

Automatic Detection of Altered Fingerprints

Anil K. Jain and Soweon Yoon
Michigan State University



A new algorithm detects changes to fingerprints due to mutilation and other similar measures criminals use to evade identification.

For more than a century, law enforcement investigators and forensic scientists have successfully used fingerprint recognition to identify criminals and victims. The technology advanced rapidly during the 1970s with the development of automated fingerprint identification systems (AFISs), spearheaded by the Federal Bureau of Investigation, which made it possible to quickly and accurately match a suspect's fingerprints with records in a large-scale database.

Local, state, and federal law enforcement agencies around the world routinely acquire fingerprints from apprehended criminal suspects on formatted 10-print cards to submit to organizations such as the FBI and Interpol along with latent prints collected from crime scenes. The FBI alone holds 10-prints from approximately 70 million criminal subjects and nearly 32 million civil and military employees in its Integrated AFIS (IAFIS).

The success of fingerprint identification in law enforcement and forensics has encouraged its use in various government and civilian applications ranging from

international border control to civil registration. For example, the US Department of Homeland Security relies on the US-VISIT system at border crossings to identify terrorists and other high-profile criminal suspects on watch lists as well as to detect possible visa fraud (www.dhs.gov/files/programs/usv.shtm). The

Unique Identification Authority of India is issuing 12-digit ID numbers linked to biometric data, including fingerprints, to the country's entire population (www.uidai.gov.in).

The widespread deployment of AFIS has prompted some criminals and illegal aliens to alter or obfuscate their fingerprints to evade detection.

IDENTITY SCIENCES SPOTLIGHT

To promote the study of identity sciences, this column will occasionally feature spotlights highlighting breakthrough technologies.

This spotlight focuses on the 2011 International Joint Conference on Biometrics (www.cse.nd.edu/IJCB_11). Held 11-13 October in Crystal City, Virginia, IJCB 2011 combined two highly successful biometrics conference series: the IEEE International Conference on Biometrics Theory, Applications, and Systems (2012: www.cse.nd.edu/BTAS_12) and the International Association of Pattern Recognition (IAPR) International Conference on Biometrics (2012: <http://icb12.iitd.ac.in>).

With more than 320 submissions and 107 accepted papers (31 oral and 76 poster presentations) from 26 different countries, IJCB 2011 was a huge success. The conference featured four tutorial sessions, a doctoral student consortium, and three eminent invited speakers: the University

of Southampton's Mark Nixon ("A History of Biometrics in the Media"), the University of Queensland's Brian C. Lovell ("Remote Face, Iris, and Appearance Biometrics for Border and Transport Security"), and the Intelligence Advanced Research Projects Activity's Michael C. King ("Current Successes and Future Directions of the BEST Program"). Video conference proceedings are available at <http://techtalks.tv/events/65>.

This month's Identity Sciences column is derived from the winner of the IAPR Best Biometrics Student Paper Award at IJCB 2011, an article that investigates the problem of falsified fingerprints by intentional physical mutilation.

To learn more about biometrics and IJCB 2011, view the video report from the conference by the University of Michigan's Charles Severance at <http://youtu.be/Qme90A5QpJc>.

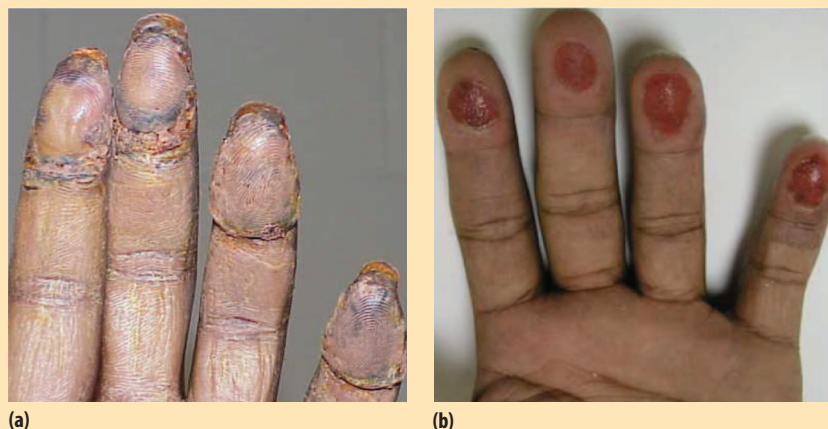


Figure 1. Examples of fingertip mutilation: (a) transplanted friction ridge skin from sole of foot and (b) bitten fingertips.

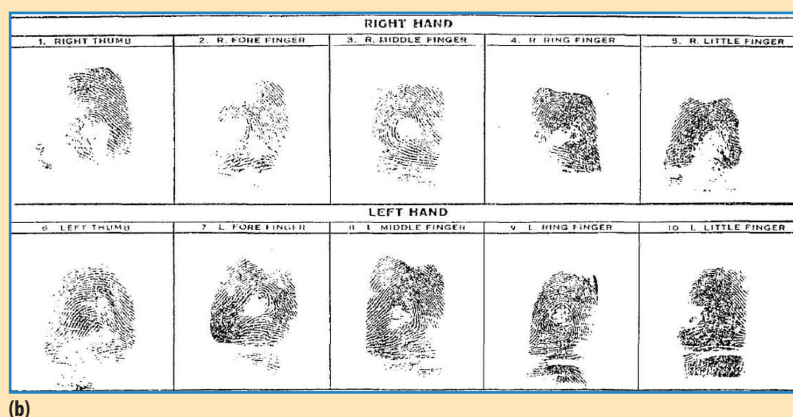


Figure 2. Early cases of fingerprint alteration. (a) Mutilation caused the fingerprint pattern of gangster Gus Winkler to change from twin loop (left) to left loop (right). (b) John Dillinger obfuscated the central part of his fingertips by applying acid to them.

FINGERPRINT ALTERATION

Criminals are increasingly using extreme measures including abrading, cutting, burning, biting, or surgically modifying their fingertips to mask their identity (K. Singh, "Altered Fingerprints," 27 Oct. 2008, Interpol General Secretariat, Lyon, France; www.interpol.int/Public/Forensic/fingerprints/research/alterdfingerprints.pdf).

Figure 1 shows two recent examples. In 2005, an alleged drug dealer paid an Arizona plastic surgeon \$20,000 to transplant skin from the sole of his foot to his fingertips to avoid apprehension (Figure 1a); a car thief arrested by the Massachusetts State Police in 2007 chewed off the central part of his fingertips while in custody to avoid conviction (Figure 1b).

In 2009, a woman initially bypassed Japan's immigration AFIS by swapping the skin on the fingertips of her left and right hands (K.M. Huessner, "Surgically Altered Fingerprints Help Woman Evade Immigration," *ABC News*, 11 Dec. 2009).

As Figure 2 shows, fingerprint alteration isn't a new phenomenon. As early as 1933, Gus Winkler, a bank robber and contract killer, slashed and abraded the flesh on his fingers, altering the pattern type of one of his fingerprints from twin loop to left loop. Around the same time, the infamous John Dillinger applied acid to his fingertips, obfuscating the central parts of some of his fingerprints.

Both the purpose and methodology of fingerprint alteration distinguish it from fingerprint spoofing—using fake fingerprints, typically of glue or silicone, to adopt another person's identity. Although the biometrics literature on fingerprint spoofing is substantial, researchers have given little attention to fingerprint alteration.

Fingerprint alteration is a serious threat to AFISs: low similarity between an altered fingerprint and its prealtered mates can significantly degrade matching performance.

Figure 3 shows three different fingerprints from a single finger; the images in Figures 3a and 3b were obtained before the fingertip was altered, and the image in Figure 3c was obtained after alteration. The two prealtered impressions match almost perfectly on a commercial matching system; their genuine match score is 21,083, which is very close to the matcher's highest possible similarity score. However, when the system compares the two prealtered fingerprints to the altered fingerprint, the scores are 2,898 and 1,861, respectively; they are deemed impostor matches.

DETECTING ALTERED FINGERPRINTS

A system that automatically detects altered fingerprints is on the

desired list of most border control agencies, which would use it to identify subjects with questionable fingerprints such as to screen these individuals more carefully to validate their identity.

At Michigan State University, we've developed an algorithm that automatically detects altered fingerprints by assessing abnormality in two fundamental fingerprint features: the *orientation field* (OF), which describes the ridge flow, and the *minutiae*, ridge bifurcation and ending points (S. Yoon, J. Feng, and A.K. Jain, "Altered Fingerprints: Analysis and Detection," to appear in *IEEE Trans. Pattern Analysis and Machine Intelligence*, 2012; www.cse.msu.edu/~yoonsoo/Publications/AlteredFP_PAMI2011.pdf). Figure 4 illustrates how the process works.

The local ridge structure's tangential direction identifies a fingerprint's OF. In a natural fingerprint, the OF is continuous except in the neighborhood of singular points known as cores and deltas, where ridge flow abruptly changes. In contrast, an altered fingerprint's OF is discontinuous where there are scars or in mutilated areas.

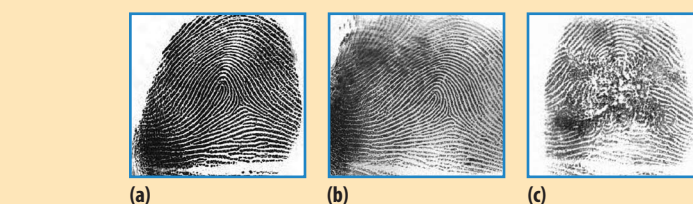


Figure 3. Three different fingerprint impressions of the same finger obtained (a) and (b) before alteration and (c) after alteration. While the genuine match score between (a) and (b) is 21,083, alteration severely degrades match performance: the match score between (a) and (c) is 2,898 and the match score between (b) and (c) is 1,861.

To determine OF discontinuity in a fingerprint, the algorithm computes the difference between the OF extracted from the fingerprint image and the OF fit by a polynomial model. Figures 4b and 4g show the OFs extracted from a natural fingerprint in Figure 4a and an altered fingerprint with a z-shaped cut in Figure 4f, respectively. The discontinuity in the natural OF is evident only in local areas corresponding to cores and deltas (Figure 4c), while the altered fingerprint has a discontinuous OF over a larger area along the scars (Figure 4h).

Another indication of fingerprint alteration is the spatial distribution of minutiae. Most fingerprint-matching

algorithms determine the similarity between a pair of fingerprints by comparing the spatial distributions of two minutiae sets. Minutiae in altered fingerprints tend to form clusters in the altered region—for example, a scar generates a large number of ridge endings—while minutiae in natural fingerprints are distributed rather uniformly.

Our algorithm uses the Parzen window method to estimate minutiae density. A map for the altered fingerprint (Figures 4i and 4j) shows higher density along the scarred area compared to the natural fingerprint (Figures 4d and 4e).

An initial search of the 27,000 fingerprints in the National Institute

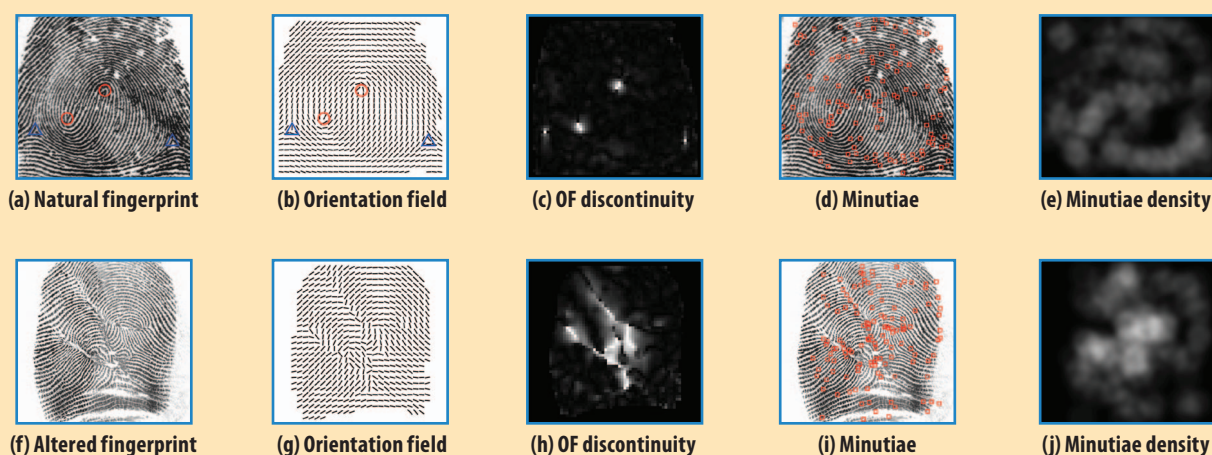


Figure 4. Altered fingerprint detection. Orientation field (OF) discontinuity and minutiae density features from (a)-(e), a natural fingerprint, and (f)-(j), an altered fingerprint. Circles and triangles in (a) and (b) indicate cores and deltas where fingerprint ridge flow abruptly changes.



NEW ISSUE ALERTS!

Stay connected with the IEEE Computer Society Transactions by signing up for our new and improved Issue Alerts. They are free and contain valuable information like:

- News about your favorite transactions,
- Contributions from the Editorial Board,
- Information about related conferences,
- Top 5 recent downloaded papers,
- And much more.

Not a subscriber? Don't worry. You can still sign up to receive news about the transactions.

Visit <http://www.computer.org/newsletters> to sign up today!



IEEE computer society




(a)



(b)

Figure 5. Potentially altered fingerprints identified in NIST SD14, a public domain fingerprint database.

of Standards and Technology's Special Database 14, a public domain database, using the algorithm revealed the presence of multiple potentially altered fingerprints. Figure 5 shows two examples.

We continue to research ways to identify subjects with altered fingerprints. We are currently refining our algorithm to utilize information in unaltered areas of the fingerprint. 

Anil K. Jain is a University Distinguished Professor in the Department of Computer Science and Engineering at Michigan State University. Contact him at jain@cse.msu.edu.

Soweon Yoon is a PhD student in the Department of Computer Science and Engineering at Michigan State University. Contact her at yoonsowo@cse.msu.edu.

Editor: Karl Ricanek Jr., director of the Face Aging Group at the University of North Carolina Wilmington; ricanekk@uncw.edu

NEW

ESSENTIAL INDUSTRIAL IMPLEMENTATIONS OF FLOATING-POINT UNITS DURING THE LAST DECADE:

VOLUMES 1 & 2

Transactions on Computers {EssentialSets} Available:

Edited by TC AE Elisardo Antelo, this EssentialSet surveys the industrial design of floating-point units during the last decade. This EssentialSet is broken into two volumes, sold separately.

PDF edition • \$15 each (\$9 members)

Order Online: computer.org/store.



IEEE computer society

