ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

A Review on Fake Finger and Fingerprint Liveness Detection

Akshata S.Shet

M.E. Student, Dept. of E&TC., MIT College of Engineering, Savitribai Phule Pune University, Pune, India

ABSTRACT: Fingerprints have been most widely employed for diverse security systems due to the high-level accuracy and users convenience. Since fingerprints begin to be broadly utilized in the smartphones and tablets for payment as well as security, high-performed algorithms have been explored in literature. At the same time, such mobile systems are highly required to detect spoofing attacks by fabricated fingerprints with malicious intends. In this paper, we briefly review of fingerprint liveness detection and classification techniques are discussed.

KEYWORDS: Fingerprint liveness, classification techniques

I. INTRODUCTION

Biometrics authentication system refers to the identity identification based on their physiological and behavioural characteristics. Therefore, biometric recognition systems are commonly used for authentication in various security applications.The ability of fingerprint authentication system to discriminate whether the fingerprint samples presented are really from a live finger tip or spoofed one, which is called liveness detection. In order to prevent spoofing, many kinds of detection methods have been proposed in recent years.

The advantage of using biometrics for authentication purpose comes from the unique features of each individual. Iris and fingerprints are unique for every human. Fingerprints are most generally used for numerous security systems due to the high-level accuracy and users covenience. Nowdays, such fingerprints are used to a key application, e.g., payment, on mobile devices by the small size of fingerprint sensors. Even though the high-performed recognition methods have been systematically developed, most of them still suffer from spoofing attacks using different materials, e.g., silicone, gelatin, wood glue, etc. [1] Moreover, fingerprints can be easily captured from scanning the stolen device, which are readily employed to penetrate the security. To address this drawback, early studies have explored spatial characteristics of ridges and valleys within the fingerprint. Fingerprint liveness detection has been an active research topic over the last several years. It has been proven that it is possible to spoof.

As illustrated in Fig. 1, we observe that it is very difficult to visually differentiate between live and fake fingerprints.The possibility to spoof a fingerprint based authentication system creates the need to develop a method which can distinguish between live and fake fingerprint images.

Both hardware and software based approaches can be used to solve this problem.However, hardware based approaches require additional devices to measure finger temperature, odor, pulse, oxiometry etc. In addition, hardware based approaches are typically costlier due to the additional sensors required.

DOI: 10.15680/IJIRCCE.2017. 0504152

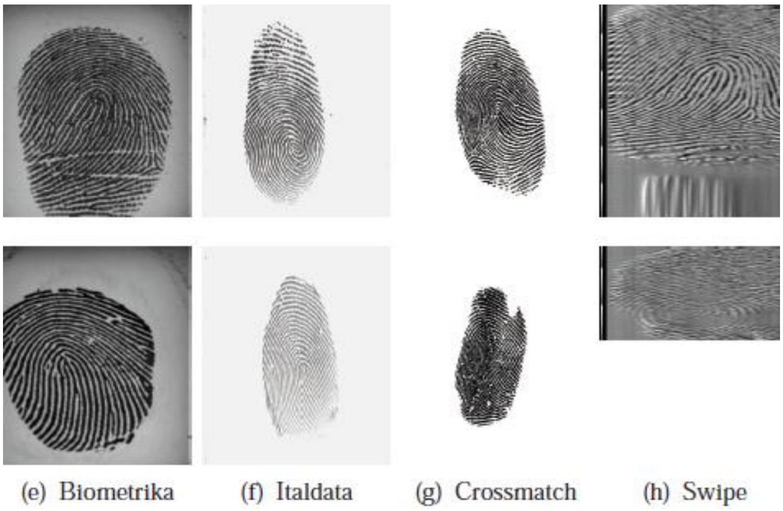

Fig 1: Example of live (above) and fake (below) fingerprints acquired with 4 sensors

II. RELATED WORK

In this section, we discuss the literature in the field of software based fingerprint liveness detectionD. Yambayet. al. [2] "Liveness detection", a system used to decide the vitality of a submitted biometric, has been implemented in fingerprint scanners in recent years. The goal for the LivDet 2013[2] andLivDet 2015[3] competition is to compare software-based fingerprint liveness detection strategies as well as fingerprint frameworks which incorporate liveness detection capabilities utilizing a standardized testing protocol and large quantities of spoof and live fingerprint images. LivDet is the worldwide public competition for software-based fingerprint liveness recognition and first public assessment of framework based fingerprint liveness recognition.

Rodrigo [4]proposed a system based on convolutional neural networks (CNNs) for fingerprint liveness detection. This system is evaluated on the data sets used in the liveness detection competition of the years 2009, 2011, and 2013, which comprises almost 50000 real and fake fingerprints images. In this system compare four different models: two CNNs pretrained on natural images and fine-tuned with the fingerprint images, CNN with random weights, and a classical local binary pattern approach. Data set augmentation is used to increase the classifiers performance, not only for deep architectures but also for shallow ones.

Perspiration-based method: Because sweat glands can produce moisture, the real fingerprint images from fingerprint devices will change slightly in a short time span. However the obtained spoof ones from sensor devices can not generate moisture. Therefore, researchers detect the fingerprint vitality through the study of Perspiration. The authors Tan and Schuckers[5] obtain a skeleton of the ridge structure and this skeleton determine extracted ridge signal. The signal is analysed by using wavelets and classified between the fake and real fingers. In this paper, Tan and Schuckers [6] also analyse the middle ridge signal generate from the centres of the ridges structure of skeleton. On account of the perspiration phenomenon, the middle ridge signal obtained from a real finger is of a periodic nature determined by the periodic occurrence of the active sweat pores. Because of the absence of the sweating process, the middle ridge signals obtained from the fake and do not exhibit this significantly periodic nature.

Decann et al. [7] have proposed a fingerprint liveness detection algorithm that utilises an adaptation of the standard computer vision region labelling technique. In the initial step, they get the skeletons of the fingerprint ridge structure and the fingerprint valley structure. Afterwards, the difference image between the scans that have been acquired at subsequent points intime, is computed.

Sweat pores: The sweat pores are very small circular structures present in the fingerprint ridges of the living fingers that are the endings of internal skin structures called sweat glands.

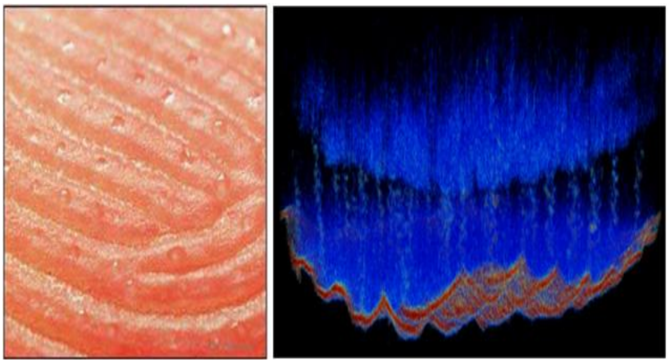

Fig 2:Sweat pores and sweat glands: tiny structures, present in the fingerprint ridges.

The sweat glands are responsible for production ofsweating fluid. The liveness detection methods based on the analysis of the sweat pores usually expect that such small structures would be very difficult to reproduce with sufficient quality when the fake finger is produced.

Champod [8] reported that even though it ispossible to replicate the sweat pores by using the fake fingerprint fabrication methods, the quantities of the pores differ in the fingerprints generated by the real living fingers compared with the fingerprints generated by the fake fingers and the difference can be used as a measure of the livenessdetection.

Texture analysis: Agarwal have published several methods based on the statistical analysis of the fingerprint scans. They have experimented with features based on a combination of the grey-level co-occurrence matrices (GLCMs) and the wavelet transform [9], the Ridgelet transform [10, 11], the Gabor filters [12] and the Curvelet transform [13]. In addition,they tried to obtain the features by application of the local binary patterns along with the wavelet transform [14]. By using the above mentioned approaches, they obtained a large number of features that could be used to distinguish between the live and the fake fingers.They reduce thenumber of features by means of the principal component analysis.

Electrical properties: In this methodthe difference in the electrical properties of the living skin compared with the fake materials. Martinsen et al. [15] have used an electrode array to measure the impedance of the fingerprint tissue. The system performs liveness detection by means of multiple measurements using different electrodes on the array. By comparision of different the results from different electrodes with different distances from each other, they can indicate the presence of a living fingertip with a multi-layer structure of the living skin.

III. PROPOSED ALGORITHM

The system architecture is illustrated in Fig. 2

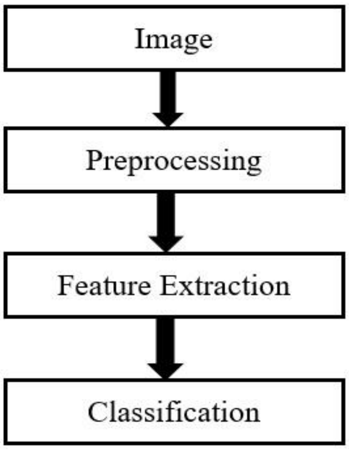

Fig 2: Proposed system block diagram

In this work, we divide the system into three main sequential blocks:

- Image Pre-processing Stage
- Feature Extraction Stage
- Image Classification Stage

A. Image Preprocessing Stage

This is initial stage of system. A low quality fingerprint image is usually noisy, exhibits solid line and has low contrasts between valleys and ridges. These effects will happen throughout image acquisition, as result of dry or wet skin. Since the image acquisition stage is not always monitored for accepting only high quality images, fingerprint image enhancement and noise reduction are, therefore, important pre-processing factors in accurately detecting fingerprint liveness.

We can enhanced the quality of the image by cropping the fingerprint region in the image and then performing histogram equalization to increase the perception information. In order to remove noise captured during image acquisition, median filtering is then applied on the cropped images without reducing the sharpness of the input image.

B. *Feature Extraction Stage:*

In fingerprint authentication systems, the image is usually captured from multiple subjects usingdifferent scanners.Therefore, fingerprintimages are typically found to be of different scales and rotations. In certain scenarios, the fingerprint images are partially captured due to human errors. In order to obtain features that are invariant to these problems, we use variousfeatures that capture properties of live fingerprint images.

In our work, we choose to use SURF as it is invariant to illumination, scale and rotation. SURF is also used because of its concise descriptor length.We also use Gabor Wavelet to extract featuresfrom fingerprint images for texture analysis. Gabor filters have optimal localization properties in both the frequency and spatial domain.

C. Classification

The grouping is separate for real and fake fingerprint. Once the features have been extracted, we continue advance by grouping the images and distinguishing the fingerprint. For this arrangement we have different algorithms but we use deep stacking network as classifier for distinguishing real and fake fingerprint.

IV. CONCLUSION

Fingerprint authentication systems are quite vulnerable to sophisticated spoofing attacks. To keep a good level of security, reliable spoofing detection tools are necessary, preferably implemented as software modules. .all the main techniques and functions in this liveness detection area are included in this paper but have some limitations .

REFERENCES

1. Rohit Kumar Dubey,JonathanGoh,andVrizlynn L L Thing “Fingerprint liveness detection from single image using Low level feture and shape analysis” IEEE Transactions on, Information Forensics and Security DOI 10.1109/TIFS.2016.
2. L. Ghiani, D. Yambay, V. Mura, S. Tocco, G.L. Marcialis, F. Roli, and S. Schuckcrs, “Livdet 2013 fingerprint liveness detection competition 2013,” in Biometrics (ICB), 2013 International Conference on, June 2013, pp. 1–6.
3. Valerio Mura, Luca Ghiani, Gian Luca Marcialis, Fabio Roli “LivDet2015 fingerprint liveness detection competition 2015,” in Biometrics Theory, Application and System (BTAS),2015 IEEE 7th International Conference on Sept 2015.
4. Rodrigo FrassettoNogueira, Roberto de AlencarLotufo, and Rubens Campos Machado,” Fingerprint Liveness Detection Using Convolutional Neural Networks”, IEEE transactions on information forensics and security, vol. 11, no. 6, June 2016
5. Tan, B., Schuckers, S.: ‘Liveness detection for fingerprint scannersbased on the statistics of wavelet signal processing’. Proc. ComputerVision and Pattern Recognition Workshop (CVPRW ‘06), 2006, pp. 26.
6. Tan, B., Schuckers, S.: ‘Spoofing protection for fingerprint scanner byfusing ridge signal and valley noise’, Pattern Recognit., 2010, 43, (8),pp. 2845–2857.
7. Decann, B., Tan, B., Schuckers, S.: ‘A novel region based livenessdetection approach for fingerprint scanners’. Proc. Third Int. Conf. onAdvances in Biometrics (ICB ‘09), 2009, pp. 627–636.
8. Espinoza, M., Champod, C.: ‘Using the number of pores on fingerprint images to detect spoofing attacks’. Proc. Int. Conf. on Hand-Based Biometrics (ICHB), 2011, pp. 1–5.

9. Nikam, S., Agarwal, S.: 'Wavelet energy signature and GLCMfeatures-based fingerprint anti-spoofing'. Proc. Int. Conf. on Wavelet Analysis and Pattern Recognition (ICWAPR '08), 2008, vol. 2,pp. 717–723.
10. Candes, E.J., Donoho, D.L.: 'Ridgelets: a key to higher-dimensional intermittency?',Philos. Trans. Lond. R. Soc., 1999, 357, pp. 2495–2509.
11. S.B., Agarwal, S.: 'Ridgelet-based fake fingerprint detection',Neurocomputing, 2009, 72, (10–12), pp. 2491–2506
12. Nikam, S., Agarwal, S.: 'Gabor filter-based fingerprint anti-spoofing'.Advanced Concepts for Intelligent Vision Systems, 2008 (LNCS,5259), pp. 1103–1114.
13. Nikam, S., Agarwal, S.: 'Fingerprint liveness detection using curvelet energy and co-occurrence signatures'. Proc. Fifth Int. Conf. on Computer Graphics, Imaging and Visualisation (CGIV '08), 2008,pp. 217–222.
14. Nikam, S., Agarwal, S.: 'Texture and wavelet-based spoof fingerprint detection for fingerprint biometric systems'. Proc. First Int. Conf. on Emerging Trends in Engineering and Technology (ICETET '08),2008, pp. 675–680.
15. Martinsen, O., Clausen, S., Nysaether, J., Grimnes, S.: 'Utilizingcharacteristic electrical properties of the epidermal skin layers todetect fake fingers in biometric fingerprint systems – a pilot study',IEEE Trans. Biomed. Eng., 2007, 54, (5), pp. 891–894.

BIOGRAPHY

Akshata S. Shetis a ME student in the Electronics and Telecommunication Department, MIT College of Engineering, SavitribaiPhule Pune University,Pune. She received Bachelor of Technology (B.Tech) degree in 2015 from Dr.BabasahebAmbedkarTechnogical University, Lonere, Maharashtra, India.