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.

© 2015 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license
(http://creativecommons.org/licenses/by-nc-nd/4.0/).
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

1877-0509 © 2015 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license
(http://creativecommons.org/licenses/by-nc-nd/4.0/).
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.

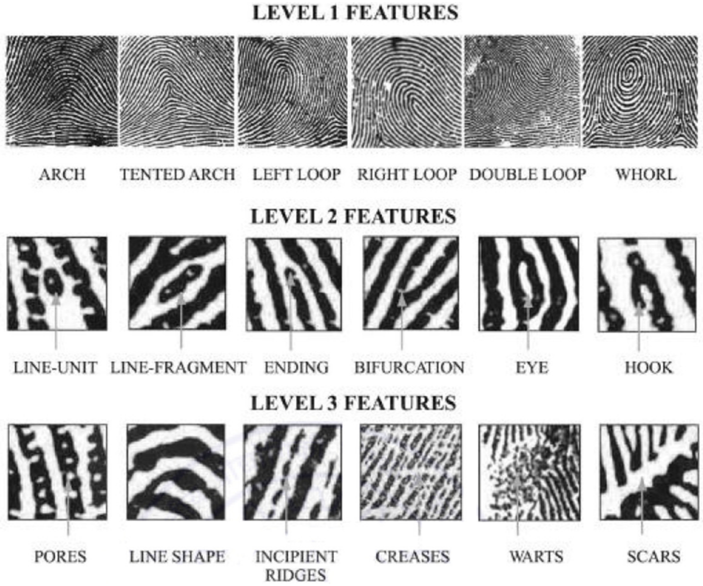

Fig. 1. Fingerprint features at Level 1, Level 2 and Level 3[2,3].

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.

Download English Version:

https://daneshyari.com/en/article/487387

Download Persian Version:

https://daneshyari.com/article/487387

Daneshyari.com