Birzeit University
Information Technology
Department of Computer Science
Computer Security Course | COMP432
Dr. Moahhmed Al-Khanfseh | Section 1
Final Project

Prepared by: Sondos Aabed, 1190652

Iris Presentation Attack Detection (PAD)

Abstract

In this report, the Iris Presentation Attack Detection (PAD) field is presented. It is a kind of attack that happened with biometric-based using the Iris-eye Authentication where an imposter tries to mislead the model. This report investigates PAD methods as security countermeasures, covers threats posed by PAs, and existing PAD techniques. Finally, the report discusses future challenges in PAD.

***Keywords**:* presentation attack Detection (PAD), presentation attack (PA), Iris Recognition (IR), Biometric Authentication, Cybersecurity

1. Introduction

The science of Cybersecurity has become essential and irreparable in modern life. With the rise of information technology, the fragility and vulnerability also increases. One of the aspects that cybersecurity addresses is the sophisticated kinds of cybercrime and cyberespionage activities, as well as cyber-terror and cyberwar. Another aspect that cybersecurity addresses is Controlling Access for computer resources, with a known framework called: the triple A's (AAA) [1] it stands for Authentication, Authorization, and Accounting. This report is concerned with the first A: the Authentication part. Simply put, Authentication is when the user provides information to the system that affirm they are who they claim to be. There are three main types of authentication:

- **Something you know**, like a password.
- **Something you have**, like a Universal Serial Bus (USB) key.
- **Something you are**, such as fingerprint or other biometrics.

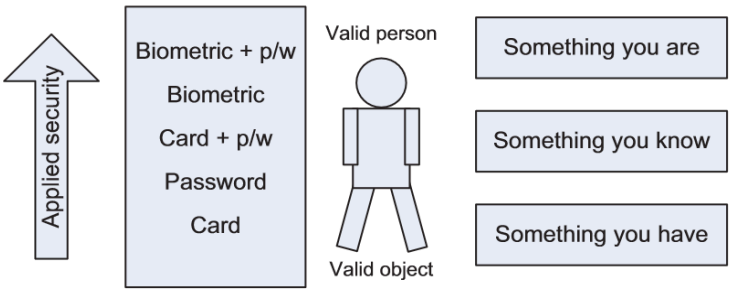

Fig. 1: Access control: Perceived level of applied security [2]

Something you are or Biometric-based authentication has gained attention in authentication due to what it brought to the table as against somethings you know and somethings you have. It overcame and introduced negative and positive recognition. However, biometric-based raises privacy concerns in terms of collection. [3] That introduces to the organisations who use the biometric-based data protection tasks. In this report, the focus is on Iris biometric authentication. The Iris-Recognition has been widely used in identification for these reasons: [4]

1. **Unique**: there are not any iris having the same physical characteristic as others, even if they come from the same person or identical twins;
2. **Stability**: the iris is formed during childhood, and it generally maintains unchangeable physical characteristics throughout life;
3. **Informative**: the iris has rich texture information such as spots, stripes, laments and coronas.
4. **Safety**: Since the iris is located in a circular area under the surface of the eye between the black pupil and the white sclera, it is rarely disturbed by external factors. As a result, it is difficult to forge the iris pattern;
5. **Contactless**: Iris Recognition (IR) is more hygienic than biometrics that requires contact, such as fingerprint recognition.

Despites the latter, the biometric-based authentication systems may still be susceptible to certain types of attacks. This introduces us to one type of attack that this report will be addressing which is called the Presentation Attacks (PA). They are those presentations to a biometric capture which aims to drive the authentication system into an incorrect decision whether this is the actual person or not. This brings us to Presentation Attacks Detection (PAD) which is competing against such sophisticated attacks to detect it. In this report, elaborations on methods, history of such attacks and the prevention, detection are presented. It happens with different motivations either: [5]

- **Identity concealment:** *untargeted attacks* aim to prevent the subject from being recognized. The attacker misleads the model into predicting incorrect classifications. The most common tool for Concealer Attack Presentation is textured contact lenses, which obscure significant portions of the iris, thereby preventing the recognition system from identifying the user.
  Various brands of textured contact lenses are available. The primary objective of this attack is to ensure the user's anonymity. While textured contact lenses could theoretically be used in Impostor Attacks by transcribing a genuine iris texture onto the lens, there are no known successful demonstrations of this type of impostor attack.[11]

- **Identity Theft or Impersonation:** These targeted attacks involve misleading the model into identifying the attacker as someone else. Impostor Attack Presentation typically uses authentic images of an iris. For instance, attackers might use an iris image of someone who has access to a system to gain unauthorised entry.
  Common methods include using paper printouts of iris images or replay attacks, where genuine iris images are displayed on a screen and presented to the sensor. Generally, executing a successful Impostor Attack is more challenging than a concealer attack because it requires the recognition software to identify the attacker as a known individual, whereas a concealer attack merely needs the system to fail to recognize the attacker. [11]

1.1 Motivation and research questions

Motivation:

The motivation arises from the initial project, in which an Iris based authentication system was developed. Despite achieving high accuracy, it's essential to address a potential vulnerability in such a security system to evaluate the model's ability in achieving Authentication purpose. Specifically, the presentation attacks and the mitigation of such vulnerabilities.

Research Questions:

- **Q0:** What are the threats and risks of the PA attacks?
- **Q1**: What are the types of PA?
- **Q2:** What are the current and past countermeasures used for the PA attack?
- **Q3:** What are the future challenges that may arise in PA attack?

2. Background

The anatomy of the human eye has inspired computer vision tasks from the beginning. As shown in the following figure, the Iris is located between the white sclera and the cornea. That is a contactless area from the human face. [6] It is worth mentioning that left and right iris have distinctive patterns too for the same person.

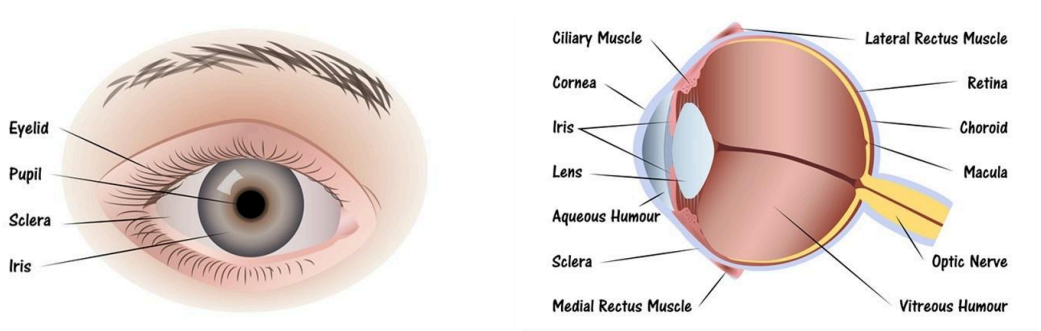

Fig. 2: Human-Eye Anatomy [6]

2.1 Iris Recognition Technology

Iris Recognition technology is the use of automated methods of biometric identification that depends on mathematical induction of rules that define such complex patterns. [7] The idea is to minimise the the **intra** which is the patterns (within) that helps identify the person, while also maximise the **inter** which is the patterns (between) that differs that person from the other one. The process starts by acquisition stage, it could be done using different devices such as the one shown in the following which is a secure Kit used portable for enrollment and recognition:

Fig. 3: Iris scanner PIER 2.3 (Portable Iris Enrollment and Recognition) from SecuriMetrics [8]

Once the individual Iris is acquired using these devices, the features then are extracted. It could be implicitly or explicitly extracted to create a unique template matrix. The template will then be matched and compared against the other templates. The Authorization is granted or denied based on the Authentication of the Iris results. [7]

Two Iris templates from the same eye will be forming a genuine pair. While two different eyes will form an imposter pair. The matching comparison between the templates includes correlation ana;ysis, both the genuine pairs and the imposter are correlated, but the correlation from the same eye are stronger. [9]

2.2 Iris Recognition System Vulnerabilities

The following figure shows the block diagram of the Iris Recognition System and indicates the vulnerabilities (it is the same in biometric-based authentication systems). There are different subsystems (modules) each would have vulnerability. The modules and the vulnerabilities are as follows: communication protocols, data storage or resilience to artifact presentations, and others.

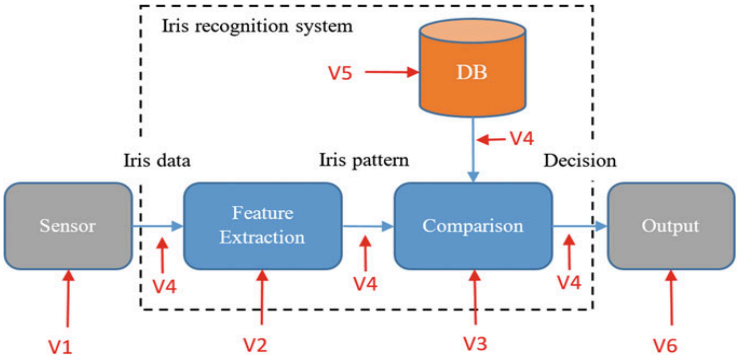

Fig. 4: Iris Recognition System Vulnerabilities (Block Diagram) [10]

- **Sensor (Vulnerability 1):** Sensors include visible and near-infrared imaging. The capture of the iris pattern could be an image or a video. The main vulnerability here is the presentation of artifacts (e.g., photos, videos, synthetic eyes) that mimic real iris characteristics. That is our focus on this report. [10]

- **Feature extraction and matcher modules (Vulnerabilities 2 and 3):** Feature extractor could include explicitly preprocessing, segmentation or implicit feature extraction using deep learning. Matching modules include template generation, and comparison. Vulnerability of those modules can involve altering algorithms to perform illegitimate operations (e.g., modified templates, altered comparisons). [10]

- **Database (Vulnerability 5):** the structured data related to subject information, devices, and iris templates. Alteration to this information can impact the system's final response therefore it's a vulnerability. The security level of database storage varies by application, and using encrypted templates is crucial to ensure unlinkability between systems and prevent attacks based on weak links. [10]

- **Communication channel and actuators (Vulnerability 4 and 6):** Internal communications (e.g., between software modules) and external communications (e.g., with mechanical actuators or cloud services). The primary vulnerabilities lie in the potential alteration of information transmitted and received by the different modules of the IRS. [10]

2.3 Presentation Attack Threats and risks

Presentation Attack (PA) happens in the stage of acquisition for recognition. The attacker or perpetrator will either use someone else's Iris biometric data. If the attacker succeeds in getting the Authorization then a serious breach to the system is done. The successful PAs have serious consequences for starting the Unauthorised access to the system resources, leading to data breach, financial losses and breaking the trust of the user. Violation of privacy too.

For the risk assessment, the damage caused by a successful PA increases with the increased value of the assets being protected. The risk is even higher based on the attacker's motivation. It could be financial gain, espionage, or other malicious intents. These threats detection of the PA will be elaborated upon in the literature review section.

2.4 Presentation Attack Types

The presentation attacks could occur on three different types either **Presentation attack for textured contact lens** which involves using contact lenses designed to imitate the iris pattern of another individual (impostor attack) or to conceal one's identity (identity concealer attack). Although replicating a real iris pattern onto contact lenses is theoretically possible, practical challenges reduce the likelihood of such an attack. The second scenario is particularly concerning because a significant number of people wear contact lenses, with approximately 125 million users worldwide. [10]

There are two types of contact lenses to consider: transparent and textured contact lenses. Textured contact lenses alter the original iris information by overlaying synthetic patterns, such as those used in cosmetic lenses to change eye colour. While primarily intended for cosmetic use, this technology could be used to print realistic iris patterns. If users are enrolled in the Iris Recognition System (IRS) while wearing these lenses, the system can be deceived. Asking users to remove contact lenses before recognition is undesirable as it reduces comfort and usability. [10]

The following figure, if you look at a zoom in, the printed lens are noticed above the real person Iris. In the first one it shows the transparent one, and the second one show the textured lens:

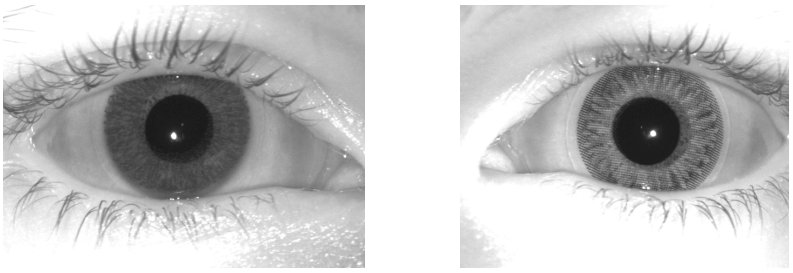

Fig. 5: Iris Presentation Attack for textured contact lens [11]

The second type of presentation attack is **Presentation attack for print iris images**. In this attack, a printed photo, digital image, or video of the spoofed iris is displayed directly to the sensor of the System (IRS). With the social media platforms (e.g., Flickr, Facebook, Instagram), headshots of targeted individuals, from which their iris patterns can be extracted, are becoming accessible. Although facial features and voice patterns are more commonly exposed in biometric modes, iris patterns can still be captured from high-resolution face images (e.g., 200 dpi resolution). [10]

High-quality iris photographs can be easily printed using commercial cameras (with up to 12-megapixel sensors, commonly found in modern smartphones) and inkjet printers (typically

offering 1200 dpi resolution). Many mobile devices, such as smartphones and tablets, are equipped with high-resolution screens capable of displaying realistic images and videos in the visible spectrum. Video attacks, which are more advanced than photo attacks, can replicate both the static and dynamic features of the eye. The following figure shows an example of printed Iris images:

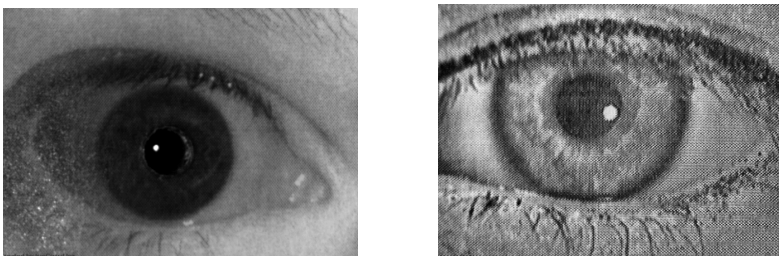

Fig. 6: Iris Presentation Attack for printed Iris images [11]

The last type is the **Presentation attack for synthetic eyes.** It is the most sophisticated type of presentation attack. These attacks utilise artificial eyes designed to replicate the characteristics of real ones. Prosthetic eyes have been employed since the early 20th century to address the aesthetic issues associated with eye loss due to blindness or amputation. Modern prosthetic manufacturing technologies can create highly realistic eyes, accurately imitating key attributes and even using materials with similar physical properties, such as elasticity and density. [10]

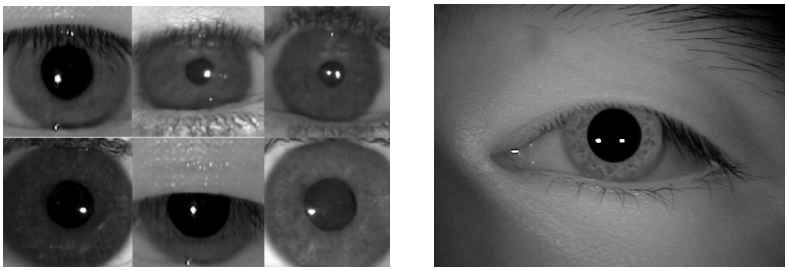

Fig. 7: Iris Presentation Attack for synthetic eyes [11]

2.5 Presentation Attack Detection Error Rates

The following list shows the basic PAD-related error metrics include: [11]

1. **Imposter Attack Presentation Match Rate (IAPMR)**: the proportion of impostor attack presentations that are successful, where the biometric reference for the targeted identity is matched (analogous to the false match rate (FMR) in identity verification).
2. **Concealer Attack Presentation Non-Match Rate (CAPNMR)**: the proportion of concealer attack presentations that are successful, where the biometric reference of the concealer is not matched (analogous to the false non-match rate (FNMR) in identity verification).
3. **Attack Presentation Classification Error Rate (APCER)**: the proportion of attack presentations incorrectly classified as bona fide presentations.
4. **Bona Fide Presentation Classification Error Rate (BPCER):** the proportion of bona fide presentations incorrectly classified as presentation attacks.

3. Systematic Literature Review

The field has gone through the typical development of approaching a computer vision problem. There are three pipelines that are shown below in a systematic tabular literature review:

1. Traditional Computer Vision-Based Methods
2. Deep Learning-Based Methods
3. Hybrid Methods

3.1 Traditional Computer Vision-Based Methods

Traditional computer vision-based methods have been the first of Iris Presentation Attack Detection (PAD) techniques. The features are handcrafted and classical machine learning algorithms are used to identify presentation attacks. The problem with these is the struggle with generalisation to unseen attack types. The following table summarises traditional computer vision-based approaches:

Table 3.1: Traditional Computer Vision-Based Methods Systematic Literature Review

Authors	Method	Description	Performance
[12]	Open Source PAD Method Based on 2D Iris Texture Features	Open-source PAD method using multi-scale BSIF features and classifiers (SVM, MLP, RF). Leveraged commercial iris sensor alignment.	Competitive with LivDet-Iris 2017
[13]	Multi-Spectral Iris Sensor with Five Frequency Bands	Sensor with 5 frequency bands using texture (LBP, GLCM), image quality (BRISQUE), and spectral variation features.	0% BPCER, 5% APCER
[14]	Photometric Stereo-Based 3D PAD Method (OSPAD-3D)	Uses photometric stereo to detect shadow differences in iris images with/without textured contact lenses.	-
[15]	Curvature Change Detection of Outer Cornea Surface	Detects contact lenses by changes in outer cornea curvature.	0% error rate on self-collected data
	OSPAD-Fusion	Combines 2D textural (OSPAD-2D) and 3D photometric stereo (OSPAD-3D) features. Cascaded fusion improves overall detection.	Best on ND-CLD'15, NDIris3D

3.2 Deep Learning-Based Methods

Deep learning-based methods have revolutionised the field of Iris PAD since 2018 by introducing neural network architectures capable of learning features directly from raw data. These methods achieved superior performance to traditional approaches and reached the state of the art performances, particularly in terms of robustness and generalisation to different attack types. However, the challenge is the need for large annotated datasets and significant computational resources. The following table summarises Deep Learning-based approaches:

Table 3.2: Deep Learning-Based Methods Systematic Literature Review

Authors	Method	Description	Performance
[16]	Ensemble CNNs	Transforms BSIF representations into more discriminative features using an ensemble of neural networks.	Outperforms state-of-the-art

[17]	DensePAD	Uses DenseNet for normalised iris images to detect bona fide or attack samples, addressing textured contact lenses.	Good cross-dataset/attack performance
[18]	CNNs for Iris and Ocular	CNNs for iris region patches and ocular region analysis. Three CNNs fused for decision-making.	Strong cross-dataset performance
[19]	IrisCode Information	Uses un-normalized irises with three CNNs to detect textured contact lenses and paper printouts.	More accurate with un-normalized irises
[20]	Fine-Tuned VGG-16	Detects post-mortem samples with analysis on class activation maps.	Strong for post-mortem, no cross-attack analysis
[21]	CNN Feature Extractors	Combines CNN features for global and local iris regions, using SVMs for score generation.	Better than end-to-end CNN, resilient against unseen attacks
[22, 23]	Adversarial Learning	Uses GANs with RaSGAN and relativistic discriminator for synthetic iris generation and attack detection.	High generalisation capabilities
[24]	Latent Representations with GANs	Uses GANs to learn latent representations invariant to attack type, aiming for robust generalisation.	Limited by small dataset, promising results

3.3 Hybrid Methods

Hybrid methods combine the strengths of both traditional computer vision and deep learning approaches to enhance the robustness and accuracy of Iris PAD systems. Integrating handcrafted features with deep learning-based features. Hybrid approaches often result in improved performance and generalisation across different datasets and attack scenarios. The following table summarises Hybrid approaches:

Table 3.3: Hybrid Methods Systematic Literature Review

Authors	Method	Description	Performance
[25]	Haralick + VGG Features	Combines Haralick texture features in the RDWT domain with VGG features reduced by PCA, input to a 3-layer MLP for classification.	Outperforms individual features and several baselines
[26]	Group Sparsity Feature Selection	Uses six traditional features and one deep feature from VGG. Group sparsity and dropout to avoid overfitting and reliance on certain features.	Outperforms state-of-the-art on NDCLD'13, IIITD, and Clarkson LivDet-Iris 2013
[27]	Score-Level Fusion	Fuses data-driven features from Densenet121 and handcrafted features. Guided by Friedman test to select top k features. Evaluated on multiple datasets.	Outperforms Group Sparsity Feature Selection and state-of-the-art in most experiments

4. Future Research Directions

The potential challenges in these fields that may arise in the future and already arising includes: open source code, Reasonable AI specifically fairness and finally the generalisation to unknown attack types. [11]

- **Open Source Code Availability:** Ensuring that PAD methodologies are openly accessible through source code availability is crucial for benchmarking. Having open-source methods enables researchers to build upon existing frameworks.

- **Reasonable AI and Fairness:** Recent studies have addressed the importance of fairness in iris PAD systems. They identified gender bias in some experimental classifiers, revealing lower error rates for males compared to females. This raises critical concerns about demographic bias and fairness in biometric systems. Future research could expand on this work to explore biases related to other demographic factors, such as eye colour and race.

- **Generalisation to Unknown Attack Types**: Approaches using Generative Adversarial Networks (GANs) have shown promise by creating tight boundaries around bona fide iris samples, enhancing accuracy against novel attack types. Existing research indicates a trade-off between performance on known versus unseen attacks. Future research could explore hybrid approaches that balance robustness against known attacks while maintaining sensitivity to emerging threats, and their ability to generalise to unseen attacks.

5. Summary

In this report, the Iris Presentation Attack Detection (PAD) field is explored. It is a kind of attack that happened with biometric-based using the Iris-eye Authentication where an imposter tries to mislead the model. This report investigates PAD methods as security countermeasures and reviews literature using three different pipelines: traditional computer vision, deep learning and hybrid. It also covers threats posed by PAs, and existing PAD techniques. Finally, the report discusses future challenges and research directions in PAD such as open source code, Reasonable AI specifically fairness and the generalisation to unknown attack types. These areas are critical for advancing the reliability and resilience of biometric security amid evolving cyber threats.

References

[1] What is Authentication, Authorization, and Accounting (AAA) Security?
[2] Brooks, D. J.. Defeating biometric fingerprint systems: An applied testing methodology, 2009
[3] Biometrics vs Passwords: Understanding Authentication Methods
[4] Yin, Y., He, S., Zhang, R., et. al. Deep Learning for Iris Recognition: A Review, 2024
[5] B. Aidan, et. al State Of The Art In Open-Set, Iris Presentation Attack Detection, 2022
[6] Anatomy of the Human Eye
[7] Unlocking the Mystery of Iris Recognition
[8] Iris recognition - Wikipedia
[9] PPT - Iris Recognition PowerPoint Presentation, free download - ID:2809942
[10] M. Aythami, Introduction to Iris Presentation Attack Detection, PAD book Chapter 6,
[11] B. Aidan, Iris Presentation Attack Detection: Where Are We Now?, 2020

[12] J. McGrath, K. W. Bowyer, and A. Czajka. Open source presentation attack detection baseline for iris recognition, 2018.
[13] S. Venkatesh, R. Ramachandra, K. Raja, and C. Busch. A new multi-spectral iris acquisition sensor for biometric verification and presentation attack detection. 2019.
[14] A. Czajka, Z. Fang, and K. Bowyer. Iris presentation attack detection based on photometric stereo features. 2019.
[15] J. Wang and Q. Tian. Contact Lenses Detection Based on the Gaussian Curvature. 2019.
[16] A. Kuehlkamp, A. Pinto, et. al. Ensemble of Multi-View Learning Classifiers for Cross-Domain Iris Presentation Attack Detection. 2019.
[17] D. Yadav, N. Kohli, et. al. Detecting Textured Contact Lens in Uncontrolled Environment using DensePAD, 2019.
[18] S. Hoffman, et. al Convolutional neural networks for iris presentation attack detection, 2018.
[19] C. Chen and A. Ross. Exploring the use of iriscodes for presentation attack detection, 2018.
[20] M. Trokielewicz, et. al. Presentation attack detection for cadaver iris. 2018.
[21] D. Nguyen, et. al. Deep learning-based enhanced presentation attack detection for iris recognition by combining features from local and global regions based on NIR camera sensor. 2018.
[22] S. Yadav, et. al. Relativistic Discriminator: A One-Class Classifier for Generalised Iris Presentation Attack Detection, 2019.
[23] S. Yadav, et. al. Synthesizing Iris Images using RaSGAN with Application in Presentation Attack Detection. 2019.
[24] P. Ferreira, et. al. Adversarial learning for a robust iris presentation attack detection method against unseen attack presentations. 2019.
[25] D. Yadav, et. al. Fusion of handcrafted and deep learning features for large-scale multiple iris presentation attack detection. 2018.
[26] D. Poster, et. al. Deep sparse feature selection and fusion for textured contact lens detection, 2018.
[27] M. Choudhary, et. al. Iris anti spoofing through score-level fusion of handcrafted and data driven features. 2020.