



A survey on data-driven iris spoof detectors: state-of-the-art, open issues and future perspectives

Palak Verma¹ · Arvind Selwal¹ · Deepika Sharma¹

Received: 25 May 2022 / Revised: 3 August 2022 / Accepted: 23 September 2022 /
Published online: 10 October 2022

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract

In the modern era of computing, the iris-based biometric systems are gaining significant attention for secured and automatic human authentication. However, past decades have witnessed numerous spoofing assaults on these iris-based recognition systems where an attacker impersonates an exact replica of biometrical information of the genuine user. Particularly, these direct attacks are targeted on the iris sensor module of the biometric system by presenting the fake artefacts of a bonafide iris trait. With the emergence of data-driven paradigm (i.e. handcrafted feature learners such as support vector machine (SVM), decision tree (DT), k-nearest neighbor (KNN), ensembles, etc. or automatic image features extraction-based classifiers such as convolutional neural networks (CNN), generative adversarial networks (GAN)), mitigating these iris spoof attacks has become comparatively an easier and accurate task of computer vision. An iris spoof detector (ISD) is a mechanism through which the vitality of a presented iris trait is measured intelligently by classifying it as genuine or counterfeit. In this study, we explicate a taxonomy-based comparative analysis of state-of-the-art (SOTA) ISDs that employ machine learning or deep learning-based approaches. We expound a novel taxonomy for classifying ISDs based on underlying criterion such as feature type, learning algorithm, pre-trained models, data augmentation, hybrid, etc. Furthermore, we investigate and analyze various benchmark datasets employed in the various data-driven iris spoof detectors (D²ISD). We also illustrate prominent performance evaluation protocols that are widely adopted in the SOTA approaches. Though, pioneer contributions related to D²ISD is reported in the literature, but several potential open research problems still exist, that requisite a futuristic attention of the investigators in this active field of research.

Keywords Iris recognition · Spoof attacks · Spoof detectors · Data augmentation · Handcrafted features · CNN · Transfer learning

✉ Palak Verma
pv07111998@gmail.com

¹ Department of Computer Science and Information Technology, Central University of Jammu, Samba 181143, India

1 Introduction

In today's era of digitization, biometric-based recognition systems [70] are replacing traditional methods of human authentication. These systems recognize human on the basis of single biometrical modalities such as gait, palm print, fingerprint, voice, face, iris, etc. or fusion of multiple biometric traits [80]. Fig. 1 illustrates a historical evolution of various biometrical traits that are deployed for human recognition over the decades. The prominent biometrical characteristics [46, 47] are widely used as these possess certain properties such as uniqueness, universality, acceptability, measurability and reliability. Among all, iris recognition [45] has become one of the most reliable techniques for human authentication due to its exceptional features as it offers in terms of accuracy, performance, and processing speed. Iris spoof detection is a significant image classification [7–13] problem that is very prevalent now a days. The iris' visual texture forms during fetal development and stabilizes over the first two years of life; however, the pigmentation changes over time. These complex iris textures carry unique information that can assist in personal identification.

Further, visible light or near infrared (NIR) illuminated sensors could be used to capture a high-contrast image of an individual's iris to pick up distinctive patterns that are not visible to the naked eyes. Daugman [24] proposed the first pioneer commercial tool thorough investigation of the iris in the field of biometric identification, which is extensively applied in many real-time systems. Iris codes are proven to be unique not just across unrelated persons but also between the twins and the right and left irises of the same person. Due to its measurability and accuracy, iris-based recognition systems have called forth its wide-scale deployment for applications areas such as airport security, border control, smart phones authentication, forensic investigations, and national identification projects. However, despite of numerous advantages, iris biometric systems are susceptible to a variety of attacks. In a typical biometric-based system, Ratha et al. in 2001 [67] identified eight vulnerable spots. Among all, spoof or presentation attacks are most widely and easier attempted at the sensor level to various types that can degrade the overall performance of system. To countermeasure these attacks on various biometric recognition systems (i.e., fingerprint, face, iris, etc.) a variety of solutions are available [1, 15, 30, 33, 44, 48, 58, 72, 73, 75–77, 86] that may be generally classified as:

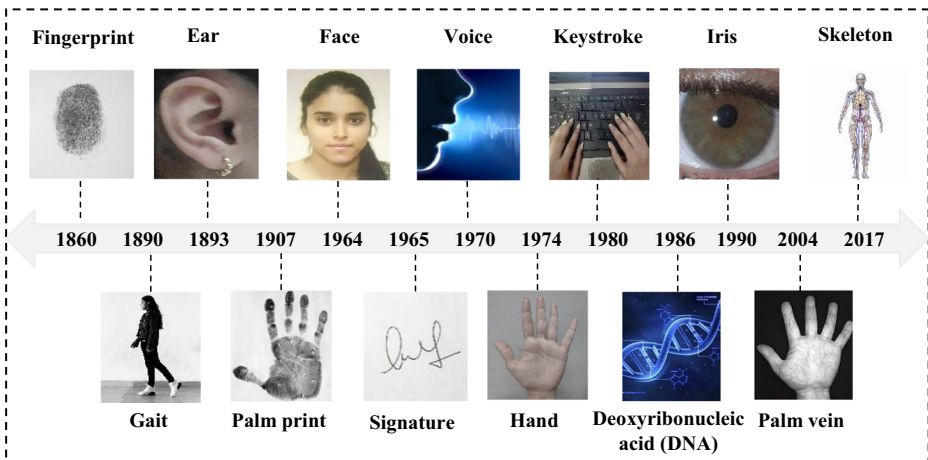


Fig. 1 A timeline showing the evolution of biometrical traits over the decades

hardware or data-driven based approaches. For the hardware-based methods to distinguish between a real and counterfeit iris trait, we utilize an extra sensing device. Due to its limited capabilities to tackle different types of iris spoof attacks and additional cost of extra hardware device, these approaches are not widely used.

With the emergence of machine learning algorithms and contemporary paradigms shift to deep learning-based CNN models, a more accurate as well as robust solution for iris spoof detection is possible. Figure 2 depicts the developments of various iris spoof detection mechanisms during last couple of years. It can be seen that significant contributions in the field of ISDs has led to a clear paradigm shift from traditional feature descriptors and classifiers to the most recent deep CNNs. The literature exhibits a significant growth in this active field of research where the pioneer contributions from several investigators are reported. Earlier, Czajka and Bowyer [21] (2018) presented a well-structured study that cover a review of various aspects of iris attacks, iris anti-spoofing datasets and software-based solutions. However, this study covers many key domains but limited attention has been put forward to latest deep learning (DL)-based approaches and it includes SOTA approaches up to 2017. In another study, Agarwal and Jalal [2] (2020) presented a brief analysis of iris attacks, datasets and hardware-based as well as software-based approaches. It may be analysed that some of the significant aspects related to data-driven approaches are missing in this study. As majority of the approaches in recent times rely on two important characteristics i.e., robustness of the features and classifiers, a more detailed analysis of recent SOTA ISD is requisite.

Therefore, to address these gaps in the existing review studies, our work aims to present an in-depth and a systematic investigation of D²ISD SOTA approaches through the proposed taxonomy. The goal of our analysis is to compliment the aforementioned existing studies by including more recent aspects that are related to data-driven approaches (i.e., recent benchmark datasets, handcrafted features-based detectors, deep learning-based models, transfer learning, hybrid methods, evaluation protocols, etc.).

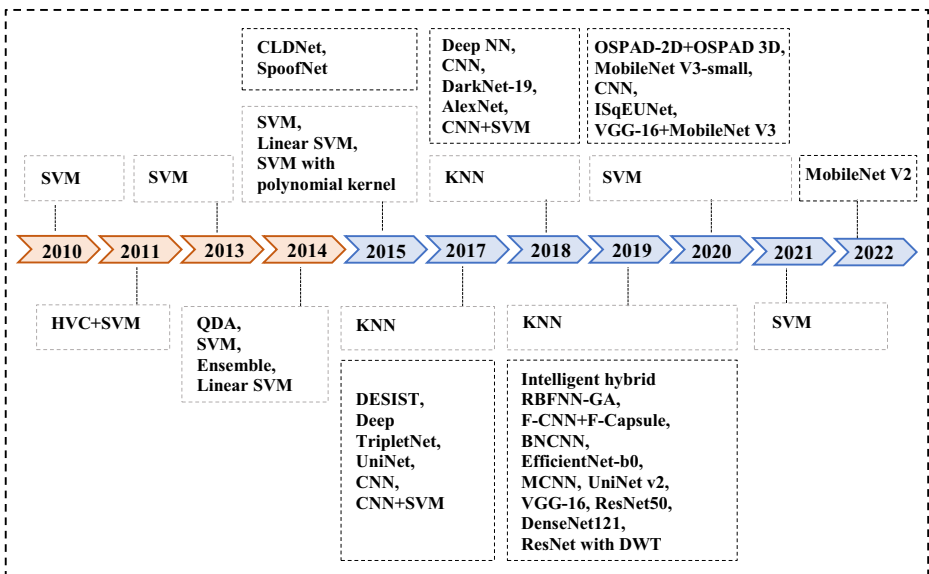


Fig. 2 An illustration of developments and progression of ISDs

The foremost contributions of this article may be stated as follows:

- We present a taxonomy for the classification of various iris spoof detection approaches.
- We expound an in-depth study and analysis of SOTA data-driven based iris anti-spoofing mechanisms.
- A summary of several benchmark iris anti-spoofing datasets that are frequently used for evaluating the presentation attack detection (PAD) algorithms is presented.
- We present a comparative analysis of some most recent iris SOTA mechanisms through various standard evaluation metrics.
- At last, we identify several open research challenges from this study and suggest some viable solutions that may provide future directions to the researchers.

The remainder of the article is structured as per the roadmap shown in Fig. 3. Section 2 introduces the study’s scope and coverage. A brief overview of iris presentation attack instruments is provided in Section 3. A detailed review and analysis of D²ISD approaches as well as our proposed taxonomy is presented in Section 4. Performance evaluation protocols and a comparative analysis of recent SOTA approaches are put forward under Section 5.

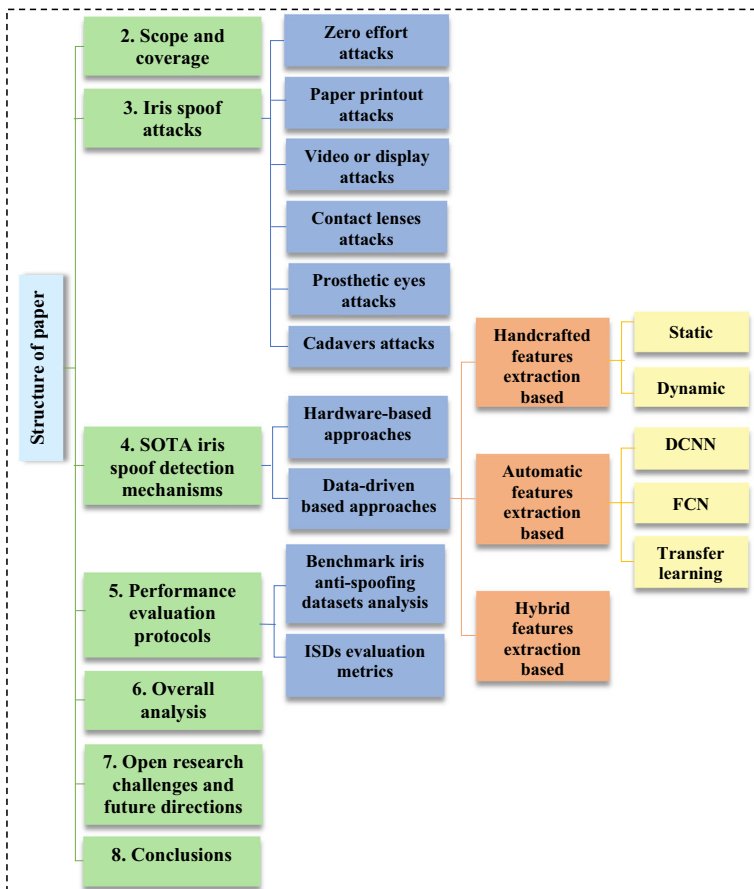


Fig. 3 A roadmap of the overall article

Section 6 includes the overall analysis of D²ISD approaches. The major identified open problems along with suggested remediation are provided in Section 7. Section 8 provides concluding remarks and the future direction of this investigation. Some symbols and acronyms used in the article are listed in Table 8 under Appendix section.

2 Scope and coverage

The key motivation behind this study is to present a thorough analysis of recent SOTA iris anti-spoofing algorithms from 2010 to 2022. Henceforth, we explored more than 150 articles from reputed repositories such as: IEEExplore, Scopus, Web of science, ResearchGate, etc. Thereafter, an intense examination of the literature, led us to finally select a total of 97 articles that are consequently included in the study. Our survey is based on the most recent literature that is advocated by Fig. 4a, where it is meticulously seen that majority of the articles are selected from the period between 2018 to 2022. It is also observed that the pioneer contributions in the field of iris anti-spoofing mechanisms are published in the top-rated transactions or journals that are supported by Fig. 4b, where articles type distribution of the study is depicted. Figure 4c indicate that the majority of the reviewed iris spoof detection approaches are based on static features extraction-based mechanisms. The publisher wise distribution of the selected articles for our analysis is depicted in Fig. 4d.

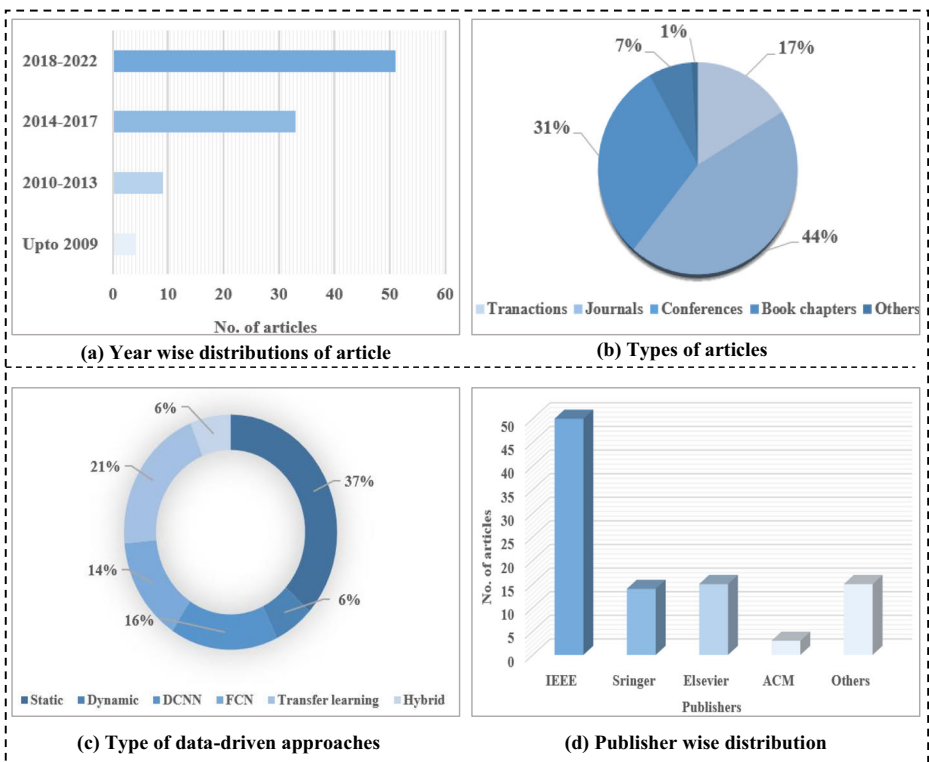


Fig. 4 Overall distribution of D²ISD literature (a) Year wise distributions of article (b) Types of articles (c) Type of data-driven approaches (d) Publisher wise distribution

3 Iris spoof attacks

A spoof attack, as well-defined by ISO/IEC 30107 [16], is a presentation to a biometric model's sensor that aims to influence these systems to make false identification determinations. The process is used to subvert an iris-based biometric system by presenting a genuine biometric artefact of the legitimate user to the sensor to obtain an illegitimate access to data, either by imitating a verified user or by obscuring the identity of attackers. Fig. 5 illustrates a broad categorization of these attacks. Usually, contact lenses (CL), paper printouts (PP) and plastic artefacts are used to subvert the iris recognition systems. Thus, the relevance of effective security measures against these invasions become paramount. In the succeeding subsection, we briefly deliberate some common spoof attacks on iris biometrics [37].

3.1 Zero effort attacks

Generally, these attacks are carried out by the attacker's own iris. Hence, no artefacts or knowledge about the legitimate user under assault is required. The success of an attack is determined by the false match rate (FMR), which is computed as the percentage of times the attacker's iris pattern is successfully matched with that of a valid user. The FMR is associated to the false non-match rate (FNMR), which occurs when the system rejects legitimate users. The higher the FMR, the more vulnerable the system is to this attack. As most of the iris recognition systems have a low FMR, impact of these attacks is expected to be minimal.

3.2 Paper printout attacks

A legitimate iris is directly presented to the iris recognition system's sensor via a printed photo or digital image. Paper printout attacks are the easiest to spoof as it is moderately easier to access an iris image from the headshots of users on social networking sites (e.g., Twitter, Instagram, Picasa web, and etc.), and it is comparatively easier to print superior quality iris photographs using cameras and ink printers. A sample depiction of paper printout attack is shown in Fig. 6a.

3.3 Video or display attacks

Video assaults make it possible to imitate both the dynamic information as well as its static patterns of an iris. Figure 6b illustrates an iris spoof attack via replaying a video. The expected

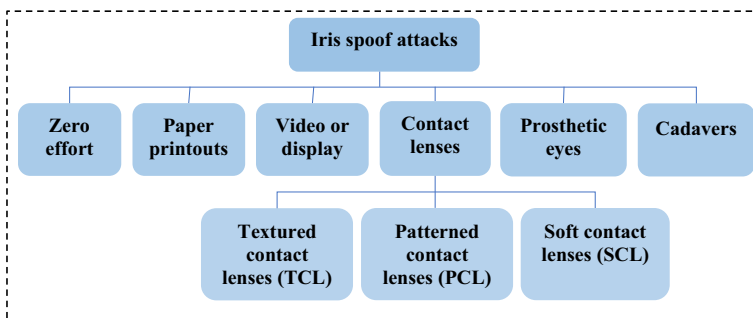


Fig. 5 A broad categorization iris spoof attacks

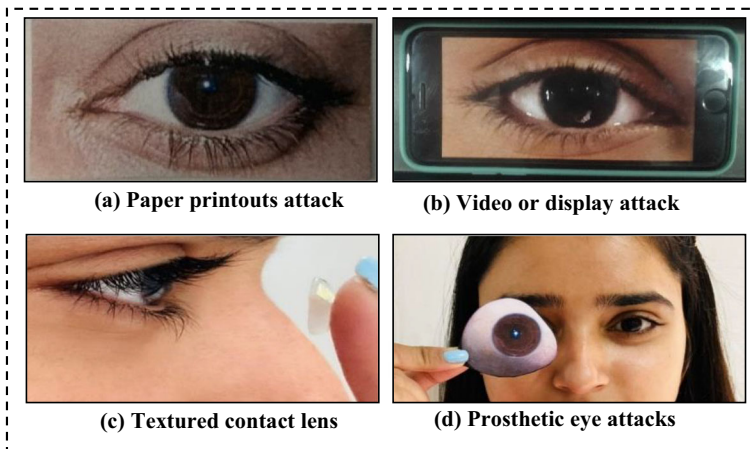


Fig. 6 Few instances of iris presentation attacks (a) Paper printouts attack (b) Video or display attack (c) Textured contact lens attack (d) Prosthetic eyes attack

impact of these attacks is considerably more as high-quality graphic may reproduce digital images and videos. Therefore, it enables iris spoof attacks based on visible spectrum imaging a challenging task but not as much in case of NIR sensors in commercial systems.

3.4 Contact lens attacks

The contact lenses such as textured, patterned or soft could be used for two different types of attacks. The first is an impostor attack, in which the iris pattern of a valid user is imitated. The information required for these attacks is the iris pattern of a genuine user. The masquerade attack, often known as identity concealing, is the second type of attack, where the information of the user is not required. Figure 6c depicts a sample image of textured contact lens of a genuine user. These attacks demand a significant effort for either automatic iris spoof detection or human visual examination.

3.5 Prosthetic eyes attacks

The synthetically generated eyes (SYN) are exploited to imitate the characteristics of real eyes. Figure 6d illustrate a sample iris image of prosthetic eye. These techniques are extensively used for medical purposes ever since the twentieth century, and recent technologies for prosthetic fabrication allow for realistic replication of key characteristics of real eye. These attacks are rarely used by the adversaries and their detection by iris spoof detection methods based on image features is comparatively difficult.

3.6 Cadavers attacks

These attacks are carried out by presenting a deceased person's iris to a human authentication system's sensor. It is feasible to attain the post-mortem iris images using commercial iris sensor, and obtain a correct match rate between the samples even upto 30 days after death. However, there isn't any stated effective attack on the iris authentication systems employing cadaver eye.

4 State-of-the-art iris spoof detection mechanisms

In the previous section, we contemplated that iris recognition systems are vulnerable to a range of spoof attacks at the sensor level. These attacks make the sensor module incompetent of discriminating an authentic or a spoofed biometrical trait. An anti-spoofing mechanism [34] is essential to safeguard sensors from such assaults. Therefore, in this section we explore various countermeasures to presentation attacks (PAs) in iris recognition systems. We have proposed a taxonomy as shown in Fig. 7 that clearly classifies the PAD mechanism into two broad categories i.e., hardware-based and data-driven based approaches. In the following subsections, we examine the existing PAD approaches, including their key concepts, datasets deployed and performance measures.

4.1 Hardware-based approaches

Hardware-based approaches [26, 42, 63] are also called as sensor-based approaches, these may use an extra sensing device in count to the standard iris sensor to measure the physical (e.g., density of the eye tissues) and biological traits (e.g., textural pattern of iris) of the eye. The methods like multispectral imaging, 3D imaging, and electrooculography are used in this approach.

Although hardware-based approaches [20, 43, 53, 64] perform better in a known environment scenario but with an additional cost of further sensor that differentiate between live and fake iris images. As these methods mainly rely on some live characteristics (i.e., impedance, temperature, blood cells, image quality) of an iris image, therefore these approaches have been proved to be comparatively less robust to perform well in unknown environment scenario.

4.2 Data-driven-based approaches

To overcome the confines of contemporary hardware-based iris anti-spoofing techniques, a viable solution is to make use of machine learning-based algorithm. These approaches are

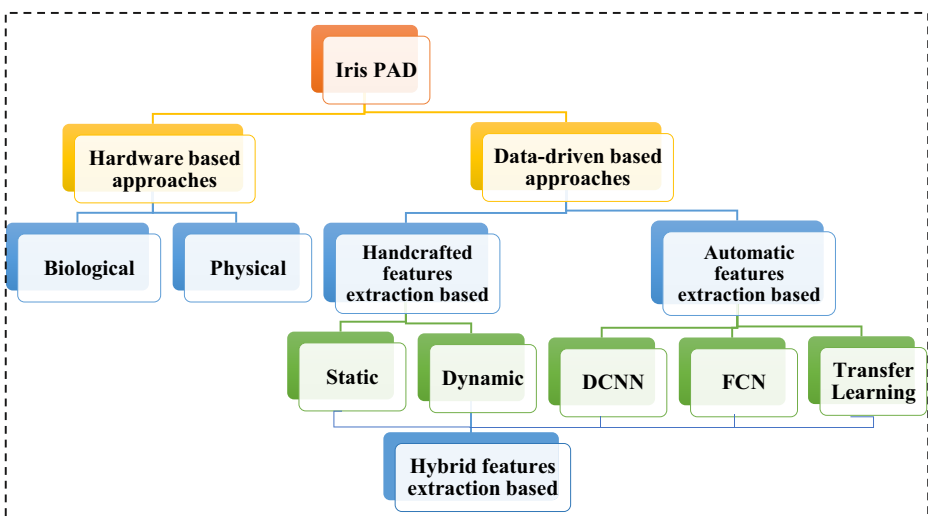


Fig. 7 Our proposed taxonomy of iris anti-spoofing methods

mainly based on learning a model by using a variety of handcrafted features from iris images. As these methods, requires training samples to build an iris anti-spoofing model, therefore these are called as data-driven approaches. In the case of data-driven based approaches, there are two significant notions namely: a classifier and a training dataset. One of the major concerns is the quality and diversity in the datasets (higher inter-class and low intra-class diversity) that are being provided to the system for training and testing purpose. The more the inter-class diversity and higher the quality, the better classification decision a system will be able to make. The process to understand the deployment of data-driven-based ISDs in human authentication system is shown in Fig. 8. Based upon the type of method used to extract features from iris images, data-driven approaches may be broadly classified in two categories: manually or automatic crafted features. In the following sub-sections, we present a detailed study and analysis of SOTA iris anti-spoofing methods that employ hand-crafted or automatic feature engineering process.

4.2.1 Handcrafted features extraction-based approaches

In these methods, distinctive features are extracted from iris images to train a classifier for building an iris anti-spoofing model. These may include some image characteristics, micro-textural, color, and statistical features. Among all, micro-textural features of iris images have been explored by majority of the researchers, mainly due to its capability to discriminate between both classes in more efficient manner. Another key aspect is to decide upon the number of samples acquired to build an anti-spoofing model. Hence, these approaches are further classified as static (a single image is used) or dynamic (multiple samples or a small video of iris trait is captured). Fig. 9 illustrates a generic framework for handcrafted features-based ISDs.

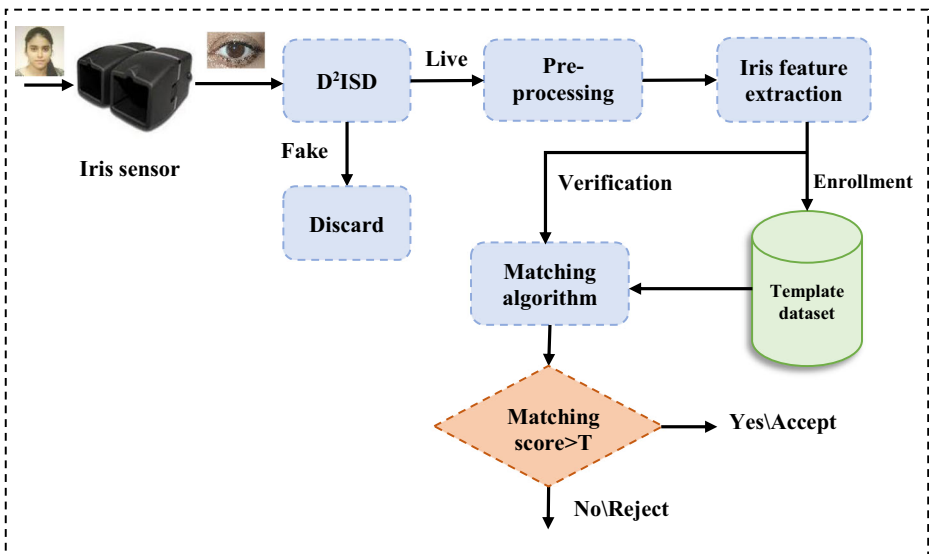


Fig. 8 A depiction of data-driven iris spoof detectors in human authentication system

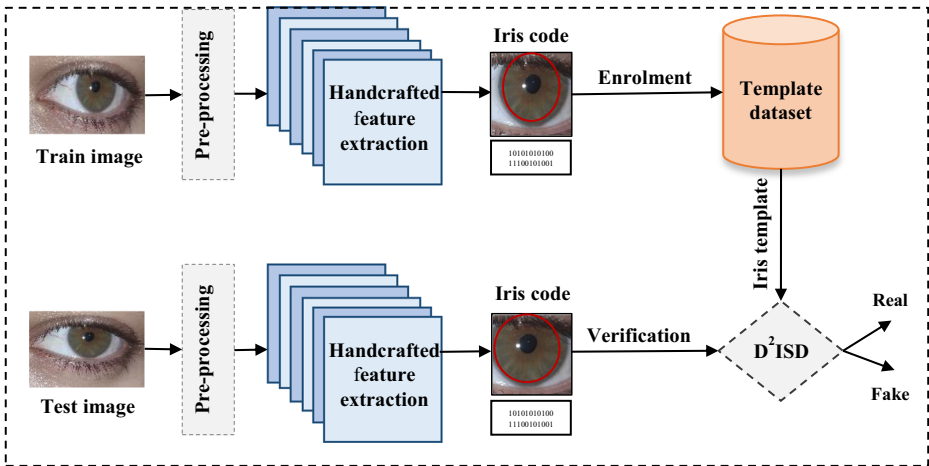


Fig. 9 A generic framework for handcrafted features-based D²ISD

Static features-based approaches These approaches only rely on features extracted from static images of the training dataset. The image features such as micro-textural properties, shape, color features and image quality are frequently explored by the researchers to learn a classifier that discriminate a given image to live or fake. The effectiveness of these iris spoof detection approaches relies on the appropriate robust feature set and a strong learner. Fig. 10 shows a timeline for various feature descriptors deployed in iris spoof detection mechanisms. In the following paragraphs, we present an investigation of various static software-based ISDs.

Earlier, Zhang et al. [94] propounded an iris spoof detection mechanism using scale-invariant feature transform (SIFT) and weighted-local binary patterns (W-LBP) feature descriptors. An SVM classifier is used to discriminate the genuine and artefact iris traits. Though, the experimental results in known attack scenario shows an excellent correct classification rate (CCR) of 99.14%, but the accuracy rate in unknown attack scenario is relatively low. Another solution for iris spoof detection is put forward by Zhang et al. [95] using SIFT descriptor for feature extraction and hierarchical visual codebook (HVC) with SVM for classification

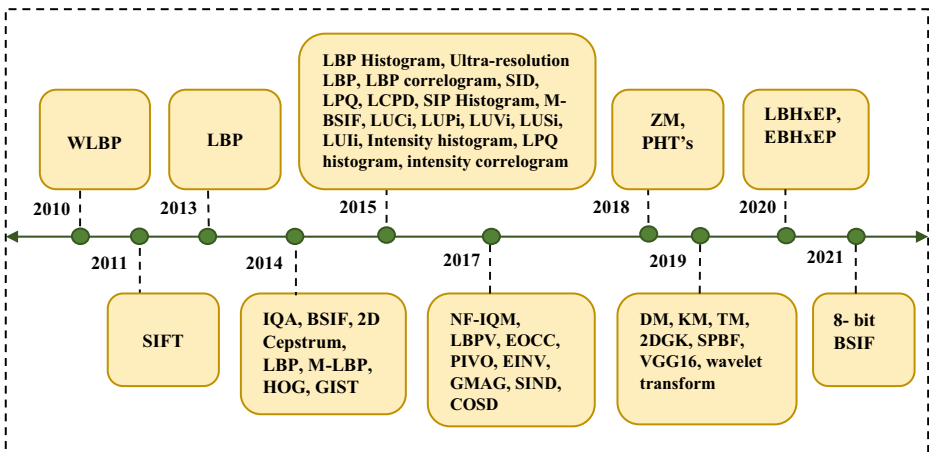


Fig. 10 A timeline of various image feature deployed in iris PAD mechanisms

purpose. To translate the distinct and robust texture primitives of genuine and counterfeit iris images, the HVC approach uses both LLC and vocabulary tree techniques. This approach lowers the vocabulary tree's dependence on upper-level coding and achieves low quantization error, sparsity, and capturing salient patterns. Other handcrafted features extraction-based PAD approaches using local binary patterns (LBP) as a feature extractor and SVM as a classifier have been deliberated by Kohli et al. [51] and Gragnaniello et al. [35]. Both the approaches show promising results in terms of accurately classifying the given iris image in two classes but a limited robustness of handcrafted features is observed in these mechanisms.

The concept of quadratic discriminant analysis (QDA) for classification is adopted by Galbally et al. [31]. Performance of the proposed technique is evaluated on ATVS-Fir, CASIA-IrisV1 and, WVU- synthetic iris database and analyzed a half total error rate (HTER) of 2.2% on iris-spoof and 2.1% on iris-synthetic. Another work by Raghavendra & Busch [62] utilize the capabilities of binarized statistical image features (BSIF) for statistical feature extraction and 2D cepstrum analysis for cepstral feature extraction. In this approach, a linear SVM classifier is used for classifying the iris images as real or fake. The suggested iris spoof detection mechanism has an exceptional average classification error rate (ACER) of 0% on ATVS-Fir dataset. Unravelling the effect on textured contact lens on iris recognition system Yadav et al. [89] proposed an approach using modified LBP with an ensemble learning. Whereas, Gupta et al. [38] introduced an iris spoof detection method using three different descriptors namely; LBP, Histogram of Oriented Gradient (HoG), global image descriptor (GIST) and an SVM is employed for classification.

Gragnaniello et al. [36] also addressed a generalized approach to counter liveness detection using LBP, SIFT, BSIF, scale invariant descriptor (SID), local contrast-phase descriptor (LCPD) and multi-resolution LBP descriptors to extract the features from a presented iris image and build a model using an SVM as classifier. The proposed approach achieves a comparable accuracy in most cases except when analyzed on IITD dataset. Meanwhile, Bhogal et al. [14] used non-reference image quality measures (NF-IQM) consisting of NIQE, BLIINDS-II, BIQAA, BRISQUE, DIIVINE, BIQI and a KNN learner is used in the proposed work and classification accuracy of 85.81% on best IQM combinations is achieved. Yang et al. [40] deliberated an iris vitality detection through regional features. These regional features seek the dispersal of the low-level features extracted from neighboring regions and high-level feature distribution that provides profound insight into the distribution in a different region. The proposed approach uses two models i.e., spatial pyramid and relational measure to construct regional features that seek the feature distributions in a region with varying size and shape respectively. Then fusing the outcomes, of the two models at the score level and using an SVM classifier it is decided whether it is a live or a counterfeit iris image. The proposed method is evaluated on four benchmark iris anti-spoofing datasets i.e., Warsaw, Clarkson, MobBIOfake and Notre Dame consisting of live iris images and fake iris that are captured by simulating two different attacks on iris recognition i.e., contact lenses and printout attacks in NIR illumination and visible light. The approach demonstrates that regional features attain analogous performance to SOTA features with precise iris localization and a appropriate pre-processing with reliable feature selection but this approach resulted in a high error rate.

Another robust scheme using Multi-scale BSIF and linear SVM is adopted by Raghavendra and Busch [65], using a novel comparatively significant Visible Spectrum Iris Artefact (VSIA) database consisting of real and counterfeit samples captured by simulating five diverse range of attacks on iris recognition system. Extensive experimentation is carried out in this work and concludes that the proposed PAD scheme has an ACER of 0.29%. Similarly, using orthogonal

features a cross-sensor iris spoof detection technique is proposed by kaur et al. [50]. A rotational-invariant feature-set encompassing of polar harmonic transforms and Zernike moments that extracts local intensity variations for detection of iris presentation attacks is introduced. The KNN classifier is used for discriminating genuine and fake iris images. The presented system's performance is assessed using four publicly accessible iris spoofing datasets: IITD-CLI, IIS, Clarkson LivDet-Iris 2015, and Warsaw LivDet-Iris 2015. The detailed experiments show that proposed system detects iris spoofing assaults with an ease, even when multiple sensors are deployed, making the scheme ideal for commercial real-time applications. Another work on iris spoof detection using combination of KNN classifier and discrete orthogonal moments-based invariant feature-set comprising of Dual-Hahn, Tchebichef, Krawtchouk moments to capture local intensity distribution of the iris texture is adopted by Kaur [49]. To accommodate geometric alterations when images are taken in an uncontrolled environment, the orthogonal moment-based feature-set is made translation, rotation, and scale-invariant. The proposed method's performance is assessed using four publicly accessible databases: IITD-Contact Lens Iris, IITD Iris Spoofing, Clarkson LivDet 2015, and Warsaw LivDet 2015. Their results demonstrate that detecting iris spoofing improves the biometric system's reliability but the performance degrades when unknown spoofing attack is encountered.

Also, Ahmadi et al. [5] proposed an iris recognition method based on extracting the iris tissue features in 3 steps by using two dimensional Gabor kernel step filtering and polynomial filtering methods. A combination of radial basis function neural network (RBFNN) with genetic algorithm (GA) classifier is applied on iris feature vector for classification purpose. The proposed model is implemented on CASIS-Iris V3, UBIRIs V1 and UCI machine learning datasets. The two-performance metric, receiver operating characteristic (ROC) curve and equal error rate (EER) are used to access the proposed model and result show that the method is able to determine subsets of feature with superior classification accuracy, but it require a large memory space and is a complex approach. Agarwal et al. [4] and Agarwal et al. [3] propounded new descriptors namely; Local binary hexagonal extrema pattern (LBHxEP) and Enhanced binary hexagonal extrema pattern (EBHxEP) respectively. An SVM classifier has been used in both of these approaches and their performance is evaluated on IITD-CLI, ATVS-Fir datasets and it is inferred that EBHxEP has lower average error rate (AER) as compared to LBHxEP. Recently, Dronky et al. [25] bring forward a method where 8-bit BSIF with an SVM learner is applied for liveness detection. In order to determine if the segmentation stage in liveness detection may be eliminated for a better applicability in real-life scenarios, the method's effectiveness is evaluated on four distinct datasets in both segmented and unsegmented modes. The outcomes demonstrated that the technique was capable of accurately identifying various assaults. In both techniques of employing NIR datasets, the classification rate for assaults like plastic, synthetic, and print is approximately 100%, however using the entire image improves the ability to identify print attacks in datasets using visible light.

Dynamic features-based approaches In comparison to static approaches, the dynamic features-based mechanisms utilize multiple image samples of a user acquired during different intervals of time (i.e., a video). Thereafter, features are extracted from multiple image samples to train the anti-spoofing model. However, these methods are comparatively better in accuracy but are computational inefficient due to enlarged training overhead. Few studies have explored the notion of dynamic iris detection that are discussed in the succeeding paragraph.

Raja et al. [66] suggested an approach based on decomposing the images into Laplacian pyramid of various scale and the obtain frequency response in different orientations. The extracted features in the proposed approach are classified using SVM in addition to a polynomial kernel. The proposed technique is further extended with majority voting to classify the artefact for video-based iris recognition systems. Performance of the proposed method is measured on presentation attack video iris database (PAVID) and LivDet Iris 2013 warsaw dataset. And, ACER of 0.64% and 1.37% is measured on PAVID and LivDet Iris 2013 warsaw respectively. Whereas, Rigas and Komogortsev [69] propounded a methodology relying on eye movement traits for the extraction of features indicating iris presentation attack. Due to the artificial nature of the iris paper prints, the devised system is capable of statistically modelling the basic distortions occurring in the eye movement signals during iris print assaults. The suggested technique employs an SVM classifier with a rbf kernel, and it is evaluated using a database of eye movement signals from 200 participants that includes both genuine eye movement signals and signals from the print attack. With an average classification rate (ACR) of 96.5% and an error rate (EER) of 3.4%, the recommended approach also offers strong detection performance. The subjects' heads are gently stabilized by the use of a headrest, and the trials are conducted in a controlled setting with no outside factors. However, more recent methods of remote eye monitoring provide a different level of head movement. Additionally, some physical, behavioral, and physiological factors (such as weariness) have an effect on the observed eye movements, resulting in fixational signals that are more positionally variable than usual. Recently, Fang et al. [28] put forward a robust iris PAD method that combines 2D (textural) and 3D (shape) information. The convexity of the observed iris surface is next assessed using the normal vector map to determine whether or not the subject is wearing textured contact lenses. The extensive testing with the NDCLD'15 and NDIris3D datasets shows that the proposed method outperforms the existing iris PAD methods in various open set testing scenarios.

From the comparative analysis of handcrafted features-based approaches as specified in Table 1 it can be inferred that there is a limited robustness in the handcrafted features and in the pioneer contributions the LBP descriptor is used may be because of its computational simplicity or its robustness to monotonic grey-scale changes. It may also be analyzed that SVM is one of the most widely used classifier as it works relatively well in most cases and is more effective in high dimensional spaces. Moreover, IIITD-CLI is one of the extensively used dataset in this approach with an accuracy ranging from 72.96% to 99.8%.

4.2.2 Automatic features extraction-based approaches

Manual feature extraction is exploited in handcrafted feature-based approaches, where image descriptors such as BSIF and LBP are used to represent discriminating characteristics. The extraction procedure becomes challenging due to variations in the collected iris images, and there is an inherent issue in these techniques to pre-fix the number of features. The automated feature-based approaches help to address some of these issues. These approaches are also known as deep feature engineering; it constructs new features from the existing data that are used to train the model. Newer DL methods typically use automated feature extraction as they require a large training sample to achieve the high detection accuracy. The concepts of data augmentation and transfer learning could be used to generate larger datasets.

Table 1 A comparative analysis of handcrafted features-based ISDs

Paper id	Year	Author(s)	Approach (static or dynamic)	Features descriptor (s)	Classifier	Datasets	Performance	
							Known	Unknown
H1	2010	Zhang et al. [94]	Static	SIFT and W-LBP descriptor	SVM	Proprietary database	Mixed Database CCR: 99.14%	Cross-camera validation CCR: 88.05%
H2	2011	Zhang et al. [95]	Static	SIFT	HVC and SVM	Proprietary database	CCR for single DB: Print=99.61%, Contact=99.64%, Synthetic=99.76%, Plastic=99.79% Verification accuracy at lens type N-N	CCR for cross-DB: Print=89.04%, Contact=66.32%, Synthetic=89.96%, Plastic=98.94% Cross-sensor Verification accuracy at lens type N-N
H3	2013	Kohli et al. [51]	Static	LBP	SVM	IIITD Contact lens	Cogent=98.9% Vista=99.8%	accuracy at lens type N-N: 97.9%
H4	2014	Galbally et al. [31]	Static	Full reference (FR) IQA and Non-reference (NR) IQA	QDA	ATVS-Fir, CASIA-IrisV1, WVU- Synthetic Iris DB	HTER: Iris-spoof=2.2%, Iris-synthetic=2.1%	—
H5	2014	Raghavendra & Busch [62]	Static	Statistical features using BSIF and Cepstral features using 2D Cepstrum analysis	Linear SVM	ATVS-Fir	ACER=0%	—
H6	2014	Gragmiello et al. [35]	Static	LBP	Linear SVM	MobBIOfake MICHE database	HTER of LBP (o-basic) MobBIOfake: on image=4.75% on residual=0.00%	—
H7	2014	Yadav et al. [89]	Static	Modified LBP	Ensemble	IIIT-D contact lens iris DB, Notre Dame 2013 contact lens detection	Multi-sensor validation:	—

Table 1 (continued)

Paper id	Year	Author(s)	Approach (static or dynamic)	Features descriptor (s)	Classifier	Datasets	Performance
							Known Unknown
H8	2014	Gupta et al. [38]	Static	LBP, HOG and GIST	SVM	IIITD iris spoofing database	Total lens classification result on: IIITD combined = 72.96%, ND III = 73.20% Classification accuracy type 2-class: Original vs Print+Scan LBP = 100%, HoG = 97.22%, GIST = 65.19%, LBP+HoG = 92.32% Original vs Print+Capture LBP = 95.26%, HoG = 81.04%, GIST = 58.66%, LBP+HoG = 72.38%
H9	2015	Graganiello et al. [36]	Static	LBP, SIFT, SID, BSIF, LCPD, Multi-resolution LBP	Linear SVM	Warsaw, ATVS, Notre Dame and IIITD	Error Rate in case of SID: for both Warsaw and ATVS = 0%, ND I = 0.1% ND II = 0.0%, IIT Cogent = 6.2%, IIT Vista = 3.5%
H10	2015	Raja et al. [66]	Dynamic	Laplacian pyramid and frequency responses in	SVM with a polynomial kernel	PAVID and LivDet Iris 2013 Warsaw Dataset	ACER: PAVID = 0.64%, LivDet Iris 2013 Warsaw = 1.37%

Table 1 (continued)

Paper id	Year	Author(s)	Approach (static or dynamic)	Features descriptor (s)	Classifier	Datasets	Performance
H11	2015	Yang et al. [40]	Static	dissimilar orientations LBP histogram, LBP correlogram, Intensity histogram, intensity correlogram, LPQ histogram, LPQ, SID histogram	SVM	Clarkson, Warsaw, Notre Dame, MobBIOfake	Score level fusion: Mean classification error rate (MCER): Clarkson=2.43%, Warsaw=1.05%, Notre Dame=0.41%, MobBIOfake=2.40% ACER: VISA =0.29% on attack1 and 0% on remaining 4 attacks, ATVS Fir=0.00%, Mobilive 2014=0.0%, LivDet-Iris 2013 Warsaw=1.27% Maximum ACR=96.5% and minimum EER=3.4% Best IQM combinations: Classification accuracy=85.81% Total CCR after fusion: IIITD-CLJ=98.49%, IIS=96.93%, Max CCR for feature set DM+KM+TM
H12	2015	Raghavendra and Busch [65]	Static	Multi-scale Binarized Statistical Image Features (M-BSIF)	Linear SVM	VISA, ATVS Fir, Mobilive 2014, LivDet-Iris 2013 Warsaw	
H13	2015	Rigas and komogortsev [69]	Dynamic	LUC, LUP, LUV, LUS, LUI	SVM (gaussian rbf kernel)	Proprietary database	
H14	2017	Bhagal et al. [14]	Static	NF-IQM (NIQE, BLIINDS-II, BIQAA, BRISQUE, DIVINE, BIQI)	KNN	ATVS-Fir	
H15	2018	Kaur et al. [50]	Static	ZM, PHT's (PCET, PCT, PST)	KNN	IIITD-CLJ, IIS, Warsaw LivDet 2015, Clarkson LivDet 2015	

Table 1 (continued)

Paper id	Year	Author(s)	Approach (static or dynamic)	Features descriptor (s)	Classifier	Datasets	Performance	
							Known	Unknown
H16	2019	Kaur [49]	Static	Discrete orthogonal moments-based features (DM/KM/TM)	KNN	IIITD-CLI, IIS, Warsaw LivDet 2015, Clarkson LivDet 2015	Warsaw LivDet 2015=96.98%, Clarkson LivDet 2015=98.56% Total CCR after fusion: IIITD-CLI=98.56%, IIS=99.28%, Warsaw LivDet 2015=99.39%, Clarkson LivDet 2015=99.68%	is in case of IIITD-CLI dataset in S-S=100% Cross-sensor evaluation: Max CCR for feature set DM+KM+TM is in case of IIITD-CLI dataset in S-S and T-T=100%
H17	2019	Ahmadi et al. [5]	Static	2-DGK, SF, PF	Intelligent hybrid RBFNN-GA	CASIS-Iris V3, UBIRs V1 and 3 datasets from UCI machine learning repository	Accuracy rate: CASIS-Iris V3 after 300 iterations=99.9914%, UBIRs V1 after 300 iterations=99.9889%, UCI after 200 iteration on Breast cancer, Iris flower & Wine=99.98%	—
H18	2020	Agarwal et al. [4]	Static	LBHxEP	SVM	IIITD-CLI, ATVS-Fir	AER: IIITD-CLI=4.8% and 1.2%, ATVS-Fir=1.8%	—
H19	2020	Agarwal et al. [3]	Static	EBHxEP	SVM	IIITD-CLI, ATVS-Fir	AER: —	—

Table 1 (continued)

Paper id	Year	Author(s)	Approach (static or dynamic)	Features descriptor (s)	Classifier	Datasets	Performance
H20	2020	Fang et al. [28]	Dynamic	2D (textural features) by BSIF and 3D (shape) by photometric stereo methods	OSPAD-2D (Ensemble) + OSPAD-3D (Normal maps estimated from photometric stereo)	NDCLD'15 and NDIris3D	IIITD-CU=3.9% and 0.58%, ATVS-FII= 1.6% BPCR on NDIris3D when OSPAD-fusion is done: LG4000=4.12% AD100=5.92% Cross sensor BPCR when trained on irregular set and tested on regular set=8.87%
H21	2021	Dronky et al. [25]	Static	8-bit BSIF	SVM	MobBIOfake CASIA iris Syn, Clarkson 2013, CASIA-Iris-Fake	CCR for Clarkson 2013 DB: Phase 1 s=91.6667% u=67% Residual filter 1 s=93.3333% u=75.6667% Residual filter 2 s=67% u=85.3333% Sobel filter s=86.3333% u=77%

Deep convolution neural network (DCNN)-based approaches The emergence of deep neural networks, facilitates the task of computer vision, is comparatively easier than traditional handcrafted feature-based mechanisms. The DL-based approaches are frequently employed for counter measuring iris spoofing attacks since the year 2014. A series of benchmark DCNN models such as Inception [81], VGG-16 [79], EfficientNet [82], ResNet50 [39], etc. have been developed that are trained on millions of images from ImageNet dataset. A DCNN model may be viewed as a stacked layered architecture of alternating sequence of convolutional, pooling and drop out layers. A generic architecture of DCNN model employed for iris anti-spoofing is depicted in Fig. 11.

The first $N-1$ layers of the model extract deep level features and the last layer perform the task of classification. As DL-based models have been proved as a powerful tool for image classification, therefore these models are recently explored to countermeasure iris spoof attacks. The further analysis are focused on the analysis of DL-based ISDs. Earlier, Silva et al. [78] propounded an approach to detect three-class iris contact lens detection i.e., textured lens, soft contact lens and no lenses based on deep image representations by means of learning weights named as CLDNet. Additionally, a CNN model with a fully connected layer is used to build deep image representation with softmax regression to classify the images. The proposed method is evaluated on Notre Dame 2013 and IIIT-Delhi iris databases for contact lens detection. The stated experimentation validates that the proposed method can achieve a 30% performance gain over SOTA on the 2013 Notre Dame and comparable results on IIIT-Delhi database, but this approach does not allow pre-processing, segmenting and localization of the iris. A similar deep CNN-based approach using architectural and filter optimization is followed by Menotti et al. [59]. This approach is evaluated on Warsaw, Biosec and, MobBIOfake datasets of iris images. It can be inferred that Warsaw achieved a lowest HTER rate of 0.16% compared to other datasets. Utilizing the capabilities of deep convolution generative adversarial networks and iris quality metrics Kohli et al. [52] proposed a framework, iris deep convolutional generative adversarial network (iDCGAN) for the generation of realistic appearing synthetic iris images.

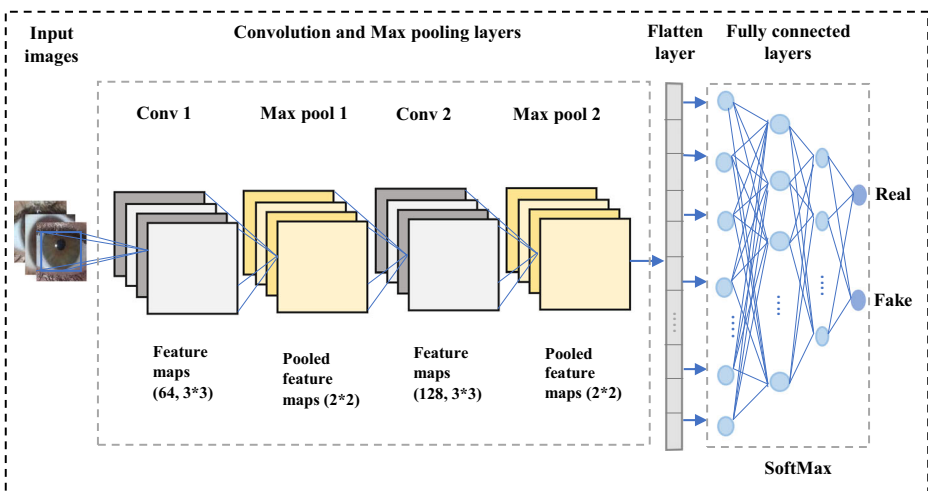


Fig. 11 A generic multi-layer CNN architecture for iris spoof detector

The effectiveness of a PDA framework called DESIST to distinguish between artificially generated and genuine iris images is examined. The multi-order Zernike moments and local binary pattern with variance (LBPV) are deployed for feature extraction from these iris images. Accuracy rate achieved by DESIST to classify iris image generated by iDCGAN is 85.95%. Furthermore, it is observed that the synthetically generated iris image from the iDCGAN framework is more challenging to be detected by DESIST compared to the existing synthetic iris database. Pala and Bhanu [61] adopted a deep TripletNet embedding network for iris recognition. The proposed approach makes use of euclidean distance to match the input iris image features with the already stored features. This approach can work in real-time scenario and has comparable accuracy on two benchmarking datasets. A different approach to avoid losing useful information while discarding the parts of input image beyond the boundary of iris that are influenced by noises is bring forward by Liu et al. [56]. The approach is based on fuzzifying the region beyond the boundary of iris to improve the signal-to-noise ratio by using the triangular fuzzy average and triangular fuzzy median smoothing filters to pre-process the iris images. The improved images are then used to train deep learning systems using fuzzy operations that speeded up the convergence process while simultaneously increasing identification accuracy. The fuzzified image filters are also proven to make images more informative for deep learning and the suggested fuzzy image operation provided a robust approach for many additional deep-learning image processing, analysis, and prediction applications.

Similarly, Long and Zeng [57] also proposed an iris liveness detection approach by batch normalized CNN to evade the issue of overfitting and gradient disappearing during the training process. The results after evaluation shows that the suggested technique can effectively extract micro features from an image and can provide high accuracy. Hu et al. [41] suggested an end-to-end deep neural network for iris authentication model based on EfficientNet-b0. The designed model is evaluated on hybrid iris databases composed of CASIA thousand and Mmu2. The evaluation resulted into a low valid loss of 0.41% as compared to the previously proposed mixnet_I, resnext50d, resnet50, seresnext and, Senet154 models. In analogy to that, a micro stripe analyses (MSA) solution to sense spoof attack is given by Fang et al. [29]. The MSA focus on the difference of the image dynamics around the iris border area. For classification, decision multiple overlapping stripes is fused by the majority vote. Although this MSA method outperforms the present SOTA, it does not show the problem of confounding genuine clear lenses with assault textured ones.

As per the comparisons among the illustrated SOTA DCNN features extraction-based approaches as stated in Table 2, it can be analyzed that various CNN-based frameworks have been put forward and majority of these approaches are evaluated on well-known IIT-Delhi and CASIS iris datasets in known environment. But limited evaluation of DCNN approaches in unknown environment is done where the accuracy ranges from 69.47% to 91.77%.

Fully connected network (FCN)-based approaches As per the above-mentioned CNN-based technique, it may be inferred that giving an entire iris image as an input to the model is inefficient. Since the pixels are lying on the outside iris region are not considered, thus we can take into consideration small iris patches to the learning classifiers for efficient training purpose. The FCN model [55, 83] is a deep learning-based network relying on conventional CNN model without a fully connected layer and it combines expression and prior-knowledge similarities as the input. In the subsequent paragraph, we analyze the locally supervised FCN-based iris spoof detection approaches. Varkarakis et al. propose a deep learning strategy for segmentation of deformed iris areas using FCN in head mounted display. [88]. The proposed

Table 2 A comparison among SOTA DCNN-based ISDs

Paper id	Year	Author(s)	Key concept	Classifier	Dataset	Performance	
						Known	Unknown
D1	2015	Silva et al. [78]	Weights of all layers are learned by back-propagation	CLDNet a CNN followed by an additional fully connected single layer with softmax regression for classification	2013 NDCL, IIIT-Delhi	Multi-sensor CCR results for: 2013 NDCL=82.80%, IIIT-D=69.28%	—
D2	2015	Menotti et al. [59]	Architecture optimization and filter optimization	SpoofNet a CNN based model and learning weights	Warsaw, Biosec, MobBIOfake	HTER for Warsaw=0.16%, Biosec=1.17%, MobBIOfake=1.38%	—
D3	2017	Kohli et al. [52]	Multi-order Zernike moments and LBPV	DESIST framework using neural networks as a classifier	iDCGAN trained on IIIT contact lens DB, IIT Delhi iris DB, Multi-Sensor Iris DB (Combined iris spoofing DB)	Accuracy of DESIST on the proposed database=85.95% with EER=14.19%	—
D4	2017	Pala and Bhanu [61]	Matching is performed using euclidean distance	Deep TripletNet embedding network for iris liveness detection	Iris-2013:Warsaw, IIIT-CLI	ACER: Iris-2013:Warsaw=0.0%, IIIT-cogent=5.5%, IIIT-vista=0.7%	—
D5	2019	Liu et al. [56]	Hough transform, fuzzified image filter, boundary detection and fuzzy methods	F-CNN, F-capsule network	CASIA-Iris-Thousand, IIITD-CLI, ATVS-Fir	Accuracy (ANOVA): CASIA=83.1%, IIITD-CLI Cogent=83.3%, IIITD-CLI vista=89.2%, ATVS-Fir=88.4%	—
D6	2019	Long and Zeng [57]	Batch normalized CNN (BNCNN) to extract deep seated iris features	BNCNN	CASIA Iris lamp& ND contact	False recognition rate: CASIA-Iris lamp=0%, ND contact=0%	—
D7	2019	Hu et al. [41]	CNN for features extraction	EfficientNet-b0 is used to composite model of neural network	CASIA thousand and Mmu2 iris database	Valid acc=99.65% and Valid loss=0.41%	—
D8	2020	Fang et al. [29]	MSA	MSA	CCR:	CCR:	Cross-database evaluation:

Table 2 (continued)

Paper id	Year	Author(s)	Key concept	Classifier	Dataset	Performance
						Known
				MobileNet V3-small is a base structure for classification (where processed MSA is fed to neural network classifier with majority voting)	NDCLD-2015, IIITD LivDet-2017, WVU	NDCLD15 = 99.31% IIITD (mixed) = 98.24% WVU (mixed) = 99.19%
						Unknown
						Highest CCR for CL: NDCLD15 = 91.77% IIITD (mixed) = 69.47% WVU (mixed) = 90.38%

network offers a good accuracy of 99.34% and 99.12% on datasets namely; CASIA thousand and Bath-800 respectively. Another robust iris segmentation technique using FCN with dilated convolution is suggested by Yang et al. [93]. The suggested model does not require any pre-processing of the input iris images and provides end-to-end prediction.

Tobji et al. [87] propounded an FM_{net} algorithm using FCN for manual segmentation and multi-scale convolutional neural network (MCNN) for feature extraction and classification purpose. The performance is evaluated on three datasets i.e., CASIA-Iris-Thousand, UBIRIS.v2 and, LG2200 where the recognition accuracy reported for CASIA-Iris-Thousand is 95.63%, UBIRIS.v2 is 99.41% and, LG2200 is 93.17%. Zhao and Kumar [96] developed a framework using FCN which generates spatial consistent iris feature descriptors. Also, an extended triplet loss (ETL) function is used to integrate bit-shifting and non-iris masking. By extending the work done in 2019 a DL-based unified framework for iris spoof detection, segmentation and recognition is propounded by Zhao and Kumar [97]. The proposed framework UniNet.v2 consists of three modules: Mask R-CNN for image localization and segmentation using optimized FCN, normalized layer and FeatNet for feature learning and matching.

While comparing various FCN-based iris spoof detection methods reported in Table 3, it can be inferred that in most of the approaches a fully connected network is used for segmentation. It may be because of its structure agnostic property and a CNN framework with some modification that is used for classification task. Moreover, to evaluate the performance, the majority of these approaches have used the CASIA V4 iris datasets with an accuracy rate of 95.63% to 99.34%.

Transfer learning-based approaches One of the critical issues in the CNN-based approaches is to extract deep level features to design a robust ISD that perform well in unknown attacking scenario. To tackle these problems, a recent paradigm in deep learning is to utilize the knowledge of the pre-trained models in a specific domain that can be effectively transferred to build an efficient ISD. The transfer learning offers numerous advantages such as reduced training time, improved performance (in most cases), also it doesn't require a huge amount of data. The conception of transfer learning that is used to effectively import the knowledge from source domain to the target domain for building an efficient ISD is illustrated in Fig. 12. In a recent study, Ribeiro et al. [68] investigated the texture transfer learning for super resolution that is applied to low resolution images. The designed approach is evaluated on the subset of CASIA iris image dataset and the best performance of EER 6.07% in factor 2 is achieved when describable texture dataset (DTD) is used. The fusion between the best datasets with the enrolment results is not explored in this work. Chen and Ross [18] proposed multi-task PAD system inspired by an object detection method. The suggested method is computationally effective and can be used in real-time environment. But the technique is not investigated in the scenarios where the training and test datasets have different attacks.

Gautam and Mukhopadhyay [32] presented a transfer learning technique relied on (AlexNet) pre-trained DCNN for feature extraction followed by principal component analysis (PCA) for dimensionality reduction. Cubic SVM (cSVM) based on error-correcting output code (ECOC) multi-class model is further used for classification purpose. For multi-sensor evaluation the CCR of 81.40% and 86.33% is achieved for IIITD and ND dataset respectively. Efficient comprehension and exploitation of hybrid classifiers as well as powerful feature extraction techniques in combination with deep image representation are still open issues to be addressed in this work. The conception of transfer learning that is used to effectively import the knowledge from. An effective iris authentication system based on transfer learning with

Table 3 A comparative illustration of FCN-based ISDs

Paper id	Year	Author(s)	Key concept	Classifier	Dataset	Performance	
						Known	Unknown
F1	2017	Zhao and Kumar [96]	FCN for image segmentation	UniNet combining FeatNet and MaskNet	ND-IRIS-0405, CASIA.v4-distance, IITD, WVU Non-ideal	EER for within-DB: ND IRIS 0405=0.99%, Casia.v4=3.85%, IITD=0.73%, WVU Non-ideal=2.28%	EER for cross-DB: Casia.v4=4.54%, IITD=0.64%, WVU Non-ideal=2.83%
F2	2018	Varkarakis et al. [88]	FCN for image segmentation	Deep neural network	CASIA Thousand and Bath-800	Accuracy: CASIA Thousand=99.34%, Bath-800=99.12%	–
F3	2018	Yang et al. [93]	FCN with dilated convolutions	CNN	CASIA-iris-interval-v4, UBIRIS v2 and IITD Delhi	F-score: CASIA-iris-interval-v4=98.6%, IITD Delhi=98.4%, UBIRIS v2=95.7%	–
F4	2019	Tobji et al. [87]	FMnet using FCN for segmentation and MCNN for feature extraction	MCNN classifier	CASIA-Iris-Thousand, UBIRIS.v2 and LG2200	Recognition accuracy: CASIA-Iris-Thousand=95.63%, UBIRIS.v2=99.41%, LG2200=93.17%	–
F5	2019	Zhao and Kumar [97]	Optimized FCN	UniNet.v2 framework with FeatNet for feature learning and matching	ND IRIS 0405, Casia.v4, IITD, WVU Non-ideal	EER for within-DB: ND IRIS 0405=1.12%, Casia.v4=4.07%, IITD=0.76%, WVU Non-ideal=2.20%	EER for cross-DB: Casia.v4=4.41%, IITD=0.68%, WVU Non-ideal=2.36%

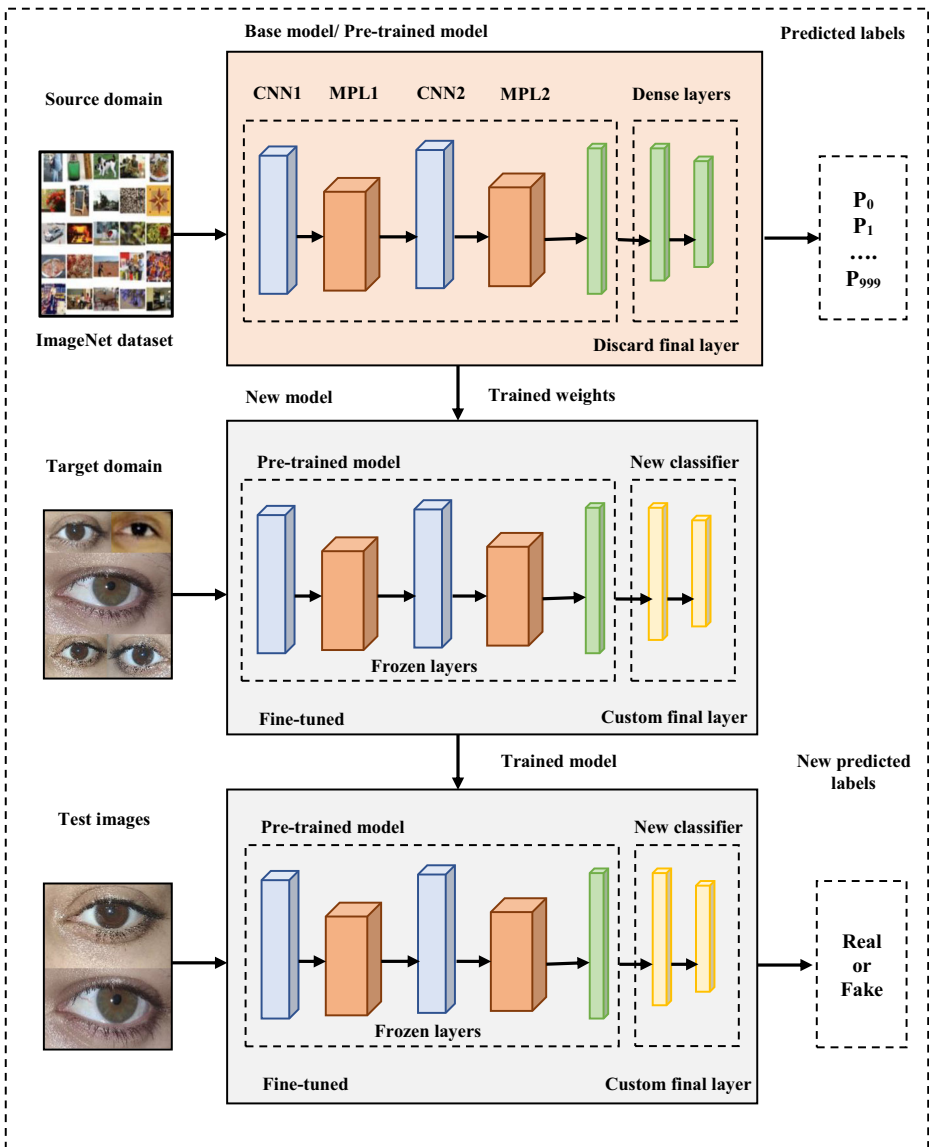


Fig. 12 An architecture of transfer learning-based iris spoof detector

CNN is suggested by Alaslani and Elrefaei [6]. To adopt this strategy, a pre-trained VGG-16 model for feature extraction and classification is tuned. Thereafter, the IITD, CASIA-Iris-V1, CASIA-Iris-thousand, and CASIA-Iris-Interval public datasets are used to assess the performance of the iris recognition system. The findings reveal that the suggested approach has a very high accuracy rate of 100% in case of IITD. A deep learning framework fine-tuned on pre-trained CNN model (ImageNet) is put forward by Minaee and Abdolrashidi [60]. The performance of the technique is assessed using IITD dataset and the accuracy rate of 95.5% is obtained. A novel densely connected contact lens detection network (DCLNet) based on DCNN with addition of SVM on top for classification is proposed by Choudhary et al. [19].

The DCLNet is a densely connected convolutional network with fewer layers and learning parameters than other networks. It learns more significant iris traits due to the dense connections between layers. The experimental results reaffirm that the proposed approach improves the CCR up to 4% as compared to the SOTA. However, it can be inferred that normalization can cause degradation in the model's accuracy in majority of the cases.

Depending on the architecture of a deep learning model for images of a person's left and right irises, a multimodal biometric real-time technique IrisConvNet is adopted by Therar et al. [85]. The feature extraction and classification task are dependent on CNN and transfer learning techniques to generate special features that are supplied to a multi-class SVM algorithm. The performance of IrisConvNet is measured on two publicly available datasets IITD and CASIA-Iris-V3. The accuracy rate of IITD is 99% for both left and right iris and CASIA-Iris-V3 is 94% and 93% for the left and right iris respectively. Sardar et al. [71] introduced an interactive variant of Unet i.e., deep Interactive Squeeze Expand Unet (ISqEUNet) model with interactive learning to lower the training time while improving the storage efficiency by reducing the number of involved parameters. The performance being evaluated on three publicly available dataset shows that NICE. I has a mean true positive rate (mTRP) of 0.983% and mean error rate (MER) of 0.261%. Another ISD solution based on multi-layer fusion is propounded by Fang M. et al. [27]. Two level fusion i.e. feature level and score level is done on the feature extracted from the last several convolution layers. Although, result shows that multi-layer fusion technique performs better as compare to the best single layer feature extractor using pre-trained VGG-16 but while trained from scratch this technique perform well only on larger dataset such as the IITD-WVU database in comparison to the Notre Dame database. Recently, Tapia J. et al. [84] deliberated a two-stage serial framework for PAD focused on detecting bonafide images. For this approach the largest iris PA database by combining several other databases is developed and model is tested when trained from scratch and using fine-tuning. Although comparable results are obtained in known environment the performance of proposed two stage networks is not measured in unknown attack scenarios.

From the comparative analysis of various transfer learning-based iris spoof detection approaches as discussed in Table 4, it can be inferred that in most of the techniques a pre-trained model on ImageNet is used. The reason behind this is, it consists of over 14 million images of roughly 20,000 categories and training a new model using this may reduce the overall training time. Moreover, IITD iris anti-spoofing dataset is widely used in these approaches. Besides, the accuracy rate for IITD dataset in transfer learning-based approaches ranges from 81.40% to 100%.

4.2.3 Hybrid features extraction-based approaches

The handcrafted ISDs have shown promising performance in known attack scenarios but exhibits limited generalization capabilities in unknown attacking environments. Hence, to overcome these problems the DL-based iris spoof detection approaches have proved to be of worth in unknown scenarios, however with an additional training overhead. Our analysis presented in the previous sections indicates a trade-off among design and performance parameters of anti-spoofing mechanisms. Therefore, an alternative solution is to explore the approaches that employ the pros of both handcrafted and DL-based ISDs. These mechanisms may utilize the highly discriminatory feature sets generated by CNN models followed by a traditional classifier such as: SVM, KNN, DT, etc. A generic illustration of hybrid features extraction-based approach is shown in Fig. 13.

Table 4 A comparative summary of transfer learning-enabled ISDs

Paper id	Year	Author(s)	Pre-trained model	Classifier	Dataset	Performance	
						Known	
						Unknown	
T1	2017	Ribeiro et al. [68]	Single-Image Super Resolution (SRCNN) and deeper CNN VDSR	CNN based on transfer learning for image classification	Texture databases, natural image databases, iris databases	In case of EER the best result for: factor 2 (11.5X115) is when DTD is used=6.07% and for factor 4 (57X57) is when bicubic interpolation is used.	-
T2	2018	Chen and Ross [18]	Darknet-19 model trained on ImageNet	Multi-task CNN framework (MT-PAD) with no fully connected layer	ND-Contact, CASIS iris, LivDet iris 2015 Warsaw, BERC-Iris-Fake, LivDet iris 2017 clarkson	BPCR: ND-Contact, CASIS iris=0.5%, LivDet iris 2015 Warsaw=0%	BPCR for Cross sensor: BERC-Iris-Fake = 1.66%, LivDet iris 2017 clarkson=20.44%
T3	2018	Gautam and Mukhopadhyay [32]	Transfer learning relying on (AlexNet) pre-trained DCNN	eSVM learner-based ECOC multi-class model	IIITD, ND	Multi sensor evaluation: Total CCR in case of: IIITD combined = 81.40%, ND combined = 86.33%	-
T4	2019	Alaslami and Elrefaie [6]	The Softmax classifier in pre-trained VGG-16	Transfer learning with pre-trained CNN and then static formula or SVM for classification	IIITD, CASIA-Iris-V1, CASIA-Iris-thousand and, CASIA-Iris-Interval	Recognition accuracy: IIITD iris = 100%, CASIA-Iris-V1 = 98.3%, CASIA-Iris-thousand = 95% and, CASIA-Iris-Interval = 91.6%	-
T5	2019	Minaee and Abdolrashidi [60]	ResNet50 trained on ImageNet	Transfer learning model using deep residual CNN	IIT Delhi	Accuracy rate = 95.5%	-
T6	2019	Choudhary et al. [19]	DenseNet121 a preeminent	DCLNet based on DCNN with an additional SVM classifier	IIITD-CLI, Notre Dame (ND)	CCR for multi sensor validation: IIITD combined = 94.93%, ND combined = 96.04%	-

Table 4 (continued)

Paper id	Year	Author(s)	Pre-trained model	Classifier	Dataset	Performance	
						Known	
						Unknown	
T7	2020	Therar et al. [85]	CNN model that is pre-trained on ImageNet CNN with transfer learning	IrisConvNet with softmax classifier and multi-class SVM classifier	IITD and CASIA-Iris-V3	Accuracy rate: IITD=99% for both left and right irises, CASIA-Iris-V3=94% and 93% for the left and right irises respectively	–
T8	2020	Sardar et al. [71]	Pre-trained ISqEUNet model	Deep ISqEUNet model with interactive learning	CASIA-Iris-V4-Interval, IITD, NICE.I	NICE.I: mTRP=0.983% MER=0.261%	–
T9	2020	Fang M. et al. [18]	Pre-trained VGG-16 and trained from scratch MobileNet V3	Multi-layer fusion (on feature level and score level)	LivDet-iris 2017 (Notre Dame and IITD-WVU datasets)	Notre Dame (HTER): VGG-16=2.31% MobileNet=8.89% IITD-WVU (HTER): VGG-16=20.88% MobileNet=15.09%	–
T10	2022	Tapia J. et al. [32]	MobileNet V2 and a model trained from scratch	Two stage classification using MobileNetv2a and MobileNetv2b	LivDet-Iris 2020	ACER=29.78%	–

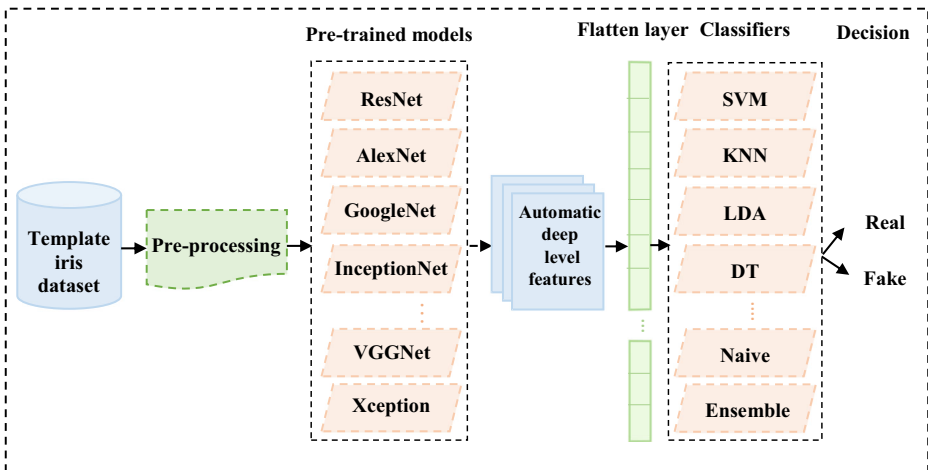


Fig. 13 An illustration of generic hybrid feature extraction-based ISD's

The most recent studies as hybrid iris spoof detection is presented by Czajka et al. [22] in 2017 to countermeasure the spoofing attacks generated by rotating the iris image or the sensor during acquisition and correctly recognizing the left / right (L/R) and upright / upside-down (U/D) orientation of the iris images. Two approaches namely feature engineering (using SVM) and feature learning (using CNN) are compared and evaluated on the proprietary iris dataset by both same-sensor and cross sensor tests. The CCR achieved in case of SVM for L/R is 99.8% and for U/D is 97.3% and in case of CNN is nearly 100% in both the cases (in known environment). It has been observed that CNN-based approach performed better for same-sensor, and presented slightly worse to unknown sensors experiments when compared to an SVM classifier. An ensemble of multi-view-CNN for cross domain iris PAD is proposed by Kuehlkamp et al. [54]. Capabilities of BSIF feature descriptors is utilized and the performance measured by meta-fusing (via SVM) on four benchmark datasets shows that the lowest HTER is in case of Warsaw (0.44% & 0.79%) in known environment and unknown environment. But in test unknown partitions scenario this approach achieves HTER of 20.92% that is higher as compare to others. Another contribution using discrete wavelet transform (DWT) for feature extraction and modified deep residual neural network for spoof detection is done by Chatterjee et al. [17]. Although, the classification accuracy of DWT + modified ResNet for ATVS-Flr and CASIS outperforms the previously implemented modified VGG Net and DWT + modified VGG Net. But, comparatively lesser detection accuracy is achieved when modified ResNet classification technique is employed.

Analyzing the illustrated hybrid iris spoof detection approaches as stated in Table 5 that combines the pros of both handcrafted and deep learning-based approaches it can be deduced that majority of these techniques are evaluated on publicly available datasets with an accuracy ranging from 82.4% to 92.57%.

5 Performance evaluation protocols

The effectiveness and correctness of D²ISD mechanisms is measured through widely accepted evaluation protocols such as anti-spoofing datasets and performance measuring metrics. In this section, we present an evaluation protocols-based analysis of various approaches.

Table 5 An illustration of SOTA hybrid ISDs

Paper id	Year	Author(s)	Features Descriptor(s)	Classifier	Dataset	Performance
Y1	2017	Czajka et al. [22]	EOCC, PIVO, EINV, GMAG, SIND, COSD	SVM, CNN	Proprietary database	<p>Known</p> <p>CCR for SVM: L/R recognition = 99.8% and U/D = 97.3% CCR for CNN: nearly 100% in both cases</p> <p>Unknown</p> <p>Cross-sensor evaluation: CCR for SVM: L/R recognition = 98.4% and U/D = 95.5% CCR for CNN: In worst case: L/R recognition = 89.4% and U/D = 87.7% Cross-domain evaluation: Meta-fusion via SVM: HTER on test unknown partitions: Clarkson = 2.37%, Warsaw = 0.44%, Notre-Dame = 1.22%, IIITD-WVU = 14.92%</p>
Y2	2018	Kuehlkamp et al. [54]	BSIF	Meta fusion of multi-view-CNN (RF, MV, BWVVA, BWVVI) using SVM	Clarkson, Warsaw, Notre-Dame, IIITD-WVU	<p>Known</p> <p>Meta-fusion via SVM: HTER on test known partitions: Clarkson = 2.37%, Warsaw = 0.44%, Notre-Dame = 1.22%, IIITD-WVU = 14.92%</p> <p>Classification accuracy of DWT + modified ResNet:</p> <p>ATVS-Flr = 92.57%, CASIA two class = 90.80%, CASIA cropped = 82.4%</p>
Y3	2019	Chatterjee et al. [17]	Wavelet Transform and Deep Residual Neural Net	Modified ResNet with DWT	ATVS-Flr, CASIA	<p>Known</p> <p>Classification accuracy of DWT + modified ResNet: ATVS-Flr = 92.57%, CASIA two class = 90.80%, CASIA cropped = 82.4%</p>

5.1 Benchmark iris anti-spoofing datasets analysis

An iris anti-spoofing database signifies the well-organized collection of iris data that is primarily used for developing and evaluating the iris spoof detection algorithms. A sufficient size of database consistent to diverse iris sensing approaches and fabrication components are required to evaluate these algorithms. Figure 14 shows few samples of iris images from the benchmark iris anti-spoofing datasets. In this section, we present a review of several existing iris anti-spoofing databases that are widely used in the literature of iris spoof detection mechanisms. The most prominent databases are from publicly available Liveness detection competition series: LivDet-2020 [23], LivDet-2017 [92], LivDet-2015 [91], LivDet-2013 [90], MobBIOfake [74], etc. The details of ISDs datasets are listed in Table 6 along with the sensor technology used for capturing iris images at various resolution and image sizes.

After assessment, two imperative assumptions may be drawn from the benchmark iris anti-spoofing datasets given in Table 6. First indicate that the most prominently used dataset for performance evaluation of iris spoof detection approaches is IIITD-CLI, and the second is the size of datasets used for iris spoof detection techniques consists of only few thousands iris images, that is inadequate for learning an effective DL-based iris spoof detector (DISD). CASIS-IrisV3 is the largest of all consisting of 22,035 images.

5.2 ISDs evaluation metrics

The well-known performance metrics are used to assess the extent to which possible mechanisms, solutions, or D^2 ISD models are able to meet the expectations through extents of their performance, limitations, and trade-off. The standard metrics for evaluating the effectiveness of an iris PAD are defined by the International Standard Organization (ISO/IEC 30107–3:2017) and is summarized in Table 7.

The analysis of the evaluation metrics that are employed for iris spoof detection approaches as illustrated in Table 7, it may be observed that the FRR is the most widely used protocol for evaluating the performance of anti-spoofing mechanisms.

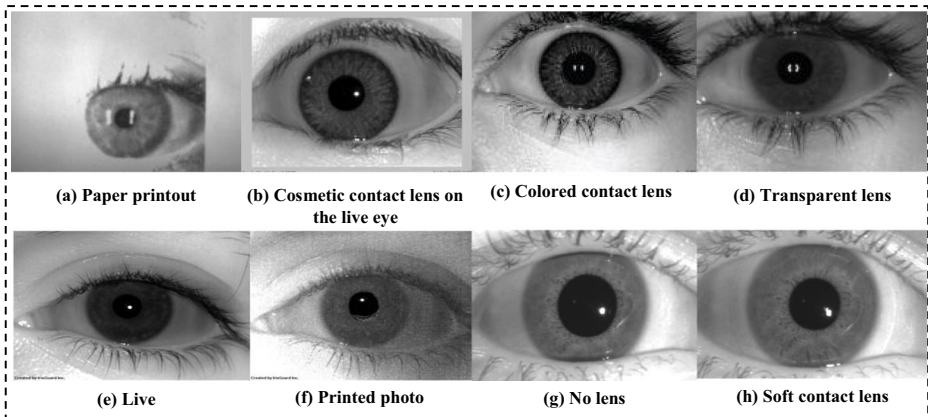


Fig. 14 Some sample images from benchmark datasets (a) LivDet Iris-2020 (b) LivDet Iris-2020 (c) IIITD-CLI (d) IIITD-CLI (e) LivDet 2015 Warsaw (f) LivDet 2015 Warsaw (g) LivDet 2013 Notre Dame (h) LivDet 2013 Notre Dame

Table 6 A comparative analysis of benchmark iris anti-spoofing datasets

S.No.	Dataset name	Wavelength	Image size/ Resolution	Sensors used	Number of images (Training and Testing)	Types of fakes	References
1	LivDet Iris-2020	NIR	224 × 224	LG 4000, AD 100, Iris ID iCAM7000 and IriTech IriShield	12,432	PP, CL, Fake/ prosthetic/ printed eyes with add- ons, eyes displayed on kindle, cadaver eye	[84]
2	LivDet-iris-2017 Clarkson	NIR, VIS	640 × 480	LG IrisAccess EOU2200	8095	PP, CL	[17, 18, 23, 54, 92]
3	LivDet 2017 Warsaw	NIR	640 × 480	IrisGuard AD100 and Aritech ARX-3M3C camera with SONY EX-View CCD sensor	11,823	PP	[54]
4	LivDet-2017 IIITD	NIR	640 × 480	LG 4000 and AD 100 sensors	4800	TCL, SCL	[29]
5	LivDet-2017 WVU	NIR, VIS	640 × 480	Mobile iris sensor and IriShield MK2120U mobile iris sensor	9057	PP, TCL, PCL	[29]
6	LivDet 2017 IIITD-WVU	NIR, VIS	640 × 480	IriShield MK2120U mobile iris sensor, HP LaserJet Enterprise P3015 (in black and white mode) and Konica Minolta Bizhub C454E (in color mode)	10,459	TCL, PP	[54]
7	LivDet 2017 Notre Dame	NIR	640 × 480	IrisGuard AD100 and IrisAccess LG4000	4800	CL	[27, 54]
8	LivDet 2015 Clarkson LG	NIR	1200 dpi v/s 2400 dpi	LG IrisAccess EOU2200	3726	TCL, PP	[49, 50]
9	LivDet 2015 Dalsa	NIR	1200 dpi v/s 2400 dpi	Dalsa camera	4255	CL, PP	[49, 50]
10	LivDet 2015 Warsaw	NIR	up to 1200 dpi	IrisGuard AD100	7559	PP	[18, 36, 49, 50]
11	LivDet 2015 NDCLD	NIR	640 × 480	IrisGuard AD100 and IrisAccess LG400	4068	TCL	[28, 29]
12	LivDet 2013 Clarkson	NIR	up to 1200 dpi	Dalsa camera	1356	CL	[15, 25]
13	LivDet 2013 Warsaw	NIR	Up to 600 dpi		1667	PP	

Table 6 (continued)

S.No.	Dataset name	Wavelength	Image size/ Resolution	Sensors used	Number of images (Training and Testing)	Types of fakes	References
14	LivDet 2013	NIR	640 × 480	Panasonic ET-100 and IrisGuard AD100	4200	TCL	[36, 40, 59, 61, 65]
15	Noire Dame MobBIOflake	VIS	250 × 200	LG 4000 and IrisGuard AD-100 sensor Mobile sensor	1600	PP	[18, 19, 32, 36, 40, 57, 78, 89] [25, 35, 40, 59, 65]
16	IIITD Iris Spoofing (IIS)	NIR	–	Cogent CIS 202 dual eye iris scanner and a HP flatbed optical scanner	4848	Print+Scan, Print+Capture (TCL, SCL)	[6, 38, 49, 50, 97]
17	IIT Delhi	NIR	320 × 240	JRIS, JPC1000 and digital CMOS camera	1120	PP	[60, 93]
18	IIITD-CLI	VIS	640 × 480	Cogent dual iris sensor (CIS 202) and VistaFAZE single iris sensor	6570	TCL, SCL	[3, 4, 19, 32, 36, 49–51, 56, 61, 78, 89]
19	ATVS Fir	NIR	640 × 480	LG IrisAccess EOU3000 sensor	1600	PP	[3, 4, 14, 17, 31, 56, 62, 65]
20	CASIS-IrisV1	NIR	320 × 280	CASIA iris camera	1010	–	[6, 31]
21	CASIS-IrisV3	NIR	320 × 320	CASIA close-up iris camera and OKI IRISPASS-h	22,035	–	[5, 85]
22	CASIS-IrisV3 Interval	NIR	320 × 280	CASIA close-up iris camera	2639	–	–
23	CASIS-IrisV3 lamp	VIS	640 × 480	OKI IRISPASS-h	16,212	–	[57]
24	CASIS-IrisV3 twins	VIS	640 × 480	OKI IRISPASS-h	3183	–	–
25	CASIA-IrisV4 Interval	NIR	320 × 280	CASIA close-up iris camera	2639	–	[71, 93, 97]
26	CASIS-IrisV4 thousand	VIS	640 × 680	Irisking IKEMB-100	20,000	–	[6, 41, 56, 87, 88]
27	CASIA-IrisV4 distance	NIR	2352 × 1728	CASIA long-range iris camera	2567	–	[96]
28	CASIS-IrisV4 Syn	NIR	640 × 480	CASIA iris image synthesis algo	10,000	SYN	[25]
29	UBIRIS V1	VIS	1704 × 2560	Camera Model Nikon E5700 and Software E5700v1.0	1877	–	[5]

Table 6 (continued)

S.No.	Dataset name	Wavelength	Image size/ Resolution	Sensors used	Number of images (Training and Testing)	Types of fakes	References
30	UBIRIs V2	VIS	300 × 400	a Canon EOS 5D DSLR camera	11,000		[87, 93]
31	Biosec	NIR	640 × 480	LGfris/AccessEOU3000 camera	1600	PP	[59]
32	Mmu2 iris database	VIS	320 × 238	Panasonic BM-ET100US	995	CL, Glasses	[41]

Table 7 An analysis of various evaluation metrics used for ISDs

S.No.	Acronym	Metric	Description	Formula	References
1	APCER	Attack presentation classification error rate	The ratio of attack presentation with the identical presentation attack instrument that are misclassified as bonafide presentations to the total number of presented samples.	$APCER = \frac{FP}{FP+TP}$	[18, 28, 29, 49, 50, 54, 61, 62, 65, 66, 69]
2	BPCER/ NPCER	Bona-fide presentation classification error rate/ normal presentation classification error rate	The ratio of bonafide presentations presented to the D-ISD subsystem which are misclassified as attack presentations in a particular situation to the total number of presented samples.	$BPCER = \frac{FN}{FP+FN}$	[16, 18, 28, 29, 49, 50, 54, 61, 62, 65, 66]
3	ACER/ HTER	Average classification error rate/ half total error rate	It is the average of APCER and BPCER with a predefined threshold.	$ACER = \frac{APCER+BPCER}{2}$	[27, 29, 31, 35, 36, 49, 50, 54, 59, 62, 65, 66, 84]
4	MCER	Mean classification error rate	It is defined as the mean of APCER and BPCER with a predefined threshold.	$MCER = \frac{APCER+BPCER}{2}$	[40]
5	ACR	Average classification rate	It is defined as the average percentage of correctly classified test feature vectors (live or fake).	$ACR = \frac{100\% - APCER + BPCER}{2}$	[16, 61]
6	FAR/ FGR / FMR	False accept rate/ false gen rate/ false match rate	Probability of false samples that are considered as real.	$FAR = \frac{FP}{FP+TN} * 100$	[3–5, 31, 35, 36, 38, 51, 62, 89, 94]
7	FRR/ FFR/ FNMR	False reject rate/ false fake	Probability of real samples that are considered as fake.	$FRR = \frac{FN}{FP+FN} * 100$	[3–5, 14, 16, 20, 26, 31, 35, 36, 38, 40, 42, 49–51, 53,

Table 7 (continued)

S.No.	Acronym	Metric	Description	Formula	References
8	GAR	rate/ false non-match rate Genuine acceptance rate	GAR is the overall accuracy measurement of the biometric recognition system.	$GAR = 1 - FRR$	[62–65, 89, 94, 96, 97] [5]
9	EER	Equal error rate	It may be defined as the point in ROC curve where imposter score overlaps with the genuine score i.e., $FMR = FNMR$.	$EER = \frac{FMR + FNMR}{2}$	[5, 16, 22, 50, 52, 59, 68, 95–97]
10	CCR	Correct classification rate	It is defined as the number of times the genuine user is correctly matched with the goal.	$CCR = 1 - EER$	[18, 19, 22, 25, 29, 32, 49, 50, 78, 89, 94, 95]
11	ACCR	Average correct classification rate	It is the average of the number of times the genuine user is correctly matched with the goal.	$ACCR = \frac{\text{Genuine user match attempts}}{\text{attempts}}$	[22]
12	AER	Average error rate	It is the average of FAR and FRR.	$AER = \frac{FAR + FRR}{2}$	[3, 4, 17]
13	ACA	Average classification accuracy	It is used to measure the correct classification performance of the given algorithm.	$ACA = \frac{TP + TN}{N}$	[3, 4]
14	PSNR	Peak signal to noise ratio	PSNR is the ratio of maximum possible power of a signal to the power of corrupting noise.	$PSNR = 10 \cdot \log_{10} \frac{MAX^2}{MSE}$	[68]
15	SSIM	Structural similarity index measure	SSIM is used to measure the similarities between two images.	$S(x, y) = f(l(x, y), c(x, y), s(x, y))$	[68]
16	Accuracy	Accuracy	It is defined as the number of correct predictions to the total number of predictions made by the system.	$Accuracy = \frac{TP + TN}{TP + FN + TP + FN}$	[32, 41, 60, 85, 87, 88]
17	Precision	Precision	Precision is the ratio of number of correct positive result to the number	$Precision = \frac{TP}{TP + FP}$	[32, 88]

Table 7 (continued)

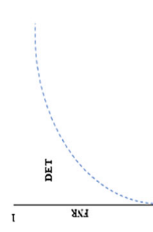
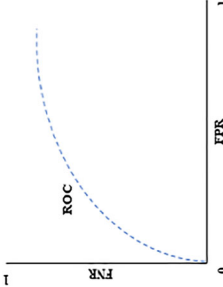
S.No.	Acronym	Metric	Description	Formula	References
18	Sensitivity/ Recall/ TPR	Sensitivity/ recall/ true positive rate	of positive results predicted by the classifier. It is defined as the ratio of number of correct positive result to all the relevant samples.	$Sensitivity = \frac{TP}{TP+FN}$	[17, 32, 88]
19	Specificity/TNR	Specificity/ true negative rate	It is defined as the probability of an actual negative is test negative.	$Specificity = \frac{TN}{TN+FP}$	[32, 88]
20	FPR	False positive rate	It is defined as the ratio of number of incorrect positive result to all the relevant samples.	$FPR = \frac{FP}{FP+TN}$	[88, 93]
21	FNR	False negative rate	It is defined as the probability of an incorrect negative is test negative.	$FNR = \frac{FN}{FN+TP}$	[88, 93]
22	nice1	Nice1	It calculates the proportion of disagreeing pixels using XOR operators over all the image.	$Nice1 = \frac{1}{N * m * r} * \sum_{k=1}^N \sum_{i,j \in (m,r)} G(I, J) \oplus O(i, j)$	[93]
23	nice2	Nice2	It is defined as the average between FPR and FNR.	$nice2 = \frac{FPR+FNR}{2}$	[93]
24	F-score	F-score	F-score is defined as the harmonic mean of precision and recall.	$F\text{-score} = 2 * \frac{precision * recall}{precision+recall}$	[32, 88, 93]
25	DET curve	Decision error threshold curve/ detection error trade-off curve	It is a graphical representation of performance of any biometric system.		[49]
26	D-EER	Detection equal error rate	It is a point where both APCER and BPCER is equal.	$D\text{-EER} = \frac{APCER+BPCER}{2}$	[49]
27	MER	Mean error rate			[71]

Table 7 (continued)

S.No.	Acronym	Metric	Description	Formula	References
28	DSC	Dice similarity coefficient	MER provides the ratio of the false pixel's predictions in the whole given image. DSC is the spatial overlap index, which provides the measure of similarities between the prediction and the ground truth.	$MER = \frac{1}{N_{\text{true}}} * \sum_{i=1}^I \sum_{j=1}^C P(I, j) \oplus G(I, j)$ $DSC = 2 * \frac{ P \cap G }{ P + G }$	[71]
29	mFPR	The mean true positive rate	The mFPR is used to compute average ratio of predicted ground truth pixel to the total ground truth foreground pixels.	$mTPR = \frac{TP}{N(TP+FN)}$	[71]
30	ROC curve	Receiver operating characteristic curve	It is a graphical representation of performance of any classification model at all classification thresholds.		[3–5, 17, 19, 32, 36, 38, 51, 69, 89, 94, 95]

6 Overall analysis

With the thorough investigations and analysis of D²ISD approaches, certain broad inferences can be drawn as an outcome of the study. Figure 15 depicts the overall outcomes of the comparative analysis particularly based on the descriptors used, learning algorithms, spoofing attack types, etc. Our analysis from Fig. 15a indicate that LBP and its variants are most widely deployed image descriptors in handcrafted features-based ISD methods.

One of the reasons behind this is the robustness and ability of LBP descriptors to tackle the inconsistencies in iris images that include rotational, scale and illumination variations. Another image BSIF descriptor that extracts robust features from iris images is also a popular choice to the designers of ISDs. The classification is a vital task of any ISD that

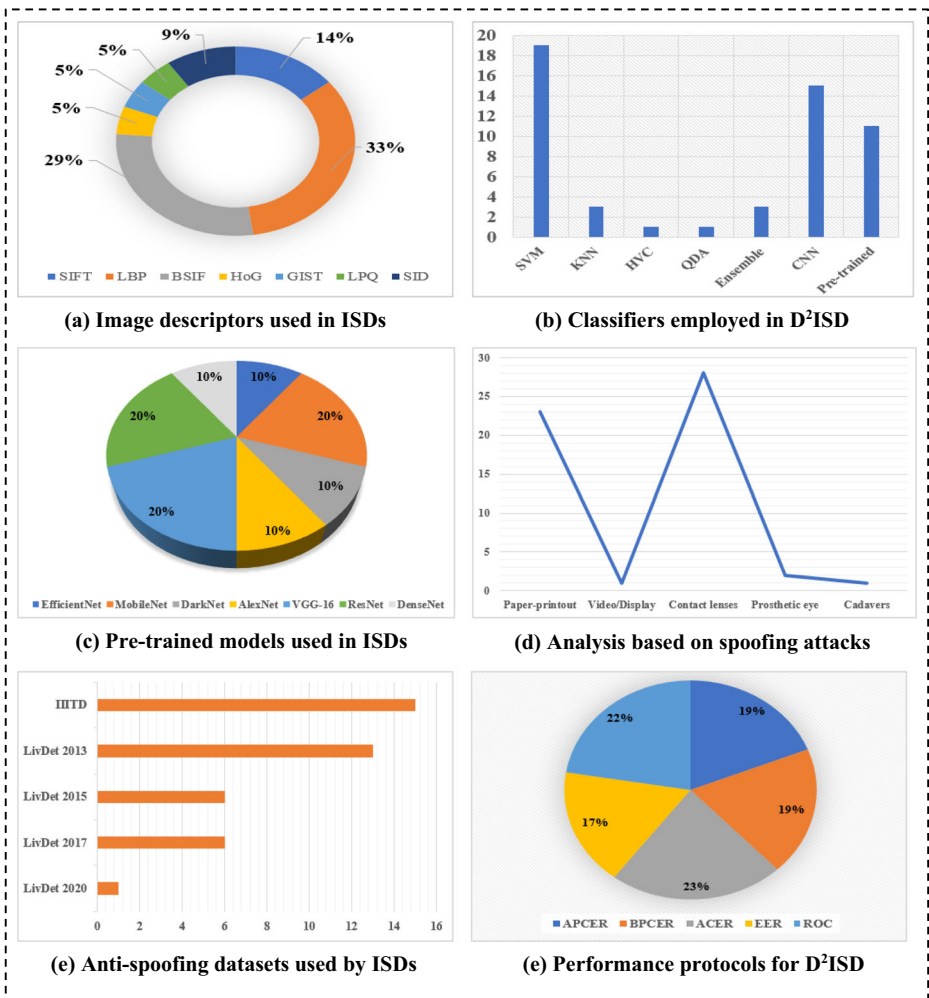


Fig. 15 An illustration of overall analysis of various ISDs (a) Image descriptors used in ISDs (b) Classifiers employed in D²ISD (c) Pre-trained models used in ISDs (d) Analysis based on spoofing attacks (e) Anti-spoofing datasets used by ISDs (f) Performance protocols for D²ISD

discriminate a given iris image as live or fake. From the Fig. 15b, the literature witnesses the use of SVM in majority of the handcrafted features-based ISDs. In comparison to other classifiers, the SVM discriminate between the bonafide and fake samples via a hyperplane with maximum margin. Moreover, SVM is efficient in terms of training overhead and it supports its utilization in majority of the traditional approaches. On the other hand, in the contemporary ISDs, the deep CNN with additional notion of data augmentation or pre-trained models is a prevailing scenario. Apart from this, Fig. 15c shows that pre-trained models such as MobileNet, VGGNet, and ResNet are also being used for developing efficient ISD approaches. Counter measuring iris attacks are also an important design issue for a potent ISD. Our analysis from Fig. 15d shows a comparison among the type of iris attacks tackled by existing ISDs. Moreover, the study infers that most of the ISDs countermeasures paper printout and contact lens attacks. Only a few mechanisms have been developed that may prevent the sensor module from video, prosthetic eye, and cadavers' attacks. From the overall analysis it is also inferred that the benchmark IIT Delhi and LivDet 2013 are the most widely used iris anti-spoofing datasets to evaluate the performance of model as demonstrated in Fig. 15e. In the last, a comparison based on the performance evaluation protocols is presented in Fig. 15f. The ACER and ROC curve are the frequently used metrics to compute the performance of an ISD.

7 Open research challenges and future directions

The critical investigation and study in the previous sections has led to identification of several open research issues that need futuristic exploration in the future research. In this section, we deliberate various research problems and opportunities for further study to tackle PAs in the iris biometric systems. The major open problems and the viable opportunities that have emerged from our overall analysis are explained as follows.

i. Open research problem. Limited robustness of handcrafted features: The majority of iris spoof detection methods have used a single descriptor for image classification ([2–4, 16, 20, 26, 31, 34–38, 42, 43, 51, 53, 62–65, 89, 94, 95] and [25]) that results in low discrimination power for accurately discriminating an image to be a real or fake iris traits. Therefore, a challenge is to build a model that can efficiently extract robust feature sets from iris images that may accurately classify a given iris image into a real or fake label.

Future directions: To build more accurate ISD, the future direction orient towards exploring a novel combination of multiple features. The compatibility and upper limit on the number of features need a thorough analysis for avoiding the curse-of-dimensionality issues. The choice of features sets is dependent upon the discrimination power to accurately classify a given iris image as real or fake. The design of novel methods for feature or decision level fusion of multiple image features is another future scope for the researchers. Another design issue for multi-features-based ISD methods is to select appropriate classification algorithms.

ii. Open research problem. Requirement of robust learner: Our analysis clearly indicate that majority of the existing handcrafted features-based ISD's used a single classifier such as: SVM or KNN ([3, 4, 14, 25, 31, 35, 36, 38, 50, 94] and [69]). In some cases, these alone classifiers may not perform well to tackle the problem of imbalanced datasets or the model does not offer the desired performance, hence results in overfitting the ISD model. Moreover, the decision capabilities of various classifiers vary in different environmental conditions as well as inconsistencies in the training datasets.

Future directions: One of the viable solutions that is least explored is to employ the notion of ensemble learning [89], where the decision of multiple weak classifiers is consolidated to result in the final outcome. Additionally, these approaches are particularly significant in the case when the ISD is built on multiple handcrafted-features. A diverse range of simple (e.g. majority voting, weighted sum, etc.) as well as complex (e.g. bagging, AdaBoost, etc.) ensembles are available that may be explored in designing more robust learners for iris spoof detection.

iii. Open research problem. Limited performance of handcrafted approaches in unknown attack scenario: One of the utmost attributes of an ISD is to perform excellently well in known as well as unknown attack scenario such as (i.e. cross-sensor, cross-database and cross-material). From our analysis, it is observed that only few existing approaches ([49–51, 94, 95] and [28]) are evaluated in unknown attacking scenario. Moreover, these approaches offer limited performance to tackle the problems of unknown attacks.

Future directions: The future research should be oriented towards developing robust handcrafted features-based ISDs that are well trained on iris images of diverse range of variations covering samples from different sensors, datasets and iris spoof materials.

iv. Open research problem. Adversarial attacks on CNN models: A recent paradigm has shifted to deep-level features via CNN for building an accurate iris spoof detection network. However, these models are also vulnerable to attacks that may be hosted by an adversary, where the underline architecture of the CNN model is altered. In this manner, the knowledge learned by an CNN-based ISD model accumulated as model weights may be either completely stolen or altered.

Future directions: As a future research, the secured CNN models can be developed to overcome the different types of adversarial attacks. Alternatively, the effective mechanisms can be explored to counter the attacks on CNN-based ISD models.

v. Open research problem. Limited performance of CNN-based methods in unknown attack scenario: Though, CNN-based iris spoof detection approaches demonstrates excellent performance in known environment, but our study examined that limited work has focused on unknown attack scenarios [29]. Surprisingly, these approaches are only evaluated on cross-dataset scenarios.

Future directions: To further boost up performance of CNN-based ISDs, the models should be trained on iris images captured from different sensors as well as spoofed artefacts created from various materials. To anticipate, the artefact created from unknown materials the iris spoof detection model should actively learn from previously misclassified fakes.

vi. Open research problem. Inadequate dataset for DL-based iris spoof detector: One of the critical design issues for DISD is the requirement of appropriate and adequate size of iris anti-spoofing datasets. In other words, the DL-based approaches are most effective when the model is trained on millions of images. From our investigations it may be seen that the existing benchmark anti-spoofing datasets are comprised of only few thousands iris images [23, 74, 90–92], that is inadequate for learning an effective DISD.

Future directions: One of the solutions is to develop a large-scale dataset covering millions of iris images acquired in different environmental conditions. However, this is time consuming and tedious mechanism, therefore an alternative is to explore data augmentation to enlarge the size of existing datasets. Another mechanism may explore the concept of transfer learning that use the power of well-known pre-trained CNN models on millions of images.

vii. Open research problem. Lack of lightweight DL-enabled ISD models: An iris anti-spoofing method may be viewed as a simple binary classification problem to categorize an input image as either real or fake. The existing DL-based models that employ deeper architectures (higher number of layers) result in larger training overhead due to millions of trainable parameters.

Future directions: An alternative and efficient approach is to develop novel architecture that is comprised of comparatively lesser number of layers. However, to tackle this problem the concept of domain adaptation may be adopted where the knowledge of source domain may be transferred for learning lightweight DISD.

viii. Open research problem. Need of hybrid approaches for efficient models: The overall analysis from the presented study draws a clear inference that there exists a trade-off between classical handcrafted features and contemporary DL-based iris spoof detection approaches. Both the mechanisms exhibit conciliation between accuracy and training overhead as well as performance in unknown attack scenarios. Although, some studies are available in literature that are based on hybrid iris spoof detection mechanisms ([22, 54] and [17]), but the further improvements in this field is requisite.

Future directions: To offer viable and efficient iris anti-spoofing solutions, the futuristic approaches can exploit the pros of both the classical as well as modern iris spoof detection approaches. Therefore, the DL-based ISD can integrate some of the initial layers as handcrafted features followed by convolutional, pooling, drop out and fully connected layers.

8 Conclusions

In this study, we presented an in-depth review of SOTA iris anti-spoofing approaches. Our study has analyzed several ISDs that make use of different types of image features along with a diverse range of classification algorithms. However, handcrafted features and DL-based ISDs show their respective merits and demerits but a clear trade-off between these methods is a major investigation of the presented study. It has led researchers to explore new hybrid ISD mechanisms that complement the pros of both the schemes. Apart from this, evaluation protocols-based analysis of D²ISD approaches offers a clear futuristic perspective for designing improved anti-spoofing mechanisms. Among all, one of the critical issues is to build an appropriate anti-spoofing iris dataset as the data-driven approaches are heavily dependent on the quality as well as quantity of the training dataset. Moreover, the choice of a strong classifier is an imperative design issue in the classical approaches that employs multiple image features. Our study clearly infers that the modern paradigm has shifted towards DL-based ISD approaches, hence the training overhead due to the requirement of larger dataset led to additional challenge. The future research can be oriented towards designing robust and lightweight iris spoof detectors via transfer learning or active learning. The expansion of benchmark anti-spoofing iris datasets covering broader perspectives may help to tackle the problem of unknown attacks scenarios. The analysis presented in this study, infers that majority of the work has focused on counter measuring photo or cosmetic lens attacks. Therefore, the future work may target preventing from other iris attacks such as display, prosthetic eye, etc. It is also observed that SOTA iris spoof detectors demonstrate superb performance in known attack environments while results in satisfactory accuracy in unseen attacks. In future, robust ISD mechanisms can be explored that performs well in unseen attack scenarios (i.e. cross-database, cross-sensor, and cross-materials).

Appendix

Table 8 Some symbols and acronyms with their descriptions

Acronyms	Description
ACER	Average Classification Error Rate
ACR	Average Classification Rate
AER	Average Error Rate
BSIF	Binarized Statistical Image Features
CCR	Correct Classification Rate
CL	Contact Lenses
CNN	Convolutional Neural Networks
cSVM	Cubic SVM
DCLNet	Densely Connected Contact Lens Detection
DCNN	Deep Convolution Neural Network
D ² ISD	Data-Driven Iris Spoof Detector
DISD	Deep Iris Spoof Detector
DL	Deep learning
DT	Decision Tree
DTD	Describable Texture Dataset
DWT	Discrete Wavelet Transform
EBHxEP	Enhanced Binary Hexagonal Extrema Pattern
ECOC	Error-Correcting Output Code
EER	Equal Error Rate
ETL	Extended Triplet Loss
FCN	Fully Connected Network
FMR	False Match Rate
FNMR	False Non-Match Rate
GA	Genetic Algorithm
GIST	Global Image Descriptor
HoG	Histogram of Oriented Gradient
HTER	Half Total Error Rate
HVC	Hierarchical Visual Codebook
iDCGAN	Iris Deep Convolutional Generative Adversarial Network
ISD	Iris Spoof Detector
ISqEUNet	Deep Interactive Squeeze Expand Unet
KNN	K-Nearest Neighbors
LBHxEP	Local Binary Hexagonal Extrema Pattern
LBP	Local Binary Pattern
LBPV	Local Binary Pattern with Variance
LCPD	Local Contrast-Phase Descriptor
M-BSIF	Multi-Scale Binarized Statistical Image Features
MCER	Mean Classification Error Rate
MCNN	Multi-Scale Convolutional Neural Network
MER	Mean Error Rate
MSA	Micro Stripe Analyses
mTRP	Mean True Positive Rate
NF-IQM	Non-Reference Image Quality Measures
NIR	Near Infrared
PA	Presentation Attacks
PAD	Presentation Attack Detection
PAVID	Presentation Attack Video Iris Database
PCA	Principle Component Analysis
PCL	Patterned Contact Lenses

Table 8 (continued)

Acronyms	Description
PP	Paper Printouts
QDA	Quadratic Discriminant Analysis
RBFNN	Radial Basis Function Neural Network
RBFNN-GA	Radial Basis Function Neural Networks-Genetic Algorithm
ROC	Receiver Operating Characteristic
SCL	Soft Contact Lenses
SID	Scale Invariant Descriptor
SIFT	Scale-Invariant Feature Transform
SOTA	State-Of-The-Art
SVM	Support Vector Machine
TCL	Textured Contact lenses
VSIA	Visible Spectrum Iris Artefact

Data availability The datasets used/generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

Declarations

Competing interests All the authors declare that they do not have any conflict of interest.

References

1. Abdellatef E, Ismail NA, Abd Elrahman SESE, Ismail KN, Riham M, Abd el-Samie FE (2019) Cancelable multi - biometric recognition system based on deep learning. *Vis Comput* 36(0123456789):1097–1109. <https://doi.org/10.1007/s00371-019-01715-5>
2. Agarwal R and Jalal AS (2021) “Presentation attack detection system for fake Iris: a review,” *Multimed. Tools Appl*, <https://doi.org/10.1007/s11042-020-10378-7>.
3. Agarwal R, Jalal AS, Arya KV (2020) Enhanced binary hexagonal Extrema pattern (EBHXEP) descriptor for Iris liveness detection. *Wirel Pers Commun* 115(3):2627–2643. <https://doi.org/10.1007/s11277-020-07700-9>
4. Agarwal R, Jalal AS, Arya KV (2021) Local binary hexagonal Extrema pattern (LBHXEP): a new feature descriptor for fake iris detection. *Vis Comput* 37(6):1357–1368. <https://doi.org/10.1007/s00371-020-01870-0>
5. Ahmadi N, Nilashi M, Samad S, Rashid TA, Ahmadi H (2019) An intelligent method for iris recognition using supervised machine learning techniques. *Opt Laser Technol* 120(December 2018):105701. <https://doi.org/10.1016/j.optlastec.2019.105701>
6. Alaslani MG, Elrefaie LA (2019) Transfer learning with convolutional neural networks for IRIS recognition. *Int J Artif Intell Appl* 10(5):49–66. <https://doi.org/10.5121/ijaiia.2019.10505>
7. Bakkouri I, Afdel K (2020) Computer-aided diagnosis (CAD) system based on multi-layer feature fusion network for skin lesion recognition in dermoscopy images. *Multimed Tools Appl* 79(29–30):20483–20518. <https://doi.org/10.1007/s11042-019-07988-1>
8. Bakkouri I, Afdel K, Benois-Pineau J, Catheline G, For the Alzheimer’s Disease Neuroimaging Initiative (2022) *BG-3DM2F: Bidirectional gated 3D multi-scale feature fusion for Alzheimer’s disease diagnosis*, vol. 81, no. 8
9. Bhatti UA, Huang M, Wang H, Zhang Y, Mehmood A, Di W (2018) Recommendation system for immunization coverage and monitoring. *Hum Vaccines Immunother* 14(1):165–171. <https://doi.org/10.1080/21645515.2017.1379639>
10. Bhatti UA, Huang M, Wu D, Zhang Y, Mehmood A, Han H (2019) Recommendation system using feature extraction and pattern recognition in clinical care systems. *Enterp Inf Syst* 13(3):329–351. <https://doi.org/10.1080/17517575.2018.1557256>

11. Bhatti UA, Yu Z, Li J, Nawaz SA, Mehmood A, Zhang K, Yuan L (2020) Hybrid watermarking algorithm using Clifford algebra with Arnold scrambling and chaotic encryption. *IEEE Access* 8:76386–76398. <https://doi.org/10.1109/ACCESS.2020.2988298>
12. Bhatti UA, Zeeshan Z, Nizamani MM, Bazai S, Yu Z, Yuan L (2022) Assessing the change of ambient air quality patterns in Jiangsu Province of China pre-to post-COVID-19. *Chemosphere* 288(2):132569. <https://doi.org/10.1016/j.chemosphere.2021.132569>
13. Bhatti UA et al (2022) Local Similarity-Based Spatial–Spectral Fusion Hyperspectral Image Classification With Deep CNN and Gabor Filtering. *IEEE Trans Geosci Remote Sens* 60. <https://doi.org/10.1109/TGRS.2021.3090410>
14. Bhogal APS, Sollinger D, Trung P, Uhl A (2017) Non-reference image quality assessment for biometric presentation attack detection. *Proc - 2017 5th Int Work Biometrics Forensics, IWBF 2017*. <https://doi.org/10.1109/IWBF.2017.7935080>
15. Boulkenafet Z, Komulainen J, Hadid A (2018) On the generalization of color texture-based face anti-spoofing. *Image Vis Comput* 77:1–9. <https://doi.org/10.1016/j.imavis.2018.04.007>
16. Busch C (2017) “The ISO/IEC standards for testing of Presentation Attack Detection,”. [Online]. Available: <https://christoph-busch.de/files/Busch-PAD-standards-170329.pdf>.
17. Chatterjee P, Yalchin A, Shelton J, Roy K, Yuan X, Edoh KD (2019) Presentation attack detection using wavelet transform and deep residual neural net, vol 11637. Springer International Publishing, LNCS
18. Chen C, Ross A (2018) “A Multi-Task Convolutional Neural Network for Joint Iris Detection and Presentation Attack Detection,” no. March
19. Choudhary M, Tiwari V, Venkanna U (2019) An approach for iris contact lens detection and classification using ensemble of customized DenseNet and SVM. *Futur Gener Comput Syst* 101:1259–1270. <https://doi.org/10.1016/j.future.2019.07.003>
20. Czajka A (2015) Pupil dynamics for iris liveness detection. *IEEE Trans Inf Forensics Secur* 10(4):726–735. <https://doi.org/10.1109/TIFS.2015.2398815>
21. Czajka A, Bowyer KW (2018) Presentation attack detection for iris recognition: An assessment of the state-of-the-art. *ACM Comput Surv* 51(4). <https://doi.org/10.1145/3232849>
22. Czajka A, Bowyer KW, Krumdick M, Vidalмата RG (2017) Recognition of image-orientation-based Iris spoofing. *IEEE Trans Inf Forensics Secur* 12(9):2184–2196. <https://doi.org/10.1109/TIFS.2017.2701332>
23. Das P et al. (2020) “Iris Liveness Detection Competition (LivDet-Iris) - The 2020 Edition,” *IJCB 2020 - IEEE/APR Int. Jt. Conf. Biometrics*, <https://doi.org/10.1109/IJCB48548.2020.9304941>.
24. Daugman J (1994) “Biometric Personal Identification System Based on Iris Analysis,” no. 19
25. Dronky MR, Khalifa W, Roushdy M (2021) Using residual images with BSIF for iris liveness detection. *Expert Syst Appl* 182(March 2020):115266. <https://doi.org/10.1016/j.eswa.2021.115266>
26. “FAKE IRIS DETECTION USING STRUCTURED LIGHT Connell J, N Ratha, James Gentile, Ruud Bolle (2013) Yorktown Heights , NY 10598 { jconnell , ratha } @ us . ibm . com.” pp. 8692–8696
27. Fang M, Damer N, Boutros F, Kirchbuchner F, Kuijper A (2020) “Deep learning multi-layer fusion for an accurate iris presentation attack detection,” *Proc. 2020 23rd Int. Conf. Inf. Fusion, FUSION 2020*, <https://doi.org/10.23919/FUSION45008.2020.9190424>.
28. Fang Z, Czajka A, Bowyer KW (2021) Robust iris presentation attack detection fusing 2D and 3D information. *IEEE Trans Inf Forensics Secur* 16:510–520. <https://doi.org/10.1109/TIFS.2020.3015547>
29. Fang M, Damer N, Boutros F, Kirchbuchner F, Kuijper A (2021) Cross-database and cross-attack Iris presentation attack detection using micro stripes analyses. *Image Vis Comput* 105:104057. <https://doi.org/10.1016/j.imavis.2020.104057>
30. Farmanbar M, Toygar Ö (2017) Spoof detection on face and palmprint biometrics. *Signal, Image Video Process* 11(7):1253–1260. <https://doi.org/10.1007/s11760-017-1082-y>
31. Galbally J, Marcel S, Fierrez J (2014) Image quality assessment for fake biometric detection: application to Iris, fingerprint, and face recognition. *IEEE Trans Image Process* 23(2):710–724. <https://doi.org/10.1109/TIP.2013.2292332>
32. Gautam G, Mukhopadhyay S (2018) “Contact Lens Detection using Transfer Learning with Deep Representations,” *Proc. Int. Jt. Conf. Neural Networks*, vol. 2018-July, pp. 1–8, <https://doi.org/10.1109/IJCNN.2018.8489590>.
33. Gomez-Barrero M, Rathgeb C, Li G, Ramachandra R, Galbally J, Busch C (2018) Multi-biometric template protection based on bloom filters. *Inf Fusion* 42:37–50. <https://doi.org/10.1016/j.inffus.2017.10.003>
34. Goshitasby AAA (2012) Advances in computer vision and pattern recognition
35. Gragnaniello D, Sansone C, Verdoliva L (2015) Iris liveness detection for mobile devices based on local descriptors. *Pattern Recogn Lett* 57:81–87. <https://doi.org/10.1016/j.patrec.2014.10.018>
36. Gragnaniello D, Poggi G, Sansone C, Verdoliva L (2015) An investigation of local descriptors for biometric spoofing detection. *IEEE Trans Inf Forensics Secur* 10(4):849–863. <https://doi.org/10.1109/TIFS.2015.2404294>

37. Gupta R, Sehgal P (2016) A survey of attacks on iris biometric systems. *Int J Biometeorol* 8(2):145–178. <https://doi.org/10.1504/IJBM.2016.077833>
38. Gupta P, Behera S, Vatsa M, Singh R (2014) On iris spoofing using print attack. *Proc - Int Conf Pattern Recognit*:1681–1686. <https://doi.org/10.1109/ICPR.2014.296>
39. He K, Zhang X, Ren S, Sun J (2016) “Deep residual learning for image recognition,” *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, vol. 2016-Decem, pp. 770–778, <https://doi.org/10.1109/CVPR.2016.90>
40. Hu Y, Sirlantzis K, Howells G (2016) Iris liveness detection using regional features. *Pattern Recogn Lett* 82: 242–250. <https://doi.org/10.1016/j.patrec.2015.10.010>
41. Hu Q, Yin S, Ni H, Huang Y (2020) An end to end deep neural network for Iris recognition. *Procedia Comput Sci* 174(2019):505–517. <https://doi.org/10.1016/j.procs.2020.06.118>
42. Huang X, Ti C, Hou QZ, Tokuta A, Yang R (2013) An experimental study of pupil constriction for liveness detection. *Proc IEEE Work Appl Comput Vis*:252–258. <https://doi.org/10.1109/WACV.2013.6475026>
43. Hughes K, Bowyer KW (2013) Detection of contact-lens-based iris biometric spoofs using stereo imaging. *Proc Annu Hawaii Int Conf Syst Sci*:1763–1772. <https://doi.org/10.1109/HICSS.2013.172>
44. Ishfaq DSR, Selwal A (2021) “Fingerprint Spoofing Attacks and their Deep Learning-enabled Remediation: State-of-the-art, Taxonomy, and Future Directions,” pp. 22–28
45. Jain AK, Ross A, Prabhakar S (2004) An introduction to biometric recognition. *IEEE Trans Circuits Syst Video Technol* 14(1):4–20. <https://doi.org/10.1109/TCSVT.2003.818349>
46. Jain AK, Flynn P, Ross AA (2007) Handbook of biometrics
47. Jamdar SD et al (2017) Biometrics: A Tool for Information Security Anil. *IEEE Trans Inf Forensics Secur* 1(Iccmc):125–143
48. Kapur PK, Singh G, Klochkov YS, Kumar U (2020) Decision analytics applications in industry.
49. Kaur B (2020) Iris spoofing detection using discrete orthogonal moments. *Multimed Tools Appl* 79(9–10): 6623–6647. <https://doi.org/10.1007/s11042-019-08281-x>
50. Kaur B, Singh S, Kumar J (2019) Cross-sensor iris spoofing detection using orthogonal features. *Comput Electr Eng* 73:279–288. <https://doi.org/10.1016/j.compeleceng.2018.12.002>
51. Kohli N, Yadav D, Vatsa M, Singh R (2013) Revisiting iris recognition with color cosmetic contact lenses. *Proc - 2013 Int Conf Biometrics, ICB 2013* 1. <https://doi.org/10.1109/ICB.2013.6613021>
52. Kohli N, Yadav D, Vatsa M, Singh R, Noore A (2018) “Synthetic iris presentation attack using iDCGAN,” *IEEE Int. Jt. Conf. Biometrics, IJCB 2017*, vol. 2018-Janua, pp. 674–680 <https://doi.org/10.1109/BTAS.2017.8272756>.
53. O. V Komogortsev, S. Marcos, A. Karpov, and S. Marcos (2013) “Liveness Detection via Oculomotor Plant Characteristics : Attack of Mechanical Replicas”
54. Kuehlkamp A, Pinto A, Rocha A, Bowyer KW, Czajka A (2019) Ensemble of Multi-View Learning Classifiers for cross-domain Iris presentation attack detection. *IEEE Trans Inf Forensics Secur* 14(6):1419–1431. <https://doi.org/10.1109/TIFS.2018.2878542>
55. Liu N, Li H, Zhang M, Liu J, Sun Z, Tan T (2016) Accurate iris segmentation in non-cooperative environments using fully convolutional networks. *2016 Int Conf Biometrics, ICB:2016*. <https://doi.org/10.1109/ICB.2016.7550055>
56. Liu M, Zhou Z, Shang P, Xu D (2020) Fuzzified image enhancement for deep learning in Iris recognition. *IEEE Trans Fuzzy Syst* 28(1):92–99. <https://doi.org/10.1109/TFUZZ.2019.2912576>
57. Long M, Zeng Y (2019) “Detecting Iris Liveness with Batch Normalized Convolutional Neural Network,” *vol. 58*, no. 2, pp. 493–504. <https://doi.org/10.32604/cmc.2019.04378>.
58. Mehmood R, Selwal A (2020) Polynomial based fuzzy vault technique for template security in fingerprint biometrics. *Int Arab J Inf Technol* 17(6):926–934. <https://doi.org/10.34028/iajit/17/6/11>
59. Menotti D, Chiachia G, Pinto A, Robson Schwartz W, Pedrini H, Xavier Falcao A, Rocha A (2015) Deep representations for Iris, face, and fingerprint spoofing detection. *IEEE Trans Inf Forensics Secur* 10(4):864–879. <https://doi.org/10.1109/TIFS.2015.2398817>
60. Minaee S, Abdolrashidi A (2019) “DeepIris: Iris Recognition Using A Deep Learning Approach,” [Online]. Available: <http://arxiv.org/abs/1907.09380>.
61. Pala F Bhanu B (2017) “Iris Liveness Detection by Relative Distance Comparisons,” *IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Work.*, vol. 2017-July, pp. 664–671 <https://doi.org/10.1109/CVPRW.2017.95>.
62. “Presentation attack detection algorithm for face and iris biometrics” (2014) pp. 1387–1391
63. Puhane NB, Sudha N, Hegde S (2011) A new iris liveness detection method against contact lens spoofing. *Proc Int Symp Consum Electron ISCE*:71–74. <https://doi.org/10.1109/ISCE.2011.5973786>
64. Raghavendra R, Busch C (2014) Presentation attack detection on visible spectrum iris recognition by exploring inherent characteristics of Light Field Camera. *IJCB 2014–2014 IEEE/IAPR Int Jt Conf Biometrics*. <https://doi.org/10.1109/BTAS.2014.6996226>

65. Raghavendra R, Busch C (2015) Robust scheme for iris presentation attack detection using multiscale binarized statistical image features. *IEEE Trans Inf Forensics Secur* 10(4):703–715. <https://doi.org/10.1109/TIFS.2015.2400393>
66. Raja KB, Raghavendra R, Busch C (2015) “Presentation attack detection using Laplacian decomposed frequency response for visible spectrum and Near-Infra-Red iris systems,” 2015 *IEEE 7th Int. Conf. Biometrics Theory, Appl. Syst. BTAS 2015*, <https://doi.org/10.1109/BTAS.2015.7358790>.
67. Ratha NK, Connell JH, Bolle RM (2001) An analysis of minutiae matching strength. *Lect Notes Comput Sci (including Subser Lect Notes ArtifIntell Lect Notes Bioinformatics)* 2091 LNCS(2015):223–228. https://doi.org/10.1007/3-540-45344-x_32
68. Ribeiro E, Uhl A (2017) Exploring Texture Transfer Learning via Convolutional Neural Networks for Iris Super Resolution. *Lect Notes Informatics (LNI), Proc - Ser Gesellschaft fur Inform* (00736):0–4. <https://doi.org/10.23919/BIOSIG.2017.8053505>
69. Rigas I, Komogortsev OV (2015) Eye movement-driven defense against iris print-attacks. *Pattern Recogn Lett* 68:316–326. <https://doi.org/10.1016/j.patrec.2015.06.011>
70. Rui Z, Yan Z (2019) A survey on biometric authentication: toward secure and privacy-preserving identification. *IEEE Access* 7(c):5994–6009. <https://doi.org/10.1109/ACCESS.2018.2889996>
71. Sardar M, Banerjee S, Mitra S (2020) Iris segmentation using interactive deep learning. *IEEE Access* 8: 219322–219330. <https://doi.org/10.1109/ACCESS.2020.3041519>
72. Selwal A, Gupta S, Kumar S (2016) A Scheme for Template Security At Feature Fusion Level in Multimodal Biometric System. *Adv Sci Technol Res J* 10(31):23–30. <https://doi.org/10.12913/22998624/64062>
73. Selwal A, Gupta SK, Surender (2017) Low overhead octet indexed template security scheme for multimodal biometric system. *J Intell Fuzzy Syst* 32(5):3325–3337. <https://doi.org/10.3233/JIFS-169274>
74. Sequeira AF, Oliveira HP, Monteiro JC, Monteiro JP, Cardoso JS (2014) “Mobilive 2014 - Mobile Iris Liveness Detection Competition,” *IJCB 2014–2014 IEEE/IAPR Int. Jt. Conf. Biometrics*, <https://doi.org/10.1109/BTAS.2014.6996290>.
75. Sharma D, Selwal A (2021) *An intelligent approach for fingerprint presentation attack detection using ensemble learning with improved local image features*, no. 0123456789. Springer US.
76. Sharma D, Selwal A (2021) FinPAD: State-of-the-art of fingerprint presentation attack detection mechanisms, taxonomy and future perspectives. *Pattern Recogn Lett* 152(March 2005):225–252. <https://doi.org/10.1016/j.patrec.2021.10.013>
77. Sharma D, Selwal A (2021) HyFiPAD : a hybrid approach for fingerprint presentation attack detection using local and adaptive image features. *Vis Comput* 38(0123456789):2999–3025. <https://doi.org/10.1007/s00371-021-02173-8>
78. Silva P, Luz E, Baeta R, Pedrini H, Falcao AX, Menotti D (2015) “An Approach to Iris Contact Lens Detection Based on Deep Image Representations,” *Brazilian Symp. Comput. Graph. Image Process.*, vol. 2015-Octob, pp. 157–164 <https://doi.org/10.1109/SIBGRAP.2015.16>.
79. Simonyan K, Zisserman A (2015) “Very deep convolutional networks for large-scale image recognition,” *3rd Int. Conf. Learn. Represent. ICLR 2015 - Conf. Track Proc.*, pp. 1–14
80. Singh M, Singh R, Ross A (2019) A comprehensive overview of biometric fusion. *Inf Fusion* 52:187–205. <https://doi.org/10.1016/j.inffus.2018.12.003>
81. Szegedy C, Vanhoucke V, Ioffe S, Shlens J, Wojna Z (2016) Rethinking the Inception Architecture for Computer Vision. *Proc IEEE Comput Soc Conf Comput Vis Pattern Recognit* 2016:2818–2826. <https://doi.org/10.1109/CVPR.2016.308>
82. Tan M, Le QV (2019) “EfficientNet: Rethinking model scaling for convolutional neural networks,” *36th Int. Conf. Mach. Learn. ICML 2019*, vol. 2019-June, pp. 10691–10700
83. Tann H, Zhao H, Reda S (2019) A resource-efficient embedded iris recognition system using fully convolutional networks. *ACM J Emerg Technol Comput Syst* 16(1):1–23. <https://doi.org/10.1145/3357796>
84. Tapia JE, Gonzalez S, Busch C (2022) Iris liveness detection using a Cascade of dedicated deep learning networks. *IEEE Trans Inf Forensics Secur* 17:42–52. <https://doi.org/10.1109/TIFS.2021.3132582>
85. Therar HM, Mohammed LDEA, Ali APDAJ (2021) “Multibiometric System for Iris Recognition Based Convolutional Neural Network and Transfer Learning,” *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1105, no. 1, p. 012032, <https://doi.org/10.1088/1757-899x/1105/1/012032>.
86. Tirunagari S, Poh N, Windridge D, Iorliam A, Suki N, Ho ATS (2015) Detection of face spoofing using visual dynamics. *IEEE Trans Inf Forensics Secur* 10(4):762–777. <https://doi.org/10.1109/TIFS.2015.2406533>
87. Tobji R, Di W, Ayoub N (2019) FMnet: Iris segmentation and recognition by using fully and multi-scale CNN for biometric security. *Appl Sci* 9(10):1–17. <https://doi.org/10.3390/app9102042>

88. Varkarakis V, Bazrafkan S, Corcoran P (2018) “A deep learning approach to segmentation of distorted iris regions in head-mounted displays,” 2018 IEEE Games, Entertain. Media Conf. GEM 2018, pp. 402–406 <https://doi.org/10.1109/GEM.2018.8516446>
89. Yadav D, Kohli N, Doyle JS, Singh R, Vatsa M, Bowyer KW (2014) Unraveling the effect of textured contact lenses on iris recognition. *IEEE Trans Inf Forensics Secur* 9(5):851–862. <https://doi.org/10.1109/TIFS.2014.2313025>
90. Yambay D, Doyle JS, Bowyer KW, Czajka A, Schuckers S (2014) “LivDet-iris 2013 - Iris Liveness Detection Competition 2013,” *IJCB 2014–2014 IEEE/IAPR Int. Jt. Conf. Biometrics*, <https://doi.org/10.1109/BTAS.2014.6996283>.
91. Yambay D, Czajka A, Li F (2015) “LivDet-Iris 2015 – Iris liveness detection competition 2015 University of Naples”
92. Yambay D *et al.* (2018) “LivDet iris 2017 - Iris liveness detection competition 2017,” *IEEE Int. Jt. Conf. Biometrics, IJCB 2017*, vol. 2018-Janua, pp. 733–741, <https://doi.org/10.1109/BTAS.2017.8272763>.
93. Yang Y, Shen P, Chen C (2019) A robust iris segmentation using fully convolutional network with dilated convolutions. *Proc - 2018 IEEE Int Symp Multimedia, ISM 2018*:9–16. <https://doi.org/10.1109/ISM.2018.00010>
94. Zhang H, Sun Z, Tan T (2010) Contact lens detection based on weighted LBP. *Proc - Int Conf Pattern Recognit*:4279–4282. <https://doi.org/10.1109/ICPR.2010.1040>
95. Zhang H, Sun Z, Tan T, Wang J (2011) “Learning hierarchical visual codebook for Iris liveness detection”
96. Zhao Z, Kumar A (2017) “Towards More Accurate Iris Recognition Using Deeply Learned Spatially Corresponding Features.” *Proc. IEEE Int. Conf. Comput. Vis.*, vol. 2017-October, pp. 3829–3838, <https://doi.org/10.1109/ICCV.2017.411>.
97. Zhao Z, Kumar A (2019) A deep learning based unified framework to detect, segment and recognize irises using spatially corresponding features. *Pattern Recogn* 93:546–557. <https://doi.org/10.1016/j.patcog.2019.04.010>

Publisher’s note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.