International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 5, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

A Survey Paper on Altered Fingerprint Identification & Classification

Ram Kumar, Jasvinder Pal Singh, Gaurav Srivastava

Abstract – **Fingerprint recognition is one of the most commonly used biometric technology. Even if fingerprint temporarily changes (cuts, bruises) it reappears after the finger heals. Criminals started to be aware of this and try to escape the identification systems applying methods from ingenious to very cruel. It is possible to remove, alter or even fake fingerprints (made of glue, latex, silicone), by burning the fingertip skin (fire, acid, other corrosive material), by using plastic surgery (changing the skin completely, causing change in pattern – portions of skin are removed from a finger and grafted back in different positions, like rotation or "Z" cuts, transplantations of an area from other parts of the body like other fingers, palms, toes, soles). This paper presents a new algorithm for altered fingerprints detection based on fingerprint orientation field reliability. The map of the orientation field reliability has peaks in the singular point locations. These peaks are used to analyze altered fingerprints because, due to alteration, more peaks as singular points appear with lower amplitudes.**

Keywords – **Fingerprints, alteration, image enhancement, reliability, singular points.**

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. 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].

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 work is to introduce the problem of fingerprint alteration and to develop methods to automatically detect and classify altered fingerprints.

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

II. Literature Review

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 alteredones. 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 Fig. 2. Ridge endings (marked with white circles) and ridge bifurcations (marked with black squares). Image is cropped from fingerprint F0134 in NIST SD4 database [4]. 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 [5]. The bottom

International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 5, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

(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 [6]. Superficial cuts on the surface ridges that do not damage the bottom ridges only temporarily change the surface ridges; after theinjury 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.

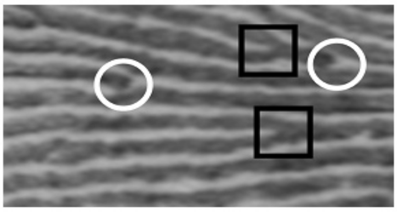

Fig.2. Ridge endings (marked with white circles) and ridge bifurcations (marked with black squares). Image is cropped from fingerprint F0134 in NIST SD4 database [4].

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 [7]. 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. 2). 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. 3) [8]. 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 finge nail) [6]. 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. 3) [7]. 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.

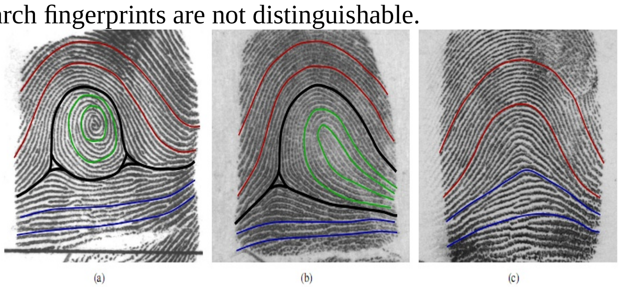

Fig.3. Three major fingerprint pattern types: (a) whorl, (b) loop, and (c) arch. Three different ridge systems [8] are marked with lines in different colors(red for distal transverse ridges, green for pattern area ridges, and blue for proximal transverse ridges). Type lines are shown as wide black lines

A. 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) [9], [10]. 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 [10]), no specific software is yet available to reconstruct the original pattern of altered fingerprints.

III. 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

International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 5, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

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 transplanttation 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).

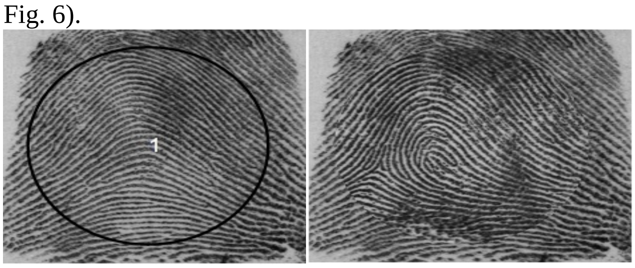

Fig.5. Simulation of large-area transplantation between two fingerprints: (a) Original fingerprint (b) altered fingerprint by transplanting central area

Transplanted fingerprints can successfully evade existing fingerprint quality control software. If the surgical scars due to the transplantation are small, it can even deceive inexpe- rienced 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. Small area transplantation is probably a more complicated surgery.

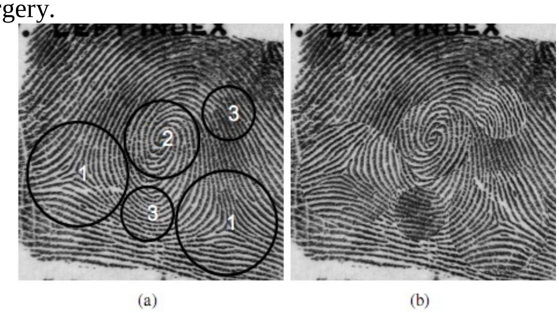

Fig.6. Simulation of small-area transplantation within a finger. (a) Original fingerprint and (b) altered fingerprint. Simulation is performed by exchanging and rotating circular regions (marked with the same number) to match the local ridge orientation or just rotating circular regions(marked with number 2) by 180 degrees

IV. Proposed 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 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.

V. Methodology

The NFIQ algorithm is not suitable for detecting altered fingerprints, especially the distortion and imitation types. In fact, the distorted and imitated fingerprints are very hard to detect for any fingerprint image quality assessment algorithm that is based on analyzing local image quality[11]. In this section, we consider the problem of

International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 5, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

automatic detection of alterations and classification based on analyzing singular point reliability map of orientation field. The flowchart of the proposed alteration type detector is given in Fig. 7. Flow Chart for proposed Algorithm.

A set of features is first extracted from the ridge orientation field of an input fingerprint and then a fuzzy classifier is used to classify it into natural or altered fingerprint and its alteration type.

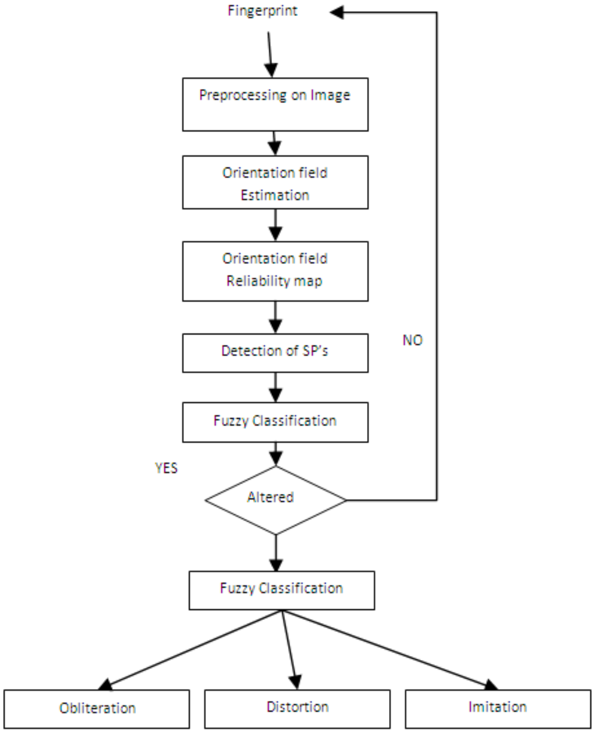

Fig.7. Flow Chart for proposed Algorithm

VI. Experiment Result

The natural fingerprints are compared with the altered fingerprints, by observing the values of the reliability singular points. In this dissertation, the singular point is defined as the point with maximum curvature on the convex ridge. For natural fingerprints, the reliability orientation image generally has one sharp point, while in altered fingerprints more point are detected with smaller values. Starting from this observation, the altered fingerprint analysis can be done using the density and the count of the singular points.

The proposed algorithm for fingerprint analysis based on the estimation of orientation field and the computation of the reliability was tested with real altered fingerprint and simulated altered fingerprint obtained from natural fingerprint images by using synthetic method due to unavailability of altered fingerprint database.

The real altered fingerprint by distortion shaped is shown in Figure 8 (a). Experimental results show that multiple singular points are detected shown in figure 8 (b)

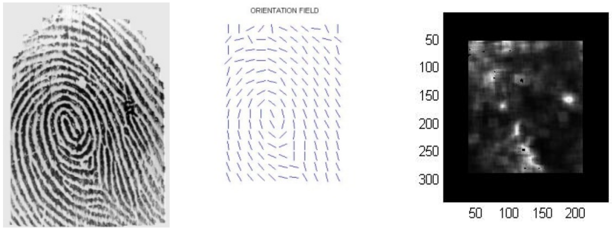

Fig.8 (a) Singular point estimation using reliability map (original)

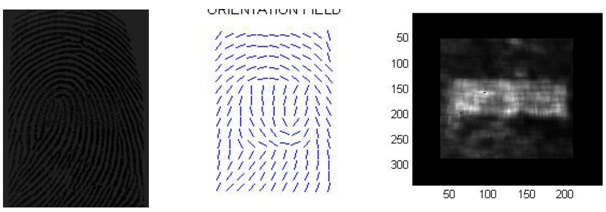

Fig.8. (b) Singular point estimation using reliability map (Altered by obliteration)

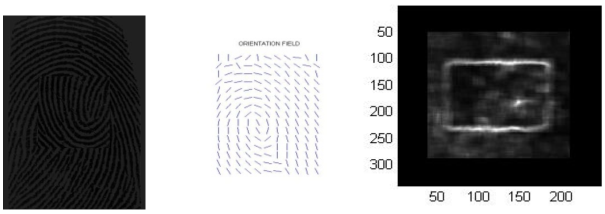

Fig.8. (b) Singular point estimation using reliability map (Altered by Distortion)

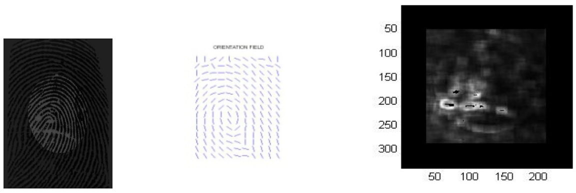

Fig.8. (b) Singular point estimation using reliability map

(Altered by Imitation)

In this paper, singular points are used to differentiate between netural fingerprint and altered figure print and that we used this for classifying altered fingerprints altered by three different technology.

Testing the efficiency of the orientation field reliability, the experimental results indicate that the reliability has strong information that can be used for future research. The singular value decomposition of reliability leads to obtaining essential features for discrimination and has good stability. The results obtained in altered fingerprints analysis using orientation field reliability are persuasive and could be employed for automatic detection of biometric obfuscation.

The orientation field reliability map has a maximum number of singular point locations in altered fingerprint rather than natural fingerprints and these locations are used to analyze altered fingerprints. Due to alteration, more numbers of singular points appear with lower amplitudes.

The experimental results demonstrate that the proposed algorithm can provide important information in order to automatically detect altered fingerprints.

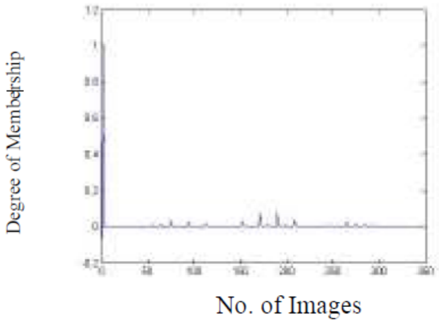

Fig.9. Fuzzy test on database
(Original and Altered fingerprint)

Conclusion and Future Work

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/alteredfingerprints.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, Jianjiang Feng ,”Altered Fingerprints:Analysis and De tection”,IEEE transaction on pattern analysis and machine intelligence , Vol.34, 2012