Fingerprint Spoof Detection using of Minutiae-Centered Patches and Energy

Ms. Tajane Prajakta[1] Ms. SukeshniGawai[2] Ms. Nakhate Swapna[3] Ms. KadlagTejashree[4]
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]Dr. D. Y. Patil Polytechnic, Akurdi, Pune, India

Abstract— The individuality of fingerprints is being used tremendously now a days, for a day today applications, ranging from unlocking a smartphone to every security device's out there. While the major purpose of a fingerprint recognition system is to ensure a reliable and accurate user authentication, the security of the recognition system itself can be jeopardized by spoof attacks. This study addresses the problem of developing accurate and generalizable algorithms for detecting fingerprint spoof attacks. We propose a system which utilizing local patches extracted around fingerprint minutiae. The individuality of fingerprints is being used for a day-to-day applications, ranging from unlocking a smartphone to major military applications. While the primary purpose of a fingerprint recognition system is to ensure a reliable and accurate user authentication, the security of the recognition system itself can be jeopardized by spoof attacks. This study addresses the problem of developing accurate and generalizable algorithms for detecting fingerprint spoof attacks.

Key words: Fingerprint Spoof Detection, Presentation Attack Detection, Convolutional Neural Networks, Minutiae-Based Local Patches, Liveness Detection

I. Introduction

Fingerprint spoof detection methods are very much urgently needed to avoid such attacks on fingerprint authentication systems, thereby increasing the security and trust in such systems. The various anti-spoofing approaches that has been proposed in the literature can be broadly classified into hardware-based and software-based solutions respectively. The hardware-based solutions typically require the fingerprint reader to be augmented with sensor(s) to detect the characteristics of vitality, such as blood flow, skin distortion, and odor and so on. There are also special types of fingerprint sensors, such as Luminism's multispectral scanner and Compact Imaging's multiple reference optical coherence tomography (OCT), that capture sub-dermal ridge patterns in the finger. An open-source fingerprint readers with a multi camera design provides two complementary streams of information which is useful for spoof detection. Software-based solutions, on the other hand, extract features from presented fingerprint image (frame sequence) acquired by the fingerprint sensors, without including any additional hardware cost, to differentiate between live and spoof fingers.

One of the limitations caused by many of the published anti-spoof methods is that, their inability to generalize across spoofing materials. Studies in have shown that when a spoof detected, spoofs fabricated using materials that were not seen during training, there can be up to a three-fold increase in the spoof detection error rates. To generalize an algorithm's effectiveness across fabrication materials, called cross-material performance, some studies have approached spoof detection as an open-set.

A. Existing System

Among these, fingerprint spoof attack (i.e. Printed targets and gummy fingers) are the most common forms of presentation attacks, with a multitude of fabrication processes ranging from the basic molding and the casting to utilizing 2D and 3D printing techniques. The various anti-spoofing approaches proposed, and they can be broadly classified into hardware-based and software-based solutions. The hardware-based solutions generally require the fingerprint reader to be augmented with sensor(s) to detect the characteristics of the system.

Software-based solutions, extracts the features from the fingerprint image presented(or a sequence of frames) taken by the fingerprint sensors, without including or adding any additional hardware cost, to differentiate between live and spoof fingers.

B. Disadvantages

One of the limitations of many of the published anti spoof methods is their poor generalization performance across spoof materials. when a spoof detector is evaluated on spoofs fabricated using

Materials that were not seen during training, there can be up to a three-fold increase in the spoof detection error rates.

II. Proposed System

Fingerprint spoof detection methods are urgently needed to thwart such attacks on fingerprint authentication systems, thereby increasing user confidence in such systems. Utilized fingerprint domain-knowledge to design a robust fingerprint spoof detector, where local patches centered and aligned using fingerprint minutiae are utilized for training and also used energy component. This differs from other published approaches which have generally used the whole fingerprint image for spoof detection.

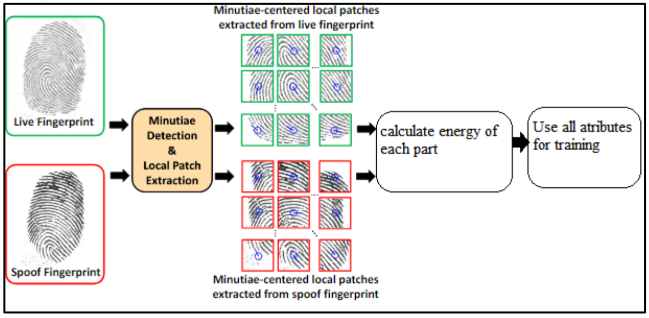
Minutiae-centered local patches extracted from live fingerprint
Live Fingerprint
Minutiae Detection & Local Patch Extraction
calculate energy of each part
Use all atributes for training
Spoof Fingerprint
Minutiae-centered local patches extracted from spoof fingerprint

Fig. 1: System Architecture

III. Advantages

1) Finger print reader operator to visually examine the local regions of the fingerprint highlighted as live or spoof,

instead of relying on a single score, as output by the traditional approaches.

2) Efficiently use all attributes.

IV. Requirements:

A. *Hardware Requirements*

System Processors	:	Core2Duo
Speed	:	2.4 GHz
Hard Disk	:	150 GB

B. *Software Requirements:*

Operating system	:	64bit Windows 7 and on words
Coding Language	:	MATLAB

V. Conclusion

We have utilized fingerprint domain knowledge by extracting local patches centered on minutiae locations and it combines with a directional wavelet approach for getting better results. The local patch-based approach provides salient cues to differentiate spoof fingerprints from live fingerprints. The proposed approach is able to achieve a significant reduction in the error rates.

References

[1] T. Chugh, K. Cao, and A. K. Jain, “Fingerprint Spoof Detection using Minutiae-based Local Patches,” in IEEE International Joint Conference on Biometrics (IJCB), 2017.

[2] S. Marcel, M. S. Nixon, and S. Z. Li, Handbook of Biometric Anti- Spoofing. Springer, 2014.

[3] ODNI, IARPA, “IARPA-BAA-16-04 (Thor),” https://www.iarpa.gov/index.php/research-programs/odin/odin-baa, 2016.

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

[5] 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.