



Fingerprint Presentation Attack Detection Using Transfer Learning Approach

Rajneesh Rani, National Institute of Technology, Jalandhar, India

 <https://orcid.org/0000-0003-2104-227X>

Harpreet Singh, National Institute of Technology, Jalandhar, India

 <https://orcid.org/0000-0002-5716-2196>

ABSTRACT

In this busy world, biometric authentication methods are serving as fast authentication means. But with growing dependencies on these systems, attackers have tried to exploit these systems through various attacks; thus, there is a strong need to protect authentication systems. Many software and hardware methods have been proposed in the past to make existing authentication systems more robust. Liveness detection/presentation attack detection is one such method that provides protection against malicious agents by detecting fake samples of biometric traits. This paper has worked on fingerprint liveness detection/presentation attack detection using transfer learning for which the authors have used a pre-trained NASNetMobile model. The experiments are performed on publicly available liveness datasets LivDet 2011 and LivDet 2013 and have obtained good results as compared to state of art techniques in terms of ACE(average classification error).

KEYWORDS

Biometrics, Fingerprints, Presentation Attack Detection, Transfer Learning

1. INTRODUCTION

For decades, human civilization has been strongly subjected to the need for authentication systems to prove their identity. Traditional methods for authentication like cards with pins and passwords are no longer safe(Yuan et al., 2019a) as they can be lost or stolen. So biometrics became very popular as it is more robust and secure as authentication is concerned.

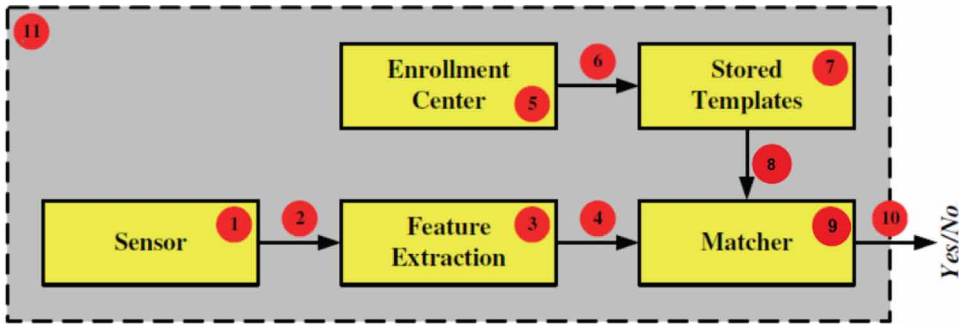
Biometrics based on behavioral or physiological traits are used for authentication. Physiological biometric traits, fingerprints are widely used across the globe due to their best-known properties such as individuality, durability, and universality (Ghani et al., 2013b). Mobile phones are widely used for money transactions these days(Kim, 2016). Many government-issued identities are fully dependent on fingerprint biometric systems which have surged the use of fingerprint authentication. This high-level dependency comes with the risk of critical attacks such as presentation attacks, spoofing attacks, etc. Replica of an original fingerprint can be created by materials like gelatin, silicon, wood glue, etc which is very hard to distinguish from the original one. The whole biometric system can be fooled in a number of ways (Paridah et al., 2016) which comprises attacks at various stages of the biometric system as shown in Figure 1.

At stage 1, a hacker can perform a direct attack by manipulating sensor to obtain fake fingerprint as an authentic one, at stage 2 biometrics previously collected by the sensor can be resent to fool

DOI: 10.4018/IJIT.2021010104

This article published as an Open Access Article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

Figure 1. Basic Components biometric system (Paridah et al., 2016)



the system. At stage 3 and 4 features can be changed in the feature extraction stage to stop a real user from getting recognized. In the enrolment center at stage 5, there is a great risk of enrolling fake fingerprints similar to stage 1. The attack on the transmission channel between the module and registration databases can also be performed in stage 6. Even if the sensor is not manipulated and features are extracted properly the database can still be hacked to steal stored templates or features to perform a reply attack in stage 7. While at stage 8 the attack on the transmission channel between the database templates and the comparison module can be performed. Finally, at stages 9 and 10 the decision of a biometric system can be changed by a hacker to allow the fake user or restrict the actual user. All stages were targeted to a particular component of the biometric system but as in stage 11, the whole standalone application can also be attacked. The features, database and final output can be secured by utilizing the regular computerized protection methods (digital signature, encryption, hash function, access control,) or by keeping vulnerable parts of a system in a safe place. But these techniques still fail to discriminate fake fingerprints and live fingerprints.

Liveness detection /presentation attack detection is the field that comes with a solution to this problem which includes both hardware and software methods (Naccache et al., 2011). Hardware-based methods require additional hardware units to detect traits such as blood pressure, heartbeat, odor, etc. whereas software-based methods are more popular because they require a single standard sensor thus are comparatively cheap and scalable.

In this paper, we have used a pre-trained NASNet Mobile model which was further modified at last layer and retrained on liveness datasets LivDet 2011 and LivDet 2013 to classify fake and live images. We have evaluated results for whole dataset training, cross-dataset training, and cross material training scenarios.

We have divided this paper into five more sections. Related work and state of art techniques are reviewed in Section 2, the methodology stating the basics and our proposed model in has been discussed in Section 3, datasets and performance metrics used in experiments are covered in Section 4, the results for experiments are shown in Section 5 and finally, in Section 6, we have concluded our work along with future scope.

2. RELATED WORK

Many creators have worked on fingerprint ridges for liveness task, Schuckers(Abhyankar and Schuckers, 2006)used multi-resolution textures and frequencies of ridges for detecting liveness of fingerprints and achieved 1.4% of error rate on a dataset collected in their own lab.

Manivanan(Manivanan et al., 2010)proposed a technique to detect active sweat pores on fingerprints to conclude fingerprints as fake or live. This study was able to successfully achieve a 94.12 to 97.41% classification rate on their own dataset.

13 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/fingerprint-presentation-attack-detection-using-transfer-learning-approach/272008

Related Content

DEAL: A Distributed Authorization Language for Ambient Intelligence

Irini Genitsaridi, Antonis Bikakis and Grigoris Antoniou (2011). *International Journal of Ambient Computing and Intelligence* (pp. 9-24).

www.irma-international.org/article/deal-distributed-authorization-language-ambient/61137

Software Effort Estimation: Harmonizing Algorithms and Domain Knowledge in an Integrated Data Mining Approach

Jeremiah D. Deng, Martin Purvis and Maryam Purvis (2011). *International Journal of Intelligent Information Technologies* (pp. 41-53).

www.irma-international.org/article/software-effort-estimation/58055

Multilogistic Regression by Product Units

P. A. Gutiérrez, C. Hervás, F. J. Martínez-Estudillo and M. Carbonero (2009). *Encyclopedia of Artificial Intelligence* (pp. 1136-1144).

www.irma-international.org/chapter/multilogistic-regression-product-units/10383

The EMPRISES pan-European Framework: Monitoring and Combatting Serious Organised Economic Crime

Simon Polovina, Simon Andrews, Babak Akhgar, Andrew Staniforth and Dave Fortune (2014). *International Journal of Conceptual Structures and Smart Applications* (pp. 76-87).

www.irma-international.org/article/the-empri-ses-pan-european-framework/134889

Rough ISODATA Algorithm

S. Sampath and B. Ramya (2013). *International Journal of Fuzzy System Applications* (pp. 1-14).

www.irma-international.org/article/rough-isodata-algorithm/101766