed of right loop type, and the match score between this pair of fingerprints is only 19. Recall that the threshold on match score corresponding to 0 percent FAR of the matcher was 41. The altered fingerprint in Fig. 11b was generated by an exquisite surgical procedure to have very natural ridge flow even along the surgical scars. This fingerprint also has the highest NFIQ value of 1 with a match score between pre/post-altered fingerprint pair of only 28.

To match altered fingerprints in Fig. 11, matching algorithms that are robust to distortion and inconsistency need to be developed. In the case where fingerprints from different fingers are swapped, fingerprint matching without using finger position information (i.e., the left thumb is allowed to match to the right index finger) may help in determining the true identity at the expense of significantly higher matching time.

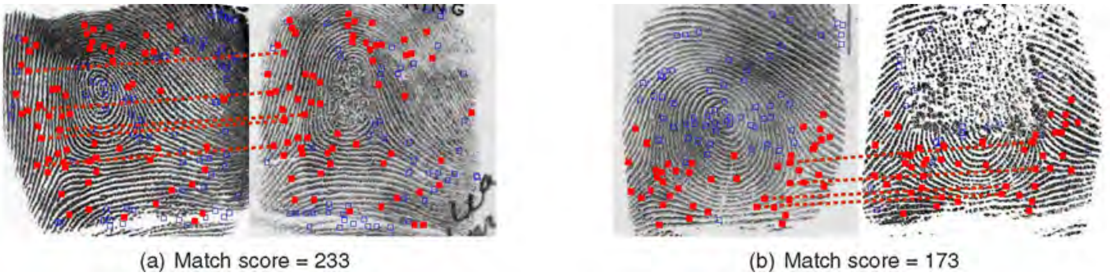
3.4 Effectiveness of Fingerprint Quality Assessment Algorithm

To learn the effectiveness of the commonly used fingerprint quality control softwares in detecting altered fingerprints, quality levels of altered fingerprints and natural fingerprints were estimated using the NFIQ software [12], which is the de facto standard of fingerprint quality. To construct a natural fingerprint database, we used the 27,000 fingerprints in NIST SD14 [33]. From the histograms of NFIQ values for altered and natural fingerprints shown in Fig. 12, we can observe that:



(a) (b)

Fig. 7. Examples where fingerprint alteration severely degrades the matching score with the pre-altered mates. (a) Mutilation over a large area. (b) Ridge transformation. These altered fingerprints have a match score of 0 with their true mates. All squares indicate minutiae extracted from the image and squares filled with red color represent matched minutiae between the pre/post-altered fingerprints.



(a) Match score = 233

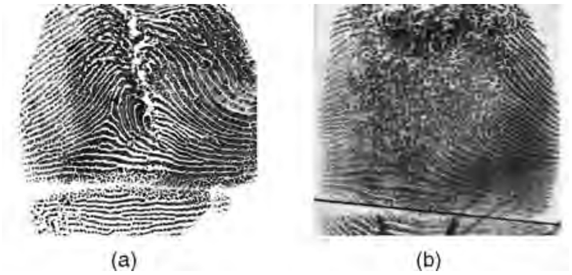
(b) Match score = 173

Fig. 8. Examples where the pre/post-altered fingerprint mates are correctly matched despite fingerprint alteration. (a) Alteration with a small damaged area and no ridge distortion. (b) Sufficient number of minutiae in the unaltered area even with severe fingerprint alteration. Only a few corresponding minutiae are connected with dotted lines.

1. A significant portion of altered fingerprints have the lowest quality level of 5 while only a small percentage of natural fingerprints have this lowest quality level. In particular, the obliterated fingerprints have the largest portion at the NFIQ level of 5. By contrast, the distorted and imitated fingerprints have relatively small portion at the level of 5.
2. A large number of altered fingerprints have good quality; about 7 percent of altered fingerprints have the highest quality level of 1 in total, and a significant portion of distorted and imitated fingerprints have the highest quality level.
3. If the NFIQ value of 5 is used as a criterion for detecting altered fingerprints, it will lead to a true

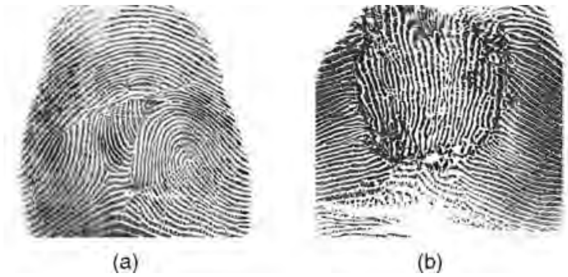
TABLE 2
Exclusive Categorization of the Altered Fingerprints into Three Types

Type	Obliteration		Distortion		Imitation
	Scar	Mutilation	Z-cut	Transplantation	
Number of Images	1,457	2,480	297	148	51



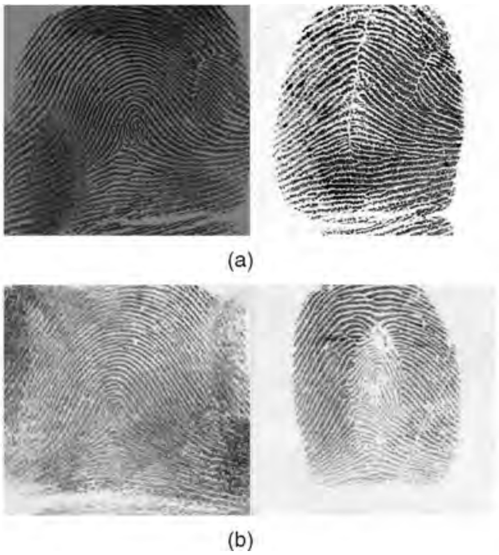
(a) (b)

Fig. 9. Fingerprint obliteration. Examples of (a) scar and (b) mutilation.



(a) (b)

Fig. 10. Fingerprint distortion. Examples of (a) transplantation within a finger by "Z" cut and (b) transplantation from other friction ridge skin, e.g., from the palm.



(a)

(b)

Fig. 11. Fingerprint imitation. Left: pre-altered fingerprint, and right: its post-altered fingerprint mate. (a) Removal of a portion of skin. (b) Exquisite transplantation from other friction ridge skin.

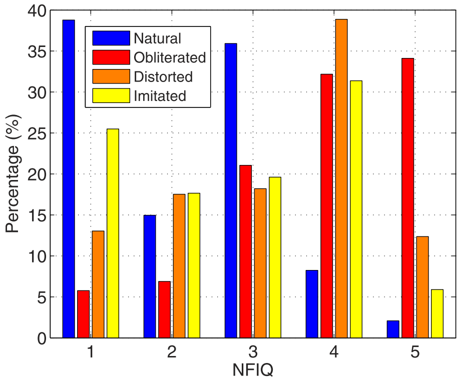


Fig. 12. Histograms of NFIQ values of 27,000 natural fingerprints in NIST SD14 and 4,433 altered fingerprints in our altered fingerprint database according to the type of alteration. Recall that $\mathrm{NFIQ} = 1$ indicates the highest quality.

positive (an altered fingerprint is correctly classified as an altered fingerprint) rate of 31.6 percent at a false positive (a natural fingerprint is misclassified as an altered fingerprint) rate of 2.1 percent.

4 Automatic Detection of Altered Fingerprints

In the previous section, we showed that the NFIQ algorithm is not suitable for detecting altered fingerprints, especially the distortion and imitation types. In fact, the distorted and imitated fingerprints are very hard to detect for any fingerprint image quality assessment algorithm that is based on analyzing local image quality. In this section, we consider the problem of automatic detection of alterations based on analyzing ridge orientation field and minutiae distribution. The flowchart of the proposed alteration detector is given in Fig. 13.

4.1 Analysis of Orientation Field

Orientation field[4] describes the ridge flow of fingerprints and is defined as the local ridge orientation in the range $[0, \pi)$. Good quality fingerprints have a smooth orientation field except near the singular points (e.g., core and delta). Based on this fact, many orientation field models have been developed by combining the global orientation field model for the continuous flow field of the fingerprint with the local orientation field model around the singular points [34], [35], [36]. The global orientation field model represents either arch-type fingerprints, which do not have any singularity, or the overall ridge orientation field except singularity in fingerprints. If the global orientation field model alone is used for orientation field approximation, the difference between the observed orientation field and the model will ideally be nonzero only around the singular points. On the other hand, for obfuscated fingerprints, the model fitting error is observed in the altered region as well. Thus, we use the difference between the observed orientation field extracted from the fingerprint image and the orientation field approximated by the model as a feature vector for classifying a fingerprint as natural fingerprint or altered one. The main steps of the proposed algorithm are described below:

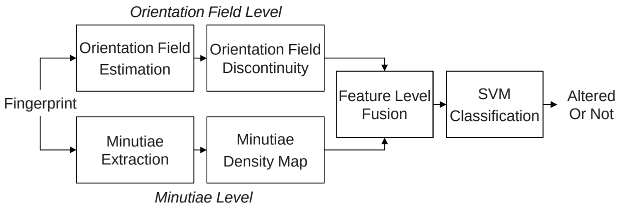


Fig. 13. Flowchart of the proposed algorithm.

1. Normalization. An input fingerprint image is normalized to 512×480 pixels by cropping a rectangular region of the fingerprint, which is located at the center of the fingerprint and aligned along the longitudinal direction of the finger, using the NIST Biometric Image Software (NBIS) [37]. This step ensures that the features extracted in the subsequent steps are invariant with respect to translation and rotation of finger.
2. Orientation field estimation. The orientation field of the fingerprint, $\theta(x, y)$, is computed using the gradient-based method [38]. The initial orientation field is smoothed by a 16×16 averaging filter, followed by averaging the orientations in 8×8 pixel blocks. A foreground mask is obtained by measuring the dynamic range of gray values of the fingerprint image in local blocks and morphological process for filling holes and removing isolated blocks is performed.
3. Orientation field approximation. The orientation field $\theta(x, y)$ is approximated by a polynomial model to obtain $\hat{\theta}(x, y)$.
4. Feature extraction. The error map, $\varepsilon(x, y)$, is computed as the absolute difference between $\theta(x, y)$ and $\hat{\theta}(x, y)$ and used to construct the feature vector.

More details of Steps 3 and 4 are given below.

4.1.1 Orientation Field Approximation

To represent the global orientation field, a set of polynomial functions is used, which is not only computationally efficient, but also provides a good approximation in orientation field modeling. Let $\theta(x, y)$ denote the orientation field. Then, the cosine and sine components of the doubled orientation at (x, y) can be represented by polynomials of order n:

$$g_c^n(x, y) \triangleq \cos 2\theta(x, y) = \sum_{i=0}^{n} \sum_{j=0}^{i} a_{i,j} x^j y^{i-j}, \tag{1}$$

$$g_s^n(x, y) \triangleq \sin 2\theta(x, y) = \sum_{i=0}^{n} \sum_{j=0}^{i} b_{i,j} x^j y^{i-j}, \tag{2}$$

where $a_{i,j}$ and $b_{i,j}$ are the polynomial coefficients for $g_c^n(x, y)$ and $g_s^n(x, y)$, respectively.

As the order of the polynomials increases, the model becomes more flexible in representing abrupt changes in the orientation field. When the order of the polynomial model is too low, the orientation field approximated by the model is quite different from the true orientation field. However, the order of the polynomial model does not need to be very

[4] Orientation field is often called ridge flow.

high; polynomial models with 6 or higher order do not make a significant difference in the fitting results. Thus, we select the order of the polynomial model as 6 ($n = 6$).

Using the orientation field $\theta(x, y)$ obtained in Step 2, the polynomial coefficients $a_{i,j}$ and $b_{i,j}$ can be estimated by the least squares method. For simplicity, we represent (1) and (2) in matrix form:

$$g_c(x, y) = \mathbf{x}^T\mathbf{a}, \quad g_s(x, y) = \mathbf{x}^T\mathbf{b}, \tag{3}$$

where $\mathbf{x} = [1 \;\; x \;\; y \;\; x^2 \; xy \;\; y^2 \;\; \cdots \;\; x^n \;\; \cdots \;\; y^n]^T$, and $\mathbf{a}$ and $\mathbf{b}$ are the corresponding coefficient vectors. The problem of estimating $\mathbf{a}$ and $\mathbf{b}$ can be formulated as

$$\hat{\mathbf{a}} = \arg\min_{\mathbf{a}} \|\mathbf{g}_c - \mathbf{X}\mathbf{a}\|^2, \quad \hat{\mathbf{b}} = \arg\min_{\mathbf{b}} \|\mathbf{g}_s - \mathbf{X}\mathbf{b}\|^2, \tag{4}$$

where

$$\mathbf{g}_c = \begin{bmatrix} g_c(x_1, y_1) \\ g_c(x_2, y_2) \\ \vdots \\ g_c(x_N, y_N) \end{bmatrix}, \mathbf{g}_s = \begin{bmatrix} g_s(x_1, y_1) \\ g_s(x_2, y_2) \\ \vdots \\ g_s(x_N, y_N) \end{bmatrix}, \text{ and } \mathbf{X} = \begin{bmatrix} \mathbf{x}_1^T \\ \mathbf{x}_2^T \\ \vdots \\ \mathbf{x}_N^T \end{bmatrix},$$

from N observations of $\theta(x, y)$, where $(x, y) \in \mathbf{R}$, $\mathbf{R} = \{(x, y)\text{: } (x, y) \text{ in foreground}\}$.

Finally, the orientation field approximated by the polynomial model, $\hat{\theta}(x, y)$, is obtained by

$$\hat{\theta}(x, y) = \frac{1}{2}\tan^{-1}\left(\frac{\hat{g}_s(x, y)}{\hat{g}_c(x, y)}\right), \tag{5}$$

where $\hat{g}_c(x, y) = \mathbf{x}^T\hat{\mathbf{a}}$ and $\hat{g}_s(x, y) = \mathbf{x}^T\hat{\mathbf{b}}$.

4.1.2 Feature Extraction

While the low-order polynomial model can adequately represent smooth (global) changes in the orientation field, it cannot accurately model the abrupt changes in the orientation field in local areas, e.g., around the cores and deltas in natural fingerprints. One of the observed characteristics of altered fingerprints is that their ridge flow can be discontinuous in nonsingular regions as well, such as severely scarred areas (Fig. 9a), mutilated areas (Fig. 9b), and distorted ridge areas (Figs. 10a and 10b). The difference between the observed orientation field and the modeled orientation field indicates the locations and the amount of the abrupt changes in the ridge flow.

We define the error map $\varepsilon(x, y)$ as

$$\varepsilon(x, y) = \min(|\theta(x, y) - \hat{\theta}(x, y)|, \pi - |\theta(x, y) - \hat{\theta}(x, y)|)/(\pi/2). \tag{6}$$

Fig. 14 shows the error maps of a natural fingerprint and four different altered fingerprints. The size of the error map is in the size of 60×60 blocks after removing two columns from each side of the error map.

The feature vector from the error map consists of histograms of local spatial regions [39]. The error map is divided into 3×3 cells, where each cell is of size 20×20 blocks. Histogram of the error map in each cell is computed in 21 bins in the range $[0, 1]$, and the histograms from all the nine cells result in a 189-dimensional feature vector.

4.2 Analysis of Minutiae Distribution

A minutia in the fingerprint indicates ridge characteristics such as ridge ending or ridge bifurcation. Almost all fingerprint recognition systems use minutiae for matching. In addition to the abnormality observed in orientation field, we also noted that minutiae distribution of altered fingerprints often differs from that of natural fingerprints.

Based on the minutiae extracted from a fingerprint by the open source minutiae extractor in NBIS, a minutiae density map is constructed by using the Parzen window method with uniform kernel function. Let $\mathbf{S_m}$ be the set of minutiae of the fingerprint, i.e.,

$$\mathbf{S_m} = \{\mathbf{x} | \mathbf{x} = (x, y) \text{ is the position of minutia}\}.$$

Then, the minutiae density map from $\mathbf{S_m}$ is computed as follows:

1. Initial estimation. The initial minutiae density map, $M_d(\mathbf{x})$, is obtained by

$$M_d(\mathbf{x}) = \sum_{\mathbf{x_0} \in \mathbf{S_m}} K_r(\mathbf{x} - \mathbf{x_0}), \tag{7}$$

   where $K_r(\mathbf{x} - \mathbf{x_0})$ is a uniform kernel function centered at $\mathbf{x_0}$ with radius r (r is set to 40 pixels).
2. Low-pass filtering. $M_d(x, y)$ is smoothed by a Gaussian filter of size 30×30 pixels with a standard deviation of 10 pixels.
3. Normalization. $M_d(x, y)$ is transformed to lie in the interval $[0, 1]$ by

$$M_d(x, y) = \begin{cases} M_d(x, y)/T, & \text{if } M_d(x, y) \le T, \\ 1, & \text{otherwise,} \end{cases} \tag{8}$$

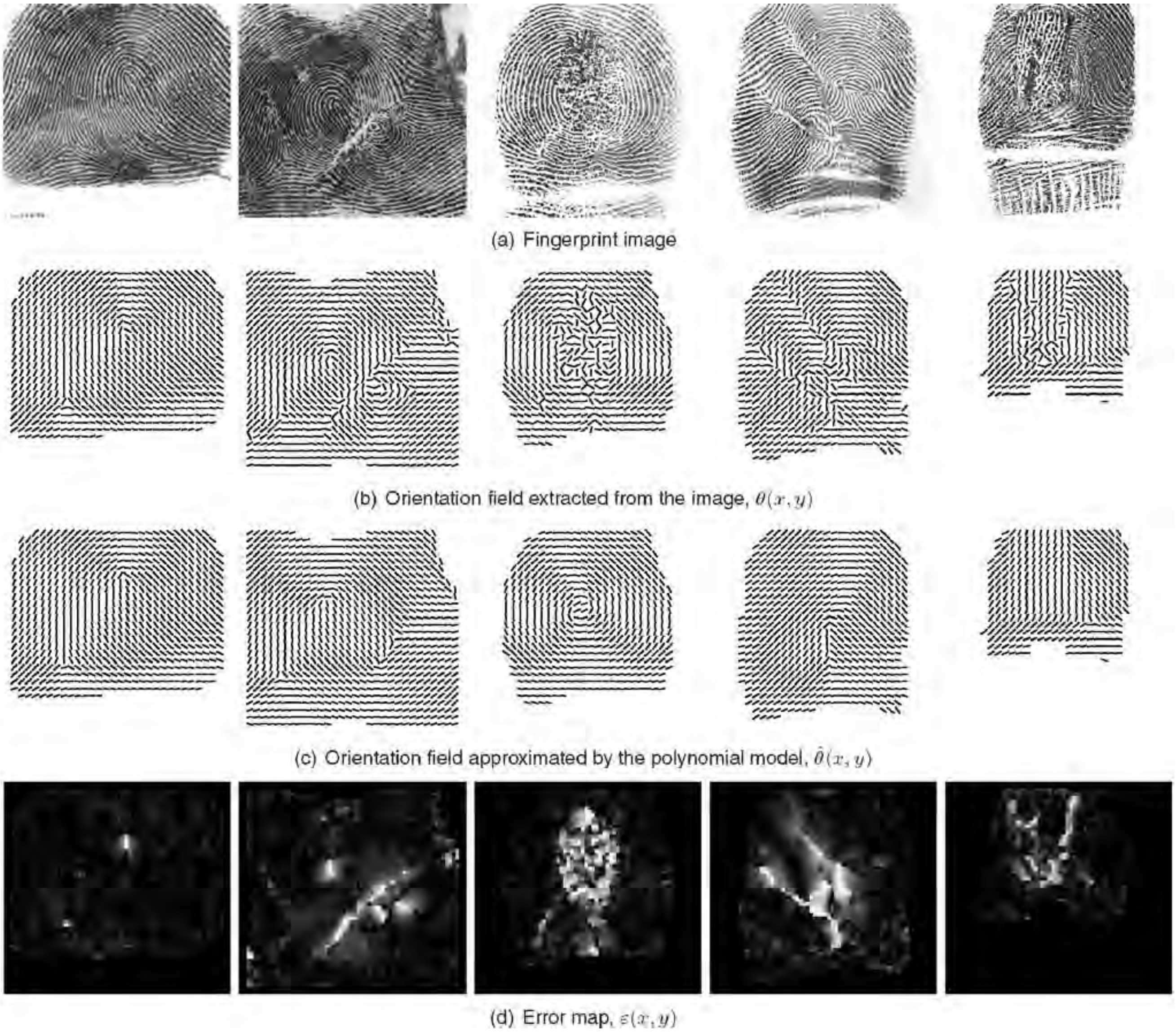
   where T is a predetermined threshold.

Fig. 15 shows the minutiae density maps of a natural and three altered fingerprints. In the natural fingerprint, minutiae are well spread and distributed almost uniformly. In the altered fingerprints, on the other hand, the distributions of minutiae are quite different: 1) Many spurious minutiae are extracted along scars and in the obliterated region due to ridge discontinuity, and 2) an excessive number of minutiae appear when a new ridge-like pattern is formed after alteration. These examples demonstrate that minutiae distribution can be useful for detecting altered fingerprints.

The feature vector from the minutiae density map is also constructed by local histograms in 3×3 cells. Then, the feature vectors from the orientation field discontinuity map and the minutiae density map are combined by concatenating local histograms in each cell and fed into a support vector machine (SVM) for classification.

5 Experiments

The proposed algorithm was evaluated at two levels: finger level (one finger) and subject level (all 10 fingers). At the finger level, we evaluate the performance of distinguishing between natural and altered fingerprints. At the subject level, we evaluate the performance of distinguishing between subjects with natural fingerprints and those with altered fingerprints. Since most AFIS used



(a) Fingerprint image

(b) Orientation field extracted from the image, $\theta(x, y)$

(c) Orientation field approximated by the polynomial model, $\hat{\theta}(x, y)$

(d) Error map, $\varepsilon(x, y)$

Fig. 14. Orientation field discontinuity. Column 1: Natural fingerprint (NIST SD14, F0000001). Column 2: Scarred fingerprint. Column 3: Mutilated fingerprint. Column 4: Distorted fingerprint by "Z" cut. Column 5: Distorted fingerprint by transplantation from other friction ridge skin.

in law enforcement, national ID, and border control applications process all 10 fingerprints of a person, the subject level performance utilizes this information of the application domain.

5.1 Finger-Level Evaluation

The altered fingerprint database available to us contains 4,433 fingerprints from 535 tenprint cards. For a nonaltered fingerprint database, we use 27,000 fingerprints from the 2,700 tenprint cards in the NIST SD14 [33]. This database contains two impressions for each finger, called file and search; the file impression is used in our experiments.

LIBSVM [40] with radial basis kernel function is used for classification with 10-fold cross-validation. The scores output by LIBSVM are linearly scaled to the range $[0, 1]$. The normalized score is termed a measure of the *fingerprintness* of the input fingerprint. When the fingerprintness of an input image is smaller than a predetermined threshold value, the system raises an alarm to indicate that the image is a possible altered fingerprint. If this image is indeed an altered fingerprint, it is deemed to be a true positive; otherwise, it is deemed to be a false positive. Similarly, true negative indicates that a natural fingerprint is correctly classified as natural and false negative indicates that an altered fingerprint is not detected as altered.

The Receiver Operating Characteristic (ROC) curves of the proposed approach and the NFIQ software for detecting altered fingerprints are given in Fig. 16. At the false positive rate of 2.1 percent, where natural fingerprints in NIST SD14 with the NFIQ value of 5 are determined as altered fingerprints, the proposed algorithm attains a 70.2 percent true positive rate while the true positive rate of the NFIQ is only 31.6 percent. Fig. 16a shows the ROC curves of three approaches for detecting altered fingerprints (orientation field discontinuity, minutiae distribution, and their feature level fusion) and the NFIQ algorithm. Fig. 16b shows the ROC curves of the proposed fusion algorithm and the NFIQ algorithm according to alteration type. Both obliterated and distorted fingerprints can be detected by the proposed algorithm at similar accuracy, while NFIQ can only identify

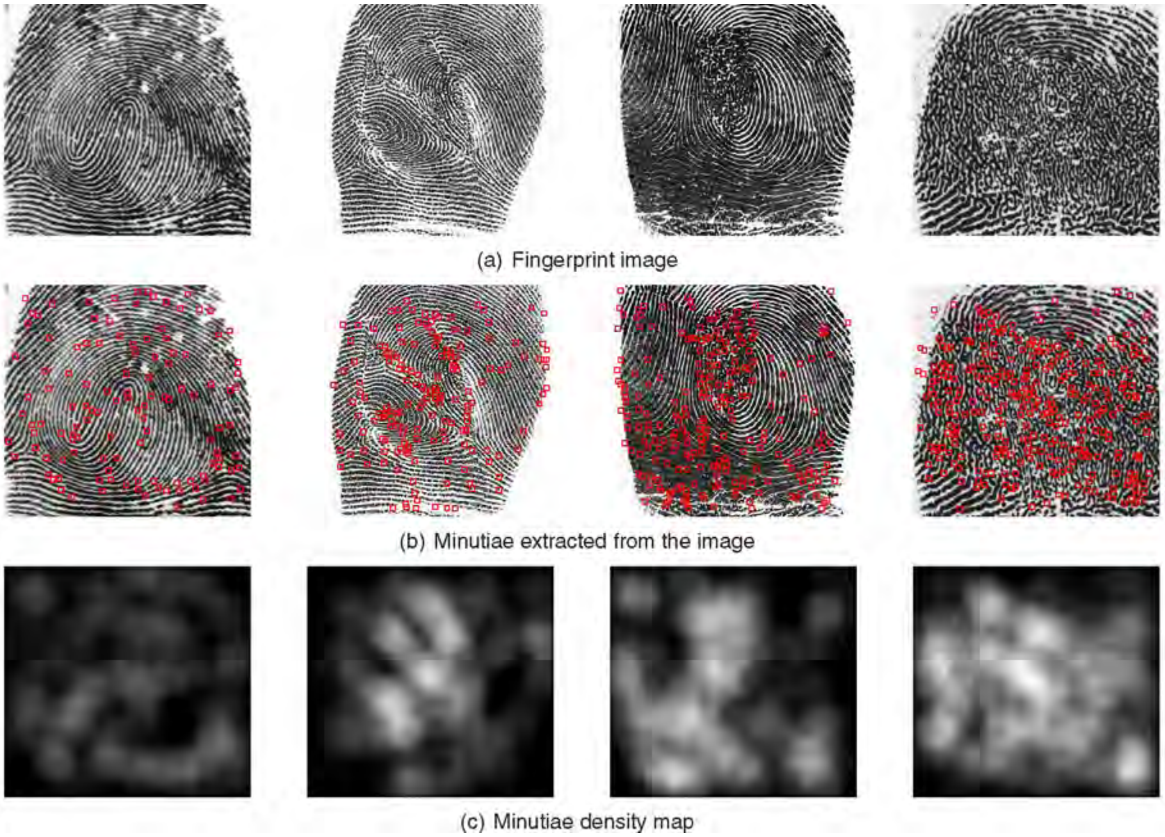


Fig. 15. Minutiae density map. Column 1: Natural fingerprint (NIST SD14, F0001826). Column 2: Distorted fingerprint with dense minutiae along scars. Column 3: Obliterated fingerprint with dense minutiae distribution in the altered area. Column 4: Obliterated fingerprint with dense minutiae distribution over the entire altered area due to ridge-like pattern formed by alteration. Note that the minutiae density maps are scaled to the same gray scale range.

obliterated cases. On the other hand, imitated fingerprints are challenging for both algorithms.

At the false positive rate of 1 percent (which means 270 fingerprints among the 27,000 in NIST SD14 would be misclassified as altered fingerprints), the threshold value for fingerprintness score is 0.60. Fig. 17 shows examples of successfully detected alterations using the proposed algorithm even though the NFIQ measure assigns acceptable quality level to these images.

Not all of the altered fingerprints can be detected by the proposed algorithm. If the altered area is too small (Fig. 18a), the evidence of alteration is difficult to detect. In the imitation case, the ridge structure is very natural even at the boundary of altered region; the orientation field is continuous and there is insignificant abnormality in minutiae density along scars (Fig. 18b).

The main reasons for false positive cases are: 1) poor image quality, leading to incorrect fingerprint feature

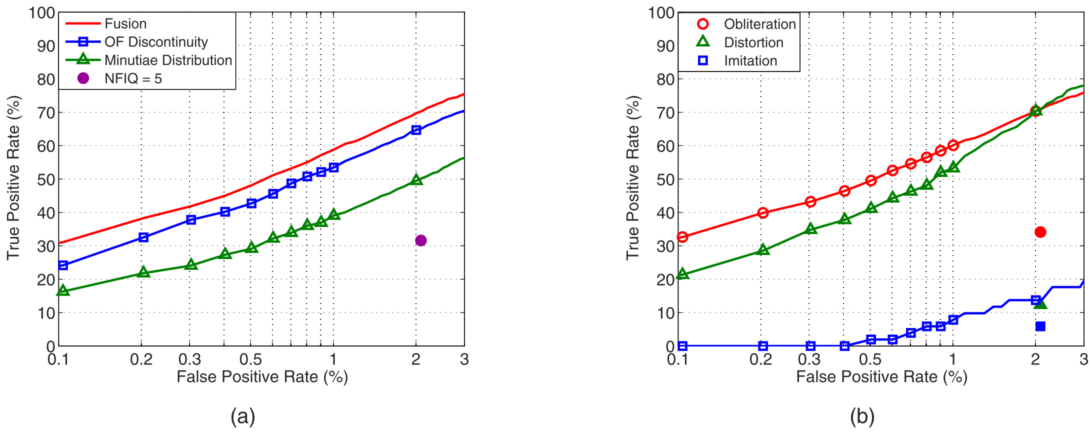


Fig. 16. ROC curves of the proposed algorithm and the NFIQ criterion in detecting altered fingerprints. (a) The ROC curves of the three approaches in the proposed algorithm and the NFIQ algorithm. (b) The ROC curves of the proposed fusion algorithm and the NFIQ algorithm for each type of altered fingerprints. The ROC curve of the NFIQ criterion is shown as a set of points (only one point is visible in the range of false positive rate plotted here) because its output can only take one of the five quality levels.

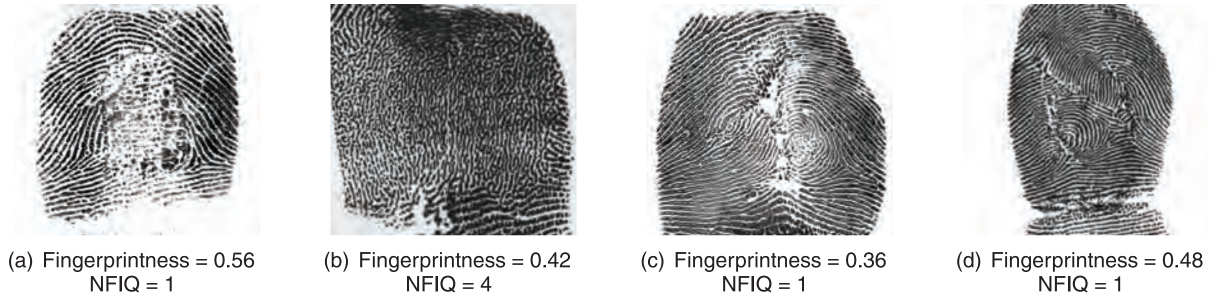

(a) Fingerprintness = 0.56 NFIQ = 1
(b) Fingerprintness = 0.42 NFIQ = 4
(c) Fingerprintness = 0.36 NFIQ = 1
(d) Fingerprintness = 0.48 NFIQ = 1

Fig. 17. True positive detection cases by (a) Orientation field discontinuity. (b) Minutiae distribution. (c) and (d) Fusion of both approaches.

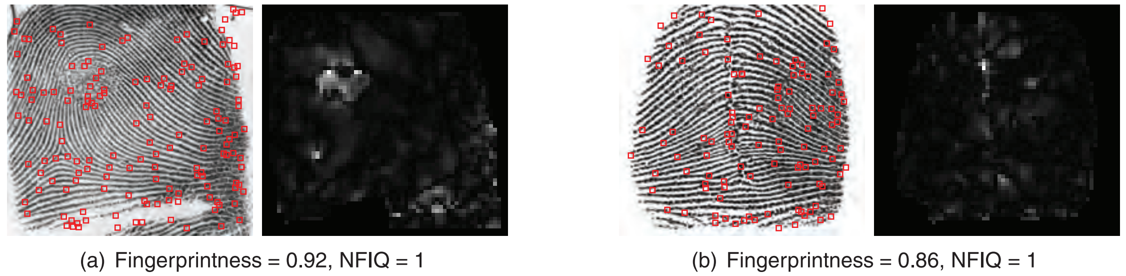

(a) Fingerprintness = 0.92, NFIQ = 1
(b) Fingerprintness = 0.86, NFIQ = 1

Fig. 18. False negative examples of the proposed algorithm. Minutiae and orientation field discontinuities of each example are shown. (a) Fingerprint with small altered area. (b) Imitated fingerprint. Note that NFIQ also fails to detect these two altered fingerprints.

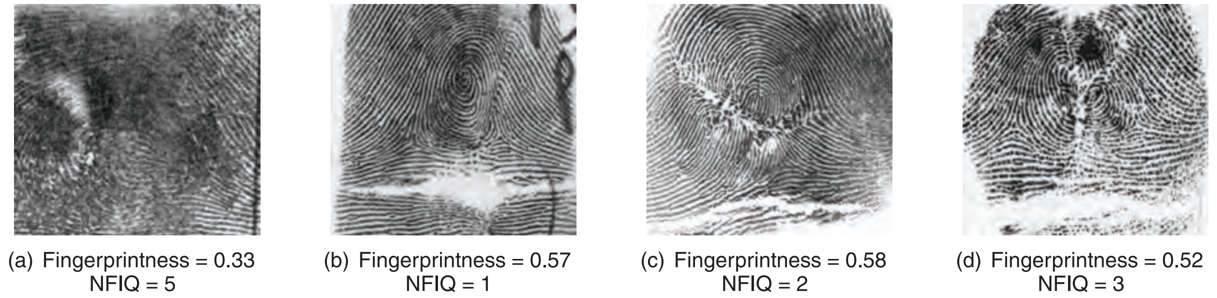

(a) Fingerprintness = 0.33 NFIQ = 5
(b) Fingerprintness = 0.57 NFIQ = 1
(c) Fingerprintness = 0.58 NFIQ = 2
(d) Fingerprintness = 0.52 NFIQ = 3

Fig. 19. False positive examples of the proposed algorithm. Poor ridge patterns: (a) NIST SD14, F0010811. Possibly altered fingerprints: (b) F0019979, (c) F0002962, (d) F0018103.

extraction (see Fig. 19a), and 2) ground truth error; some of the fingerprints in NIST SD14 may possibly have been altered (see Figs. 19b, 19c, and 19d)! Table 3 shows the NFIQ distribution of the false positive examples found by the proposed algorithm at the false positive rate of 1 percent. Most of the false positive images have NFIQ of 4 or 5. Note that it is acceptable to raise alarms on poor quality fingerprints since 1) poor quality images need to be manually checked and 2) criminals may purposely present poor quality fingerprints to the fingerprint system to evade identification [41]. All three false positive cases with $\mathrm{NFIQ} = 1$ or 2 appear to have been altered (two of them are shown in Figs. 19b and 19c).

5.2 Subject-Level Evaluation

In our altered fingerprint database, we observed that when a person resorts to fingerprint alteration, he tries to alter as many fingers as possible (Fig. 4). This makes sense since large-scale AFIS applications typically use a fusion of match scores from all 10 fingerprints for identification. So, altering just one or two fingerprints is not likely to change the identification decision. Based on this observation, we use the following decision level fusion rule to perform the subject level detection for altered fingerprints. When six or more fingerprints are detected as altered, the subject is claimed to have altered fingerprints. Subjects with fewer than six altered fingerprints are not considered as a threat to AFIS since even five (out of 10) natural fingerprints are generally sufficient for reliable identification.

For the subject level evaluation, 453 tenprint cards with more than five altered fingerprints and 2,700 tenprint cards in NIST SD14 are used. Fig. 20 shows the ROC curves of the proposed algorithm (including three approaches) as well as the NFIQ criterion for detecting subjects with altered fingerprints. At a false positive rate of 0.3 percent, where the NFIQ criterion determines subjects with six or more fingerprints of $\mathrm{NFIQ} = 5$ in NIST SD14 as people who altered the fingerprints, the proposed algorithm attains a true positive rate of 66.4 percent, while the NFIQ criterion obtains a 26.5 percent true positive rate.

Fig. 21 shows an example of a tenprint card where the subject level decision is successful. Even though one altered

TABLE 3
NFIQ Distribution for False Positives Detected at the Rate of 1 Percent by the Proposed Algorithm

NFIQ Value	1	2	3	4	5
Number of Images	2	1	39	145	83

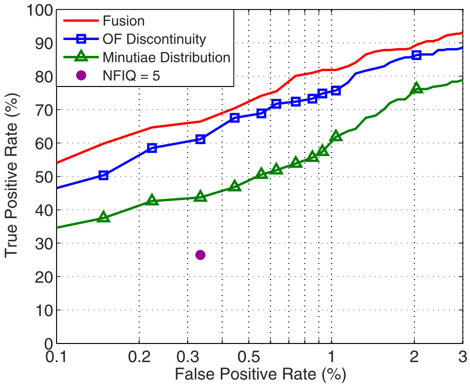


Fig. 20. ROC curves of the proposed algorithm (including three approaches) and the NFIQ criterion for detecting altered fingerprints at subject level.

finger is not correctly detected due to the smoothness of the orientation field and the absence of abnormality in minutiae distribution in altered area, our subject level fusion algorithm still flags this person because as many as nine fingers are determined to be altered.

Fusion of multiple fingerprints also helps to reduce the false positive for a person who either did not alter his fingerprints or simply has one or two fingerprints that appear to have been altered due to accidents or occupational reasons. Fig. 22 shows one such example. In this case, however, the NFIQ criterion will falsely raise an alarm for this subject since six of the 10 fingerprints are assigned the NFIQ value of 5.

We also have access to a small altered fingerprint database (254 images) from another government agency. This database has larger variance in terms of image format such as compression method, image resolution, and image type (single finger impressions, slap impressions, and tenprint cards). As a result, we report the detection performance on this database separately. We trained an SVM using all of the 4,433 images in our first altered fingerprint database and tested on this second small database. The same NFIQ criterion was also used as a comparison. At the false positive rate of 2.1 percent, the proposed algorithm shows a 33.1 percent true positive rate compared to 9.4 percent for the NFIQ criterion.

6 Conclusions and Future Work

The success of AFIS and their extensive deployment all over the world have prompted some individuals to take extreme measures to evade identification by altering their fingerprints. The problem of fingerprint alteration or obfuscation is very different from that of fingerprint spoofing, where an individual uses a fake fingerprint in order to adopt the identity of another individual. While the problem of spoofing has received substantial attention in the literature, the problem of obfuscation has not been addressed in the biometric literature, in spite of numerous documented cases of fingerprint alteration for the purpose of evading identification. While obfuscation may be encountered with

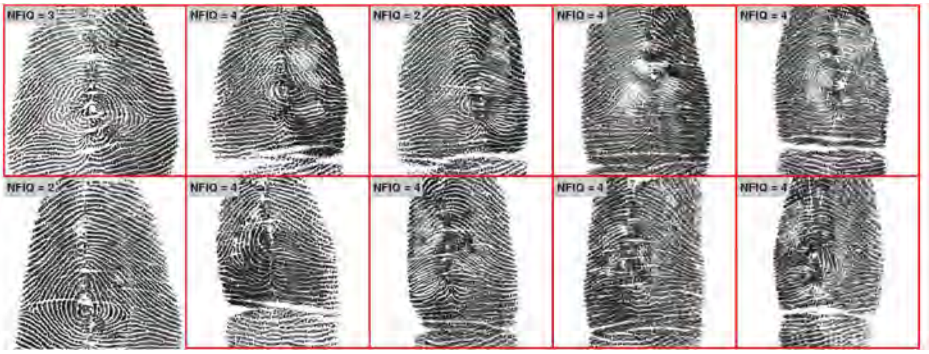


Fig. 21. True positive example of detection at subject level by the proposed algorithm. Although one of the altered fingerprints was not detected, this subject is still detected as having altered fingerprints with high confidence since the other nine fingerprints (boxed fingerprints) are correctly detected as altered. None of the 10 fingerprints is detected as altered using the NFIQ criterion.

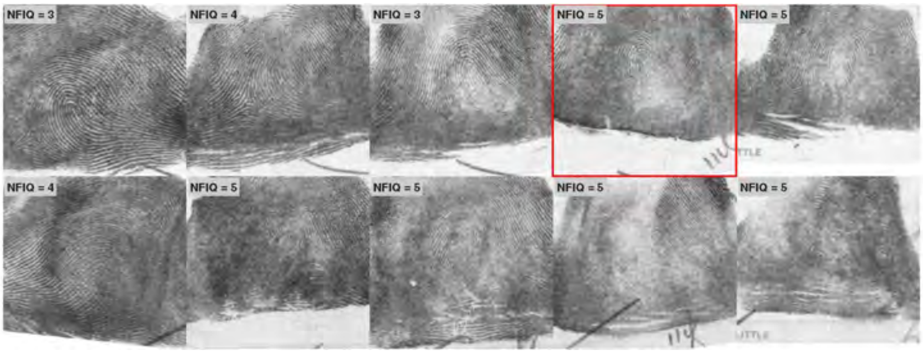


Fig. 22. True negative example at subject level identified by the proposed algorithm (NIST SD14, F0000121-F0000130). This subject can pass our alteration detector since the nine fingerprints are determined to be natural fingerprints by the proposed algorithm. However, the NFIQ criterion raises a false alarm for this subject since six of the fingerprints have the NFIQ value of 5.

other biometric modalities (such as face and iris), this problem is especially significant in the case of fingerprints due to the widespread deployment of AFIS in both government and civilian applications and the ease with which fingerprints can be obfuscated.

We have introduced the problem of fingerprint alteration and conducted a quantitative analysis of the threat of altered fingerprints to a commercial fingerprint matcher. We also evaluated the capability of a well-known fingerprint image quality assessment software, NFIQ, for detecting altered fingerprints. Since the NFIQ has limited ability in distinguishing altered fingerprints from natural fingerprints, we developed an algorithm to automatically detect altered fingerprints based on the characteristics of the fingerprint orientation field and minutiae distribution. The proposed algorithm based on the features extracted from the orientation field and minutiae satisfies the three essential requirements for alteration detection algorithm: 1) fast operational time, 2) high true positive rate at low false positive rate, and 3) ease of integration into AFIS. The proposed algorithm and the NFIQ criterion were tested on a large public domain fingerprint database (NIST SD14) as natural fingerprints and an altered fingerprint database provided by a law enforcement agency. At a false positive rate of 0.3 percent, the proposed algorithm can correctly detect 66.4 percent of the subjects with altered fingerprints, while 26.5 percent of such subjects are detected by the NFIQ algorithm.

This study can be further extended along the following directions:

1. Determine the alteration type automatically so that appropriate countermeasures can be taken.
2. Reconstruct altered fingerprints. For some types of altered fingerprints where the ridge patterns are damaged locally or the ridge structure is still present on the finger but possibly at a different location, reconstruction is indeed possible.
3. Match altered fingerprints to their unaltered mates. A matcher specialized for altered fingerprints can be developed to link them to unaltered mates in the database utilizing whatever information is available in the altered fingerprints.
4. Use multibiometrics [42] to combat the growing threat of individuals evading AFIS. Federal agencies in the United States have adopted or are planning to adopt multibiometrics in their identity management systems (the FBI's NGI [43] and DoD's ABIS [44]). However, other biometric traits can also be altered successfully. It has been reported that plastic surgery can significantly degrade the performance of face recognition systems [45] and that cataract surgery can reduce the accuracy of iris recognition systems [46]. To effectively deal with the problem of evading identification by altering biometric traits, a systematic study of possible alteration approaches for each major biometric trait is needed.

ACKNOWLEDGMENTS

The authors would like to acknowledge the support of Morpho during the course of this research. An early version of this research [1] was supported by a grant from the NSF Center for Identification Technology Research (CITeR). The authors would like to thank John Manzo of the FBI and Laura Tierney and Arun Vemury of the DHS for providing access to the altered fingerprint images. Part of Anil Jain's research was supported by the WCU (World Class University) program funded by the Ministry of Education, Science and Technology through the National Research Foundation of Korea (R31-10008). All correspondence should be directed to Anil K. Jain.

REFERENCES

[1] J. Feng, A.K. Jain, and A. Ross, "Detecting Altered Fingerprints," *Proc. 20th Int'l Conf. Pattern Recognition*, pp. 1622-1625, Aug. 2010.
[2] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition,* second ed. Springer-Verlag, 2009.
[3] The U.S. Department of Homeland Security, US-VISIT, http://www.dhs.gov/usvisit, 2011.
[4] The Fed. Bureau of Investigation (FBI), Integrated Automated Fingerprint Identification System (IAFIS), http://www.fbi.gov/hq/cjisd/iafis.htm, 2011.
[5] H. Cummins, "Attempts to Alter and Obliterate Finger-prints," *J. Am. Inst. Criminal Law and Criminology,* vol. 25, pp. 982-991, 1935.
[6] Surgically Altered Fingerprints, http://www.clpex.com/images/FeetMutilation/L4.JPG, 2011.
[7] K. Singh, Altered Fingerprints, http://www.interpol.int/Public/Forensic/fingerprints/research/alteredfingerprints.pdf, 2008.
[8] M. Hall, "Criminals Go to Extremes to Hide Identities," *USA Today,* http://www.usatoday.com/news/nation/2007-11-06-criminal-extreme_N.htm, Nov. 2007.
[9] Criminals Cutting off Fingertips to Hide IDs, http://www.thebostonchannel.com/news/15478914/detail.html, 2008.
[10] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake Finger Detection by Skin Distortion Analysis," *IEEE Trans. Information Forensics and Security,* vol. 1, no. 3, pp. 360-373, Sept. 2006.
[11] K.A. Nixon and R.K. Rowe, "Multispectral Fingerprint Imaging for Spoof Detection," *Proc. SPIE, Biometric Technology for Human Identification II,* A.K. Jain and N.K. Ratha, eds., pp. 214-225, 2005.
[12] E. Tabassi, C. Wilson, and C. Watson, "Fingerprint Image Quality," NISTIR 7151, http://fingerprint.nist.gov/NFIS/ir_7151.pdf, Aug. 2004.
[13] F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, J. Gonzalez-Rodriguez, H. Fronthaler, K. Kollreider, and J. Bigun, "A Comparative Study of Fingerprint Image-Quality Estimation Methods," *IEEE Trans. Information Forensics and Security,* vol. 2, no. 4, pp. 734-743, Dec. 2007.
[14] R. Cappelli, D. Maio, and D. Maltoni, "Synthetic Fingerprint-Database Generation," *Proc. 16th Int'l Conf. Pattern Recognition,* pp. 744-747, Aug. 2002.
[15] K. Wertheim, "An Extreme Case of Fingerprint Mutilation," *J. Forensic Identification*, vol. 48, no. 4, pp. 466-477, 1998.
[16] History of Fingerprint Removal, http://jimfisher.edinboro.edu/forensics/fire/print.html, 2011.
[17] J. Patten, Savvy Criminals Obliterating Fingerprints to Avoid Identification, http://www.eagletribune.com/punews/local_story_062071408.html, 2008.
[18] Woman Alters Fingerprints to Deceive Taiwan Immigration Fingerprint Identification System, http://www.zaobao.com/special/newspapers/2008/10/hongkong081002r.shtml, (In Chinese), Oct. 2008.
[19] Sweden Refugees Mutilate Fingers, http://news.bbc.co.uk/2/hi/europe/3593895.stm, 2004.
[20] Asylum Seekers Torch Skin off Their Fingertips So They Can't Be ID'd by Police, http://www.mirror.co.uk/sunday-mirror/2008/06/29/asylum-seekers-torch-skin-off-their-fingertips-so-they-can-t-be-id-d-by-police-98487-20624559/, 2008.
[21] Surgically Altered Fingerprints Help Woman Evade Immigration, http://abcnews.go.com/Technology/GadgetGuide/surgically-altered-fingerp rints-woman-evade-immigration/story?id=9302505, 2011.

[22] Three Charged with Conspiring to Mutilate Fingerprints of Illegal Aliens, http://www.eagletribune.com/local/x739950408/Three-charged-with-conspiring-to-mutilate-fingerprints-of-illegal-aliens, July 2010.

[23] EURODAC: a European Union-Wide Electronic System for the Identification of Asylum-Seekers, http://ec.europa.eu/justice_home/fsj/asylum/identification/fsj_asylum_identification_en.htm, 2011.

[24] Neurotechnology Inc., VeriFinger, http://www.neurotechnology.com/vf_sdk.html, 2011.

[25] NIST Special Database 4, NIST 8-Bit Gray Scale Images of Fingerprint Image Groups (FIGS), http://www.nist.gov/srd/nistsd4.htm, 2011.

[26] J.W. Burks, "The Effect of Dermabrasion on Fingerprints: A Preliminary Report," *Archives of Dermatology,* vol. 77, no. 1, pp. 8-11, 1958.

[27] Men in Black, http://www.imdb.com/title/tt0119654/, 1997.

[28] M.V. de Water, "Can Fingerprints Be Forged?" *The Science News-Letter,* vol. 29, no. 774, pp. 90-92, 1936.

[29] M. Wong, S.-P. Choo, and E.-H. Tan, "Travel Warning with Capecitabine," *Annals of Oncology,* vol. 20, p. 1281, 2009.

[30] K. Nandakumar, A.K. Jain, and A. Ross, "Fusion in Multibiometric Identification Systems: What about the Missing Data?," *Proc. Second Int'l Conf. Biometrics,* pp. 743-752, June 2009.

[31] H. Plotnick and H. Pinkus, "The Epidermal versus the Dermal Fingerprint: An Experimental and Anatomical Study," *Archives of Dermatology,* vol. 77, no. 1, pp. 12-17, 1958.

[32] Altered Fingerprints Detected in Illegal Immigration Attempts, http://www.japantoday.com/category/crime/view/altered-fingerprints-dete cted-in-illegal-immigration-attempts, 2011.

[33] NIST Special Database 14, NIST Mated Fingerprint Card Pairs 2 (MFCP2), http://www.nist.gov/srd/nistsd14.htm. 2011.

[34] J. Zhou and J. Gu, "A Model-Based Method for the Computation of Fingerprints' Orientation Field," *IEEE Trans. Image Processing,* vol. 13, no. 6, pp. 821-835, 2004.

[35] S. Huckemann, T. Hotz, and A. Munk, "Global Models for the Orientation Field of Fingerprints: An Approach Based on Quadratic Differentials," *IEEE Trans. Pattern Analysis and Machine Intelligence,* vol. 30, no. 9, pp. 1507-1519, Sept. 2008.

[36] Y. Wang and J. Hu, "Global Ridge Orientation Modeling for Partial Fingerprint Identification," *IEEE Trans. Pattern Analysis and Machine Intelligence,* vol. 33, no. 1, pp. 72-87, Jan. 2010.

[37] C. Watson, M. Garris, E. Tabassi, C. Wilson, R.M. McCabe, S. Janet, and K. Ko, "NIST Biometric Image Software," http://www.nist.gov/itl/iad/ig/nbis.cfm, 2011.

[38] A.M. Bazen and S.H. Gerez, "Systematic Methods for the Computation of the Directional Fields and Singular Points of Fingerprints," *IEEE Trans. Pattern Analysis and Machine Intelligence,* vol. 24, no. 7, pp. 905-919, July 2002.

[39] N. Dalal and B. Triggs, "Histograms of Oriented Gradients for Human Detection," *Proc. IEEE Computer Vision and Pattern Recognition Conf.,* vol. 1, pp. 886-893, June 2005.

[40] C.-C. Chang and C.-J. Lin, *LIBSVM: A Library for Support Vector Machines,* software http://www.csie.ntu.edu.tw/cjlin/libsvm, 2001.

[41] L.M. Wein and M. Baveja, "Using Fingerprint Image Quality to Improve the Identification Performance of the U.S. Visitor and Immigrant Status Indicator Technology Program," *Proc. Nat'l Academy of Sciences USA,* vol. 102, no. 21, pp. 7772-7775, 2005.

[42] A. Ross, K. Nandakumar, and A.K. Jain, *Handbook of Multibiometrics.* Springer Verlag, 2006.

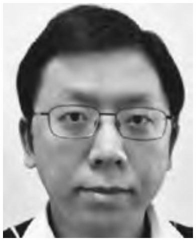
[43] The FBI's Next Generation Identification (NGI), http://www.fbi.gov/hq/cjisd/ngi.htm, 2011.

[44] DoD Biometrics Task Force, http://www.biometrics.dod.mil/, 2011.

[45] R. Singh, M. Vatsa, H.S. Bhatt, S. Bharadwaj, A. Noore, and S.S. Nooreyezdan, "Plastic Surgery: A New Dimension to Face Recognition," *IEEE Trans. Information Forensics and Security,* vol. 5, no. 3, pp. 441-448, Sept. 2010.

[46] R. Roizenblatt, P. Schor, F. Dante, J. Roizenblatt, and R. Belfort, "Iris Recognition as a Biometric Method After Cataract Surgery," *Am. J. Ophthalmology,* vol. 140, no. 5, pp. 969-969, 2005.

Soweon Yoon received the BS and MS degrees from the School of Electrical and Electronic Engineering, Yonsei University, Seoul, Korea, in 2006 and 2008, respectively. Currently, she is working toward the PhD degree in the Department of Computer Science and Engineering, Michigan State University. Her research interests include pattern recognition, image processing, and computer vision, with applications in biometrics. She is a student member of the IEEE.



Jianjiang Feng received the BS and PhD degrees from the School of Telecommunication Engineering, Beijing University of Posts and Telecommunications, China, in 2000 and 2007, respectively. Currently, he is working as an assistant professor in the Department of Automation at Tsinghua University, Beijing. From 2008 to 2009, he was a postdoctoral researcher in the Pattern Recognition and Image Processing Laboratory at Michigan State University. His research interests include fingerprint recognition, palmprint recognition, and structural matching. He is a member of the IEEE.

Anil K. Jain is a university distinguished professor in the Department of Computer Science and Engineering at Michigan State University, East Lansing. His research interests include pattern recognition and biometric authentication. He served as the editor-in-chief of the *IEEE Transactions on Pattern Analysis and Machine Intelligence* (1991-1994). He is the coauthor of a number of books, including *Handbook of Fingerprint Recognition* (2009), *Handbook of Biometrics* (2007), *Handbook of Multibiometrics* (2006), *Handbook of Face Recognition* (2005), *BIOMETRICS: Personal Identification in Networked Society* (1999), and *Algorithms for Clustering Data* (1988). He served as a member of the Defense Science Board and The National Academies committees on Whither Biometrics and Improvised Explosive Devices. He received the 1996 *IEEE Transactions on Neural Networks* Outstanding Paper Award and the Pattern Recognition Society best paper awards in 1987, 1991, and 2005. He has received Fulbright, Guggenheim, Alexander von Humboldt, IEEE Computer Society Technical Achievement, IEEE Wallace McDowell, ICDM Research Contributions, and IAPR King-Sun Fu awards. He is a fellow of the AAAS, ACM, IAPR, SPIE, and IEEE.