Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 58 (2015) 447 – 452

Procedia
Computer Science

Second International Symposium on Computer Vision and the Internet (VisionNet'15)

A Minutiae Count Based Method for Fake Fingerprint Detection

Kumar Abhishek*, Ashok Yogi

Department of Electronics and Electrical Engineering, Indian Institute of Technology Guwahati, Assam, India - 781039

Abstract

Fingerprint based biometric systems are ubiquitous because they are relatively cheaper to install and maintain, while serving as a fairly accurate biometric trait. However, it has been shown in the past that spoofing attacks on many fingerprint scanners are possible using artificial fingerprints generated using, but not limited to gelatin, Play-Doh and Silicone molds. In this paper, we propose a novel method based on the minutiae count for detecting the fake fingerprints generated using these methods. The proposed algorithm has been tested on the standard FVC (Fingerprint Verification Competition) 2000-2006 dataset and the accuracy was reported to be well above 85%. We also present a literature survey of the previous algorithms for fake fingerprint detection.

Peer-review under responsibility of organizing committee of the Second International Symposium on Computer Vision and the Internet (VisionNet'15)

Keywords: Fingerprint, minutiae, fake fingerprint, ridge ending, biometrics, spoofing, fingerprint scanner

1. Introduction

A fingerprint is an impression of the friction ridges from the surface of a fingertip. Being unique to each individual and the fact that they do not change over time, fingerprint based authentication and identification is one of the most important and popular biometric technologies. Factors like fingerprint distinctiveness, persistence, ease of acquisition and high confidence matching rates are the primary reasons why fingerprint based authentication systems dominate the biometrics market, accounting for as much as over 52% of the total authentication systems based on biometric traits[1].

* Corresponding author. Tel.:+91-9401574154.
E-mail address: abh.kumar@iitg.ernet.in

Peer-review under responsibility of organizing committee of the Second International Symposium on Computer Vision and the Internet (VisionNet'15)
doi:10.1016/j.procs.2015.08.061

The features extracted from a fingerprints friction ridge impression can be broadly categorized as[2,3]:

- **Level 1:** Arches, Loops, Whorls
- **Level 2:** Ridge Endings, Bifurcations, Eyes, Hooks, Line Units, Line Fragments
- **Level 3:** Pores, Line Shapes, Incipient Ridges, Creases, Warts, Scars.

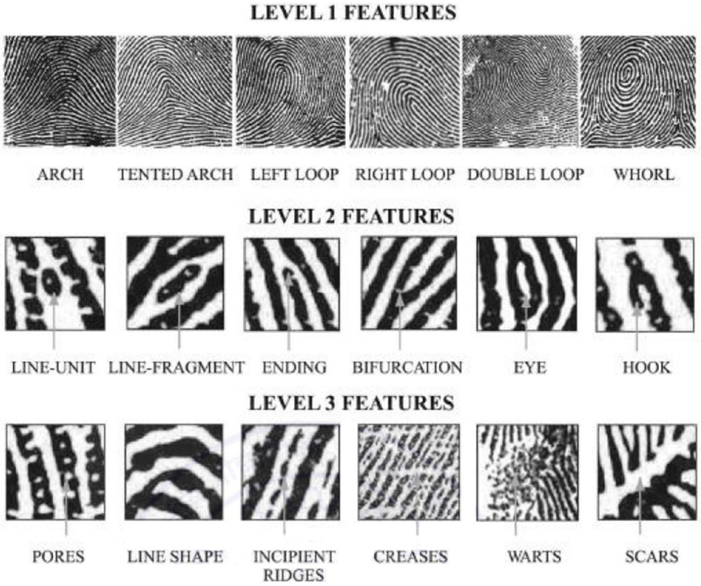

Fig. 1. Fingerprint features at Level 1, Level 2 and Level 3[2,3].

Antonelli[4] *et al.* (2006) proposed the detection of fake fingerprints using the property of human skin elasticity. A user is asked to deliberatively increase the recorded screen distortion by moving the finger against the scanner surface. The distortion obtained is then used as a feature to detect fake fingerprints.

Baldisserra[5] *et al.* (2006) propose to place an odor sensor alongside the fingerprint scanner to detect fake fingerprints. The odor sensors samples the odor signal, which is then used to discriminate the finger skin odor from that of materials that fake fingerprints might be made of *viz.* latex, silicone or gelatin.

Abhyankar and Schuckers[6] (2008) proposed a wavelet based perspiration liveliness check to be integrated with the fingerprint matcher. The intuitive idea behind using this as a feature was that perspiration changes along the fingerprint ridges, which can be used to determine liveliness as this can be observed only in live people. The proposed algorithm was tested on live, spoof and cadaver fingerprint images.

Choi *et al.*[7] (2009) proposed the use of multiple static features extracted from the fingerprint images to as a liveness test. The representative static features chosen were power spectrum, histogram, directional contrast, ridge thickness and ridge signal of each fingerprint.

Nikam and Agarwal[8] (2009) proposed a ridgelet-transform based method to detect fake fingerprints using ridgelet energy and co-occurrence signatures to characterize the texture of the fingerprints. The proposed algorithm was tested on real, fun-doh and gummy fingerprints.

Tan and Schuckers[9,10] (2010) proposed the usage of the gray level perspiration patterns along the ridges and valleys in spatial, frequency and wavelet domains as an anti-spoofing detection method. Based on these features, classification trees and neural networks were trained, and the proposed algorithm was tested on live fingerprints and spoof fingerprints (Play-Doh, gelatin and silicone molds in multiple sessions).

Gragnaniello *et al.*[11] (2014) proposed to use a wavelet-Markov local descriptor in order to use the joint dependencies amongst wavelet coefficients, which can be used as to test fingerprint liveness.

2. Proposed Approach

2.1 Minutiae

Introduced by Sir Francis Galton in his well-known book titled “Fingerprints”[12], Level 2 features or minutiae features indicate the different ways that a local ridge can be discontinuous. These are essentially Galton characteristics, namely ridge endings and ridge bifurcations. A ridge ending is defined as the ridge point where a ridge ends abruptly. A bifurcation is defined as the ridge point where a ridge bifurcates into two ridges.

Minutiae are the most prominent features because of their stable and robust nature. In addition, the distribution of minutiae in a fingerprint is unique and this property is used by most of the fingerprint recognition algorithms. Statistical analysis shows that the minutiae features have sufficient discriminating power to establish the individuality of fingerprints.

Previous work done by Nikam and Agarwal[8] towards detection of fake fingerprints suggests that the gray level variations are random in real fingerprints, while they tend to be either uniform or periodic in case of fake fingerprints, depending upon the material used to generate the fake fingerprints, as shown in Fig. 2. Similar pattern is observed in the local texture analysis of the fingerprint images. Owing to this, the ridge endings in real fingerprints tend to larger in number than in fake fingerprints. Therefore, it is intuitive that the number of ridge endings can be an effective feature in differentiating the real fingerprints from the fake ones. A simple threshold based classification scheme on the number of ridge endings gives a pretty good accuracy.

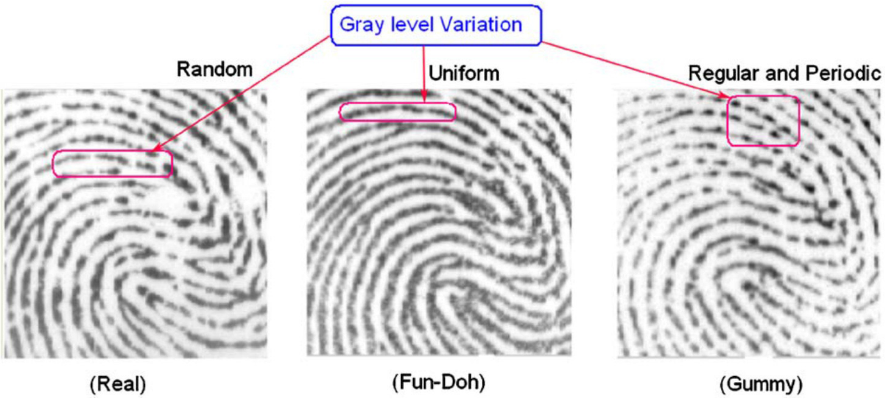

Fig. 2. Gray level variation in real fingerprints as compared to fake fingerprints[8].

2.2 The Algorithm

1. Given a fingerprint image I, perform Otsu’s segmentation to obtain a binary image IB.
2. Perform morphological thinning iteratively on IB, until each ridge is only 1 pixel thick to obtain the image IT.
3. For finding the ridge endings, consider a 3x3 window around each pixel and count the number of black pixels in each window. An iteratively thinned ridge ending will have only two black pixels in the window (as shown in Fig. 3) – the ridge ending pixel and the pixel connecting to it.
4. If the number of black pixels in a 3x3 window centered at the ith pixel is exactly 2, then the center pixel is said to be a ridge ending.
5. Count the total number of ridge endings for each fingerprint image. Let this be denoted by CRE.
6. Apply a simple threshold operation. If CRE > K, then the fingerprint is a real fingerprint, otherwise it is a fake fingerprint. Here, K is some threshold.

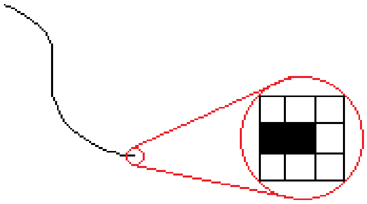

Fig. 3. A ridge ending has 2 black pixels in a 3x3 window

3. Results

The proposed algorithm was tested on the FVC[1] (Fingerprint Verification Competition) datasets, available from BioLab, University of Bologna, Italy. The typical results obtained on a real and a fake fingerprint are shown in Fig. 4 and Fig. 5 respectively. It is clear from the results that the number of ridge endings detected in real fingerprints is larger than those detected in fake fingerprints.

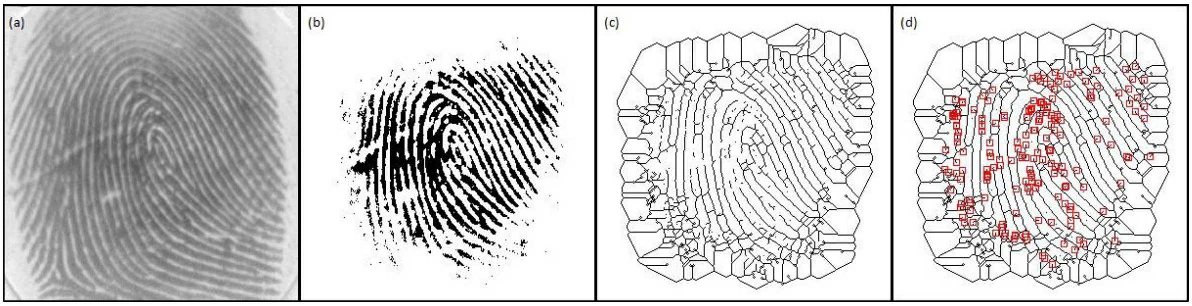

Fig. 4. Real Fingerprint (a) Original Fingerprint Image (b) Binary Image (c) Iteratively Thinned Image (d) Detected Ridge Endings

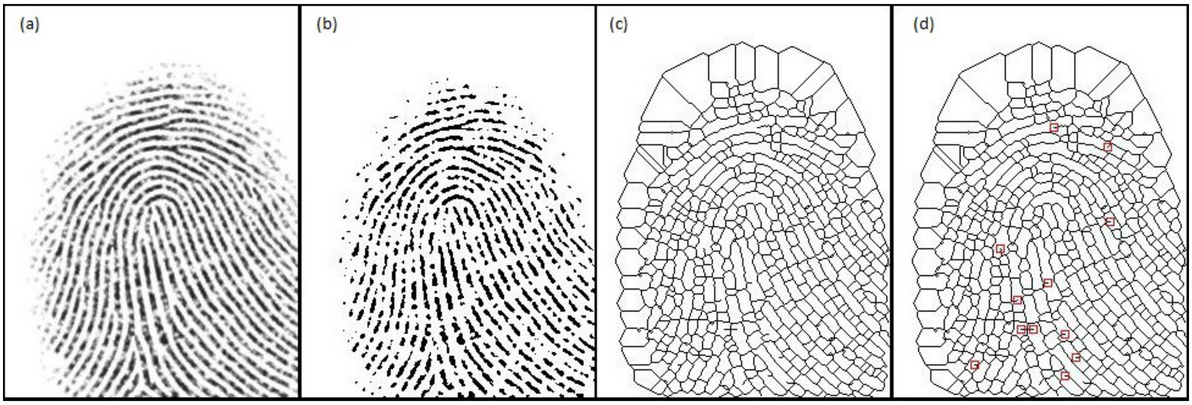

Fig. 5. Fake Fingerprint (a) Original Fingerprint Image (b) Binary Image (c) Iteratively Thinned Image (d) Detected Ridge Endings

The results obtained for this classification task are tabulated as:

Table 1. Classification performance for both classes – Real and Fake fingerprints.

Class	Precision	Recall	F-Measure
Real Fingerprints	0.9634	0.7667	0.8539
Fake Fingerprints	0.8659	0.9125	0.8885

In the performance analysis of a binary classification such as the one in hand, the F-Measure[13] is a measure of accuracy. The F-Measure for each class is computed as the harmonic mean of the precision and the recall of the particular class. As is evident from Table 1 (constructed with the threshold **K** set to 10), the proposed algorithm gives an accuracy of more than 85% for each of the two classes – Real and Fake fingerprints.

Another performance evaluation criterion of a binary classification scheme is the Receiver Operating Characteristic (ROC) curve[14]. A ROC curve is a graphical plot that illustrates the performance of a binary classification scheme as its discrimination threshold (**K** in this case) is varied in multiples of 5. The ROC plot obtained has been shown is Fig. 6.

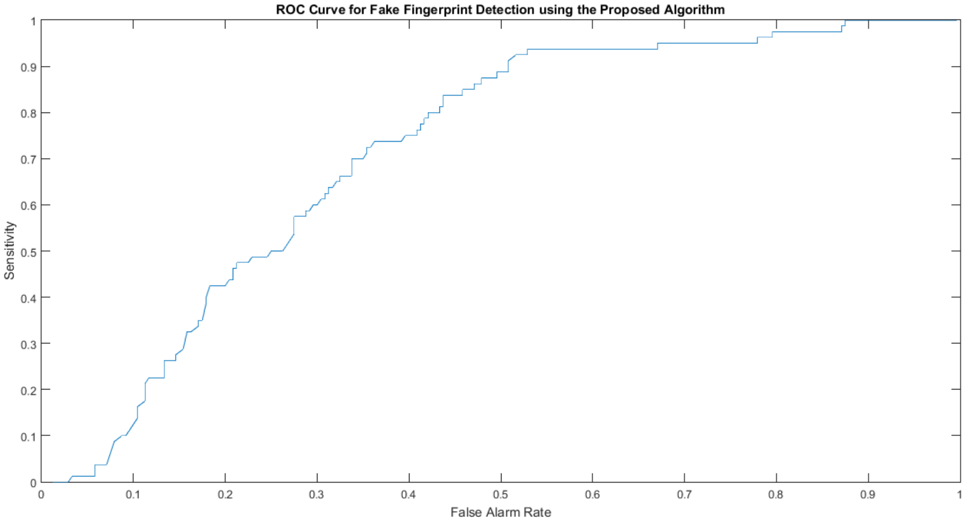

Fig. 6. ROC curve for the proposed algorithm with varying threshold.

4. Conclusion

In this paper, we have proposed a simple yet efficient algorithm to detect the fake fingerprints based on minutiae count. The algorithm yielded an accuracy of over 85% over the standard FVC Fake Fingerprint Dataset. This algorithm when used in conjunction with algorithms discussed previously can greatly enhance the fake fingerprint detection accuracy. When a fingerprint is to be tested, this algorithm can be used as preliminary test to straight away reject it or retain it to perform further tests upon it. The algorithm is computationally efficient and is very fast, making it possible to be easily integrated into biometric systems for fake fingerprint detection.

Acknowledgements

The authors are thankful to Dr. M. K. Bhuyan, Associate Professor, Department of Electronics and Electrical Engineering, IIT Guwahati for his constant support and motivation as well as for his wonderful course on Biometrics.

References

1. Maltoni, Davide, Dario Maio, Anil K. Jain, and Salil Prabhakar. *Handbook of fingerprint recognition*. Springer Science & Business Media, 2009.

2. The Thin Blue Line. http://www.policensw.com/info/fingerprints/finger06.html, October 2006.
3. H.v.d. Nieuwendijk, *Fingerprints* http://www.xs4all.nl/~dactyminu.htm, October 2006.
4. Antonelli, Athos, Raffaele Cappelli, Dario Maio, and Davide Maltoni. "Fake finger detection by skin distortion analysis." *Information Forensics and Security, IEEE Transactions on* 1, no. 3 (2006): 360-373.
5. Baldisserra, Denis, Annalisa Franco, Dario Maio, and Davide Maltoni. "Fake fingerprint detection by odor analysis." In *Advances in Biometrics*, pp. 265-272. Springer Berlin Heidelberg, 2005.
6. Abhyankar, Aditya, and Stephanie Schuckers. "Integrating a wavelet based perspiration liveness check with fingerprint recognition." *Pattern Recognition* 42, no. 3 (2009): 452-464.
7. Choi, Heeseung, Raechoong Kang, Kyoungtaek Choi, Andrew Teoh Beng Jin, and Jaihie Kim. "Fake-fingerprint detection using multiple static features." *Optical Engineering* 48, no. 4 (2009): 047202-047202.
8. Nikam, Shankar Bhausaheb, and Suneeta Agarwal. "Ridgelet-based fake fingerprint detection." *Neurocomputing* 72, no. 10 (2009): 2491-2506.
9. Tan, Bozhao, and Stephanie Schuckers. "Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise." *Pattern Recognition* 43, no. 8 (2010): 2845-2857.
10. Tan, Bozhao, Lewicke, Aaron, and Stephanie Schuckers. “Novel methods for fingerprint image analysis to detect fake fingers” *SPIE Newsroom*, 10.1117/2.1200805.1171
11. Gragnaniello, D., G. Poggi, C. Sansone, and L. Verdoliva. "Wavelet-Markov local descriptor for detecting fake fingerprints." *Electronics Letters* 50, no. 6 (2014): 439-441.
12. Galton, Francis. *Fingerprints*. Macmillan and Company, 1892.
13. F1 score. http://en.wikipedia.org/wiki/F1_score
14. Receiver operating characteristic. http://en.wikipedia.org/wiki/Receiver_operating_characteristic