



All



ADVANCED SEARCH

Conferences > 2023 10th International Confe... ?

Detection of Iris Template Attacks using Machine Learning and Deep Learning Methods

Publisher: IEEE

Cite This

PDF

D. Shanmugapriya ; G. Padmavathi ; A. Aysha All Authors



57 Full Text Views

Alerts

Manage Content Alerts Add to Citation Alerts

Abstract



Document Sections

- I. Introduction
- II. Related Work
- III. Proposed Methodology
- IV. Implementation and Results
- V. Conclusion

Abstract:Iris recognition is a biometric identification method that uses patterns in the iris, the coloured ring around the eye's pupil, to identify individuals. One of the most v... **View more**

Metadata

Abstract:

Iris recognition is a biometric identification method that uses patterns in the iris, the coloured ring around the eye's pupil, to identify individuals. One of the most vulnerable attacks in iris detection is the template attack. An iris template attack is a type of biometric spoofing where an attacker attempts to gain access to a secure system by presenting a fabricated iris image or video as the authentic iris of the legitimate user. It is essential to detect these attacks to ensure the security and reliability of iris recognition systems and to prevent potential misuse and abuse. Machine learning and deep learning methods can potentially be used to detect template attacks on iris recognition systems, such as attempts to deceive the system using forged or altered iris templates. These methods involve training a model on a large dataset of iris images with both genuine and altered and using the trained model to classify new iris images as genuine or attacked. Hence, we propose a methodology that uses Logistic Regression (LR) and Convolutional Neural Network (CNN) to detect the Iris template attack. Through extensive experiments with the CASIA-IrisV1 dataset, CNN achieves an average accuracy of 98.75% and surpasses LR in recognizing iris template attack. Meanwhile, the performance of CNN is enhanced by applying the max pooling property to achieve 100% accuracy.

Published in: 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)

Date of Conference: 15-17 March 2023

Publisher: IEEE



▼ ISBN Information:

Electronic ISBN:978-93-80544-47-2

Print on Demand(PoD) ISBN:978-1-6654-7703-1

☰ Contents

I. Introduction

Biometric technology has garnered much interest recently. Compared to more traditional recognition techniques, it has been widely implemented in many applications to boost user comfort and the security level of identification systems [1], [2]. Recent studies, however, have revealed that data-gathering systems can be tricked by attackers using fake samples, making biometric recognition technologies vulnerable to attacks [3]. By direct or indirect attacks on biometric templates, an unauthorized individual can be verified as genuine by a biometric identity system. In order to protect against attackers and increase the security level of a biometric recognition system, template attack detection techniques are required.

Authors	▼
Figures	▼
References	▼
Keywords	▼
Metrics	▼

More Like This

Convolutional Neural Networks for Automatic Threat Detection in Security X-Ray Images
2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)
Published: 2018

Self-supervised learning based low light image enhancement using convolutional neural networks
2022 OPJU International Technology Conference on Emerging Technologies for Sustainable Development (OTCON)
Published: 2023

Show More

IEEE Personal Account

CHANGE USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
VIEW PURCHASED DOCUMENTS

Profile Information

COMMUNICATIONS PREFERENCES
PROFESSION AND EDUCATION
TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800 678 4333
WORLDWIDE: +1 732 981 0060
CONTACT & SUPPORT

Follow



[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [IEEE Ethics Reporting](#) | [Sitemap](#) | [IEEE Privacy Policy](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2024 IEEE - All rights reserved.

IEEE Account

- » [Change Username/Password](#)
- » [Update Address](#)

Purchase Details

- » [Payment Options](#)
- » [Order History](#)
- » [View Purchased Documents](#)

Profile Information

- » [Communications Preferences](#)
- » [Profession and Education](#)
- » [Technical Interests](#)

Need Help?

- » **US & Canada:** +1 800 678 4333
- » **Worldwide:** +1 732 981 0060
- » [Contact & Support](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2024 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.