2010 International Conference on Pattern Recognition

Detecting Altered Fingerprints

Jianjiang Feng
Dept.of Automation
Tsinghua University
Beijing, China
jfeng@tsinghua.edu.cn

Anil K. Jain
Dept.of Computer Science
Michigan State University
East Lansing, MI, USA
jain@cse.msu.edu

Arun Ross
Lane Dept.of CSEE
West Virginia University
Morgantown, WV, USA
arun.ross@mail.wvu.edu

***Abstract*—The widespread deployment of Automated Fingerprint Identification Systems (AFIS) in law enforcement and border control applications has prompted some individuals with criminal background to evade identification by purposely altering their fingerprints. Available fingerprint quality assessment software cannot detect most of the altered fingerprints since the implicit image quality does not always degrade due to alteration. In this paper, we classify the alterations observed in an operational database into three categories and propose an algorithm to detect altered fingerprints. Experiments were conducted on both real-world altered fingerprints and synthetically generated altered fingerprints. At a false alarm rate of 7%, the proposed algorithm detected 92% of the altered fingerprints, while a well-known fingerprint quality software, NFIQ, only detected 20% of the altered fingerprints.**

Keywords-fingerprints; alteration; fingerprint image quality; orientation field

I. INTRODUCTION

For over 100 years, law enforcement agencies have successfully used fingerprints to identify suspects and victims. 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. Examples of large-scale fingerprint systems in include US-VISIT's IDENT system and the FBI's IAFIS system. The success of fingerprint recognition systems in accurately identifying individuals has prompted some criminals to engage in extreme measures for the purpose of evading identification.

Fingerprint alteration is not a new phenomenon. As early as in 1934, John Dillinger, the infamous bank robber and a dangerous criminal, applied acid to his fingertips [1]. Since then, there has been an increase in the reported cases of fingerprint alteration. In 1995, a criminal was found to have altered his fingerprints by making a 'Z' shaped cut into the finger and switching the finger skin the two parts (see Fig. 1). In 2009, a Chinese woman successfully deceived the Japan immigration fingerprint system by performing surgery to swap fingerprints on her left and right hands [3]. Fingerprint alteration has even been performed at a much larger scale involving multiple individuals. Hundreds of asylum seekers have cut, abraded, and burned their fingertips to prevent identification by EURODAC, a European Union fingerprint system for identifying asylum seekers [2]. Additional cases of fingerprint alteration have been compiled in [2].

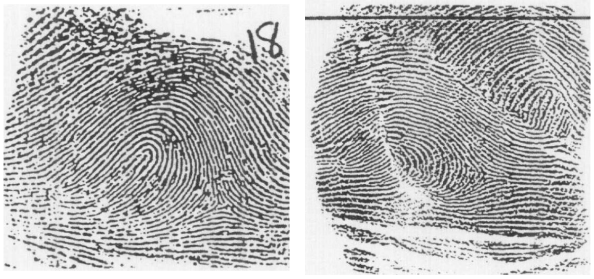


Figure 1. A fingerprint altered by switching two parts of a 'Z' shaped cut [2].

The primary purpose of fingerprint alteration [1] is to evade identification using techniques that vary from abrading, cutting, and burning fingers to performing plastic surgery. Fingerprint alteration constitutes a serious "attack" against a border control fingerprint identification system since it defeats the very purpose for which the system was deployed in the first place, i.e., to identify individuals on a watch-list.

Fingerprint image quality modules used in most fingerprint systems, such as the open source NFIQ (NIST Fingerprint Image Quality) software [4], may be useful in detecting altered fingerprints if the corresponding images are of poor image quality or contain very few minutiae. However, all the altered fingerprint images may not necessarily be of poor quality or contain a small number of minutiae (see Fig. 1). The goal of this paper is to introduce the problem of fingerprint alteration and to develop methods to automatically detect altered fingerprints.

II. 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. 2). With fingerprint obliteration, friction ridge

1051-4651/10 $26.00 © 2010 IEEE
DOI 10.1109/ICPR.2010.401

patterns on fingertips are obliterated by abrading, cutting, burning, applying strong chemicals, or transplanting smooth skin (see Fig. 2a). The damaged finger area needs to be sufficiently large to defeat fingerprint matchers. But, fingerprint quality control software can easily detect such alterations and raise an alarm prompting human operators to examine the finger. For example, the obliterated fingerprint in Fig. 2a is assigned the lowest quality level of 5 by the NFIQ software.

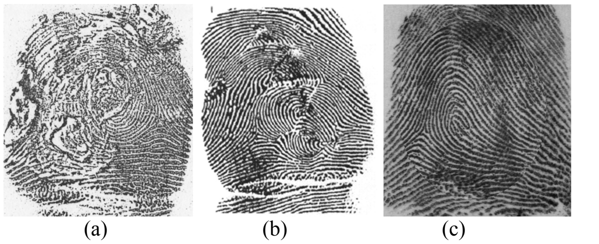


Figure 2. Three types of fingerprint alterations: (a) Obliteration, (b) distortion, and (c) imitation (simulated).

In cases of fingerprint distortion, friction ridge patterns on fingertips are turned into unnatural ridge patterns by a surgical procedure, in which portions of skin are removed from a finger and grafted back in different positions (see Fig. 2b). Distorted fingerprints may pass fingerprint quality control software as distortions do not necessarily reduce the image quality. For instance, the distorted fingerprint in Fig. 2b is assigned the highest quality level of 1 by the NFIQ software.

In fingerprint imitation, friction ridge skin from other parts of the body, such as fingers, palms, toes, and soles, is transplanted to the original finger in such a way that the altered fingerprint appears as a natural fingerprint pattern. Fig. 2c shows an example of imitation, where the central region of the original fingerprint is replaced with the central region of a different fingerprint. Imitated fingerprints can successfully evade fingerprint quality control software. If the surgical scars due to the transplantation are small, the altered fingerprints can even deceive inexperienced human operators.

III. Detection of Altered Fingerprints

In this study, 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 fingerprint quality control software, and (ii) imitated fingerprints may look very natural and there are no images of this type currently available in the public domain to undertake such a study.

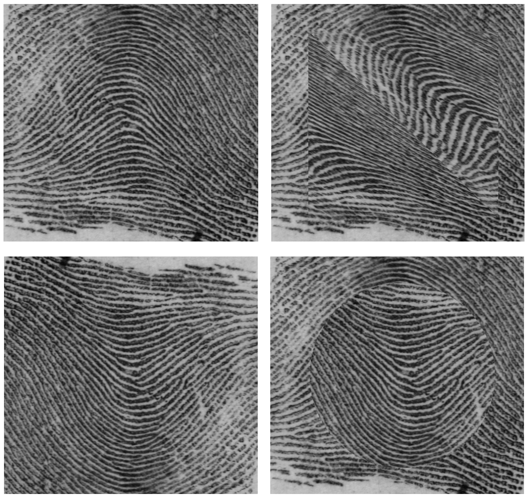


Figure 3. An original fingerprint and its altered versions: ‘Z’ cut, full rotation, and central rotation.

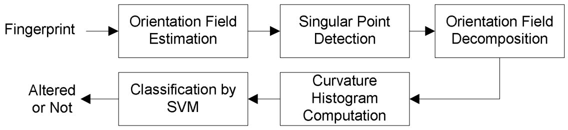

Fingerprint
Orientation Field Estimation
Singular Point Detection
Orientation Field Decomposition
Curvature Histogram Computation
Classification by SVM
Altered or Not

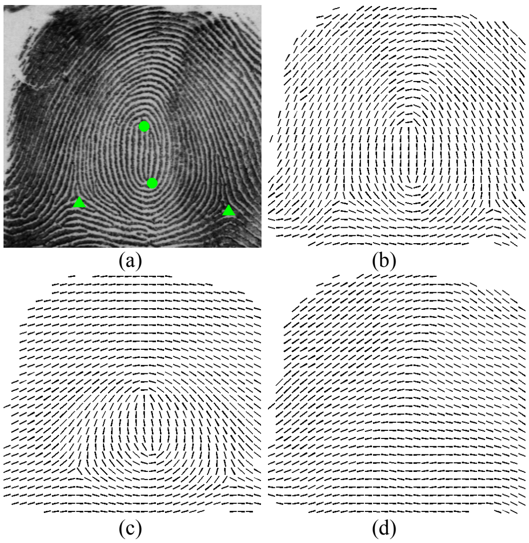
Figure 4. Flowchart of the proposed algorithm.

A. Simulation

Due to lack of a public database of altered fingerprint images, it is necessary to conduct our study on synthetically altered images. This also allows researchers to leverage the techniques designed here and utilize them in operational settings.

We used a public domain database, NIST SD4, 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 in the range [1, 4][1]. For each of these fingerprints, three types of alterations were simulated (see Fig. 3): (i) ‘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%), (ii) full rotation (the entire fingerprint is rotated by 180 degrees), and (iii) central rotation (the central region with a radius of $0.35r$ in a fingerprint is rotated by 180 degrees, where r is the shorter side length of the bounding box of the fingerprint).

[1] A fingerprint with the worst quality level (NFIQ value of 5) should raise a flag to draw an officer's attention. Thus, automatic alteration detection is not necessary for such altered fingerprints.


(a) (b)

(c) (d)

Figure 5. Decomposition of orientation field: (a) original fingerprint with marked singularities, and the associated (b) original, (c) singular, and (d) continuous orientation fields.

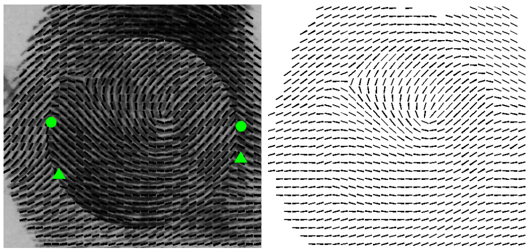


Figure 6. Original and continuous component orientation fields of an altered fingerprint simulated by central rotation.

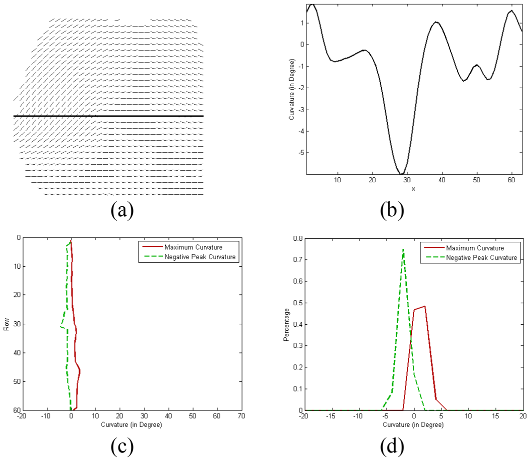
B. Detection

We detect altered fingerprints based on analyzing the ridge orientation field (see flowchart in Fig. 4). 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. 5): singular orientation field and continuous orientation field. As can be observed in Figs. 5 and 6, the continuous orientation field of the original fingerprint is indeed continuous (i.e., no singularity), but the continuous component of the orientation field of the altered fingerprint is actually not continuous! We extract high level features from the continuous orientation field and use a support vector machine (SVM) 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 from the skeleton image output by the VeriFinger SDK. Based on the orientation field, singular points are detected following the approach in [5]. Singular orientation field (zero-pole model in [6]) is subtracted from the original orientation field to obtain its continuous component. A feature vector, called the curvature histogram, is extracted from continuous orientation field using the following approach (see Fig. 7):

1) Compute difference of orientations, namely curvature, along the horizontal direction and smooth it with a Gaussian filter ($\sigma = 2$). For natural fingerprints, the curvature curve for each image row has at most one sharp negative peak and the maximum (positive) curvature value is small.
2) Find the maximum curvature and the second minimum negative peak curvature for each image row.
3) Compute the histograms of maximum curvatures and negative peak curvatures for all image rows in 21 bins in the range [-20, 20], which are collectively termed as the curvature histogram.

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



(a) (b)

(c) (d)

Figure 7. Computation of curvature histograms of a fingerprint: (a) Continuous orientation field, (b) curvature curve for the marked row in (a), (c) maximum curvature and negative peak curvature curves, and (d) curvature histogram.

C. Experimental Results

Four images (original fingerprint and three types of altered fingerprints) of the first 1,000 fingerprints in SD4 are used to train LIBSVM [7] The remaining 976 fingerprints and its altered versions 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, system raises an alarm for altered fingerprints. If this image is indeed an altered fingerprint, it is a true detection; otherwise it is a false alarm.

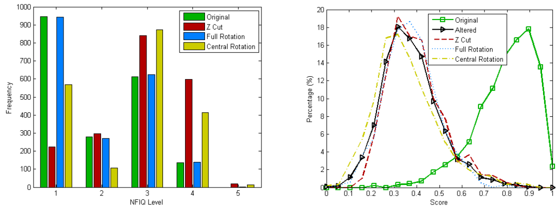


Figure 8. Distributions of NFIQ (left) and fingerprint-ness (right) of original fingerprints in NIST SD4 and three types of altered fingerprints.

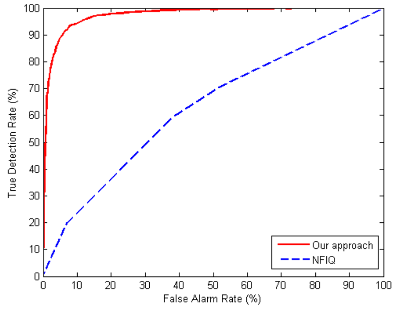


Figure 9. ROC curves of NFIQ and our approach.

The distributions of NFIQ values and fingerprint-ness of original and altered fingerprints are shown in Fig. 8. The proposed algorithm can separate original fingerprints from altered fingerprints much better than NFIQ. As shown in the ROC curves in Fig. 9, at a false alarm rate of 7% (NFIQ value of 4, our threshold value of 0.58), 92% of the altered fingerprints were detected using our approach, but only 20% of them were detected by NFIQ.

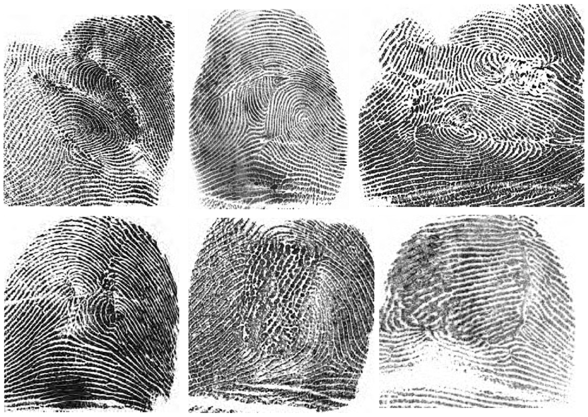


Figure 10. Real-world altered fingerprints.

We have also tested our method on ten real-world altered fingerprints whose NFIQ values are in the range [1, 4]. The scores of seven of them according to our algorithm are below the threshold value of false alarm rate of 7%. The other three (bottom row of Fig. 10) cannot be detected because the altered area is small.

IV. Summary and Future Work

The success of automated fingerprint identification systems has prompted some criminals to take extreme measures to evade identification by altering their fingerprints. It is necessary to develop a method that can automatically detect altered fingerprints. Available fingerprint quality control software modules were not designed to distinguish altered from natural fingerprints. We have developed an algorithm to automatically detect altered fingerprints. The underlying idea is that altered fingerprints often show unusual ridge patterns. A set of features is extracted from the ridge orientation field and then a support vector classifier is used to classify the fingerprint as natural or altered. The proposed algorithm was tested using altered fingerprints synthesized in ways typically observed in operational cases and a small number of available real altered fingerprints.

We have not yet considered an important clue for detecting altered fingerprints, namely scars, which often appear along the cuts on finger skin. We are currently working on combining orientation field and scar information to further improve the detection rate of altered fingerprints.

Acknowledgment

This research was supported by a grant from CITeR. We would like to thank John Manzo of the FBI during the course of this study. Anil Jain's research was partially supported by WCU (World Class University) program through the National Research Foundation of Korea funded by the Ministry of Education, Science and Technology (R31-2008-000-10008-0).

References

[1] H. Cummins, “Attempts to Alter and Obliterate Fingerprints,” Journal of American Institute of Criminal Law and Criminology, vol. 25, pp. 982–991, 1935.

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

[3] Surgically Altered Fingerprints Help Woman Evade Immigration, Dec. 2009. http://abcnews.go.com/

[4] E. Tabassi, C. Wilson, and C. Watson, “Fingerprint Image Quality,” NISTIR 7151, August 2004.

[5] J. Zhou, F. Chen, and J. Gu, “A Novel Algorithm for Detecting Singular Points from Fingerprint Images,” IEEE PAMI, vol. 31, no. 7, pp. 1239–1250, 2009.

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

[7] C.-C. Chang and C.-J. Lin, LIBSVM: a library for support vector machines, 2001.