International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

# Review on Automatic Detection of Altered Fingerprints

**Luckyson Koijam**

MSC Forensic Science; Vivekananda Global University; Jaipur, India

**Abstract:** ***Due to the extensive usage of Automatic Fingerprint recognition Systems (AFIS) in border control and law enforcement, some people with criminal histories have purposefully altered their fingerprints to avoid recognition. Since change does not necessarily result in a decrease in implicit image quality, most altered fingerprints are not detected by the fingerprint quality assessment algorithms now in use. In this research, we present an algorithm to detect changing fingerprints and classify the identified changes in the functional database into three groups. Studies were carried out using artificially generated and real - world modified fingerprints. The suggested technique identified 92% of changed fingerprints with a false alarm rate of 7%, compared to just 20% detected by the well - known fingerprint quality program NFIQ. [1] Understanding changed fingerprints and the patterns that can be utilized to identify those images is the aim of this effort. This article contributes in the following ways in this regard: In order to circumvent the system, people have altered their fingerprints in the following ways: (a) case studies of those cases are produced; (b) the observed changes are categorized into three main groups and potential countermeasures are suggested; (c) a method is developed for creating altered fingerprints without actual data; (d) fingerprint recognition technology is modified; and (e) test results are presented that include both real and artificially produced modified prints. The experimental findings demonstrate the viability of the suggested method for identifying modified fingerprints and emphasize the necessity of carrying with this research project. [2]***

**Keywords:** Fingerprint Alteration, forensic analysis, identification method, proposed methods, algorithm

## 1. Introduction

For more than a century, fingerprint identification has been utilized successfully by law enforcement organizations and forensic scientists to identify offenders and victims. When the Federal Bureau of Investigation spearheaded the creation of Automatic Fingerprint Identification Systems (AFIS) in the 1970s, technology improved quickly. AFIS allowed for the rapid and accurate fingerprinting of suspects using a sizable database of records. Together with latent prints taken from crime scenes, local, state, and federal law enforcement agencies throughout the world get the fingerprints of criminal suspects who have been caught and send them to agencies like the FBI and Interpol on formatted 10 - print cards. In the Integrated AFIS System (IAFIS), the FBI alone has 10 prints of almost 70 million criminals and nearly 32 million civilians and military members. The widespread use of fingerprint identification in administrative and civilian applications, ranging from population registration to international border control, has been facilitated by its success in law enforcement and forensics. For example, to identify potential visa fraud and compile watch lists of high - level criminal suspects and terrorists, the US Department of Homeland Security uses the US - VISIT system at border crossings. Because fingerprint identification technologies are so successful at correctly identifying persons, some people have resorted to drastic means to get around the system. The primary goal of fingerprint alteration [4] is to prevent identification by a variety of methods, such as plasticizing, scorching, rubbing, and cutting fingers.

The use of altered fingerprints to hide identity is a major "attack" against a biometric system for border control, as it defeats the purpose for which the system was originally introduced, i. e., identifying persons from a watch list. It should be noted that altered fingerprints are different from forged fingerprints. The use of fake fingers made of glue, latex or silicone is a well - publicized method to evade fingerprint systems. On the other hand, altered fingerprints (no pun intended!) are real fingers that are used to hide identity to avoid detection by a biometric system. Thus, people usually use artificial fingers to assume the identity of another person, while altered fingers are used to hide one's own identity. [2]

### Types of Fingerprint Alteration

According to the changes made in the brush patterns, fingerprint changes can be classified into three types: erasure, distortion and imprint. In the removal of fingerprints, the friction strips on the fingertips are removed by grinding, cutting, burning, using strong chemicals or moving the smooth skin. The affected finger area must be large enough to override fingerprint scanners. But fingerprint quality control software can easily detect such changes and create an alert that prompts people to examine the finger. In fingerprint distortions, the friction ridge patterns on the fingertips are changed into unnatural ridges through a surgical procedure in which sections of the skin are removed from the finger and moved back into different positions. Distorted fingerprints can pass fingerprint quality control software, as the distortion may not degrade the quality of the image. For example, NFIQ software assigns the highest quality level to a distorted fingerprint as 1. [2]

### Detecting Altered Fingerprints

The detection of altered fingerprints is based on the analysis of the orientation field of the brush. Due to differences in the number and location of individual dots, the directional fields of natural fingerprints also differ between individuals. Therefore, we divide the original orientation field into two components, a single orientation field and a continuous orientation field. The continuous orientation field of the original fingerprint is indeed continuous (i. e., no singularity), but the continuous component of the transformed fingerprint orientation field is not actually continuous. Extract advanced features from the continuous

direction field and use Support Vector Machine (SVM) to classify the fingerprint as natural or modified fingerprint. [2]

## 2. Identification Method

Materials In the case of biometric research, it is generally assumed that the proposed methods are based on publicly available datasets so that research results can be reproduced. There is no such material for the research discussed in this article. Due to the nature of the interesting topic, it is not possible to ask a large number of volunteers to exchange fingerprints or to carry out a special data collection. Apparently, it would be possible to use forensic and immigration control databases. Generally, individuals seek to avoid criminal charges or immigration blacklisting, and altered fingerprints, if detected, are subject to legal protection. This limitation forced researchers in the field to test their methods either using synthetically generated datasets of altered fingerprints or to compare them with small datasets containing altered fingerprint samples. [3]

**1) Density analysis of individual points**

Patterns caused by scars and distortions cause deviations in the pixel - specific orientation field of fingerprint recognition. Aberrations can be detected as additional singularities in the orientation field that can be detected by approaches designed to detect real single points in real fingerprints. The Poincare index [16], ´P (x, y), is usually used as the first step in identifying the unit, core and delta points of a fingerprint.

**2) Minutia orientation analysis**

Altered fingerprints usually have anomalies in the flow of brush orientation due to scarring from incisions and amputations. Up close, you can find details with very different orientations in an unchanged fingerprint. In altered fingerprints, scars introduce additional details that often do not follow the expected directional flow. Minutia Orientation Analysis extracts patterns based on the orientation differences of details that are close to each other. [3]

## 3. Proposed Method

All fingerprint images are pre - processed using the FDB method [9]. First, the region of interest (ROI) is estimated using the FDB method, and then the images are automatically adjusted by removing all rows and columns containing only background pixels. A visual check was performed to ensure that the automatic pre - processing using the FDB method produced the correct ROIs for all images. [4] PADI METRICS, DATABASE RESULTS International standards for biometric performance measurement for fingerprint recognition are established under ISO/IEC 19795 - 1 [18] and define algorithm errors such as false match rate (FMR) and false non - match rate (FNMR). must be reported. Unfortunately, such well - established concepts for testing the detection of impersonation attacks did not previously exist. ISO/IEC recently started work on a standard covering impersonation detection and metrics to demonstrate the effectiveness of fingerprint change detection methods in combating subversive attacks. The draft standard ISO/IEC 30107 Detection of Biometric Image Attacks provides a harmonized definition of terms related to attack techniques and test methods to measure resistance to such attacks. [4]

**PAD Metrics, Database, and Results**

International standards for biometric performance measurement for fingerprint recognition are established under ISO/IEC 19795 - 1 [18] and define algorithm errors such as false match rate (FMR) and false non - match rate (FNMR) must be reported. Unfortunately, in the past there were no such well - established concepts for testing the detection of impersonation attacks. ISO/IEC recently started work on a standard covering impersonation detection and metrics to demonstrate the effectiveness of fingerprint change detection methods in combating subversive attacks. The draft standard ISO/IEC 30107 Detection of Biometric Image Attacks provides a harmonized definition of terms related to attack techniques and test methods to measure resistance to such attacks. [4]

## 4. Discussion and Conclusion

Available fingerprint quality control software modules have a very limited ability to distinguish altered fingerprints from natural fingerprints. We have developed an algorithm that automatically detects altered (distorted) fingerprints. The basic idea is that altered fingerprints often have unusual ridges. A set of features is first extracted from the brush direction field of the input fingerprint, and then a support vector classifier is used to classify it as a natural or modified fingerprint. The proposed algorithm was tested using modified fingerprints typically synthesized for use cases with good performance. Once an altered fingerprint is detected, it is a very important process to match it with an unaltered fingerprint, which is likely to be stored in a database. In some altered fingerprints, such as loss or displacement of a small area, the ridge patterns are locally damaged. It is possible to reconstruct the ridge pattern of the changed region using the unchanged ridge pattern of the neighbourhood. [2]

A new method for detecting altered fingerprints is developed, which performs competitively with the state - of - the - art method of Yoon et al., and achieves a TADR of 92.0% and an FNADR of 2.3% on the classification dataset. In addition, the classification efficiency can be further improved to 94.6% for TADR and 2.4% for FNADR by combining Yoon et al. and the proposed method. Future work would include testing a larger dataset from government sources, such as the FBI's modified fingerprint database, which Yoon et al used as another source of validation. [3]

## References

[1] Yoon, S., Feng, J., & Jain, A. K. (2012). Altered fingerprints: Analysis and detection. IEEE transactionsonpattern analysis and machine intelligence, 34 (3), 451 - 464.
[2] Jain, A. K., & Yoon, S. (2012). Automatic detection of altered fingerprints. Computer, 45 (1), 79 - 82.
[3] Selvarani, S. M. C. A., Jebapriya, S., & Mary, R. S. (2014, March). Automatic identification and detection of altered fingerprints. In 2014 International Conference

on Intelligent Computing Applications (pp.239 - 243). IEEE.

[4] Feng, J., Jain, A. K., & Ross, A. (2010, August). Detecting altered fingerprints. In 2010, 20th International Conference on Pattern Recognition (pp.1622 - 1625). IEEE.

[5] Kumar, R., Singh, J. P., & Srivastava, G. (2012). A Survey Paper on Altered Fingerprint Identification & Classification. International Journal of Electronics Communication and Computer Engineering, 3 (5).

[6] Feng, J., Jain, A. K., & Ross, A. (2009). Finge