Journal of Autonomous Intelligence (2024) Volume 7 Issue 2
doi: 10.32629/jai.v7i2.1012

ORIGINAL RESEARCH ARTICLE

Iris presentation attack detection: Research trends, challenges, and future directions

Noura S. Al-Rajeh*, Amal A. Al-Shargabi

Department of Information Technology, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia

*** Corresponding author:** Noura S. Al-Rajeh, 411200195@qu.edu.sa

ABSTRACT

Currently, interest in biometrics has increased, and personal identity verification is ubiquitous. Iris recognition techniques have recently attracted considerable attention from researchers and are considered one of the most popular topics as they are used for verification purposes. Because of the increasing use of iris recognition, many potential risks have emerged as a natural result of the increased deployment of these technologies. One of the most serious risks is the so-called presentation attack (PA). A PA is the presentation of a sample to an iris sensor to trick the biometric system into making an incorrect decision. Iris presentation attacks are used to spoof or disguise a person's identity. Many studies have focused on iris presentation attack detection techniques, which are a subset biometric recognition. However, some gaps remain unsolved, and new challenges are rapidly emerging. Despite significant advances in the literature, the problems in iris presentation attack detection have not been adequately addressed and remain open questions. This paper provides a comprehensive overview of iris presentation attack detection from various aspects (e.g., detection techniques, attack types, datasets, and performance measurements). It also attempts to explore the main challenges that may affect presentation attack detection models in terms of important aspects. The challenges that remain to be unresolved are summarised to facilitate problem solving. This review concludes with some directions for future research to help researchers focus on important aspects of the field and try to improve what previous researchers have started. Furthermore, it is likely that this review will be used as a reference for scientists/researchers in the existing science of iris presentation attack detection.

Keywords: presentation attacks; biometric; iris recognition; attack detection; spoofing; detection techniques

ARTICLE INFO

Received: 20 July 2023
Accepted: 1 September 2023
Available online: 25 December 2023

1. Introduction

Account passwords, Personal Identification Number (PINs), and security questions have become important information and personal security tools in the business world for verifying personal identity. Currently, in the age of technology, the need to verify personal identity is almost everywhere (at work, hospitals, government agencies, bank ATMs, airport immigration processes, and entry security gates), and interest in biometrics has increased.

Iris scanning is a comparatively modern technology, which contrasts with the significant investment that law enforcement and immigration authorities in some countries have made in fingerprint recognition technology. However, fingerprints are difficult to recognise after years of physical labour, making irises distinct from them.

The increasing use of biometric recognition systems in many fields and places has created many potential risks that are a natural

consequence of the increased use of these technologies. In the new technological community, the security of these systems against attacks has become a key issue. Presentation attacks are among the most common types of security breaches. A presentation attack occurs when a pattern is presented to an iris sensor to trick the biometric system into making a false judgment. Presentation attack instruments are the biometric properties of materials used for presentation attacks[1].

The reliability of iris recognition systems against attacks is because of their diverse and unique characteristics[2].

Recently, the term "presentation attack" was coined in discussions of the ISO/IEC SC37 standard and is now included in the ISO standards[3]. The term "attacks" is used to refer to the various images of presentation attack. A related but less formal term is "spoofing"[4]. Spoofed images can be printed using an iris, contact lenses, or a prosthetic iris. The term "live images" is generally used to refer to real irises. In some studies, real irises are referred to as "Bonafide" or "genuine irises".

In addition, presentation attacks can imitate someone or disguise the identity of the attacker[5]. Attack detecting has become an important research problem in biometrics because it has a significant influence on system security. This review paper evaluates the existing science of iris presentation attack detection and points out possible security flaws and other things that must be improved to make biometric science a mainline security technology; the main goal is going to be a good reference for researchers planning to improve the science. Such an extensive investigation into the science does not widely exist; therefore, the contribution should likely be considered novel and useful.

The main objectives of the research are as follows:

1) Evaluate and extend existing state-of-the-art research on iris presentation attacks.
2) Introduce a thorough analysis of the different types of iris presentation attack detection techniques.
3) Draw attention to the limitations and pitfalls of current solutions in terms of research frontiers and future directions.

The main contributions of this review are as follows:

1) Conducting a systematic review of 58 articles on iris presentation attack detection.
2) Investigating four aspects aiming to cover all components of attack detection techniques and evaluating them.
3) Defining limitations in the literature and emphasising open issues and future work.

The rest of this review is divided into six sections. The methodology of this review is presented in section 2. Section 3 presents the results of the survey. The limitations and challenges of iris presentation attack detection that still must be solved are presented in section 4. Section 5 provides suggestions for future research. The review is concluded in section 6.

Background

The term biometrics refers to the automatic identification of a person[6]. To identify or authenticate the identity of a person, biometrics evaluates the characteristic features of an individual[7].

Currently, government applications rely on biometric technology in many areas, such as ID cards, electronic passports, border control, and securing online wallets[8]. The extensive use of biometric identification has greatly improved the effectiveness of e-government and e-business in serving citizens[9]. For example, India's Aadhaar program, Amsterdam airport, and United States-Canada border crossings[10] are common examples of these services in commercial and government applications[11].

On the economic side, the global biometric authentication market is expected to grow by approximately $100 billion in 2027, according to recent market research reports. Moreover, the market is expected to grow

at a compound annual growth rate of 14.6% between 2019 and 2027[12]. Many biological characteristics are used for identification, such as palm print, face, iris, fingerprints, speech measurements, signature, DNA, gait, keystroke, and tongue[13]. In the era of e-commerce, researchers are trying to keep up with the rapid developments in biometrics. Several modern models for the recognition of biometric characteristics have been proposed for the face[14–16], finger-vein[14], multiple biometric systems[6], and eyes (irises)[13,17–21]. Using automatic recognition algorithms, biometrics can identify a person seeking access to devices and systems. Therefore, the vulnerability of these systems to presentational attacks is an attractive area of research[15].

Time management and attendance, ATM, surveillance, border control, e-commerce and banking services, PC/network access, citizen identity, and other applications can benefit from biometric recognition.

Iris recognition is an extremely accurate and suitable method for identifying and verifying individuals, and its non-contact use enables better hygiene[9]. In addition, the iris has been shown to have extremely low false match rates in large datasets under limited circumstances for all biometric features tested. The intricate texture pattern of its stroma, the apparent consistency of its distinguishing characteristics, and its broad universality confirm this discovery[11]. To improve the security of recognition systems, iris recognition systems should ensure that only living iris images can generate templates for registration, verification, and identification[16]. The iris is the circular area of the eye surrounding the pupil[17]. Iris images contain unique, stable, and complex patterns that cannot be identical in two individuals, even if they are twins[18]. From a technological perspective, iris recognition can be used in many real-time systems thanks to advances in machine learning and computer vision techniques[19]; however, these systems are vulnerable to challenges, such as presentation attacks by imposters. In a presentation attack, the sample may be an artefact, such as a prosthetic iris, lenses, a printed iris, or even an authentic iris (including a cadaver iris)[20]. The different application domains of iris recognition systems are shown in **Figure 1**.

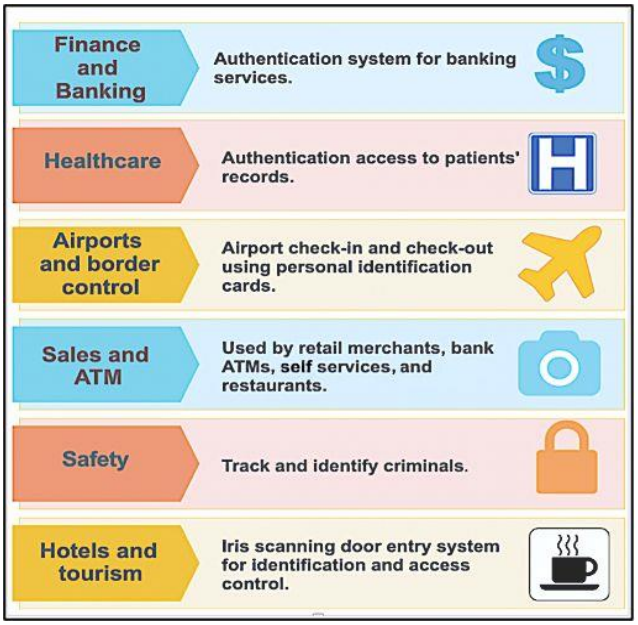

Figure 1. Application domains for iris recognition systems.

Iris identification was initially performed using manually extracted features (i.e., features were created specifically to distinguish individuals based on their iris patterns). This requires a significant amount of time to search for specific features, pre-processing the iris image to extract the features effectively, and developing difficult learning algorithms[21]. The iris is an annulus between the sclera and the pupil, protected by the cornea. In addition, irises differ in shape, size, pattern, and colour; they are characterised as complex structures that include various features such as corona, ridges, freckles, crypts, furrows, and arching ligaments[7]. The

structure of a human iris is shown in **Figure 2**. Examples of artefacts used in iris presentation attacks are shown in **Figure 3**.

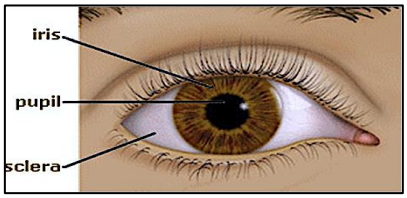

Figure 2. Structure of the iris[13].

(a) **(b)** **(c)**

Figure 3. Examples of artefacts used in iris presentation attacks (PAs): **(a)** printed images; **(b)** plastic eyes; and **(c)** cosmetic contacts[22].

LivDet-Iris (liveness detection competitions) are international competitions for individuals from academia and industry to evaluate and report progress in iris presentation attack detection (PAD). It was launched in 2013[15], and editions took place in 2015, 2017[23], and 2020[15]. The basic task of the competition is to evaluate the efficiency of the algorithms in detecting presentation attacks. Therefore, the LivDet competition series has had a significant influence on iris spoofing and liveness detection. Typically, the contests provide a combined database containing images from multiple sources. **Table 1** shows the LivDet-Iris competition editions summary.

Table 1. Summary of LivDet-Iris competition editions[22].

Year	Presentation attack samples in test data	New training/testing data by organisers	Best performance	
			APCER	BPCER
2013	Printed irises, patterned contact lenses	Yes/yes	5.7%	28.6%
2015	Printed irises, patterned contact lenses	Yes/yes	5.48%	1.68%
2017	Printed irises, patterned contact lenses	Yes/yes	14.71%	3.36%
2020	Printed irises, patterned contact lenses, fake/prosthetic/printed eyes with add-on eyes displayed on Kindle, cadaver irises	No/yes	59.10%	0.46%

2. Methodology

A systematic literature review served as the basis for this study to ensure that iris presentation attack concerns were fully covered in the literature.

2.1. Research questions and motivation

The goal of this study is to analyse, evaluate, and summarise current techniques for detecting iris presentation attacks. Current studies lack an in-depth investigation of the various iris presentation attack detection techniques and their critical aspects. The primary objective of this study is to focus on the current

knowledge of various iris presentation attack detection techniques, different types of attacks, publicly available datasets, and performance metrics used in iris presentation attack detection. This was accomplished by answering four research questions (RQs), which are summarised in **Table 2**.

Table 2. Research questions and motivation.

ID	Research questions	Motivation
RQ1	What iris detection techniques are used to detect presentation attacks?	To explore various techniques for detecting iris presentation attacks.
RQ2	What are the various types of iris presentation attacks?	To provide knowledge about the types of iris presentation attacks to increase the security of iris recognition systems.
RQ3	Which datasets are used in the literature?	To recognise different iris datasets.
RQ4	How are these techniques validated and evaluated?	To discuss the evaluation metrics that are used most frequently for iris presentation attack detection techniques.

2.2. Research strategy

Research method: A database-driven search method was used in this study, and a number of papers were selected and completed with forward and backward snowballing. Scopus and Web of Science digital databases were used to find relevant studies for this study. These studies were published in different journals and related international conferences, as shown in **Table 3**. These databases are sufficient to cover the most recent and authoritative literature on iris recognition issues and the existing challenges.

As shown in **Figure 4**, the literature search from 2015 to 2022 was very extensive. From the figure, it can be seen that various methods to detect iris presentation attacks have gained popularity over the past five years as new attacks emerged, with a significant increase in the number of studies, particularly in 2018.

Figure 5 shows the distribution of sources in the studies based on their types, whether they are from journals or conferences. As depicted in the figure, there are 27 journal papers, whereas there are 31 conference papers.

Table 3. Inclusion and exclusion criteria.

Criteria	Description
Inclusion	1) The study included all related publications written in English.
	2) Studies that used computer vision, machine learning, and deep learning to detect iris presentation attacks.
	3) The publication was more than three pages long and was published between 2015 and 2022.
Exclusion	1) The publication was not written in English.
	2) Studies that used techniques other than computer vision, machine learning, and deep learning (e.g., sensors or device-based techniques) to detect iris presentation attacks.
	3) Short papers less than four pages long and published before 2015.

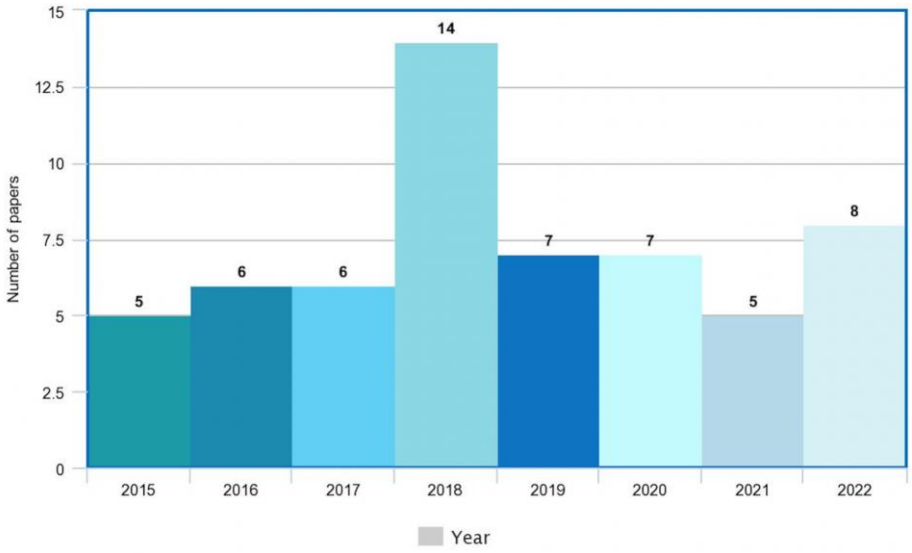

Figure 4. Number of papers selected over the years.

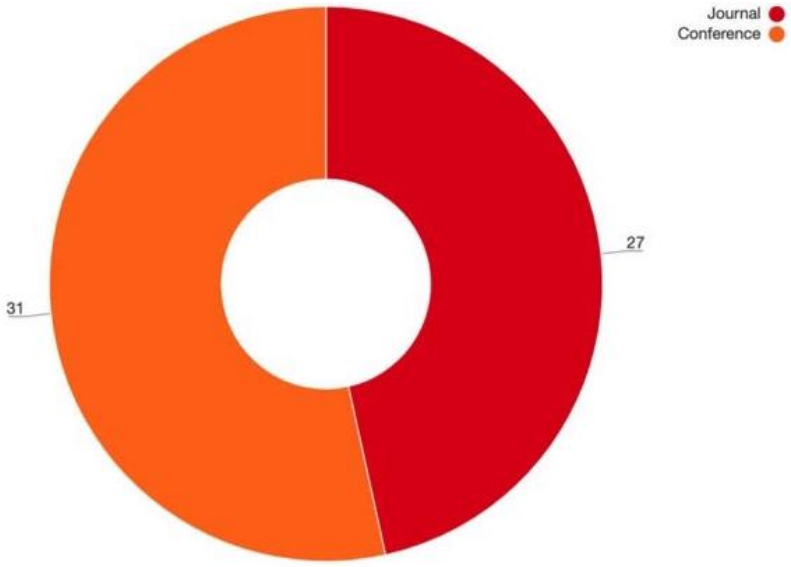

Figure 5. Studies source distribution.

Research string: In this study, we searched for studies using a variety of search keywords that were created through a reduplication process to increase the number of relevant studies and obtain precise search results (optimal results). Thus, the most frequently used word combinations included “iris security”, “presentation attack detection”, “iris presentation attacks”, “biometrics security”, and “iris spoofing detection”. The studies were categorised based on these keywords to map the relevant studies. This process involves extracting keywords and concepts from the study abstracts that reflect the contributions of the studies. Only titles, abstracts, and keywords matched the search string. Data sources were searched using a filter based on publication year, and only papers published on or after 1 January 2015 to 31 October 2022 were included as the use of the iris as a biometric has gained popularity in different security fields.

2.3. Inclusion and exclusion criteria

At this stage, the inclusion and exclusion criteria for this study were established. For inclusion, papers that provided the main contribution to sensors for presentation attack detection, such as specific lenses or types of illumination, were not considered. Studies published before 2015 and those with less than four pages were excluded. The inclusion and exclusion criteria are listed in **Table 3**.

A total of 2612 publications were identified during the search. After removing duplicate publications, the total number decreased to 1686. A total of 1599 publications were removed because they did not address any type of iris presentation attack. Of the remaining publications, 58 were deemed as relevant.

3. Results and analysis

This section summarises the results of the data synthesis. In each section, the analytical results are presented.

3.1. Iris presentation attack detection techniques

This section presents the classification of the detection techniques for the studies under investigation. **Figure 6** provides a summary of the proposed taxonomy of iris presentation attack detection techniques.

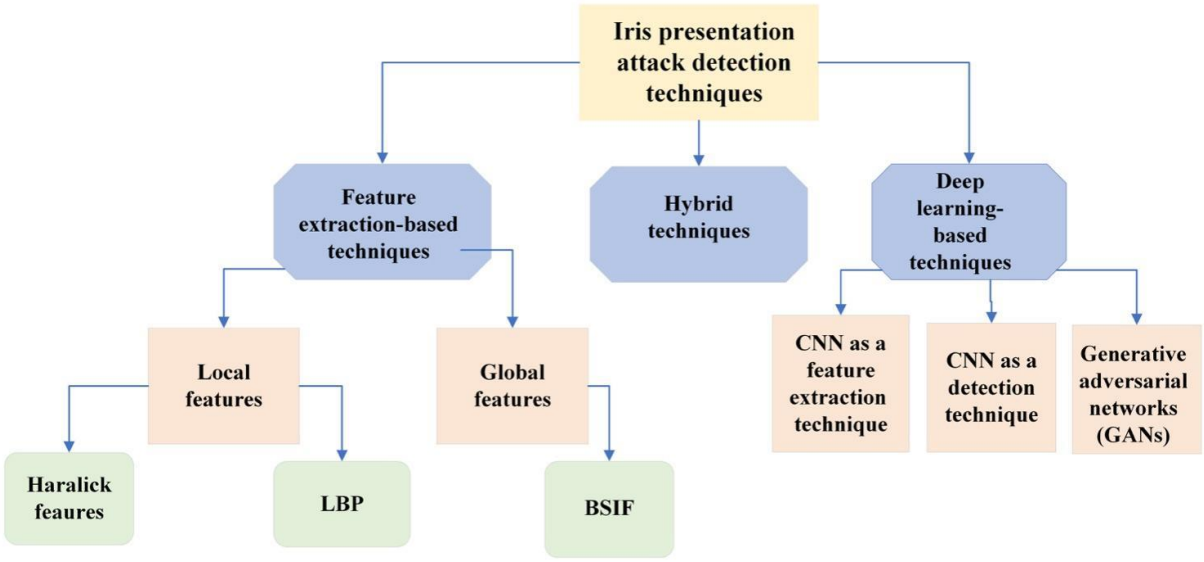

Figure 6. Summary of iris presentation attack detection techniques.

3.1.1. Feature extraction-based techniques

With seminal work on iris feature extraction and matching, Daugman et al.[24] paved the way for commercial systems and motivated researchers[25]. As the field of computer vision is likely to improve rapidly, scientists and researchers have used conventional computer vision-based methods and feature extraction to detect iris presentation attacks[26]. In the study by Subban et al.[7] improved an iris identification algorithm using the Haralick feature extraction method, which extracts the main features of the iris. They use the fuzzy-guided PSO algorithm of the extracted features to perform optimal feature selection. Then, a relevance vector machine (RVM) classifier is used to determine the proper class for each iris characteristic. Finally, the database is queried for samples and provides a confirmation message for the image that matches the iris characteristics. Sinha et al.[13] proposed a wavelet parcel change-based iris identification system based on a light support vector machine. They used natural eye flash and motion detection to determine the vitality of real iris images before comparing them with recorded templates. In addition, Raghavendra and Busch[27] presented a presentation attack detection algorithm based on multi-scale binarised statistical image features (M-BSIF) and linear support vector machines (SVM). To detect presentation attacks, this method integrates micro texture variations extracted from multiple scales at both the feature and decision levels. As shown in **Figure 7**, the proposed system is composed of four components: iris segmentation and normalisation, periocular region extraction, the proposed PAD algorithm, and the baseline iris recognition system.

Saranya et al.[28] used image quality assessment as a statistical approach in image processing to determine the authenticity of a biometric sample. To minimise complexity, they selected 26 image quality features. Furthermore, a study by McGrath et al.[29] provided an open-source presentation attack detection (PAD) approach to separate legitimate iris images (with clear contact lenses) from iris photos with textured contact lenses. Furthermore, this approach does not require segmentation of the iris picture (refer to **Figure 8**). Moreover, binary statistical image features (BSIF) are used to extract features related to presentation attacks and classify them using support vector machine classifiers.

Wang and Tian[30] developed a depth-based technique for contact lens identification. The sum of squared deviations was used to extract features; then, they used the Gaussian curvature of the cornea as a stable physical feature. Fang et al.[31] compared four open-source methods and then fused them with the two best methods. Their solution addresses the challenge of spoof detection by combining two-dimensional (textural characteristics) and three-dimensional (photometric stereo features) features of the iris. OSPAD-2D extracts binary statistical image features (BSIF) from iris images, whereas OSPAD-3D classifies them based on the difference between the contact lens-generated shadows on the iris surface and photometric stereo normal maps. Also, Raja et al.[32] developed multipatch deep features based on deep sparse filters to create robust iris identification features for maximum likelihood classification and express them in a collaborative subspace. Kaur[33] used the characteristic of constructing a constant feature set composed of Dual-Hahn, Tchebichef, and Krawtchouk moments to describe iris textural patterns.

The work of Shahriar et al.[34] presented a novel authentication system that prevents presentation attacks by generating both iris and QR codes using HaarCascade and local binary patterns (LBP) classifiers. It uses the iris code as the user ID, whereas the QR code serves as the password. Moreover, Kaur et al.[35] detected iris spoofing attacks using a rotation-invariant orthogonal feature set based on continuous moments: Zernike moments and polar harmonic transform.

Malhotra and Gupta[36] proposed a counterattack strategy based on statistical factors in the presence of variable light sources. A self-quotient image was used to compensate for changing illumination conditions. In addition, by comparing the feature score of the training images with those of the test image, a binary SVM classifier was used to determine whether the tested image was genuine or fake. Raja et al.[37] proposed a method for detecting video replay attacks and artefact iris images by extracting characteristics from the frequency response maps of the images using Laplacian pyramid decomposition and an SVM classifier, as well as majority voting.

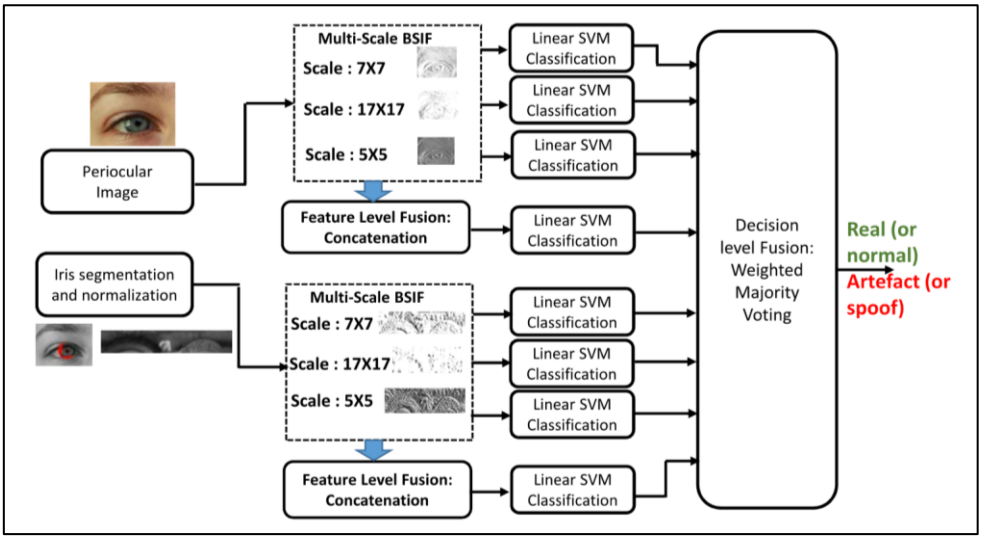

Figure 7. Proposed iris presentation attack detection scheme[27].

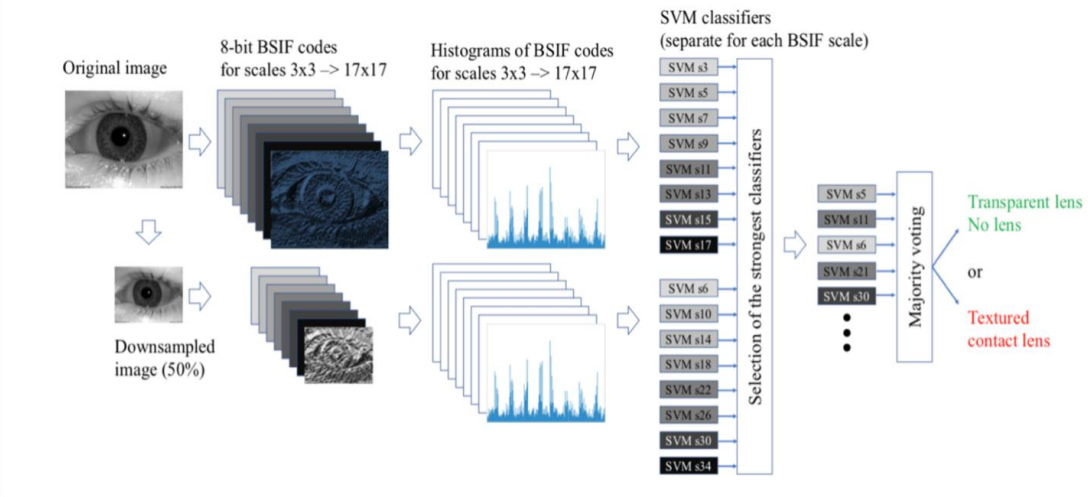

Figure 8. Proposed open-source solution for iris PAD[29].

The work of Fathy et al.[38] uses discriminative statistical characteristics to distinguish genuine and fake iris pictures. Moreover, in the work of Kohli et al.[39], a framework named DESIST was suggested for detecting faked iris pictures. It is a framework for calculating multi-order dense Zernike moments and representing textural changes in a faked iris picture using a local binary pattern with variance. In addition, the work of Gragnaniello et al.[40] evaluated different image descriptors based on local characteristics for identifying the authenticity of fingerprint, iris, and face images. Both simple descriptors with separate feature quantification and more complicated descriptors with combined quantisation of extensive features were examined. In addition, Agarwal et al.[41] presented a local binary hexagonal extrema pattern as a feature descriptor for presentation attack detection. The suggested description uses the link between the central pixel and its neighbouring hexagonal pixel. Das et al.[42] proposed a multimodal ocular biometric detection technique based on image quality features in the visible-light range. The framework proposes a method for identifying inter-class/class-level liveness by combining domain transformations, contrast measurements, and geometric ratios. Another technique was proposed in the work of Czajka et al.[43] based on three-dimensional features estimated by the photometric stereo of an observed iris region. Photometric stereo allows the estimation of normal surface vectors in the unoccluded iris area. The score for presentation attack detection was determined based on the variability of the normal vectors.

i. Common features used in feature extraction-based techniques

Table 4 displays the most common feature extraction techniques and the studies that have implemented them. The following provides an explanation of these features.

Table 4. Feature extraction techniques.

Feature	Study
Haralick features	[7], [44]
Binary statistical image features (BSIFs)	[3], [33], [35], [31]

- Haralick features

Haralick features are commonly used as statistical feature descriptors for textual information encoding in photographs. They have been successfully used in a variety of applications, such as texture classification; medical image classification; and facial, fingerprinting, and iris presentation attack detection. Haralick features are generated using grey-level co-occurrence matrices, which are defined as the frequency distribution of co-occurring pixel intensity values in an image (I) at a given offset (Δp, Δq) at a given position (x, y)[44].

- Binary statistical image features (BSIFs)

Binary statistical image features are global features that describe an entire iris image. Global feature extraction is fast and simple, because it works with a complete image rather than individual image patches. Kannala and Rahtu[45] proposed binary statistical image features by convolving an image with a linear filter and then binarising the filter outputs to create a binary code string for each pixel. The number of filters used determines the length of the binary code[46]. The histogram of pixel code values allows the quantitative analysis of texture qualities within the image subregions. Consequently, the use of the BSIF is justified specifically for detecting visible iris presentation attacks and seems to be a suitable option because it successfully collects microtextured information that can be used to identify the artefact[27].

- Local binary pattern (LBP) features

As a simple feature extraction technique, a local binary pattern (LBP) tags pixels in an iris image by determining the adjacent pixels and accepting the result as a binary code. Many studies have used these characteristics to distinguish between genuine and attacked images[47].

ii. Classifiers

In machine learning, classifiers are given features that are extracted from the images. Recognition systems use various machine-learning classifiers to categorise input images, and these classifiers have been trained for iris recognition. Machine learning classifiers such as random forest (RF), support vector machine (SVM), and k-nearest neighbour (k-NN) are commonly used. SVM is a classification algorithm that outlines linearly separable data into a high-dimensional hyperspace fragmented by a hyperplane[36].

According to Czajka et al.[48], SVM-based classification is a good way to solve sensor interoperability problems and has shown high generalisation ability. At the same time, the SVM classifier has achieved the best average classification accuracy with the radial basis function kernel[49]. In addition, k-NN performs best with moment-based features for discriminating between classes. It is also suitable for large databases[33]. Compared to conventional SVM or neural networks, a RVM performs fast classification in real time and reduces computational complexity by generating minimal relevance vectors as per the study of Subban et al.[7]. Moreover, and as in the study of Saranya et al.[34], the Haar cascade classifier is commonly used for iris recognition because it achieves high accuracy and therefore performs better than the LBP classifier in the experiments. **Table 5** shows the classifiers that frequently used in literature

Table 5. Classifiers frequently used in literature.

Classifier	Study
Support vector machines (SVMs)	[13, 27, 31], [48], [37], [36], [37], [40], [29], [50], [51], [52], [41], [49].
Random forest (RF)	[3], [31].
K-nearest neighbour (k-NN)	[33], [35].
Relevance vector machine (RVM)	[7].
Haar cascade	[34].
Local binary pattern (LBP)	[34].

3.1.2. Deep learning-based techniques

Because deep learning has gained prominence, much of the research on iris presentation attack detection research has shifted to deep learning approaches, which seem ideal for improving the use of the iris recognition system. Deep learning can take several forms. The techniques used vary from using a convolutional neural network (CNN) as a feature extractor to CNN as an iris image recognition technique.

i. CNN as a feature extraction technique

Wang et al.[9] investigated a self-learned feature derived from CNNs with SoftMax cross-entropy loss for cross-spectral iris recognition (**Figure 9**). Moreover, iris recognition was implemented using supervised discrete hashing. In addition to CNN, experimental results have been obtained with a variety of other deep learning architectures, such as Siamese networks, triplet networks, VGG, and deep residual networks (ResNet). In addition, Menon et al.[21] used a single CNN on both iris images to extract two sets of features (one for each particular length) and computed their similarity. For recognition, the technique used the (ResNet18) CNN.

The work of Nguyen et al.[50] presented a novel presentation attack detection approach for iris identification based on a near-infrared (NIR) light camera sensor. CNNs and support vector machines were used to combine characteristics collected from both local and global iris regions, and the recognition results for each type of image feature were merged using two fusion methods to improve the recognition capacity of each type of image feature. Moreover, Choudhary et al.[51] developed a unique framework for locating the region of interest (RoI) within the iris by using the You Only Look Once (YOLO) technique and performing selective image enhancement to improve important structural elements.

The work of Menotti et al.[53] investigated a deep representation-based method termed SpoofNet: two deep learning approaches for many features, including the iris. The first approach involves learning appropriate convolutional network topologies for each feature, whereas the second approach uses backpropagation to learn the weights of the network. Moreover, Chen and Ross[54] investigated whether IrisCodes, which are commonly used for iris identification, can be used to detect presentation attacks. IrisCodes are binary phasor characteristics obtained from the annular iris area after it is converted into a rectangular object. In addition, Furthermore, Sharma and Ross[55] presented a D-NetPAD iris presentation attack detector that is built on the DenseNet convolutional neural network architecture that can recognise attack photos from aesthetic representations captured by a variety of mobile iris sensors. Each layer in the DenseNet design is connected to every other layer in a feed-forward manner. The characteristics of the various layers are correlated with their respective resolutions.

In the work of Choudhary et al.[56], a densely connected contact lens detection network (DCLNet) was developed to detect contact lenses in iris images acquired by different types of sensors (heterogeneous). The network is a deep convolutional network with dense connections between the layers and the addition of an SVM. Feature analysis is performed by displaying iris features learned through arbitrary layers.

In the study by Dhar et al.[57], trained a single deep multi-task learning network for eye authentication and PAD without any pre-processing. The authors believe that their technique, which combines knowledge distillation with the specificity of multitask learning, is effective. In addition, Fang et al.[58] proposed to fuse data from multiple deep neural network layers to provide recognition judgments for iris presentation attacks. The features were extracted from multiple convolutional layers of pre-trained and freshly generated neural networks. The data extracted from the final few convolutional layers are then combined at two levels: features and scores.

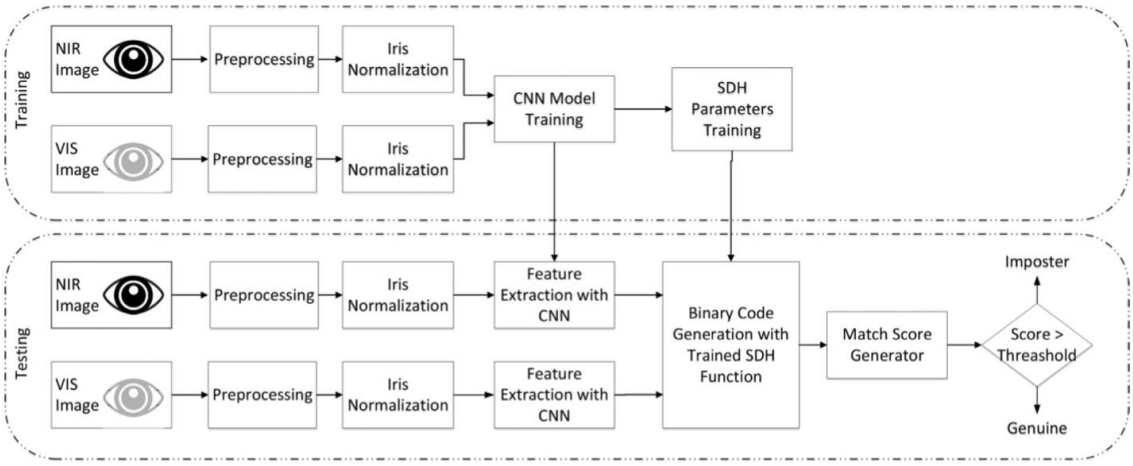

Figure 9. Proposed framework for cross-spectral iris recognition[9].

Furthermore, Arora and Bhatia[59] found that classification error increases significantly when a system deals with more than one attack. In their framework, they used CNNs to detect spoofing attempts in an iris recognition system. Moreover, in the last layer, classification is performed using the SoftMax activation function to determine whether the iris is genuine or spoofed and to predict the nature of the attack. He et al.[60] proposed a multi-patch convolutional neural network (MCNN). The output of each patch is sent to the decision layer, which makes the final decision. In categorising of genuine and fake iris images, a CNN was used by the system to automatically learn the most effective texture characteristics.

ii. CNN as a detection technique

The work of Raghavendra et al.[2] proposed a different approach for contact lens identification based on deep convolutional neural networks (D-CNN). **Figure 10** shows a block diagram of the contact lens classification scheme using D-CNN of this study. As shown in the figure, the described CNN architecture (ContlensNet) was developed and tuned to solve a three-class detection challenge (irises with textured contact lenses, soft contact lenses, and no contact lenses). The Majority voting was used to classify iris patches associated with the iris sample. In addition, Hoffman et al.[22] fused the outputs of three PA detectors based on CNNs, each of which analysed a different part of the input image. The first CNN dealt only with the iris, the second with the entire ocular region, and the third with a subset of the ocular patches. Furthermore, Trokielewicz et al.[61] developed a deep learning-based system for iris PAD using iris photos obtained from dead people. The methodology was based on the VGG-16 architecture. In addition, this technique evaluates the characteristics and locations that the network considers the most important for PAD categorisation by displaying class-activation maps.

The work of Fang et al.[62] established a system for identifying iris presentation attacks using microstrip analysis, particularly attacks involving contact lenses. Moreover, this approach succeeded in generalising the experiments in cross-attack (unknown attack) detection. In addition, a new technique proposed by Boyd et al.[63] for iris presentation attack detection using a variational autoencoder consists of a ResNet50 encoder and decoder. The variational autoencoder was trained to reliably reconstruct real irises. The authors used the latent vector to train a multilayer perceptron for the binary classification of real and attacked samples.

The study by Fang et al.[64] proposed a new attention-based deep pixel-wise binary supervision (A-PBS) technique for iris presentation attack detection. By using an attention mechanism, the goal of the A-PBS solution is to capture fine-grained pixel/patch-level cues and use the regions that contribute the most to an appropriate PAD decision. Moreover, Yadav et al.[65] presented DensePAD, a new approach for iris

presentation attack detection that leverages a DenseNet-based convolutional neural network architecture to detect textured contact lenses in uncontrolled environments and cross-sensor datasets.

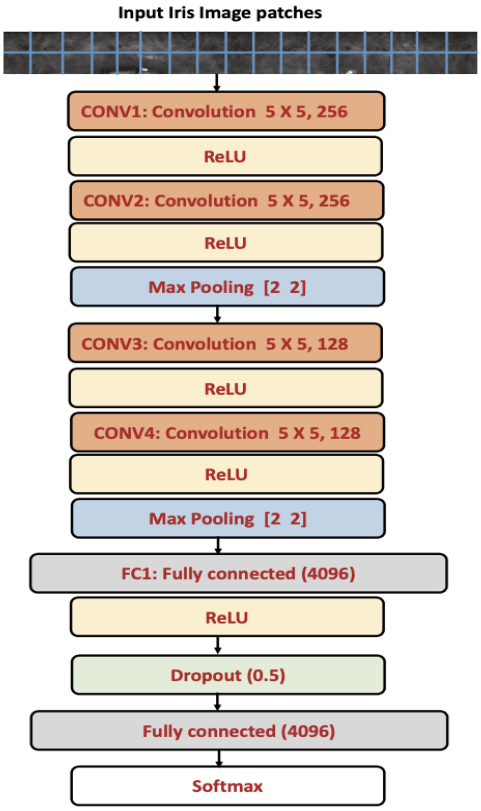

Figure 10. Block diagram of the contact lens classification scheme using D-CNN[2].

The approach of Hoffman et al.[66] use iris patches instead of the entire iris or ocular image as the input to allow for data augmentation during the training phase. The CNN is then trained on patches emanating from all regions of the cropped iris image. Consequently, the CNN focuses on PA artefacts rather than location artefacts. **Figure 11** shows the CNN architecture used in this work.

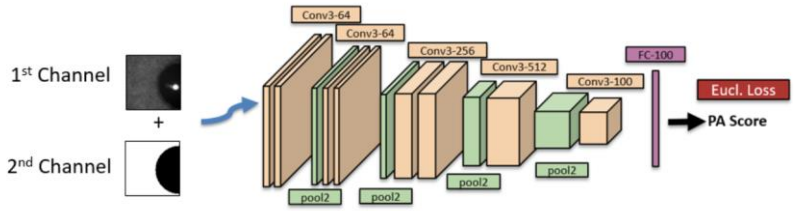

Figure 11. CNN architecture used in the study of Hoffman et al.[66].

To prevent spoofing attacks, Chatterjee and K.[67] used deep CNNs, called modified VGGNet, based on VGGNet and AlexNet. In addition, the sigmoid function was used to accelerate the 2D binary classification and validation. By adding appropriate regularisation terms to the loss function, Gragnaniello et al.[68] proposed a convolutional neural network tailored for spoofing detection. In this study, they presented the MVANet architecture, a deep learning-based design that uses numerous representation layers. In the proposed approach, multiple FC layers were combined in parallel with the final convolutional layer to learn the different feature representations of an image. Furthermore, Parzianello and Czajka[69] proposed an iris recognition technique for textured contact lenses. To rudder the network with real iris features, a convolutional neural network-based segmenter and a Siamese network-based feature extraction model were used. In addition, Chen and Ross[70]

presented a method for multi-task convolutional neural network learning (PAD). The proposed MT-PAD performs iris localisation and presentation attack detection simultaneously. A single neural network was used to predict the bounding box that defines the geographical position of the iris and to produce a PA score indicating the probability that the observed iris is a presentation attack.

In the study by Raju et al.[71], a deep learning model was used to analyse captured iris movement signals. The authors focused on print attacks and investigated the feasibility of distinguishing between a genuine iris from a fake iris using features based on eye movement signals. To improve the effectiveness of iris presentation attack detection systems, the work of Fang et al.[72] used several data augmentation methods to generate variability, such as shift, rotation, and brightness. The results showed that the augmentation methods improved iris PAD performance.

Finally, Pala and Bhanu[73] proposed a presentation attack detection method based on triplet convolutional networks with two genuine and two fake iris patches as input. The goal was to increase the number of training examples and to create a representation that can distinguish between genuine and fake iris patches.

iii. Generative adversarial networks (GANs)

Numerous current approaches to detecting iris presentation attacks have used generative adversarial networks (GANs). Yadav et al.[1] trained a relativistic average standard generative adversarial network (RaSGAN) with an authentic iris to create a high-quality synthetic iris **(Figure 12)**. They then used a relativistic discriminator (RD) extracted from the resulting RaSGAN to distinguish genuine irises from their synthetic counterparts. Because the discriminator does not require data from PA samples in the training phase, it functions as a one-class classifier. To evaluate the performance, the proposed RD-PAD was evaluated using a small number of attack samples and PAs that were not used during training.

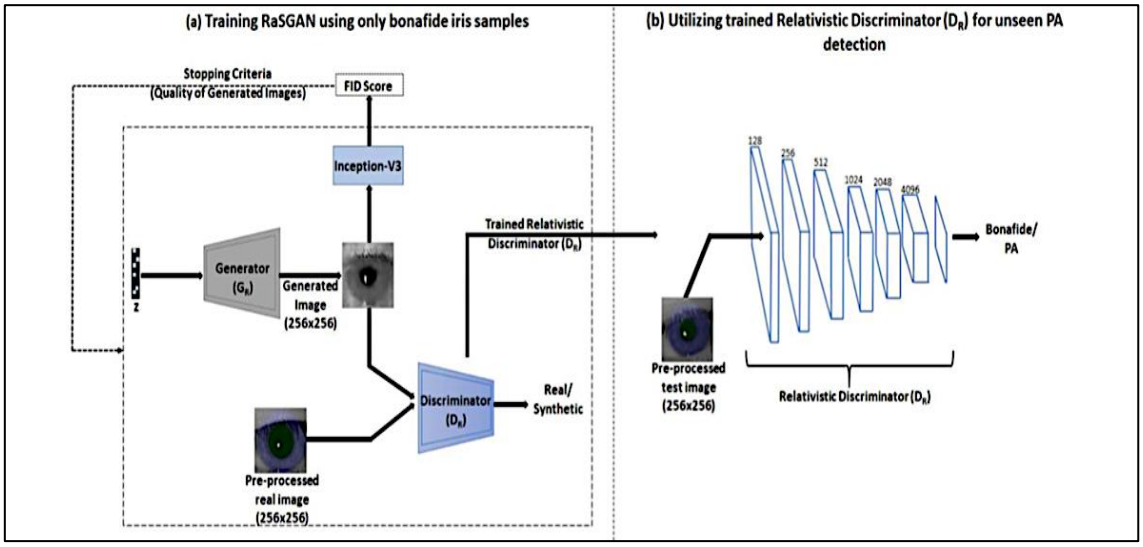

Figure 12. Proposed presentation attack detector[1].

3.1.3. Hybrid techniques

Some studies have combined both conventional and deep learning to detect iris presentation attacks; these combinations are called hybrid techniques. The work of Kuehlkamp et al.[3] developed a novel method for detecting iris presentation attacks by combining CNNs with altered input spaces through binarised statistical picture characteristics (BSIFs). In addition, they proposed an approach for selecting the task's best (and most discriminative) predictors. **Figure 13** shows an overview of the proposed method in the study of Kuehlkamp et al.[3].

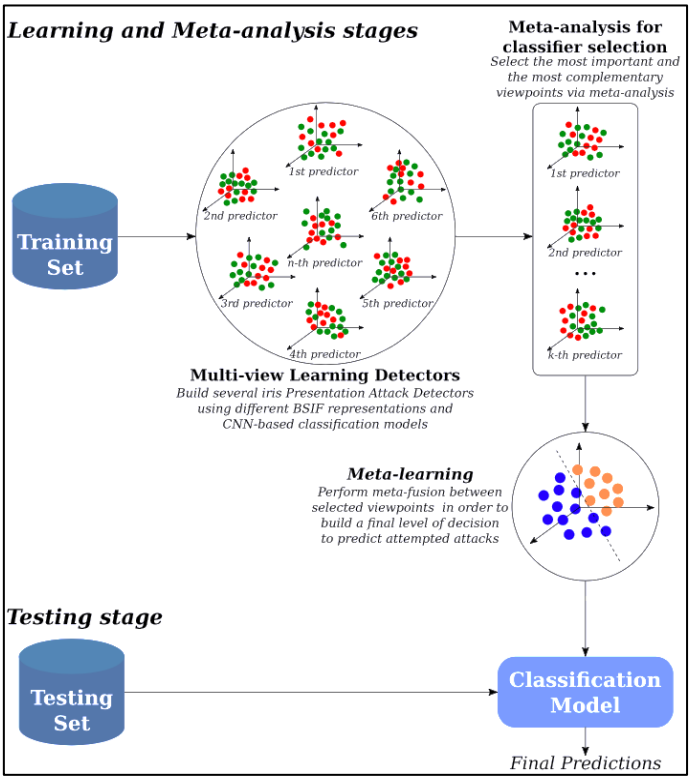

Figure 13. Overview of the proposed method in the study of Kuehlkamp et al.[3].

In addition, Yadav et al.[44] presented an approach for detecting iris presentation attacks that incorporates both hand-crafted and deep learning-based features. To encode the texture changes between genuine and fake iris samples, the proposed technique combines local and global Haralick texture features with VGG features in the multilevel redundant discrete wavelet transform domain. Furthermore, the work of Czajka et al [48] looked at spoofing methods where the relative position of the eye and sensor (either by rotating/flipping the image or rotating the sensor) were altered. Using the same data, two techniques were compared: feature engineering, which uses hand-crafted and classified features, and feature learning, which uses data-driven and classified features learned and classified by a CNN.

The work of Choudhary et al.[49] suggested a fusion-based strategy for discriminating between live iris and contact lens pictures, which incorporates both hand-made and data-driven characteristics. To develop a combined feature set, the DCCNet features were blended with handmade analogues. In addition, the ideal features were found by top-k feature selection and fused via score-level fusion. Furthermore, Nguyen et al.[52] proposed an approach for PAD using NIR camera images. Their approach combined hand-crafted image characteristics with deep features.

Moreover, the approach of Poster et al.[74] extends the existing hand-crafted image features and neural network designs by selecting and effectively integrating the most relevant collection of features. Moreover, , the A-PBS method was proposed by Fang et al.[75], in which pixel/patch level monitoring first detects fine-grained pixel/patch-level signals. Then, the attention mechanism directs the network to the areas that are the most important in the accurate selection of PAD.

Furthermore, A novel few-shot one-class domain adaptation technique based on only some real samples was proposed in the study of Li et al.[76]. The frequency-based attention module (FAM) and frequency mixing module (FMM) integrate frequency-related information using this technique. Simultaneously, the FMM monitors the blending of the low-frequency components of the source images with the high-frequency components of the real target samples. Finally, in the study by Luo et al.[77], using light-field imaging and deep

learning, a framework was proposed to detect the differences in 3D geometric structure and 2D spatial texture captured by LF cameras between genuine and fake irises. The framework investigates the standard deep neural network features of planar-oriented and sequence-oriented deep neural networks (DNNs).

3.1.4. Issues regarding iris presentation attack detection techniques

This section summarises the performance comparison of the iris presentation attack detection methods in this study. Conventional computer vision-based methods achieve acceptable performance, but they require a disproportionate amount of effort to identify valuable features, effectively pre-process the iris image to extract the features, and design a fine-tuned parameterisation (learning algorithm)[21]. In the literature, the characteristics based on local texture analysis are often used to determine iris liveness. In addition, when hand-crafted features are used, the researcher has greater control over the information used by the method to make decisions[78]. Unfortunately, features do not seem to be a good solution when it comes to generalisation and unknown attacks[79,80].

The proposed techniques can include both full end-to-end deep learning classification as well as partial end-to-end deep learning classification. According to the literature, deep-learning-based iris identification models can be used as feature extractors for iris images. The literature has shown that the continuous augmenting fusion with classifiers does not necessarily increase classification performance.

The CNN's end-to-end solution saves a lot of time and effort during the feature-extraction step. The data available for training may not be sufficient to take full advantage of the CNN's learning capabilities, but there is much room for improvement, and increasing the amount of training data will undoubtedly improve the network's performance. The difficulties associated with deep learning are generalisable. Deep learning works well, and both the training and test data come from the same source. However, PAD has the distinction that we cannot predict the nature of future attacks; therefore, strategies must be robust. Existing PA detection systems lack generalisation capabilities and often fail in cross-dataset situations where training and testing occur on completely different datasets.

GANs have been used in modern approaches to detect iris presentation attacks. Researchers have attempted to train the same discriminator to reliably determine whether a manufactured sample is genuine. These methods are still emerging, require more work, and do not appear to be reliable in the real world. Although the reported results indicated that GANs improved the performance of the models in unknown attacks, the performance decreased in known attacks. In addition, hybrid methods have generally performed well but are not practical for commercial use or in lightweight devices because they consume time and resources.

There is little literature on the generalisability of iris PAD algorithms across PAs, sensors, and datasets not included in the training data. For real-world applications, an iris PAD method should be able to work on across datasets and cross-attacks, as it is difficult to predict in advance which attacks an adversary will launch[22]. In addition, most of these methods focus on a single form of iris presentation attack, such as lenses or printed images, while overlooking other state-of-the-art types. Finally, studies agree that it is important to develop deep learning approaches, as this is one of the most effective and promising methods. **Table 6** illustrates the classification of iris presentation attack detection methods, their strengths, and weaknesses.

Table 6. Classification of iris presentation attack detection methods, their strengths, and weaknesses.

Type	Description	Strength	Weakness	Primary studies
Feature extractors	Traditional hand-crafted feature extraction and classification.	• Ease and simplicity. • There are no training parameters, or a large amount of training data required. • Good performance in known attacks.	• If a sufficient iris region is not visible, or the image is non-ideal and low quality, the test may fail. • It takes a long time to extract useful features. • To extract features efficiently, the iris image must be pre-processed.	[7], [13], [24]–[43]
CNN as a feature extraction technique	Ensemble of neural networks used to extract image features that allow the network to make more accurate predictions.	• Good performance in known attacks. • Accurate in image recognition tasks.	• Poor in generalisation capability. • Large amount of training data is required. • High computational cost.	[9], [21], [53]–[60]
CNN as a detection technique	Ensemble of neural networks that are used to perform classification on an iris region.	• Accurate in image recognition tasks. • Good performance in known attacks.	• Slow training on CPU. • A large amount of data is required for training. • Poor in generalisation capability. •Time consuming.	[2], [22], [61]–[73]
GAN-based detection methods	Using a generative adversarial network (GAN) to detect iris presentation attacks.	• Good performance in unknown attacks.	• Poor performance in known attacks.	[1]
Hybrid methods	Using computer vision methods side by side with deep learning techniques.	• More accurate results. • Good performance in known attacks.	• Time consuming. • Poor in generalisation capability.	[3], [44], [48], [49] [52] [74]–[77]

3.2. Iris presentation attack types

In general, presentation attacks on biometric systems are relatively simple, requiring little technical knowledge regarding of the system's structure or the execution of an algorithm. Presentation attacks on iris recognition systems can be conducted in a variety of ways. **Figure 14** shows the different types of presentation attacks discussed in the literature whereas **Figure 15** depicts the most attacks used in literature experiments.

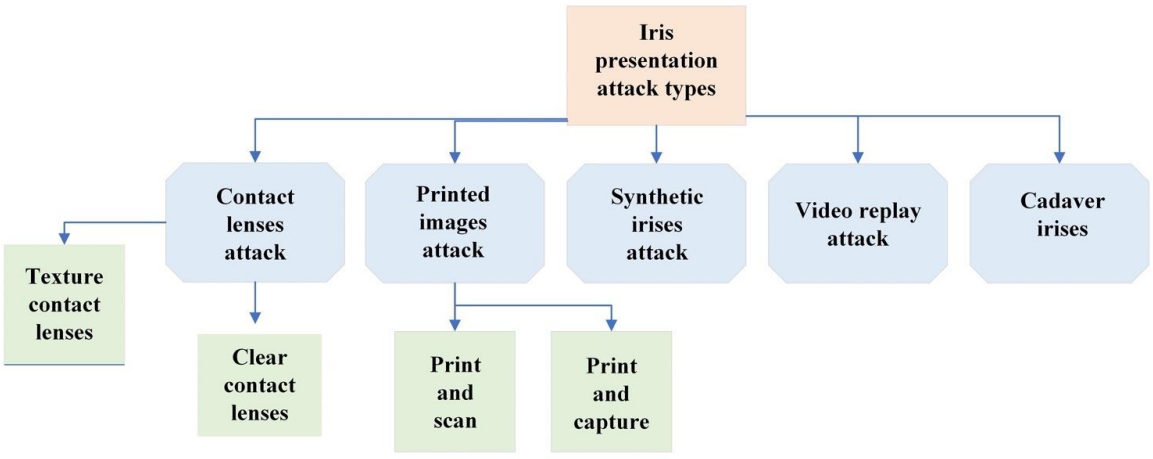

Figure 14. Different types of iris presentation attacks.

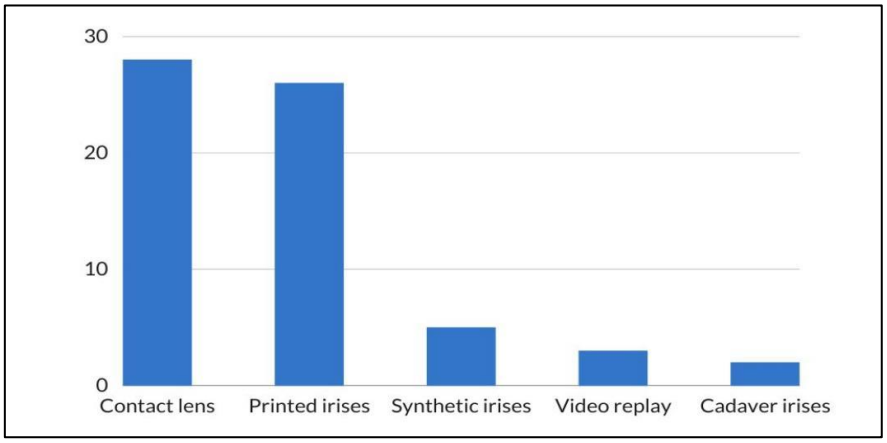

Figure 15. The most attacks used in literature experiments.

3.2.1. Contact lens attacks

Recently, contact lenses have gained popularity worldwide as a means of vision correction and aesthetic beautification, whereas textured lenses are used in cosmetics[81]. In case of recognition, these lenses contain the natural texture of the iris, which drastically reduces the effectiveness of iris recognition systems. Contact lenses are classified in the literature as textured contact lenses and clear contact lenses. Textured contact lenses are commonly used in the literature to describe contact lenses, while clear contact lenses are neither coloured nor have a discernible texture and are therefore considered to be true irises Several feature extraction techniques have been used to identify contact lens attacks. In a study by Fang et al.[31], only two images were used to detect contact lenses with unknown texture contact lenses using 2D and 3D iris information. Although the training and test sets contained identical samples from the same manufacturers, the PAD process is complicated by the fact that the texture qualities of the same brand of textured contacts manufactured today may differ from those manufactured seven years ago. To obtain accurate results, iris PAD techniques must be regularly updated to include training samples of the latest contact lenses, even if they are manufactured by the same manufacturer.

3.2.2. Printed image attacks

This is the simplest form of a presentation attack. An attacker offers a printed image of a real iris to a biometric sensor or system. A high-quality printer and paper, as well as the quality of the printed iris, may significantly deceive iris recognition systems. There are two types of attacks: those in which the iris is printed on a high-quality printer and then scanned (print and scan attacks) and those in which the image is captured with a scanner (print and capture attacks). According to research, attacks that combine print and scan and print and capture have the potential to reduce iris recognition accuracy by less than 10% at 0.01 percent FAR[82]. The success of this type of attack relies on the ability to produce high-quality photographic prints[27]. Researchers have used a variety of feature extraction approaches in the literature to identify print attacks. Manual feature extraction is the most commonly used approach.

3.2.3. Synthetic iris attacks

This technology creates an iris pattern that resembles a real iris image and matches that of the actual user. To create synthetic iris images, iris textures were automatically generated from unique iris images. Synthetic samples pose a challenge for biometric systems because it can be difficult to distinguish them from genuine images. Although “synthetic irises” seem to be a serious problem, it is difficult to represent this type of attack as a biometric sensor. An attacker must print an image or perform a replay attack to display synthetic irises to the biometric sensors. Current synthetic iris generation technologies produce results that are physically similar to the original iris patterns. The number of studies on these attacks is still limited[59].

In the work of Kohli et al.[83], a domain-specific generative adversarial network (iDCGAN) was introduced for generating synthetic iris images. The analysis step uses quality score distributions for both actual and synthetic iris images. The authors used a commercial system to demonstrate the effects of synthetically generated iris images as a presentation attack on iris recognition. In addition, the synthetic iris images of the proposed iDCGAN framework were evaluated using iris quality metrics and a synthetic iris as a presentation attack. In the work of Yadav et al.[17] a novel approach for synthesising synthetic irises based on a RaSGAN was developed. The proposed approach synthesises high-quality iris images using the generative power of a RaSGAN. The images were tested for their useability as genuine images and for their attack potential using PAD algorithms, such as DESIST, BSIF + SVM, Iris-TLPAD, and pre-trained VGG-16. Yadav and Ross [84] presented a GAN architecture that uses an image-to-image translation mechanism called the cyclic image translation generative adversarial network (CIT GAN) to synthesise images for different iris presentation attack domains. The performance of the synthetic samples was tested using with various iris presentation attack detection approaches, including VGG-16, BSIF, DESIST, D-NetPAD, and AlexNet. The Fréchet inception distance score was used to evaluate the quality of the generated samples.

3.2.4. Video replay attacks

In a video-replay attack, the imposter displays a video of an authorised identity's iris in a biometric sensor. This type of system is designed to detect whether a person is alive by examining the motion data. Because a video contains sufficient motion information, a biometric authentication system can be easily bypassed. Because of the scarcity of iris video datasets, video attacks have been used less frequently in the literature to detect iris presentation attacks than for other types of attacks. Some studies have focused on video attacks[1]. To date, there is no evidence in the literature that video-spoofing attacks can be identified using deep learning techniques[82].

3.2.5. Cadaver irises

In this variant, an impostor places the eye of a deceased person in front of a biometric scanner. Up to one month after death, it is possible to obtain a post-mortem image of the iris that can be used to disguise the identity of the deceased. Some researchers have looked at cadaver attacks such as the studies of Fang et al.[61] and Fang et al.[63].

3.2.6. Issues regarding iris presentation attack types

Currently, available solutions are designed to detect specific forms of iris presentation attacks. However, iris recognition systems should be able to handle and identify multiple iris presentation attacks under real-world conditions. Print attacks are successful only when high-quality photographic prints are produced. As contact lens manufacturing processes change, authors in the literature suggest that successful approaches to contact lens attacks will "age" over time and become less efficient[31]. As a result, models that do not make decisions based on contact lens texture will outperform others. Existing approaches to iris PAD are unable to generalise adjustments to lens patterns created over time by the same manufacturers, which is a major problem with contact lenses. This means that iris PAD techniques must be updated regularly to maintain accuracy and incorporate training data for the latest contact lenses, even if they are manufactured by the same company[31]. Literature suggests that while post-mortem iris samples are relatively easy to identify, iris samples taken immediately after a person's death may cause identification algorithms to malfunction, because of post-mortem changes that are not yet apparent[61]. Finally, experiments have shown that the contact lenses and synthetic iris images are the most difficult to recognise[63]. **Table 7** shows the different types of presentation attacks discussed in the literature.

Table 7. Types of attacks in the literature.

Attack type	Study
Clear contact lens (clear, textured)	[1], [3], [30], [55], [33], [66], [39], [42], [43], [54], [31], [57], [35], [73], [60], [63], [64], [58], [68], [81], [44], [49]–[82], [72], [69].
Printed images	[1], [3], [22], [27], [33], [34], [44], [39], [42], [54]–[55], [57], [66], [73], [60], [50], [64], [58], [70], [71], [72], [59], [83], [36].
Synthetic irises	[39], [60], [63], [70], [44].
Video replay attacks	[1], [37], [63].
Cadaver irises	[61], [63].

3.3. Datasets

In this section, we analyse several widely used, publicly available datasets for detecting iris-presentation attacks. Existing dataset types, critical issues, and challenges were investigated. To achieve effective research results, a suitable dataset with a sufficient number of quality images to test and train the system must first be identified. There are three types of datasets: datasets based on the environment, datasets based on the sample type, and datasets based on features. Another type of iris dataset is the proprietary/custom dataset, collected by the respective authors for their research and to train their model, which has been used in some studies, such as Das et al.[22], Das et al.[48], Dhar et al.[55], and. Because appropriate information about proprietary datasets is not available, this study focused exclusively on other public types of datasets. **Figure 16** proposed a taxonomy of current iris datasets.

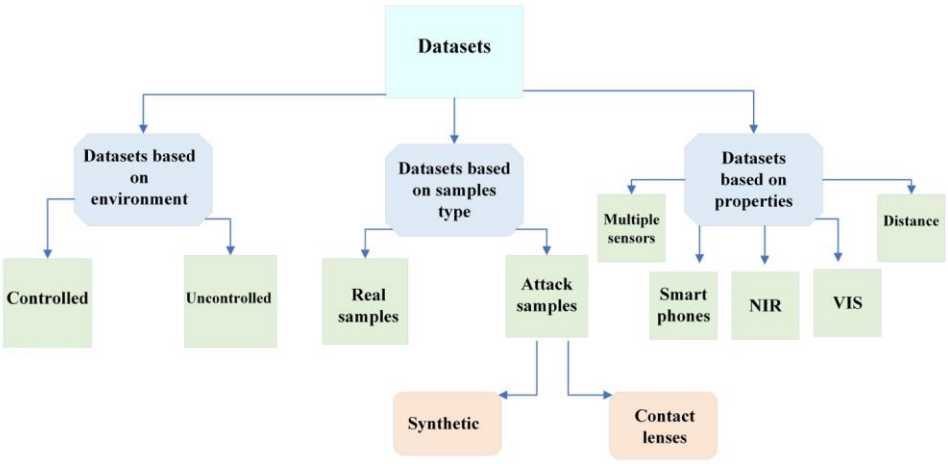

Figure 16. Taxonomy of current iris datasets.

3.3.1. Datasets based on environment

Environmental control factors were used to distinguish between controlled and uncontrolled environments in the datasets. Controlled images were captured in a controlled environment, while the characteristics of the iris (spectrum where the iris is captured, environmental conditions, conjugate specular reflections, iris size, and illumination) were kept constant throughout the acquisition process, because changes in the environment could adversely affect the evaluation[84]. When iris images are captured in an uncontrolled environment, it is permissible for various properties, such as light, distance, angle, and size, to fluctuate. This is an example of a controlled environment dataset that has been used in the literature. The CASIA-Iris dataset is available in four distinct formats. The latest versions of these datasets help study the effects of different variables; CASIA-Iris-Lamp[85] investigates the influence of intraclass variance, while CASIA-Iris-Twins[85] investigates the role of twin correlations. The CASIA-Iris-Interval[85] is a collection of 2639 images (395 classes) taken in an indoor environment with a bespoke NIR camera. The specific characteristics of iris texture

were the research objectives of this dataset. The CASIA-Iris-Lamp[85] includes 16,212 images (819 classes) taken with an iris scanner for this purpose. Images were captured in rooms illuminated with visible light. CASIA-Iris-Lamp is shown in **Figure 17**, and CASIA-Iris-Interval is shown in **Figure 18**.

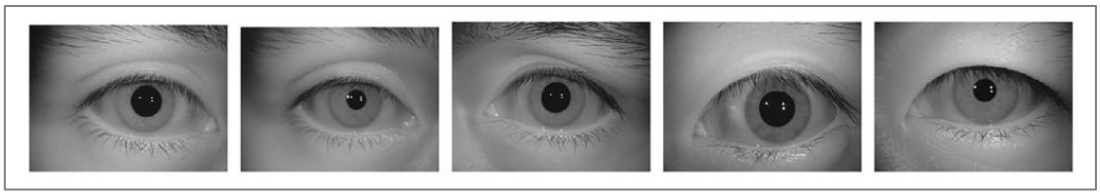

Figure 17. CASIA-Iris-Lamp[94].

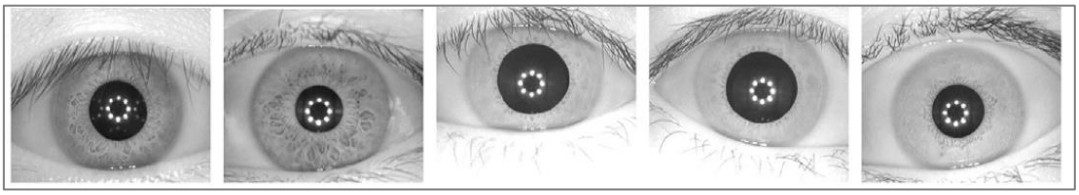

Figure 18. CASIA-Iris-Interval[85].

3.3.2. Datasets based on type of samples

i. Real samples

Various terms are used in the literature to refer to real samples. In some studies, they are also referred to as “bonafides” or “genuine irises”.

ii. Attack samples

Attack datasets contain a variety of attack images, including prints of the original iris shown as a spoofed image, iris images while wearing contact lenses, a fake iris (plastic), post-mortem iris images, and prosthetic eyes made with various technologies. Consequently, datasets containing spoofed samples from real-world scenarios are ideal for detecting iris presentation attacks. The iris spoofing (IIS) dataset from the IIITD[86] includes 4848 pictures of 101 individuals (202 classes). Print attack examples were created using the IIIT-Delhi contact lens iris (CLI) dataset, a cogent CIS 202 dual iris scanner, and an HP flatbed optical scanner. The ATVS-FIr dataset[87] was created at the Universidad Autonoma de Madrid. It contains 800 images of 50 real individuals (100 classes). It also includes 800 fake iris images from 50 fake identities (100 classes). The fictitious images were created using high-resolution printed images.

- Synthetic

Synthetic sample datasets have emerged as a viable solution to the limitations (privacy, logistics, and size) encountered when collecting genuine biometric data. Currently, computer vision applications have evolved to the point where synthetic iris images can be generated with similar characteristics to the real iris. In addition, virtually all image-related parameters (e.g., noise, reflections, iris structure, and rotation) can be adjusted more precisely when capturing real images. Although synthetic images may be more precisely controlled, databases of genuine biometric photos remain the gold standard[82]. Most studies have used the CASIA-Iris-Synthetic dataset[85] for iris spoofing attack detection because it contains more realistic iris images. The CASIA-IrisV4-Syn database[85] includes ten thousand images classified into 1000 classes. It was built by analysing genuine iris images and then redesigning them to create new samples using patch-based sampling. Samples of the CASIA-IrisV4-Syn dataset are shown in **Figure 19**.

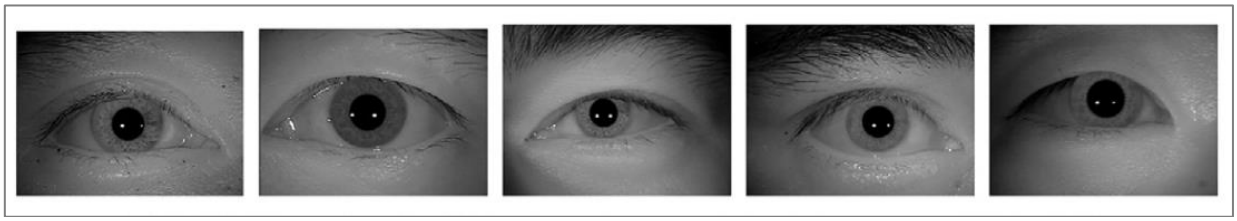

Figure 19. CASIA-IrisV4-Syn dataset[94].

- Contact lenses

Contact lenses can distort or disrupt the patterns of the iris making recognition more difficult. Contact lenses are divided into two types: soft (transparent) and cosmetic (textured). The most commonly used dataset of iris images taken with contact lenses is the 2015 ND contact lens dataset[88], published by the University of Notre Dame. This dataset of 7300 images was created to evaluate contact lens recognition under various experimental conditions. The ND contact lens detection 2013 dataset is another widely used dataset published by the University of Notre Dame[89]. It includes 5100 photographs divided into two datasets, each with a training set and a test set. Other datasets included images of irises taken with contact lenses. In addition, information was collected with special iris sensors equipped with NIR sensors. Samples of the ND contact lens 2015 datasets are shown in **Figure 20**.

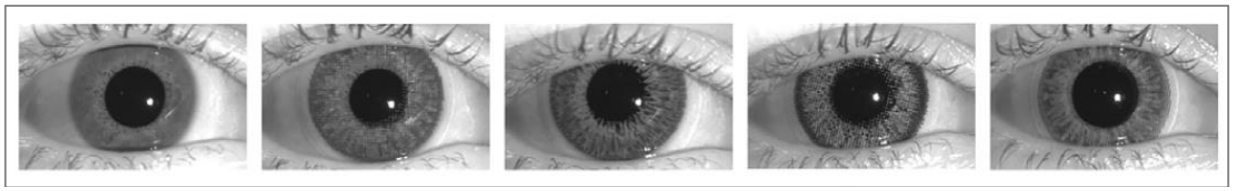

Figure 20. ND contact lens 2015[97].

3.3.3. Datasets based on properties

As iris recognition has gained popularity in a variety of applications, more standards and publicly available iris sample datasets are needed. The term "properties" refers to features associated with the technical configuration and execution of the iris capture process[84]. Each new dataset often uses one or more features for iris recognition. These features fall into two categories: sensor type, spectrum in which the iris was acquired, and acquisition distance. Based on the number of sensors, the dataset was divided into single-sensor and multi-sensor images and images captured with a mobile phone or smartphone.

i. Multiple sensors

A variety of sensors have been used in iris-recognition systems. A variety of companies have manufactured sensors for recognition systems. Logic dictates that sensor quality and image acquisition processes affect the variability of iris recognition rates. Cross-sensor iris datasets are advantageous for iris recognition systems, because they capture iris images from multiple sensors. In addition, the images captured by multiple sensors under varying environmental conditions have varying resolutions and light distributions, which helps to improve identification performance. Additionally, literature shows that datasets containing images captured by multiple sensors are more common than datasets containing photographs captured by a single sensor. Thus, a large dataset helps in performance optimisation. The IIITD-WVU dataset[90] was created as a database for cross-sensor training and testing in various shooting situations. The collection contained 2250 genuine and 1000 textured contact lens iris images from the IIIT-Delhi CLI database. The collection includes 4209 iris photographs for testing purposes (702 classes).

ii. Smartphones

Smartphones with cameras are widely available to the public. Numerous researchers have worked on iris recognition in the mobile environment over the past two decades, as smartphones have become increasingly popular. Smartphones have built-in cameras with good resolution. An important research question is whether these smartphones can be used for iris recognition. When smartphone cameras are used, the visible spectrum is used rather than the NIR range. Some mobile phones/applications include an iris-based authentication system, which is becoming more common. Fujitsu launched the world's first smartphone with an iris identification mechanism on 25 May 2015[82]. Because of the simplicity with which iris capture can be performed, smartphone camera sensors can be used to create numerous datasets. Although iris images captured by smartphone cameras are visible light, the presence of noise generally degrades their quality. Many researchers have used commercial iris recognition sensors because their resolution and quality are better compared to smartphone photos. Therefore, datasets obtained from smartphones have been used only for iris liveness detection applications on smartphones.

iii. Near-infrared spectrum

Near-infrared illumination is commonly used to capture iris images. It operates at wavelengths of 700 nm and 900 nm. The photographs emphasise the intricate structure of the iris rather than its colouration. This helps in correctly depicting the texture of dark-coloured irises. This improves the recognition accuracy.

iv. Visible-light spectrum

Although near-infrared imaging is the main standard in iris imaging, few studies have focused on visible-light imaging. When iris images are acquired with visible light, numerous properties, such as brightness, distance, angle, and size can be altered. However, visible light iris imaging brings other difficulties, such as environmental conditions, optical systems, and passive illumination[84]. UBIRIS-V2 is one of the best known datasets of this type[91]. The UBIRIS database contains photographs taken in a more natural setting. As for UBIRIS-V2, the dataset includes 11,102 photos of 261 subjects taken from a distance and in motion (522 classes). Images of the iris taken in visible light are more susceptible to noise than images taken in a controlled environment. Samples of the UBIRIS-V2 dataset are shown in **Figure 21**.

Figure 21. UBIRIS-V2[91].

v. Distance

Iris imaging from a distance is a critical challenge in iris recognition. Capturing iris images from a distance is related to a number of image acquisition issues, including the size of the eye, the amount of light reflected from the iris, and motion issues in capturing and focusing the iris. Numerous publicly available iris datasets have been created to facilitate remote iris imaging research, including the UBIRIS-V2 collection, which contains 11,102 photographs of 261 individuals (522 classes). The images in the collection were taken under visible light in less crowded or open environments, with the subject approaching the camera from a distance of 4 m to 8 m.

3.3.4. Problems with iris presentation attack detection datasets

From the literature, iris image identification in visible light performs much worse than near infrared iris image identification[32]. This is because the abundance of iris texture is difficult to detect in VIS images,

particularly for dark-coloured irises. This is an important reason why most authors use NIR iris images in their systems. Another critical limitation to note is that not all datasets contain both real and fake examples in the visible light spectrum. The majority of published datasets contain instances of two to three different forms of spoofing attacks. Researchers will benefit from a combination of these categories. Therefore, a single dataset is needed that includes all known forms of attacks. In addition, one of the observed problems was that the authors did not rely on images captured by smartphone cameras. Although images captured by smartphone cameras are visible light, the presence of noise degrades their quality. This is a known problem because smartphone cameras are not technologically superior to NIR cameras[92]. Almost all authors facing the same issue have relied on commercial iris recognition sensors[82]. Commercial sensors that use NIR iris matching techniques produce images that have higher resolution and quality than those captured by smartphone cameras, where iris textures appear much better when illuminated at a wavelength of 700–900 nm[93]. The datasets obtained through cell phones were only used for iris recognition applications on smartphones. However, cross-sensor iris datasets are useful for identifying iris attacks because they capture iris images from multiple sensors. Moreover, multiple sensors capture images with varying resolutions and light distributions, resulting in improved identification performance. Researchers in this discipline should be aware of relevant datasets to compare their results and facilitate their study with existing datasets rather than creating their own. Existing datasets face numerous challenges and issues, which are discussed below. Finally, Boulkenafet et al.[84] have established a website to clarify the availability of datasets.

i. Privacy regulations

New data privacy regulations that protect individual privacy are a relatively new issue. In Europe, the GDPR law provides for the right to erasure (also known as the right to be forgotten)[94], which allows for the deletion of previously used data and the deletion of subject-related information[84]. Globally, similar regulations have been used and discussed. In addition, many self-generated datasets contain personal information about an individual's biometric identity. Consequently, such a sensitive dataset is not available to the public.

ii. Lack of details

Some authors have considered many of the details irrelevant to their research, but this information may be necessary for others and may expand the potential application areas of the dataset[84]. These details may relate to the characteristics of optical systems, the protocol for capturing images, descriptions of the spectra of captured images, and sensor type or model, where many datasets are deficient in their descriptions.

iii. Unpopularity of synthetic images

These studies suggest that datasets containing synthetic images are rarely used in investigations of iris presentation attacks. Researchers prefer real images although synthetic datasets contain a large number of samples because the effects studied are not realistic[84].

iv. Comparison difficulties

Numerous accessible datasets share a variety of features, such as near-infrared samples. Despite the use of a predetermined baseline, the results differed significantly because of the range of implementation methodologies, datasets, and assessment processes[95]. These differences make comparison of techniques impossible, a challenge compounded by the frequent unavailability of the dataset. Many concerns must be addressed by developing benchmark datasets, conducting independent reviews, and providing publicly available datasets with symmetric metrics. **Figure 22** shown the number of used datasets over years, and **Figure 23** illustrates the percentage of the studies that used NIR and VIS spectrums in experiments. **Table 8** shown datasets that are used frequently in reviewed studies, types of attacks, year and total of images.

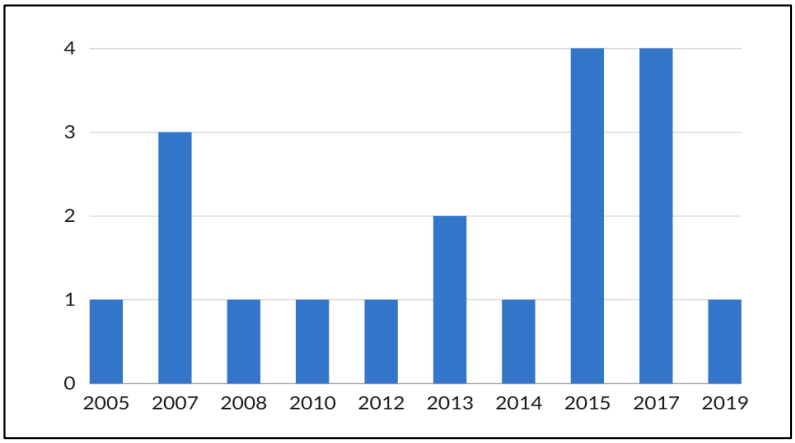

Figure 22. The number of used datasets over years.

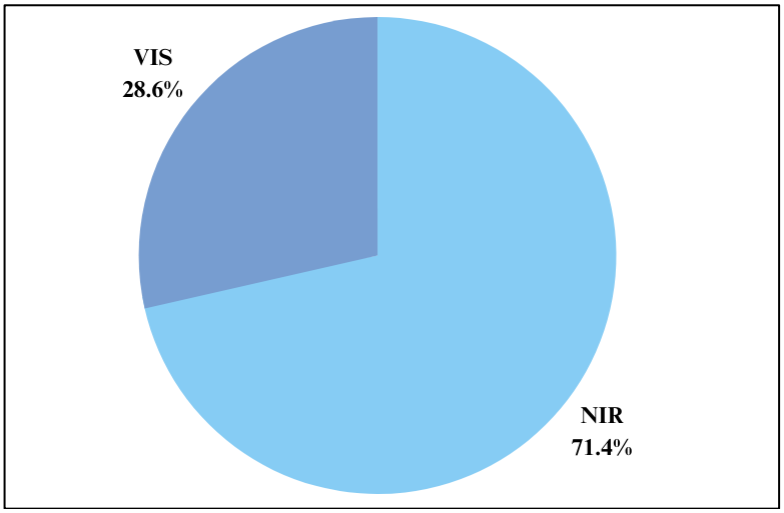

Figure 23. The percentage of the studies that used NIR and VIS spectrums in experiments.

Table 8. Publicly available datasets, types of attacks, and year of reviewed studies.

Dataset	Availability	Live images	Contact lens	Print attack	Synthesised iris	Artificial iris	Camera type	Year	Total images	Study
Notre Dame cosmetic-contact-lenses-2013 (NDCLD13)	Available	✓	✓				NIR + VIS	2013	5100 images	[2], [40], [57], [64], [68], [70], [82], [44], [75].
Notre Dame contact lens 2015 (NDCLD'15)	Available	✓	✓				NIR + VIS	2015	7300 images	[29], [55], [43], [50], [62], [57], [75]–[52], [74], [44]–[31].
Visible spectrum iris artefact (VSIA)	Not available	✓					VIS	2015	3300 images	[27], [36], [67].
ATVS fake iris (FIR)	Available	✓		✓			NIR	2007	1600 images	[27], [40], [41], [63].
LivDet Iris-2013 (Warsaw)	Not available	✓	✓	✓			NIR	2013	1667 images	[27], [37], [40], [60], [44].
LivDet Iris-2015 (Warsaw)	Not available	✓		✓			NIR	2015	7559 images	[22], [33], [66], [63], [35], [70].
LivDet Iris-20117 (Warsaw)	Not available	✓		✓			NIR	2017	12,013 images	[3], [50], [55], [81], [52].
LivDet Iris-2017 (Notre Dame)	Available	✓	✓				NIR + VIS	2017	3000 images	[3], [55], [57]–[51], [63], [64], [72], [74], [96], [75]
IIIT-D contact lens iris (IITD-CLI)	Available	✓	✓				NIR	2012	6570 images	[2], [33], [35], [41], [56], [75]–[64], [49], [62].
IIIT-D iris spoofing (IIS)	Available		✓	✓			NIR	2014	4848 images	[33], [35], [39].
CASIA-IrisV3 (interval, lamp, twins.)	Available	✓					NIR	2005 2007	22,034 images	[7], [63], [66], [67].
CASIA-Iris-Syn V4	Available	✓			✓		N/A (synthetic)	2008	10,736 images	[38].
LivDet Iris-2015 (Clarkson)	Available	✓	✓	✓			NIR	2015	4255 images	[33], [35], [63].
LivDet Iris-2017 (Clarkson)	Available	✓	✓	✓			NIR	2017	8095 images	[3], [54], [55], [63], [64], [70], [49], [72], [96], [75].
UBIRIS-V2	Available	✓					RGB	2010	11,102 images	[21]
BERC-Iris-Fake	Not available	✓	✓	✓		✓	NIR	2007	4780 images	[22], [63], [66], [70].
WVU uncon-strained multi-sensor iris presentation attack (Un-MIPA)	Available		✓				NIR	2019	18706 images	[62], [65]
IIITD-WVU	Available	✓	✓	✓			NIR + VIS	2017	10459 images	[3], [55], [58], [59], [75], [64], [72], [96], [55]

3.4. Performance measures

The performance of this method is critical to the practical application of various iris presentation attack detection solutions. Numerous metrics have been used to evaluate the performance of biometric systems. The ISO/IEC 1979 series of standards standardises the assessment of biometric performance, which is performed in collaboration with ISO/IEC[82]. This section presents the results of the analysis of the performance measures used in primary studies.

3.4.1. Attack presentation classification error rate (APCER)

The APCER measure represents the percentage of incorrectly attacked images. APCER is a popular measure. The APCER is equivalent to the true detection rate, and the lower the APCER, the better is the performance. The formula for APCER is as follows:

$$\text{APCER} = \frac{FP}{(TN) + (FP)} \tag{1}$$

where *FP* is false positive, and *TN* is true negative samples.

3.4.2. Bonafide presentation classification error rate (BPCER)

The BPCER measure is the percentage of images misclassified. BPCER is equivalent to the false detection rate (FDR), and the lower the BPCER, the better is the performance.

The formula for BPCER is as follows:

$$\text{BPCER} = \frac{FN}{(TP + FN)} \tag{2}$$

where *FN* is false negative, and *TP* is true positive samples.

3.4.3. Accuracy

Accuracy was defined as the ratio between the correctly identified photos and the total number of images. When the classes are balanced, the amount of real and fake samples is equal, and the accuracy is satisfactory. Accuracy is among the most commonly used performance measures in the literature to evaluate the performance of an iris recognition system. The formula for accuracy is as follows:

$$\text{Accuracy} = \frac{(TP + TN)}{(TP + TN + FP + FN)} \tag{3}$$

where *TP* is true positive, *TN* is true negative, *FP* is false positive, and *FN* is false negative samples.

3.4.4. Average classification error rate (ACER)

The average classification error rate (ACER) is a commonly used metric to evaluate the performance of a detection system. The ACER value is the average of the APCER and BPCER values. A low ACER value indicates that the detection system is working properly. The formula for ACER is as follows:

$$\text{ACER} = \frac{(\text{APCER} + \text{BPCER})}{2} \tag{4}$$

3.4.5. Correct classification rate (CCR)

The CCR is estimated by dividing the total number of samples by the sum of correctly classified genuine samples and correctly classified presentation attacks.

3.4.6. Half total error rate (HTER)

The half total error rate (HTER) corresponds to the average of the BPCER and ACPER.

3.4.7. Equal error rate (EER)

Equal error rate (EER): Points or values at which ACPER and BPCER are equal. The point at which both errors are equal is considered optimal. **Table 9** below shown the performance measures in reviewed studies. **Figure 24** presents the most frequently used performance measures in the literature.

Table 9. Performance measures in reviewed studies.

Measure	Study
Attack presentation classification error rate (APCER)	[1], [3], [31], [65], [35], [73], [43], [75], [50], [57]–[44], [61]–[33], [81], [70]–[49], [37], [72]–[62].
Bonafide presentation classification error rate (BPCER)	[1], [3], [31], [65], [43], [75], [50], [57]–[44], [61]–[52], [58], [81], [70], [49], [73], [72]–[62].
Accuracy	[3], [7], [21], [31], [42], [53], [51], [68], [49].
Average classification error rate (ACER)	[33], [35], [73], [50], [51], [37], [71], [49], [59], [72], [83].
Correct classification rate (CCR)	[2], [48], [33], [35], [56], [60], [62], [63], [70], [29], [82].
Half total error rate (HTER)	[3], [36], [53], [57], [58], [75], [64], [68], [96], [62].
Equal error rate (EER)	[9], ,[39], [57], [51], [69], [71], [49], [83].

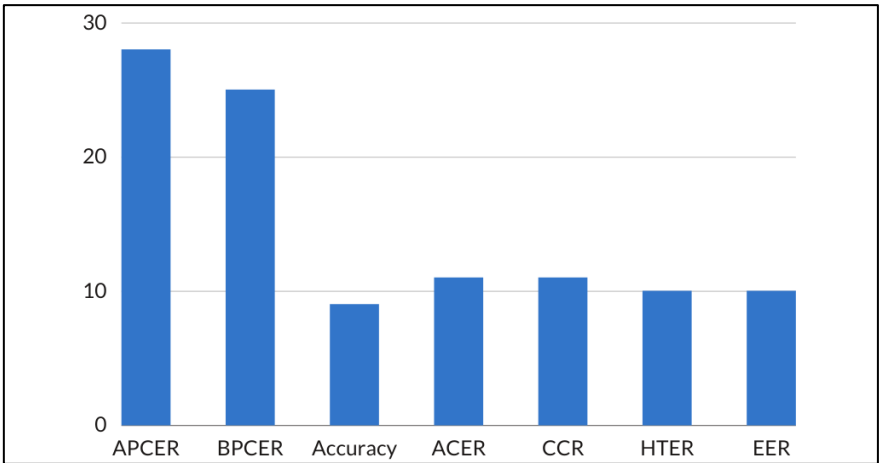

Figure 24. The most frequently used performance measures in the literature.

3.4.8. Problems in evaluating performance of iris presentation attack detection

The performance of the iris recognition model can be evaluated using several metrics. The ISO/IEC introduced a standardised evaluation of the 1979 series of standards. Different metrics for iris attack detection are more commonly used in the literature, but logically, the metrics provide correct results when approximately equal samples are used. Currently, there are no metrics to measure the performance of unbalanced datasets.

4. Limitations and challenges of iris presentation attack detection research

Although businesses and governments have widely embraced iris recognition technology, presentation attack detection research is still at an early stage. Many current gaps in detection techniques and attacks remain unresolved, and new challenges have emerged. The following subsections summarise the main open challenges that require further investigation.

4.1. Limited training data

Existing research assumes that a system is subject to a certain form of iris presentation attack, such as lenses or printed irises. In real-world circumstances, where the iris recognition system is vulnerable to a variety of presentation attacks, this may not be the case. There is a dearth of training data in the literature for detecting

multiple iris-presentation attacks.

4.2. Generalisation to new attacks

Cross-database evaluation is considered a more difficult challenge than intra-database evaluation (i.e., training on a single dataset and testing on a disjoint subset of the same dataset). Moreover, iris presentation attack detection must account for many variations, such as sensor characteristics, sample acquisition environments, and unknown presentation attacks. Therefore, algorithms with high generalisability and transferability in real-world scenarios are required.

4.3. Adversarial attack

Recent technologies create an iris pattern that resembles a real iris image and matches that of the actual user. To create an adversarial attack, iris textures were automatically generated from unique iris images. Adversarial attacks pose a challenge for biometric systems because it can be difficult to distinguish them from genuine images. Current synthetic iris generation technologies produce results that are physically like the original iris patterns. The number of studies on these attacks is still limited.

4.4. Computational complexity

Although deep learning-based approaches efficiently address a wide range of problems, they have numerous drawbacks, such as overfitting because of a small number of training samples and many model parameters. Recent applications need to perform fast classification in real-time and reduce computational complexity while detecting presentation attacks.

4.5. Ethical and privacy concerns

Existing datasets face numerous challenges and issues, such as the privacy regulations that protect biometrics datasets. In addition, authors should streamline the administrative processes for researchers to have sufficient clarity when a dataset is needed. This is because certain datasets require the signature of a legal, institutional representative, which is a significant hurdle for researchers. Moreover, studies urge that the entire license agreement be posted on the dataset website along with a selection of images from the dataset. This allows a determination of whether the dataset is appropriate for a particular research project before initiating the approval process.

4.6. Evaluation metrics

The performance of the iris recognition model can be evaluated using several metrics. The ISO/IEC introduced a standardised evaluation of the 1979 series of standards. Different metrics for iris attack detection are more commonly used in the literature, but logically, the metrics provide correct results when approximately equal samples are used. Currently, there are no metrics to measure the performance of unbalanced datasets.

5. Future research directions

This section outlines the potential avenues for future research, building upon the challenges that have been previously addressed. **Table 10** provides a concise overview of these research directions, highlighting the advantages they bring to the field of iris presentation attack detection. Subsequently, each direction is discussed in detail to provide a comprehensive understanding.

Table 10. Future research directions.

Future research direction	Advantage
Visible light images	Iris images captured under visible illumination can be used for various e-business and surveillance applications.
Live-tissue verification	Unsupervised applications, such as home security and door access control need to make sure that the image captured and compared is from a living body part of the human being to be identified and that it is not a fake sample.
Uncontrolled environment	Outdoor locations with high light intensity need to develop accurate presentation attack detection algorithms for iris images.
Synthetic iris images	Up to now, datasets for synthetic iris images are only available upon request and after a formal licensing agreement has been signed.
Bias in presentation attack detection	The biased behaviour of the recognition systems leads to problems in the accuracy of the results. So, understanding biases and clarifying them could increase trust, fairness, and confidentiality in iris recognition systems.
Data augmentation techniques	Data augmentation techniques can affect the performance and generalisability of iris presentation attack detection.

5.1. Visible light images

Near-infrared images are commonly used as input in iris recognition systems because they result in less reflection in the cornea of the eye, resulting in higher quality and stronger input images[21]. However, this requires the use of highly sophisticated near-infrared sensors. At a time when smartphones are widely used, recognising people from visible-range photographs is more advantageous because visible-range images can be easily captured with smartphone cameras. Iris images captured under visible illumination can be used for various e-business and surveillance applications. Therefore, accurate cross-spectral iris recognition capabilities are highly desirable.

5.2. Live-tissue verification

The fundamental problem of live tissue verification has not yet been satisfactorily solved in the field of iris recognition[13]. The reliability of any biometric recognition system relies on the fact that the image captured and compared is from a living body part of the human being to be identified and that it is not a fake sample. Many commercially available iris recognition systems can be easily fooled by producing a high-quality image of an iris instead of a genuine object. This makes them unsuitable for unsupervised applications, such as home security and door access control. In supervised applications (e.g., immigration control), where image-capture is monitored by a human officer, live-iris recognition is less problematic.

5.3. Uncontrolled environment

Because biometric iris recognition is reliable, it will be used in the next generation of mobile handsets. This feature is advantageous in a variety of circumstances, but it also poses unforeseen research obstacles. For example, it may be difficult to capture iris photographs in outdoor locations with high light intensity. Other difficulties such as algorithm complexity must be addressed. However, most research has been conducted in a controlled environment. Therefore, it is important to develop accurate presentation attack detection algorithms for iris images captured with a mobile sensor[47].

5.4. Synthetic iris images

Although existing extant synthetic iris image datasets contain many more samples than genuine iris image datasets, their popularity remains limited[84]. There is uncertainty about the extent to which synthetic iris images exhibit the features and characteristics of the natural iris. Despite the lack of personally identifiable information, datasets for synthetic iris images are only available upon request and after a formal licencing agreement has been signed.

5.5. Bias in presentation attack detection

Recently, much attention has been paid to bias in facial recognition systems. Studies have shown that a bias occurs for a variety of reasons (gender, colour, and demographic groups). This biased behaviour of the recognition systems leads to problems in the accuracy of the results. Understanding biases and clarifying them could increase trust, fairness, and confidentiality in biometric systems[97]. This could help in the development of new fair-minded solutions. The first study to investigate demographic and gender biases in PAD was Fang et al., which showed that males have lower error rates than females, and females seem to be less protected by iris PAD. The authors mention possible future extensions to studying bias in eye colour. There might also be space to study the accuracy of the iris PAD in different ethnicities[5]. Despite the fact that an iris sample contains significantly less demographic information, the study of bias is a worthwhile endeavour.

5.6. Data augmentation techniques

Data augmentation techniques can affect the performance and generalisability of iris presentation attack detection. Shift, rotation, brightness, and generative adversarial networks are examples of data-augmentation methods. Fang et al.[72] studied the effects of different data augmentation methods on the performance of iris PAD. Their experimental results showed that augmentation methods significantly improved iris PAD performance in several cases. Nevertheless, little attention has been paid to the exact effects of data augmentation on the iris PAD performance. This makes these methods interesting directions in which to search.

6. Conclusion

In the post-COVID-19 world, iris recognition removes the criticism of fingerprint scanners that require a finger to contact a surface or screen to be scanned. As a result, this feature can be widely used in the future. The recognised individual did not have to touch a device that had recently been touched by a stranger. Despite the many advantages in the cyber security world, the use of irises to recognise individuals raises significant security issues that are seen as barriers to the widespread implementation of the feature. In this study, techniques, attack types, datasets, performance measures, and challenges associated with iris presentation attack detection have been discussed. The challenges appear to be difficult, such as the difficulty of technique comparison, diversity and modernisation of attacks, difficulty of generalising to unknown attacks, non-exploitation of deep learning techniques, complexity of procedures and restrictions, and monopolisation of data. In addition, we presented future research directions that seem interesting, such as using more visible light images and synthetic iris images in experiments, live-tissue verification, using images taken in an uncontrolled environment, and looking for biases in presentation attack detection and data augmentation techniques. Although significant progress has been made in the literature, challenges related to the detection of iris presentation attacks have not been properly addressed and remain open. This is a call to researchers to the importance of the exploitation of computer vision and image recognition techniques to develop solutions.

Author contributions

Conceptualization, NSAR and AAAS; methodology, NSAR; software, NSAR; validation, NSAR; resources, NSAR; data curation, NSAR and AAAS; writing—original draft preparation, NSAR; writing—review and editing, AAAS; visualization, NSAR; supervision, AAAS; project administration, AAAS; funding acquisition, AAAS. All authors have read and agreed to the published version of the manuscript.

Acknowledgments

The authors gratefully acknowledge Qassim University, represented by the Deanship of "Scientific Research, on the financial support for this research under the number (COC-2022-1-2-J-30393) during the academic year 1444 AH/2022 AD".

Conflict of interest

The authors declare no conflict of interest.

Abbreviations

CNN	Convolutional neural networks
NIR	Near-infrared
PA	Presentation attacks
PAD	Presentation attacks detection
SVM	Support vector machines
VIS	Visible-light

References

1. Yadav S, Chen C, Ross A. Relativistic discriminator: A one-class classifier for generalized iris presentation attack detection. In: Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (WACV); 1–5 March 2020; Snowmass, CO, USA. pp. 2624–2633.
2. Raghavendra R, Raja KB, Busch C. ContlensNet: Robust iris contact lens detection using deep convolutional neural networks. In: Proceedings of the 2017 IEEE Winter Conference on Applications of Computer Vision (WACV); 24–31 March 2017; Santa Rosa, CA, USA. pp. 1160–1167.
3. Kuehlkamp A, Pinto A, Rocha A, et al. Ensemble of multi-view learning classifiers for cross-domain iris presentation attack detection. IEEE Transactions on Information Forensics and Security 2019; 14(6): 1419–1431. doi: 10.1109/TIFS.2018.2878542
4. Czajka A, Bowyer KW. Presentation attack detection for iris recognition: An assessment of the state-of-the-art. ACM Computing Surveys 2018; 51(4): 1–35. doi: 10.1145/3232849
5. Boyd A, Fang Z, Czajka A, Bowyer KW. Iris presentation attack detection: Where are we now? Pattern Recognition Letters 2020; 138: 483–489. doi: 10.1016/j.patrec.2020.08.018
6. Pravallika P, Prasad KS. SVM classification for fake biometric detection using image quality assessment: Application to iris, face and palm print. In: Proceedings of the 2016 International Conference on Inventive Computation Technologies (ICICT); 26–27 August 2016; Coimbatore, India. pp. 1–6.
7. Subban R, Susitha N, Mankame DP. Efficient iris recognition using Haralick features based extraction and fuzzy particle swarm optimization. Cluster Computing 2018; 21(1): 79–90. doi: 10.1007/s10586-017-0934-0
8. Gupta M, Singh V, Agarwal A, et al. Generalized iris presentation attack detection algorithm under cross-database settings. In: Proceedings of the 2020 25th International Conference on Pattern Recognition (ICPR); 10–15 January 2021; Milan, Italy. pp. 5318–5325.
9. Wang K, Kumar A. Cross-spectral iris recognition using CNN and supervised discrete hashing. Pattern Recognition 2019; 86: 85–98. doi: 10.1016/j.patcog.2018.08.010
10. Choudhary M, Tiwari V, Venkanna U. Enhancing human iris recognition performance in unconstrained environment using ensemble of convolutional and residual deep neural network models. Soft Computing 2020; 24(15): 11477–11491. doi: 10.1007/s00500-019-04610-2
11. Nguyen K, Fookes C, Jillela R, et al. Long range iris recognition: A survey. Pattern Recognition 2017; 72: 123–143. doi: 10.1016/j.patcog.2017.05.021
12. Sava JA. Biometric authentication and identification market revenue worldwide in 2019 and 2027. Available online: https://www.statista.com/statistics/1012215/worldwide-biometric-authentication-and-identification-market-value/ (accessed on 25 February 2022).
13. Sinha VK, Gupta AK, Mahajan M. Detecting fake iris in iris bio-metric system. Digital Investigation 2018; 25: 97–104. doi: 10.1016/j.diin.2018.03.002
14. Bok JY, Suh KH, Lee EC. Detecting fake finger-vein data using remote photoplethysmography. Electronics 2019; 8(9): 1016. doi: 10.3390/electronics8091016

15. Das P, Mcfiratht J, Fang Z, Boyd A, et al. Iris liveness detection competition (LivDet-Iris)—The 2020 edition. In: Proceedings of the 2020 IEEE International Joint Conference on Biometrics (IJCB); 28 September 2020–1 October 2020; Houston, TX, USA. pp. 1–9.
16. Chen R, Lin X, Ding T. Liveness detection for iris recognition using multispectral images. Pattern Recognition Letters 2012; 33(12): 1513–1519. doi: 10.1016/j.patrec.2012.04.002
17. Yadav S, Chen C, Ross A. Synthesizing iris images using RaSGAN with application in presentation attack detection. In: Proceedings of the 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW); 16–17 June 2019; Long Beach, CA, USA. pp. 2422–2430.
18. Gautam G, Mukhopadhyay S. Challenges, taxonomy and techniques of iris localization: A survey. Digital Signal Processing 2020; 107: 102852. doi: 10.1016/j.dsp.2020.102852
19. Meenakshi K, Maragatham G. A comprehensive survey on iris presentation attacks and detection based on generative adversarial network. In: Proceedings of the 2020 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS); 10–11 December 2020; Chennai, India. pp. 1–9.
20. Czajka A. Is that eye dead or alive? Detecting new iris biometrics attacks. Biometric Technology Today 2021; 2021(5): 9–12. doi: 10.1016/S0969-4765(21)00060-6
21. Menon H, Mukherjee A. Iris biometrics using deep convolutional networks. In: Proceedings of the 2018 IEEE International Instrumentation and Measurement Technology Conference (I2MTC); 14–17 May 2018; Houston, TX, USA. pp. 1–5.
22. Hoffman S, Sharma R, Ross A. Iris + ocular: Generalized iris presentation attack detection using multiple convolutional neural networks. In: Proceedings of the 2019 International Conference on Biometrics (ICB); 4–7 June 2019; Crete, Greece. pp. 1–8.
23. Yambay D, Becker B, Kohli N, et al. LivDet iris 2017—Iris liveness detection competition 2017. In: Proceedings of the 2017 IEEE International Joint Conference on Biometrics (IJCB); 1–4 October 2017; Denver, CO, USA. pp. 733–741.
24. Daugman JG. High confidence visual recognition of persons by a test of statistical independence. IEEE Transactions on Pattern Analysis and Machine Intelligence 1993; 15(11): 1148–1161. doi: 10.1109/34.244676
25. Fang Z, Czajka A. Open source iris recognition hardware and software with presentation attack detection. In: Proceedings of the 2020 IEEE International Joint Conference on Biometrics (IJCB); 28 September 2020–1 October 2020; Houston, TX, USA. pp. 1–8.
26. Zhao J, Masood R, Seneviratne S. A review of computer vision methods in network security. IEEE Communications Surveys & Tutorials 2021; 23(3): 1838–1878. doi: 10.1109/COMST.2021.3086475
27. Raghavendra R, Busch C. Robust scheme for iris presentation attack detection using multiscale binarized statistical image features. IEEE Transactions on Information Forensics and Security 2015; 10(4): 703–715. doi: 10.1109/TIFS.2015.2400393
28. Saranya S, Sherline SV, Maheswari M. Fake biometric detection using image quality assessment: Application to iris, fingerprint recognition. In: Proceedings of the 2016 Second International Conference on Science Technology Engineering and Management (ICONSTEM); 30–31 March 2016; Chennai, India. pp. 98–103.
29. McGrath J, Bowyer KW, Czajka A. Open source presentation attack detection baseline for iris recognition. arXiv 2018. doi: 10.48550/arXiv.1809.10172
30. Wang J, Tian Q. Contact lenses detection based on the gaussian curvature. Journal of Computers 2019; 30(2): 158–164. doi: 10.3966/199115992019043002014
31. Fang Z, Czajka A, Bowyer KW. Robust iris presentation attack detection fusing 2D and 3D information. IEEE Transactions on Information Forensics and Security 2020; 16: 510–520. doi: 10.1109/TIFS.2020.3015547
32. Raja KB, Raghavendra R, Venkatesh V, Busch C. Multi-patch deep sparse histograms for iris recognition in visible spectrum using collaborative subspace for robust verification. Pattern Recognition Letters 2017; 91: 27–36. doi: 10.1016/j.patrec.2016.12.025
33. Kaur B. Iris spoofing detection using discrete orthogonal moments. Multimedia Tools and Applications 2020; 79(9): 6623–6647. doi: 10.1007/s11042-019-08281-x
34. Shahriar H, Haddad H, Islam M. An iris-based authentication framework to prevent presentation attacks. In: Proceedings of the 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC); 4–8 July 2017; Turin, Italy. pp. 504–509.
35. Kaur B, Singh S, Kumar J. Cross-sensor iris spoofing detection using orthogonal features. Computers & Electrical Engineering 2019; 73: 279–288. doi: 10.1016/j.compeleceng.2018.12.002
36. Malhotra A, Gupta R. Iris anti-spoofing under varying illumination conditions. In: Proceedings of the 2016 1st India International Conference on Information Processing (IICIP); 12–14 August 2016; Delhi, India. pp. 1–6.
37. Raja KB, Raghavendra R, Busch C. Presentation attack detection using Laplacian decomposed frequency response for visible spectrum and near-infra-red iris systems. In: Proceedings of the 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS); 8–11 September 2015; Arlington, VA, USA. pp. 1–8.

38. Fathy WSA, Ali HS, Mahmoud II. Statistical representation for iris anti-spoofing using wavelet-based feature extraction and selection algorithms. In: Proceedings of the 2017 34th National Radio Science Conference (NRSC); 13–16 March 2017; Alexandria, Egypt. pp. 221–229.
39. Kohli N, Yadav D, Vatasa M, et al. Detecting medley of iris spoofing attacks using DESIST. In: Proceedings of the 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS); 6–9 September 2016; Niagara Falls, NY, USA. pp. 1–6.
40. Gragnaniello D, Poggi G, Sansone C, et al. An investigation of local descriptors for biometric spoofing detection. IEEE Transactions on Information Forensics and Security 2015; 10(4): 849–863. doi: 10.1109/TIFS.2015.2404294
41. Agarwal R, Jalal AS, Arya KV. Local binary hexagonal extrema pattern (LBHXEP): A new feature descriptor for fake iris detection. The Visual Computer 2021; 37(6): 1357–1368. doi: 10.1007/s00371-020-01870-0
42. Das A, Pal U, Ferrer MA, Blumenstein M. A framework for liveness detection for direct attacks in the visible spectrum for multimodal ocular biometrics. Pattern Recognition Letters 2016; 82: 232–241. doi: 10.1016/j.patrec.2015.11.016
43. Czajka A, Fang Z, Bowyer K. Iris presentation attack detection based on photometric stereo features. In: Proceedings of the 2019 IEEE Winter Conference on Applications of Computer Vision (WACV); 7–11 January 2019; Waikoloa, HI, USA. pp. 877–885.
44. Yadav D, Kohli N, Agarwal A, et al. Fusion of handcrafted and deep learning features for large-scale multiple iris presentation attack detection. In: Proceedings of the 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW); 18–22 June 2018; Salt Lake City, UT, USA. pp. 685–6857.
45. Kannala J, Rahtu E. BSIF: Binarized statistical image features. In: Proceedings of the 21st International Conference on Pattern Recognition (ICPR2012); 11–15 November 2012; Tsukuba, Japan. pp. 1363–1366.
46. Boulkenafet Z, Komulainen J, Hadid A. Face spoofing detection using colour texture analysis. IEEE Transactions on Information Forensics and Security 2016; 11(8): 1818–1830. doi: 10.1109/TIFS.2016.2555286
47. Yadav D, Kohli N, Yadav S, et al. Iris presentation attack via textured contact lens in unconstrained environment. In: Proceedings of the 2018 IEEE Winter Conference on Applications of Computer Vision (WACV); 12–15 March 2018; Lake Tahoe, NV, USA. pp. 503–511.
48. Czajka A, Bowyer KW, Krumdick M, et al. Recognition of image-orientation-based iris spoofing. IEEE Transactions on Information Forensics and Security 2017; 12(9): 2184–2196. doi: 10.1109/TIFS.2017.2701332
49. Choudhary M, Tiwari V, Venkanna U. Iris anti-spoofing through score-level fusion of handcrafted and data-driven features. Applied Soft Computing 2020; 91: 106206. doi: 10.1016/j.asoc.2020.106206
50. Nguyen DT, Pham TD, Lee YW, Park KR. Deep learning-based enhanced presentation attack detection for iris recognition by combining features from local and global regions based on NIR camera sensor. Sensors 2018; 18(8): 2601. doi: 10.3390/s18082601
51. Choudhary M, Tiwari V, Uduthalapally V. Iris presentation attack detection based on best-k feature selection from YOLO inspired RoI. Neural Computing and Applications 2021; 33(11): 5609–5629. doi: 10.1007/s00521-020-05342-3
52. Nguyen DT, Baek NR, Pham TD, Park KR. Presentation attack detection for iris recognition system using NIR camera sensor. Sensors 2018; 18(5): 1315. doi: 10.3390/s18051315
53. Menotti D, Chiachia G, Pinto A, et al. Deep representations for iris, face, and fingerprint spoofing detection. IEEE Transactions on Information Forensics and Security 2015; 10(4): 864–879. doi: 10.1109/TIFS.2015.2398817
54. Chen C, Ross A. Exploring the use of irisCodes for presentation attack detection. In: Proceedings of the 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS); 22–25 October 2018; Redondo Beach, CA, USA. pp. 1–9.
55. Sharma R, Ross A. D-NetPAD: An explainable and interpretable iris presentation attack detector. In: Proceedings of the 2020 IEEE International Joint Conference on Biometrics (IJCB); 28 September 2020–1 October 2020; Houston, TX, USA. pp. 1–10.
56. Choudhary M, Tiwari V, Venkanna U. An approach for iris contact lens detection and classification using ensemble of customized DenseNet and SVM. Future Generation Computer Systems 2019; 101: 1259–1270. doi: 10.1016/j.future.2019.07.003
57. Dhar P, Kumar A, Kaplan K, et al. EyePAD++: A distillation-based approach for joint eye authentication and presentation attack detection using periocular images. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR); 18–24 June 2022; New Orleans, LA, USA. pp. 20186–20195.
58. Fang M, Damer N, Fadi B, et al. Deep learning multi-layer fusion for an accurate iris presentation attack detection. In: Proceedings of the 2020 IEEE 23rd International Conference on Information Fusion (FUSION); 6–9 July 2020; Rustenburg, South Africa. pp. 1–8.
59. Arora S, Bhatia MPS. Presentation attack detection for iris recognition using deep learning. International Journal of System Assurance Engineering and Management 2020; 11(2): 232–238. doi: 10.1007/s13198-020-00948-1
60. He L, Li H, Liu F, et al. Multi-patch convolution neural network for iris liveness detection. In: Proceedings of the 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS); 6–9 September 2016; Niagara Falls, NY, USA. pp. 1–7.

61. Trokielewicz M, Czajka A, Maciejewicz P. Presentation attack detection for cadaver iris. In: Proceedings of the 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS); 22–25 October 2018; Redondo Beach, CA, USA. pp. 1–10.
62. Fang M, Damer N, Boutros F, et al. Cross-database and cross-attack Iris presentation attack detection using micro stripes analyses. Image and Vision Computing 2021; 105: 104057. doi: 10.1016/j.imavis.2020.104057
63. Boyd A, Speth Jeremy, Parzanello L, et al. State of the art in open-set iris presentation attack detection. arXiv 2022. doi: 10.48550/arXiv.2208.10564
64. Fang M, Boutros F, Damer N. Intra and cross-spectrum iris presentation attack detection in the NIR and visible domains using attention-based and pixel-wise supervised learning. arXiv 2022.
65. Yadav D, Kohli N, Vatsa M, et al. Detecting textured contact lens in uncontrolled environment using DensePAD. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW); 16–17 June 2019; Long Beach, CA, USA. pp. 2336–2344.
66. Hoffman S, Sharma R, Ross A. Convolutional neural networks for iris presentation attack detection: Toward cross-dataset and cross-sensor generalization. In: Proceedings of the 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW); 18–22 June 2018; Salt Lake City, UT. pp. 1701–1708.
67. Chatterjee P, Roy K. Anti-spoofing approach using deep convolutional neural network. In: Mouhoub M, Sadaoui S, Ait Mohamed O (editors). Recent Trends and Future Technology in Applied Intelligence, Proceedings of the International Conference on Industrial Engineering and Other Applications of Applied Intelligent Systems; 25–28 June 2018; Montreal, QC, Canada. Springer, Cham; 2018. Volume 10868, pp. 745–750.
68. Gragnaniello D, Sansone C, Poggi G, Verdoliva L. Biometric spoofing detection by a domain-aware convolutional neural network. In: Proceedings of the 2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS); 28 November 2016–1 December 2016; Naples, Italy. pp. 193–198.
69. Parzianello L, Czajka A. Saliency-guided textured contact lens-aware iris recognition. In: Proceedings of the 2022 IEEE/CVF Winter Conference on Applications of Computer Vision Workshops (WACVW); 4–8 January 2022; Waikoloa, HI, USA. pp. 330–337.
70. Chen C, Ross A. A multi-task convolutional neural network for joint iris detection and presentation attack detection. In: Proceedings of the 2018 IEEE Winter Applications of Computer Vision Workshops (WACVW); 15 March 2018; Lake Tahoe, NV, USA. pp. 44–51.
71. Raju MH, Lohr DJ, Komogortse O. Iris print attack detection using eye movement signals. In: Proceedings of the 2022 Symposium on Eye Tracking Research and Applications; 8–11 June 2022; Seattle, WA, USA. pp. 1–6.
72. Fang M, Damer N, Boutros F, et al. The overlapping effect and fusion protocols of data augmentation techniques in iris PAD. Machine Vision and Applications 2022; 33(1): 1–21. doi: 10.1007/s00138-021-01256-9
73. Pala F, Bhanu B. Iris liveness detection by relative distance comparisons. In: Proceedings of the 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW); 21–26 July 2017; Honolulu, HI, USA. pp. 664–671.
74. Poster D, Nasrabadi N, Riggan B. Deep sparse feature selection and fusion for textured contact lens detection. In: Proceedings of the 2018 International Conference of the Biometrics Special Interest Group (BIOSIG); 26–28 September 2018; Darmstadt, Germany. pp. 1–5.
75. Fang M, Damer N, Boutros F, et al. Iris presentation attack detection by attention-based and deep pixel-wise binary supervision network. In: 2021 IEEE International Joint Conference on Biometrics (IJCB); 4–7 August 2021; Shenzhen, China. pp. 1–8.
76. Li Y, Lian Y, Wang J, et al. Few-shot one-class domain adaptation based on frequency for iris presentation attack detection. In: Proceedings of the ICASSP 2022—2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP); 23–27 May 2022; Singapore, Singapore. pp. 2480–2484.
77. Luo Z, Wang Y, Liu N, Wang Z. Combining 2D texture and 3D geometry features for reliable iris presentation attack detection using light field focal stack. IET Biometrics 2022; 11(5): 420–429. doi: 10.1049/bme2.12092
78. Sequeira AF, Sliva W, Pinto JR, et al. Interpretable biometrics: Should we rethink how presentation attack detection is evaluated? In: Proceedings of the 2020 8th International Workshop on Biometrics and Forensics (IWBF); 29–30 April 2020; Porto, Portugal. pp. 1–6.
79. El-Din YS, Moustafa MN, Mahdi H. Deep convolutional neural networks for face and iris presentation attack detection: Survey and case study. IET Biometrics 2020; 9(5): 179–193. doi: 10.1049/iet-bmt.2020.0004
80. Galbally J, Marcel S, Fierrez J. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. IEEE Transactions on Image Processing 2013; 23(2): 710–724. doi: 10.1109/TIP.2013.2292332
81. Choudhary M, Tiwari V, Venkanna U. Iris liveness detection using fusion of domain-specific multiple BSIF and DenseNet features. IEEE Transactions on Cybernetics 2022; 52(4): 2370–2381. doi: 10.1109/TCYB.2020.3005089
82. Khade S, Ahirrao S, Phansalkar S, et al. Iris liveness detection for biometric authentication: A systematic literature review and future directions. Inventions 2021; 6(4): 65. doi: 10.3390/inventions6040065
83. Kohli N, Yadav D, Vatsa M, et al. Synthetic iris presentation attack using iDCGAN. In: Proceedings of the 2017 IEEE International Joint Conference on Biometrics (IJCB); 1–4 October 2017; Denver, CO, USA. pp. 674–680.

84. Yadav S, Ross A. CIT-GAN: Cyclic image translation generative adversarial network with application in iris presentation attack detection. In: Proceedings of the 2021 IEEE/CVF Winter Conference on Applications of Computer Vision (WACA); 3–8 January 2021; Waikoloa, HI, USA. pp. 2411–2420.
85. CASIA iris database V4. Available online: http://biometrics.idealtest.org/dbDetailForUser.do?id=14#/ (accessed on 9 March 2022).
86. Gupta P, Behera S, Vatsa M, Singh R. On iris spoofing using print attack. In: Proceedings of the 2014 22nd International Conference on Pattern Recognition; 24–28 August 2014; Stockholm, Sweden. pp. 1681–1686.
87. Fierrez J, Ortega-Garcia J, Toledano DT, Gonzalez-Rodriguez J. Biosec baseline corpus: A multimodal biometric database. Pattern Recognition 2007; 40(4): 1389–1392. doi: 10.1016/j.patcog.2006.10.014
88. Doyle JS, Bowyer KW. Robust detection of textured contact lenses in iris recognition using BSIF. IEEE Access 2015; 3: 1672–1683. doi: 10.1109/ACCESS.2015.2477470
89. Doyle JS, Bowyer KW, Flynn PJ. Variation in accuracy of textured contact lens detection based on sensor and lens pattern. In: Proceedings of the 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS); 29 September 2013–2 October 2013; Arlington, VA, USA. pp. 1–7.
90. WVU mobile iris spoofing dataset. Available online: https://iab-rubric.org/resources/biometric-datasets/iris (accessed on 1 November 2023).
91. Proença H, Filipe S, Santos R, et al. The UBIRIS.v2: A database of visible wavelength iris images captured on-the-move and at-a-distance. IEEE Transactions on Pattern Analysis and Machine Intelligence 2010; 32(8): 1529–1535. doi: 10.1109/TPAMI.2009.66
92. Trokielewicz M, Czajka A, Maciejewicz P. Iris recognition after death. IEEE Transactions on Information Forensics and Security 2019; 14(6): 1501–1514. doi: 10.1109/TIFS.2018.2881671
93. Mostofa M, Mohamadi S, Dawson J, Nasrabadi NM. Deep GAN-based cross-spectral cross-resolution iris recognition. IEEE Transactions on Biometrics, Behavior, and Identity Science 2021; 3(4): 443–463. doi: 10.1109/TBIOM.2021.3102736
94. Regulation (EU) 2016/679 of the European parliament and of the council. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679 (accessed on 6 October 2022).
95. Bowyer KW, Hollingsworth K, Flynn PJ. Image understanding for iris biometrics: A survey. Computer Vision and Image Understanding 2008; 110(2): 281–307. doi: 10.1016/j.cviu.2007.08.005
96. Fu B, Damer N. Towards explaining demographic bias through the eyes of face recognition models. In: Proceedings of the 2022 IEEE International Joint Conference on Biometrics (IJCB); 10–13 October 2022; Abu Dhabi, United Arab Emirates. pp. 1–10.
97. Fang M, Damer N, Kirchbuchner F, Kuijper A. Demographic bias in presentation attack detection of iris recognition systems. In: Proceedings of the 2020 28th European Signal Processing Conference (EUSIPCO); 18–21 January 2021; Amsterdam, Netherlands. pp. 835–839.