International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT2063204

Fingerprint Distortion Detection

Harshada Kanade*, Gauri Uttarwar, Shweta Borse, Archana. K
Department of Computer Engineering, Dr. D. Y. Patil Institute of Technology, Pimpri, Pune, Maharashtra, India

ABSTRACT

Fingerprint is widely used in biometrics, for identification of individual's identity. Biometric recognition is a leading technology for identification and security systems. It has unique identification among all other biometric modalities. Most anomaly detection systems rely upon machine learning. Calculations are performed to identify suspicious occasion. The primary purpose of this system is to ensure a reliable and accurate user authentication; this study addresses the problem of developing accurate, generalizable, and efficient algorithms for detecting fingerprint spoof attacks. The approach is to utilize local patches centered and aligned using fingerprint details. That proposed approach is to provide accuracies in fingerprint spoof detection for intra-sensor, cross material, crosssensor, as well as cross-dataset testing scenarios. The principle used is similar to the working of some cryptographic primitives, in particular to present the key into the plan so that a couple of operations are infeasible without knowing it.

Keywords : Fingerprint, Biometric, Security, Distortion detection, Spoof

I. INTRODUCTION

Biometrics is an automated recognition of individuals based on their biological and behavioural characteristics such as fingerprints, face, voice, and iris. Well-duplicated artificial fingerprints are referred to as spoof artifacts, can be presented to a fingerprint sensor in order to deceive the recognition system. This corresponds to a sensor-level attack where an adversary intends to gain unauthorized access to a system by using the biometric traits of someone who is legitimately enrolled in the system. Furthermore, an attacker may create a new "identity" using an artificial biometric trait that can be enrolled in the system and then shared between different people.

Several spoofing techniques have been reported till now, includes the use of artificial fingerprints made of gelatine, moldable plastic, Play-Doh, and silicon, produced by using a mold obtained from a live finger or from a latent fingerprint.

Biometric forms of authentication are more convenient than passwords and PINs, and have other advantages that enhance the security of mobile devices. But just like passwords and PINs, biometric forms of identity.

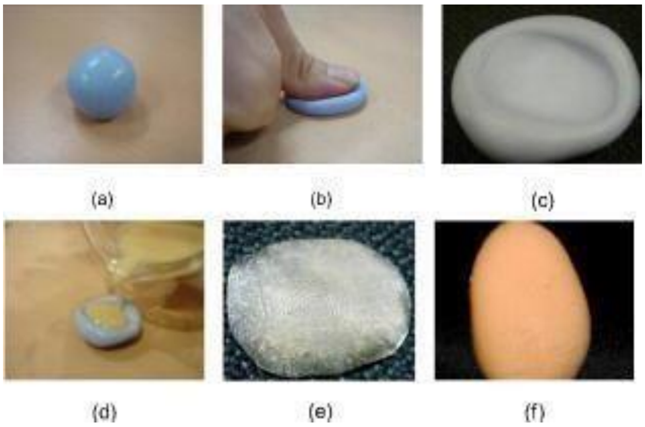
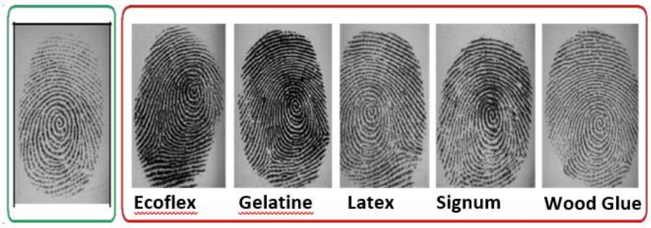


Fig 1: Module of fingerprint



[a] Live Fingerprint [b] Spoofing of fingerprint

Fig 2: Visual comparison between [a] a live Fingerprint, and [b] the corresponding spoofs made with different materials.

II. EXISTING SYSTEM

There are sensors which can detect and sense odour or smell. In existing system, fingerprint distortion was detected by the odour of spoof technique. An additional device called electronic nose. An electronic nose is a device intended to detect odours or flavours. Over the last decades, "electronic sensing" or "esensing" technologies have undergone important developments from a technical and commercial point of view. The basic idea is to detect the chemical constituents that contribute to the odour in the substance. The sensor surface consists of materials that could respond to the odorous compounds differently.

A. Limitations

The major disadvantage in this technique was that anybody can fake the smell to the sensor or device by applying perfume. Due to this, the device will be unable to detect the smell.

III. PROPOSED SYSTEM

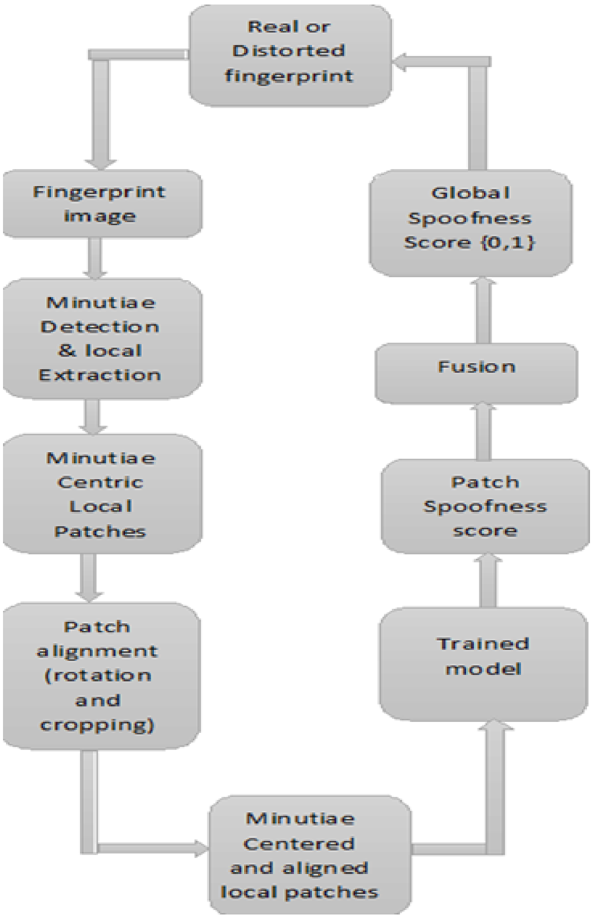
Distortion detection is viewed as a two-class classification problem, for which the registered ridge orientation map and period map of a fingerprint are used as the feature vector and a SVM classifier is trained to perform the classification task. Distortion rectification (or equivalently distortion field estimation) is viewed as a regression problem, where the input is a distorted fingerprint and the output is the distortion field. To solve this problem, a database of various distorted reference fingerprints and corresponding distortion fields is built in the offline stage, and then in the online stage, the nearest neighbour of the input fingerprint is found in the reference database and the corresponding distortion field is used to transform the input fingerprint into a normal one.

A. Objectives

1. To implement an algorithm or design for fingerprint distortion detection.
2. To analyze and implement different techniques used for spoofing.
3. To understand liveness of the fingerprint.
4. Use of additional device can increase cost .
5. To design a system that will recognize and rectify the distortion for identification of error.
6. To detect the distorted area.

A. System Architecture

The proposed approach includes two steps, an offline training stage and an online testing stage. The offline training step consists of (i) detecting minutiae in the sensed fingerprint image (live or spoof), (ii) extracting local patches centered and aligned using minutiae orientation and location, and (iii) training MobileNet models on the aligned local patches. During the testing stage, the spoof detection decision is made based on the average of spoofnesss cores for individual patches output from the MobileNet model. The system architecture begins from taking a fingerprint as an input to the system. Features are extracted by minutiae detection and local patches are also extracted minutiae centric patches. The output of this extraction is again analysed for patch alignment by rotating and cropping similar patterns. Training MobileNet models on the aligned local patches. the spoof detection decision is made based on the average of spoofnesss cores for individual patches output from the MobileNet model.


Real or Distorted fingerprint
Fingerprint image
Minutiae Detection & local Extraction
Minutiae Centric Local Patches
Patch alignment (rotation and cropping)
Minutiae Centered and aligned local patches
Trained model
Patch Spoofness score
Fusion
Global Spoofness Score {0,1}

IV. RESULTS AND DISCUSSION

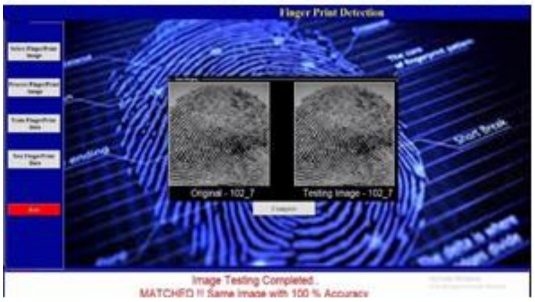


Image Testing Completed..
MATCHED !! Same Image with 100 % Accuracy

A. Comparison between Existing and the Proposed System

The Detection based on odor analysis requires an additional hardware, ie- Electronic nose which indirectly increases the cost. This system does not required any additional hardware parts. The active pore extraction and detection method to identify the fingerprint. Whereas the pore may not be active due to many reasons including the sweat. So this system focuses on minutiae rather than on pores.

The accuracy rate of this system is higher as the dataset which was used consists of multiple images for a single fingerprint.

V. CONCLUSION

False nonmatch rates of fingerprint matchers are very high in the case of severely distorted fingerprints. This generates a security hole in automatic fingerprint recognition systems which can be utilized by criminals and terrorists to use the unauthorized data. Therefore, it is necessary to develop a fingerprint distortion detection and rectification algorithms to fill the hole.

This algorithm describes a distorted fingerprint detection and rectification. To detect the distortion, the ridge orientation map of a fingerprint is used as the feature vector and a classifier is trained to classify the input fingerprint as distorted or normal. To rectify distortion, a nearest neighbour regression approach is used to predict the distortion field from the input distorted fingerprint. Afterwards the inverse of the distortion field is used to transform the distorted fingerprint. Both the rectification and detection steps can be used to speed up if a robust and accurate fingerprint registration algorithm can be developed. It becomes difficult to collect many rolled fingerprints with various distortion types.

VI. REFERENCES

[1]. Fingerprint Spoof Buster: Use of Minutiae-centered Patches TarangChugh*, Student Member, IEEE, Kai Cao, and Anil K. Jain, Life Fellow, IEEE.

[2]. D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, “Fake fingerprint detection by odor analysis,” in Proc. ICB. Springer, 2006, pp. 265–272.

[3]. Analysis of Fingerprint Pores for Vitality Detection Gian Luca Marcialis, Fabio Roli, and Alessandra Tidu Department of Electrical and Electronic Engineering – University of Cagliari Piazza d’Armi – I-09123 Cagliari (Italy).

[4]. Survey on Fingerprint Spoofing, Detection Techniques and Database, Samruddhi S Kulkarni.

[5]. A. Krizhevsky, I. Sutskever, and G. E. Hinton, “ImageNet classification with deep convolutional neural network”, in proc.Adv.NIPS,2012,pp.1097-1105.

[6]. Nogueira, R. F., de AlencarLotufo, R., & Campos Machado, R. (2016). Fingerprint Liveness Detection Using Convolutional Neural Networks. IEEE Transactions on Information Forensics and Security, 11(6), 1206–1213.doi:10.1109/tifs.2016.2520880.

[7]. Fingerprint Liveness Detection from Different Fingerprint Materials Using Convolutional Neural Network and Principal Component Analysis.

[8]. Memon, S., Manivannan, N., & Balachandran, W. (2011). Active pore detection for liveness in fingerprint identification system. 2011 19thTelecommunications Forum (TELFOR) Proceedings of Papers. doi:10.1109/telfor.2011.6143624.

[9]. K. Cao and A. K. Jain, “Hacking mobile phones using 2D Printed Fingerprints,” MSU Tech. report, MSU- CSE-16-2, 2016.

[10]. S. S. Arora, K. Cao, A. K. Jain, and N. G. Paulter, “Design and Fabrication of 3D Fingerprint Targets,” IEEE TIFS, vol. 11, no. 10,pp. 2284–2297, 2016.

[11]. F. Chollet, “Xception: Deep learning with depthwise separable convolutions,” arXiv preprint arXiv:1610.02357, 2016.

[12]. K. Simonyan and A. Zisserman, “Very deep convolutional networks for large-scale image recognition,” arXiv preprint arXiv:1409.1556, 2014.

[13]. D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, “An investigation of local descriptors for biometric spoofing detection,” IEEE TIFS, vol. 10, no. 4, pp. 849–863, 2015.

[14]. Zhao, Q., Zhang, L., Zhang, D., Luo, N., & Bao, J. (2008). Adaptive pore model for fingerprint pore extraction. 2008 19th International Conference on Pattern Recognition. doi:10.1109/icpr.2008.4761458.

Cite this article as :

Harshada Kanade, Gauri Uttarwar, Shweta Borse, Archana. K, "Fingerprint Distortion Detection", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 3, pp. 559-562, May-June 2020. Available at doi : https://doi.org/10.32628/CSEIT2063204
Journal URL : http://ijsrcseit.com/CSEIT2063204