Chapter 10
Aletheia:
A Hybrid AI Framework for Fake Biometric Fingerprint Detection

Claudia Mattar
https://orcid.org/0009-0002-4813-9100
Issam Fares Faculty of Technology, University of Balamand, Lebanon

Claritta AlSaneh
https://orcid.org/0009-0005-7256-8054
Issam Fares Faculty of Technology, University of Balamand, Lebanon

Soraia Oueida
https://orcid.org/0000-0002-6720-2307
College of Engineering and Technology, American University of the Middle East, Kuwait

ABSTRACT

The purpose of this work is to create a fake biometric detection system that detects fake biometric images. The system utilizes generative artificial intelligence, particularly a Deep Convolutional Generative Adversarial Network, to generate fake fingerprints in the best accuracy possible. Tested on fingerprint images, extracted from SOCOFing database, the system resulted with an accuracy of 99.17%. Two different datasets: the real dataset and the fake dataset are then passed through a Support Vector Machine model with linear Kernel to test and calculate the accuracy of detection of both systems. A Sanity Check Accuracy test is performed to check the sanity of the system, offering promising results after label shuffling and retraining of the SVM. The proposed system also uses image quality analysis like Laplacian Blur estimation, Local Binary Pattern features, Edge density, and Histogram Entropy to extract features for testing and training the SVM.

DOI: 10.4018/979-8-3373-4972-5.ch010

Copyright © 2026, IGI Global Scientific Publishing. Copying or distributing in print or electronic forms without written permission of IGI Global Scientific Publishing is prohibited. Use of this chapter to train generative artificial intelligence (AI) technologies is expressly prohibited. The publisher reserves all rights to license its use for generative AI training and machine learning model development.

INTRODUCTION

Biometric authentication systems, such as fingerprint and iris recognition, have become integral components of modern security infrastructure due to their convenience and uniqueness. These systems are becoming more necessary with time due to the widespread use of authentication techniques and technologies. The word biometric indicates any unique characteristics that can lead to revealing a person's identity, because each person has unique features in their biometrics which made researchers over time rely on this type of authentication for better security and identity protection. However, despite their widespread adoption, these systems are increasingly susceptible to spoofing attacks, in which adversaries use artificial biometric traits such as printed fingerprints or synthetic iris images to deceive the authentication process. These vulnerabilities pose serious risks to the integrity and reliability of biometric-based security systems. The issues caused by the use of fake biometrics can have a significant impact on today's society; for example, the lack of diversity in authentication systems may lead some programs to identify real images as fake. This issue is called the False Positives and False Negatives issue in which the system is left uncapable of distinguishing between real and fake data samples. Also, spoofing attacks resulting from these fake biometric detection systems can lead to big ethical and legal issues in terms of increase in identity thief and other identification problems. In addition, privacy concerns are a major issue when it comes to biometric detection. A stolen or synthetic biometric can lead to sensitive information leaking of the user, alongside other issues like misuse of private information such as credit card numbers, banking financial transactions and social media profiles. In terms of big companies, especially those who work in the field of finance, a certain attack or spoofed identity to their system can cause unmanageable financial and data loss, in which a single stolen identity can result in system manipulation and data breaches. Potential of surveillance and abuse could be another risk to pay attention to, in particular applications that use live location or real time IP cameras that record real time video data. The system, when deceived in these cases, can higher the risk of surveillance and abuse, potentially causing a social issue to the user due to an unsafe environment. To address this critical challenge, the proposed framework, Aletheia, aims to develop an intelligent system capable of distinguishing between genuine and spoofed biometric samples. Aletheia means in Greek the truth. While not heavily mythologized, Aletheia represents truth and sincerity. By leveraging machine learning and deep learning techniques, the system analyzes image quality metrics and subtle features imperceptible to the human eye to accurately detect forged biometric inputs. The main goal here is to enhance the robustness and trustworthiness of biometric authentication systems by introducing a layer of automated fake biometric detection. This not only strengthens security

26 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/chapter/aletheia/402972

Related Content

Assessment of Fuzzy Logic Radioisotopic Pattern Identifier on Gamma-Ray Signals with Application to Security
Miltiadis Alamaniotis, Jason Youngand Lefteri H. Tsoukalas (2014). *International Journal of Monitoring and Surveillance Technologies Research (pp. 1-21).*
www.irma-international.org/article/assessment-of-fuzzy-logic-radioisotopic-pattern-identifier-on-gamma-ray-signals-with-application-to-security/116730

Evaluation of Human Machine Interface (HMI) on a Digital and Analog Control Room in Nuclear Power Plants Using a Fuzzy Logic Approach
Pola Lydia Lagari, Antonia Nasiakouand Miltiadis Alamaniotis (2016). *International Journal of Monitoring and Surveillance Technologies Research (pp. 50-68).*
www.irma-international.org/article/evaluation-of-human-machine-interface-hmi-on-a-digital-and-analog-control-room-in-nuclear-power-plants-using-a-fuzzy-logic-approach/167694

Improving the Supervised Learning of Activity Classifiers for Human Motion Data
Liyue Zhao, Xi Wangand Gita Sukthankar (2013). *Human Behavior Recognition Technologies: Intelligent Applications for Monitoring and Security (pp. 282-303).*
www.irma-international.org/chapter/improving-supervised-learning-activity-classifiers/75296

Efficient Delivery Of Government Schemes Using Blockchain Technology And Cryptography: E Governance using Blockchain Technology
(2022). *International Journal of Smart Security Technologies (pp. 0-0).*
www.irma-international.org/article//287872

Introduction to Eye and Gaze Trackers
Dan Witzner Hansen, Arantxa Villanueva, Fiona Mulveyand Diako Mardanbegi (2012). *Gaze Interaction and Applications of Eye Tracking: Advances in Assistive Technologies (pp. 288-295).*
www.irma-international.org/chapter/introduction-eye-gaze-trackers/60046