Fingerprint Alteration

Jianjiang Feng, Anil K. Jain, and Arun Ross

Abstract—**The widespread deployment of Automated Fingerprint Identification Systems (AFIS) in law enforcement and border control applications has heightened the need for ensuring that the security afforded by these systems is not compromised. While several issues related to fingerprint system security have been investigated in the past, including the use of fake fingerprints for masquerading identity, the problem of fingerprint alteration or obfuscation has received no attention in the biometric literature. Fingerprint obfuscation refers to the deliberate alteration of the fingerprint pattern by an individual for the purpose of masking his or her identity. Several cases of fingerprint obfuscation have been described in the media. Existing image quality assessment software cannot detect such altered fingerprints since the implicit image quality during alteration may not change significantly. The goal of this paper is to understand the problem of altered fingerprints and to design solutions that can be used to detect these images. In this regard, this paper makes following contributions: (a) compiling case studies of incidents where individuals were found to have altered their fingerprints for circumventing fingerprint systems; (b) classifying the observed alterations into three broad categories and suggesting possible counter-measures; (c) a method to synthetically generate altered fingerprints in the absence of real-world data; (d) a technique to detect altered fingerprints; and (e) experimental results involving both real-world altered prints and synthetically generated altered prints. Experimental results show the feasibility of the proposed approach in detecting altered fingerprints and highlights the need to further pursue this research agenda.**

Index Terms—**Biometrics, obfuscation, fingerprints, alteration, ridge pattern, IAFIS, image quality.**

I. Introduction

FINGERPRINT recognition has been used by law enforcement agencies to identify suspects and victims for several decades. Recent advances in automated fingerprint identification technology, coupled with the pronounced need for reliable person identification, have resulted in the increased use of fingerprints in both government and civilian applications such as border control, employment background check and secure facility access [1]. Examples of large scale fingerprint systems in the government arena include US-VISIT's IDENT program [2] and the FBI's IAFIS service [3].

The success of fingerprint recognition systems in accurately identifying individuals has prompted some individuals to engage in extreme measures for the purpose of circumventing the system. The primary purpose of fingerprint alteration [4] 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 has been deployed in the first place, i.e., to identify individuals in a watch-list.

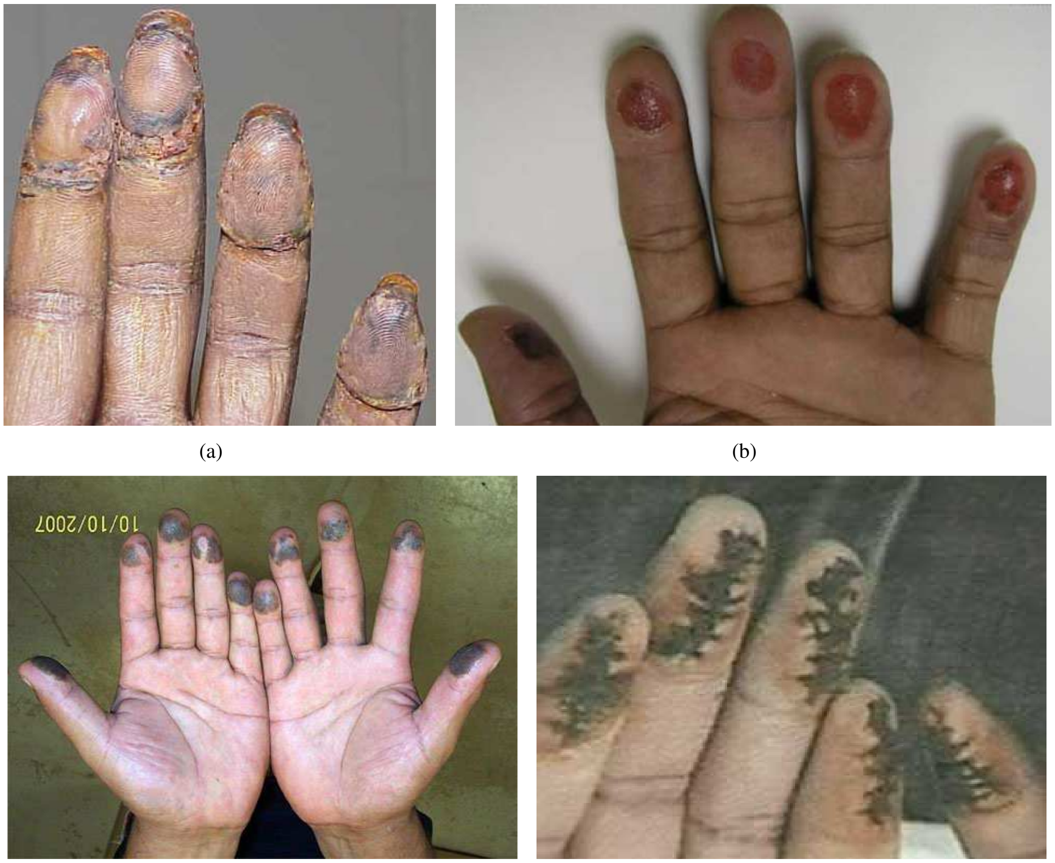
It should be noted that *altered* fingerprints are different from *fake* fingerprints. The use of fake fingers - made of glue, latex or silicone - is a well publicized method to circumvent fingerprint systems. Altered fingerprints, on the other hand (no pun intended!), are real fingers that are used to conceal one's identity in order to evade identification by a biometric system. Thus, fake fingers are typically used by individuals to adopt another person's identity while altered fingers are used to mask one's own identity. In order to detect attacks based on fake fingers, many software [5] and hardware [6] solutions have been proposed. However, the problem of altered fingers has hitherto not been systematically studied in the literature and there are no well established techniques to address it. Furthermore, the lack of public databases comprising of altered fingerprint images has stymied research in this area. One of the goals of this paper is to highlight the urgency of the problem and present some preliminary results on this important, yet understudied, topic.

The aforementioned problem involving altered fingers falls under a broader category of attacks know as *biometric obfuscation*. Obfuscation can be defined as a deliberate attempt by an individual to mask their 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: (i) fingerprint systems are much more widespread in large scale identification systems than systems based on other modalities (face and iris); (ii) it is relatively easy to alter one's fingerprints using chemicals and abrasives compared to, say, one's iris or face where a surgical procedure may be necessary; and (iii) the problem of mutilated fingerprints is being already observed by law enforcement and immigration officials thereby underscoring the urgency of the problem.

Fingerprint quality control routines used in most fingerprint systems, such as the open source NFIQ (NIST Fingerprint Image Quality) software [10], may be useful in detecting altered fingerprints if the corresponding images are of poor image quality. But altered fingerprints may not necessarily be of inferior quality. Since existing fingerprint quality algorithms [11] are designed to examine if an image contains enough reliable details (say, minutiae) for matching, they have very limited capability in determining if an image is a natural

J. Feng and A. K. Jain are with the Department of Computer Science and Engineering, Michigan State University, 3115 Engineering Building, East Lansing, MI 48824-1226, USA (e-mail: jfeng@cse.msu.edu, jain@cse.msu.edu)

A. Ross is with the Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, WV 26506, USA (e-mail: arun.ross@mail.wvu.edu).


(a)

(b)

(c)

(d)

Fig. 1. Photographs of altered fingerprints. (a) Transplanted fingerprints from feet (http://www.clpex.com/images/FeetMutilation/L4.JPG), (b) bitten fingers [7], (c) fingers burned by acid [8], and (d) stitched fingers [9].

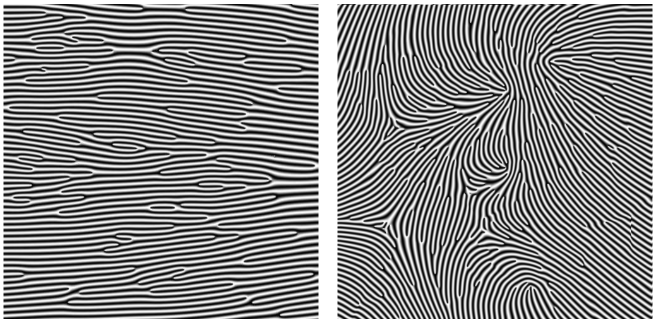
fingerprint or an altered fingerprint. For example, while the synthesized ridge patterns in Fig. 2 are not likely to appear on fingertips, their quality level according to the NFIQ measure is 1[1].

The goal of this paper is to introduce the problem of fingerprint alteration and to design methods to automatically detect obfuscated fingerprints. The rest of the paper is organized as follows. Section II lists examples of cases in which altered fingerprints were encountered by law enforcement officers. In Section III, the biological underpinnings of fingerprints and the vulnerability of practical fingerprint identification systems are discussed. In section IV, three different categories of altered fingerprints are introduced and potential countermeasures are suggested. The proposed approach for detecting altered fingerprints is presented and evaluated in Section V. Finally, Section VI contains future directions on this topic.

II. Case Studies

A. High Profile Cases

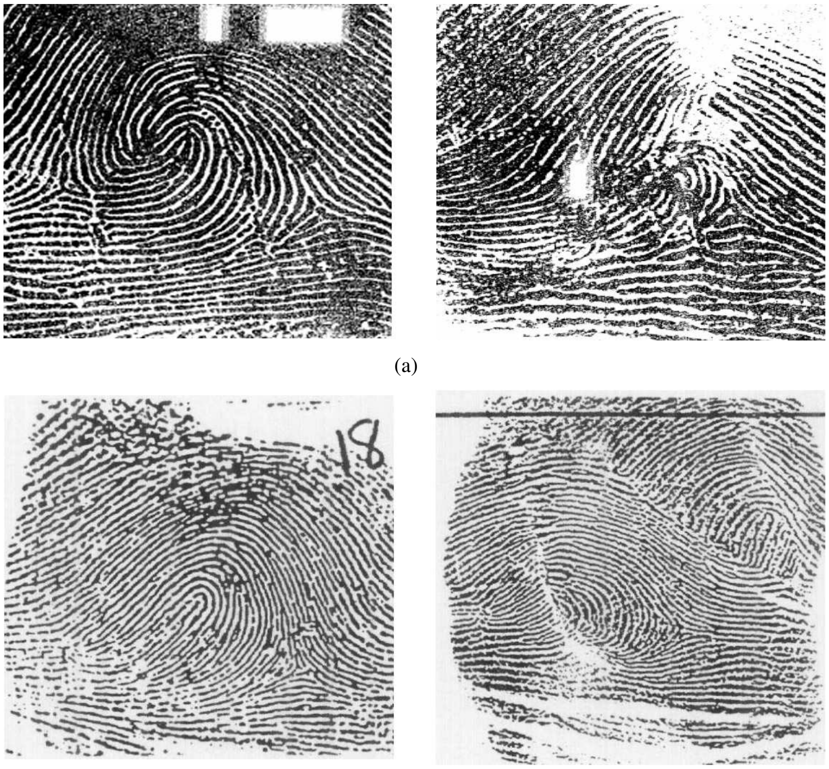
As early as in 1933, “Gus” Winkler, a murderer and bank robber, was found to have altered the fingerprints of his left hand except for the thumb by slashing and tearing the flesh of the fingers [4]. Further, the pattern type of one finger was altered from whorl to loop (see Fig. 3a). In 1934, John Dillinger, the infamous bank robber and a dangerous criminal, was found to have applied acid to his fingertips [15]. However, the altered fingerprints still had sufficient information to enable a match with the original fingerprints since only the central area of the fingertips were damaged. In 1941, Roscoe Pitts (also known as Robert J. Philipps), a habitual criminal, had a plastic surgeon remove the skin of his fingertips and replace them with skin grafts from his chest [15]. After he was arrested


(a)

(b)

Fig. 2. Synthetic ridge patterns. NFIQ [10] value for both these two synthetic ridge patterns is 1, the highest quality level. The synthetic ridge pattern in (a) is generated by the approach in [12] and the synthetic ridge pattern in (b) is generated by following the approach of SFINGE [13].

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



(a)

(b)

Fig. 3. Inked impressions before and after fingerprint alteration. (a) Fingerprints of “Gus” Winkler [4] (pattern type is altered from whorl to loop), and (b) fingerprints of Jose Izquierdo [14] (altered by switching two parts of a ‘Z’ shaped cut).

by the police, his true identity was revealed by the plastic surgeon and confirmed by comparing the second joints of his fingers with the original fingerprint card.

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 mutilated 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 Izquiredo who was an absconding drug criminal [14]. His fingerprint mutilation process consisted of three steps: making a ‘Z’ shaped cut on the fingertip, lifting and switching two triangles, and stitching them back. Unlike most of the other cases where the person concerned was identified using non-fingerprint evidence, this case was solved solely based on fingerprints although they had been surgically altered. In September 2005, a drug dealer named Marc George was caught because his limping gait as a result of a surgery caught the attention of border officials. A plastic surgeon, who was later arrested and convicted, had performed the surgery to replace Marc George’s fingerprints with the skin from his feet (see Fig. 1a) [15]. In August 2007, a person arrested for vehicle theft bit his fingers in custody in order to avoid identification (see Fig. 1b) [7]. In October 2007, Mateo Cruz-Cruz, who was caught by border patrol agents when he attempted to scale the border fence, was found to have blackened fingerprints, as a result of applying acid (see Fig. 1c) [8]. In February 2008, a man using the name Edgardo Tirado arrested on drug charges was found to have thick stitches on his fingertips (see Fig. 1d). He was believed to have altered his fingerprints by cutting the fingertips longitudinally and then stitching them back together. Edgardo Tirado was recognized by a detective as Gerald Perez [16] who had altered his fingerprints in order to avoid being linked to his criminal record and deported.

It is not just the criminals who have been found to alter their fingerprints. In June 2007, a woman, whose fidgety behavior caught the attention of police, was found to have vague fingerprints. She admitted that she had a surgery, at a cost of $2,000, to alter her fingerprints in order to illegally enter the United States [8]. In October 2008, it was reported that a woman had successfully deceived the two-thumbprint-based Taiwan border control identification system by performing plastic surgeries to alter both her face and fingerprints [17]. She had spent $1,025 to have her thumbprints altered by ‘Z’ cuts (similar to the case in [14]) and five other fingerprints altered using laser. Three fingerprints (left little, right ring and little fingers) were left unaltered due to the financial burden of the procedure. The three unaltered fingerprints were used by a ten-print matching system to reveal her true identity after her altered fingerprints were found by an official during a manual examination of fingerprint records in the immigration database. In June 2009, it was reported that four people were caught attempting to illegally enter Japan after having their fingerprints surgically altered at a cost of around $730 per person [18]. The individuals were apprehended after the fingerprint system triggered an alarm upon encountering their altered fingerprint patterns. The Japanese border control fingerprint system has been upgraded based on a case in January 2009 where a woman deceived the system by obfuscating her true fingerprints with tape-made fake ones [19].

Fingerprint alteration has even been performed at a much larger scale involving multiple individuals. It was reported that in Sweden [20] and France [21], hundreds of asylum seekers had cut, abraded and burned their fingertips to prevent identification by EURODAC [22], a European Union-wide fingerprint system for identifying asylum seekers.

B. Comments

Although the number of publicly disclosed cases of altered fingerprints is not very large, the severity of the consequence of this type of obfuscation should not be underestimated. This is because in biometric applications involving watch-lists, persons in the target population (a small portion of the whole population) have a strong motive to alter their fingerprints. In addition, it is extremely difficult to estimate the number of individuals who have successfully evaded identification by fingerprint systems in the past as a result of fingerprint alteration.

To combat the problem of masking one's identity by altering fingerprints, we need to first detect such fingerprints and then determine the true identity of the person. In most of the disclosed cases, altered fingerprints were in fact detected by human officers (and not by the automatic systems). Further, the true identification was accomplished based on ancillary evidence (although fingerprints may have been used to confirm the identity). Only in one case [14] was the identification conducted using reconstructed fingerprints. If the authorities have little prior information about the person altering his fingerprints, such as in the case involving asylum seekers [20], [21], the only source of information that they can rely on is the fingerprints themselves. However, identifying altered fingerprints is not an easy problem as illustrated in [14] where the search process stretched over two weeks. If the surgery to the fingers had been a little more complex - such as implanting the cut friction ridge skin among different fingers - the search could have taken even longer!

III. Fingerprint Identification

In this section, we first introduce the two fundamental premises of fingerprint identification, which make fingerprints a powerful biometric trait even in the presence of various fingerprint alterations. Then we describe the characteristics of fingerprints that distinguish natural fingerprints from altered ones. Finally, we discuss practical fingerprint identification systems and their vulnerability to altered fingerprints.

A. Premises of Fingerprint Identification

Permanence and *uniqueness* are the two fundamental premises that form the basis of friction ridge identification, namely fingerprint and palmprint identification. The friction ridge skin on human finger, palm, toe and sole consists of two layers: the outer layer, *epidermis*, and the inner layer, *dermis*. Both the surface and the bottom of the epidermis contain ridge-like formations [23]. The bottom (primary) ridges correspond to the generating (or basal) layer of the epidermis that generates new cells that migrate upwards to the finger surface and slough off. The surface (friction) ridge pattern is a mirror of the bottom ridges, which itself is formed as a result of the buckling process caused by the stress during the growth of fetus at around the fourth month of gestation [24]. Superficial cuts on the surface ridges that do not damage the bottom ridges only temporarily change the surface ridges; after the injury heals, the surface ridges will grow back to the original pattern. Abrading fingers using rasp only temporarily flattens the friction ridges and they will grow back to the original pattern after some time.

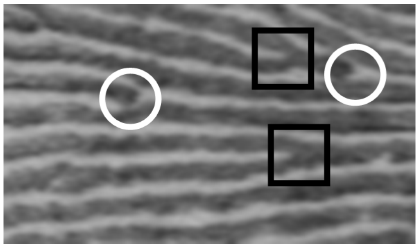


Fig. 4. Ridge endings (marked with white circles) and ridge bifurcations (marked with black squares). Image is cropped from fingerprint F0134 in NIST SD4 database [26].

It is generally understood and agreed that friction ridge patterns are not influenced exclusively by genetic factors but also by random physical stresses and tensions that occur during fetal development [25]. These random effects result in the uniqueness property of fingerprints. Even a small portion of friction ridge pattern (e.g., latent fingerprints) contains sufficient detail for establishing one's identity.

In order to evade identification, fingerprints must be altered to get around these two premises.

B. Characteristics of Fingerprints

The friction ridge pattern on a fingertip consists of friction ridges, which are locally parallel and are separated by furrows. The position where a ridge abruptly ends or bifurcates is called a minutia (see Fig. 4). While each fingerprint is unique in detail (such as minutiae and ridge shapes), the overall ridge flow pattern of human fingerprints (and toe prints) is quite similar.

Galton classified fingerprints into three basic pattern types: whorl, loop and arch (Fig. 5) [27]. It is believed that such patterns are related to the location and shape of volar pads and the boundary of friction ridges on fingertips (joint crease, and finger nail) [24]. Ridges in whorl and loop fingerprints are separated into three ridge systems: pattern area, distal transverse and proximal transverse systems, by type lines (black lines in Fig. 5) [25]. Delta is the position where three ridge systems meet and core is the innermost position of concentric or loop ridges. Ridge systems in arch fingerprints are not distinguishable. Although ridge flow in the central

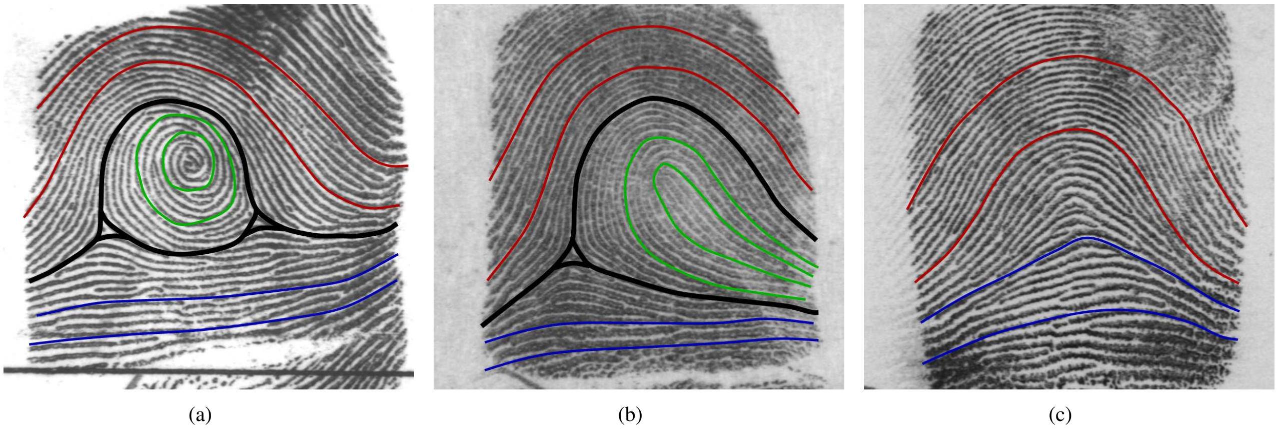


Fig. 5. Three major fingerprint pattern types: (a) whorl, (b) loop, and (c) arch. Three different ridge systems [25] are marked with lines in different colors (red for distal transverse ridges, green for pattern area ridges, and blue for proximal transverse ridges). Type lines are shown as wide black lines. These three fingerprints are labeled as S0644, F0060, and F0006 in NIST SD4 database, respectively.

area of fingerprints with different pattern types are quite different, almost all fingerprints have similar ridge flows near the fingerprint boundary. The Poincaré index[2] along the fingerprint boundary is zero and, therefore, the numbers of loops and deltas in a full fingerprint are always the same [28], [29]. Generally, whorl type fingerprints have two or more core/delta; Loop and tented arch fingerprints have one core/delta; Arch fingerprints do not have any core or delta. While the distributions of core and delta in fingerprints of the same pattern type are not fixed, they are not random either [30].

Friction ridges are often broken by flexion creases (Figs. 6a and b) and sometimes by scars due to injury (Figs. 6c and d). Narrow scars look very similar to minor creases except for the two differences that can be used to distinguish them: (i) ridges broken by narrow scars are often misaligned, but ridges broken by creases are still aligned very well, and (ii) minor creases are not as stable as narrow scars. Minor creases tend to become narrow or even disappear in inked impressions, live-scan images of wet fingers, or impressions made by excessive pressure during fingerprint capture.

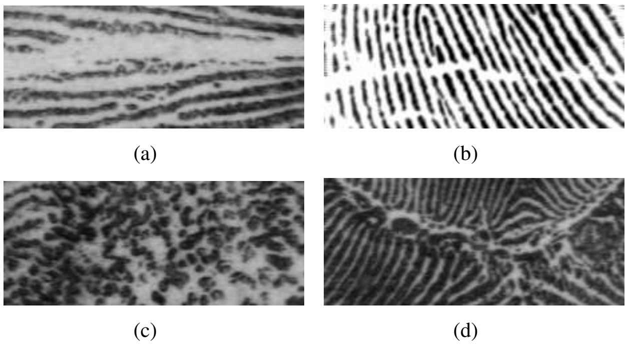


Fig. 6. Flexion creases and scars in fingerprints. (a) A major crease between finger joints, (b) a minor crease, (c) large area scar, and (d) a narrow scar. The image in (b) is cropped from fingerprint 10_3 in FVC2002 DB1 [31] and the other three images are cropped from fingerprints F0201, F1022 and F0693 in NIST SD4 [26], respectively.

C. Vulnerability of Fingerprint Identification Systems

Although the structure of fingerprint patterns can be exploited, to some extent, in order to combat alteration attempts, operational fingerprint identification systems are indeed vulnerable to such attacks.

It is very difficult for the state-of-the-art AFIS (Automated Fingerprint Identification Systems) to identify significantly altered fingerprints. Note that it is not necessary to alter the entire friction skin region on the human hand since only a portion of the friction ridge pattern is used in most practical identification systems. Depending on the level of security and the intended application, friction ridge areas recorded and compared by identification systems can vary from the whole hand to a single finger. Furthermore, many non-forensic fingerprint systems use plain (or flat) fingerprint images instead of rolled images. It is also not necessary to completely alter the fingerprints input to automated systems, since their identification accuracy is constrained by image quality, throughput requirements, and database size (false accept rate has to be very low in large-scale systems with millions of enrolled subjects) [32], [33]. Although the accuracy of automated systems in identifying low quality fingerprints can be significantly improved with the help of human operators (as observed in latent identification practice [34]), no specific software is yet available to reconstruct the original pattern of altered fingerprints [14].

It is very difficult for current fingerprint quality control software to detect altered fingerprints. As illustrated in Fig. 2, current quality assessment algorithms cannot determine whether an input ridge pattern pertains to an actual finger [10], [35], [36], [11], [37]. Such a determination can be easily made by experienced human operators based on visually examining the fingerprint. However, in many applications, automatic detection of altered fingerprints is necessary as the process of fingerprint matching is required to be extremely fast (with limited human intervention) and the operators themselves may not have received sufficient training that would allow them to

[2] The total change of orientation along a closed boundary on orientation field.

distinguish altered fingerprints from natural ones.

IV. Types of Altered Fingerprints

According to the changes made to the ridge patterns, fingerprint alterations may be categorized into three types: *obliteration*, *distortion*, and *imitation* (see Fig. 7). For each type of alteration, its characteristics and possible countermeasures are described.

A. Obliteration

Friction ridge patterns on fingertips can be obliterated by abrading [38], cutting [4], burning [20], [21], [39], [17], applying strong chemicals (Fig. 1c), and transplanting smooth skin [15]. Further, factors such as skin disease (such as leprosy [40]) and side effects of a cancer drug [41] can also obliterate fingerprints.

Obliterated fingerprints can defeat automated fingerprint matchers and successfully pass fingerprint quality control software, depending on the depth and area of damages. If the damage does not reach the generating layer in the epidermis (depth of around 1 mm [25]), the skin will regenerate to the original ridge pattern after a few months time. However, if the damage is done to the generation layer, scar tissues, instead of well-defined ridge details, will replace the damaged area. If the affected finger area is small, automated matchers are likely to successfully match the damaged fingerprint to the original mated fingerprint. But, if the affected area is sufficiently large to defeat automated matchers, human operators or fingerprint quality control software can easily detect the damage. For example, the obliterated fingerprint in Fig. 7a is assigned the lowest quality level of 5 by the NFIQ software.

Appropriate threshold values need to be set in fingerprint quality control software to detect significantly obliterated fingerprints that automated matchers can not identify. To identify individuals with severely obliterated fingerprints, it may be necessary to treat these fingerprints as latent images, perform an AFIS search using manually marked features, and adopt an appropriate fusion scheme for tenprint search [42]. 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 [43].

B. Distortion

Friction ridge patterns on fingertips can be turned into unnatural ridge patterns by plastic surgery, in which portions of skin are removed from a finger and grafted back in different positions [9], [14], [18] (see Fig. 7b). Friction skin transplantation resulting in unnatural ridge patterns also belongs to this category (see Fig. 8).

Surgical procedures needed to distort fingerprints are not complicated and the resulting distorted fingerprints are very difficult to match against the original mated fingerprints by automated matchers. Distorted fingerprints may pass fingerprint quality control software or even examination by inexperienced human operators as distortion does not necessarily reduce the image quality. For instance, the distorted fingerprint in Fig. 7b is assigned the highest quality level of 1 by the NFIQ measure. Similarly, the altered fingerprint by ‘Z’ cut in Fig. 3b is assigned the second highest quality level of 2 by the NFIQ measure.

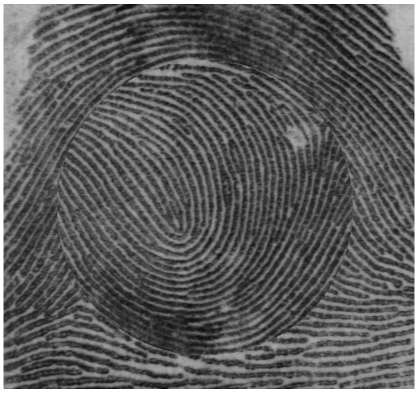


Fig. 8. An unnatural ridge pattern is simulated by cuting off the central region of a fingerprint (NIST SD4, F0235) and stitching it back upside down. NFIQ value for this altered fingerprint is 1, indicating the highest quality.

This type of fingerprint alteration has been increasingly observed in border control applications. Therefore, it is imperative to upgrade current fingerprint quality control software to detect this type of altered fingerprints. Once detected, the following actions may be taken to assist the automated fingerprint matcher: (i) identify unaffected regions of the fingerprint and manually mark features (i.e., the minutiae) in these regions and (ii) reconstruct the original fingerprint as done by the latent examiner in the ‘Z’ cut case [14].

C. Imitation

Here, a surgical procedure is performed in such a way that the altered fingerprints appear as a natural fingerprint ridge pattern. Such surgeries may involve the transplantation of a large-area friction skin from other parts of the body, such as fingers, palms, toes, and soles (see Fig. 1a and simulation in Fig. 9), or even cutting and mosaicking multiple small portions of friction skin (see simulation in Fig. 10).

Transplanted fingerprints can successfully evade existing fingerprint quality control software. If the surgical scars due to the transplantation are small, it can even deceive inexperienced human operators. As long as the transplanted area is large, matching altered fingerprints to the original (unaltered) fingerprints is not likely to succeed. Plain images captured by fingerprint scanners used in most border control applications may not be able to reveal the surgical scars in large-area transplantation. But the large-area transplantation has the risk of being matched to the donor print (if the donor print that is contained in the database is also searched). Further, reconstructing the original fingerprint is not difficult since transplantation is generally performed using friction skin of the same person as in the Marc George’s case [15][3]). Small-area transplantation is probably a more complicated surgery.

[3] Updegraff, a plastic surgeon, claimed that skin grafts between humans or between humans and animals are seldom successful [45].

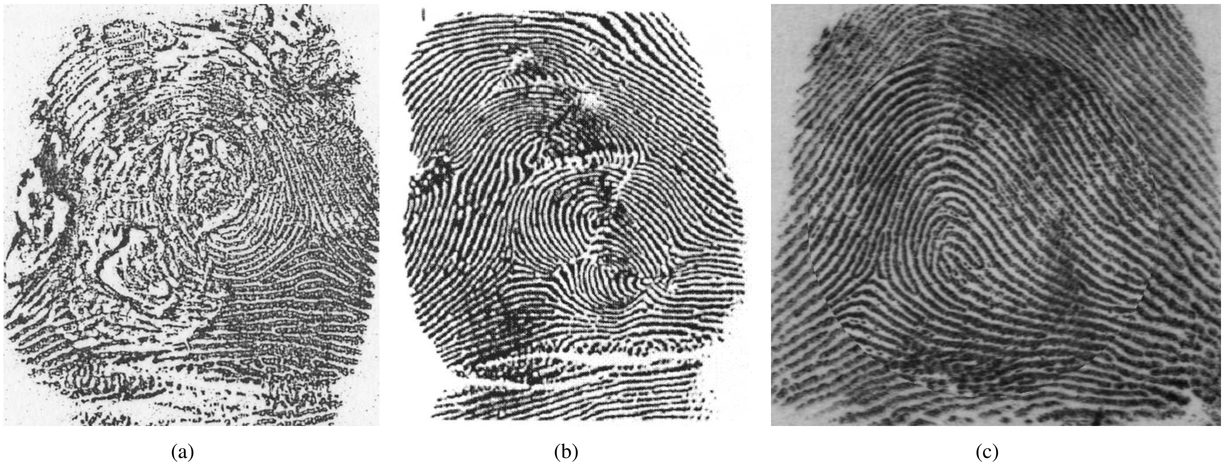


Fig. 7. Three types of altered fingerprints. (a) Obliterated fingerprint (e.g., by burning, NFIQ=5) provided by Michigan State Police, (b) distorted fingerprint (NFIQ=1) provided by DHS, (c) imitated fingerprint (simulated by replacing the central region of the original fingerprint (NIST SD4, F1251) with the central region of a different fingerprint (F1253), NFIQ=1).

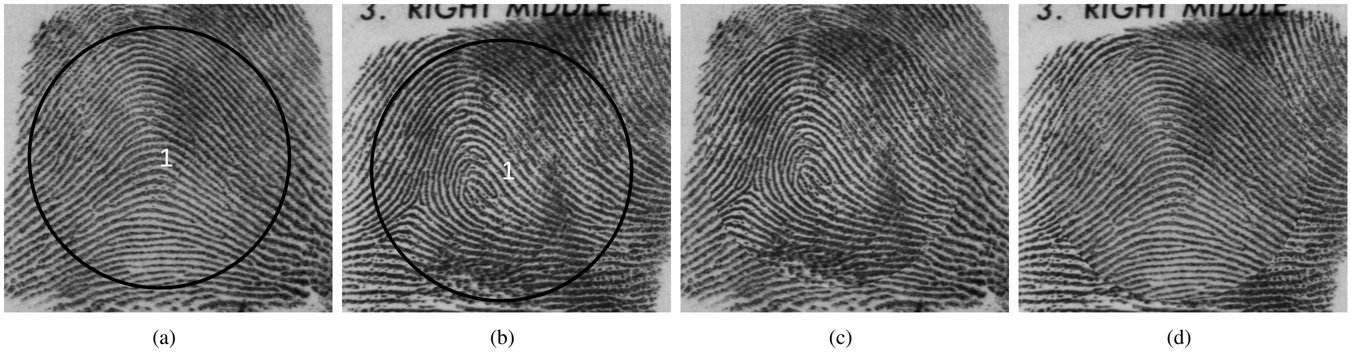


Fig. 9. Simulation of large-area transplantation between two fingerprints: (a) Original fingerprint (NIST SD4, F1251), (b) original fingerprint (F1253), (c) altered fingerprint by transplanting central area in (b) to (a), and (d) altered fingerprint by transplanting central area in (a) to (b). NFIQ values of all these four fingerprints are 1. According to VeriFinger SDK [44], the altered fingerprints are not similar to the original ones (similarity scores are 25 and 8) but very similar to the donor fingerprints (similarity scores are 165 and 126).

To avoid identification, areas exhibiting clusters of minutiae have to be altered (see Fig. 10). While it is difficult to match altered fingerprints that have been generated by extracting and mosaicking small portions of friction skin from either the original print or a donor print, there may be obvious surgical scars present in both rolled and plain impressions of the altered fingerprints.

The main clue to detect transplanted fingerprints is the presence of surgical scars. To detect scars caused by large-area transplantation, rolled fingerprints instead of plain fingerprints have to be captured and analyzed [45]. In the case where the donor print is taken from other fingerprints of the same person, fingerprint matching without using finger position information (i.e., left thumb or right index finger) may help in determining the true identity, although the response time will significantly increase. To reconstruct original fingerprints in small-area transplantations, an efficient automatic solution is preferred over tedious manual search [14].

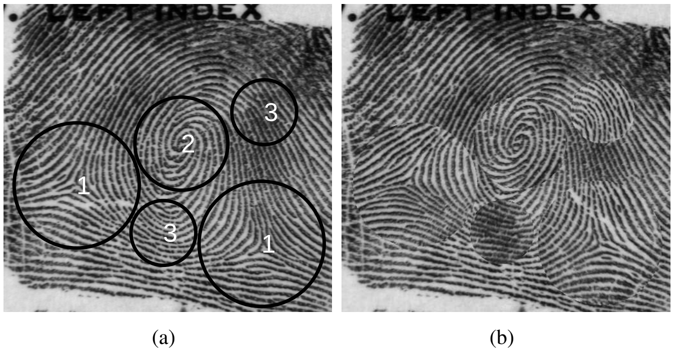


Fig. 10. Simulation of small-area transplantation within a finger. (a) Original fingerprint (NIST SD4, F0046) and (b) altered fingerprint. Simulation is performed by exchanging and rotating circular regions (marked with the same number) to match the local ridge orientation or just rotating circular regions (marked with number 2) by 180 degrees. NFIQ values of both fingerprints are 1. The similarity score with the mated search fingerprint (S0046) according to VeriFinger SDK [44] is reduced from 372 to 22 due to alteration.

V. Automatic Detection of Distorted Fingerprints

In the previous section, we had discussed the various categories of altered fingerprints and provided suggestions on how these types of prints can be automatically detected. In this section, we consider the problem of automatic detection of alterations that result in distorted (unnatural) fingerprints.

We do not consider the other two types of altered fingerprints because: (i) the image quality of obliterated fingerprints is either so good that they can be successfully matched to the mated fingerprint by automatic matchers or so poor that they can be easily detected by a fingerprint quality control software, and (ii) imitated fingerprints may look very natural and there is no data currently available in the public domain to undertake such a study.

A. Simulation

Due to the lack of a public database comprising of altered fingerprint images, it is essential that the study be undertaken on synthetically altered images. This would allow researchers to leverages the technique designed here and utilize them in operational settings.

We used NIST SD4 [26] to simulate altered fingerprints. This dataset contains 2,000 different fingers and each finger has two rolled images, termed as file and search, respectively. We selected a subset of 1,976 file fingerprints whose NFIQ quality level is less than 5 (i.e., not the worst). For each of these fingerprints, three types of alterations are simulated (see Fig. 11):

1) 'Z' cut. The four vertices of 'Z' correspond to the vertices of a rectangle obtained by resizing the bounding box of the fingerprint region by 80%.
2) Full rotation. The entire fingerprint is rotated by 180 degrees.
3) Central rotation. The central region of a fingerprint is rotated by 180 degrees. The radius of the circular region in the fingerprint center is $0.35r$, where r is the shorter side length of the bounding box of the fingerprint.

To examine the identifiability of these three types of altered fingerprints, namely if the altered fingerprints can be correctly identified, each altered fingerprint was matched to the mated search fingerprint in NIST SD4 using VeriFinger SDK [44] to generate genuine match scores. For comparison purposes, original file fingerprints were also matched to original search fingerprints to generate genuine match scores and impostor match scores. Figure 12 shows the score distributions of four types of genuine matches and impostor matches. The genuine match scores using altered fingerprints are in the same range as impostor match scores, which means that they can not be correctly identified.

To examine the detectability of altered fingerprints according to existing fingerprint quality control software, quality levels of three types of altered fingerprints and original fingerprints were estimated using the NFIQ software [10]. From the distribution of NFIQ values shown in Fig. 13, we can observe that:

1) Full image rotation does not reduce image quality.
2) Image quality of some of the fingerprints is reduced due to 'Z' cut and central rotation.
3) Only a very small number of altered fingerprints have the lowest quality level of 5.
4) Suppose the fingerprint system raises an alarm for NFIQ quality levels of 4 and 5. The false alarm[4] rate will be 7% and only 20% of altered fingerprints can be detected.

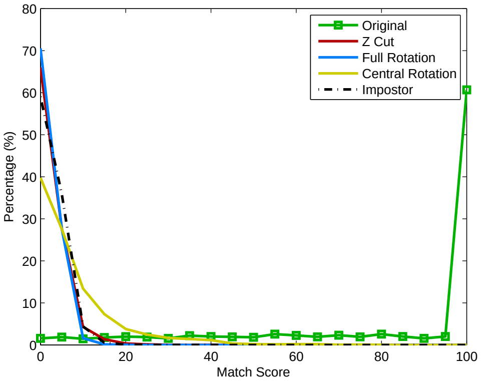


Fig. 12. Match score distributions of genuine matches using original fingerprints, genuine matches using three types of altered fingerprints, and impostor matches using original fingerprints. Only a part of the whole range of similarity score is shown (most genuine match scores using original fingerprints are much larger than 100).

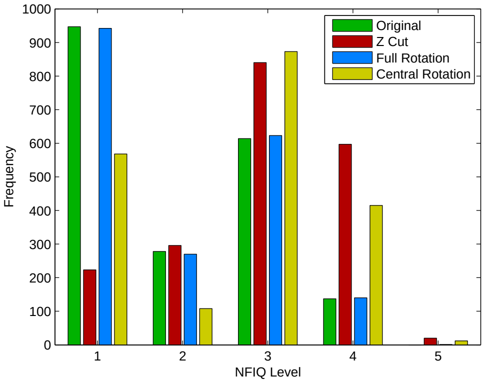


Fig. 13. Histogram of NFIQ values of 1,976 original file fingerprints in NIST SD4 and three types of altered fingerprints. Quality values of original natural fingerprints and altered ones are not well separated.

B. Detection

We detect altered fingerprints based on analyzing the ridge orientation field. Due to variations of singular points in terms of their number and location, the orientation fields of natural fingerprints also vary across individuals. Therefore, we decompose the original orientation field into two components (see Fig. 14): singular orientation field and continuous orientation field (explained later). Figure 15 shows the continuous orientation fields of two original fingerprints and two altered fingerprints. As can be observed in Fig. 15, the continuous orientation fields of original fingerprints are indeed continuous (i.e., no singularity), but the "continuous" orientation fields of altered fingerprints are acturally not continuous. We extract high level features from the continuous orientation field and

[4] A false alarm occurs when an unaltered (original) fingerprint is wrongly detected as an altered fingerprint.

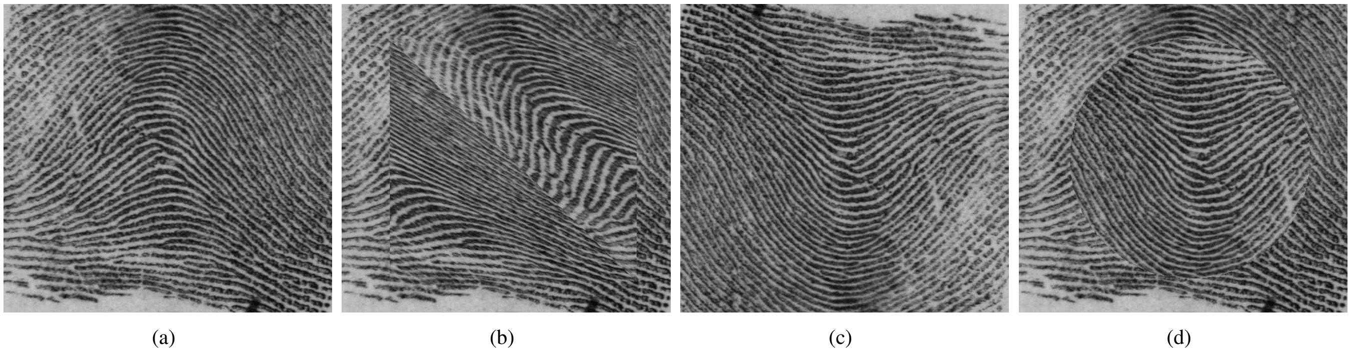


Fig. 11. Natural and simulated altered fingerprints in our dataset. (a) Original fingerprint (NIST SD4, F0020), (b) 'Z' cut, (c) full rotation, and (d) central rotation.

use a support vector machine for classifying a fingerprint as natural fingerprint or altered one. The main steps of the proposed algorithm are described below.

The orientation field of a fingerprint is estimated using the following approach.

1) The skeleton image of the fingerprint, which is output by the VeriFinger SDK [44], is converted to a grayscale image using a distance transform.
2) Based on the distance transform image, a blockwise (8×8 pixels) binary image is created to mark foreground and background regions. A block of 8×8 pixels is set as foreground if at least 80% of its pixels have values smaller than 10.
3) Based on the distance transform image, a gradient-based method [46] is used to estimate the orientation field in foreground blocks.
4) Orientation values in holes of foreground (missing data) are interpolated using values on their boundary.

Based on the orientation field, singular points are detected following an approach inspired by Zhou et al. [29].

1) Initial singular points are detected using Poincaré index method on the blockwise orientation field.
2) Orientation on the boundary is smoothened using a 2-D Gaussian filter ($\sigma = 4$).
3) The Poincaré index of the whole image is computed along the boundary.
4) Given the Poincaré index of the whole image, all valid combinations of singular points are determined [29].
5) For each valid combination of singular points, an energy function is evaluated. The combination that leads to the maximum energy is selected to give real singular points. The energy function measures the consistency, E, of the continuous orientation field θ_C:

$$E = \|mean(cos(2\theta_C)) + j \cdot mean(sin(2\theta_C))\|, \quad (1)$$

where θ_C is obtained by subtracting the orientation field determined by this set of singular points according to the Zero-Pole model [47] from the original orientation field [48].

Real singular points (if they exist) are removed from the original orientation field to obtain the continuous orientation field. A feature vector, termed as curvature histogram, is extracted from the continuous orientation field using the following approach:

1) For each row in the orientation field, difference of orientations, namely curvature, at adjacent blocks is computed and smoothened with a Gaussian filter ($\sigma = 2$). For natural fingerprints, the curvature curve generally has at most one sharp negative peak and its maximum curvature value is relatively small. While in altered fingerprints, this is not the case (see Fig. 16).
2) For the curvature curve for each row, the maximum curvature and the second minimum negative peak curvature are found (see Fig. 16).
3) The histograms of maximum curvatures and negative peak curvatures for all rows are computed each in 21 bins in the range $[-20, 20]$, which are collectively termed as curvature histogram.

The combined 42-dimensional curvature histogram is input to a support vector classifier for distinguishing between natural and altered fingerprints.

C. Performance

The four types of fingerprints (natural fingerprint and three types of altered fingerprints) of the first 1,000 fingerprints are used to train LIBSVM [49] and the four types of fingerprints of the remaining 976 fingerprints are used to test the algorithm. The scores output by LIBSVM are linearly scaled to the range $[0, 1]$. The normalized score is termed as *fingerprint-ness*. When the fingerprint-ness of an input image is smaller than a predetermined threshold value, the system raises an alarm for altered fingerprints. If this image is indeed an altered fingerprint, it is deemed to be a true detection; otherwise it is deemed to be a false alarm. The fingerprint-ness distribution shown in Fig. 17 indicates that natural fingerprints and altered fingerprints are well separated using our detection algorithm. The Receiver Operating Characteristic (ROC) curves of the proposed approach and NFIQ software are given in Fig. 18. At the same false alarm rate of 7% (NFIQ quality threshold value of 4, our threshold value of 0.58), around 92% altered fingerprints can be correctly detected using our approach, but only 20% altered fingerprints can be correctly detected using the NFIQ software.

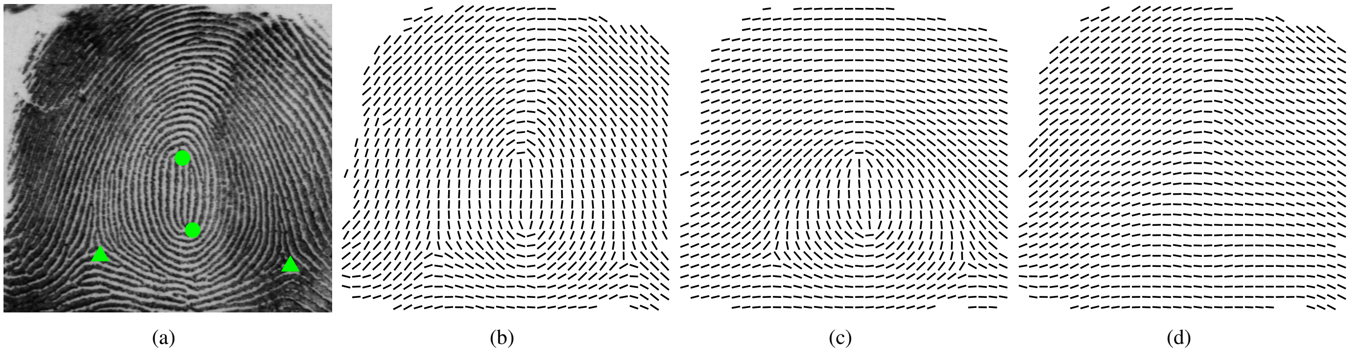


Fig. 14. Decomposition of orientation field. (a) Fingerprint image (NIST SD4, F0101. Core marked with disk, delta marked with triangle), (b) original orientation field, (c) singular orientation field, and (d) continuous orientation field.

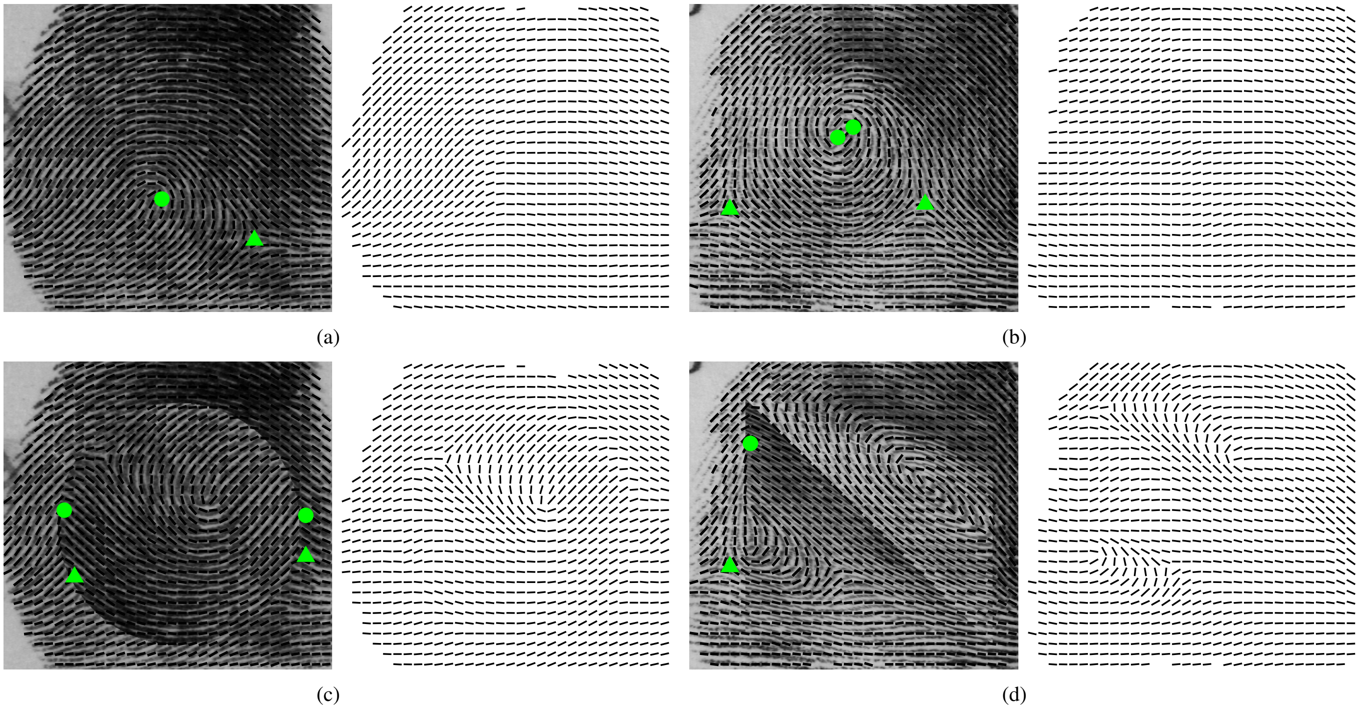


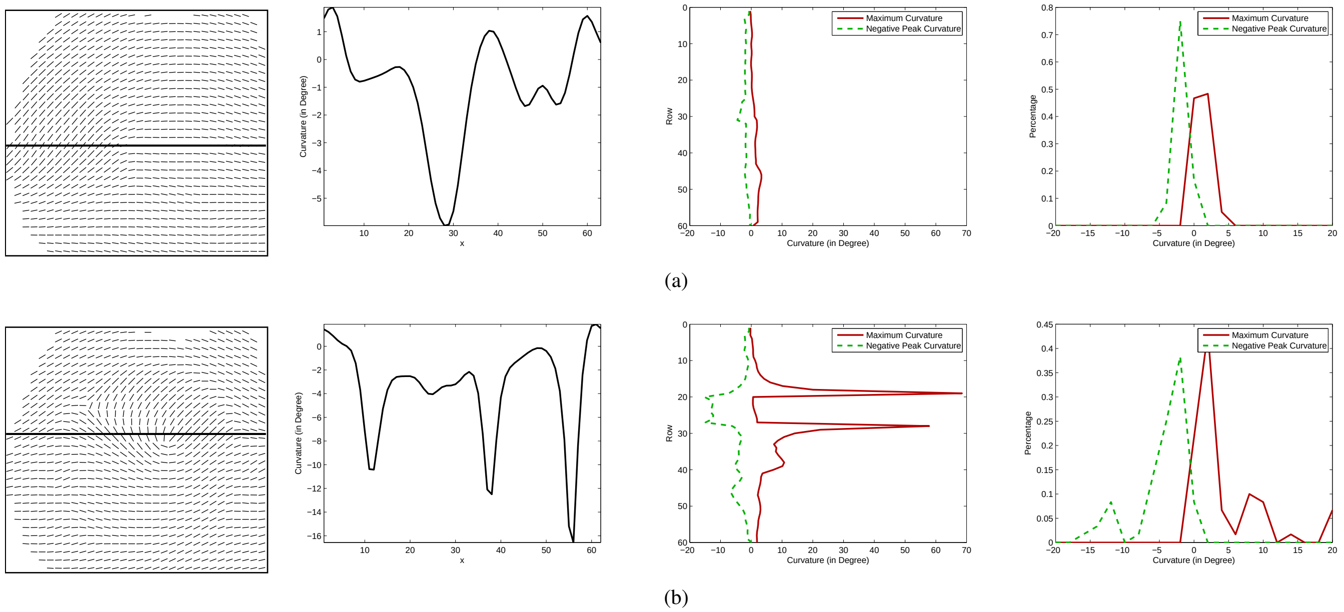
Fig. 15. Original orientation field and continuous orientation field, where real (optimal) singular points (core marked with disk, delta marked with triangle) are removed. (a) Original loop fingerprint (NIST SD4, F0017), (b) original whorl fingerprint (F0014), (c) altered fingerprint by central rotation (F0017), and (d) altered fingerprint by 'Z' cut (F0014).

We have also tested the proposed approach on two real altered fingerprints: the altered fingerprint in Fig. 3b and the altered fingerprint in Fig. 7b. NFIQ levels of these two altered fingerprints are 2 and 1, respectively. The scores of these two altered fingerprints according to our detection algorithm are 0.45 and 0.55, respectively. Both of them can be correctly detected, since their scores are below the threshold value of 0.58 at a false alarm rate of 7%.

VI. Summary and Future Work

The success of automated fingerprint identification systems has 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 increased attention in the literature, the problem of obfuscation has not been discussed in the biometric literature in spite of numerous documented cases of fingerprint alteration to evade identification. The lack of public databases containing altered fingerprints has further stymied research on this topic. While obfuscation may be encountered in biometric systems adopting other types of modalities (such as face and iris), this problem is especially significant in the case of fingerprints due to the widespread deployment of fingerprint systems in both government and civilian application and the ease with which these "attacks" can be launched. We have introduced the problem of fingerprint obfuscation and discussed a categorization scheme to characterize the various types of altered fingerprints that have been observed.

It is desirable to develop a method that can automatically



(a)

(b)

Fig. 16. Computation of curvature histograms of (a) a natural loop fingerprint (NIST SD4, F0017) and (b) an altered fingerprint by central rotation (F0017). From left to right: remaining orientation field (one row is marked), curvature curve on the marked row, maximum curvature curve and negative peak curvature curve on all rows, and curvature histogram.

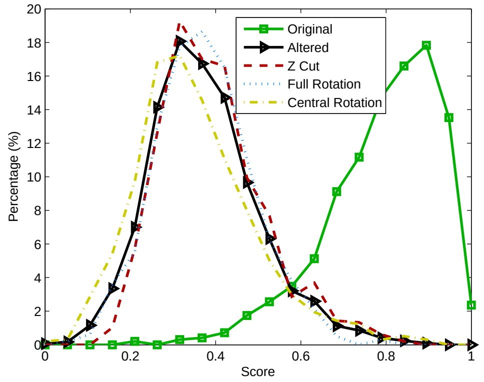


Fig. 17. Fingerprint-ness distributions of natural fingerprints, all altered fingerprints, and each of the three types of altered fingerprints of the last 976 fingerprints in NIST SD4.

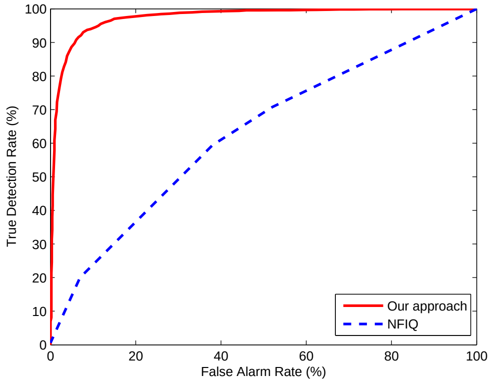
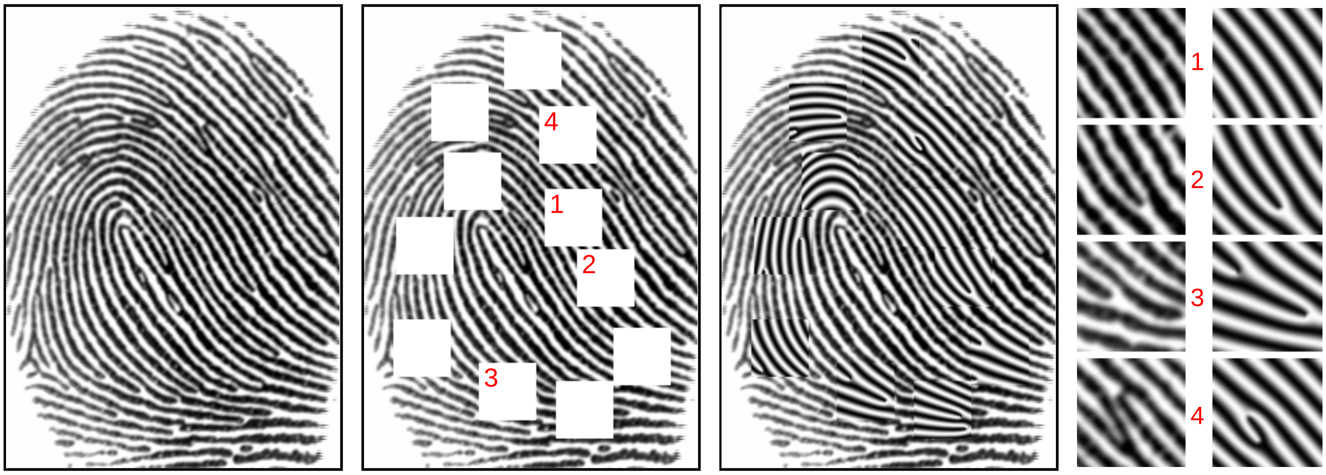


Fig. 18. ROC curves of our approach and NFIQ software in detecting altered fingerprints. Natural and three types of altered fingerprints of the last 976 fingerprints in NIST SD4 are used.

detect altered fingerprints and raise an alarm. Available fingerprint quality control software modules have very limited capability in distinguishing altered fingerprints from natural fingerprints. We have developed an algorithm to automatically detect altered (distorted) fingerprints. The underlying idea is that altered fingerprints often show unusual ridge patterns. A set of features is first extracted from the ridge orientation field of an input fingerprint and then a support vector classifier is used to classify it into natural or altered fingerprint. The proposed algorithm was tested using altered fingerprints synthesized in the way typically observed in operational cases with good performance.

The current altered fingerprint detection algorithm can be improved along the following directions:

1) Acquiring a database of real altered fingerprints. Our current algorithm is designed based on observing only a few real altered fingerprints. Its performance on fingerprints altered in different ways is not known. One way to identify real altered fingerprints is to run the current algorithm on operational government databases to find candidates which can be further verified manually.
2) Simulating more realistic altered fingerprints by modeling scars and improving the current skin distortion model.
3) Detecting scars. Scars often appear along the cuts on skin and are an important clue for altered fingerprints. By combining orientation field and scar information, it is possible to improve the detection rate of altered fingerprints.
4) Detecting alteration using all ten fingerprints by consid-



(a) (b) (c) (d)

Fig. 19. Reconstruction of original fingerprint from altered fingerprint. (a) Original fingerprint (FVC2002 DB1, 8_2), (b) simulated altered fingerprint, (c) reconstructed fingerprint from (b), and (d) the original images and the reconstructed images in four altered regions (marked in (b)). The similarity score between the original fingerprint in (a) and another image (8_8) of the same finger is 568 (according to VeriFinger SDK). After performing the alteration, the similarity score is reduced to 98. But after applying our reconstruction algorithm to the altered fingerprint in (b), the similarity score is improved to 331.

ering the fact that corresponding fingers in left and right hands of a person tend to be symmetric in pattern type and similar in ridge width [25].

5) Detecting alteration in plain fingerprints, which are more popular than rolled fingerprints in non-forensic applications.

After an altered fingerprint is detected, the process of successfully matching it against the mated unaltered fingerprint, which is very likely to be stored in the database, is very important. In some types of altered fingerprints, such as obliteration (Fig. 7a) or small-area transplantation (Fig. 10), ridge patterns are damaged locally. It is possible to reconstruct ridge pattern in the altered region using the unaltered ridge pattern in the neighborhood. We have tried a phase model based approach to interpolate the missing or altered region [50], [12]. The phase of local ridge pattern is modeled by a sum of a third-order polynomial and the spiral phase. Parameters are estimated by fitting the model to the phase on the boundary of the missing region. A preliminary result is shown in Fig. 19. The similarity score between the altered fingerprint and the mated unaltered fingerprint is significantly improved (from 98 to 331) after reconstruction, even though the reconstructed minutiae do not match the original ones perfectly.

Another approach to combat the growing threat of evading AFIS is the use of multibiometrics [51]. Federal agencies in the United States have adopted or are planning to adopt multibiometrics in their identity management systems, such as the FBI's NGI [52] and DoD's ABIS [53]. However, other biometric traits can also be altered successfully without affecting the basic function of the altered traits. It has been reported that plastic surgery can significantly degrade the performance of face recognition systems [54] and that cataract surgery can reduce the accuracy of iris recognition systems [55]. 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 necessary.

Acknowledgment

The authors would like to thank Brad Wing, NIST, for bringing this problem to their attention, and also recognize the assistance of Inspector Greg Michaud and Scott Blanchard, Michigan Forensic Laboratory, during the course of this study.

References

[1] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition (Second Edition)*. Springer-Verlag, 2009.

[2] The U.S. Department of Homeland Security, US-VISIT, http://www.dhs.gov/usvisit.

[3] The Federal Bureau of Investigation (FBI), Integrated Automated Fingerprint Identification System (IAFIS), http://www.fbi.gov/hq/cjisd/iafis.htm.

[4] H. Cummins, "Attempts to Alter and Obliterate Finger-prints," *Journal of American Institute of Criminal Law and Criminology*, vol. 25, pp. 982–991, 1935.

[5] 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, 2006.

[6] K. A. Nixon and R. K. Rowe, "Multispectral Fingerprint Imaging for Spoof Detection," in *Proc. SPIE, Biometric Technology for Human Identification II*, A. K. Jain and N. K. Ratha, Eds., vol. 5779, 2005, pp. 214–225.

[7] K. Singh, Altered Fingerprints, 2008, http://www.interpol.int/Public/Forensic/fingerprints/research/alteredfingerprints.pdf.

[8] M. Hall, "Criminals go to extremes to hide identities," *USA TODAY*, Nov. 6 2007, http://www.usatoday.com/news/nation/2007-11-06-criminal-extreme_N.htm.

[9] Criminals cutting off fingertips to hide IDs, 2008, http://www.thebostonchannel.com/news/15478914/detail.html.

[10] E. Tabassi, C. Wilson, and C. Watson, "Fingerprint Image Quality," NISTIR 7151, August 2004, http://fingerprint.nist.gov/NFIS/ir_7151.pdf.

[11] 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, 2007.

[12] J. Feng and A. K. Jain, "FM Model Based Fingerprint Reconstruction from Minutiae Template," in *Proc. 2nd International Conference on Biometrics (ICB)*, June 2009, pp. 544–553.

[13] R. Cappelli, D. Maio, and D. Maltoni, "Synthetic Fingerprint-Database Generation," in *Proc. 16th International Conf. on Pattern Recognition*, August 2002, pp. 744–747.

[14] K. Wertheim, “An Extreme Case of Fingerprint Mutilation,” *Journal of Forensic Identification*, vol. 48, no. 4, pp. 466–477, 1998.

[15] History of Fingerprint Removal, http://jimfisher.edinboro.edu/forensics/fire/print.html.

[16] J. Patten, Savvy criminals obliterating fingerprints to avoid identification, 2008, http://www.eagletribune.com/punews/local_story_062071408.html.

[17] Woman Alters Fingerprints to Deceive Taiwan Immigration Fingerprint Identification System, October 2008, http://www.zaobao.com/special/newspapers/2008/10/hongkong081002r.shtml (In Chinese).

[18] Altered fingerprints detected in illegal immigration attempts, http://www.japantoday.com/category/crime/view/altered-fingerprints-detected-in-illegal-immigration-attempts.

[19] Woman uses tape to trick biometric airport fingerprint scan, January 2 2009, http://www.crunchgear.com/2009/01/02/woman-uses-tape-to-trick-biometric-airport-fingerprint-scan/.

[20] Sweden Refugees Mutilate Fingers, 2004, http://news.bbc.co.uk/2/hi/europe/3593895.stm (accessed July 2009).

[21] Asylum Seekers Torch Skin off Their Fingertips So They Can’t Be ID’d by Police, 2008, 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/.

[22] 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.

[23] D. R. Ashbaugh, *Quantitative-Qualitative Friction Ridge Analysis: An Introduction to Basic and Advanced Ridgeology*. CRC Press, 1999.

[24] M. Kcken and A. C. Newell, “Fingerprint Formation,” *Journal of Theoretical Biology*, vol. 235, no. 1, pp. 71 – 83, 2005.

[25] H. Cummins and M. Midlo, *Finger Prints, Palms and Soles: An Introduction to Dermatoglyphics*. New York: Dover Publications, 1961.

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

[27] F. Galton, *Finger Prints (reprint)*. New York: Da Capo Press, 1965.

[28] R. Penrose, “The Topology of Ridge Systems,” *Annals of Human Genetics*, vol. 42, pp. 435 – 444, 1979.

[29] J. Zhou, F. Chen, and J. Gu, “A Novel Algorithm for Detecting Singular Points from Fingerprint Images,” *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 31, no. 7, pp. 1239–1250, 2009.

[30] R. Cappelli and D. Maltoni, “On the Spatial Distribution of Fingerprint Singularities,” *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 31, no. 4, pp. 742 – 748, 2009.

[31] FVC2002: the Second International Fingerprint Verification Competition, http://bias.csr.unibo.it/fvc2002/.

[32] C. L. Wilson, M. D. Garris, and C. I. Watson, “Matching Performance for the US-VISIT IDENT System Using Flat Fingerprints,” NISTIR 7110, May 2004, ftp://sequoyah.nist.gov/pub/nist_internal_reports/ir_7110.pdf.

[33] 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. National Academy of Sciences of the U.S.A.*, vol. 102, no. 21, pp. 7772–7775, 2005.

[34] V. N. Dvornychenko and M. D. Garris, “Summary of NIST Latent Fingerprint Testing Workshop,” NISTIR 7377, November 2006, http://fingerprint.nist.gov/latent/ir_7377.pdf.

[35] A. Yoshida and M. Hara, “Fingerprint Image Quality Metrics That Guarantees Matching Accuracy,” in *Proc. NIST Biometric Quality Workshop II*, March 2006, http://www.itl.nist.gov/iad/894.03/quality/workshop/proc/hara_nec_qualitymetrics.pdf.

[36] M. Hara, “Thoughts on Fingerprint Image Quality and Its Evaluation,” in *Proc. NIST Biometric Quality Workshop II*, November 2007, http://www.itl.nist.gov/iad/894.03/quality/workshop07/proc/Hara_NEC_Quality_NIST2007_Final.pdf.

[37] P. Lo, B. Bavarian, and Y. Luo, “Method and Apparatus for Determining Print Image Quality,” US Patent Application Publication No. 2008/0013803A1, 2008.

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

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

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

[41] M. Wong, S.-P. Choo, and E.-H. Tan, “Travel Warning with Capecitabine,” *Annals of Oncology*, 2009.

[42] K. Nandakumar, A. K. Jain, and A. Ross, “Fusion in Multibiometric Identification Systems: What about the Missing Data?” in *Proc. 2nd International Conference on Biometrics (ICB)*, June 2009, pp. 743–752.

[43] H. Plotnick and H. Pinkus, “The Epidermal vs. the Dermal Fingerprint: An Experimental and Anatomical Study,” *Archives of Dermatology*, vol. 77, no. 1, pp. 12 – 17, 1958.

[44] Neurotechnology Inc., VeriFinger, http://www.neurotechnology.com.

[45] H. L. Updegraff, “Changing of Fingerprints,” *The American Journal of Surgery*, vol. 26, pp. 533–534, 1934.

[46] L. Hong, Y. Wan, and A. K. Jain, “Fingerprint Image Enhancement: Algorithm and Performance Evaluation,” *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 20, no. 8, pp. 777–789, 1998.

[47] B. G. Sherlock and D. M. Monro, “A Model for Interpreting Fingerprint Topology,” *Pattern Recognition*, vol. 26, no. 7, pp. 1047 – 1055, 1993.

[48] J. Zhou and J. Gu, “Modeling Orientation Fields of Fingerprints with Rational Complex Functions,” *Pattern Recognition*, vol. 37, no. 2, pp. 389 – 391, 2004.

[49] C.-C. Chang and C.-J. Lin, *LIBSVM: a library for support vector machines*, 2001, software available at http://www.csie.ntu.edu.tw/~cjlin/libsvm.

[50] K. G. Larkin and P. A. Fletcher, “A Coherent Framework for Fingerprint Analysis: Are Fingerprints Holograms?” *Optics Express*, vol. 15, pp. 8667–8677, 2007.

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

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

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

[54] R. Singh, M. Vatsa, and A. Noore, “Effect of Plastic Surgery on Face Recognition: A Preliminary Study,” in *Proc. CVPR Workshop on Biometrics*, June 2009.

[55] R. Roizenblatt, P. Schor, F. Dante, J. Roizenblatt, and R. Belfort, “Iris Recognition As a Biometric Method after Cataract Surgery,” *American Journal of Ophthalmology*, vol. 140, no. 5, pp. 969 – 969, 2005.