*inventions*

MDPI

*Review*

# Iris Liveness Detection for Biometric Authentication: A Systematic Literature Review and Future Directions

**Smita Khade [1], Swati Ahirrao [1,*], Shraddha Phansalkar [2], Ketan Kotecha [3,*], Shilpa Gite [1,3] and Sudeep D. Thepade [4]**

[1] Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune 412115, India; smita.khade.phd2020@sitpune.edu.in (S.K.); shilpa.gite@sitpune.edu.in (S.G.)
[2] Department of Computer Engineering, MIT Art, Design and Technology University, Pune 412201, India; shraddhaphansalkar@gmail.com
[3] Symbiosis Centre for Applied Artificial Intelligence, Symbiosis International (Deemed University), Pune 412115, India
[4] Department of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune 411044, India; sudeepthepade@gmail.com
* Correspondence: swatia@sitpune.edu.in (S.A); head@scaai.siu.edu.in (K.K.)

**Abstract:** Biometrics is progressively becoming vital due to vulnerabilities of traditional security systems leading to frequent security breaches. Biometrics is an automated device that studies human beings' physiological and behavioral features for their unique classification. Iris-based authentication offers stronger, unique, and contactless identification of the user. Iris liveness detection (ILD) confronts challenges such as spoofing attacks with contact lenses, replayed video, and print attacks, etc. Many researchers focus on ILD to guard the biometric system from attack. Hence, it is vital to study the prevailing research explicitly associated with the ILD to address how developing technologies can offer resolutions to lessen the evolving threats. An exhaustive survey of papers on the biometric ILD was performed by searching the most applicable digital libraries. Papers were filtered based on the predefined inclusion and exclusion criteria. Thematic analysis was performed for scrutinizing the data extracted from the selected papers. The exhaustive review now outlines the different feature extraction techniques, classifiers, datasets and presents their critical evaluation. Importantly, the study also discusses the projects, research works for detecting the iris spoofing attacks. The work then realizes in the discovery of the research gaps and challenges in the field of ILD. Many works were restricted to handcrafted methods of feature extraction, which are confronted with bigger feature sizes. The study discloses that dep learning based automated ILD techniques shows higher potential than machine learning techniques. Acquiring an ILD dataset that addresses all the common Iris spoofing attacks is also a need of the time. The survey, thus, opens practical challenges in the field of ILD from data collection to liveness detection and encourage future research.

**Keywords:** biometric authentication; iris; liveness detection; identification; machine learning; deep learning; feature extraction; classification; iris datasets

check for updates

**Citation:** Khade, S.; Ahirrao, S.; Phansalkar, S.; Kotecha, K.; Gite, S.; Thepade, S.D. Iris Liveness Detection for Biometric Authentication: A Systematic Literature Review and Future Directions. *Inventions* **2021**, *6*, 65. https://doi.org/10.3390/inventions6040065

Academic Editor: Shoou-Jinn Chang

Received: 24 August 2021
Accepted: 26 September 2021
Published: 6 October 2021

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

**Copyright:** © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

## 1. Introduction

During the primeval eras, there were restricted choices and ways for personal identification. Nowadays, we have an era of computer vision and biometrics, which does not involve any external artifact or token to recognize others. Instead, individuals can be acknowledged with their own biological or behavioral features with the aid of biometrics as an alternative to their associations, possessions, or any secret information.

The necessity of mechanized and precise identification directed us to biometrics, which controls technology to accelerate the course of human identification and authentication. The biometric ID has been originated and replaced the printed IDs. This allows you to verify your identity, deprived of carrying any card or document (www.bayometric.com

(accessed on 4 August 2021)). The authentication is a vital stage for offering admittance to the resources to the approved individuals. Conventional authentication systems such as a pin, card, and password cannot differentiate between real users and imposters who have fraudulently accessed the system [1,2]. There are many possibilities of forgetting the password/pin or stealing and misplacement of the card. The device that allows the automatic identification of an individual is known as a biometric system. The biometric authentication system is easy to use, and there is no need to remember a password, card, and pin code.

Biometrics have been extensively discovered for their automation, approachability, and accuracy with the mounting security needs of our everyday lives. It is a mechanized device that studies human beings' physiological and behavioral features [3] for their unique classification as the technology has differentiated from detection to criminal identifications and forensics.

There are several diverse markets of biometric technology which exist today. Most of the markets appear to be mounting swiftly. The global biometric technologies market is anticipated to reach 19.08 billion US dollars in 2021, while the contactless biometric technologies market is predicted to grow to over 30.15 billion US dollars by 2027 (www.statista.com (accessed on 4 August 2021)). Biometrics have been successfully deployed in a variety of applications where security is of primary concern. For example, airport check-in and check-out personal identification cards [3]; sensitive information from unauthorized users, and credit card authentication.

Several biometric characteristics such as the fingerprint, iris, palm print, and the face, are used for authentication and recognition. As compared to fingerprint and face, the iris-based authentication provides stronger contactless identification of the user. Table 1 displays various applications domains for iris biometric detection.

**Table 1.** Various application domains for biometric iris recognition system.

| Application Areas | Usage |
| --- | --- |
| Finance and Banking | Authentication system for banking domain [4]. |
| Healthcare and welfare | Tracking the patient registration, repetitive treatment, supporting national or private health insurance cards [5]. |
| Immigration and border control | The United States, Canadian airports, the Netherlands, in Europe, and Heathrow airport, in London [6]. |
| Public safety | Used by law enforcement agencies to track and identify criminals [6]. |
| Point of sale and ATM | Used by bank ATMs, retail merchants and restaurants [7]. |
| Hospitality and tourism | Iris scanning door entry system for guest identification and access control [8]. |

The contactless approach helps to prevent the spread of viruses and diseases such as COVID-19. Iris has complex textures and unique features, so it is widely used in identifying and authentication the person in many applications [9]. Aadhar project uses the biometric system to identify the citizens of India, Amsterdam airport, and the US Canadian border [10]. Even though the iris has a unique texture pattern, there is a possibility of spoofing by the imposter. People attack the biometric device to obtain the rights of others.

Iris detection systems can be easily spoofed by using different types of contact lens such as transparent lenses, colored lenses, and textured lenses. By using the transparent lenses, the fraudster cannot alter the iris texture but can modify the reflection property of the Iris recognition system [11]. An imposter can conceal the real texture of an Iris with the aid of textured color lenses. The system can also be rapidly spoofed by replaying a video as well as a print attack. This means the iris pattern is acquainted with the machine by printing an iris image. Print attacks are performed in two modes: [12]. First is print and scan, in which the high-quality printed iris pattern is scanned, and second is print and capture, in which the scanner takes the snapshot.

Due to vulnerabilities in traditional security systems that lead to frequent security breaches, biometrics is increasingly becoming important [3]. Thus, ILD for biometric authentication is a significant research area.

### *1.1. Significance and Relevance*

As the field advanced, several biometric characteristics developed, and from time to time, faded away. Nevertheless, "one biometric trait that has assuredly endured the test of time is iris recognition. The iris pattern is exclusive. It consequently offers high discrimination power, making it suitable in distinguishing even identical twins." [13]. Furthermore, compared to fingerprint and face, the iris-based authentication provides stronger and contactless user identification. Thus, iris biometrics has become the preferable research field with its secured identity and serves as the basis for the innovative biometric system. However, iris biometric devices are enormously vulnerable by using printed iris images or artifacts to spoof invader challenges and disrupt the iris recognition system. For this reason, several researchers focus on noticing iris liveness to guard the biometric system from attack [14].

Hence, it is vital to classify the prevailing researches precisely associated with the biometric of ILD, with the purpose to address how evolving technologies can offer explanations to lessen the developing threats [15].

The existing literature on ILD focuses on hardware and software trends, and different classification techniques using ML-based and DL-based approaches [16]. It is indispensable to have a "comparative analysis of these techniques based on" numerous evaluation metrics. It is obligatory to work out the relevant papers and academic works methodically to recognize what research has been steered concerning biometric and ILD [15]. This survey aims to shed light on a variety of datasets, performances measures used, iris spoofing attacks, and techniques used for detection of iris liveness.

### *1.2. Evolution of Iris Biometric Authentication System*

The earlier work on biometric identification was performed by using fingerprints and other biometric traits. In 1985 first time, irises, which were unique to everyone, were proposed. The first iris recognition algorithm was developed in 1994.

Since 2013, machine learning (ML) technology has been widely used in ILD research. The ability of ML to classify and forecast is a significant reason for employing these algorithms. ILD employs various algorithms, including logistic regression, SVM, Ad Boost, and Random Forest. Figure 1 displays the timeline of iris biometric authentication (fingercheck.com (accessed on 4 August 2021)) highlights some of the most pivotal historical moments in the development of itis biometrics. Deep learning (DL) algorithms are used to process enormous amounts of information. With the introduction of deep learning approaches for iris liveness detection, the researchers began using deep Learning technology.

As the deep learning algorithms offer better features than traditional handcrafted features, researchers have chosen DL approaches for iris liveness detection. Some researchers started working on the pre-trained network such as convolutional neural networks (CNN), VGG16, ResNet50, the Inception-v3 model, GoogleNet, and AlexNet, used for iris liveness detection.

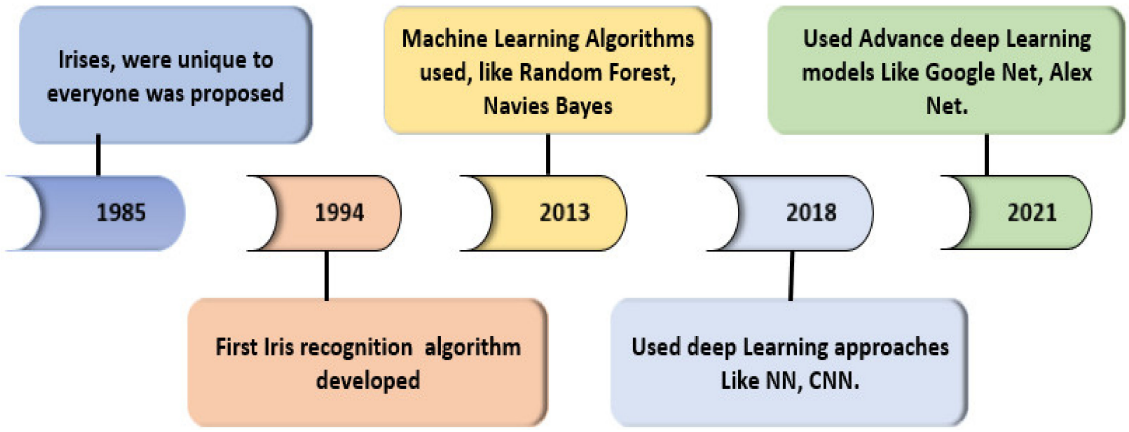



**Figure 1.** Evolution of iris biometric identification.

### *1.3. Prior Research*

"There are very scarce systematic literature reviews (SLR)" obtainable in the ILD research area to the best of our knowledge. The study [17] is one of the current and important SLR providing a good outline of liveness detection techniques to face anti-spoofing. Furthermore, the study enhances value to the literature by contributing valued perceptions into various liveness detection techniques and face anti-spoofing techniques.

The authors discussed how face liveness detection can be used for biometric identification of the person. The authors highlighted some important techniques used for liveness detection, such as liveness detection techniques based on motion analysis, texture analysis, liveness based on life sign indicators, and some other liveness indicators. The author also discussed different publicly available datasets for face liveness detection.

However, the survey lacks a thorough conversation of the prevailing liveness detection techniques for Iris Biometric Authentication.

Chen et al. [14] converse Sensor-level and Feature-level methods of Iris Liveness Detection. Sensor-level methods have a reasonable detection rate but are comparatively expensive and inflexible, while feature-level methods are accepted as cost-effective and flexible. Furthermore, the authors claim that the approach based on analyzing variations in texture patterns has an extraordinary presentation.

Nguyen et al. [18] conducted a widespread study of long-range Iris Recognition. The study converses the prevailing systems and their restrictions and three easily accessible general population datasets, "UBIRIS V2.0, CASIA-Iris-Distance", and MBGC. The authors also converse the limits of the recognition methods. Dronky et al. [19] claim that the maximum of the ILD was planned to identified certain sorts of "fake iris patterns or used private datasets. This is not appropriate in real-world situations", where the system should detect diverse varieties of spoofing attacks. Thus, the author claims a scope for up-gradation in ILD techniques to guard the iris recognition systems contrary to spoofing attacks.

Rattani and Derakhshani [20] offered an overview of visible-spectrum optical recognition methods. The authors depict the seven datasets acquired in the visible spectrum. However, several of the datasets referenced by the researchers are no more accessible despite the assertions of the unique researchers of the datasets. In their future work, the authors described that the researchers might emphasize the data upgrading techniques. Our SLR converses the few data upgrading techniques, in that way escalating the performance of the model.

As the part of the previous study few limitations are noted that can be described as follows:

1. Only one SLR is available related to this domain.
2. The Prevailing literature does not scrutinize the generalizability of the spoofing attacks techniques to recognize the diverse sorts of attacks.

3. The discussion on the different performances measures used is not revealed in the prevailing assessments.
4. There are limited studies that surveyed feature extraction techniques and datasets obtainable for the iris liveness detection.

Our SLR is thorough in showcasing the up-to-date growths or trends and challenges associated with the ILD by endeavoring thorough surveys on handcrafted based and deep learning-based liveness detection techniques, accessibility, and the of publicly available datasets and evaluation metrics. Furthermore, our SLR presents a relative analysis of the techniques used for iris liveness detection. It also offers future research directions by stressing the research gaps. The role aim of the paper is to present the high-level framework of a robust attack detection system in iris liveness detection.

### *1.4. Motivation*

The literature displays an absence of SLR that attends on the ILD techniques concealing their obvious advantages, drawbacks, ontologies, and comparative study. The prevailing literature lacks a complete survey fixated on the publicly accessible datasets and self-built datasets. The literature also lacks a thorough study on diverse techniques used for ILD and performances measures used during the application. The previous work shows a lack of detection of iris spoofing attacks.

The crux of this SLR is to focus on the existing facts regarding:

- The prevailing ILD techniques and their confines to recognize spoofing attacks.
- The comparative analysis of different types of spoofing attacks used in iris liveness detection.
- Publicly available datasets for iris biometric detection.
- Different performance measures used for implementation of iris liveness.

Therefore, the planned SLR intends to offer the visions on multiple feature extraction techniques, spoofing attacks, datasets, and performances measures used for iris biometric detection.

### *1.5. Research Goals*

This investigation aims to examine the prevailing studies and their outcomes and compare the existing Biometric ILD techniques. Therefore, to get a thorough survey of iris liveness detection, research questions are projected. Table 2 displays the survey questions that were organized to make this SLR study more intensive.

**Table 2.** Research Question.

| RQ No | Research Questions (RQ) | Objective/Discussion |
|---|---|---|
| RQ1 | What are the different Features Extraction Techniques for Iris Liveness Detection? | Find out different Feature Extraction Techniques used for Iris Liveness Detection. |
| RQ2 | What are the different types of spoofing attacks performed on Iris Liveness Detection? | This question provides information about the types of attacks needed to consider for implementing the ILD system. Considering all the types of attacks increases the security of Biometric systems. |
| RQ3 | Which are the relevant datasets available for iris liveness detection? | By identifying different publicly available datasets, which can serve as benchmarks, evaluate performances of the different approaches and provide the jump start to the new researchers. |
| RQ4 | What are the different evaluation measures used for iris liveness detection? | Different standards and metrics used most frequently for liveness detection are discussed. |

### *1.6. Contributions of the Study*

The following are the contributions of our systematic literature review:

- A comparison of the methodologies in literature employed for detecting and classifying iris liveness was presented.
- To study feature extraction techniques which were used with ILD in the literature.
- Survey identified, to detect all the types of iris spoofing attacks and the literary works addressing the same were studied.
- To study and compare available data sets in the literature constructed for detecting ILD and spoofing attacks.
- To analyze ILD methods using various evaluation metrics.
- Figure 2 depicts how our SLR is organized into distinct segments.

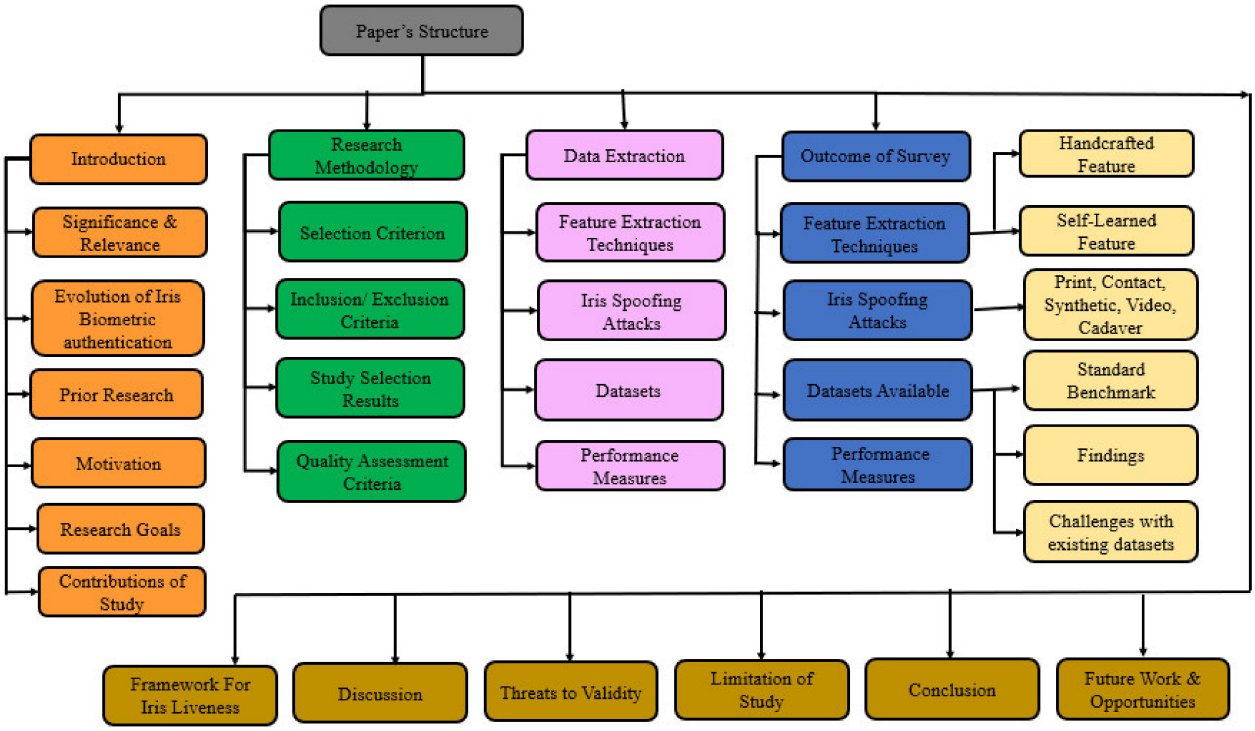



**Figure 2.** Organization of SLR.

## 2. Research Methodology

Table 2 depicts the research questions with their respective goals. Formulating the research question is a crucial task in a systematic literature review. Figure 3 shows the PRISMA flowchart guidelines, which were suggested by Kitchenham and Charters [21] to answer the framed research questions by opting for the most appropriate research studies. Finally, Figure 4 displays the SLR process followed for ILD.

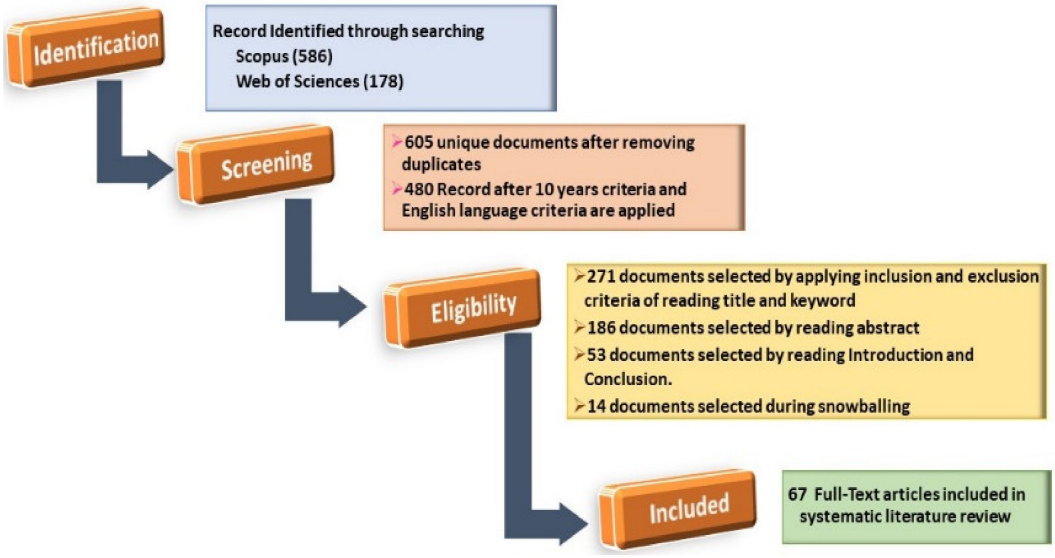



**Figure 3.** PRISMA flowchart for the selection of relevant papers.

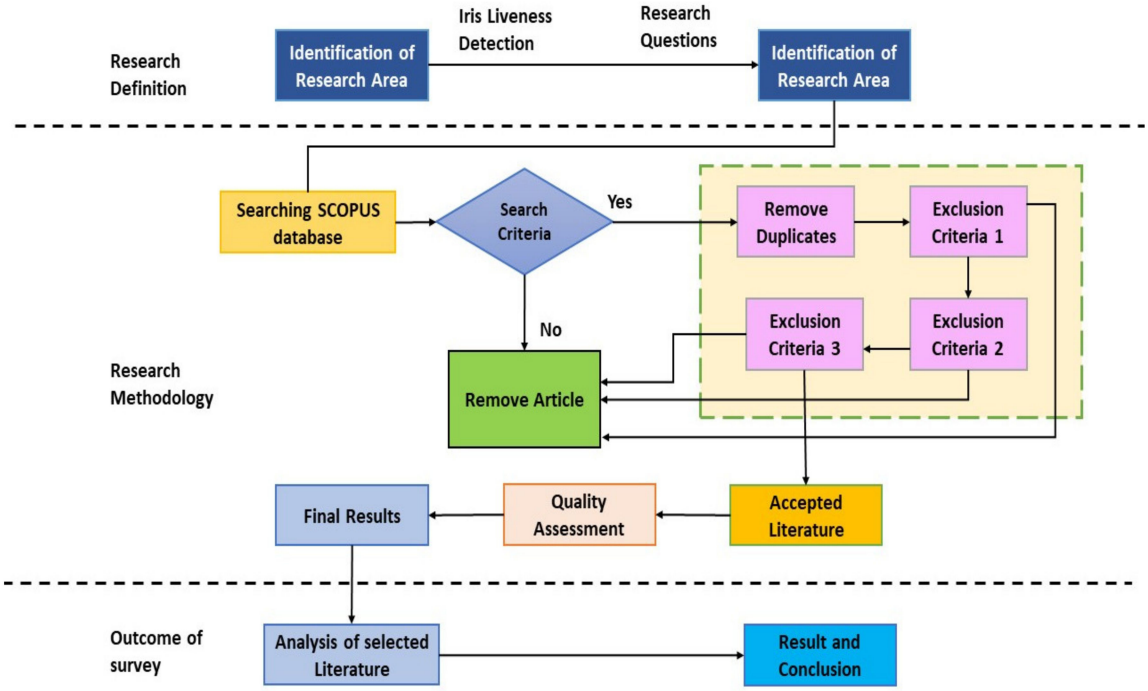



**Figure 4.** Systematic literature review (SLR) process.

### *2.1. Selection Criterion for Research Studies*

It was perceived that different digital libraries recurrently gave back those numerous papers through carrying out introductory searches. After bearing in mind this fact, we decided to use only Scopus, ACM, and Web of Sciences databases. The search was conducted on 28 June 2021 between January 2010 and June 2021 in the Scopus and Web of Sciences. The search query was defined by using different keywords related to the iris biometric liveness detection system using the iris identity in the following way:

Biometric AND (Recognition OR Identification OR Detection OR Liveness OR Classification OR Feature Extraction) AND (Iris OR Multimodal) AND (Deep Learning OR Artificial Intelligence OR Machine Learning OR AI OR Network Analysis)

It is also perceived that search queries were expressed to attain all the relevant results connected to the research questions presented in this study based on iris biometric detection. The results obtained and the query passed to each dataset are presented in Table 3.

**Table 3.** Results from searches conducted on databases.

| Database | Query | Search Result |
| --- | --- | --- |
| Scopus | TITLE-ABS KEY (“Biometric” AND (“Recognition “OR “Identification” OR “detection” OR “Liveness” OR “Classification” OR “Feature Extraction”) AND (“Iris” OR “Multimodal”) AND (“Deep Learning” OR “artificial intelligence” OR “machine learning” OR “AI” OR “network analysis”)) | 586 |
| Web of sciences | TOPIC: ((“Biometric” AND (“Recognition “OR “Identification” OR “detection” OR “Liveness” OR “Classification” OR “Feature Extraction”) AND (“Iris” OR “Multimodal”) AND (“Deep Learning” OR “artificial intelligence” OR “machine learning” OR “AI” OR “network analysis”)) | 178 |
| ACM | [All: “biometric”] AND [[All: “recognition “] OR [All: “identification”] OR [All: “detection”] OR [All: “liveness”] OR [All: “classification”] OR [All: “feature extraction”]] AND [[All: “iris”] OR [All: “multimodal”]] AND [[All: “deep learning”] OR [All: “artificial intelligence”] OR [All: “machine learning”] OR [All: “ai”] OR [All: “network analysis”]] | 331 |

### *2.2. Inclusion and Exclusion Criteria*

Our requirements for inclusion and exclusion are presented in Table 4. To limit the application domain, context, and form of the outcome, three inclusion criteria were set. First, excluded articles, such as keynotes, books, dissertations, papers not published in English, and papers that were not peer-reviewed. By including peer-reviewed articles, it was assured that our results are originated from a high-quality source. Second, it should be clarified that short articles (less than six pages) did not explicitly exempt work-in-progress papers and pre-print papers, such as most other SLR reports. The purpose is that this field of study is far from advanced, so it is still important to review the several initial thoughts or in-progress articles.

**Table 4.** Inclusion and exclusion criteria for the primary studies.

| Inclusion Criteria | Exclusion Criteria |
| --- | --- |
| A context in Iris Liveness Detection, either in broad or tailored to a certain application domain. | Papers not peer-reviewed, Duplicate papers. |
| Aimed at Software-based Liveness Detection approaches. | Written in the languages except for English. |
| Aimed at ILD approaches for Deep Learning-based and Machine Learning-based. | Absence of full text |

During this study, conference articles included, as in this field some really good work is published in the top international conferences. In addition, a series of meetings were also conducted with all the co-authors to validate the relevance of the selected papers to the topic.

During this study, we included conference articles, as in this field some really good work is published in the top international conferences. We also conducted a series of meeting with all the co-authors to validate the relevance of the selected papers to the topic.

### *2.3. Study Selection Results*

As outline in Figure 3, the selection process consisted of four parts as given below:

Stage 1 (Identification): Ran the search string on the Web of Sciences, ACM and Scopus Index database and retrieved 1095 papers.

Stage 2 (Screening): After eliminating those duplicated papers, we had 605 papers. At the end of this stage, we selected 480 records by applying ten years (January 2010–June 2021) and English language criteria.

Stage 3 (Eligibility): The papers were recognized through dataset searching and omitted publications based on title and keywords. The publications were maintained for further research if they could not be omitted merely by reading titles and keywords. Finally, 271 papers were chosen and refined further by reading abstracts. As a result, 186 prospective papers relevant to our SLR's study topic were found.

Read the prologue and conclusion before making a decision. Then, the reasons for the exclusion for each excluded paper were recorded. Finally, papers that were irrelevant or for which complete full texts were unavailable were removed.

As a result, it was ended up with 53 papers. On these papers, backward snowballing applied (this involves looking to see if any other relevant papers were published after the chosen one and cited the chosen one). In our SLR, mainly backward snowballing was adapted to take in the additional papers. However, to keep the breadth of the snowballing to a minimum, only looked at references published between 2010 and 2021.

Stage 4 (Included): 14 new relevant papers were found from snowballing. To conclude, for a detailed review, 67 articles as primary investigations were considered. The first author directed the selection process with the confrontational discussions with the second and third authors.

### *2.4. Quality Assessment Criteria for the Research Studies*

For any research publication to pass the demarcated selection phase, a wide-ranging quality assessment criterion was well-defined. A score from 1 to 4 (1 being the least relevant and 4 the most relevant) for each designated article was provided. According to our criteria and experience, choosing only those that scored from 3 to 4. Table 5 shows that four quality assessment criteria to estimate the primary studies have been defined. Hence, the research studies that satisfied a quality score of 4 were engaged in the ultimate selection. All of the 67 primary studies that were chosen passed these quality checks.

**Table 5.** Quality Assessment Criteria.

| Quality Assessment Criteria | Score |
|---|---|
| Have the studies provided findings and results? | Yes = 1 No = 0 |
| Has the study provided an empirical proof on the findings? | Yes = 1 No = 0 |
| Are the research objectives and arguments well justified in the paper? | Yes = 1 No = 0 |
| Is the study well written and cited? | Yes = 1 No = 0 |

## 3. Focus Areas in Study of Iris Liveness Detection Literature

A thematic diagram was formed by reviewing the title, abstract, and full text of the designated work of ILD literature. Figure 5 shows every liveness detection study, follows themes such as liveness detection techniques, spoofing attacks, datasets, and performance measures. These themes are planned by the first author and revised by the second and third authors. Following the theme, information from the specific literature was selected depending on the study questions. Following the theme extraction, nine kinds of information from the particular papers were retrieved, as shown in Table 6.

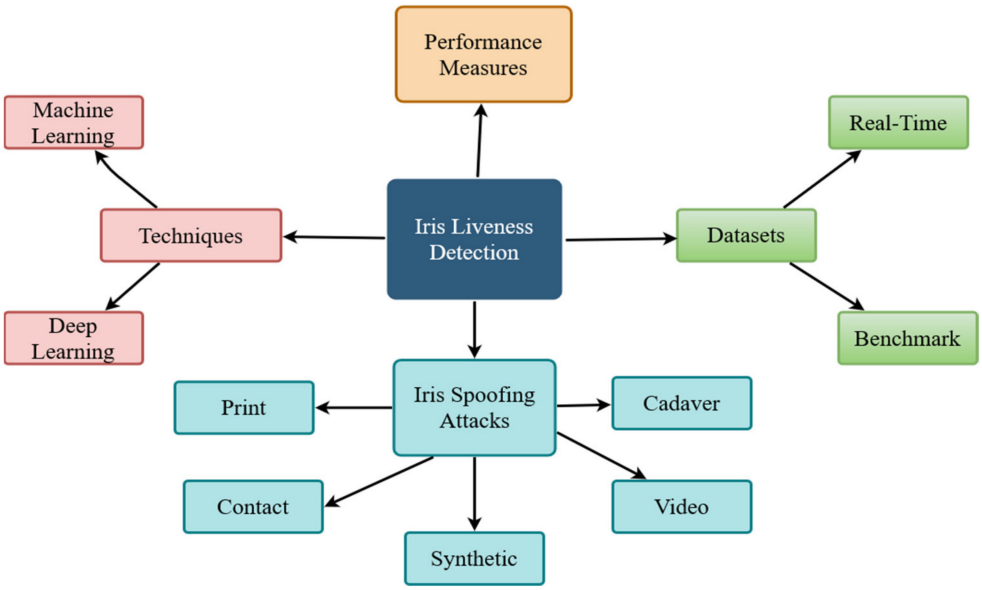



**Figure 5.** Thematic diagram for iris liveness detection.

**Table 6.** Data from iris liveness detection literature.

| Scheme | Data |
|---|---|
| 1 | Title |
| 2 | Year of the document |
| 3 | Conference or journal name |
| 4 | Keywords in the document |
| 5 | AI category (we created the categories: Machine Learning and Deep Learning) |
| 6 | Machine\Deep Algorithm Used (CNN, DNN, Texture analysis) |
| 7 | Datasets used |
| 8 | Type of attack identified (we created the categories: Print, Contact, Synth, Video, Cadaver). |
| 9 | Performance Measure used (ACE, Accuracy) |

Depending on the research questions, "information was extracted from the selected articles. For RQ1, literary works on ILD were classified as machine learning", and deep learning approaches. The different types of handcrafted and deep learning feature extraction techniques used for ILD are extracted from the literature. Reading the entire text of the literature was used to get this information. For RQ2, diverse types of iris attacks identified in the literature are extracted. To answer RQ3, we originated different datasets, dimensions of those datasets, the number of spoofed and live images sensors used to obtain those images. The diverse evaluation metrics used for ILD were extracted for answering RQ4.

The next sections were condense the in-depth discussions of themes, scrutiny of the eliminated data, and its significance in the ILD study. Figure 5 displays the flow and taxonomy of themes in which the prevailing literature is analyzed to respond to all the expressed research questions. Finally, a thematic diagram is constructed using the title, abstract, and entire transcript of the selected works. Techniques, spoofing attacks, datasets, and performance measures are the four key themes in the ILD thematic diagram. The first author creates the themes, which the second and third authors then review.

### *3.1. Feature Extraction Techniques Used for Iris Liveness Detection*

In the machine learning approach of iris liveness detection, the researchers apply handcrafted image feature extraction algorithms to retrieve image features from iris images. First, handcrafted feature extraction techniques such as LBP, local descriptors, quality analysis, SIFT, BSIF, histogram, and wavelet transform are used for feature extraction. Then the classification methods are used, such as support vector machines (SVM), random

forest, MLP, Naive Bayes, random trees, etc., to categorize the images into two classes of live images spoofed images, based on the extracted image features. The preceding methods' findings indicate that hand-engineered features are suitable for overcoming the PAD issue in "iris recognition systems". However, their disadvantage is that the design and selection of Handcrafted Feature Extractors are chiefly based on the expert knowledge of the researchers on the" problem.

The Deep Learning-based approach is alike the ML-based approach. The only variance lies in the "Detection algorithms and the used Models. Deep learning comprises the different models such as convolutional neural networks (CNNs)", VGG-16, ResNet, Google Net, and Alex Net, etc. The DL-based approach employs two types of models: regular models, which are models that are trained from the ground up using training data, and pre-trained models, which are models that are trained on data or features extracted from the same domain. Studies that used handcrafted feature extraction using machine learning approaches are explained in detail in Section 4.1.1. and deep learning approaches are explained in Section 4.1.2.

### *3.2. Iris Spoofing Attacks*

"Iris biometric systems are inclined to the spoofing attacks that lessen their security [19]". The diverse types of spoofing attacks undertaken on the system are recorded below:

- Print attacks—The imposter offers a printed image of validated iris to the biometric sensor.
- Contact Lenses attacks—The imposter wears contact lenses on which the pattern of a genuine iris is printed.
- Video attacks—"Imposter plays the video of registered identity in front of a biometric system" [14].
- Cadaver attacks—Imposter uses the eye of a dead person in front of biometric system.
- Synthetic attacks—"Embedding the iris region into the real images makes the synthesized images more realistic" [22].

All these attacks are explained in detail in the Section 4.2.

### *3.3. Datasets Used for Iris Liveness Detection*

For implementing iris liveness detection, two different types of datasets are used:

- Real-Time datasets—Some authors created their own datasets for testing the modal of iris liveness detection.
- Standard Benchmark Datasets—Many universities created datasets and published datasets so that anyone can use them for implementation. Standard available datasets for ILD are explained in detail in Section 4.3.

### *3.4. Performance Measures*

The diverse types of performance measures are used in literature to measure the performance of the ILD system. ILD is a classification problem. Therefore, many authors used accuracy, precision, recall, F-ratio, and ROC curve, which is recurrently used classification metrics. In addition, some authors used standardized biometric performance measures, which are clarified in Section 4.4.

## 4. Outcome of Survey

In this section, every RQ discusses in detail. What are the various feature extraction approaches used for detecting iris liveness? What types of assaults are made against the iris biometric system? What are the available standard datasets? What are the different performances measures used for identifying iris spoofing attacks?

### *4.1. Feature Extraction Techniques Used for Iris Liveness Detection (RQ1)*

Feature extraction is a process that identifies the important attributes from the iris image. It is competently signified, so that appropriate information of the Iris image is

captured effectually. Feature extraction helps to reduce the amount of redundant data from the images. Furthermore, it increases the accuracy of iris detection models by extracting features from the input iris image. These extracted features are used to differentiate between real and spoof iris images.

The two types of feature extraction techniques were identified in the literature used for biometric iris detection, namely handcrafted feature extraction and self-learned feature extraction. Selected literature categorized based on feature extraction techniques used for iris liveness detection. Figure 6 displays different feature extraction techniques for iris liveness detection.

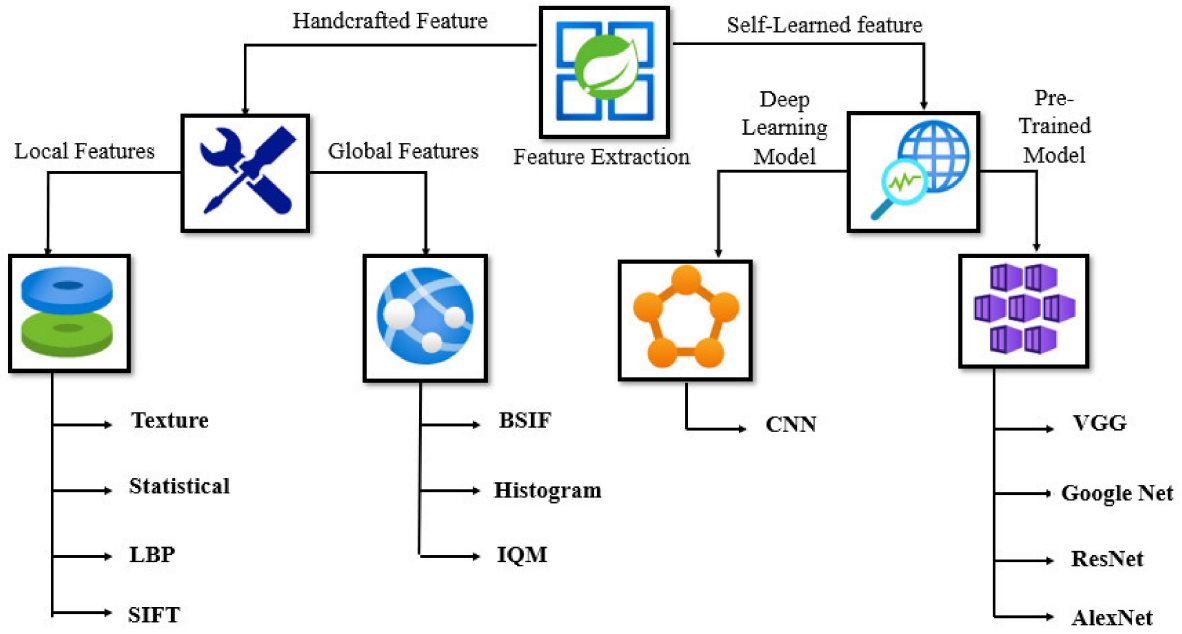



**Figure 6.** Feature extraction techniques for iris liveness detection.

#### 4.1.1. Handcrafted Feature Extraction

In handcrafted Feature Extraction techniques, manually selected features are used to solve the PAD problem related to the iris recognition systems. Based on the size of image patches considered for feature extraction from the iris image, handcrafted features are categorized into two types, local features extraction and global features extraction.

A. Local Features Extraction

Local Features describe the image patches (small group of pixels) from iris images. Local feature extraction methods are based on the analysis of texture features. While extracting local features, small patches of the images are considered, making local features extraction from the iris images more complex and time-consuming. In spite of this, local features extraction methods are used more frequently because of their excellent performances [14]. The local features commonly used for biometric iris detection are texture features, statistical features, LBP, and SIFT.

B. Global Features Extraction

Global Features describe the entire image of iris. Global feature extraction is fast and easy to extract, as it works on an entire image instead of small image patches. The global features are used for the detection and classification of the object [14]. Some of the commonly used global features for the biometric iris detection are BSIF, histogram, image quality measures, and wavelet transform.

(A) Local Features Extraction

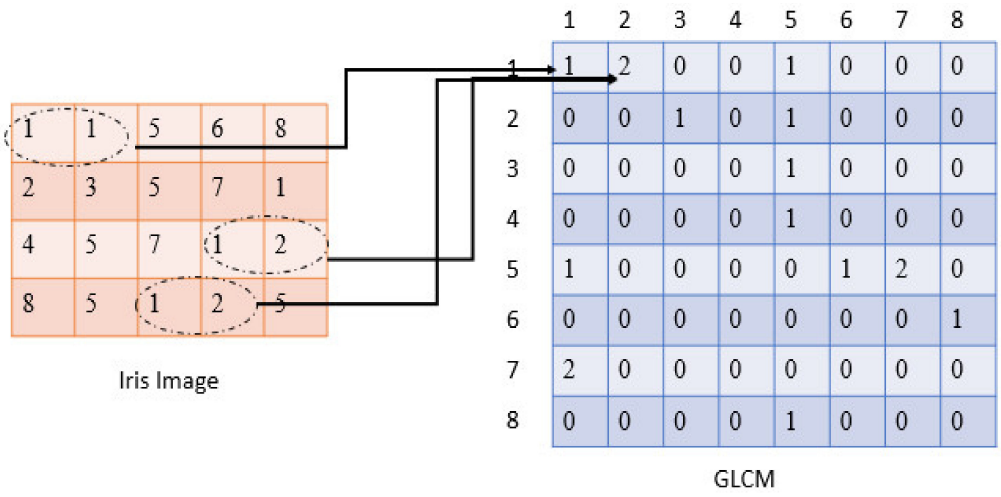
Commonly used local features extraction techniques for biometric iris identification are explained here.

(1) Texture Features

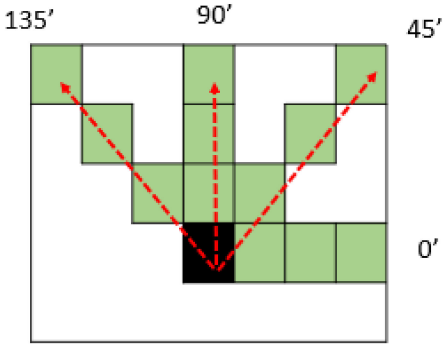
The texture is one of the important characteristics of identifying objects or regions of interest in an Iris image. The characteristics such as color, intensity, shapes, contrast, correlation, energy, reflectance are used as texture features. Texture features of a real iris image are different from a fake iris image [23]; Therefore, the texture features are used more frequently in literature. Gray level co-occurrence matrix (GLCM) is used to extract the texture features from iris images.

The co-occurrence matrix of an image is formed grounded on the correlations between iris image pixels. "For a k-bit image with $L = 2k$ brightness levels, an $L \times L$ matrix is formed of which elements are the number of occurrences of a pair of pixels with the brightness of a, b disconnected by d pixels in a certain direction. After calculating the matrix, the texture characteristics of the second statistic are calculated" [23].

For example, in Figure 7a, an image with eight "levels of intensity show which its co-occurrence matrix has eight rows and eight columns". "Typically, the co-occurrence matrix is defined for the four main directions (0, 45, 90, and 135)". In Figure 7b, a dislocation of three between "two pixels represents four different angles across two pixels with angles (0, 45, 90, and 135) degrees" [23].




(**a**) How to extract a co-occurrences matrix from an image.




(**b**) Four different directions to generate a co-occurrences matrix.

**Figure 7.** GLCM feature extraction technique for iris liveness detection.

The statistical properties can be determined from the output of the co-occurrence matrix after it has been formed. For "example, six statistical properties (*contrast*, *correlation*, *energy*, *homogeneity*, *entropy*, and *maximum probability*) can be deduced from the co-occurrence matrix" [23].

$$Contrast = \sum_{i,j} |i-j|^2 \, Pi, j \quad (1)$$

$$Correlation = \sum_{i,j} \frac{(\mathrm{i} - \mu_i)(j_- \mu_j) Pi, j}{\sigma i \sigma j} \quad (2)$$

$$Energy = \sum_{i,j} P\, i, j^{\,2} \quad (3)$$

$$Homogeneity = \sum_{i,j} \frac{P\, i, j}{1 + |i - j|} \quad (4)$$

$$Entropy = -\sum_{i,j} P\, i, j\, log2\, P\, i, j \quad (5)$$

$$Maximum\ Probability = Max(pi, j) \quad (6)$$

In the above equations, the

$pi,j$ is the normalized co-occurrence matrix $\mu_i$ quantity is an average that is calculated along rows of matrixes.

$\mu_j$ is the average that is calculated along with the columns.

$\sigma i$ and $\sigma j$ are standard deviations, which are calculated along rows and columns [24].

(2) Statistical Features

To extract statistical features from the iris image, mean and variances are used [25]. The statistical features are calculated using measures such as variance, mean, median, standard deviation, etc. The mean gives a clue about pixels that are white, black, 50% gray, etc. The variance gives a clue about how the pixel values are spread: example, if iris's image mean pixel value is 50% gray, most of the other pixels are also 50% gray which is then a small variance. The mean and variance are computed as the class mean and class variance from the training images for iris liveness detection. The closest class mean and variance are considered as the predicted class.

(3) LBP

Local binary pattern (LBP) is a simple feature extraction method that labels the pixels of an iris image by thresholding the neighborhood of each pixel and considers the result as a binary code. For every image point, a neighborhood is initially measured in this method, as shown in Figure 8a. "Then the strength of the central pixel is related with the intensity of the neighboring pixels. Suppose the intensity of the nearby pixel illumination is larger than the central pixel. In that case, the value for that neighbor, In the extracted binary pattern, is considered one. Otherwise, it is zero" [23], as shown in Figure 8b. Weights are assigned in the clockwise direction as shown in Figure 8c. Finally, we get a "binary-weighted sum of the values in the binary extraction" pattern, the value of which is called as the LBP code as shown in Figure 8d. This process is figured across the whole iris image. After calculating the LBP code for the entire iris image histogram for the entire image is computed. The mean LBP histogram is computed as the class histogram from the training images and ILD. Using distance measures, the closest class histogram is predicted, which is considered the predicted class [26].

(4) SIFT

SIFT descriptor is used to discover the local features such as orientations, and magnitude from iris images, generally known as the 'key points 'of the image. The key benefit of SIFT features is that it is mainly invariant to the variations of scale and rotation [27].

The entire process can be divided into four parts as given below:

Constructing a Scale Space: Firstly, the blurring technique is applied to the iris image to ensure that features are scale-independent. This eliminated the inconsequential details such as background, noise and saved the information such as the shape and edges. It is required to blur the iris images for multiple scales. The ideal number of scaling down the iris image is four (is known as octaves).

Secondly, to reduce noise, the difference of gaussians or DoG is applied to an image. DoG subtracts one blurred version of an Iris image from another less blurred version of the

iris image. After applying DoG, noise is removed from the iris image, and then the features get improved [27].

Key point Localization: To identify the suitable features or key points from the extracted features, local maxima and local minima are used. To trace the local maxima and minima, we have experienced every pixel in the iris image and compared it with its neighboring pixels. After applying that, we have crucial points that signify the images and are scale-invariant [27].

Orientation Assignment: In this stage, it was confirmed that the vital points are rotation invariant. To assign an orientation to each of these key points, it must calculate the magnitude and orientation. Histograms are created by using magnitude and orientation. The magnitude signifies the intensity of the pixel, and the orientation gives the direction for the same.

Key point Descriptor: It has stable key points that are scale-invariant and rotation invariant to date. In this stage, the neighboring pixels, their orientations, and magnitude are used to create an exclusive key point called a 'descriptor.' The surrounding pixels are used to make the descriptors partially invariant to the illumination of the iris images [27].

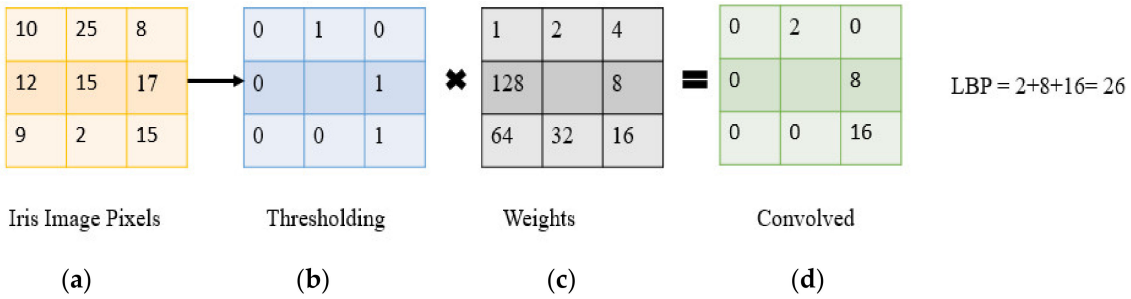



**Figure 8.** Feature extraction by using LBP method for iris liveness detection. (**a**) Iris Image Pixels; (**b**) Thresholding Iris Image; (**c**) Calculating Weights; (**d**) Convolution and calculating LBP code.

(B) Global Features Extraction:

Commonly used global features extraction techniques for biometric iris identification are, explain here:

(1) BSIF

Binarized statistical image features are used for feature extraction from the iris image. In BSIF, the filters are constructed using the natural iris images instead of synthetic filters [28]. "A set of filters of patch size p × p is learned using original iris images. Patch size p is defined as: p = (2 xn + 1) such that n ranges from {1, 2 . . . 8} [29]. The set of filters from original iris images is used to extract the texture features from images. If an iris image is represented using $I$(x, y) and the filter is signified by $Hi$(x, y) where $i$ signifies the basis of the filter, the linear response of the filter $Si$ can be given as:

$$Si = \sum_{i,j} I(u,v)Hi(u,v) \tag{7}$$

where x, y represents the dimension of iris image and "filter. The response is further binarized based on the obtained response value. If the linear filter response is greater than the threshold, a binarized value of one is assigned." This operation can be expressed as:

$$bi = \begin{cases} 1, \ if \ si > 0 \\ 0, \ otherwise \end{cases} \tag{8}$$

This process is computed across the whole Iris image. After computing the gray code for the entire iris image, histogram computed. For iris liveness detection, the mean histogram is computed as the class histogram from the training images. By using dis-

tance measures, the closest class. The histogram is predicted, which is considered as the predicted class [30].

(2) Histogram

"The histogram of an image is a statistical explanation of the distribution in terms of the rate of pixel intensities [31]. An image histogram is merely counting the number of pixels intensity levels that fall into various disjoint intervals, known as bins. Normally bin size is presumed to be 256 for any image, so the size of the histogram vector is also" 256. It is specified by the formula given below:

$$N = \sum ni \tag{9}$$

H = $[n_0, n_1, n_2, \ldots n_{255}]$

$N$—number of pixels of an image.

H—Histogram feature vector.

The resemblance "between two iris images can be measured by using the cross-correlation between the histograms of the particular iris images. Cross-correlation is a usual method of assessing the degree to which two vectors are correlated [31]. Given two histogram vectors $x(i)$ and $y(i)$ where $i = 0, 1, 2 \ldots, \beta - 1$ where β is the number of bins. The cross-correlation coefficient r" is defined as:

$$r(t) = \left| \frac{\sum[(x(i) - \mu x) \times (y(i-t) - \mu y)]}{\sqrt{\sum(x(i) - \mu x)^2 \sum(y(i-t) - \mu y)^2}} \right| \tag{10}$$

where "$\mu x$ and $\mu y$ are the means of the corresponding vectors [31]. The correlation coefficients lie between $0 \leq r \leq 1$ where 1 is demonstrating maximum correlation and 0 indicating no correlation. The maximum correlation coefficient in the correlation vector is taken as the measure of similarity and used in the histogram matching process". In the iris recognition application, two iris images are matched using the histogram matching process.

Figure 9 shows the iris image after extracting texture GLCM features, SIFT, LBP, and BSIF features from the real iris image.

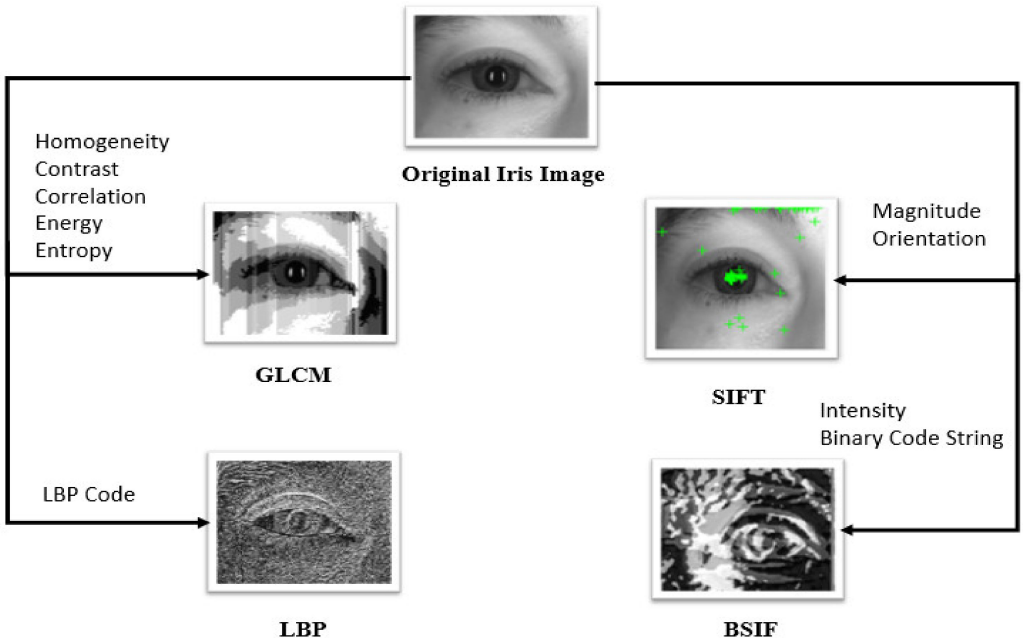



**Figure 9.** Results of feature extraction techniques on iris images for iris liveness detection (original iris image used from Clarkson 2015 dataset [32]).

(3) Image Quality Measures

Different measures are used to extract the features using image quality measures (IMQ) from iris images. A fake iris image has a different quality than the real iris image. Therefore, quality measures play a very important role while identifying spoof iris images. Figure 10 displays all 25 IMQ used for iris liveness detection. These features are categories into five different categories and subcategories.

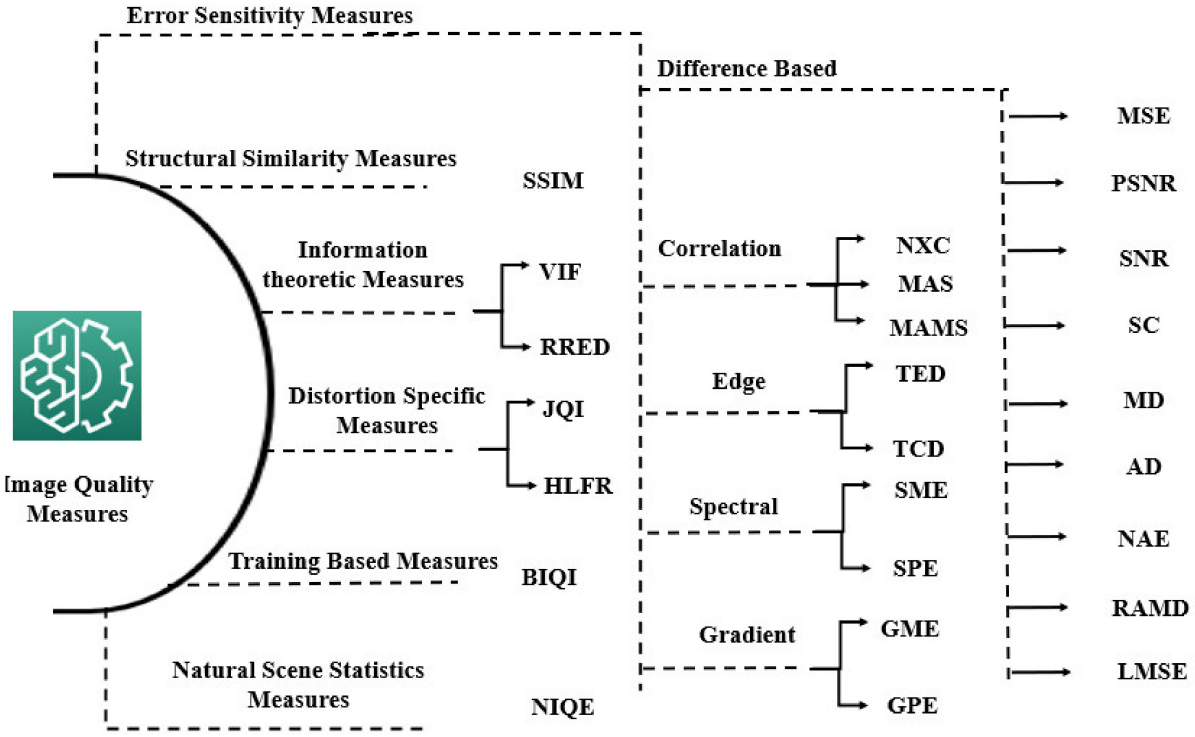



**Figure 10.** Image Quality Measures used in biometric liveness Detection.

Input Iris "Image I (of size N × M) is filtered with a low-pass Gaussian kernel" (size 3 × 3) to generate a smoothed version ˆI. Then, the quality between both the images (I and ˆI) is computed according to the corresponding IQA metric. A detailed explanation of the IQA metric is shown in Table 7.

(a) Error Sensitivity Measures: Traditional iris image quality assessment approaches are based on measuring the errors between the distorted and the real iris images. These features are simple to calculate and typically have very low computational complexity [33].

(b) Pixel Difference Measures: These features compute the misrepresentation between two Iris images based on their pixelwise differences. Here we take in: Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), Structural Content (SC), Maximum Difference (MD), Average Difference (AD), Normalized Absolute Error (NAE), R-Averaged Maximum Difference (RAMD) and Laplacian Mean Squared Error (LMSE)". Formal definition and formulas are conversed in [33].

(c) Correlation-based Measures: The resemblance between two digital images can also be quantified in terms of the correlation function. A type of correlation-based measures can be obtained by considering the statistics of the angles between the pixel vectors of the original and distorted images. These features comprise of Normalized Cross-Correlation (NXC), Mean Angle Similarity (MAS) and Mean Angle- Magnitude Similarity (MAMS)". Formal definition and formulas are conversed in [33].

(d) Edge-based Measures: Edges and corners, are some of the most enlightening parts of an image. Structural alteration of an iris image is firmly connected with its edge

degradation. Two edge-related quality measures are used as: Total Edge Difference (TED) and Total Corner Difference (TCD) [34].

(e) Spectral distance Measures: "The Fourier Transform is another traditional image processing tool that has been applied to the field of image quality assessment. For the extracting of IQ spectral-related features: the Spectral Magnitude Error (SME)and the Spectral Phase Error (SPE)" are used. Formal definitions and formulas are conversed in [33].

(f) Gradient-based Measures: Many of the distortions that can distress an image are replicated by a modification in its gradient. Consequently, using such information, structural and contrast changes can be effectually captured. Two simple gradient-based features are comprised in the biometric protection system: Gradient Magnitude Error (GME) and Gradient Phase Error (GPE), formal definition and formulas as conversed in [33].

(g) Structural Similarity Measures: Human visual system is vastly improved to extract the structural information from the viewing field. Hence, distortions in an image which are caused due to disparities in lighting, "such as contrast or brightness changes (nonstructural distortions), should be treated" in a different way from the structural distortions.

(h) Information-Theoretic Measures: The central idea related to these approaches is that: an image source connects to a receiver through a channel that confines the amount of information that could flow through it, by this means presenting distortions. "The goal is to relate the visual quality of the test image to the total of information shared between the test and the reference signals." To extract information-theoretic features: the Visual Information Fidelity (VIF) and the Reduced Reference Entropic Difference index (RRED) are used, which is discoursed in [33].

(i) Distortion-Specific Approaches: These techniques count on the knowledge formerly acquired, "about the form of visual quality loss triggered by a precise distortion. The ultimate quality measure is computed, as per the model trained on clean images and on images affected by this certain distortion. Two of these measures" are JPEG Quality index and high-low frequency index" as conversed in [33].

(j) Training-based Approaches: In this technique, "a model is trained using clean and distorted images. At that time, the quality score is computed based on a number of extracted features from the test image and linked to the general model. However, unlike the former approaches, these metrics aim to offer a general quality score" which is not associated with an explicit distortion. Thus, the Blind Image Quality Index (BIQI) follows a two-stage framework, in which the specific measures of different distortion-specific experts are joint to create one global quality score.

(k) Natural Scene Statistic Approaches: This approach is surveyed by the Natural Image Quality Evaluator (NIQE). The NIQE is completely a blind image quality analyzer based on the construction of a quality aware collection of statistical features (derived from "a corpus of natural undistorted images). It is related to a multivariate Gaussian natural scene statistical model."

(C) Drawback of Handcrafted Methods:

The above methods show that the manually engineered features are suitable for solving the PAD problem for iris recognition systems. However, their shortcoming is stated below:

- The range of handcrafted feature extractors profoundly depend on the expertise of the researchers on the problem".
- Handcrafted features frequently replicate restricted aspects of the problem with frequent sensitivity to fluctuating "acquisition conditions, such as camera devices, lighting conditions, and Presentation Attack Instruments (PAIs)".
- The Detection accuracy differs suggestively among different databases, signifying that the handcrafted features have the poor generalizing ability. Therefore, they fail to have the complete solution for the PAD problem.

- The obtainable cross-database tests in the literature propose that the performance of hand-engineered texture-based techniques can worsen intensely, when it functions in unfamiliar circumstances [35].

These glitches of the conventional approach are overcome by using self-learned feature extraction/deep learning-based liveness detection techniques.

**Table 7.** Image Quality Measures.

| Type | Sub-Type | Name |
|---|---|---|
| Error Sensitivity Measures | Difference Based | Mean Squared Error |
| | | Peak signal to Noise ratio |
| | | Signal to Nosie ratio |
| | | Structural Content |
| | | Maximum Difference |
| | | Average Difference |
| | | Normalized Absolute Error |
| | | R- Averaged MD |
| | | Laplacian MSE |
| | Correlation Based | Normalized Cross correlation |
| | | Mean Angle Similarity |
| | | Mean Angle Magnitude Similarity |
| | Edge Based | Total Edge Difference |
| | | Total Corner Difference |
| | Spectral Based | Spectral Magnitude Error |
| | | Spectral Phase Error |
| | Gradient Based | Gradient Magnitude Error |
| | | Gradient Phase Error |
| Structural Similarity Measures | | Structural Similarity Index |
| Information theoretic Measures | | Visual Information Fidelity |
| | | Reduced Ref. Entropic Difference |
| Distortion Specific Measures | | JPEG Quality Index |
| | | High-Low Frequency Index |
| Training Based Measures | | Blind Image Quality Index |
| Natural Scene Statistics Measures | | Naturalness Image Quality Estimator |

#### 4.1.2. Self-Learned Feature Extraction

In Self-Learned Feature Extraction techniques, features are automatically extracted from iris images to resolve the PAD problem for iris recognition systems. The different deep learning Models are used for the automatic extraction of these features. These models are characterized into two types, first the regular model or deep learning model, which is "trained from scratch using the training data, and second pre-trained models that are the models trained on data or features extracted from the same domain".

A. Deep Learning Model

(1) Convolutional Neural Network (CNN):

(a) The main building component of CNN, the convolution layer [33], conducts the majority of the intensive computing tasks. This layer's parameters consist of filter banks (kernels) that extract more complex features. Thus, the input image is convoluted using filter banks in this layer (kernels). The dot product of the filter entries and the input image is then computed. This creates the feature maps for the equivalent filter kernels. Accordingly, the network learns filters that

trigger when it notices some precise type of feature at the same spatial position in the input.

(b) The maxpooling layer is used to reduce the size of the representation and the hyper-parameters in the network, which reduces computing overheads. This layer functions with filters of size 2 × 2. This layer also regulates the over-fitting problem.

(c) "A fully connected layer reflects all of the features to obtain information about the image's overall shape. The final layer calculates a probability score based on the number of classes for which the network has been trained."

B. Pre-Trained Model

Deep Learning Models demand a large dataset for training. The training from scratch with Deep Learning is a lengthy process that involves complex experimentations with different parameter values such as weights, number of filters, and layers, amongst others. This is the reason why most researchers use Pre-trained models like, Inception, VGGNet, AlexNet, DenseNet [36].

A preceding study by Nguyen et al. [37] demonstrated the success of using five different CNN pre-trained models for iris recognition. The five pre-trained models are VGGNet, Inception, AlexNet, ResNet, and DenseNet. DenseNet accomplished the highest accuracy, followed by ResNet, Inception, VGGNet, and AlexNet [38].

The transfer learning can be used to deal with the nonappearance of a large iris dataset. CNN's that have been trained on other large datasets such as ImageNet [39], can be assumed directly to the iris recognition domain. In detail, CNN models pre-trained on ImageNet, have been effectively shifted to many computers vision tasks [25]. Minaee et al. [26] presented that the VGG model, although pre-trained on ImageNet to classify objects from diverse sorts, works practically fine for the task of iris recognition [37].

(1) Very Deep Convolution Network (VGG):

The model's input is a fixed-size image (224 × 224) throughout training. The images are passed through a stack of Convolutional (Conv) layers, where small receptive filters of size 3 × 3 are used. To preserve the spatial resolution after convolution, the padding of 1 pixel for 3 × 3 Convolutional layers is employed. In addition, stride 2 is used to accomplish max-pooling over a 2 × 2 -pixel window. A stack of convolutional layers preceded by three fully connected (FC) layers has been applied with varying depths in various designs. There are 4096 channels in the first two FC layers and 1000 channels in the third FC layer. The third fully connected layer executes the "ImageNet Large Scale Visual Recognition Challenge (ILSVRC) classification." The Soft-Max layer is the model's final layer. The FC layers are the same in all of this model's topologies. VGG comes in various forms, the two most popular of which are VGG-16 and VGG-19, which have 16 and 19 layers, respectively.

(2) Inception-v3 (GoogLeNet):

This model is made known by Szeged et al. [40,41]. The main origination introduces an inception module, which plays an important role as a subnetwork within a larger network [41]. The new insight used a 1 × 1 convolutional block to combine and decrease features before invoking the expensive parallel blocks. This aids in the better combination of Convolutional features, which is not possible by adding more Convolutional layers. To produce Inception v2 and v3, the authors offered several enhancements in batch normalization and revised the filter configuration in the inception module [42]. Most newly, in Inception v4, they improved the gradient flows by adding residual connections [37,43].

(3) Deep Residual Network Architectures (ResNet):

This model is proposed by He et al. [44]. ResNet model is based on the VGG nets. In this model, the convolutional layers have 3 × 3 filters. ResNet feeds the output of two consecutive convolutional layers and ignores the subsequent layer's input [45]. This lasting connection progresses the inclined flow in the network, agreeing that the network becomes

very deep with 152 layers. With SoftMax, the model culminates "with an average pooling layer and a 1000-way fully linked layer. In this case, there are 50 weighted layers. This model has fewer filters and is simpler than VGG nets".

### *4.2. Iris Spoofing Attacks (RQ2)*

The mechanism Iris spoofing enables the impersonation of the individual identity [46]. "Biometric systems" are inclined to "spoofing attacks" that lessen their safety [14]. The purpose of the numerous types of researches is to emphasize the analysis of the weak spots in biometric systems, to notice any unlawful admittance. The lives of the common people have been affected owing to the usage of biometrics spoofing. The iris scanner of the smartphone "Samsung S8 was spoofed in 2017 with a photo" [47]. The USA police used the fingerprints of the deceased accused to open their iPhones in 2018 [48].

Spoofing attacks are comparatively simple as the least technical information is required about the method of the working system or the use of an algorithm. Spoofing attacks can be carried out in a variety of ways. For example, Figure 11 shows different types of Irises spoofing attacks used in iris liveness detection.

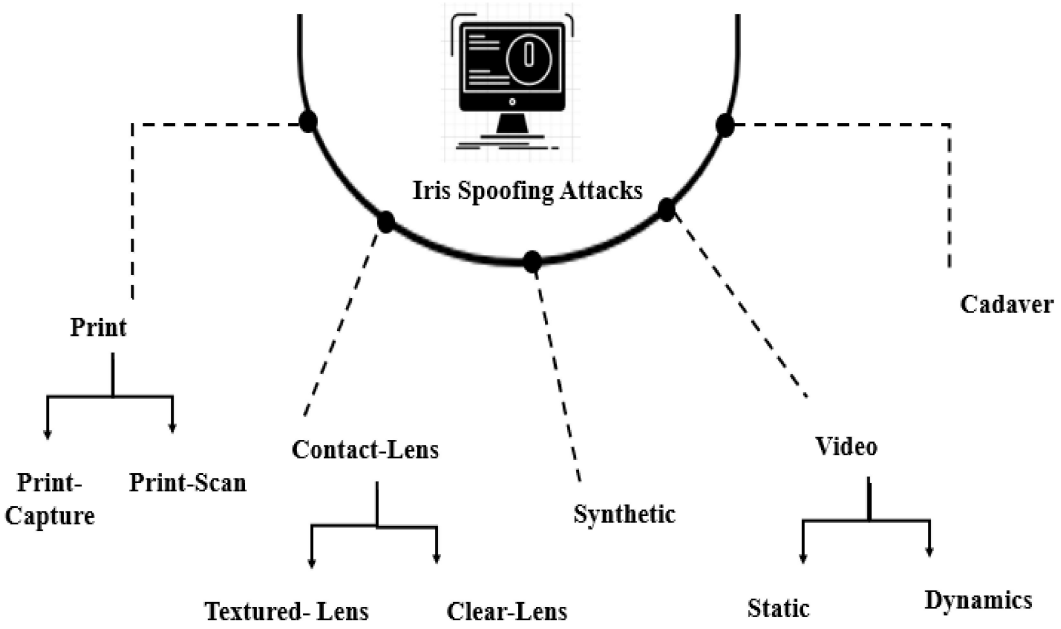



**Figure 11.** Different types of iris spoofing attacks used in iris liveness detection.

#### 4.2.1. Print Attacks

This attack is the simplest to instigate. It comprises an image presentation of an iris to the sensor. Presenting a printed image of an iris to the scanner/system can aid in copying the identity of an individual. An iris recognition system can be considerably misled with a suitable printer and paper combination and the quality of printed iris [21]. Print attacks can be performed in two ways (print and scan) and (print and capture). In (print and scan) attacks, the pattern of Iris is printed with the help of a high-quality printer and then scanned. In (print and capture) attacks photo is captured by the scanner. "The study by Gupta et al. [46] had shown that both (print and scan) and (print and capture) attacks could reduce the iris detection accuracy to less than 10% at 0.01% FAR. Raghavendra and Busch [49] proposed a multi-scale binarized statistical image feature (m-BSIF) on iris images along with linear support vector machines to detect images print attacks."

Many studies focus on the print attacks in literature [10,13,21,22,44,50–52]. While identifying the print attacks, authors used different feature extraction techniques in the literature. The most frequently used are Handcrafted Feature Extraction techniques.

"Raghavendra and Busch [49] proposed a Multi-Scale Binarized Statistical Image Feature (m-BSIF) on iris images with the Linear Support Vector Machines to" notice the images of the Print attack. The most frequently used handcrafted feature extraction techniques to identify the Print attacks are LBP [21,22,50], Texture analysis [44], and Image quality measures [33,53].

The SVM classifier gives the best Spoof Detection accuracy for the classification of Live and Print attack images. After SVM [10], Random Forest and Decision Tree classifiers give good classification accuracy. In [22], Fathy proves that Wavelet Packets (WPs) and LBP with SVM as the classifiers give 99.92% Print image detection accuracy.

Recently in literature, CNN and different versions of CNN were also used to identify the Print at-tacks. Many authors used CNN [13,43,52,54–57], for Print attacks identification. The author [52] shows that a Convolutional Neural Network (CNN) gives the best classification accuracy of the Print attacks. Figure 12 shows the sample images of the different types of spoofing attacks.

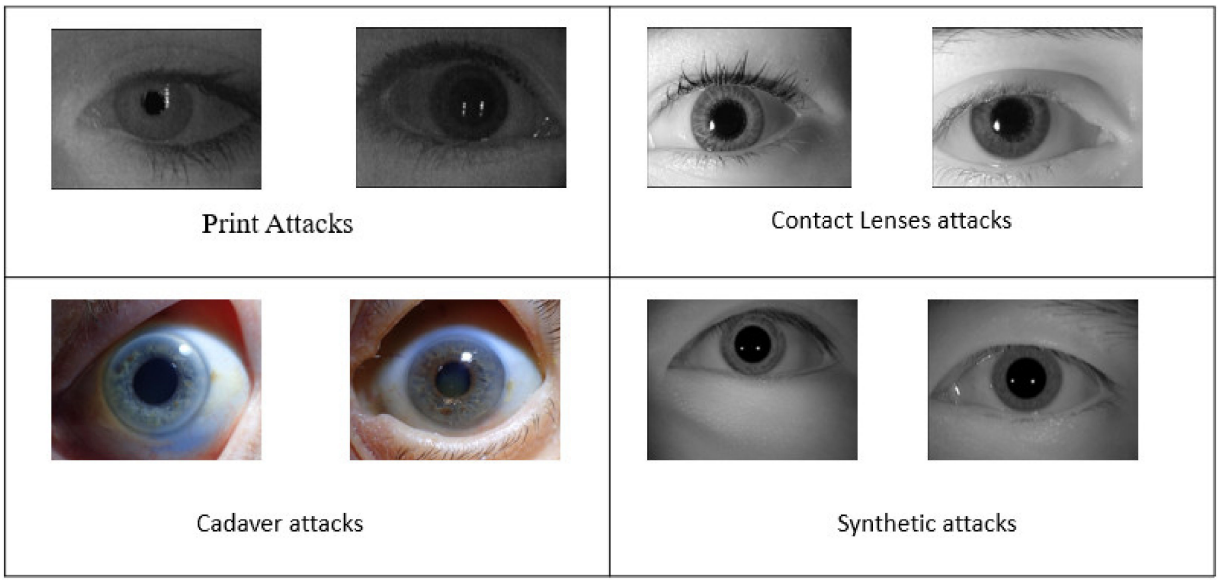



**Figure 12.** Different types of iris spoofing attacks. (Print Attacks [32] Contact Lenses Attacks [32], Cadaver Attacks [58], Synthetic Attacks [59]).

#### 4.2.2. Contact Lenses Attacks

Contact lenses are acquiring fame worldwide with the developments in technology and attributable to the affordable low costs. They are not only used for eyesight correction but also increasingly used for cosmetic purposes. The original texture of the iris is enclosed by these textured lenses, which can severely worsen the performance of iris recognition systems [21].

The contact lenses have three categories, Texture contact lens, Color contact lens, and Clear contact lens. In literature, the term Textured Contact Lenses normally refers to the contact lenses. These contact lenses are made with a visual texture in mind. Though no visual texture was printed on the colored contact lens, it was tinted with a certain color. "Clear contact lenses are neither colored nor have a visible texture".

Cosmetic contact lenses are also occasionally used in literature for textured contact lenses and colored contact lenses. An invader can use "textured contact lenses to copy a targeted enrollment." The contact lens pattern partially overlaps the normal iris texture, which is an elementary problem. Henceforth the texture of an iris wearing textured contact lenses combines contact lens texture and natural iris texture.

Several studies [10,21,24,44,50,51,60] have confirmed the necessity for sensing contact lenses. The transparent (Clear) and textured (cosmetic) lenses have been revealed to affect the iris recognition systems. To identify the contact lens attacks, different feature extraction

techniques are used in the literature. Texture analysis [44], LBP [50], and Histogram [51] are more frequently used handcrafted feature extraction techniques to identify contact lenses.

For the classification of live and contact lens, the SVM classifier's best Spoof detection accuracy is followed by the Random Forest and Decision Tree classifiers.

Recently Deep Learning algorithms [11,13,52,57,61–63] are also used for Iris spoofing attack detection. The author [64] proves that using BNCNN with self-learn features gives a 100% correct recognition rate.

#### 4.2.3. Synthetic Iris Attacks

The synthetic iris images are an additional probable attack that can replicate a live/real iris pattern. "Synthetic samples pose a problem" to biometric systems, as the individuals may have to struggle to discriminate amid "a good synthetic sample and a genuine iris" [65].

To generate the synthesized iris images, the iris textures of images are synthesized automatically from the unique Iris Images. Then the iris ring regions are fixed into the actual iris images, making the artificial iris images more realistic. The author [66] proves that synthetic iris images from the CASIA-Iris-Synthetic [67] dataset are useful in training Iris Biometric systems, making the system more robust to unseen attacks. Galbally et al. planned a genetic algorithm-based synthetic iris creation technique. This technique iris-pattern is created, which looks such as a live iris image and matches a genuine user [21]. These created images still pose the problem of the presentation of these samples to a biometric sensor. Even though "synthetic irises" can betray "software solutions," it is tough to depict this attack type to a biometric sensor. To present synthetic irises to biometric sensors, we need to take the printouts of an image or used a replay attack [65].

Many studies from the literature identified synthetic irises spoofing attacks [22,54,64,68]. Most studies refer CASIA-Iris-Synthetic dataset to detect Iris spoofing attacks, as datasets have more realistic iris Images. The iris ring regions were fixed into the actual iris images. This makes the fake iris images more accurate, comprising 10,000 synthesized iris images of 1000 classes.

The author [22] used Wavelet Packets (WPs), Local Binary Pattern (LBP) to detect the synthetic iris attacks in Iris biometric system. The author used SVM for classification, which gives an average classification accuracy of 99.92%. Author [21] used multi-order dense Zernike moments with LBP for synthetic Iris attack identification.

CNN is also used to identify the synthesis images more accurately. The author [64] proved that BNCNN could detect synthesis iris with CCR = 100%. By using Google Net, it proves that synthetic iris can be identified with 100% accuracy [54].

#### 4.2.4. Video Attacks

In this attack at the front of a biometric system, the imposter shows the authorized identity's Eye video. Video attacks are also referred to as replay attacks. The purpose of Video attacks is to interrupt the biometric system, which engages iris "video-based authentication." [41]. This sort of system is made to sense the aliveness of the person by scrutinizing the motion information. "However, video attacks" leap forward the biometric authentication system. As the video consists of enough motion information, it is easy to break through a biometric "authentication system" [14].

The static, along with the dynamic patterns of the eye, can be copied using the Video attacks. The photos of the iris are the one information required to emulate the static pattern of the eye.

However, compared to all other attacks, video attacks are less identified in the literature of iris biometric authentication. Figure 13 shows that only one paper from the selected studies identified the video attacks because of the unavailability of the standard large-scale iris video datasets.

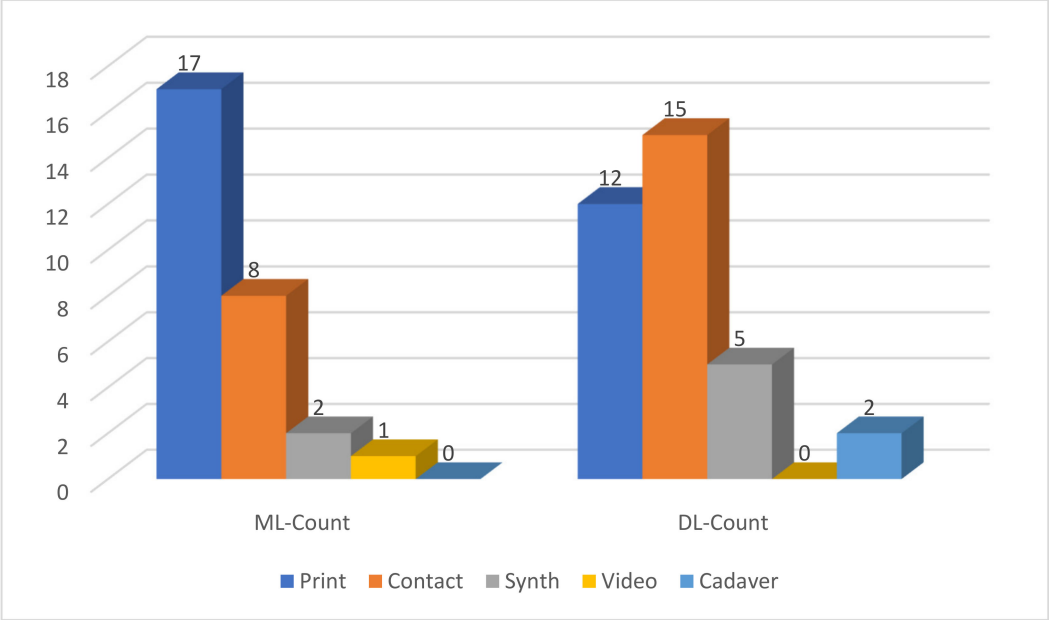



**Figure 13.** Number of spoofing attacks identified in Machine Learning and Deep Learning approaches.

So, Raja et al. constructed a new iris video dataset in the visible spectrum using two smartphones and trained a model for ILD [41]. The author formed the PAVID video dataset by taking 152 exclusive eye instances from 76 subjects. A video of an extent of 1–3 s is attained for each subject.

For Feature extraction, the author used an image decomposition into "Laplacian pyramids" and obtained the "frequency responses in different orientations." SVM classifiers give the best ACER of 0.64% for video replay attacks on iris recognition systems. Till now, in literature, no one has identified video spoofing attacks by using deep learning algorithms.

Figure 13 shows number of spoofing attacks identified in selected literature.

#### 4.2.5. Cadavers Eyes Attacks

The clue of using inanimate parts in presenting attacks has perhaps developed from the cinemas. We are unaware of any effective "attack a commercial iris detection system based on cadaver eyes." [58]. It is probable to obtain a "post-mortem iris image" up to 1 month after death, using commercial iris sensors in cold temperatures (around 6 °C/42.8 °F). This may result in an accurate match between this sample and its antemortem counterpart [58].

Theoretically, the dead person's post-mortem iris could be used as a fake. "However, it is realistic that somebody may use an image of a post-mortem sample to conceal their identity. Post-mortem iris samples thoroughly bear a resemblance to living irises in the formative stages after death. Thus, the detection of these samples in the wild may prove to be difficult" [65].

Trokielewicz was the one who carried out the initial tests using post-mortem iris scans [58]. The author was the foremost "to present the biometric recognition accurateness of the post-mortem iris recognition up to 34 days after death. He published the sole dataset of the post-mortem iris images available" up to the present time.

In literature, deep learning techniques are used for the identification of cadaver attacks. [58] the author used VGG-16 to detect cadaver iris with 99% accuracy. No one attempted to identify the cadaver iris spoofing attacks with the handcrafted feature extraction techniques.

From Figure 13, it observed that, "in the literature, the researchers have been attentive towards one specific type of iris spoofing attack and have offered algorithms to address it" [24,56,60,69]. However, iris recognition systems ought to handle and spot all types of spoofing attacks in practical situations [69] So, there is an urgent need to develop a framework that detects all the types of popular spoofing attacks.

### *4.3. Iris Datasets (RQ3)*

This section comprises the analysis of some of the extensively practiced publicly available datasets for ILD (ILD). The crucial problems and challenges with the prevailing datasets (RQ3) were reviewed. Data plays a very important role while building a model. This gives better accuracy to the model. The model performance and accuracy improve if the data with good quality and relevance is obtained.

The majority of the researchers endeavored the collection of data and the use of the existing standard datasets for ILD. Datasets are classified into two types: Standard benchmark datasets and custom/real-time datasets. The datasets used in PAD (presentation attack detection competition), with wide availability, are known as standard benchmark datasets. The datasets collected by the respective authors for their study and model training are called custom/real-time datasets. This study exclusively stresses standard benchmark datasets as the appropriate information related to custom real-time datasets is inaccessible [70].

#### 4.3.1. Standard Benchmark Datasets

It was detected that the diverse datasets had been exercised by the researchers for preparing the model for ILD. To get effective research findings, you need to find the correct dataset with enough amount and quality data for testing and training the system.

Datasets that were not available publicly have been used in early ILD research. Every team of researchers acquired the datasets individually for a particular study or paper. For example, as in the UAE dataset, John Daugman's findings were the first to be accurately reported.

The Chinese Academy of Sciences (CASIA) v.1 [71,72] was the first publicly available dataset. Since 2003, the updated versions of the CASIA dataset are available. The updated versions of the CASIA dataset have made it the most widely used standard in the analysis process of iris recognition methods [70].

These standard datasets are classified into different categories based on the image acquisition process. The image acquisition process is used during building a dataset. The categorization into controlled environment and uncontrolled environment datasets are based on the control factors in the environment. The control factors in the environment are used to capture iris images. The dataset is categorized into single-sensors (cross-sensors) and mobile/smartphone captured images based on the diversity of sensors. The diversity of sensors is used to capture iris images. The majority of datasets focus on the detection and classification of the varied iris spoofing attacks. Figure 14 shows the Classification of iris datasets.

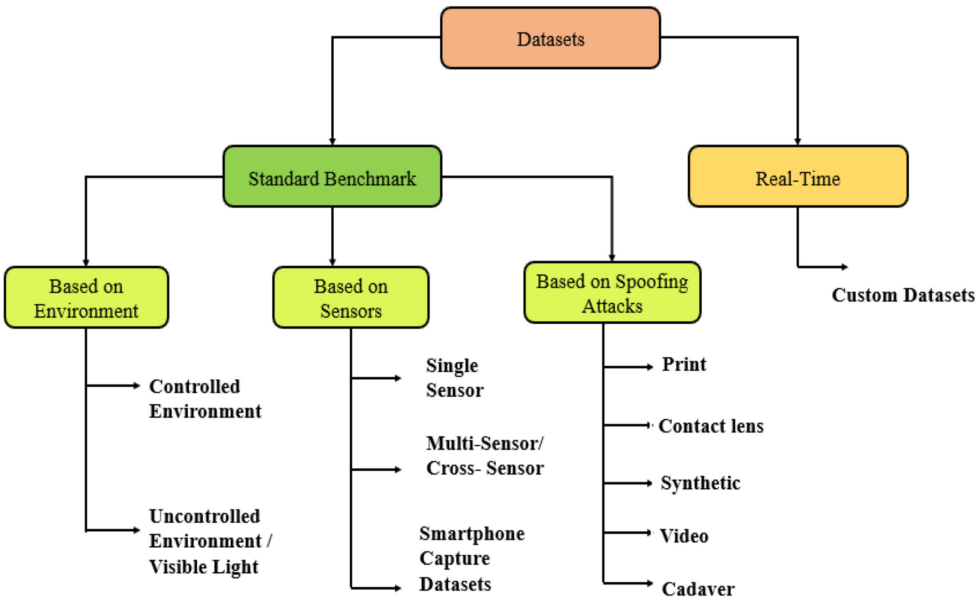



**Figure 14.** Taxonomy of datasets used for iris.

A. Controlled Environment Datasets

Controlled environment datasets are those datasets in which the images are captured taking the following factors into consideration:

1. The Conditions during the image captures include:
   - The spectrum at which the iris is captured (Near InfraRed (NIR) or visible spectrum)
   - The size of the iris in the image
   - The influence of eye glasses and conjunct specular reflections
2. Factors with environmental conditions like:
   - Light
   - Illumination
   - Sound (in case of iris video datasets)

The early researchers captured the publicly available datasets in a precise environment. The purpose of these datasets was to execute vital research on iris recognition and detection and to include the real variability of irises captures. The early researchers were engrossed in the progress of the vital facets of the recognition methods.

The first publicly available controlled environment dataset was the "CASIA iris Dataset v.1 collected by the National Laboratory of Pattern Recognition, Institute of Automation, CASIA". While capturing the dataset, the environment was controlled by Eight 850 nm NIR illuminators, which were spherically organized around the sensor. This was undertaken to confirm the effective and consistent illumination of the iris. Iris images are typically captured using Near-InfraRed (NIR) illumination. It has a wavelength ranging between 700 nm and 900 nm. The images are attained using such wavelengths. The images are inclined to focus on the complex texture of the iris instead of its pigmentation. This aids inaptly capturing the texture of dark-colored irises. It thus contributes to better recognition performance. This aids inaptly capturing the texture of dark-colored irises. It thus contributes to better recognition performance.

Table 8 displays all iris datasets listing, rows Nos. 1 to 30 represent the controlled environment datasets [70].

**Table 8.** All the available iris datasets.

| Sr. No | Paper ID | Dataset Name | Environment Used | Sensors Used | Capturing Sensor | Types of Images | No of Iris Images | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Live | Fake | Total |
| 1 | [73] | ND Iris3D | CON | MS | LG4000, Iris-Guard AD 100 | CL | 3458 | 3392 | 6850 |
| 2 | [74] | Warsaw-BioBase-Postmortem-Iris-v2 | CON | MS | IriShield MK2120U, Olympus TG-3 | PM | 1200 | 1200 | 2400 |
| 3 | [74] | Warsaw-BioBase-Postmortem-Iris-v3 | CON | MS | IriShield MK2120U, Olympus TG-3 | PM | 0 | 785 | 785 |
| 4 | [75] | Warsaw-BioBase-Pupil-Dynamics v3.0 | CON | MS | SD | PD | 117,117 | 0 | 117,117 |
| 5 | [76] | LivDet-Iris Clarkson 2017 | CON | MS | L2, DA, IP | PP, CL | 3954 | 4141 | 8095 |
| 6 | [77] | IIITD-WVU4 | CON | MS | C, V, IS, HP, KM | PP, CL | 2952 | 4507 | 7459 |
| 7 | [78] | IIITD Contact Lens Iris | CON | MS | C, V | PP, CL | NR | NR | 6570 |

**Table 8.** *Cont.*

| Sr. No | Paper ID | Dataset Name | Environment Used | Sensors Used | Capturing Sensor | Types of Images | No of Iris Images | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Live | Fake | Total |
| 8 | [77] | IIITD Iris Spoofing | CON | MS | C, V, HP | PP, CL | 0 | 4848 | 4848 |
| 9 | [21] | IIITD Combined Spoofing | CON | MS | C, V, HP | PP, CL, SY | 9325 | 11,368 | 20,693 |
| 10 | [79] | ND CLD 2013 | CON | MS | A, L4 | CL | 3400 | 1700 | 5100 |
| 11 | [80] | ND CLD 2015 | CON | MS | A, L4 | CL | 4800 | 2500 | 7300 |
| 12 | [81] | EMBD v2 | CON | MS | TX, EL, PS | EM | 1808 | 0 | 1808 |
| 13 | [58] | ETPAD v1 | CON | MS | EL, BM | EM, PP | 400 | 800 | 1200 |
| 14 | [58] | ETPAD v2 | CON | MS | EL, BM | EM, PP | 800 | 800 | 1600 |
| 15 | [82] | CASIA-Iris-Syn V4 | CON | N/A | N/A | SY | 0 | 10,000 | 10,000 |
| 16 | [44] | MobBIOfake | CON | MB | AT | PP | 800 | 800 | 1600 |
| 17 | [71] | CASIA-IrisV4-Thousand | CON | MS | Irisking IKEMB-100 | NR | 20,000 | NR | 20,000 |
| 18 | [71] | CASIA-IrisV4-Lamp | CON | SS | OKI Irispass-H | NR | 16,212 | NR | 16,212 |
| 19 | [71] | CASIA-IrisV4-Interval | CON | SS | Irisking IKEMB-100 | NR | 2639 | NR | 2639 |
| 20 | [70] | IITD-V1 | CON | SS | NR | CL | 1120 | NR | 1120 |
| 21 | [83] | ND WACV 2019 | CON | SS | LG4000 | CL | 1404 | 2664 | 4068 |
| 22 | [84] | WVU Un-MIPA | CON | SS | IrisShield BK 2121U, CMITECH EMX-30, Irishield MK2120U | CL | 9319 | 9387 | 18,706 |
| 23 | [32] | LivDet-Iris Clarkson 2015 Dalsa | CON | SS | DA | PP, CL | 1078 | 3177 | 4255 |
| 24 | [85] | ATVS-Fir | CON | SS | L3 | PP | 800 | 800 | 1600 |
| 25 | [86] | LivDet-Iris Warsaw 2013 | CON | SS | A | PP | 852 | 815 | 1667 |
| 26 | [32] | LivDet-Iris Warsaw 2015 | CON | SS | A | PP | 2854 | 4705 | 7559 |
| 27 | [76] | LivDet-Iris Warsaw 2017 | CON | SS | A, PWUT-1 | PP | 5168 | 6845 | 12,013 |
| 28 | [36] | Pupil-Dynamics v1.013 | CON | SS | PWUT-2 | PD | 204 | 0 | 204 |
| 29 | [87] | ND CCL 2012 | CON | SS | L4 | CL | 2800 | 1400 | 4200 |
| 30 | [88] | CASIA-Iris-Fake | CON | SS | H | PP, CL, PE, SY | 6000 | 4120 | 10,120 |
| 31 | [89] | VISSIV | VIS | MS | NL, IP | RA | 248 | 248 | 496 |
| 32 | [90] | MICHE-I | VIS | MS | GS, IP, GT | PP | 800 | 800 | 1600 |
| 33 | [72] | CAVE | VIS | MS | | EV | 5880 | 0 | 5880 |

**Table 8.** *Cont.*

| Sr. No | Paper ID | Dataset Name | Environment Used | Sensors Used | Capturing Sensor | Types of Images | No of Iris Images | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Live | Fake | Total |
| 34 | [72] | ND-CrossSensor-Iris-2013 | VIS | MS | LG2200 EOU, LG iCam 4000 | NR | 146,550 | NR | 146,550 |
| 35 | [91] | IIITD-WVU Iris Spoofing | VIS | MS | Cogent dual iris sensor (CIS 202), VistaFA2E, Irishield MK2120U | CL | 2250 | 4000 | 6250 |
| 36 | [90] | MICHE DB | VIS | MB | NR | PP | 3732 | 0 | 3732 |
| 37 | [92] | CASIA Iris M1 (mobile) | VIS | MB | CL | MB | 11,000 | 0 | 11,000 |
| 38 | [92] | CASIA BTAS | VIS | MB | | MB | 4500 | 0 | 4500 |
| 39 | [93] | ND-CrossSensor-Iris-2012 | VIS | NR | LG2200 EOU, LG iCam 4000 | | 147,442 | NR | 147,442 |
| 40 | [93] | UPOL | VIS | NR | | | 384 | NR | 384 |
| 41 | [94] | Eye SBU | VIS | SS | NR | | 70 | NR | 70 |
| 42 | [72] | UBIRIS-V2 | VIS | SS | NR | | 11,102 | NR | 11,102 |
| 43 | [72] | UBIRIS-V1 | VIS | SS | NR | | 1877 | NR | 1877 |
| 44 | [59] | Post-Mortem-Iris v1.0 | VIS | SS | NR | PM | 0 | 480 | 480 |

In iris liveness detection, the images captured using a controlled environment are less frequently used [58] than those captured in visible light/uncontrolled environment. The images captured in the controlled environment do not include the variances of the real-world situations, one as the environmental conditions such as lighting, distances, and reflections. It was noticed that all these controlled datasets do not offer both fake and real iris images. The classifier model used for iris detection or identification is less robust when used with the controlled environment datasets.

B. Uncontrolled Environment/Visible Light Datasets

Different properties such as light, distances, angle, size are allowed to vary while capturing iris images in an uncontrolled environment. The recognition of iris in visible light poses additional hurdles such as a wide range of ambient circumstances, wide-angle optical systems, and passive illumination. Table 8 displays all iris datasets listing. in which row no 31 to 44 are collected by using Visible Light\Uncontrolled environmental conditions [58,65].

The most popular datasets in the uncontrolled environment are UBIRIS-V1 [72], UBIRIS-V2 [72], and UPOL [73]. These datasets together serve as a benchmark and are referred by the majority of authors [70]. The UPOL datasets contain the high-quality of the 64 people's iris images were taken via an uncontrolled "environment. The UBIRIS datasets contain the noisy images captured" in an uncontrolled/visible light "environment, in the case of UBIRIS-V2", iris images are captured at a distance and are on the move [70].

A discrepancy was observed amid the captured datasets in the visible light. In some circumstances, the researchers employed a monochrome sensor with a band-pass filter. It is capable of capturing the complete visible light spectrum. Others use common consumer cameras that catch "visible light in three spectral bands. (Distinctly for the colors red, green, and blue)" [70].

Many researchers preferred using visible-light imaging datasets compared to controlled environment datasets [70]. The images available in uncontrolled datasets pose many variabilities such as light, distance, angle, and size. Most studies on visible-light (VIS) iris recognition have observed a major descent in recognition performances compared to NIR/controlled environment iris recognition. This is due to the richness of the iris texture, which is not simply visible in VIS images, especially for dark-colored irises [70]. Further, specular reflections can mask the iris texture, which lessens the accuracy of the recognition. The images captured using visible light are more prone to noise than those captured using the controlled environment [74]. The up-to-date performance of VIS iris recognition is poor compared to its NIR cameras.

All the visible light datasets do not offer both fake as well as real iris images. This is another challenge noticed during the analysis.

### C. Smartphone/Mobile datasets

Nowadays the smartphones with cameras are easily available to everyone. The widespread use of smartphones has enabled many researchers to begin "work on iris recognition in the context of mobile devices." Some mobile phones/applications provide an authentication system using the human iris.

Fujitsu released the first smartphone in the world with an iris authentication technique on 25 May 2015. The voracious studies started during that period on iris recognition, using smartphone captured images. The smartphones have built-in, high-resolution cameras, resulting in creating and introducing the datasets, with the easiness of capturing images. Many datasets can be created using smartphone camera sensors. Table 8 shows all iris datasets listing, in which rows No 16 and 36 to 38 represent the smartphone/mobile datasets [70].

The most prominent mobile dataset is CASIA iris M1 (mobile), which is divided into three subsets: "S1, S2, and S3". The dataset is popular because it is collected with the help of a mobile phone having an integrated NIR iris-scanning sensor. In addition, active lighting was employed in the scanning equipment. The dataset "contains 11,000 images (the three datasets combined) from 630 subjects with the data in JPEG format and the capture distance varying from 20 to 30 cm".

Even though the images captured using smartphone cameras are with the visible light spectrum, their quality is compromised due to the inclusion of the noise. This is a familiar problem as smartphone cameras are not more advanced than NIR cameras [74].

The majority of the authors used commercial iris recognition sensors. The commercial sensors provided better resolutions/quality than the images captured by a smartphone. It was observed that datasets collected using smartphones/ mobiles are used only for smartphone-based iris liveness recognition applications.

### D. Multi/cross-sensor iris datasets

The global positioning of iris recognition systems involve the use of various sensors. Different manufacturers form the sensors needed for the recognition systems. Variances influence the heterogeneity in iris recognition rates in sensor quality and image capture procedures. Several cross-sensor iris datasets were introduced to analyze these influences and acquiring images such as LG, Nokia, Vista, CMTech, Cogent, InTech, Cannon, IrisGuard, Galaxy, and Dalsa. LG sensors are used most widely while capturing iris images. LG sensors can spot the users through the user is at the distance of 3 m. It actively searches the iris even at a distance of 3 m. In Table 8, Rows no 1–14 and 31–35 enlist all the cross-sensor datasets.

IIITD-WVU iris spoofing dataset is the popular cross-sensor iris dataset, "which is composed of 2250 real and 1000 textured contact lens iris images captured by (i) a Cogent dual iris sensor (CIS 202) and (ii) a VistaFA2E" sensor.

Cross-sensor iris datasets are good for iris Liveness detection, as they use multiple sensors to acquire iris Images. Moreover, images acquired by different sensors under different environmental conditions have different resolution and illumination distributions,

contributing to a better recognition performance [18]. In addition, it is found that the Images captured using multiple sensors are high in number compared to the datasets created using a single sensor. As a result, the high size of the dataset contributes to better performance.

Although cross sensors datasets have all these benefits, there are some restrictions with the prevailing datasets. The images are captured using a variety of sensors (from two to three different camera brands). Consequently, for a larger evaluation, a dataset with added sensors could be acquainted with. Furthermore, the datasets explanations do not disclose whether numerous "different physical devices of one brand were used" nor the number of devices (single/multiple). Observations while studying these datasets are, each dataset uses different sensors to capture the iris images. The quality of the image varies depending on the used sensors. High-quality images are generated from the high-resolution sensors. The sensors such as LG, Nikon generate RGB images. Dalsa, Cogent generate grayscale images; as a result, Images captured using cross sensors are hard to compare. Sensor type was not declared in some datasets. The position of the sensor, that is, the distance from the eyes, was not revealed in the datasets document. It is found that, very few datasets offered both authentic and fake samples.

To work with iris liveness detection, we need a dataset which offers both fake and real iris images, as well needed dataset captured using Visible lights and multiple sensors for capturing images. In the next section, we list down all the datasets, which frequently used iris liveness detection.

### E. Iris spoofing and liveness detection datasets

Iris spoofing is a mechanism by which one can imitate the identity of an individual. The advance of spoofing and anti-spoofing methods established the need for research and benchmark datasets. The different datasets capture diverse spoofed images. For example, the printout of the original iris is taken and presented as a spoofed image. In some datasets, images of the iris are captured after wearing the contact lens. A few datasets have taken the images of remains of (fake) iris, and few datasets have generated the images from the original iris images with synthesis.

In this section, we tried to list out datasets, which the authors use for iris liveness detection. The datasets containing spoofed as well as real iris images are ideal for iris liveness detection. Table 9 displays the most frequently used datasets for iris liveness detection, spoofed, live, and total images.

**Table 9.** Available datasets for iris liveness detection.

| Dataset Name | Types of Images | No of Iris Images | | |
|---|---|---|---|---|
| | | **Live** | **Fake** | **Total** |
| ND WACV 2019 [83] | CL | 1404 | 2664 | 4068 |
| ND Iris3D [73,76] | CL | 3458 | 3392 | 6850 |
| Warsaw-BioBase-Postmortem-Iris-v2 [74] | PM | 1200 | 1200 | 2400 |
| WVU Un-MIPA [8] | CL | 9319 | 9387 | 18,706 |
| LivDet-Iris Clarkson 2015 Dalsa [32] | PP, CL | 1078 | 3177 | 4255 |
| LivDet-Iris Clarkson 2017 [76] | PP, CL | 3954 | 4141 | 8095 |
| IIITD-WVU4 [77] | PP, CL | 2952 | 4507 | 7459 |
| IIITD Combined Spoofing [21] | PP, CL, SY | 9325 | 11,368 | 20,693 |
| ND CCL 2012 [87] | CL | 2800 | 1400 | 4200 |
| ND CLD 2013 [79] | CL | 3400 | 1700 | 5100 |
| ND CLD 2015 [80] | CL | 4800 | 2500 | 7300 |
| ATVS-Fir [85] | PP | 800 | 800 | 1600 |

In Table 8, Rows no 1–14 and 31–35 list all the accessible ILD datasets. There is a total of twelve datasets that offer images of print spoofing attacks. Eight datasets captured images of iris after wearing a contact lens. Five datasets offer videos of real eyes reiterated on a monitor and then given to a visible-light sensor, usually a smartphone camera. Two exclusive datasets were found, one offering the images of prosthetic eyes and the other images of post-mortem irises.

In Table 9, column type of images show different types of spoofed images available in dataset:

CL means the images of iris after wearing contact lenses
PP means iris images after taking print out on paper
PM means images of Cadaver iris
PD means pupil dynamics iris Images

It was observed that none of the datasets have images of all known types of spoofing attacks together. Most of the available datasets cover two to three types of spoofing attacks. Some datasets have images specifically for one type of attack. As there is no such dataset available, the researchers need to work on multiple datasets to implement the ILD System. Therefore, to make a robust ILD model against all the types of known attacks, there is a need for a dataset that covers all the known types of attacks in a single dataset.

#### 4.3.2. Common Properties/Observation/Findings of Popular Datasets

After reviewing all the available datasets for iris liveness detection, we identified some findings from the datasets.

- The first thing to notice is that none of the datasets include both actual and fake samples. For instance, some datasets such as "IIITD iris spoofing, Post-Mortem-Iris v1.0, CASIA-Iris-Syn V4, synthetic iris textured based, and synthetic iris model-based, offer only fake samples". "In contrast, datasets such as pupil-dynamics v1.0 and CAVE offer only authentic samples". These example datasets are still helpful, and when combined with other datasets, they can provide an additional source of samples.
- The second point to consider is that there is a diversity of spoofed images in datasets. This diversity arises due to:
    - Capturing techniques in case of print attacks.
    - Vendors specific techniques in case of contact lens attacks.

Print attacks can be performed in two ways: print- capture and print scan. Many different datasets provide "images of irises printed on paper and presented to the" Biometric detection system. For example, the following datasets include printouts: "LivDet-Iris Warsaw 2013, LivDet-Iris Warsaw 2015, LivDet-Iris Warsaw 2017, LivDet-Iris Clarkson 2015 LG, ETPAD v1. In preparation for all remaining datasets, the authors presented the original printouts to the sensors. Another important factor differentiating these benchmarks datasets is whether they included contact lenses provided by different vendors. All datasets, except for CASIA-Iris-Fake, include textured contact lenses from different manufacturers [58]."

- "The IIITD iris spoofing dataset is the only benchmark that provides multiple attacks mean; it includes photographs of paper printouts of people wearing textured contact lenses. However, the authors report inferior and real comparison scores when the authentic eyes are compared to these hybrid attacks. Furthermore, it is compared either to use the textured contact lenses or the images of paper printouts of living eyes. Hence, it seems that this hybrid way of preparing the artifacts does not improve the detection accuracy of the attack".

Figure 15 displays the number of fake and live iris images, available in respective datasets. The graph displays that IIITD Combined Spoofing datasets have the maximum 20,693 images.

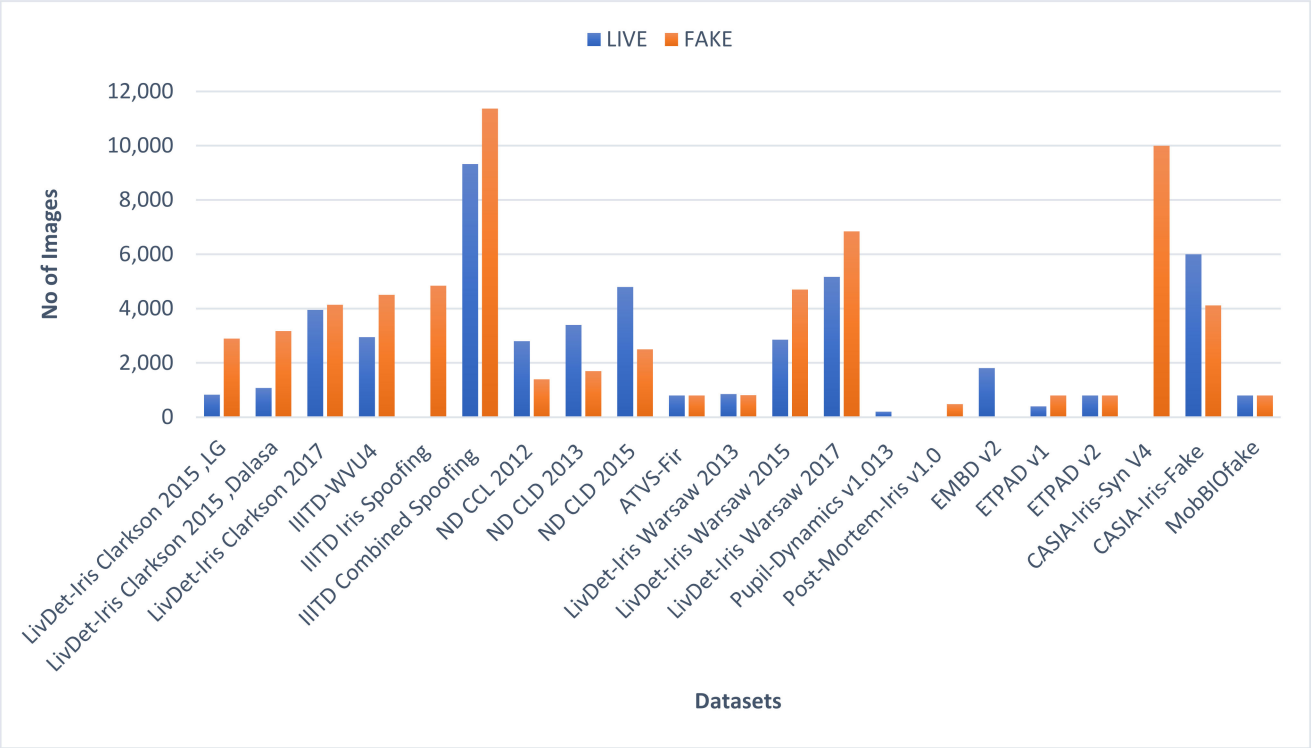



**Figure 15.** Iris datasets with the number of samples.

#### 4.3.3. Challenges/Issues with Existing Datasets

The literature from the context of the accessibility of the datasets was discovered as well as surveyed, and it is decided that the prevailing dataset has numerous open challenges/issues. Figure 16, displays these challenges/issues with the existing datasets.

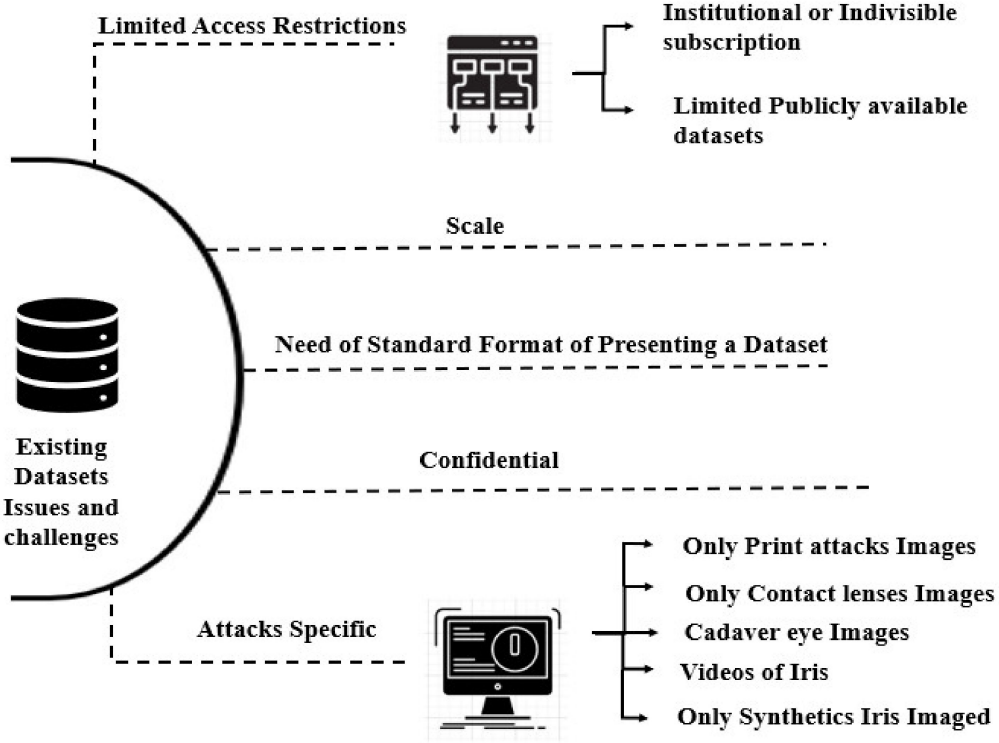



**Figure 16.** Challenges/issues with existing iris datasets.

A. Limited Access Restrictions

The prevailing datasets have to confront the challenge of the need for institutional or indivisible subscriptions for access.

For example, the datasets from Notre Dame University [92] are available only after acquiring an institutional subscription, whereas the CASIA iris dataset is available after acquiring an indivisible subscription. Such types of datasets are available free of cost only after having an institutional or indivisible subscription. A license is provided as the legal obligation for a document. Its purpose is to guard the subjects as typically.

B. Scale

"The records of subjects and images in a dataset" pose the challenge. The adequate "number of samples in a dataset is" the prerequisite in executing the statistically relevant research. The datasets with the additional samples can frequently aid as the objective benchmarks.

C. Need of Standard Format of Presenting a Dataset

The research papers present PAD benchmarks by practicing numerous formats of the data presentation and the standard results. It is chiefly an infrequent practice to offer some forged identities signified in artifacts. Dataset creators hardly discuss the qualitative analysis of the fake samples and the artifacts corresponding to the real presentation attacks.

D. Confidential

The majority of self-built datasets include confidential information about the biometric identity of the individual. Therefore, such sensitive dataset is publicly unavailable.

E. Attacks specific datasets

The prevailing publicly accessible datasets are susceptible to the attacks such as print attacks, contact lens attacks, video attacks, etc. There are no datasets available, with the inclusion of all probable and identified images of the attacks. For example, the IIITD Contact Lens Iris Dataset [65] includes iris images with clear (soft) and patterned contact lenses in four different shades. There are 6570 images in all, with 101 different subjects. Clarkson 2015 datasets contained only print attacks images.

### *4.4. Performances Measures (RQ4)*

"Biometric performance metrics assess the performance of a biometric system. There are different metrics" playing an important role in assessing the performance of the biometric system [95,96]. All the performance measures used in ILD were listed down. Figure 17 displays the outline of the performance Measures used for ILD.

Biometric performance evaluation is standardized which is performed mutually by ISO/IEC in the 1979 series of standards [96]. The standard documents are a great basis of information and aid to evade common drawbacks.

ILDis a classification problem. It is a fact that any classification model is based on the number of records appropriately and inappropriately predicted by the model. These counts are tabulated in a table called a confusion matrix which allows us to derive a lot of performance measures discussed as follows:

A. FAR (False Acceptance Rate)

"It is the probability of cases for which a biometric system" erroneously allows an unlawful person. "It is one of the normally used metrics in biometric recognition systems for evaluating the performance of the system". "For example: typically, biometric iris detection systems are used to consent to the constrained areas, only to the authorized. Suppose there are two people X and Y, Y has access to the system while X has no permission, then a false acceptance is obtained when X is known as Y (or any other a person with permission) and permits him to access reserved areas, even if they are not entitled to it".

"FAR = 0.1%, which means that in 1 out of 1000 cases, a biometric iris detection system has a probability of granting access to an unauthorized individual" [97].

In literature, many authors [54,68,98] used FAR for evaluating the performances of the iris detection system. However, FRR is "dependent on many factors including technical implementation, quality of biometrics sampled, environmental factors, etc.".

FAR is calculated by using the formula:

$$\text{FAR} = \frac{\text{FP}}{(\text{FP} + \text{TN})} \times 100\% \quad (11)$$

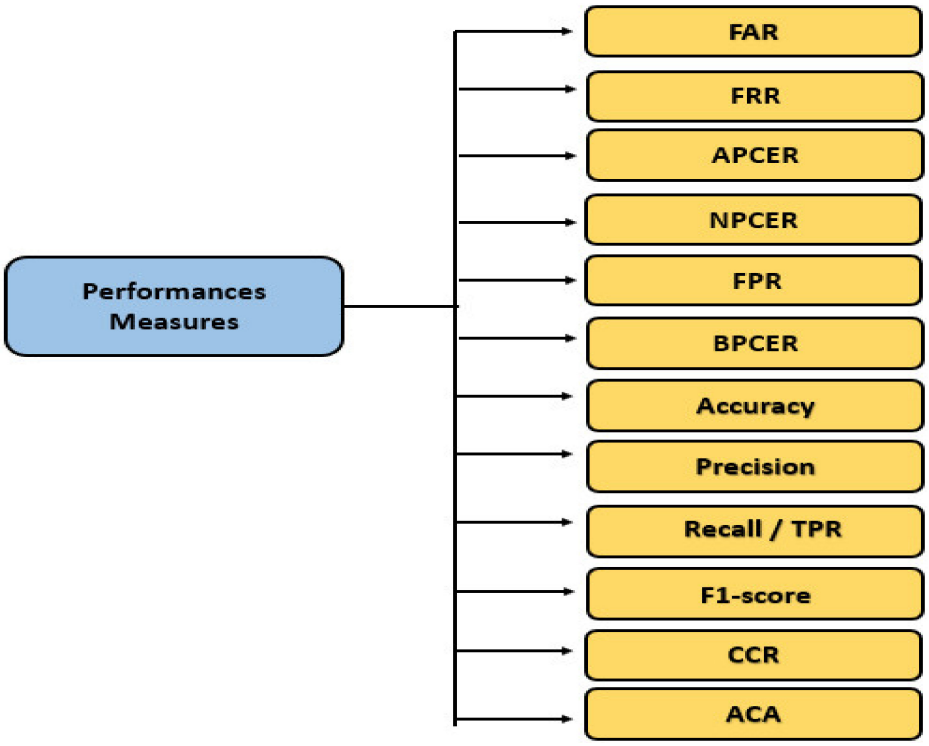



**Figure 17.** Performance measures used for iris liveness detection.

B. FRR (False Rejection Rate)

It is the probability of cases for which a biometric system erroneously rejects access to a lawful "person. The false rejection rate (FRR) is one of the vital metrics along with FAR and is generally used for evaluating the performance of a biometric system". "Like FAR, it is also expressed as a percentage of probability, in which a system erroneously refuses access to a lawful person".

"For example, if FRR = 0.01%, it means that in 1 out of 10,000 cases, a biometric system has a probability of denying access to an authorized individual" [97].

In literature, many authors [54,68,98] used FRR for evaluating the performances of the iris detection system. However, FRR is "dependent on many factors including technical implementation, quality of biometrics sampled, environmental factors, etc. Therefore, FRR meaningfully depends on user behavior and the quality of the presented Biometrics".

When the two systems are compared, the more precise "one shows lower FRR at the same level of FAR" [97].

FRR is calculated by using the formula:

$$\text{FRR} = \frac{\text{FN}}{(\text{TP} + \text{FN})} \times 100\% \quad (12)$$

C. APCER (Attack Presentation Classification Error Rate)

The part of attack images is erroneously classified as live samples; the proportion of attack presentations is wrongly classified as bona fide presentations. "APCER is the rate of misclassified spoof images (spoof called live)".

In literature, most of the authors [41,43,44,50,53,61,62,65,69] used APCER for evaluating the Performances of iris Detection system. APCER is calculated by using the formula:

$$\text{APCER} = \frac{\text{FP}}{(\text{TN}) + (\text{FP})} \tag{13}$$

D. NPCER (Normal Presentation Classification Error Rate)

"It is the rate of misclassified live images (live called spoof). It is the probability of cases for which an iris biometric system unreliably denies access to an authorized person" [62]. NPCER is calculated by using the formula:

$$\text{NPCER} = \frac{\text{FN}}{(\text{TP} + \text{FN})} \tag{14}$$

E. False Positive Rate

The number of attack images wrongly classified as live samples and "the proportion of attack presentations inaccurately classified as bona fide presentations". "FPR is the rate of misclassified spoof images (spoof called live)".

FPR and TPR are used to draw a ROC (Receiver Operating Characteristic Curve) curve. ROC graph shows the performance of an iris, the classification model at all classification thresholds. Authors [10,99–101] used TPR, FPR, and ROC for evaluating the performances of the iris detection system.

FPR is calculated by using the formula:

$$\text{FPR} = \frac{\text{FP}}{(\text{TN} + \text{FP})} \tag{15}$$

F. BPCER (Bona-Fide Presentation Classification Error Rate)

BPCER is the part of live images that were erroneously sorted as attacks and the rate of misclassified live images. The authors [62,63] used BPCER for evaluating the performances of the iris detection system. BPCER is calculated by using the formula:

$$\text{BPCER} = \frac{\text{FN}}{(\text{TP} + \text{FN})} \tag{16}$$

G. Accuracy:

Accuracy is the ratio between the number of correctly classified images and the total number of images. The Accuracy works correctly when the classes are balanced, which means the number of live samples and fake samples are equal [102]. Many authors [10,11,21,56,98,103–105] used the accuracy as the performance measure for evaluating performances of ILD model.

An Accuracy is the most commonly used matrix in literature for evaluating the performances of the iris detection system. It is a matrix that can detect, verify, and identify the iris liveness system. An accuracy is calculated by using the following formula:

$$\text{Accuracy} = \frac{(\text{TP} + \text{TN})}{(\text{TP} + \text{TN} + \text{FP} + \text{FN})} \tag{17}$$

H. Precision:

Precision offers a "number of predicted true positives iris images that were truly correct" [106]. When a dataset is imbalanced and the number of false positives is high,

precision is utilized [102]. The authors [22,105] used precision as the performance measure for evaluating the performances of the ILD model. Precision is calculated by using the formula:

$$\text{Precision} = \frac{\text{TP}}{(\text{TP} + \text{FP})} \tag{18}$$

I. Recall/True Positive Rate:

"Recall gives several real positive classes that were projected positive" [107]. When a dataset is imbalanced, and the number of false positives is high, recall is utilized [106]. In literature, recall is referred to as TPR or sensitivity. The authors [22,105] used recall as a performance measure for evaluating performances of the ILD model. The recall is calculated by using the following formula:

$$\text{Recall/Sensitivity/TPR} = \frac{\text{TP}}{(\text{TP} + \text{FN})} \tag{19}$$

J. F1-measure/F1-Score:

It associates "both precision and recall and presents their harmonic mean. F1-measure or F1-score is used when data is imbalanced, and the difference between precision and recall is important" [106]. The authors [22,105] used F1-measure as a performance measure for evaluating the performances of the ILD model. It can be stated as follows:

$$\text{F1} - \text{score } 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{20}$$

K. CCR (Correct Classification Rate):

"CCR is the summation of appropriately classified bona fide presentations and appropriately classified presentation attacks separated by the number of all presentations". In biometric detection, CCR is a more frequently used matrix. For example, the authors [54,55,59,64,68] used CCR as the performance measure for evaluating the performances of the ILD model.

L. ACA (Average Classification Accuracy):

ACA is the sum of true positive rate and true negative rate divided by two. The authors [21,22,24,60] used ACA as a performance measure for evaluating the performances of ILD model. It is stated as follows:

$$\text{ACA} = (\text{TP} + \text{TN})/2 \tag{21}$$

A biometric system's efficiency rates can be represented in a variety of ways, including decimal format (0.05), percent (1%), fractions (1/100), and powers of ten (10¬2). In literature, many authors used more than one performance measure to evaluate the performances of the iris Biometric system. While calculating performance accuracy, performance measure was used more frequently. Other measures such as FAR, FRR, TP rate, FP rate, etc., are used for plotting performance evaluation results by using the DET graph and ROC graph.

### *4.5. Summary of Survey*

This subsection summaries outcome of the survey. Figure 18 displays popular techniques used in ILD for feature extraction, classification, and deep learning models used in liveness detection. Table 10 attempts to list some papers from our literature studies with feature extraction, datasets used, and attacked identified using performance measures.

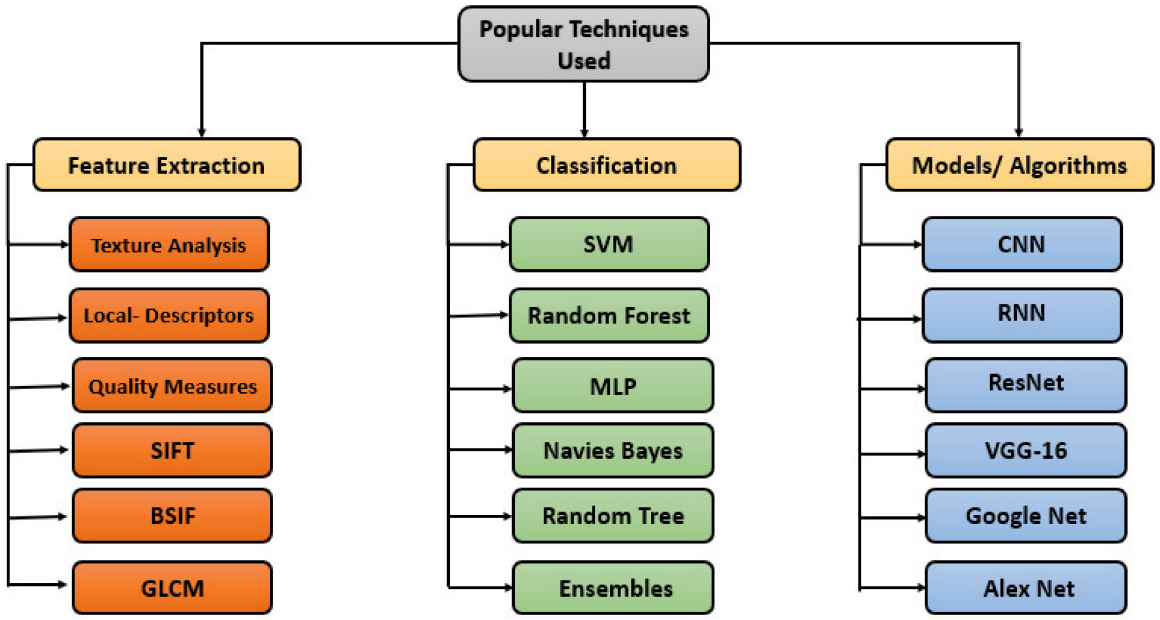



**Figure 18.** Popular techniques used for iris liveness detection.

**Table 10.** Iris liveness detection: feature extraction, attacks identified, datasets, classifiers and performances measures.

| Paper ID | Authors/Year | Feature Extraction | Attacks Identified | Datasets | Classifiers | Performances |
|---|---|---|---|---|---|---|
| [98] | Arora et al., 2021 | VGGNet, LeNet, ConvNet | NR | IIITD Iris Dataset | Softmax | FAR, Accuracy. |
| [108] | Garg et al. 2021 | 2DPCA, GA, SIFT | NR | (CASIA-Iris-Interval | BPNN | Accuracy = 96.40 %,FAR FRR Accuracy (%) F- measure Recall (%) Precision (%) MCC |
| [109] | Nguyen et al., 2020 | MLBP +CNN | Print Contact | Warsaw2017 ND2015 | SVM | APCER. |
| [110] | Adamović et al., 2020 | Stylometric features | NR | IITD and MMU | Random Forest, DT, NB, SVM | Accuracy (%) (%) Precision (%) Recall (%) F score (%) AUC" |
| [103] | Lin et al., 2020 | Haar Features | NR | CASIA1, 2 and MMU1,2 | AdaBoost | Accuracy 95.3% |
| [24] | Agarwal et al., 2020 | Texture feature, GLCM | Print | ATVS(Iris) LivDet2011 (finger) IIIT-D CLI dataset(Iris) | SVM | ACA = 96.3% |
| [50] | Agarwal et al., 2020 | Local binary hexagonal extrema pattern | Contact Print | IIIT-D CLI ATVS-FIr | SVM | AER = 1.8 %, |
| [10] | B. Kaur et al., 2019 | Orthogonal rotation-invariant feature-set comprising of ZMs and PHTs | Print + scan, Print + capture, patterned contact lenses | IIITD-CLI, IIS, Clarkson LivDet-Iris 2015, Warsaw LivDet-Iris 2015 | KNN | Accuracy= 98.49% (given differ. accuracy for diff. datasets) |

**Table 10.** *Cont.*

| Paper ID | Authors/Year | Feature Extraction | Attacks Identified | Datasets | Classifiers | Performances |
|---|---|---|---|---|---|---|
| [22] | Fathy and Ali, 2018 | Wavelet packets (WPs), local binary pattern (LBP), Entropy | Print Synthetic | ATVS-Fir CASIA-Iris-Syn | SVM | ACA= 99.92% Recall, Precision, F1. |
| [53] | Söllinger et al., 2018 | - "Non-reference image quality measures (IQM). - Natural scene statistics (NSS)." | NR | SDUMLA-HMT | KNN, SVM | "ACER using IQM features: kNN-IQM = 7.09%, SVM-IQM = 2.22% - ACER using NSS features: kNN-NSS = 0.88%, SVM-NSS = 0.06%" |
| [69] | Thavalengal et al., 2016 | Pupil localization techniques with distance metrics are used for the detection | Print | Real-time Datasets | Binary Tree Classifier | ACER= 0% |
| [60] | Das et al., 2016 | Image quality features | Contact Lens | Realtime | Euclidean distance as classifiers | ACA = 95% |
| [51] | Hu et al., 2016 | LBP, Histogram, SID. | Contact lenses, Print | Clarkson, Warsaw, Notre Dame, MobBIOfake | SVM | ER, Clarkson = 7.87%, Warsaw = 6.15% ND = 0.08%, MobBIO-fake = 1.50% |
| [21] | Naman Kohli et al., 2016 | Multi-order dense Zernike moments. -LBP with Variance | Print + Scan Print + Capture, Synthetic, Textured Contact Lens, Soft Contact Lens | IIIT-Delhi CLI, IIITD IIS, IIT Delhi Iris, Synthetic DB, Multi-sensor iris DB. | ANN as classifiers | Mean Classification Accuracy = 82.20 Std. Dev = 1.29 |
| [41] | Kiran B Raja et al., n.d. | Laplacian pyramids, STFT | Video Print | Real-Time 'Presentation Attack Video Iris Database' (PAVID). LiveDet iris 2013 | SVM | ACER = 0.64% |
| [44] | Sequeira et al., 2014 | High Frequency Power, Local Contrast, Global Contrast, Frequency Distribution Rates, Statistical Texture Analysis. | Print Contact Lense | MobBIOfake, - Clarkson, Biosec | DA, KNN, SVM | Best average Classification Error: - MobBIOfake DB using SVM = 12.50% - Clarkson DB using SVM = 5.69% - Biosec DB using KNNk 0.37%" |

**Table 10.** *Cont.*

| Paper ID | Authors/Year | Feature Extraction | Attacks Identified | Datasets | Classifiers | Performances |
|---|---|---|---|---|---|---|
| [33] | Galbally et al., 2014 | Image quality measures. | Print | ATVS CASIA-IrisV1(real images) WVU-Synthetic iris(spoofed Images) | LDA, QDA Classifiers | ER = 0.3% |
| [57] | Mateusz Trokielewicz et al., 2020 | Self-learned | Cadaver | Warsaw-BioBase-Postmortem-Iris-v1.1, Iris-v2, -Iris-v3 | DCNN | Accuracy, EER = 1% |
| [55] | Umer et al., 2020 | Self-learned | N/R | MMU1, UPOL, CASIA-Iris-distance, and UBIRIS.v2 | VGG16, ResNet50, Inception-v3 CNN | CCR= 99.64% |
| [52] | Arora and Bhatia, 2020 | Self-learned | Print Contact | IIITD-WVU dataset of LivDet 2017 Iris | DCNN | ACER = 26.19% |
| [105] | Abdellatef et al., 2020 | LBPs, ICA Mini-batch size Learning rate | N/R | CASIA-IrisV3 | CNN | Accuracy (%) Specificity (%) Precision (%) Recall (%) Fscore (%)" |
| [104] | Alay and Al-Baity, 2020 | CNN | N/R | SDUMLA-HMT, IT Delhi FERET | CNN | Accuracy = 99.35% |
| [63] | Kimura et al., 2020 | CNN | Print Contact | Clarkson, Warsaw, IIITD-WVU, Notre Dame | | APCER = 4.18% BPCER = 0% |
| [111] | Naqvi et al., 2020 | CNN model with a lite-residual encoder-decoder network | NA | NICE-II dataset, SBVPI | CNN | Average Segmentation Error = 0.0061 |
| [11] | Choudhary et al., 2019 | DenseNet | contact lens | ND Contact Lens 2013 Database, IIIT-Delhi (IIITD) Contact Lens | SVM DenseNet | Accuracy = 99.10% |
| [13] | Kuehlkamp et al., 2019 | Statistical features (BSIF). - CNN" | Print, Contact | Clarkson IIITD + WVU Notre Dame Warsaw | SVM CNN | HTER Clarkson = 9.45%, IIITD + WVU = 14.92%, Notre Dame = 3.28%, Warsaw = 0.68%" |

**Table 10.** *Cont.*

| Paper ID | Authors/Year | Feature Extraction | Attacks Identified | Datasets | Classifiers | Performances |
|---|---|---|---|---|---|---|
| [64] | Long and Zeng, 2019 | BNCNN | Synthetic, Contact | CASIA iris Lamp, CASIA iris Syn, Ndcontact | BNCNN | Correct recognition rate= 100% |
| [61] | Yadav et al., 2018 | LBP, W-LBP, DESIST, AlexNet | Contact Lens | MUIPAD database | SVM | Total Error = 1.01% APCER = 18.58% |
| [64] | D. T. Nguyen et al., 2018 | Local and global regions from iris image used for feature extraction with CNN | Print, Contact | LivDet-Iris 2017-Warsaw, Notre Dame Contact Lens Detection (NDCLD2015) | SVM | APCER, BPCER, ACER. Warsaw-2017 = 0.016% NDCLD-2015 = 0.292%" |
| [57] | Hoffman et al., 2018 | CNN | Print, Contact, Plastic. | LivDet-Iris Warsaw 2015 dataset, CASIA-Iris-Fake, BERC-Iris-Fake dataset | CNN | True Detection Rate (TDR) of: - LivDet-Iris Warsaw 2015 dataset = 95.11% - The printed PAs of the CASIA-Iris-Fake = 100% - Plastic CASIA = 43.75% - Contact PAs of the CASIA dataset = 9.30%" |
| [59] | Mateusz Trokielewicz et al., 2018 | VGG-16 | Cadaver | Real-Time Dataset | CNN | CCR = 99% |
| [54] | Yan et al., 2018 | Hierarchical Multi-class Iris Classification, Google Net | Print, Contact, Synthetic. | ND- Contact, CASIA-Iris-Interval, CASIA-Iris-Syn and LivDet-Iris-2017-Warsaw | CNN | CCR = 100%, FAR = 0%, FRR = 0% |
| [43] | Poster et al., 2017 | Eight-layer CNN and multi-layer perceptrons, VGG based network. | Contact lens. | Clarkson Livdet 2013, Notre Dame 1 and 2, Cogent and Vista IIITD Contact Lens. | CNN | ACER Clarkson = 3.25%, Cogent = 1.57% Vista IIITD = 0.22%, Notre Dame 1 = 0.1% Notre Dame 2 = 0.0%" |
| [112] | Pala & Bhanu, 2017 | CNN | Print, Contact | Iris-2013-Warsaw, IIIT Cogent and Vista | CNN | ACE = 0.0% |
| [113] | Gragnaniello et al., 2017 | CNN, Local Descriptors and Bag-of-Words | Print, Contact | Cogent, Vista, Notre dame | CNN | HTER = 1.03 Accuracy = 99.05 |

**Table 10.** *Cont.*

| Paper ID | Authors/Year | Feature Extraction | Attacks Identified | Datasets | Classifiers | Performances |
|---|---|---|---|---|---|---|
| [68] | He et al., 2016 | MCNN | Print, Contact, synthetic, plastic | ND-Contact, CASIA-Iris-Interval, CASIA-Iris-Syn, LivDet-Iris-2013-Warsaw, CASIA-Iris-Fake | MCNN | CCR = 100% FAR = 0% FRR = 0% |
| [45] | Menotti et al., 2015 | Texture analysis. -Deep Learning (neural networks). | Print | Biosec, Warsaw, MobBIOfake | SVM | ER = 0.9% |

## 5. Prototype/Framework for Iris Liveness Detection

The proposed architecture helps to identify all different types of spoofing attacks. Figure 19 shows a proposed framework for iris liveness detection. The design of the proposed system is sketched out in the phases that follow.

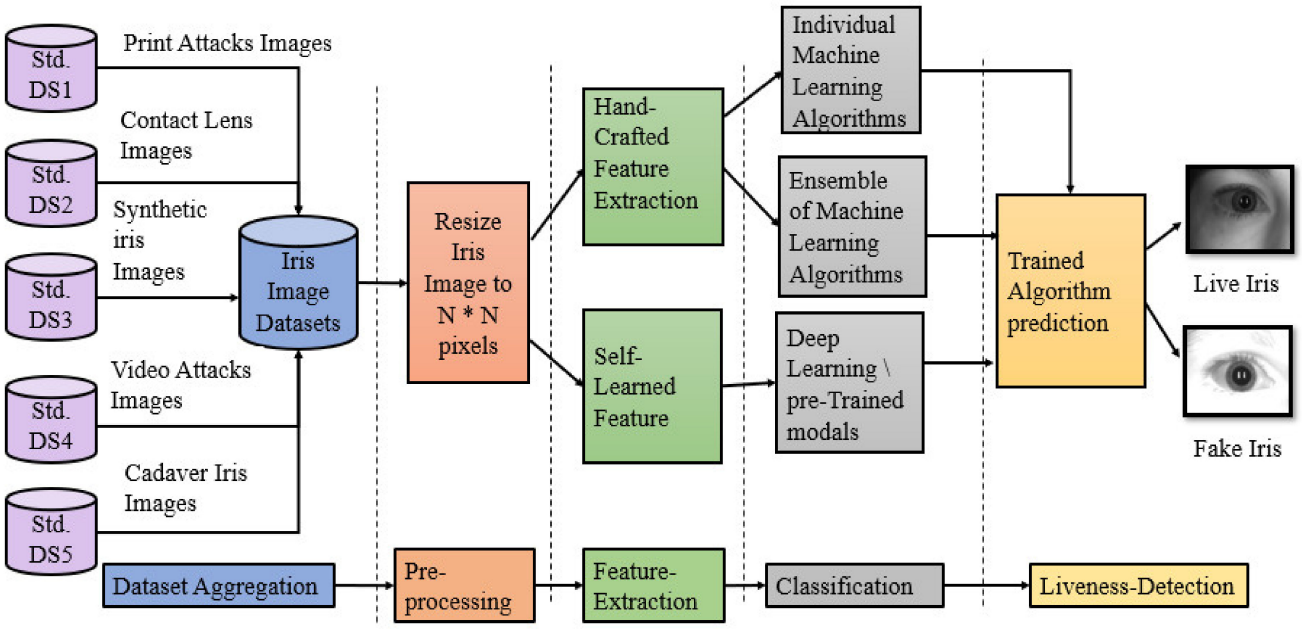



**Figure 19.** Proposed framework for iris liveness detection.

Step 1: Data Aggregation.

None of the standard datasets have all spoofing attacks images, so different spoofing attacks images need to be collected. This data is aggregated from standard benchmark datasets and used for proposed iris liveness detection. The proposed architecture needs to identify print attacks, contact lenses attacks, synthetic iris attacks, video attacks, and cadaver iris attacks.

Step 2: Data Preprocessing.

Data collection is performed on different standard datasets. Each dataset used different sensors for acquiring images, so it differs in size, and some images are colored, and some

are grayscale. To maintain integrity throughout the experiment, all images need to be converted to grayscale with uniform size.

Step 3: Feature Extraction.

In the proposed framework, both handcrafted features and self-learned features are used. For handcrafted feature extraction, cosine transform is used. The cosine transforms are applied to a resized iris image. The cosine transform enables high energy content to get accumulated in the low-frequency region in the transform domain. The low-frequency high energy region of cosine transformed iris image coefficients are taken to form feature vectors for proposed iris liveness detection. These feature vectors taken with high energy coefficients of cosine transformed iris images support reducing the size of feature vectors. Which resulting in faster iris liveness detection.

In self-learned feature extraction, VGG-16 is used. From the literature, it was observed that VGG-16 gives good accuracy for iris liveness detection. Therefore, by combining the VGG-16 pre-trained network and handcrafted features, we try to enhance the performances for iris liveness detection.

Step 4: Classification.

Extracted features from the previous step are passes to the machine and deep learning classifiers. The proposed ILD system uses different machine learning classifiers with ensembles combination. The 10-fold cross-validation approach is used for training these classifiers for iris liveness detection. The 10-fold cross-validation is one of the best approaches for the training of machine learning classifiers. It gives all samples from the dataset a chance to be part of training or test data, resulting in a less biased trained classifier. The Machine Learning Classifiers Random Forest (RF), Support Vector Machine (SVM), J48, Random Tree, and Naive Bayes (NB) with ensembles of a few of the machine learning classifiers are used.

Step 5: Liveness Detection.

The trained machine learning classifiers, ensembles of machine learning classifiers, and pretrained networks help to identified iris liveness. With the help of these trained classifiers, given images are classified as spoofed or live iris images.

## 6. Discussions

The review aids us to articulate answers to our research questions as follows; Table 11 gives overall summary of iris liveness detection survey.

**Table 11.** Summary of iris liveness detection survey.

| RQ. No | Area | Popular Techniques | Ref. | Merit | Demerits | Research Gaps |
|---|---|---|---|---|---|---|
| RQ1 | Feature Extraction Techniques | • Handcrafted Feature Textural Features, Statistical Features, SIFT, BSIF, LBP, IMQ,<br>• Self-Learned Feature CNN, VGG Net, Alex Net, DenseNet | [11,24,43,50,51,56, 59–61,63,76,98,104, 105,111] | • Manually engineered Handcrafted features are easily extracted and appropriate for resolving the PAD<br>• Self-learned features are extracted by using deep learning<br>• No training need for pre-trained models such as VGG Net, Alex Net, Google Net. | • Handcrafted feature extractors are mainly based on the proficient knowledge of the researchers on the problem.<br>• Deep learning models claim a large dataset for the training. The training from the ground up with deep learning is an extensive procedure that includes intricate experimentations with the diverse parameter values | • Handcrafted features are available in the literature with huge feature vector size, so need to focus on pre-trained models to reduce complexity and computational time. |

**Table 11.** *Cont.*

| RQ. No | Area | Popular Techniques | Ref. | Merit | Demerits | Research Gaps |
|---|---|---|---|---|---|---|
| RQ2 | Iris Spoofing Attacks | • Print,<br>• Contact Lens,<br>• Synthetic,<br>• Video,<br>• Cadaver Iris Attacks | [10,13,21,22,24,44, 50–53,57,61] | • The SVM classifier gives the best Spoof Detection accuracy for the classification of live and print attack images<br>• BNCNN with self-learn features gives a 100% correct recognition rate for contact lens.<br>• Google Net proves that synthetic iris can be identified with 100% accuracy<br>• SVM classifiers give the best ACER of 0.64% for video replay attacks<br>• VGG-16 detect cadaver iris with 99% accuracy | • Different classifiers or deep learning models are used to detect different types of attacks. Lack of single classifier model to identify all types of iris spoofing attacks | • No classifiers or ensembles of classifiers are available in the literature to identify all types of iris spoofing attacks. |
| RQ3 | Iris Dataset | • Controlled Environment,<br>• Uncontrolled Environment,<br>• Smartphone DB,<br>• Cross-sensor<br>• Iris DB,<br>• Liveness detection DB. | [65,70–77,79,80,83–85,87,91,92] | • Images acquired by different sensors under different environmental conditions have different resolution and illumination distributions, contributing to better recognition performance. | • None of the datasets have images of all known types of spoofing attacks together. Most of the available datasets cover two to three types of spoofing attacks. Some datasets have images specifically for one type of attack. | • To work with iris liveness detection, we need a single dataset that contains all types of spoofing attacks images. We also need a dataset captured using visible lights and multiple sensors to capture images. |
| RQ4 | Perfromance Measures | • FAR, FRR,<br>• APCER,<br>• NPCER,<br>• FP rate,<br>• BPCER,<br>• Accuracy,<br>• Precision,<br>• Recall,<br>• F-measure,<br>• CCR, ACA. | [21,22,24,54,55,60,64, 68] | • The diverse metrics can be used for evaluation. biometric performance. Evaluation is standardized by ISO/IEC in the 1979 series of standards. | • In the literature, accuracy is used more frequently to detect iris liveness. Accuracy gives correct results when lives and fake samples are equals. | • Lack of performance metric for imbalanced datasets |

### *6.1. RQ1. What Are the Diverse Feature Extraction Techniques Available for Iris Liveness Detection?*

Feature extraction is a process that identifies the important attributes from the iris image. These extracted features are used to differentiate between real and spoof iris images. The two significant trends were detected for removing features in existing ILD literature: liveness detection using machine learning and liveness detection using deep learning.

ML is a branch of AI that learns naturally from the data given and advances the valuation without being specifically taught. For example, in iris biometric ML is used for the recognition and sorting of spoofed identity.

Experts apply handcrafted image feature extraction algorithms in the machine learning approach to identify image features from iris images. These handcrafted features are categorized into two types, local features extraction and global features extraction. In local feature extraction, small image patches are used to extract the features. In contrast, the entire iris image is used to extract a global feature, for handcrafted feature extraction researcher used LBP [50,51], local descriptors, quality analysis [60], wavelet transform, textural features [24], statistical features, SIFT [77] BSIF, and histogram [51] as the feature extraction techniques. All the feature extraction techniques were discussed in Section 4. However, it was observed in the literature that the features extracted using image quality measures give the best performances.

These extracted features are used to classified Lived and Spoofed iris images. The different classification methods such as support vector machines (SVM) [22,24,50], Ran-

dom Forest AdaBoost [103], binary tress [69], and KNN [10] are used to classify the images into two classes of live images and spoofed images. It is observed from the service that SVM gives good performances against all the handcrafted features. Fathy and Ali proves that by using SVM with LBP features, the model gives the best performances with ACA = 99.92% [22].

"The results of the above methods display that the manually engineered features are appropriate for resolving the PAD (presentation attack detection) issue for iris recognition systems. However, their weakness is that the design and the selection of the handcrafted feature extractors are mainly based on the proficient knowledge of the researchers on the problem." Accordingly, these features frequently only reflect restricted "aspects of the problem and are often subtle to varying acquisition conditions, such as camera devices, lighting conditions, and presentation attack instruments (PAIs). This causes their detection accuracy to fluctuate suggestively among the different datasets, signifying that the handcrafted features have poor generalizability and fail to solve the PAD problem. The accessible multiple-datasets tests in the literature recommend that the performance of hand-crafted texture-based techniques can worsen intensely, operating in unidentified conditions, leading to the need the automatically extracting vision evocative features directly from the data using deep representations to support the task of presentation attack detection".

Self-learn features are extracted by using deep learning. "Deep learning depends on layer upon layer of training" of the existing data to effectively recognize the intricate patterns. DL-based "approach is similar to the ML-based approach, and the" key variance between them is the detection algorithms and the models used.

DL-based approach practices: there are "two types of models: First is the model that is standard models trained from scratch, using the training data, and second is the pre-trained models, that is, models trained on data or features taken from a similar domain."

Techniques such as Convolutional Neural Networks (CNNs) are used for ILD and classification [114] in the consistent models. Many studies from the literature used CNN for ILD [56,63,104,105,111]. CNN takes data as input that has a matrix design such as the images [114]. Therefore, CNN has been effectively functional in the areas of iris recognition.

Deep learning models claim a large dataset for the training. The training from the ground up with deep learning is an extensive procedure that includes the intricate experimentations with the diverse "parameter values, for example, weights, number of filters, and layers, amongst others". This is the cause, why many researchers use pre-trained models, for example, "Inception, VGGNet [43,59,98], AlexNet [61], DenseNet" [11]. The studies using the pre-trained model in ILD extract the unfair features. It was observed in the literature that VGG Net is used more frequently to detect iris liveness.

### *6.2. RQ2. What Are the Different Types of Spoofing Attacks Done on Iris Liveness Detection?*

The mechanism iris spoofing enables the impersonation of the individual identity [23]. Biometric devices are inclined to spoofing attacks that lessen their safety [19]. Spoofing attacks are easy to execute as the least technical information is required about the method of the working system or the use of the algorithm. Spoofing attacks can be carried out in various ways, such as print attacks, contact Lens attacks, video attacks, cadaver, and synthetic iris attacks.

The presentation of a printed image of an iris to the scanner/system can assist in copying the identity of an individual. An iris recognition system can be considerably misled with a suitable printer and paper combination and the quality of printed iris [21]. Print attacks can be performed in two ways (print and scan) and (print and capture). In (print and scan) attacks, the pattern of iris is printed with the help of a high-quality printer and, at that time, scanned. In (print and capture) attacks, the scanner captures the photo support vector machines notice the images of the print attack. The most recurrently used handcrafted feature extraction techniques to identify the print attacks are LBP [21,22,50], texture analysis [44], and image quality measures [53]. The SVM classifier gives the best spoof detection accuracy for the classification of live and print attack images. After SVM,

Random Forest and decision tree classifiers give good classification accuracy [22]. Many authors used CNN [43,54–56,63] for print attacks identification. The author [63] shows that a convolutional neural network (CNN) gives the best classification accuracy of the print attacks.

The contact lenses have three categories, texture contact lens, color contact lens, and clear contact lens. In literature, the "term textured contact lenses" typically refers to the "contact lenses". These contact lenses have a textured appearance. Even if no visual texture was printed on the colored contact lens, it was colored with a certain color. clear contact lenses neither have color nor a visible texture. To identify the contact lens attacks, different feature extraction techniques are used in the literature. Texture analysis [44], LBP [50] and histograms [51] are more frequently used handcrafted feature extraction techniques to identify the contact lenses. For the live and contact lens classification, the SVM classifier gives the best spoof detection accuracy followed by the random forest and decision tree classifiers. The author [64] proves that using BNCNN with self-learn features gives a 100% correct recognition rate.

The synthetic iris images are an additional probable attack that can replicate a Live/Real iris pattern. To generate the synthesized iris images, the iris textures of images are synthesized automatically from the exclusive iris Images. Then the iris ring regions are secured into the authentic iris images, making the artificial iris images more accurate. To present synthetic irises to biometric sensors, we need to take the printouts of an image or used a replay attack [58]. Most studies refer CASIA-Iris-Synthetic dataset to detect iris spoofing attacks, as datasets have more realistic iris Images. The author [22] used Wavelet Packets (WPs), Local Binary Pattern (LBP) to detect the synthetic iris at-tacks in iris biometric system. The author [64] proved that BNCNN could detect Synthetic iris with CCR = 100%. By using Google Net, author proves that Synthetic iris can be identified with 100% accuracy [54].

The Imposter plays the Eye video of the "registered identity in front of a biometric system" in the Video attack. Video attacks are also mentioned as replay attacks. As the video consists of enough motion information, it is easy to Step forward a Biometric Authentication system [14]. The static and dynamic patterns of the eye can be copied using Video attacks. Compared to all other attacks, video attacks are less identified in the literature of iris Biometric authentication. Till now, in literature, no one has identified video spoofing attacks by using Deep Learning algorithms.

We are unaware of any testified effective attack on a professional iris detection system based on cadaver eyes [58]. It is probable to obtain a post-mortem iris image up to 1 month after death, using commercial iris sensors in cold temperatures (around 6 °C/42.8 °F). Somebody may use an "image of a post-mortem sample" to conceal their identity. "Post-mortem iris samples" thoroughly bear a resemblance to living irises in the formative stages after death. In literature, Deep Learning techniques are used for the identification of cadaver attacks [58] the author used VGG-16 to detect cadaver iris with 99% accuracy. No one attempted to identify the cadaver iris spoofing attacks with the Handcrafted feature extraction techniques.

It was observed from this study that; many datasets are available in the kinds of literature that focus on the specific attacks. The researchers have been attentive towards one specific sort of iris spoofing attack and have presented algorithms to address it in the literature. However, in the hands-on circum-stances, iris recognition systems must handle and spot all the categories of spoofing attacks [21]. Therefore, there is the need to advance the framework that spots all the sorts of prevalent spoofing attacks

### *6.3. RQ3. Which Are Relevant Datasets Available for Iris Liveness Detection?*

Data plays a very important role while building a model which gives better accuracy. The accurate dataset comprising adequate "quantity and quality data for training and testing the model" is indispensable for good research results. It was noticed that the researchers had trained the varied datasets for making the model for ILD. Datasets are classified into two types: Standard benchmark datasets and Custom\Real-time Datasets. The

datasets used in PAD (Presentation Attack Detection Competition), with wide availability, are known as the Standard Benchmark Datasets.

These standard datasets are classified into different categories based on the Image Acquisition process. The Image Acquisition process is used during building a dataset. The categorization into Con-trolled environment and Uncontrolled environment datasets are based on the control factors in the environment. The Control factors in the environment are used to capture iris images. The dataset is categorized into Single-sensors (cross-sensors) and mobile/smartphone captured images based on the diversity of sensors. The diversity of sensors is used to capture iris images. The majority of the datasets focus on the detection and the classification of the varied iris Spoofing attacks.

Controlled environment datasets are those in which the images are captured, considering the following factors: The Conditions during the image captures, Factors with environmental conditions such as Light, Illumination. The first publicly available controlled environment dataset was the CASIA iris Dataset v.1 gathered by the "National Laboratory of Pattern Recognition, Institute of Automation, CASIA". In iris Liveness Detection, the Images captured using the controlled environment are less frequently used [58] than those captured in Visible light / Uncontrolled Environment. This is because the images captured in the Controlled environment do not include the variances of the real-world situations.

Different properties such as Light, Distances, Angle, and Size vary while capturing iris images in an Uncontrolled environment. The recognition of iris in visible light positions the further challenges such as diversity of "environmental conditions, wide-angle optical systems, and passive lighting". The most popular datasets in the Uncontrolled environment are "UBIRIS-V1 [72], UBIRIS-V2 [72], and UPOL ". Many researchers preferred using Visible light imaging datasets compared to the controlled environment datasets [70]. The images available in the uncontrolled datasets pose many variabilities such as Light, Distance, Angle, and Size. The images captured using the Visible light are prone to noise compared to those captured using the Controlled environment [74]. The up-to-date performance of VIS iris recognition is poor with its NIR cameras

The extensive use of smartphones has aided many researchers to start the work on iris recognition in the movable environment. Some mobile phones/applications offer an authentication system using the human iris. The smartphones have built-in, high-resolution cameras, resulting in creating and introducing the datasets, with the easiness of capturing images. CASIA iris M1 (mobile) is the most popular mobile dataset, which contains three subsets: S1 [52], S2 [24], and S3 [52]. The dataset is prevalent because it is collected with the assistance of a mobile phone having a combined NIR iris-scanning sensor. It was observed that the datasets collected using smartphone/mobiles are used only for smartphone-based iris Liveness Recognition applications.

The global positioning of iris recognition systems includes the usage of numerous sensors. Different manufacturers design the sensors required for the recognition systems. The variances in sensor quality and image capturing processes affect the changeability of iris recognition rates. Various cross-sensor iris datasets were introduced to analyze these influences and acquiring images such as LG, Nokia, Vista, CMTech, Cogent, InTech, Cannon, irisGuard, Galaxy, and Dalsa. LG sensors are used most widely while capturing iris images. LG sensors can spot the users, though the user is at a distance of 3 m. IIITD-WVU iris Spoofing Dataset is the popular Cross-sensor iris dataset. The-Observations while studying these datasets are:

1. Each dataset uses different sensors to capture the iris images.
2. The quality of the image varies, depending on the used sensors.
3. Sensor type was not declared in some datasets.
4. The position of the sensor, that is, the distance from eyes, was not revealed in the datasets document.

Iris spoofing is a mechanism by which one can emulate an individual identity. The different datasets capture diverse spoofed images. For example, the printout of the original iris is taken and presented as a spoofed image. In some datasets, the images of the iris are

captured after wearing the contact lens. A few datasets have taken the images of remains of (fake) iris, and few datasets have generated the images from the original iris images with the synthesis. The datasets containing the spoofed as well as the real iris images are ideal for iris Liveness Detection. In Section 4.3, Table 9 displays the most frequently used datasets for iris Liveness Detection, with Spoofed and Lived Images.

It was observed that none of the datasets have the images of all known types of spoofing attacks together. Most of the available datasets cover two to three types of spoofing attacks. In addition, some datasets have images specifically for one type of attack. As no such dataset is available, the researchers need to work on multiple datasets to implement the ILD System. So, to make a robust ILD model against all the types of known attacks, there is the need for a Dataset, which covers all the known types of attacks in a single dataset.

### *6.4. RQ4. What Are All the Different Evaluation Measures Used for Iris Liveness Detection?*

Biometric performance metrics rate the functioning of a biometric system. The diverse metrics can be used for this purpose. Biometric performance evaluation is standardized. It is completed jointly by ISO/IEC in the 1979 series of standards. The most commonly used performance measures are discussed in detail in Section 4.4.

In the literature, accuracy is used more frequently to detect iris Liveness. Accuracy is a ratio between the number of correctly classified images and the total number of images. The correctness of the Accuracy in the working depends upon the balanced classes. This means the figure for live samples and fake samples are identical. Many authors [10,21,56,103–105], used the Accuracy for evaluating the performances of Liveness Detection model.

An Accuracy is the most commonly used matrix in literature for evaluating the performances of the iris Detection System. It is a matrix that can be used for Detection, Verification, and Identification of the iris Liveness System.

After Accuracy, Attack Presentation Classification Error Rate (APCER), FAR, and FRR are usually used in literature. APCER is the part of attack images mistakenly classified as Live samples; the proportion of attack Presentations, incorrectly classified as bonafide presentations. "APCER is the rate of misclassified spoof images (spoof called live)".

In literature, most of the authors [41,43,44,50,69] used APCER for evaluating the Performances of iris Detection system.

FAR [54,68,98]" is the probability of cases for which a biometric system" inaccurately approves an unofficial person. It is one of the most usually used metrics in Biometric Recognition systems for evaluating the system's performance. FRR [54,68,98] is the probability of cases for which a biometric system inaccurately refutes admission to a lawful person. "The False Rejection Rate (FRR) is one of the significant metrics along with FAR" and is normally used for evaluating the performance of a biometric system.

The performance rates of a biometric system can be stated in many ways. For example, in decimal format (0.05), in percent (1%), as fractions (1/100), or by using powers of ten (10¬2)). In literature, many authors used more than one performance measure to evaluate the performances of the iris Biometric system. While calculating the performance accuracy, the performance measure was used more frequently. The other measures such as FAR, FRR, TP rate, FP rate, etc., are used to plot the performance evaluation results using the DET and ROC graphs.

## 7. Threats to Validity

The SLR such as this one has numerous obvious threats to its rationality, such as whether or not the suitable keywords were recognized or adequate search engines were selected. In this respect, a list of different papers shows that the search scope is adequate since no added papers have been found to follow the recognized Inclusion criteria.

Lastly, another significant risk to rationality is consistency, which emphasizes whether the data are extracted. The examination is accomplished so that other researchers can

repeat the study to get similar results. In this respect, the search term was clear, and the procedures were applied during the review so that others can simulate the study.

Even though ensuring a systematic, precise protocol, it is not certain that all the applicable works about this field are recovered. Moreover, a Biometric Authentication system such as iris detection always suffers from the threat of lesser availability to larger resources, datasets due to confidentiality and safety reasons.

## 8. Limitations of the Study

Even though it is widespread, our SLR may have omitted some applicable studies due to the restraint of the scientific dataset, precise keywords used in the search, and timeframe designated for the review. We selected only 67 studies from 2010 to 2021. We trusted manual screening of studies attained from the "libraries such as SCOPUS, ACM, and Web of Science".

This review was restricted to techniques such as Machine Learning-based Handcrafted Feature Extraction and Deep Learning-based Self- Learned features. Thus, some of the literature may have been unused during the choice of studies for this survey. This document depicts the intended ILD system's architecture as an alternative to the explored solutions in the literature concerning the variation of datasets, different sorts of attacks, and Features Extraction techniques. The proposed architecture is undergoing research. Therefore, the evaluation is not specified in this paper.

## 9. Conclusions

To carry out an executive survey in ILD and iris attacks detection concerning the important artifacts such as feature extraction techniques, iris spoofing attacks, iris datasets, and performances measures.

A systematic review was steered to perform this study, which permitted us to survey a detailed method to describe research questions and get results from the primary studies for analysis. First, peer reviews of articles concerning the inclusion and exclusion criteria were executed. To conclude, the last 67 remaining studies provided the predictable response to the research question and were designated for this study.

All the handcrafted features and self-learned features were considered. We detected that; the handcrafted features are appropriate for resolving the "PAD problem for iris recognition systems". Nevertheless, their disadvantage is that the strategy and assortment of the handcrafted feature extractors are chiefly founded on the proficiency of the researchers on the problem. It leads to the prerequisite of the automatic extraction of the features unswervingly from the data, using deep learning. We unveiled those deep learning methods which demand a large dataset for the training. This work outlines the merits and demerits of every feature extraction technique and the associated classification algorithm to lay the foundation of future research work.

The work is amongst those few studies that address the attacks related to iris liveness. It presents the scientific understanding of the attack, detection methods, and the available data sets to detect them. It opens the research challenges of the unavailability of an aggregated dataset encompassing the different types of spoofing attacks on iris liveness detection. Biometric systems are more susceptible to spoofing attacks. Iris biometric, print attacks, contact lens attacks, video attacks, synthetic iris attacks, and cadaver iris are more prevalent attacks. It was observed that only a few studies detected all types of spoofing attacks. There was no classification model present in the literature, which identified all the iris spoofing attacks. We conclude from these observations that there is a need to create a classifier or ensembles of the classifiers that identified all the types of a spoofing attacks.

In RQ3, the different datasets used by the researchers were analyzed. It was observed that the researcher prefers to work on the standard benchmark datasets instead of creating their datasets. Furthermore, we face the challenge with the "validation of datasets; biometric datasets" are not publicly available due to privacy issues. It was concluded that

there is the need to create a common repository for iris datasets, which are easily and freely accessible to all the researchers.

In RQ4, All the evaluation metrics used in ILD research were studied. It was found that accuracy and APCER are more frequently used performance measures to evaluate iris liveness detection's performances.

After carrying out the executive survey in iris liveness detection, a novel prototype for ILD has been presented. This prototype for ILD is the general framework to detect iris spoofing attacks. We aim to build up one single framework that detects all the different iris spoofing attacks. Our first contribution goes with the help of datasets construction.

The review convincingly releases the prospects for the research in iris liveness detection. This is aimed at aggregating the different data sets and building an ensemble of classifiers for the attacks.

## 10. Future Work and Opportunities

We trust that this survey will be beneficial to the researchers, intelligence analysts and government agencies to assemble the compare datasets, techniques, methods to recognize iris liveness detection.

### *10.1. Feature Extraction*

It is observed in the literature that; the handcrafted features are appropriate for resolving the PAD challenge for iris recognition systems. Moreover, the construction and implementation of "handcrafted feature extractors" is primarily founded on the proficient knowledge of the experts' on the problem along with the abilities such as fast and accurate feature extraction and the use of pre-trained models to handle enormous amounts of data for more precise ILD Research.

### *10.2. Spoofing Attacks*

"In the literature, the researchers have been attentive towards one precise type of iris spoofing attack and have presented algorithms to address it [24,56,60,69]." However, in real-world situations, iris recognition systems must grip and spot all the types of spoofing attacks [21]. Therefore, there is the prerequisite to growing the framework that senses all the types of prevalent spoofing attacks.

### *10.3. Iris Attacks Specific Datasets*

The prevailing publicly accessible datasets are susceptible to the attacks such as print attacks, contact lens attacks, and video attacks, etc. There are no datasets available, which included all the probable and identified images of the attacks. Therefore, there is a need to develop a dataset with all the possible attacks.

### *10.4. Limited Publicly Available Datasets*

The prevailing datasets have to confront the challenge of the need for institutional or indivisible subscriptions for access. This concern can be handled by creating the Centralized Dataset Repository, easily and freely accessible without any institutional subscription.

### *10.5. Standard Format for Presenting the Iris Datasets*

From the literature, it may be concluded that the dataset creators hardly discuss the verification method of the qualitative analysis of the fake samples and the artifacts corresponding to the real presentation attacks. This concern can be handled by creating the standard format to present iris datasets.

**Author Contributions:** Conceptualization, S.K., S.A., and S.P.; methodology, S.K., S.A.; data curation, S.K., S.A.; writing—original draft preparation, S.K., S.P.; writing—review and editing, S.K., S.A., S.P., S.G., K.K.; visualization, S.D.T.; supervision, K.K., S.G. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Abbreviations

| | |
|---|---|
| N/A | Not Applicable, |
| VIS | Visible Light |
| N/R | Not Reported |
| MS | Multi-Sensor |
| PP | Live + Paper Printouts |
| CL | Live + Textured Contact Lenses |
| PM | Post-Mortem (cadaver) Iris |
| MB | Mobile Datasets. |
| A | IrisGuard AD100 Sensor |
| L2 | LG 2200 Sensor |
| L3 | LG Iris Access EOU3000 Sensor |
| L4 | LG 4000 Sensor |
| V | Vista Imaging VistaFA2E Sensor |
| BM | CMTech BMT-20 f/3.5–5.6 Zoom lens Sensor |
| IS | IriTech Irishield M2120U Sensor |
| C | Cogent CIS 202 Sensor |
| PE | Live + Prosthetic Eyes |
| CON | Controlled Environment |
| SY | Live + Synthetic Irises; |
| SS | Single Sensor |
| RA | Live + Replay Attack |
| PD | Pupil Dynamics |
| EM | Eye Movement Tracking |
| EV | Eyes Video |
| LY | Lytro Light Field Camera Sensor |
| IP | iPhone 5S Sensor |
| NL | Nokia Lumia 1020 Sensor |
| GS | Galaxy Samsung IV Sensor |
| DA | Dalsa (Unknown Model) Sensor |
| GT | Galaxy Tablet 2 Sensor |
| CN3 | Canon EOS Rebel T3i with EF-S 18–135mm IS Sensor |
| H | IrisGuard H100 Sensor |

## References

1. Khade, S.; Thepade, S.D. Fingerprint Liveness Detection with Machine Learning Classifiers Using Feature Level Fusion of Spatial and Transform. Domain Features. In Proceedings of the 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA), Pune, India, 12–21 September 2019; pp. 1–6. [CrossRef]
2. Khade, S.; Thepade, S. Novel Fingerprint Liveness Detection with Fractional Energy of Cosine Transformed Fingerprint Images and Machine Learning Classifiers. In *2018 IEEE Punecon*; IEEE: Piscataway, NJ, USA, 2018; pp. 1–7. [CrossRef]
3. Gupta, R.; Sehgal, P. A survey of attacks on iris biometric systems. *Int. J. Biom.* **2016**, *8*, 145. [CrossRef]
4. Islam, I.; Munim, K.M.; Islam, M.N.; Karim, M. A Proposed Secure Mobile Money Transfer System for SME in Bangladesh: An Industry 4.0 Perspective. In Proceedings of the International Conference on Sustainable Technologies for Industry 4.0 (STI), Dhaka, Bangladesh, 24–25 December 2019; pp. 1–6. [CrossRef]
5. Jeon, B.; Jeong, B.; Jee, S.; Huang, Y.; Kim, Y.; Park, G.H.; Kim, J.; Wufuer, M.; Jin, X.; Kim, S.W.; et al. A Facial Recognition Mobile App for Patient Safety and Biometric Identification: Design, Development, and Validation. *JMIR mHealth uHealth* **2019**, *7*, e11472. [CrossRef] [PubMed]
6. Gusain, R.; Jain, H.; Pratap, S. Enhancing bank security system using Face Recognition, Iris Scanner and Palm Vein Technology. In Proceedings of the 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal, India, 23–24 February 2018; pp. 1–5. [CrossRef]
7. Hsiao, C.-S.; Fan, C.-P. EfficientNet Based Iris Biometric Recognition Methods with Pupil Positioning by U-Net. In Proceedings of the 3rd International Conference on Computer Communication and the Internet (ICCCI), Nagoya, Japan, 25–27 June 2021; pp. 1–5. [CrossRef]

8. Xu, L.; Jiao, N.T. The Design of Hotel Management System Based on Iris Recognition Research. *Appl. Mech. Mater.* **2014**, *543–547*, 4565–4568. [CrossRef]
9. Su, L.; Shimahara, T. Advanced iris recognition using fusion techniques. *NEC Tech. J.* **2019**, *13*, 74–77.
10. Kaur, B.; Singh, S.; Kumar, J. Cross-sensor iris spoofing detection using orthogonal features. *Comput. Electr. Eng.* **2018**, *73*, 279–288. [CrossRef]
11. Choudhary, M.; Tiwari, V. An approach for iris contact lens detection and classification using ensemble of customized DenseNet and SVM. *Fut. Gener. Comput. Syst.* **2019**, *101*, 1259–1270. [CrossRef]
12. Kaur, J.; Jindal, N. A secure image encryption algorithm based on fractional transforms and scrambling in combination with multimodal biometric keys. *Multimedia Tools Appl.* **2018**, *78*, 11585–11606. [CrossRef]
13. Kuehlkamp, A.; Pinto, A.; Rocha, A.; Bowyer, K.W.; Czajka, A. Ensemble of Multi-View Learning Classifiers for Cross-Domain Iris Presentation Attack Detection. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 1419–1431. [CrossRef]
14. Chen, Y.; Zhang, W. Iris Liveness Detection: A Survey. In Proceedings of the IEEE Fourth International Conference on Multimedia Big Data (BigMM), Xi'an, China, 13–16 September 2018; pp. 1–7. [CrossRef]
15. Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.-K.R. A systematic literature review of blockchain cyber security. *Digit. Commun. Netw.* **2020**, *6*, 147–156. [CrossRef]
16. Dharmadhikari, S.C.; Ingle, M.; Kulkarni, P. Empirical Studies On Machine Learning Based Text Classification Algorithms. *Adv. Comput. Int. J.* **2011**, *2*, 161–169. [CrossRef]
17. Raheem, E.A.; Ahmad, S.M.S.; Adnan, W.A.W. Insight on face liveness detection: A systematic literature review. *Int. J. Electr. Comput. Eng. (IJECE)* **2019**, *9*, 5165–5175. [CrossRef]
18. Nguyen, K.; Fookes, C.; Jillela, R.; Sridharan, S.; Ross, A. Long range iris recognition: A survey. *Pattern Recognit.* **2017**, *72*, 123–143. [CrossRef]
19. Dronky, M.R.; Khalifa, W.; Roushdy, M. A Review on Iris Liveness Detection Techniques. In Proceedings of the Ninth International Conference on Intelligent Computing and Information Systems (ICICIS), Cairo, Egypt, 8–10 December 2019; pp. 48–59. [CrossRef]
20. Rattani, A.; Derakhshani, R. Ocular biometrics in the visible spectrum: A survey. *Image Vis. Comput.* **2017**, *59*, 1–16. [CrossRef]
21. Kohli, N.; Yadav, D.; Vatsa, M.; Singh, R.; Noore, A. Detecting medley of iris spoofing attacks using DESIST. In Proceedings of the IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), Niagara Falls, NY, USA, 6–9 September 2016; pp. 1–6. [CrossRef]
22. Fathy, W.S.-A.; Ali, H.S. Entropy with Local Binary Patterns for Efficient Iris Liveness Detection. *Wirel. Pers. Commun.* **2017**, *102*, 2331–2344. [CrossRef]
23. Armi, L.; Fekri-Ershad, S. Texture image analysis and texture classification methods—A review. *arXiv* **2019**, preprint. arXiv:1904.06554.
24. Agarwal, R.; Jalal, A.S.; Arya, K.V. A multimodal liveness detection using statistical texture features and spatial analysis. *Multimed. Tools Appl.* **2020**, *79*, 13621–13645. [CrossRef]
25. Zhang, H.; Sun, Z.; Tan, T. Contact Lens Detection Based on Weighted LBP. In Proceedings of the 20th International Conference on Pattern Recognition, Istanbul, Turkey, 23–26 August 2010; pp. 4279–4282. [CrossRef]
26. He, Z.; Sun, Z.; Tan, T.; Wei, Z. *Efficient Iris Spoof Detection via Boosted Local Binary Patterns*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 1080–1090. [CrossRef]
27. Geng, J.; Li, Y.; Chian, T. SIFT based iris feature extraction and matching. In *Geoinformatics 2007 Geospatial Information Science*; International Society for Optics and Photonics: Bellingham, WA, USA, 2007; Volume 6753, p. 67532F. [CrossRef]
28. Raja, K.B.; Raghavendra, R.; Busch, C. Binarized Statistical Features for Improved Iris and Periocular Recognition In Visible Spectrum. In Proceedings of the 2nd International Workshop on Biometrics and Forensics, Valletta, Malta, 27–28 March 2014; pp. 1–6.
29. McGrath, J.; Bowyer, K.W.; Czajka, A. Open Source Presentation Attack Detection Baseline for Iris Recognition. *arXiv* **2018**, preprint. arXiv:1809.10172.
30. Raghavendra, R.; Raja, K.B.; Busch, C. Ensemble of Statistically Independent Filters for Robust Contact Lens Detection in Iris Images. In Proceedings of the Indian Conference on Computer Vision Graphics and Image Processing, Bangalore, India, 14–18 December 2014. [CrossRef]
31. Demirel, H.; Anbarjafari, G. Iris recognition system using combined histogram statistics. In Proceedings of the 23rd International Symposium on Computer and Information Sciences, Istanbul, Turkey, 27–29 October 2008; pp. 1–4. [CrossRef]
32. Yambay, D.; Czajka, A.; Ii, F. LivDet-Iris 2015—Iris Liveness Detection Competition 2015 University of Naples. In Proceedings of the IEEE International Conference on Identity, Security and Behavior Analysis (ISBA), New Delhi, India, 22–24 January 2015.
33. Galbally, J.; Marcel, S.; Fierrez, J. Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition. *IEEE Trans. Image Process.* **2013**, *23*, 710–724. [CrossRef]
34. Vasantha, K.; Ravichander, J. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. *Int. J. Recent Technol. Eng.* **2019**, *8*, 63–67.
35. El-Din, Y.S.; Moustafa, M.N.; Mahdi, H. Deep convolutional neural networks for face and iris presentation attack detection: Survey and case study. *IET Biom.* **2020**, *9*, 179–193. [CrossRef]
36. Czajka, A. Pupil Dynamics for Iris Liveness Detection. *IEEE Trans. Inf. Forens. Secur.* **2015**, *10*, 726–735. [CrossRef]

37. Nguyen, K.; Fookes, C.; Ross, A.; Sridharan, S. Iris Recognition with Off-the-Shelf CNN Features: A Deep Learning Perspective. *IEEE Access* **2017**, *6*, 18848–18855. [CrossRef]
38. System, R. Deep Learning Approach for Multimodal Biometric. *Sensors* **2020**, *19*, 5523.
39. Abed, E.A.; Mohammed, R.J.; Shihab, D.T. Intelligent multimodal identification system based on local feature fusion between iris and finger vein. *Indones. J. Electr. Eng. Comput. Sci.* **2021**, *21*, 224–232. [CrossRef]
40. Tan, C.-W.; Kumar, A. Integrating ocular and iris descriptors for fake iris image detection. In Proceedings of the 2nd International Workshop on Biometrics and Forensics (IWBF), Valletta, Malta, 27–28 March 2014; pp. 1–4. [CrossRef]
41. Raja, K.B.; Raghavendra, R.; Busch, C. Presentation attack detection using Laplacian decomposed frequency response for visible spectrum and Near-Infra-Red iris systems. In Proceedings of the IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), Arlington, VA, USA, 8–11 September 2015; pp. 1–8. [CrossRef]
42. Silva, P.; Luz, E.; Baeta, R.; Pedrini, H.; Falcao, A.X.; Menotti, D. An Approach to Iris Contact Lens Detection Based on Deep Image Representations. In Proceedings of the 28th SIBGRAPI Conference on Graphics, Patterns and Images, Salvador, Brazil, 26–29 August 2015; pp. 157–164. [CrossRef]
43. Poster, D.; Nasrabadi, N.; Riggan, B. Deep sparse feature selection and fusion for textured contact lens detection. In Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 26–28 September 2018; pp. 1–5.
44. Sequeira, A.; Murari, J.; Cardoso, J.S. Iris Liveness Detection Methods in Mobile Applications. In Proceedings of the International Conference on Computer Vision Theory and Applications (VISAPP), Lisbon, Portugal, 5–8 January 2014; pp. 22–33. [CrossRef]
45. Menotti, D.; Chiachia, G.; Pinto, A.; Schwartz, W.; Pedrini, H.; Falcao, A.X.; Rocha, A. Deep Representations for Iris, Face, and Fingerprint Spoofing Detection. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 864–879. [CrossRef]
46. Gupta, P.; Behera, S.; Vatsa, M.; Singh, R.; Gupta, P.; Behera, S.; Singh, R. On Iris Spoofing Using Print Attack. In Proceedings of the 22nd International Conference on Pattern Recognition, Stockholm, Sweden, 24–28 August 2014; pp. 1681–1686. [CrossRef]
47. CCC. Chaos Computer Clubs Breaks Iris Recognition System of the Samsung Galaxy S8. Available online: https://www.ccc.de/en/updates/2017/iriden (accessed on 12 May 2021).
48. Yes, Cops Are Now Opening iPhones with Dead People's Fingerprints. Available online: https://www.forbes.com/sites/thomasbrewster/2018/03/22/yes-cops-are-now-opening-iphones-with-dead-peoples-fingerprints/?sh=5ebb6c25393e (accessed on 12 May 2021).
49. Raghavendra, R.; Busch, C. Robust Scheme for Iris Presentation Attack Detection Using Multiscale Binarized Statistical Image Features. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 703–715. [CrossRef]
50. Agarwal, R.; Jalal, A.S.; Arya, K.V. Local binary hexagonal extrema pattern (LBHXEP): A new feature descriptor for fake iris detection. *Vis. Comput.* **2020**, *37*, 1357–1368. [CrossRef]
51. Hu, Y.; Sirlantzis, K.; Howells, G. Iris liveness detection using regional features. *Pattern Recognit. Lett.* **2016**, *82*, 242–250. [CrossRef]
52. Arora, S.; Bhatia, M.P.S. Presentation attack detection for iris recognition using deep learning. *Int. J. Syst. Assur. Eng. Manag.* **2020**, *11*, 232–238. [CrossRef]
53. Söllinger, D.; Trung, P.; Uhl, A. Non-reference image quality assessment and natural scene statistics to counter biometric sensor spoofing. *IET Biom.* **2018**, *7*, 314–324. [CrossRef]
54. Yan, Z.; He, L.; Zhang, M.; Sun, Z.; Tan, T. Hierarchical Multi-class Iris Classification for Liveness Detection. In Proceedings of the International Conference on Biometrics (ICB), Gold Coast, QLD, Australia, 20–23 February 2018; pp. 47–53. [CrossRef]
55. Umer, S.; Sardar, A.; Dhara, B.C.; Rout, R.K.; Pandey, H.M. Person identification using fusion of iris and periocular deep features. *Neural Netw.* **2019**, *122*, 407–419. [CrossRef] [PubMed]
56. Trokielewicz, M.; Czajka, A.; Maciejewicz, P. Post-mortem iris recognition with deep-learning-based image segmentation. *Image Vis. Comput.* **2019**, *94*, 103866. [CrossRef]
57. Hoffman, S.; Sharma, R.; Ross, A. Convolutional Neural Networks for Iris Presentation Attack Detection: Toward Cross-Dataset and Cross-Sensor Generalization. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Salt Lake City, UT, USA, 18–22 June 2018; pp. 1701–17018. [CrossRef]
58. Trokielewicz, M.; Czajka, A.; Maciejewicz, P. Presentation Attack Detection for Cadaver Iris. In Proceedings of the IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), Redondo Beach, CA, USA, 22–25 October 2018; pp. 1–10. [CrossRef]
59. Trokielewicz, M.; Czajka, A.; Maciejewicz, P. Human iris recognition in post-mortem subjects: Study and database. In Proceedings of the IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), Niagara Falls, NY, USA, 6–9 September 2016; pp. 1–6. [CrossRef]
60. Das, A.; Pal, U.; Ferrer, M.A.; Blumenstein, M. A framework for liveness detection for direct attacks in the visible spectrum for multimodal ocular biometrics. *Pattern Recognit. Lett.* **2016**, *82*, 232–241. [CrossRef]
61. Yadav, D.; Kohli, N.; Agarwal, A.; Vatsa, M.; Singh, R.; Noore, A. Fusion of Handcrafted and Deep Learning Features for Large-Scale Multiple Iris Presentation Attack Detection. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Salt Lake City, UT, USA, 18–22 June 2018; pp. 685–6857. [CrossRef]
62. Nguyen, D.T.; Pham, T.D.; Lee, Y.W.; Park, K.R. Deep Learning-Based Enhanced Presentation Attack Detection for Iris Recognition by Combining Features from Local and Global Regions Based on NIR Camera Sensor. *Sensors* **2018**, *18*, 2601. [CrossRef] [PubMed]

63. Kimura, G.; Lucio, D.A.B., Jr.; Menotti, D. CNN Hyperparameter Tuning Applied to Iris Liveness Detection. In Proceedings of the 15th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications—Volume 5: VISAPP, Valletta, Malta, 27–29 February 2020; pp. 428–434. [CrossRef]
64. Long, M.; Zeng, Y. Detecting Iris Liveness with Batch Normalized Convolutional Neural Network. *Comput. Mater. Contin.* **2019**, *58*, 493–504. [CrossRef]
65. Boyd, A.; Fang, Z.; Czajka, A.; Bowyer, K. Iris presentation attack detection: Where are we now? *Pattern Recognit. Lett.* **2020**, *138*, 483–489. [CrossRef]
66. Kohli, N.; Yadav, D.; Vatsa, M.; Singh, R.; Noore, A. Synthetic iris presentation attack using iDCGAN. In Proceedings of the IEEE International Joint Conference on Biometrics (IJCB), Denver, CO, USA, 1–4 October 2017; pp. 674–680. [CrossRef]
67. Center for Biometrics and Security Research. Available online: http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp (accessed on 12 May 2021).
68. He, L.; Li, H.; Liu, F.; Liu, N.; Sun, Z.; He, Z. Multi-patch convolution neural network for iris liveness detection. In Proceedings of the IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), Niagara Falls, NY, USA, 6–9 September 2016; pp. 1–7. [CrossRef]
69. Thavalengal, S.; Nedelcu, T.; Bigioi, P.; Corcoran, P. Iris liveness detection for next generation smartphones. *IEEE Trans. Consum. Electron.* **2016**, *62*, 95–102. [CrossRef]
70. Omelina, L.; Goga, J.; Pavlovicova, J.; Oravec, M.; Jansen, B. A survey of iris datasets. *Image Vis. Comput.* **2021**, *108*, 104109. [CrossRef]
71. Biometrics Ideal Test. Available online: http://biometrics.idealtest.org/findTotalDbByMode.do?mode=Iris (accessed on 5 May 2021).
72. UBIRIS. Available online: http://iris.di.ubi.pt/index.html (accessed on 5 May 2021).
73. Fang, Z.; Czajka, A.; Bowyer, K.W. Robust Iris Presentation Attack Detection Fusing 2D and 3D Information. *IEEE Trans. Inf. Forensics Secur.* **2020**, *16*, 510–520. [CrossRef]
74. Trokielewicz, M.; Czajka, A.; Maciejewicz, P. Iris Recognition After Death. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 1501–1514. [CrossRef]
75. Kinnison, J.; Trokielewicz, M.; Carballo, C.; Czajka, A.; Scheirer, W. Learning-Free Iris Segmentation Revisited: A First Step Toward Fast Volumetric Operation Over Video Samples. In Proceedings of the International Conference on Biometrics (ICB), Crete, Greece, 4–7 June 2019; pp. 1–8. [CrossRef]
76. Yambay, D.; Becker, B.; Kohli, N.; Yadav, D.; Czajka, A.; Bowyer, K.W.; Schuckers, S.; Singh, R.; Vatsa, M.; Noore, A.; et al. LivDet iris 2017—Iris liveness detection competition 2017. In Proceedings of the IEEE International Joint Conference on Biometrics (IJCB), Denver, CO, USA, 1–4 October 2017; pp. 733–741. [CrossRef]
77. Image Analysis and Biometrics Lab. IIITD Contact Lens Iris Database, Iris Combined Spoofing Database. 2016. Available online: http://iab-rubric.org/resources.html (accessed on 4 June 2021).
78. Kohli, N.; Yadav, D.; Vatsa, M.; Singh, R. Revisiting iris recognition with color cosmetic contact lenses. In Proceedings of the International Conference on Biometrics (ICB), Madrid, Spain, 4–7 June 2013; pp. 1–7. [CrossRef]
79. Doyle, J.S.; Bowyer, K.; Flynn, P.J. Variation in accuracy of textured contact lens detection based on sensor and lens pattern. In Proceedings of the IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), Arlington, VA, USA, 29 September–2 October 2013; pp. 1–7. [CrossRef]
80. Doyle, J.S.; Bowyer, K.W. Robust Detection of Textured Contact Lenses in Iris Recognition Using BSIF. *IEEE Access* **2015**, *3*, t1672–1683. [CrossRef]
81. Holland, C.D.; Komogortsev, O.V. Complex Eye Movement Pattern Biometrics: The Effects of Environment and Stimulus. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 2115–2126. [CrossRef]
82. Rathgeb, C.; Uhl, A. Attacking Iris Recognition: An Efficient Hill-Climbing Technique. In Proceedings of the 20th International Conference on Pattern Recognition, Istanbul, Turkey, 23–26 August 2010; pp. 1217–1220. [CrossRef]
83. Czajka, A.; Fang, Z.; Bowyer, K. Iris Presentation Attack Detection Based on Photometric Stereo Features. In Proceedings of the IEEE Winter Conference on Applications of Computer Vision (WACV), Waikoloa, HI, USA, 7–11 January 2019; pp. 877–885. [CrossRef]
84. Yadav, D.; Kohli, N.; Vatsa, M.; Singh, R.; Noore, A. Detecting Textured Contact Lens in Uncontrolled Environment Using DensePAD. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Long Beach, CA, USA, 16–17 June 2019; pp. 2336–2344. [CrossRef]
85. Galbally, J.; Ortiz-Lopez, J.; Fierrez, J.; Ortega-Garcia, J. Iris liveness detection based on quality related features. In Proceedings of the 5th IAPR International Conference on Biometrics (ICB), New Delhi, India, 29 March–1 April 2012; pp. 271–276. [CrossRef]
86. Czajka, A. Database of iris printouts and its application: Development of liveness detection method for iris recognition. In Proceedings of the 18th International Conference on Methods & Models in Automation & Robotics (MMAR), Miedzyzdroje, Poland, 26–29 August 2013; pp. 28–33. [CrossRef]
87. Doyle, J.S.; Flynn, P.J.; Bowyer, K.W. Automated classification of contact lens type in iris images. In Proceedings of the International Conference on Biometrics (ICB), Madrid, Spain, 4–7 June 2013; pp. 1–6. [CrossRef]
88. Sun, Z.; Zhang, H.; Tan, T.; Wang, Y. Iris Image Classification Based on Hierarchical Visual Codebook. *IEEE Trans. Pattern Anal. Mach. Intell.* **2013**, *36*, 1120–1133. [CrossRef] [PubMed]

89. De Marsico, M.; Nappi, M.; Riccio, D.; Wechsler, H. Mobile Iris Challenge Evaluation (MICHE)-I, biometric iris dataset and protocols. *Pattern Recognit. Lett.* **2015**, *57*, 17–23. [CrossRef]
90. MICHE I—Mobile Iris CHallenge Evaluation—Part, I. Available online: http://biplab.unisa.it/MICHE/index_miche.htm (accessed on 5 May 2021).
91. Khan, F.F.; Akif, A.; Haque, M.A. Iris recognition using machine learning from smartphone captured images in visible light. In Proceedings of the IEEE International Conference on Telecommunications and Photonics (ICTP), Dhaka, Bangladesh, 26–28 December 2017; pp. 33–37. [CrossRef]
92. International Conference of Information Science and Management Engineering. *ISME* **2013**, *2*, 2014.
93. Iris Database. Available online: http://phoenix.inf.upol.cz/iris/ (accessed on 5 May 2021).
94. Ali Jahanian's Website. Available online: http://facultymembers.sbu.ac.ir/eshghi/index.html (accessed on 5 May 2021).
95. Busch, C. Standards for biometric presentation attack detection. In *Handbook of Biometric Anti-Spoofing*; Springer: Cham, Switzerland, 2019; pp. 503–514.
96. Biometric Performance Metrics: Select the Right Solution. Available online: https://www.bayometric.com/biometric-performance-metrics-select-right-solution/ (accessed on 9 June 2021).
97. Arora, S.; Bhatia, M.P.S.; Kukreja, H. *A Multimodal Biometric System for Secure User Identification Based on Deep Learning*; Springer: Berlin, Germany, 2020; pp. 95–103. [CrossRef]
98. Wang, K.; Kumar, A. Cross-spectral iris recognition using CNN and supervised discrete hashing. *Pattern Recognit.* **2018**, *86*, 85–98. [CrossRef]
99. Pradeepa, S.; Anisha, R.; Jenkin, W.J. Classifiers in IRIS Biometrics for Personal Authentication. In Proceedings of the 2nd International Conference on Signal Processing and Communication (ICSPC), Coimbatore, India, 29–30 March 2019; pp. 352–355. [CrossRef]
100. Marra, F.; Poggi, G.; Sansone, C.; Verdoliva, L. A deep learning approach for iris sensor model identification. *Pattern Recognit. Lett.* **2018**, *113*, 46–53. [CrossRef]
101. Accuracy, Precision, Recall or F1? Available online: https://towardsdatascience.com/accuracy-precision-recall-or-f1-331fb37c5cb9 (accessed on 5 May 2021).
102. Lin, Y.-N.; Hsieh, T.-Y.; Huang, J.-J.; Yang, C.-Y.; Shen, V.R.L.; Bui, H.H. Fast Iris localization using Haar-like features and AdaBoost algorithm. *Multimed. Tools Appl.* **2020**, *79*, 34339–34362. [CrossRef]
103. Alay, N.; Al-Baity, H.H. Deep Learning Approach for Multimodal Biometric Recognition System Based on Fusion of Iris, Face, and Finger Vein Traits. *Sensors* **2020**, *20*, 5523. [CrossRef]
104. Abdellatef, E.; Omran, E.M.; Soliman, R.F.; Ismail, N.A.; Elrahman, S.E.S.E.A.; Ismail, K.N.; Rihan, M.; El-Samie, F.E.A.; Eisa, A.A. Fusion of deep-learned and hand-crafted features for cancelable recognition systems. *Soft Comput.* **2020**, *24*, 15189–15208. [CrossRef]
105. Wang, H.; Zheng, H. Positive Predictive Value. In *Encyclopedia of Systems Biology*; Springer: New York, NY, USA, 2013; pp. 1723–1724.
106. Wang, H.; Zheng, H. True Positive Rate. In *Encyclopedia of Systems Biology*; Springer: New York, NY, USA, 2013; pp. 2302–2303.
107. Garg, M.; Arora, A.; Gupta, S. An Efficient Human Identification Through Iris Recognition System. *J. Signal. Process. Syst.* **2021**, *93*, 701–708. [CrossRef]
108. Nguyen, D.T.; Baek, N.R.; Pham, T.D.; Park, K.R. Presentation Attack Detection for Iris Recognition System Using NIR Camera Sensor. *Sensors* **2018**, *18*, 1315. [CrossRef]
109. Adamović, S.; Miškovic, V.; Maček, N.; Milosavljević, M.; Šarac, M.; Saračević, M.; Gnjatović, M. An efficient novel approach for iris recognition based on stylometric features and machine learning techniques. *Fut. Gener. Comput. Syst.* **2020**, *107*, 144–157. [CrossRef]
110. Naqvi, R.A.; Lee, S.-W.; Loh, W.-K. Ocular-Net: Lite-Residual Encoder Decoder Network for Accurate Ocular Regions Segmentation in Various Sensor Images. In Proceedings of the IEEE International Conference on Big Data and Smart Computing (BigComp), Busan, Korea, 19–22 February 2020; pp. 121–124. [CrossRef]
111. Pala, F.; Bhanu, B. Iris Liveness Detection by Relative Distance Comparisons. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Honolulu, HI, USA, 21–26 July 2017; pp. 664–671. [CrossRef]
112. Gragnaniello, D.; Sansone, C.; Poggi, G.; Verdoliva, L. Biometric Spoofing Detection by a Domain-Aware Convolutional Neural Network. In Proceedings of the 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), Naples, Italy, 28 November–1 December 2016; pp. 193–198. [CrossRef]
113. De Gibert, O.; Perez, N.; García-Pablos, A.; Cuadros, M. Hate Speech Dataset from a White Supremacy Forum. *arXiv* **2018**, preprint. arXiv:1809.04444.
114. Yamashita, R.; Nishio, M.; Do, R.K.G.; Togashi, K. Convolutional neural networks: An overview and application in radiology. *Insights Imag.* **2018**, *9*, 611–629. [CrossRef]