Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 5, Issue. 1, January 2016, pg.178 – 182

An Analysis of Altered Fingerprint Detection, Recognition and Verification

Mr. A. Vinoth M.C.A, M.Phil, [Ph.D]
Research Scholar, Department of Computer Science, Bharathiyar University, Coimbatore – 641 046
vino.asstprof@gmail.com

Dr. S. Saravanakumar
Professor, Department Computer Science & Engineering, PR Engineering College, Vallam, Thanjur
somansk@yahoo.com

Abstract- The common positioning of Automated Fingerprint Identification Systems (AFIS) in law enforcement and border control submissions has sensitive the need for safeguarding that these systems are not compromised. Whereas numerous problems associated to fingerprint system safekeeping have been considered, including the use of phony fingerprints for masquerading personality, the problem of fingerprint alteration or obfuscation has received very little attention. Fingerprint obfuscation refers to the measured alteration of the fingerprint pattern by an individual for the purpose of screening his identity. Several cases of fingerprint obfuscation have been reported in the press. Fingerprint image quality assessment software (e.g., NFIQ) cannot always identify altered fingerprints since the implicit image quality due to alteration may not change significantly.

Keywords: Fingerprints, alteration, image enhancement

I. INTRODUCTION

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. 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 amuch larger scale involving multiple individuals. Hundreds of asylum seekers have cut, abraded, andburned 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]. The primary purpose offingerprint 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 mostfingerprint systems, such as the open source NFIQ (NISTFingerprint Image Quality) software [4], may be useful indetecting altered fingerprints if the corresponding imagesare of poor image quality or contain very few minutiae.However, all the altered fingerprint images may notnecessarily be of poor quality or contain a small

number ofminutiae (see Fig. 1). The goal of this work is to introducethe problem of fingerprint alteration and to developmethods to automatically detect and classify alteredfingerprints.

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 analysing 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.

Fig. 1. A Fingerprint altered by switching two parts of a 'Z' Shaped Cut

TABLE - 1
High Profile Cases of Fingerprint Alteration

Case	Year	Alteration Type	Description
Criminal Cases			
Gus Winkler[2]	1933	Imitation	Pattern Type Changed From Double Loop To Left Loop
John Dillinger[5]	1934	Obliteration	Fingerprint Were Mutilated By Applying Acid
Robert J. Philipps[8]	1941	Obliteration	Skin From The Chest Was Transplanted To The Fingertips
Jose Izquierdo[7]	1997	Distortion	A Finger Print With Strange Pattern Was Formed By "Z" Cut
Marc George[11]	2005	Imitation	Friction Ridge Skin From Sole Was Implanted To The Fingertips
A man Arrested For Vehicle Theft[12]	2007	Obliteration	Fingers were bitten
Mateo Cruz-Cruz[13]	2007	Obliteration	Fingerprints Were Blackened As A Result Of Applying Acid
Gerald Perez[9]	2008	Obliteration	Fingertips With Thick Stitches
Non - Criminal Cases			
A Woman at a Border Crossing[11]	2007	Obliteration	A Surgery Was Performed On Fingertips To Generate Strange Fingerprint Pattern

A Woman Attempting To Evade The Japanese Border Control Systems[15]	2009	imitation	Friction Ridge Skins From Thumbs And Index Fingers Were Swapped Between Left And Right Hands
Three Peoples Charged With Conspiring To Mutilate Fingerprints[17]	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.

II. TYPE OF ALTERED FINGERPRINT

According to the changes made to the ridge patterns, fingerprint alterations may be categorized into three types:
a) Obliteration
b)Distortion
c) Imitation (see Fig. 4).
For each type of alteration, its characteristics and possible countermeasures are described.

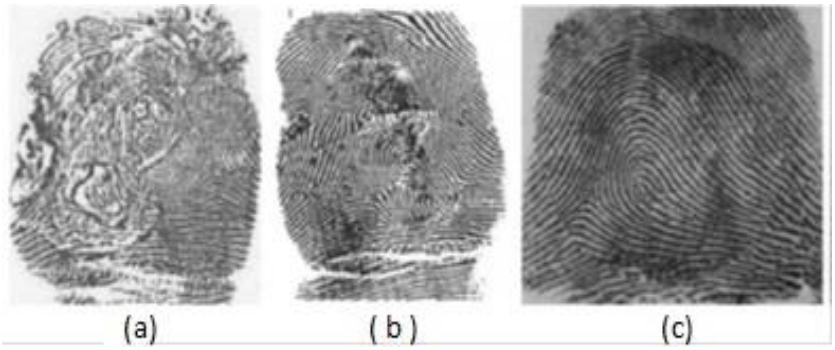

Fig.4. Three types of altered fingerprints. (a) Obliterated fingerprint (e.g., by burning,) (b) distorted fingerprint (c) imitated fingerprint (simulated by replacing the central region of the original fingerprint with the central region of a different fingerprint.

A. Obliteration

Friction ridge patterns on fingertips can be obliterated by abrading, cutting, burning, applying strong chemicals, and transplanting smooth skin. Further, factors such as skin disease (such as leprosy) and side effects of a cancer drug can also obliterate fingerprints.

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. Friction skin transplantation resulting in unnatural ridge patterns also belongs to this category. 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.

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. 5), or even cutting and mosaicking multiple small portions of friction skin (see simulation in Fig. 6).

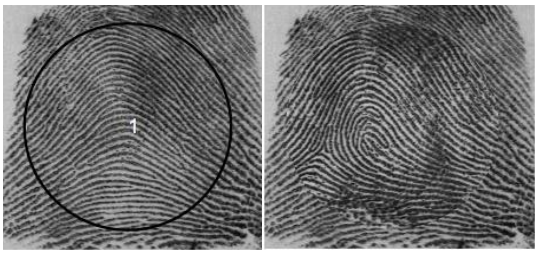

Fig.5. Simulation of large-area transplantation between two fingerprints:
(a) Original fingerprint
(b) Altered fingerprint by transplanting central area Transplanted fingerprints can successfully evade existing fingerprint quality control software. If the surgical scars due to the transplantation are small, it can even deceive in experienced 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 thesame person as in the Marc George's case. Small area transplantation is probably a more complicated surgery. Fig.6. Simulation of small-area transplantation within a finger. (a) Original fingerprint 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

III. PROPOSEDWORK

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 finger- print 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 detect altered fingerprints. Available fingerprint quality control software modules have very limited capability in distinguishing altered fingerprints from natural fingerprints. Here we proposed an algorithm to automatically detect altered (distorted) fingerprints and classify according to its type. The underlying idea is that altered fingerprints often show unusual ridge patterns.

IV. CONCLUSION AND FUTUREWORK

The proposed algorithm will be 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. Determine the alteration type efficiently and automatically so that appropriate countermeasures can be taken.
2. Reconstruct altered fingerprints. For some types of 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.

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/alte redfingerprints.pdf
[3] Surgically Altered Fingerprints Help Woman Evade Immigration, Dec. 2009. http://abcnews.go.com
[4] NIST Special Database 4, NIST 8-Bit Gray Scale Images of Fingerprint Image Groups (FIGS), http://www.nist.gov/srd/nistsd4.htm.
[5] D. R. Ashbaugh, Quantitative-Qualitative Friction Ridge Analysis: An Introduction to Basic and Advanced Ridgeology. CRC Press, 1999.
[6] M. Kcken and A. C. Newell, "Fingerprint Formation," Journal of Theoretical Biology, vol. 235, no. 1, pp. 71 – 83, 2005.
[7 H. Cummins and M. Midlo, Finger Prints, Palms and Soles: An Introduction to Dermatoglyphics. New York: Dover Publications, 1961.
[8] F. Galton, Finger Prints (reprint). New York: Da Capo Press, 1965.
[9] 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/ir7110.pdf.
[10] 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
[11] Anil K Jain, Soweon Yoon, JianjiangFeng ,"AlteredFingerprints:Analysis and De tection",IEEE transaction onpattern analysis and machine intelligence , Vol.34, 2012
[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, "AComparative Study of Fingerprint Image-Quality EstimationMethods," 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 BeID'd by Police, http://www.mirror.co.uk/sunday-mirror/2008/06/29/asylum-seekers-torch-skin-off-their fingertips-so-they-cant-be-id-d-by-police-98487-20624559/, 2008.

