*big data and cognitive computing*

MDPI

*Review*

# Face Liveness Detection Using Artificial Intelligence Techniques: A Systematic Literature Review and Future Directions

**Smita Khairnar [1,2,*], Shilpa Gite [1,*], Ketan Kotecha [1] and Sudeep D. Thepade [2]**

[1] Department of Artificial Intelligence and Machine Learning, Symbiosis Centre for Applied Artificial Intelligence (SCAAI), Symbiosis Institute of Technology, Symbiosis International (Deemed) University (SIU), Lavale, Pune 412115, India
[2] Department of Computer Engineering, Pimpri Chinchwad College of Engineering, SPPU, Pune 411044, India
* Correspondence: chavansmita31@gmail.com (S.K.); shilpa.gite@sitpune.edu.in (S.G.)

**Abstract:** Biometrics has been evolving as an exciting yet challenging area in the last decade. Though face recognition is one of the most promising biometrics techniques, it is vulnerable to spoofing threats. Many researchers focus on face liveness detection to protect biometric authentication systems from spoofing attacks with printed photos, video replays, etc. As a result, it is critical to investigate the current research concerning face liveness detection, to address whether recent advancements can give solutions to mitigate the rising challenges. This research performed a systematic review using the PRISMA approach by exploring the most relevant electronic databases. The article selection process follows preset inclusion and exclusion criteria. The conceptual analysis examines the data retrieved from the selected papers. To the author, this is one of the foremost systematic literature reviews dedicated to face-liveness detection that evaluates existing academic material published in the last decade. The research discusses face spoofing attacks, various feature extraction strategies, and Artificial Intelligence approaches in face liveness detection. Artificial intelligence-based methods, including Machine Learning and Deep Learning algorithms used for face liveness detection, have been discussed in the research. New research areas such as Explainable Artificial Intelligence, Federated Learning, Transfer learning, and Meta-Learning in face liveness detection, are also considered. A list of datasets, evaluation metrics, challenges, and future directions are discussed. Despite the recent and substantial achievements in this field, the challenges make the research in face liveness detection fascinating.

**Keywords:** artificial intelligence (AI); domain adaptation; explainable AI (XAI); face liveness detection (FLD)



**Citation:** Khairnar, S.; Gite, S.; Kotecha, K.; Thepade, S.D. Face Liveness Detection Using Artificial Intelligence Techniques: A Systematic Literature Review and Future Directions. *Big Data Cogn. Comput.* **2023**, *7*, 37. https://doi.org/10.3390/bdcc7010037

Received: 9 December 2022
Revised: 28 January 2023
Accepted: 3 February 2023
Published: 17 February 2023



## 1. Introduction

Biometric authentication has consistently outperformed conventional password-based authentication schemes [1]. Personal identification was limited in prehistoric times. Today, computer vision and biometrics can distinguish people without credentials or artifacts [2]. Biometrics can identify people instead of their affiliations, belongings, or confidential information. The need for accurate and machine-based identification led us to biometrics, which uses technology to speed up the process of identifying and authenticating people. The printed IDs have been replaced with biometric IDs, which allow for proof of 'who you are' without carrying a card or other document [3].

Verification is a crucial step in granting authorized users access to the resources. Conventional authentication solutions, which include a PIN, card, and password, cannot distinguish between legitimate users and impostors who accessed the system fraudulently [1,2]. There are numerous chances of forgetting the password/PIN or losing or misplacing the card. A biometric system is a device that enables the automatic identification of an individual. There is no need to memorize a password, card, or PIN code because the biometric authentication system is simple to use [4].

Biometrics have been intensively researched for their automation, accessibility, and precision in meeting the increasing security demands of our daily life. As the technology has evolved through monitoring crime identification and forensics, it is a machine that analyzes human individuals' physiological and behavioral characteristics [5] to classify them uniquely. As per a report by (www.statista.com (accessed on 16 January 2023)), the market of contactless biometrics would reach 37.1 billion USD whereas, by 2028, the face-based biometric recognition market would reach USD 12.11 billion due to promising applications in diverse categories, as given in the "Facial Recognition Business" report [6]. Biometrics has been effectively implemented in several areas where security is a top priority. For instance, personal identity cards for airport check-in and check-out, confidential data from unauthorized individuals, and credit card validation.

Several biometric features, including fingerprint, iris, palm print, and face, are utilized for recognition and authentication. Face-based authentication provides more secure contactless authentication of the user than fingerprints and iris. Table 1 exhibits numerous facial biometric detection application domains.

**Table 1.** Several application domains for facial biometric detection.

| Application Domain | Usage |
| --- | --- |
| Security and Law enforcement | Identify and track criminals, and accelerate investigations [5] |
| Banking and Retail | Customer verifications through eKYC, used in the authentication of banking applications, Cardless ATM Transactions, online account creations, and digital payments such as apple pay [7,8] |
| Health Sector | Detecting genetic disease, tracking patient's effect of medications, and Health insurance records management [9] |
| Immigration and border checks | Face recognition for identity checks is implemented at various airports in European countries [10] |
| Education | Campus Security, attendance monitoring, and increasing learning engagement [11] |
| Mobile Devices | FaceID in smartphones such as Apple, Samsung, Motorola, and OnePlus [12] |

However, one of the biometric recognition systems' most significant challenges is deceptive identification, widely known as a spoofing attack [13]. Submitting a facial artifact of a legitimate user could easily construct using a person's face photos or videos from a "public" social media platform; an impostor can quickly access an insecure face recognition system. In general, also referred to as presentation attacks, these are straightforward, easy to implement, and capable of fooling face recognition (FR) systems and providing access to unauthorized users. These are becoming critical threats in advanced biometric authentication systems. Effective face liveness detection systems are increasingly attracting more attention in the research community, and several challenges make it difficult.

### *1.1. Significance and Relevance*

A few biometric traits evolved as the field progressed and occasionally disappeared. To be sure, face recognition is one biometric characteristic that has stood the test of time. Face characteristics are distinctive. Face-based authentication offers a more reliable yet contactless user identity than iris and fingerprint scanning. Face biometrics, which provides a secure identity and forms the basis of an inventive biometric system, has thus emerged as the preferred study area. However, printed face images or other artifacts can be used to fake invader challenges on face biometric systems, making them highly vulnerable. Spoofed

faces can stop the face recognition system from working correctly. Various researchers concentrate on identifying facial liveness to prevent attacks on the biometric system.

Therefore, it is crucial to categorize the current research on the biometric of Face liveness detection to address how growing technologies might provide explanations to lower the emerging hazards. Facial recognition-based applications have made tremendous progress due to artificial intelligence (AI) techniques. Deep learning has advanced in recent years [14–16]. The use of artificial neural networks or convolutional neural networks (CNNs) in many computer vision tasks [17–19] has been extensively studied [20], especially with the advancement of robust hardware and enormous data sets. Image categorization and object detection were successfully solved using CNNs [21]. The existing body of literature on Face liveness detection concentrates on advances in hardware and software and various categorization methods employing ML- and DL-based methodologies. It is essential to do a comparative examination of these procedures based on several assessment criteria. It is necessary to thoroughly examine the pertinent articles and academic publications to understand what research has been directed toward biometric and face liveness detection. This study seeks to provide information on a range of datasets, performance metrics, face spoofing attacks, and methods for detecting the liveness of a face.

### *1.2. Evolution of Face Biometric Liveness Authentication*

Fingerprints and other biometric features were used in previous biometric identification research. Semi-automated facial recognition systems that were distinctive to each person were initially proposed in 1988. Early in 2010, a face-liveness detecting algorithm was created. Since 2013, Face Liveness Detection (FLD) research has extensively used machine learning (ML) technologies.

The potential of ML to forecast and classify data is a key justification for using these algorithms. The face-liveness identification techniques include logistic regression, SVM, AdBoost, and Random Forest. The progress of face biometric authentication is seen in Figure 1. Huge volumes of information are processed using deep learning (DL) algorithms. The researchers started utilizing deep learning technology when facial liveness detection algorithms were introduced. Researchers have adopted DL methods for face liveness identification because they offer superior features to conventional handmade features. Some academics began working on the pre-trained networks used for face liveness detection, including convolutional neural networks (CNN), ResNet50, Inception model, VGG16, VGG19, GoogleNet, and AlexNet [20,22,23].

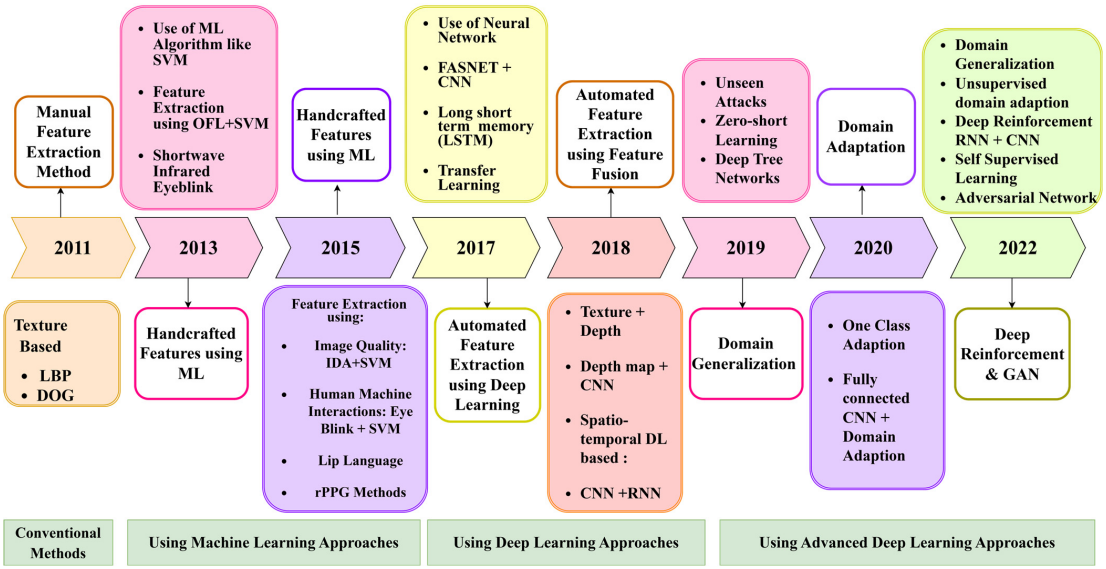


**Figure 1.** Progression of face liveness detection systems.

To uncover research trends and gaps in face liveness detection on face recognition (FR) systems, a systematic literature review (SLR) is necessary. This paper critically examines existing studies on face liveness detection and uses insights to develop new directions to achieve this goal.

### 1.3. Prior Research

Very few systematic literature review (SLR) papers are available on face liveness detection as per the authors' knowledge. One of the most recent review papers based on face anti-spoofing methods with generic consumer devices (RGB cameras) was by Ming et al. [24]. In this work, the authors discussed the typology of PAD methods, various databases available for 2D and 3D attacks, key obstacles, evolutions, and recent developments in face liveness detection and prospects. To the author's knowledge, this work gives valuable insight to researchers interested in using face anti-spoofing methods.

Thepade et al. [25] reviewed face anti-spoofing techniques comprehensively. Here, the authors discussed the texture, motion, multi-fusion-based face anti-spoofing methods, and available 2D attack databases. It also describes various face anti-spoofing techniques, including CNN, texture feature descriptors, and motion-based techniques. However, additional study is required to establish a reliable face biometric system.

Zhang et al. have done a review of the face anti-spoofing algorithm [26]. In this work, the authors show the progress of face spoofing techniques based on manual feature extraction methods based on image texture, image quality, computer interaction, and depth analysis. Then, deep learning automatically features extract, transfer learning, feature integration, and domain generalization. In 2019, a systematic literature review on insights into face liveness detection by Raheem et al. [27]. It focuses mainly on liveness indicators as a hint that helps devise a suitable solution for face spoofing problems. The paper [28] gives a comprehensive study of the state-of-the-art methods for PAD and an overview of respective labs working in this domain. Challenges and competitions in this domain are discussed in detail.

However, this paper considers a research study from 2011 to 2017. In 2021, another competition for face liveness detection (LivDet-Face2021) was conducted through Biometric Evaluation and Testing (BEAT) platform. Competition has opened several challenges to be solved by researchers [29]. In the paper, a review of the face presentation attack competition is conducted. Detail study of the various competition's opened in this domain from 2019 to 2021 is discussed, along with future challenges.

However, more existing review papers are focused on only one aspect, such as deep learning-based unimodal and multi-modal approaches [30], sensor-based approaches [31], 3D mask presentation attack detection under thermal infrared conditions [32], presentation attack detection methods for smartphones [33], various feature extraction techniques, performance metrics for detection of morph attacks [34], deep learning–based face presentation attack detection, bibliometric review of domain adaptation–based face presentation attacks detection [35] There have been few researchers that have examined feature extraction approaches and datasets available for face liveness identification.

No existing systematic review focuses on unseen presentation attack detection challenges and problems. The current systematic literature review focuses solely on a single topic, such as deep learning-based techniques, and lacks a thorough evaluation based on publicly accessible datasets. A thorough examination of the methods employed for effective and dependable face anti-spoofing systems is also lacking in the literature. Prior research relevant to this study is listed in Table 2.

**Table 2.** Prior research related to FLD.

| Ref. | Objectives and Topics | Observation and Limitations | Type |
|---|---|---|---|
| [28] 2017 | It includes state-of-the-art methods for face presentation attack detection and respective labs in the domain. It also describes challenges and competitions in the same domain. | Not following the PRISMA approach, the focus is on challenges and competitions from 2011 to 2017. | Review |
| [27] 2019 | It discusses a systematic review using the PRISMA approach. It focuses on liveness indications, particularly as a guide for determining the best solution for various spoofing issues. | In a review of research articles published between 2014–2017, the number of research articles studied is only 65, and a detailed analysis of available databases was explored. The focus is only on liveness indicator clues & lack of new trends in the research area since 2017. | Systematic Literature Review |
| [24] 2020 | It discusses the typology of presentation attacks and detection methods in various databases available for 2D and 3D attacks. Challenges, evolutions, and current trends face PAD and provide new perspectives on future research. | Not followed PRISMA approach, more focus on RGB-based methods, sensor-based PAD methods not explored in detail; more advanced research directions need to explore | Review |
| [25] 2020 | It discusses the texture, motion, multi-fusion-based face anti-spoofing methods, and available 2D attack databases. It also describes various face anti-spoofing techniques, including CNN, texture feature descriptors, and motion-based techniques. | Not followed PRISMA approach, for discussion, only last four years 2015–2019, The focus is only on deep learning-based solutions. Databases not extensively reviewed. Future directions are not discussed. | Review |
| [26] 2020 | It includes explicit feature extraction approaches based on image texture, image quality, computer interaction, depth analysis, deep learning feature extraction, transfer learning, feature integration, and domain generalization. | Few research articles were used in the study, lack of discussion of available databases for PAD, and very few future directions were explored. | Review |
| [36] 2021 | It discusses the international competitions conducted on unimodal and multi-model face presentation attack detection. | It includes the latest five competitions from 2019 to 2021, Not following the PRISMA approach. | Review |
| [30] 2021 | It includes advanced deep learning and multi-modal fusion-based methods for FPAD; an in-depth technical review is conducted, including recent deep learning approaches, datasets, and evaluation metrics. | Not following the PRISMA approach, it focuses on in-depth deep learning and a multi-modal approach, including research articles up to 2021. | Review |
| [31] 2021 | It includes deep learning methods and datasets used for the face anti-spoofing problem. It also discusses techniques for sensor-based approaches. | The PRISMA approach needs to be followed; more focus is given to deep learning methods, and advanced research directions need to be explored. | Review |

### *1.4. Motivation*

Our SLR comprehensively presents the most recent advancements related to face liveness detection by undertaking thorough surveys on machine learning-based and deep learning-based techniques and using publicly available datasets and evaluation metrics. This systematic review aims to critically examine existing research articles and their outcomes in the formulated research issue.

This research paper presented a systematic literature review (SLR) that, to the author's knowledge, is one of the foremost to cover the face liveness detection methods based on the AI approach for robust face recognition.

### 1.5. Research Goals

This study aims to compare the current biometric face liveness detection methods and to review the results of the most recent investigations. As a result, research questions are presented to analyze face liveness detection comprehensively. The research questions were developed, as shown in Table 3, to enhance the comprehensiveness of this systematic literature review study.

**Table 3.** Research Goals.

| Number | Research Questions | Motivations | Answered in Section |
|---|---|---|---|
| RQ1 | What is the distribution of published papers related to face liveness detection methods by year, publication, and publication type? | It aids in determining when, where, and who conducted the research studies. | Section 3, Section 3.1 |
| RQ2 | What are the various attacks against a facial recognition system? | It aids in exploring the different types of attacks performed on face recognition systems. | Section 3, Section 3.2 |
| RQ3 | What are the different datasets available for different types of presentation attacks? | It assists in locating a dataset with appropriate training and testing data for good research outcomes. | Section 3, Section 3.3 |
| RQ4 | What are the main methods related to artificial intelligence for face presentation attack detection? And what are the evaluation metrics used in Face liveness detection? | It aids in identifying appropriate artificial intelligence approaches for today's facial biometric applications. It helps to select the appropriate evaluation metrics for performance measures. | Section 4, Section 5 |
| RQ5 | What are the main challenges and problems faced by existing face anti-spoofing techniques? | It aids in exploring the fundamental issues that occur when studying face presentation attacks and the benefits and limitations of current solutions. | Section 6, Section 6.1, Section 6.2, Section 7 |
| RQ6 | What are future directions for a robust and reliable face liveness detection system? | It aids in finding important research avenues that have yet to explore | Section 7 |

### 1.6. Contributions of the Study

The contributions of our systematic literature review are as follows:

- An exhaustive survey of studies identified using the PRISMA Approach for face liveness detection using AI approaches, including Machine Learning and Deep Learning.
- A thorough examination of the quantity and consistency of standard datasets is carefully investigated.
- Feature extraction and Classification methods, Challenges, and issues in face liveness detection are discussed.
- Various evaluation metrics used in face liveness detection are discussed.
- Future research directions and open perspectives are conceptualized to assist researchers in selecting the best solution for robust face liveness detection in face biometric authentication systems.

### 1.7. Limitations of the Study

This SLR has some obvious risks to its logic, regardless of whether or not the appropriate keywords were detected or relevant search engines were chosen. In this regard, a list of distinct publications demonstrates that the search scope is acceptable since no other papers were discovered to meet the specified inclusion criteria. Although it is expected, our SLR may have missed some relevant research due to the limitations of the scientific dataset, specific keywords employed in the search, and review duration. From 2010 through 2022,

the author chooses only 95 studies. Authors were confident in the manual screening of studies obtained from "library services such as SCOPUS and WoS (Web of Science)."

The remaining sections of the paper are structured as follows: Section 2 discusses the proposed methodology. The findings and solutions to the submitted study questions are presented in Section 3. Section 4 examines the methods covered in a previous section, followed by Section 5, in which evaluation metrics are discussed. Sections 6 and 7 portray the challenges and future directions for face liveness detection. Section 8 is on discussion followed by conclusions. The outline of this SLR is represented in Figure 2.

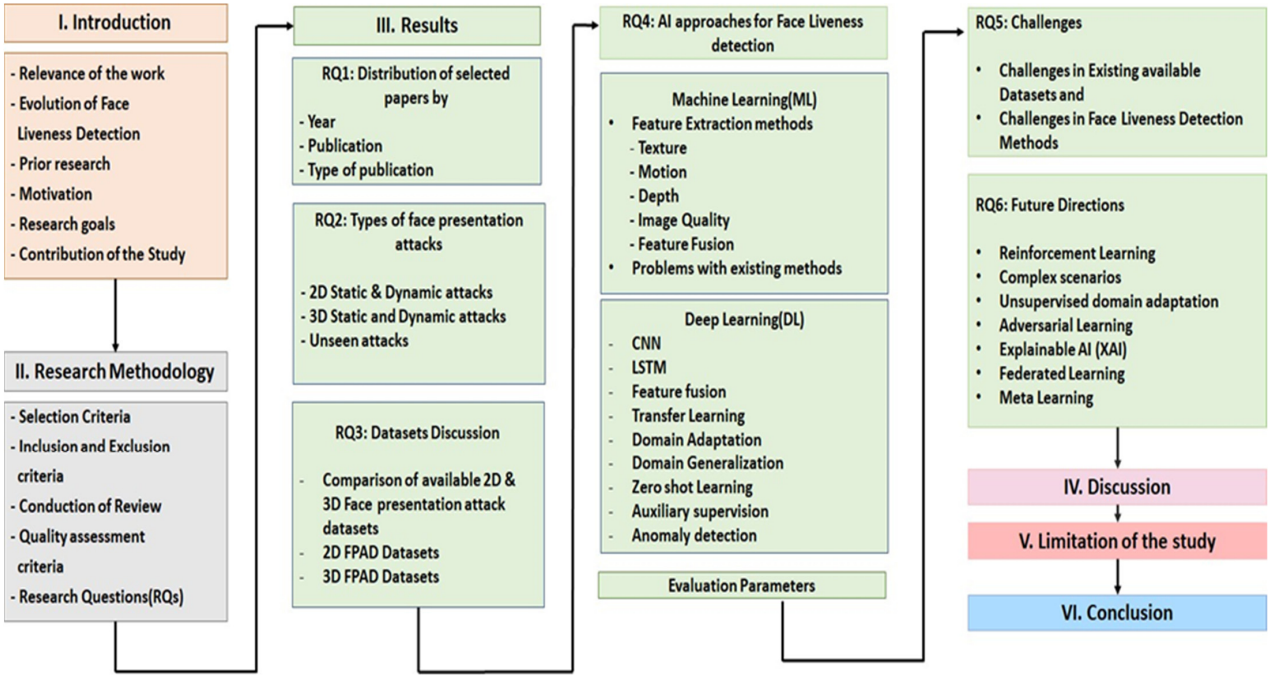


**Figure 2.** Outline of SLR.

## 2. Research Methodology

A systematic review was carried out using the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) process. A set of guidelines for conducting systematic reviews and other data-driven meta-analyses are given in PRISMA Approach [37]. The conduct of a systematic review three steps protocol is used in this paper: the formulation of research questions, the search databases, and the criteria for inclusion and exclusion of research articles—the details of these steps for research analysis are detailed in the following pages [38]. This systematic review is organized to cover the study's breadth under consideration by categorizing and evaluating existing publications. The first step is to define the research questions so that the coverage rate of current works is accurately described. There should be some perspectives that can help researchers generate new ideas by analyzing similar results. Table 3 lists the research questions used in SR Research question 1 aims to review the published work. The purpose of research question 2 is to list all possible attacks on face presentation. The detailing of the available datasets explored in FPAD is addressed with research question 3. A few prominent FPAD methods are to be studied in research question 4. The limitations and challenges of existing prominent methods have to be listed in research question 5. Future work and progress directions are expected to be chalked out in research question 6. The first step in conducting SR is to identify information sources.

Related manuscripts were found using the most popular Scopus and Web of Science. The next step is to develop procedures for reviewing the technical and scientific articles that these searches produced to identify relevant papers. The proposed approach is divided into two phases. The first phase uses Boolean operators AND/OR to identify search terms

from research questions and prepare a list of keywords. The second phase uses Boolean operators AND/OR to select queries to search for and collect all relevant data. Table 4 gives the list of fundamental, Primary & Secondary Keywords. Table 5 shows the search queries used in this article. In Table 5, # indicates the number of the initial result.

**Table 4.** List of primary and secondary keywords used.

| **Fundamental Keyword** | **"Face Anti-Spoofing"** |
|---|---|
| "Face Anti-spoofing" | "Face Liveness detection," "Face Presentation Attacks," "Artificial Intelligence," and "Domain Adaptation." |
| Secondary Keywords | "Machine Learning," "Deep Learning," "Domain Generalization," Reinforcement Learning, "Face Biometric spoofing." |

**Table 5.** Search queries.

| **Database** | **Query** | **# Initial Result** |
|---|---|---|
| Scopus | ((machine learning) OR (Deep Learning) (Artificial Intelligence) OR (Domain Adaptation) OR (Domain Generalization) OR (Reinforcement Learning)) AND ((Face Anti Spoofing) OR (Face Presentation Attacks) OR (Face Liveness Detection) OR (Face Biometric Spoofing)) | 283 |
| Web of Science (WoS) | | 188 |

### 2.1. Inclusion and Exclusion Criteria

As given in Table 6, the authors established a set of inclusion criteria for research paper selection and rejection exclusion criteria for selecting appropriate research studies for systematic review. In the screening procedure, three steps of inclusion criteria are established as follows:

(i) Abstract-based screening: Disqualify irrelevant research papers based on knowledge and keywords in research abstracts. Abstracts of research papers that met at least 40% of the inclusion criteria were considered for the following steps.
(ii) Full-text screening: The authors eliminated research papers that did not address or contribute to the search query in Table 5, i.e., abstracts that only represented minor aspects of the search query.
(iii) Quality-analysis step: The remaining research papers were subjected to a quality assessment, and those that did not meet any of the following requirements were eliminated:
(iv) C1: Findings and outcomes must include in research articles.
(v) C2: The findings of research publications are supported by empirical evidence.
(vi) C3: The research goals and findings must be well presented.
(vii) C4: Appropriate and sufficient references must use in research papers.

### 2.2. Conduction of SR

The authors utilized the following steps to choose appropriate papers for this research: As represented in the PRISMA flow diagram, the measurements of identification, screening, eligibility, and inclusion. Figure 3 depicts a PRISMA (Preferred Reporting Items for Systematic Review and Meta-Analysis) flowchart diagram showing the identification and records selection process of studies for the systematic review [37]. In Figure 3, # is used to indicate the process of screening is followed. Scopus and Web of Science (WoS) are well-known and standard research databases for searching the query. Two hundred eighty-three research articles from Scopus and 188 from WoS are retrieved using a search query. A total of 471 records are further gone through the first screening process of duplicate records removal. One hundred eighty-seven duplicate records are removed based on doi and title. Later, 284 documents were undergone through a second screening process using inclusion and exclusion criteria of the title and abstract.

**Table 6.** Summary of inclusion and exclusion criteria.

| **Inclusion Criteria** |
| --- |
| Articles should be original research articles instead of review/survey articles.<br>Research articles that were released between 2011 to 22.<br>Research papers/articles should include search keywords in the title, abstract, or full text of research articles.<br>Research articles that answer at least one research question.<br>The developed solution should aim at resolving issues with Face presentation attack detection. |
| **Exclusion Criteria** |
| Articles that are written in languages other than English<br>Duplicate research articles<br>Research articles with the unavailability of full text<br>Research articles that are not relevant to face liveness detection, face presentation attacks, face anti-spoofing |

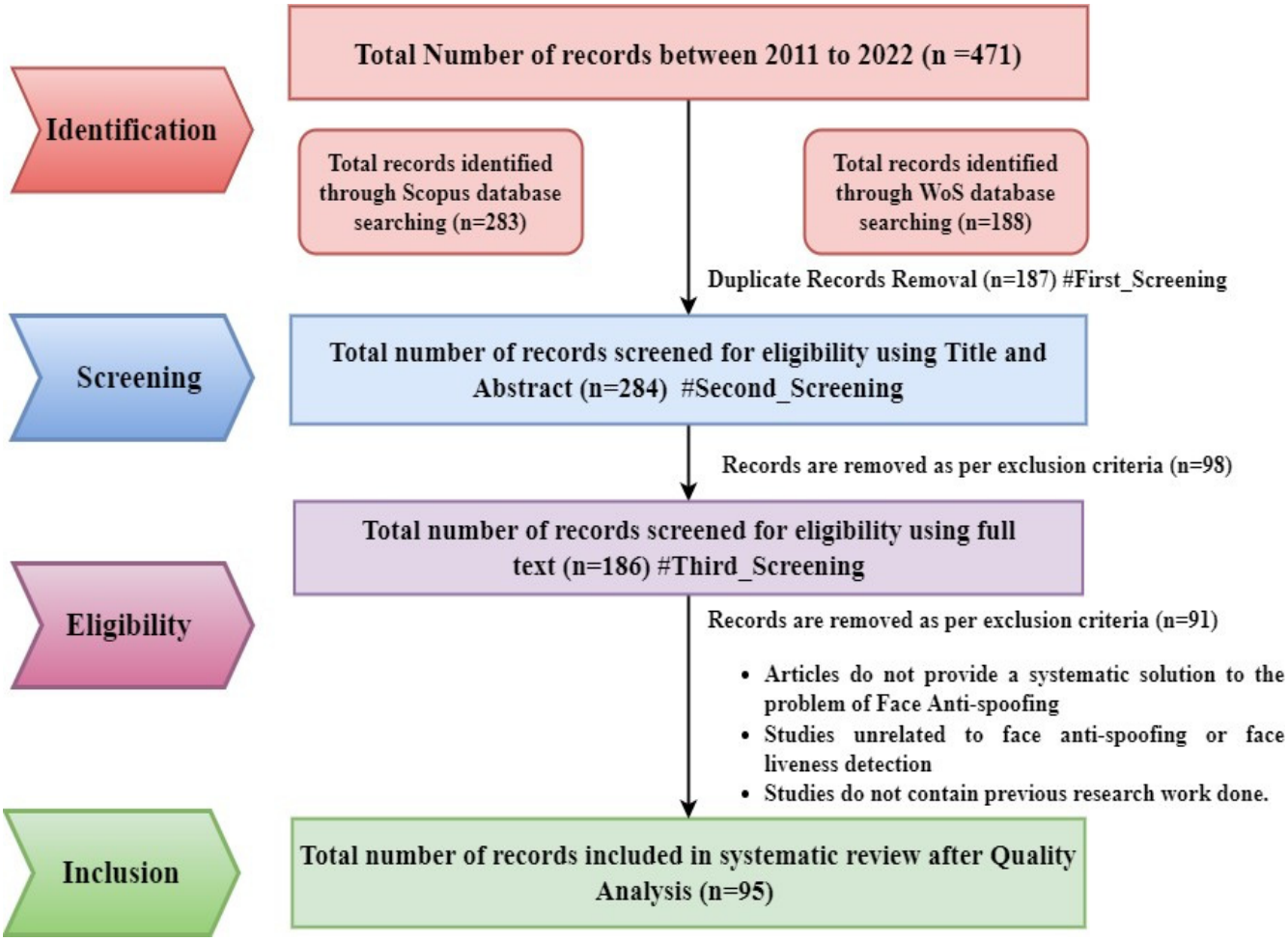


**Figure 3.** Flowchart identifies and selects studies for systematic review using the PRISMA approach [38].

Further, 98 documents still need to meet the inclusion criteria. Hence, 186 papers are forwarded to check for eligibility criteria. Based on inclusion and exclusion criteria for full text, the number of documents included for review is 95. Authors critically review these 95 research articles to find the research gaps in the existing literature and future directions in facing anti-spoofing.

## 3. Results

The findings of the systematic analysis are summarized in this section. It presents the responses to the mentioned research questions based on the findings of this review procedure, which follows an examination and analysis of 93 papers. Section 3.1 discusses research question 1 (RQ1) about the distribution of publication trends; Section 3.2 discusses research question 2 (RQ2) about various attacks on face liveness detection systems. Section 3.3 gives the comparative analysis of standard datasets used in literature that address research question 3 (RQ3) taken up for study.

### *3.1. RQ1 Distribution of Publication Trends Related to Face Liveness Detection*

**RQ1: What is the distribution of published papers related to face liveness detection techniques by year, publication, and publication type?**

Research articles used for the study were analyzed as par publication trends by year, reports by publisher, and publication type. There is a total of 95 research articles used for analysis purposes. Figure 4 shows the distribution of research articles by (a) publication year, (b) publication type, and (c) publication house. Research articles used for the study were analyzed as par publication trends by year, publisher, and publication type. There is a total of 95 research articles used for analysis purposes. In 2020 & 2021, the maximum number of research articles got published. Authors have considered research articles published up to June 2022, five papers. A maximum of 64 papers are published in IEEE and followed by Springer, 12 in the count. The research articles for this study were published as conference papers, articles, and proceeding papers. The contribution on Conference papers is 51%, Article papers are 47% & proceeding papers are 2%. As per the analysis, this topic has significant strength in research.

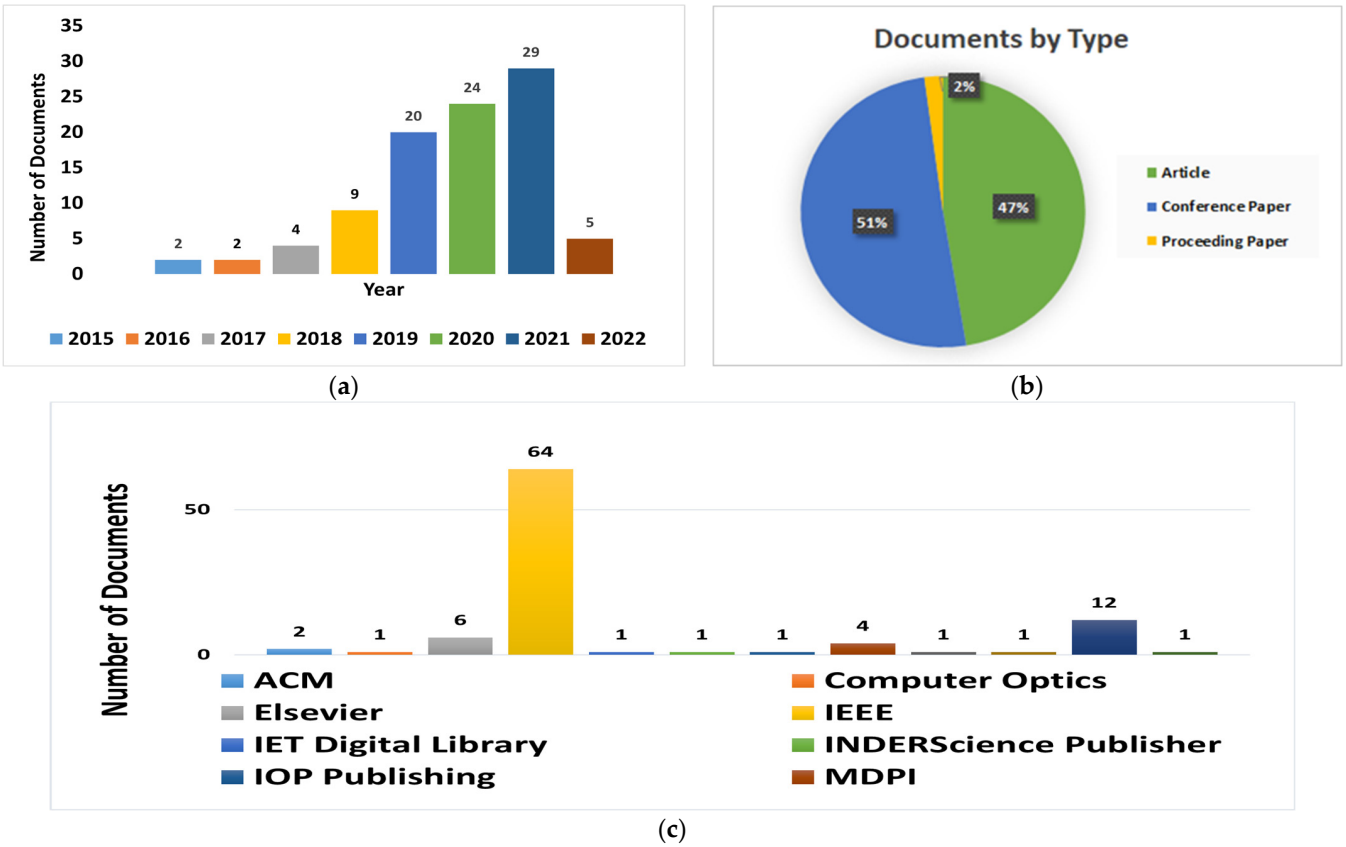


**Figure 4.** Analysis of selected research articles by (**a**) Publication Year, (**b**) Publication type, and (**c**) Publishing house.

### *3.2. RQ2 Face Spoofing Attacks*

With the advancement in technology, facial recognition systems have increased so widely. Along with that, the challenges or threats to facing recognition systems also come into the picture. Intruders use various spoofing techniques to fool the facial recognition-based authentication systems, known as Face Spoofing attacks and are also commonly termed Face presentation attacks. The different types of spoofing techniques or attacks are discussed in this section. Face Spoofing attacks are classified as shown in Figure 5.

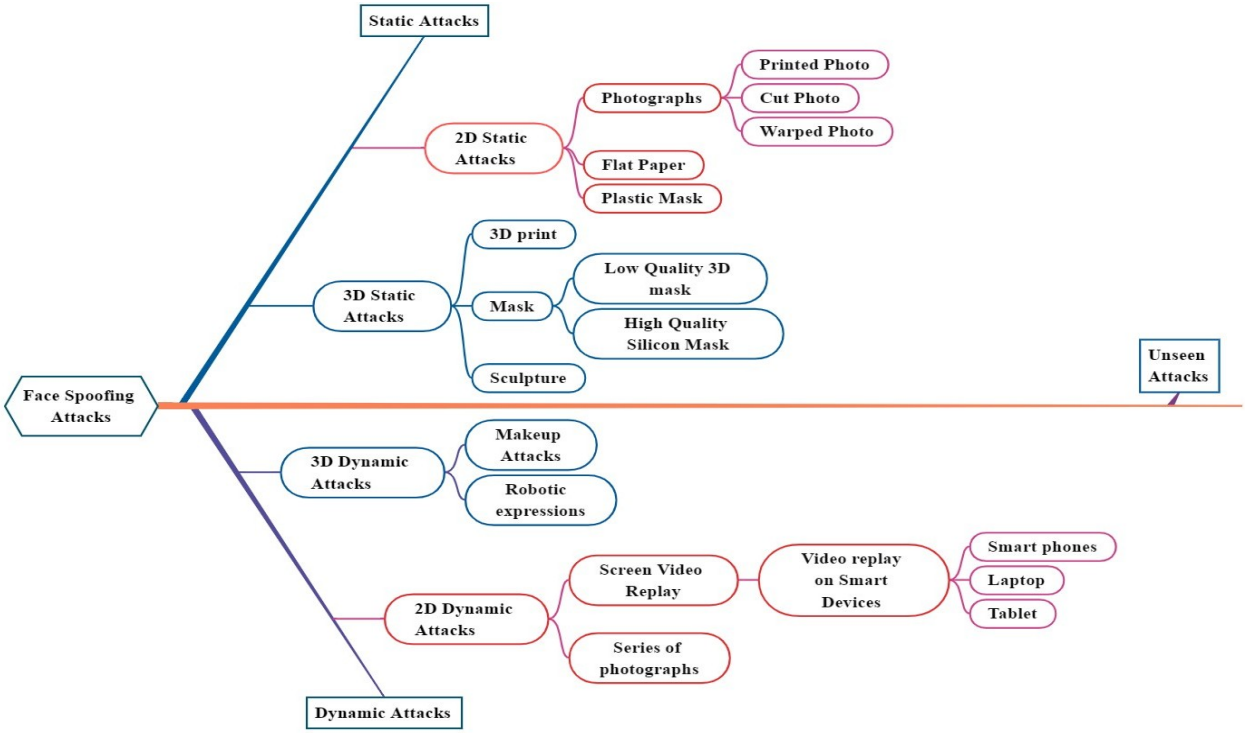


**Figure 5.** Categorization of Face Spoofing Attacks and Spoof Instruments.

The face spoofing attacks are broadly categorized as static attacks & dynamic attacks, whereas those are sub-classified by 2D or 3D static & dynamic attacks.

#### 3.2.1. 2D Static & Dynamic Attacks

2D Static Spoofing attacks are when intruders employ pictures, flattened papers, and masks for authentication. Images taken on paper are kept in front of the face recognition system by intruders to get access to the systems. A paper should be of good quality and in the A3 or A4 size. As seen in Figure 6a, printed picture attacks are one type of printed photo attack. It is the most common type of attack as it is easy to perform due to the large availability of individual pictures on social media. Another approach to spoof images is to cut a printed photo on the eyes or lips region to add some liveliness to the photo kept in front of the camera; this is known as a cut photo attack, as shown in Figure 6b. As face recognition-based systems get prone to attacks, intruders also come with different attacks. Another method for creating spoof photographs is to hold a genuine user's photo in front of the camera in a tilted position, either horizontally or vertically, to give the image depth. As demonstrated in Figure 6e, this method is known as a wrapped photo attack.

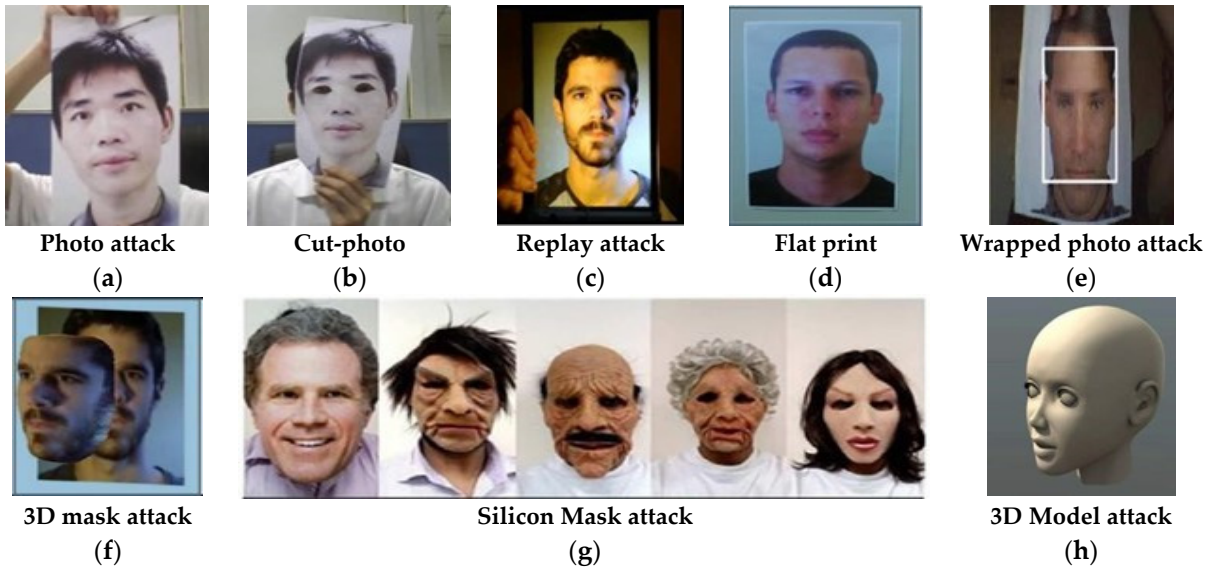


**Figure 6.** Sample Face spoofing attacks (**a**) Photo attack sample from OULU-NPU dataset [39] (**b**) Photo cut attack OULU-NPU attack [39] (**c**) Replay Attack Sample [40] (**d**) Flat Printed photo attack (**e**) Wrapped photo attack (**f**) 3D Mask generated using Face Construction using front-side faces (**g**) Sample 3D Latex mask from MLFP DB [41], (**h**) 3D model attack [42].

The matte paper and printed masks, plastic masks, are used as attacking instruments. 2D static attacks are quick and straightforward to execute in actual circumstances, necessitating sophisticated facial recognition algorithms.

Furthermore, a high-definition photo on a smartphone screen, a series of high-definition images, and a video of a genuine person on the screen of smart and portable devices shown in front of the camera of face authentication systems are other approaches to spoofing attacks. These attacks are 2D dynamic attacks. Video replay attacks are superior to 2D static photo attacks because they incorporate unique features such as eye movements, lip motions, and shifts of facial emotions to simulate liveness. Replay attacks are often harder to spot than photograph spoofs since they imitate the texture and contour of the face and its dynamics, such as eye movements, lips, and facial expressions.

Facial recognition systems vulnerable to 2D static picture attacks would perform significantly worse against 2D dynamic video attacks. Being robust against photo attacks can mean something other than being similarly strong against video attacks. As a result, appropriate measures should be designed and implemented for robust face recognition systems.

#### 3.2.2. 3D Static & Dynamic Attacks

This type of attack provides a 3D mask of the person's face. The attacker creates a three-dimensional reconstruction of the victim's face and shows it to the camera/sensor. Mask attacks involve more significant expertise than 2D static and dynamic attacks and access to additional facts to generate an accurate mask of a legitimate user. 3D static attacks employ a 3D mask as an instrument of 2D images adhered to a flexible structure such as a shirt or plastic bag. Such attacks fool low-level 3D face recognition systems. Different Sculptures are also used as attacking instruments in 3D static attacks. Two or more photos of the actual user's face, such as one frontal shot and one profile shot, can be used to create 3D models. The attacker may be able to extrapolate a 3D reconstruction of the real face using these images.

Another type of 3D attack is a makeup presentation (M- PA) attack. For impersonation, the attacker may use heavy makeup to mimic the facial look of a target subject [37]. It was discovered that high-quality makeup attacks that resemble the facial texture and form of an impersonated target subject might represent a severe threat to the security of face

recognition systems. Silicon can make high-quality 3D masks; this is another approach to 3D static attacks. Figure 6f–h shows some sample 3D mask attacks. A more advanced method is taking a direct 3D capture of a real user's face. This approach has more difficulty because 3D acquisition can only be done with specialized equipment and is impossible without the end's involvement. 3D dynamic attacks include using sophisticated robotics to reproduce expressions and complete makeup as a tool for making 3D reconstructions of real faces. However, Due to the spoofs' high realism, this attack may be more likely to succeed [39]. 3D masks present additional hurdles to the FR system; the Multi-Modal Dynamics Fusion Network (MM-DFN) technique is being investigated [42]. It gets more challenging to create effective countermeasures as the entire face structure is copied. 3D mask attacks are predicted to become increasingly common in future years as 3D acquisition sensors become more ubiquitous.

### *3.3. RQ3 Standard Benchmark Datasets Used for Face Liveness Detection*

**RQ 3: What are the different datasets available for different types of presentation attacks?** Data is the foundation of any artificial intelligence model. Obtaining particular, unbiased data from the right source would help build a more accurate and dependable model. This section discusses the most widely used publicly accessible datasets for detecting face presentation attacks. Table 7 gives an overview of existing 2D & 3D face presentation attack datasets used in the literature. In this table # sign is used to indicate the number of samples or subjects.

**Table 7.** 2D & 3D attack Datasets that are publicly available and used in the study.

| Dataset | Year | # Subjects | # Samples (Real/Fake) | Resolution | Type of Attack & Mode (Static or Dynamic) (2D or 3D) | Created by | Used in Literature |
|---|---|---|---|---|---|---|---|
| NUAA [43] | 2008 | 15 | 5105/ 7509 | 640 × 840 | Photo Attack (2D static) | Nanjing University of Aeronautics and Astronautics. | [44–52] |
| Replay-Attack [40] | 2011–2012 | 50 | 300/ 1000 | 320 × 240 | Photo Attack (2D Static)/Video Replay Attack (2D dynamic) | IDIAP Research Institute | [53–64] |
| CASIA-FASD [56] | 2012 | 50 | 150/450 | 640 × 480 1280 × 720 1920 × 1050 | Photo Attack (cut, printed, wrapped)-2D Static/Video Replay Attack (Dynamic) | IDIAP Research Institute | [64–68] |
| Morpho | 2013 | 20 | 406 | - | 2D + 3D Mask attacks | MORPHO | [69] |
| 3DMAD [42] | 2013 | 17 | 255 (170/ 85) | 640 × 480 | 3D mask paper attack | Idiap Research Institute | [70–73] |
| MSU-MFSD [74] | 2015 | 35 | 110/ 330 | 1920 × 1080 | Printed Photo attacks (2D Static), 2 × Video attacks (Dynamic) | Michigan State University | [60,75–81] |
| MSU-USSA [82] | 2016 | 1140 | 1140/9120 v | 1920 × 1080 | Printed photos, photos display (Static), 3× video replays (Dynamic) | Michigan State University | [57,83] |
| 3DFS-DB [83] | 2016 | 26 | 520 v | 640 × 480 | 3D mask attacks | Institute for the Protection and Security of the Citizen | [76,81] |
| BRSU [84] | 2016 | 137 | 141 | - | Multispectral SWIR 2D/3D attacks | Bonn-Rhein-Sieg University of Applied Sciences | [85,86] |

**Table 7.** *Cont.*

| Dataset | Year | # Subjects | # Samples (Real/Fake) | Resolution | Type of Attack & Mode (Static or Dynamic) (2D or 3D) | Created by | Used in Literature |
|---|---|---|---|---|---|---|---|
| HKBU-MAR [87] | 2016 | 12 | 1008 v (504/504) | 1280 × 720, 800 × 600 | 3D Mask attacks | University of OULU | [88,89] |
| OULU-NPU [39] | 2017 | 55 | 990/3960 v | Different Resolutions | Photo Attack/Video Replay Attack (2D) | OULU University | [90] |
| SMAD [91] | 2017 | Online | 130 (65/65)v | - | Silicon Mask attack | IIT Jodhpur | [73,92,93] |
| MLFP [41] | 2017 | 10 | 1350 (150/1200) | Different resolution | 3D late× Masks attacks, 2D Paper print Mask Attack | IIIT Delhi | [68] |
| ERPA [94] | 2017 | 5 | 86 | - | Silicone masks | Idiap Research Institute | [69] |
| SiW [95] | 2018 | 165 | 1320/3300 v | 1920 × 1080 | Printed Paper (High/Low Quality) (2D) | Michigan State University | [71] |
| ROSE-YOUTU [73] | 2018 | 20 | 3350 | 640 × 480 1280 × 720 | printed paper attack, video replay attack, paper masking attack, cropped mask, full mask, and upper mask | Tencent Corporation and the NTU ROSE Lab | [74] |
| CASIA-SURF [96] | 2019 | 1000 | 3000/18,000 v | Real Sense RGB Cam 1280 × 720 | Flat-cut/Wrapped-cut Photos (Eyes, Nose, Mouth) (2DStatic) | Institute of Automation, Chinese Academy of Sciences (CASIA) | [76,77,80] |
| WMCA [78] | 2019 | 72 | 1679(347/1332) | 1920 × 1080 1260 × 720 320 × 240 | 2D, 3D attacks 2D prints, video and photo replays, mannequin heads, paper, silicone, and rigid masks | Idiap Research Institute | [79,97] |
| CASIA-SURF CeFA [98] | 2020 | 1607 (3 Different Ethnic-ity) | 1800/5400 v | 299 × 299 | Print attack, Replay Attack, 3D print, IR, Infrared, 2D & 3D attack Subsets | Institute of Automation, Chinese Academy of Sciences (CASIA) | [82] |
| CASIA-SURF 3DMASK [99] | 2020 | 48 | 1152 (288/864) v | 30 fps and 1080 p resolution | 3Dmask attacks | Institute of Automation, Chinese Academy of Sciences (CASIA) | [83] |
| HiFi Mask [100] | 2021 | 75 | 54,600 v | - | 3D Mask attacks | Institute of Automation, Chinese Academy of Sciences (CASIA) | [84] |
| VFPAD [101] | 2022 | 24 male and 16 female with different ethnicity's | 5836 v (4046/1790) | - | photo prints, replay attack, rigid 3D, silicon 3D mask attacks | Idiap Research Institute | [101] |

# indicates the number of samples or subjects.

## 4. RQ4 Artificial Intelligence for Face Liveness Detection

The various face liveness detection AI-based techniques discussed in the literature are categorized based on the ML approach [102–105] & Deep Learning Approach [106–109]. Studies reveal that artificial intelligence-based methods for detecting face-presentation attacks are frequent. The first Section 4.1, discusses Feature extraction and Machine Learning approaches, followed by Section 4.2 on deep learning in face liveness detection.

### *4.1. Machine Learning and Feature Extraction Methods for FLD*

The numerous feature extraction methods and classifiers categorize face liveness detection strategies. Texture, depth, motion, image quality, and multi-fusion techniques were employed as features. In contrast, findings from selected literature use various machine learning classifiers such as Support vector machines (SVM), Random Forest, naïve Bayes, Decision trees, and J48 [110]. Figure 7 shows the overview of Face presentation attack detection using the ML approach.

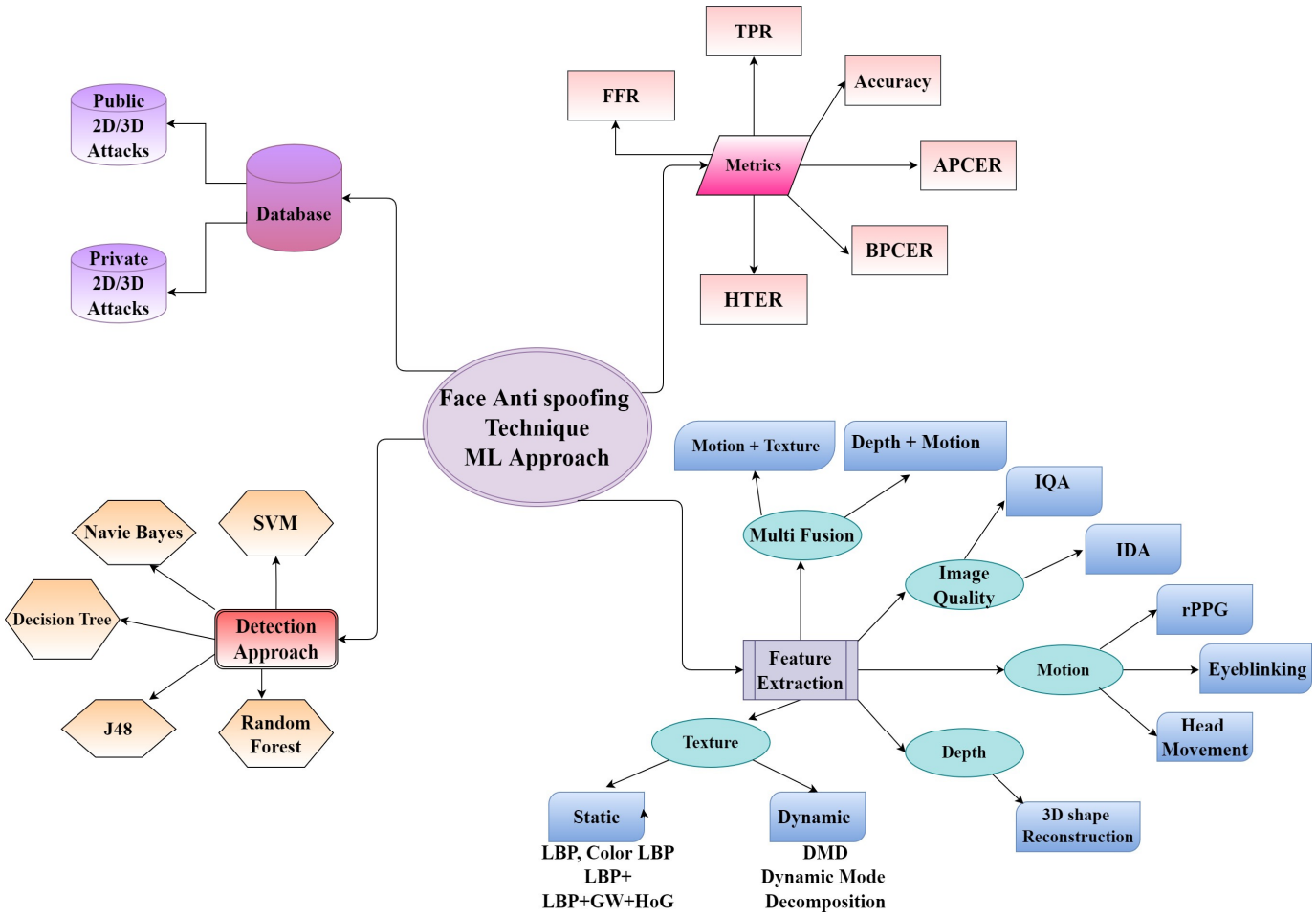


**Figure 7.** Face anti-spoofing techniques using a machine learning approach.

#### 4.1.1. Texture-Based Feature Extraction

Texture features are one of the most well-explored strategies for identifying features in literature. Photos, replays, and 3D masks were detected with this tool. In general, static and dynamic aspects are separated—static features extract features from a single image, whereas dynamic features work on video frames. Static Feature extraction methods help detect static face presentation attacks such as printed photos, cut photos, wrapped photos, printed masks, etc. In contrast, Dynamic feature extraction methods address dynamic face presentation attacks such as video replay attacks, 3D Mask occlusion attacks, etc. For

static texture feature extractions in the literature, various methods are used, such as Local Binary patterns (LBP) [40], DoG [111], Gabor wavelets, and HoG [112], whereas LBP is explored more in the literature. Each pixel is labeled by comparing its neighbors and concatenating it into a binary number using LBP texture coding. In addition to the coding strategy, other parameters include the number of neighbors and neighborhood radius. A histogram of the final calculated labels describes the texture, done for the whole image or selected image paths. The author [113] developed a color texture analysis-based face anti-spoofing solution. They created the final descriptor by connecting a single image channel LBP histogram. This method considers the three-color spaces RgB, YCbCr, and HSV to determine the most discriminating. Experiments demonstrate that the process based on color texture outperforms the grey surface in identifying diverse attacks. The same technique tailored for video attacks is used to investigate replay attack detection.

However, these approaches have the advantages of being simple to implement and requiring no user engagement. On the other hand, these approaches required feature vectors and performed poorly with low- resolution photos.

#### 4.1.2. Motion-Based Feature Extraction

Motion cue-based algorithms use motion cues in video data to discriminate between genuine (live) faces and static photo assaults. Any dynamic physiological indication of life, such as eye blinking, lip movement, lip-reading [114], changes in facial expression, and pulse rhythm, is used as liveness cues. These approaches can identify static picture attacks but not video replay using motion/liveness signals or 3D mask attacks. According to [115] research, lip language recognition employs to identify changes in facial expressions, combined with voice recognition, to determine whether the user reads the randomly selected statements under specifications. Singh et al.'s blinking and lip movements were used to make real-time judgments. The HSV (hue, saturation, value) computes to determine whether the eyes and the mouth are open. They responded to phrase prompts generated at random by the algorithm and completed the required action to prove that it was a genuine person. Ng et al. [116] developed to guide users through making random facial expressions. By measuring the SIFT flow energy of several image frames, users may judge if the mandated facial expressions are complete and genuine faces.

The human-computer interaction-based technique can successfully mitigate inter-class discrepancies in algorithm performance through correctly designed interaction actions. Therefore, it has a high recognition rate and many other applications. Real-world business issues such as public safety, medical treatment, and finance use it frequently. On the other hand, a face anti-spoofing detection approach that relies on user-computer interaction requires much calculation and time to determine whether the user has completed action from a multi-frame image.

Most deceiving faces cannot replicate critical aspects such as a heartbeat, blood flow, and micro-movements of involuntary facial muscles. When using the life information-based technique, the differences in these vital qualities are primarily used to distinguish between living and fake faces.

The most extensively used approach for monitoring the micro intensity variations in the face that correlate to blood pulse is Remote PhotoPlethysmoGraphy (rPPG cue-based techniques). It can detect photo and 3D mask attacks because these PAIs lack the periodic intensity shifts characteristic of face skin.

However, ambient light and the item's movements to be tested can readily influence the rPPG signal. Face anti-spoofing often requires cascading other traits and classifiers because the method is generally resilient.

#### 4.1.3. Depth-Based Feature Extraction

There are different depths of information in various facial areas, such as the forehead, eyes, and nose tip. The photo- or video faces are two-dimensional, with the same depth of information at multiple locations. The depth information is used to detect fakes even

though there are folded images. Depth information anti-spoofing methods typically need the usage of additional hardware. As a result of the difference in substance, the reflection properties of the fooled face differ from those of a living face's skin, eyes, lips, and brows. When viewed in visible light, the deceived face appears to be similar to a real face, but it seems very different when viewed in infrared light. As near-infrared photos and videos show deceptive faces, this method is accurate, but well-made masks are less dissimilar from real faces. Steiner et al. [117] used short-wave infrared to distinguish between facial skin and mask attacks. A second use of the depth image captured by the depth camera is for anti-spoofing detection. A convolutional neural network and depth information from Kinect was used by Wang et al. [118] to distinguish between real and fake faces, as shown in Figure 8.

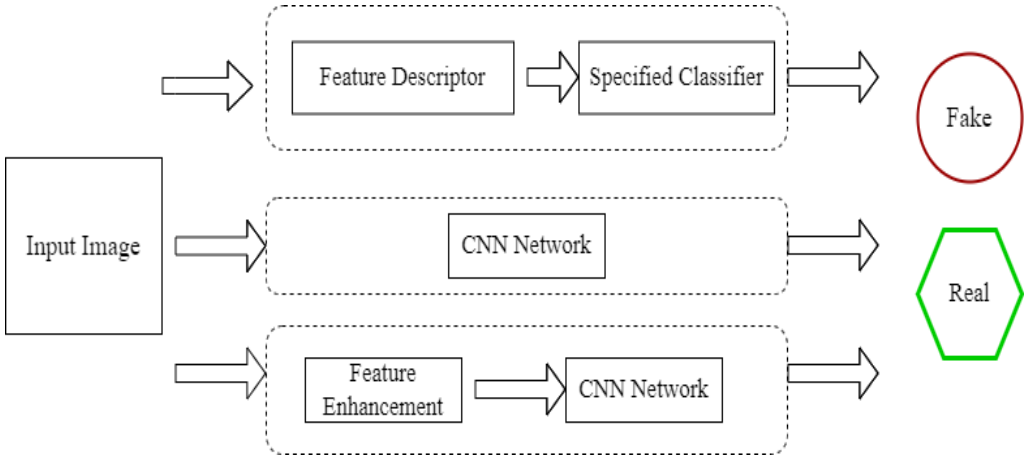


**Figure 8.** An illustration of CNN architecture used for face liveness detection.

There are several advantages to using depth information to identify face spoofing. There is a significant difference between a video face and a photo's depth map; deprived of the excessive user interface, it has a good detection effect on photos and videos. A genuine expression, however, would have to invest in new technology, which would be pricey, and the latest hardware would also limit the number of users. In the depth map, the contours of the three-dimensional face can be seen, and there is a significant contrast between it and a photo face.

#### 4.1.4. Image Quality-Based Feature Extraction

Presenting a deceptive human face necessitates plastic, silica gel, photo paper, electrical equipment, printing paper, and other media with qualities that differ from a real face's facial features and skin materials. Variances in the reflection quality of materials, such as picture paper and mobile phone display screens, can induce. Both of which exhibit specular reflections but no living faces. The majority of picture quality after deception face secondary imaging differs from that of a living face, such as color distribution distortion and blurring of the prosthetic face image, even though the deception of the face manufacturing process is high. Image quality-based techniques use the variance among reflection and image distortion qualities to distinguish authentic and false faces.

The picture quality-based method has a low computational cost and a quick detection speed, making it ideal for online real-time detection. This approach, however, is open to attack when the image quality is excellent. A higher quality human face image and a false human face image should be used as inputs to obtain good enough image quality attributes. Table 8 gives the categorization of feature extraction for face liveness detection methods.

**Table 8.** Categorization of extraction methods for face liveness detection.

| Feature Extracted | Methodology Used | Attacks Identified |
| --- | --- | --- |
| Static Texture Based | Texture Feature extraction from Input Image Frequency Texture: 2D FFT Spatial Textures: DoG [111]<br>- Handcrafted Texture Feature, LBP [102], Color LBP [112], LBP + Gabor Wavelets, LBP + GW + HoG [112]<br>- CNN Based: AlexNet [118–120] Fine Tune VGG-Face [121], DPCNN, FaceDs [102], DeepPixBis [122] | Photo Attack, Video Replay Attack, 3D mask Attack of Low Quality |
| Dynamic Texture-Based | - Spatio-Temporal Texture [120]<br>- Dynamic Mode Decomposition (DMD) [86]<br>- CNN Based: LSTM-CNN [89], STASN [121] | |
| Non-Invasive Motion-based Feature Extraction methods | - Eye Blinking [58,86,116]<br>- Head Movement [94]<br>- FDD (Frequency Dynamic Distributor) [96]<br>- Optical Flow Lines(OFL) [122] | Static Photo Attacks<br>Photo & 3D mask attack, Low-quality Video Replay Attack |
| Invasive Motion-based Feature Extraction methods | - Lips Reading Recognition (OFL) [123] | |
| rPPG Motion-based Feature Extraction methods | - rPPG Frequency Spectrum [124]<br>- Local rPPG Correlation [125]<br>- Deep rPPG [125] | |
| 3D Shape-Based (Depth-based) | Reconstructing Sparse 3D Face [117] | Planner Photo Attack |
| Pseudo Depth Map | CNN Based, NAS Based [109], 3D cloud point network [126] | Video Replay Attack |

#### 4.1.5. Problems in Existing Techniques

For spoof detection, face recognition systems use a variety of algorithms to assess static and dynamic information. Previously, used hand-crafted features to detect presentation threats in feature-based approaches. Hand-crafted feature methods used techniques such as Local Binary Patterns (LBP), Speeded-Up Robust Features (SURF), Histogram of Oriented Gradient descriptors (HOG), and Difference of Gaussian (DoG). Texture analysis extensively employs hand-crafted feature approaches. Textural characteristics vary de- pending on the spoofing medium and devices. As a result, generalization is low for these approaches. Deep learning approaches emerged, allowing for effective feature learning in various applications. Furthermore, deep learning algorithms outperformed hand-crafted methods in terms of detection. Hence, current developments show a significant move toward deep learning-based techniques for detecting face presentation attacks.

### *4.2. Deep Learning in FLD*

Deep learning-based algorithms have been effectively applied to various disciplines, including lip-reading from video, speech augmentation and recognition, medical imaging applications, security, anomaly, and so on. Convolutional neural networks have significantly advanced computer vision applications, particularly biometrics. Thanks to deep learning and its inherent feature learning capabilities, the anti-spoofing difficulty solve in a novel way. Existing deep neural network-based approaches have excellent intra-dataset performance. Figure 9 depicts the deep learning approaches for face liveness detection. In this

section, a few deep learning approaches such as Convolutional Neural Networks (CNN), LSTM, Deep tree network (DTN), Autoencoders, Deep Neural Networks (DNN), Recurrent Neural Networks (RNN), Deep Belief Networks (DBN), and Generative Adversarial Networks (GAN) are discussed.

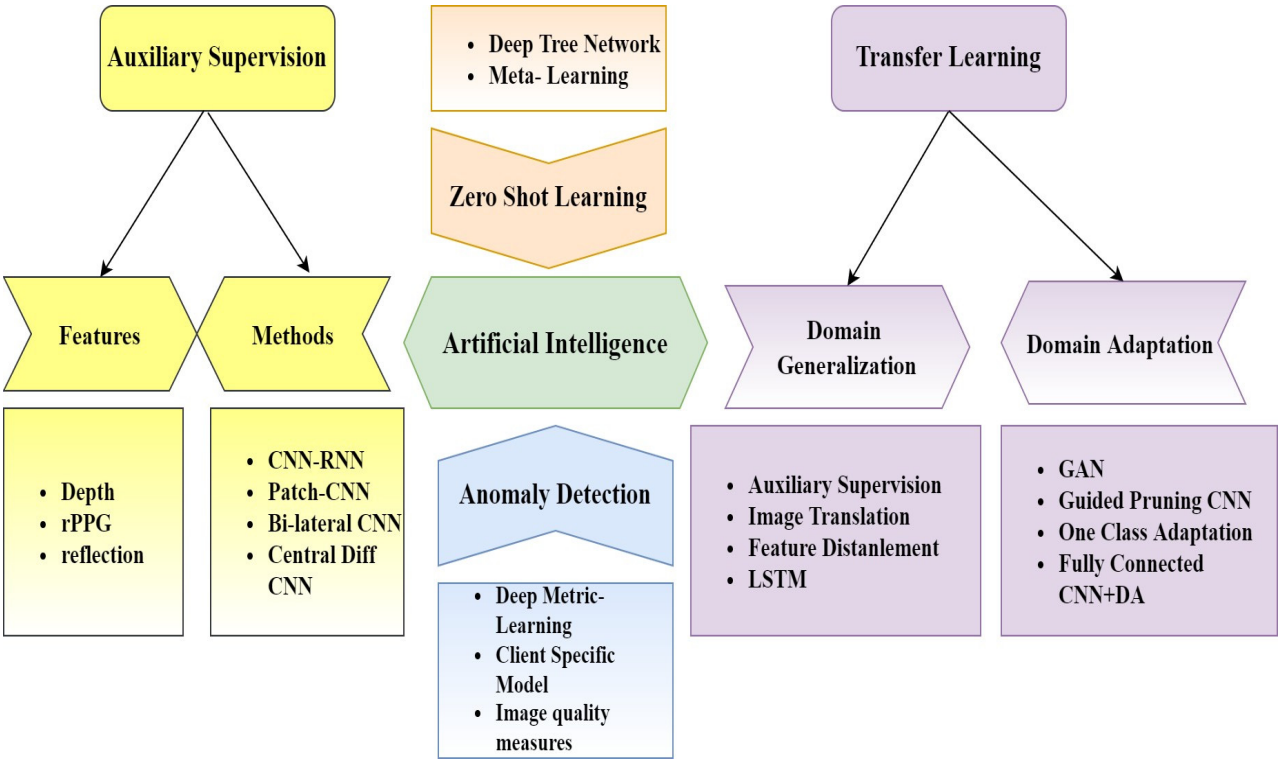


**Figure 9.** Deep learning approaches for Face liveness detection.

Deep learning-based techniques are used to learn texture properties automatically. Rather than directly creating the texture characteristics, researchers researching these methods focus on building a great neural network to learn optimal texture features [65]. In 2014, Yang et al. pioneered the road for deep learning in the arena of face anti-spoofing by introducing a Convolutional Neural Network (CNN) to extract features in face anti-spoofing.

Moreover, the features acquired from the CNN's many layers were concatenated into a single element and input into an SVM for face PAD. But this strategy is prone to overfitting because the dimension of the fused feature is much larger than the number of training samples. Principal component analysis (PCA) and so-called part features are used to minimize the feature dimension. In 2016, Patel et al. proposed CaffeNet, a face PAD end-to-end system based on one-path AlexNet. In place of the original 1000-way softmax, a two-way softmax was used as a binary classifier. CNN was pre-trained on ImageNet, and WebFace to provide an appropriate initialization and fine-tuned using existing face PAD datasets. To train a deep CNN for face PAD, Li et al. recommended utilizing the VGG-Face algorithm. An extensive dataset is used to prepare the CNN, then fine-tuned using a (much smaller) face spoofing database [127].

Depth + Texture Feature Fusion: The image depth information is crucial for determining the face's validity as the face in real life is three-dimensional, whereas the face attacked by photographs and screens is flat. The depth map differs from the real face, even if the face is deformed. A face depth map was initially used by Atoum et al. to distinguish between face spoofing. A two-channel CNN-based face anti-spoofing method was proposed in this study [96].

Spatial + Temporal Feature Fusion: Spatial characteristics of faces, such as texture and depth, are essential, but temporal factors are even more critical for anti-spoofing. Examining a human face from a time and space viewpoint can provide more helpful information and enhance classification performance.

### *4.3. Transfer Learning in Face Liveness Detection (FLD)*

Transfer learning is the most popular deep learning technique used in FPAD. A considerable amount of training data is often required to generate more distinct characteristics when using deep learning to detect face genuineness. However, there is insufficient data in the existing face anti-spoofing database, and most solutions use a neural network with only a few layers. A vast network classifier with good performance is challenging to train. Transfer learning helps avoid over-adapting to massive networks and saves a lot of computational resources when there is not enough data to train from the start [95].

Domain adaption (DA) and domain generalization (DG) used a transfer learning technique to improve generalization in FPAD. Domain adaptation is a strategy for transferring information from a source domain to a target domain. Adaptation is moving data from a source domain to a target domain using various methods.

#### 4.3.1. Domain Adaptation (DA) in FLD

In computer vision and machine learning, it is a frequent assumption that training and testing data come from the same distribution. However, many real-world scenarios (such as face recognition and spoof identification) require data from many distributions (facial appearance and pose, illumination conditions, camera devices, etc.). As a result, testing a pre-trained model with slightly different unseen data may have an over-fitting problem, resulting in a significant performance reduction. Domain adaptation is linked to transfer learning, which seeks to solve a learning issue in a target domain using training data from a source domain with a different distribution [98]. It has received much attention in recent computer vision tasks.

One of today's most pressing concerns is improving face PAD algorithms' generalization ability. Various strategies are explored, such as combining databases with a training model [128], NAS transfer learning approach [107,129] and one-class adaption [130]. Table 9 summarizes recent studies in face liveness detection.

**Table 9.** Few popular methodologies are used in Face Liveness Detection.

| Ref. and Year | Methodology | Domain Adaptation(DA)/Domain Generalization (DG) | Datasets Used | Performance Metrics and Model Performances | Intra-Database Testing | Cross-Database Testing |
|---|---|---|---|---|---|---|
| [58] 2015 | Person-Specific Domain Adaptation | DA | CASIA Dataset, Replay- Attack | Half Total Error Rate (HTER):1.40% (in case of Replay-attack dataset), 10.54% (in case of CASIA Dataset) | Y | N |
| [97] 2018 | Unsupervised Domain Adaptation framework | DA | Own Dataset-Rose-Youtu liveness database | Half Total Error Rate—27.70% | Y | Y |
| [131] 2018 | generalized deep feature representation for spatial and temporal information using 3D CNN | DG | Idiap Replay-Attack, CASIA Face Anti Spoofing, MSU mobile face spoofing database | Half Total error rate (HTER): 24.70% | Y | Y |
| [78] 2019 | Adversarial Domain Adaptation | DA | MSU-MFSD, Replay- Attack, CASIA FASD | Half Total Error Rate—20.30%, Equal Error Rate—3.20% | Y | Y |

**Table 9.** *Cont.*

| Ref. and Year | Methodology | Domain Adaptation(DA)/Domain Generalization (DG) | Datasets Used | Performance Metrics and Model Performances | Intra-Database Testing | Cross-Database Testing |
|---|---|---|---|---|---|---|
| [132] 2019 | Maximum Mean Discrepancy (MMD) to multi-layer network distribution adaptation | DA | Replay-Attack, CASIA FASD (CBSR) | Half Total Error Rate: 0.6% (Intra-tests), HTER 34.30% (Inter-tests), Equal Error Rate:0.30%, (Intra-tests) | Y | Y |
| [76] 2019 | a multi-adversarial deep domain generalization performed under a dual-force triplet-mining constraint. | DG | CASIA-MFSD, Idiap Replay-Attack, MSU-MFSD, and Oulu-NPU datasets | Half Total Error Rate (HTER): 27.98% and Area Under Curve (AUC): 80.02% | N | Y |
| [133] 2020 | (OCA-FAS) one-class adaptation face anti-spoofing | DA | OULU-NPU | Average classification error rate(ACER): 1.69% | N | Y |
| [134] 2020 | (FCN-DA-LSA) Fully Convolutional Network with Domain Adaptation and Lossless Size Adaptation | DA | CASIA-FASD, Replay-Attack dataset, and OULU-NPU dataset | Half Total Error Rate: 21.83% | N | Y |
| [135] 2020 | One class domain adaptation using domain-guided pruning of CNN | DA | OULU-NPU, Replay-Mobile, SWAN, WMCA, and IJB-C. | AUC, ROC, APCER | Y | Y |
| [136] 2020 | single-side domain generalization framework (SSDG) | DG | OULUNPU, CASIA- FASD, Idiap Replay-Attack, and MSU-MFSD | Half Total Error Rate (HTER):7.38% and Area Under Curve (AUC): 97.17% | Y | Y |
| [137] 2020 | Domain-agnostic feature learning | DG | Oulu-NPU, CASIA- MFSD, Idiap Replay-Attack, MSU-MFSD | Half Total Error Rate (HTER): 14.00% and ACER: 8.05% | N | Y |
| [138] 2020 | Total Pairwise Confusion (TPC)loss and Fast Domain Adaptation (FDA) | DG | CASIA-FASD, Replay-Attack, MSU-MFSD, Oulu-NPU, SiW | HTER:26.30% | Y | Y |
| [122] 2021 | (DR-UDA)Unsupervised adversarial domain adaptation with disentangled representation | DA | Idiap Replay-Attack, CASIA Face Anti Spoofing, MSU-MFSD, ROSEYoutu, and Oulu-NPU use the RGB modality of the CASIA-SURF | Half Total Error Rate (HTER): 28.70%, Equal Error Rate (EER): 3.20% | Y | Y |

**Table 9.** *Cont.*

| Ref. and Year | Methodology | Domain Adaptation(DA)/Domain Generalization (DG) | Datasets Used | Performance Metrics and Model Performances | Intra-Database Testing | Cross-Database Testing |
|---|---|---|---|---|---|---|
| [139] 2021 | (SSR-FCN) Self-Supervised Regional Fully Convolutional Network | DG | Spoof-in-the-Wild with Multiple Attacks (SiW- M), Oulu-NPU, CASIA-FASD & Replay-Attack | Average Classification error rate (ACER): 2.80%, Half Total Error Rate (HTER): 19.90% | N | Y |
| [53] 2021 | Camera Invariant Feature Learning for Generalized Face Anti-Spoofing | DG | CASIA-FASD, Replay-Attack Oulu-NPU, and MSU-MFSD | Equal Error Rate (EER): 0.89%, HTER: 17.60% for cross-dataset evaluation | Y | Y |
| [129] 2022 | A self-supervised approach using temporal sequence sampling | DG | CASIA-FASD, Replay-Attack, OULU-NPU, and MSU-MFSD | HTER: 5.90% (in a cross-dataset test for the Replay attack dataset) and 15.90% (in cross-dataset testing for CASIA-FASD), ACER: 0.10% (in an Intra-dataset test for OULU-NPU) | Y | Y |
| [140] 2022 | Domain Specific adaptation with CNN using Near Infrared | DA | in-Vehicle Face Presentation Attack Dataset | APCER—0.92%, BPCER—0.91%, ACER—0.91% | Y | Y |

#### 4.3.2. Domain Generalization (DG) in FLD

With the widespread use of deep learning in face anti-spoofing, many approaches have been presented. However, these methods are mainly confined to detecting known spoofing attempts, leaving unexpected spoofing assaults unnoticed. The following strategies were created to improve the generalization ability of detection systems under "invisible" attacks. Domain generalization is one of the strategies used by the biometric community to get generalizations in attack situations that are not yet known. There is a bias in existing face PAD approaches toward cues learned from training data. It is challenging to generalize against attacks that occur in various settings, devices, lighting situations, or materials. By considering both temporal and spatial information and limiting a cross-entropy loss and a generalization loss, the author [131] has aided in learning generalized feature representations. To increase the discriminability of the learned feature space, the author combined learning a generalized feature space with a dual-force triplet mining constraint [77]. Finding a compact and generalized feature space for fake faces is challenging due to the high distribution disparities among fake faces in different domains.

However, SSR-FCN is limited by the amount and quality of available training data, even though the suggested method is well-suited for generalizable face presentation attack detection. Cross-dataset generalization performance suffers when trained on a low-resolution dataset, such as Replay-Attack [129].

### *4.4. Zero-Shot Learning in Face Liveness Detection*

Face anti-spoofing prevents false faces from being recognized as actual users by face recognition systems. While sophisticated anti-spoofing solutions are developed, new types of spoof attacks are also being developed, posing a threat to all current systems. According to the author, detecting unknown spoof attacks is known as Zero-Shot Face Anti-spoofing (ZSFA). Liu. Y has presented a revolutionary Deep Tree Network (DTN) to combat the ZSFA. In an unsupervised manner, the tree is learned to segment the fake samples into

semantic sub-groups. When a data sample arrives, whether from a known or unknown attack, DTN sends it to the closest spoof cluster and makes a binary judgment.

### 4.5. Anomaly Detection in Face Liveness Detection

An anomaly detection approach was used to detect unseen attacks in recent research. The classification of one class preceded the discovery of anomalies. The types of attacks in practical applications are likely unknown, potentially occupying a large portion of the feature domain. As a result, one of the most significant potential issues in current anti-spoofing approaches is a failure to generalize on undiscovered sorts of attacks. First, the authors create novel assessment techniques for existing publicly available databases to highlight the generalization concerns of two-class anti-spoofing systems. Second, to combine the data collection efforts of many institutions, the author has created a problematic aggregated database that combines three publicly available datasets: Replay-Attack, Replay-Mobile, and MSU MFSD, and reports the result.

A unique approach is presented [140] that reformulates the Generalized Presentation Attack Detection (GPAD) problem from the standpoint of anomaly detection. A deep metric learning model was provided. A triplet focal loss is a regularization for a novel loss called 'metric-SoftMax.' It guides the learning process towards more discriminating feature representations in an embedding space. Finally, the benefits of deep anomaly detection architecture are proven by introducing a few-shot posterior probability calculation that does not require any classifier to be trained on the learned features. Table 10 summarizes the anomaly detection approaches in FLD.

**Table 10.** Anomaly detection in FLD.

| Ref. and Year | Method for Anomaly Detection | Dataset Used | Performance Metrics and Model Performance | Intra-Database Testing | Cross-Database Testing |
|---|---|---|---|---|---|
| [141] 2018 | A GMM anomaly detector and aggregated database | Aggregated database of 3 datasets Replay- Attack, Replay-Mobile, and MSU MFSD | HTER: 11.90% | Y | Y |
| [140] 2019 | a deep metric learning model | GPAD is the world's largest aggregated dataset, combining more than ten datasets into two levels of classification to reflect four fundamental components of anti-spoofing: attacks, lightning, capturing gadgets, and resolving | Attack Presentation Classification Error Rate (APCER): 14.28%, Bonafide presentation Classification Error Rate (BPCER): 5.99%, and Aver-age Classification Error Rate (ACER): 10.14%., Half Total Error (HTER): 5.41% | Y | Y |
| [142] 2020 | A hypersphere loss function | CASIA-FASD, Replay- Attack and MSU-MFSD databases, SiW-M database | ACER: 15.80% and EER: 15.20%, Area under the curve (AUC): 96.20% | Y | N |
| [143] 2020 | HOG-based face detection VGG Face base feature extraction, Pseudo negative sampling | Replay-Attack, Rose-You, OULU-NPU, and Spoof in Wild | Average Classification Error Rate (ACER):20.74%, Attack Presentation Classification Error Rate (APCER): 25.04%, Bona-fide Presentation Classification Error Rate (BPCER): 16.53% | Y | Y |
| [109] 2021 | multiple kernel fusion for anomaly detection in unseen presentations | Replay- Mobile, Replay attack, OULU-NPU, MSU-MFSD | ACER: 5.58%, AUC:100%, EER: 0.00%, HTER: 0.00% | Y | Y |
| [144] 2021 | client-specific one-class adaptation-based anomaly detection | Replay attack, Replay Mobile, ROSE-YOUTU | HTER: 8.13% | Y | Y |

## 5. RQ4 Evaluation Metrics

The performance of face liveness Detection (FLD) systems was evaluated using ISO/IEC DIS 30107-3:2017. The authors reported the evaluation measures used to test various scenarios in a face-liveness detection system. Half Total Error Rate (HTER) is the most often utilized measure in anti-spoofing settings.

Face Liveness Detection is frequently thought of as a binary classification issue. The performance is assessed using a variety of performance-related measures. Because these binary classification methods have two input classes, they are sometimes referred to as positive and negative. The types of errors they make and their approach to measuring them are used to evaluate their performance. Binary classification techniques make use of False positives and False negatives. False Positive Rate (FPR) and False Negative Rate (FNR) are two often documented error rates (FNR). They calculate the average of FRR (ratio of incorrectly rejected genuine score) and FAR yields HTER (ratio of wrongly accepted zero-effort impostor) [142]. Attack Presentation Classification Error Rate (APCER), Average Classification Error Rate (ACER), and Bonafide Presentation Classification Error Rate are the three variables (BPCER) [143]. While evaluating Face presentation attacks, the classification of attacks, the real face, intra-dataset, and cross-dataset performance are considered [145,146]. BPCER and APCER are two different methods for calculating the rates of correct and false classification errors. ACER measures performance inside a dataset, while HTER measures performance across datasets. The Receiver Operating Characteristic (ROC) curve and the Area Under the Curve (AUC) are also widely employed to evaluate the performance of face liveness detection methods in addition to the HTER and ACER scalar values. Equations (1)–(6) show the formula for calculating measures.

$$\text{HTER} = \frac{\text{FAR} + \text{FRR}}{2} \tag{1}$$

$$\text{FAR} = \frac{\text{FP}}{\text{Fake samples}} \tag{2}$$

$$\& \ \text{FRR} = \frac{\text{FN}}{\text{Genuine Samples}} \tag{3}$$

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

$$\text{where APCER} = \frac{\text{FP}}{\text{FP} + \text{FN}} \tag{5}$$

$$\text{BPCER} = \frac{\text{FN}}{\text{FN} + \text{TP}} \tag{6}$$

## 6. RQ 5 Limitations of Face Liveness Detection Methods

Despite recent and considerable improvements in the development of detection algorithms, presentation attacks remain difficult for the research community. Section 6.1 discusses the challenges in existing databases, followed by Section 6.2, which discusses challenges faced by existing liveness detection methods.

### *6.1. Limitations Existing Databases for Face Liveness Detection*

Face liveness Detection datasets are still limited in volume and diversity in terms of the types of spoofing attacks, spoof attack instruments, and acquisition devices employed for real faces, PAs, and maybe PAIs (compared to other face-related difficulties). There is currently no publicly available large-scale face PAD, although multiple such datasets exist for face recognition. It was discovered that none of the databases contained images of all known forms of spoofing attacks. The majority of published datasets cover two to three forms of spoofing attacks. Furthermore, some collections have images specialized to a specific sort of attack. Because no such dataset exists, the researchers should work on

several datasets to construct the Face Liveness Detection System. A dataset that covers all known types of attacks in a single dataset is required to build a robust Face Liveness Detection model against all known attacks. Detecting a face presentation attack is a difficult task. However, face PAD approaches are currently limited in performance due to the learning dataset's lack of quantity and diversity.

### 6.2. Limitations of Existing Face Liveness Detection Techniques

Despite recent advances in presentation attack detection approaches, unseen attack detection remains a complex subject. Existing solutions demonstrated promising results when tested using specific attacks in a controlled environment or public datasets. PAD models trained on predetermined attacks produce favorable results but are skewed toward specific attacks. The current face PAD approaches still fall short of most real-world requirements (especially generalization ability). When there isn't too much discrepancy between the conditions of actual face capture for enrolment and genuine face/PA presentation for authentication, the results are satisfactory (intra-database evaluation). However, they have a limited generalization capacity because handcrafted features are not powerful enough to capture all conceivable variations in acquisition settings.

Moreover, because the features learned by deep neural networks are of relatively high dimensions compared to the training data's restricted size, Over-fitting affects both features, resulting in poor generalization ability. Learning traits that distinguish between a genuine face and any spoofing attack, presumably in various capture conditions, is still a research problem. The sensitivity of face recognition systems to numerous face artifacts has been studied extensively, and different PAD strategies to identify these abnormalities have developed. Despite these efforts, there are still several obstacles and unresolved issues.

## 7. RQ6 Future Directions

This section discusses various scientific challenges prior face liveness detection experiments have not addressed. These issues include a significant amount of work that must be done to improve the performance of the various face-liveness detection systems. The following is a summary of several difficulties encountered in research, along with potential answers to those difficulties:

**Challenge 1:** DL models are sometimes characterized as a "black box" because it is difficult to determine their sources. As a result, an approach for automatic (parameter) optimization is required: Finding the ideal layer layout and node number values for various layers is another difficult task. The choice of parameters for the number of epochs, learning rate, and regularized strength also requires a basic understanding of the domain. Automatic optimization techniques for various DL architecture components for datasets and additional clinical datasets could be introduced as a result.

**Future directions for research: Explainable AI (XAI).**

Explainable AI (XAI) is a type of artificial intelligence (AI) that enables people to comprehend the results of a solution. It contrasts with machine learning's "black box" character, in which even the AI's architects cannot explain why it made a particular conclusion. However, users gradually delegate more computer duties as automation becomes more common. Users may find it challenging to comprehend such complicated systems because they often create "black box" Artificial Intelligence (AI). Deep learning can sometimes achieve remarkable results by focusing on incorrect/biased dataset-related information rather than domain-relevant information. Regarding the interpretability approach, the author [147] chose Grad-CAM since it allows us to obtain class-specific explanations and provides explanations for each layer of the network.

**Challenge 2:** In real-world circumstances, however, everyday unlabeled face data is continuously collected from various face recognition terminals, which might use for semi-supervised learning. One challenge is figuring out how to make the most of unlabeled unbalanced (i.e., live or fake) data while minimizing performance drops. Furthermore,

appropriate data augmentation procedures for FAS are rarely studied. Adversarial learning could be a strong fit for adaptive data augmentation across various areas.

**Future directions for research: Adversarial Learning.**

However, improving recognition efficiency in a more complex FR model is not enough; the system should endure various attacks aimed at its competency. Researchers recently discovered that (deep) FR systems are vulnerable to several attacks that produce data changes to deceive classifiers. These attacks are carried out in two ways: (a) physically altering the physical look before capturing a photograph or (b) digitally altering the captured face image. On the other hand, adversarial attacks and the variations that result from morphing attacks are essential strategies for digital invasion. However, adversarial attacks are mainly classified as digital attacks, some tactics designed to carry out physically. Adversarial attacks are noteworthy because they typically target deep neural networks (DNN) and focus on convolutional neural networks (CNN) used to build state-of-the-art FR models [148]. It is crucial in black-box attacks because access to the target model, the training dataset, and other learning parameters is impossible. A substitute neural network model trained in such situations can generate adversarial instances against the substitute model [149]. The target model would expose to these adversarial situations due to its transferability.

A new research area might be the security of CNN-based anti-spoofing against the challenges posed by the vulnerability of DL architectures to adversarial samples. The intersection of biometric anti-spoofing and adversarial attacks raises many new challenges, especially considering how quickly both fields are evolving.

Aside from the above-mentioned future study, the authors suggest further research directions in robust face presentation attack detection (FPAD) systems.

**Challenge 3:** Face images from various input disseminations and diverse spoof attacks can build an FLD model with strong generalization. It is a fact that training data (both genuine and fake photos) is not shared due to concerns about legal and privacy. Further research needs to be done to address the concerns of data privacy.

**Future directions for research: Federated Learning.**

Federated learning is a machine learning algorithm that works collaboratively without relying on centralized training data. It is a type of machine learning that's decentralized. However, a Federated Face Presentation Attack Detection (FedPAD) architecture proposes to address this issue [147], which takes advantage of extensive face PAD data available from diverse data owners while ensuring data privacy. Each data owner (known as a data center) trains its face PAD model locally in a Federated PAD architecture. A server learns a global face PAD model by repeatedly aggregating model changes from all data centers without gaining access to private data in each one.

The goal of federated learning is to address the issue of data set privacy. However, it ignores privacy concerns at the model level for FAS because training the global model necessitates numerous teams sharing their local models, potentially harming economic competition.

**Challenge 4:** New face presentation attack methods are continually developed, resulting in new spoofing faces that compromise existing face liveness detectors. It necessitates researchers to collect many samples to train classifiers to identify more contemporary assaults, which is typically expensive and leads to newly evolved attack samples remaining in tiny sizes.

**Future directions for research: Meta-Learning.**

Face anti-spoofing is a few-shot learning problem with emerging new threats described. Meta Face Anti-spoofing proposes a revolutionary face anti-spoofing strategy based on meta-learning (Meta-FAS). Meta-Learning is also term as Learning by Learning. Most existing works use Domain Adaptation (DA) or Domain Generalization (DG) methodologies to overcome insufficient abstraction to unknown attacks.

However, during training, the target domain is frequently unclear, limiting the use of DA approaches. Without seeing any target data, DG techniques can overcome this by learning domain invariant features. On the other hand, they fail to use the target data's contents. A self-domain adaptation paradigm proposes an inference that uses unlabeled

test domain data [150]. A Dual-Branch Meta-learning Network (DBMNet) is explored to extract features from unseen domains [151–153].

Furthermore, a new approach for face anti-spoofing to extract discriminated features from domain-specific information in the test domain to improve performance is needed.

**Challenge 5**: Existing texture-based feature extraction approaches often use the entire image as input and extract features from there, ignoring that different portions of the image have varying degrees of importance. Nonetheless, an input image's data is made up of a variety of discriminative components with varying degrees of discrimination. Because of differences in attack instrument and lighting, the useful discriminatory information for liveness recognition is scattered throughout the image. Consequently, the full potential of the local representation for discriminative face liveness detection is not tapped when patches are randomly selected from the face region. For more accurate and reliable face liveness detection, it is crucial to know how to find the discriminative regions better.

**Future directions for research: Reinforcement Learning.**

Reinforcement learning (RL) is a branch of machine learning that studies how intelligent creatures should behave in a given environment to maximize the concept of cumulative reward. Deep reinforcement learning also offers a wide range of applications in the face-related research field. A combination of DRL (Deep Reinforcement Learning) and RNN has been used to exploit global and local features jointly with global Feature Extraction using ResNet18 [54]. Moreover, the deep reinforcement learning method is applied to guarantee the consistency of the visual identity in synthesized faces. In addition, a researcher suggested an ethnicity balance network based on reinforcement learning to learn superior performance for multiple ethnicity's face recognition based on huge margin losses. However, applying deep reinforcement learning methods still has space for development. It would be interesting to explore how RL can extract salience features for Face liveness detection.

**Challenge 6:** Within one or more small-size datasets, classic evaluation techniques for Face presentation attacks commonly consider intra-domain, cross-domain, and cross-type testing. Because the data amount, especially in the testing set, is relatively small. State-of-the-art methods in such protocols cannot guarantee consistently good performance in practical scenarios. The protocols focus on a single factor, such as seen/unseen domains or known/unknown attack types, which cannot satisfy the need for complex real-world scenarios.

**Future directions for research: need to find a solution (protocol) for complex real-world scenarios.**

GrandTest and open-set [152] are two recent proposals for more realistic protocols. Open-set testing analyses models discriminating and generalization capabilities on known and unknown attack types, while Grand Test comprises large-scale mixed-domain data [107]. On the other hand, real-world open-set situations with multiple domains and assault kinds continue to be overlooked.

More comprehensive protocols (e.g., domain- and type-aware open-set) should be investigated to bridge the gap between academics and industry. In the case of multi-modal protocols, training data with multiple modalities is expected, and two testing settings are commonly used: 1) with multiple corresponding modalities and 2) with only one modality [54] (usually RGB). However, depending on the user terminal device, multiple modality combinations (e.g., RGB-NIR, RGB-D, NIR-D, and RGB-DNIR) are used in real-world deployment. As a result, training individual models for each multi-modal combination is expensive and inefficient. Although cross-modality translation creates false modalities, their fidelity, and stability are still inferior to modalities obtained from real-world sensors. An alternative route for endless multi-modal deployment could be to build a dynamic multi-modal framework that propagates learned multi-modal information to multiple modality combinations.

**Challenge 7:** The need to establish new approaches in face liveness detection involves explainability has been discussed in earlier sections. It is observed that No standard exists for evaluating and testing AI explanation algorithms. It is tempting to analyze explanation

frameworks to compare their quality. According to Explainable AI, an "accurate" explanation does not mean the system gave the correct response. Thus, the biometrics community must move from "decision accuracy measures" to "performance metrics for explanations," which have yet to be produced.

**Future directions for research:** need to explore experimentations to find a performance measure for explanations.

## 8. Discussion

This systematic review examined various academic research articles on face presentation attack detection using AI-based techniques. The authors answered research questions through a systematic review using the PRISMA protocol. Such as varied challenges and problems associated with the different face spoofing attacks, datasets, face presentation attack detection using artificial intelligence-based approaches used for robust face recognition systems, and future directions as follows:

Various feature extraction methods, such as handcrafted feature-based extraction, texture-based, motion-based, and depth-based methods, and the fusion of multiple feature extraction methods, are proposed in the literature. Face anti-spoofing systems use a combination of machine learning and deep learning algorithms to achieve optimum accuracy in seeing false and real faces. Even while these approaches offer correct findings for the existing types of attacks, they are vulnerable to invisible attacks or attacks that are unable to detect by the systems. Due to their lack of generalization capacity, existing approaches cannot detect invisible attacks (such as synthetic faces).

Public datasets are still a long way from accurately reproducing real-world applications. It is likely owing to the difficulties of gathering PAs and PAIs from impostors in the wild. As a result, most PA examples are obtained manually, which is time-consuming and exhausting. Moreover, generating a large-scale dataset for face anti-spoofing in the wild covers numerous real-world applicative contexts. When faced with these challenges, some researchers rely on data augmentation techniques to create synthetic (yet realistic) photographs of PA.

Face presentation attack detection (FAD) problems use various artificial intelligence-based approaches. Due to AI-based advancements, the classification of fake or real spoofs for robust face recognition systems has become possible. Literature looks at AI-based models, such as convolutional neural networks, transfer learning, domain adaptation, domain generalization, generative adversarial network, reinforcement learning, explainable AI, etc.

The handcrafted feature-based face liveness detection methods are considered to be more robust against the unknown data samples (data samples not being considered during training of the AI-based face FLD techniques). The deep learning stacks of neural networks are more reliable in performance, especially in cases where training and testing data samples are very similar. For unknown attacks such as synthetic faces (artificially created), the fusion of handcrafted and auto-extracted (through deep learning) features may perform promisingly with the help of AI techniques.

In the future, to improve the robustness of existing face liveness detection techniques, domain adaption, and generalization strategies, investigate further to deal with undetected or unseen attacks. To make existing algorithms more robust, considering employing multiple algorithms together for decision-making using either federated learning or decision fusion would be the further research direction in the field.

## 9. Conclusions

Face recognition using biometric identification techniques is widely used nowadays but has many potential threats. Though there has been active research for AI-based robust face recognition systems, researchers are still striving to get a full-proof solution. This paper examined many types of face presentation attacks and detection strategies for robust anti-spoofing using AI-based solutions. The study's key findings are the challenges existing face

liveness detection systems confront and how they affect the performance of the spoofing model. The research also finds a high-quality publicly available real-world dataset for 2D and 3D spoofing attacks, which would be the foundation for developing robust FPAD systems. It discussed challenges as well as future research goals in the domain of invisible attack detection methods. However, several unique challenges must be addressed before they are employed in real-world face recognition-based authentication systems. Although most current solutions rely on handcrafted features to combat presentation attacks, machine learning and deep learning-based feature extraction methods are also used. Although existing approaches perform better intra-testing, they lack generalization capabilities, which is crucial for unknown threats. In the real-world implementation of face anti-spoofing systems, domain adaptation, and explainable artificial intelligence need to be explored. These discoveries could serve as a foundation for future research toward face anti-spoofing that is secure and robust. The findings of this study would undoubtedly guide the biometric sector in developing safe, efficient, and trustworthy face anti-spoofing systems in the coming years of biometric technological development.

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

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

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

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

## References

1. Sébastien, M.S.; Nixon, J.F.; Marcel, N.E. *Handbook of Biometric Anti-Spoofing*, 2nd ed.; Springer: Cham, Switzerland, 2019. [CrossRef]
2. Sharma, S.B.; Dhall, I.; Nayak, S.R.; Chatterjee, P. Reliable Biometric Authentication with Privacy Protection. *Adv. Commun. Devices Netw.* **2023**, *902*, 233–249.
3. Biometrics Recognition Using Deep Learning: A Survey. Available online: https://doi.org/10.1007/s10462-022-10237-x (accessed on 8 December 2022).
4. Ross, A.; Jain, A.K. Biometrics, Overview. In *Encyclopedia of Biometrics*; Springer: Boston, MA, USA, 2015; pp. 289–294. [CrossRef]
5. Cabana, P.F. Technical and Legal Challenges of the Use of Automated Facial Recognition Technologies for Law Enforcement and Forensic Purposes. In *Artificial Intelligence, Social Harms and Human Rights*; Završnik, A., Simončič, K., Eds.; Springer International Publishing: Cham, Switzerland, 2023; pp. 35–54. [CrossRef]
6. FRB Report. "Market Research Report," marketsandmarkets.com, 2021. Available online: https://www.marketsandmarkets.com/PressRelease (accessed on 8 December 2022).
7. Kalmani, S.; Dilna, U. Application of Computer Vision for Multi-Layered Security to ATM Machine using Deep Learning Concept. In Proceedings of the 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Online, 9–11 May 2022; pp. 999–1004. [CrossRef]
8. Enhancing Bank Security System using Face Recognition, Iris Scanner and Palm Vein Technology. In Proceedings of the 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal, India, 23–24 February 2018. [CrossRef]
9. Ali, O.; AlAhmad, A.; Kahtan, H. A review of advanced technologies available to improve the healthcare performance during COVID-19 pandemic. *Procedia Comput. Sci.* **2023**, *217*, 205–216. [CrossRef] [PubMed]
10. Martins, B.O.; Lidén, K.; Jumbert, M.G. Border security and the digitalisation of sovereignty: Insights from EU borderwork. *Eur. Secur.* **2022**, *31*, 475–494. [CrossRef]
11. Andrejevic, M.; Selwyn, N. Facial recognition technology in schools: Critical questions and concerns. *Learn. Media Technol.* **2020**, *45*, 115–128. [CrossRef]
12. SonarGuard: Ultrasonic Face Liveness Detection on Mobile Devices. Available online: https://doi.org/10.1109/tcsvt.2023.3236303 (accessed on 8 December 2022).
13. Ming, Z.; Visani, M.; Luqman, M.M.; Burie, J.-C. A Survey on Anti-Spoofing Methods for Facial Recognition with RGB Cameras of Generic Consumer Devices. *J. Imaging* **2020**, *6*, 139. [CrossRef]

14. Liu, H.; Zheng, C.; Li, D.; Shen, X.; Lin, K.; Wang, J.; Zhang, Z.; Zhang, Z.; Xiong, N.N. EDMF: Efficient Deep Matrix Factorization with Review Feature Learning for Industrial Recommender System. *IEEE Trans. Ind. Inform.* **2022**, *18*, 4361–4371. [CrossRef]
15. Liu, T.; Wang, J.; Yang, B.; Wang, X. NGDNet: Nonuniform Gaussian-label distribution learning for infrared head pose estimation and on-task behavior understanding in the classroom. *Neurocomputing* **2021**, *436*, 210–220. [CrossRef]
16. Liu, T.; Wang, J.; Yang, B.; Wang, X. Facial expression recognition method with multi-label distribution learning for non-verbal behavior understanding in the classroom. *Infrared Phys. Technol.* **2021**, *112*, 103594. [CrossRef]
17. Liu, H.; Liu, T.; Zhang, Z.; Sangaiah, A.K.; Yang, B.; Li, Y. ARHPE: Asymmetric Relation-Aware Representation Learning for Head Pose Estimation in Industrial Human–Computer Interaction. *IEEE Trans. Ind. Inform.* **2022**, *18*, 7107–7117. [CrossRef]
18. Liu, H.; Liu, T.; Chen, Y.; Zhang, Z.; Li, Y.-F. EHPE: Skeleton Cues-based Gaussian Coordinate Encoding for Efficient Human Pose Estimation. *IEEE Trans. Multimedia.* **2022**, 1–12. [CrossRef]
19. Liu, H.; Fang, S.; Zhang, Z.; Li, D.; Lin, K.; Wang, J. MFDNet: Collaborative Poses Perception and Matrix Fisher Distribution for Head Pose Estimation. *IEEE Trans. Multimedia* **2022**, *24*, 2449–2460. [CrossRef]
20. Garg, D.; Jain, P.; Kotecha, K.; Goel, P.; Varadarajan, V. An Efficient Multi-Scale Anchor Box Approach to Detect Partial Faces from a Video Sequence. *Big Data Cogn. Comput.* **2022**, *6*, 9. [CrossRef]
21. Xie, X.; Bian, J.; Lai, J. Review on face liveness detection. *J. Image Graph.* **2022**, *27*, 63–87. [CrossRef]
22. Costa-Pazo, A.; Pérez-Cabo, D.; Jiménez-Cabello, D.; Alba-Castro, J.L.; Vazquez-Fernandez, E. Face presentation attack detection. A comprehensive evaluation of the generalisation problem. *IET Biom.* **2021**, *10*, 408–429. [CrossRef]
23. Khade, S.; Gite, S.; Pradhan, B. Iris Liveness Detection Using Multiple Deep Convolution Networks. *Big Data Cogn. Comput.* **2022**, *6*, 67. [CrossRef]
24. Khade, S.; Gite, S.; Thepade, S.D.; Pradhan, B.; Alamri, A. Detection of Iris Presentation Attacks Using Feature Fusion of Thepade's Sorted Block Truncation Coding with Gray-Level Co-Occurrence Matrix Features. *Sensors* **2021**, *21*, 7408. [CrossRef]
25. Zhang, M.; Zeng, K.; Wang, J. A Survey on Face Anti-Spoofing Algorithms. *J. Inf. Hiding Priv. Prot.* **2020**, *2*, 21–34. [CrossRef]
26. 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.* **2019**, *9*, 5165–5175. [CrossRef]
27. Ramachandra, R.; Busch, C. Presentation Attack Detection Methods for Face Recognition Systems: A comprehensive survey. *ACM Comput. Surv.* **2017**, *50*, 1–37. [CrossRef]
28. Komulainen, J.; Boulkenafet, Z.; Akhtar, Z. *Review of Face Presentation Attack Detection Competitions*; Springer International Publishing: Cham, Switzerland, 2019; pp. 291–317. [CrossRef]
29. Yu, Z.; Qin, Y.; Li, X.; Zhao, C.; Lei, Z.; Zhao, G. Deep Learning for Face Anti-Spoofing: A Survey. *arXiv* **2021**. Available online: http://arxiv.org/abs/2106.14948 (accessed on 8 December 2022).
30. Abdullakutty, F.; Elyan, E.; Johnston, P. A review of state-of-the-art in Face Presentation Attack Detection: From early development to advanced deep learning and multi-modal fusion methods. *Inf. Fusion* **2021**, *75*, 55–69. [CrossRef]
31. Purnapatra, S.; Smalt, N.; Bahmani, K.; Das, P.; Yambay, D.; Mohammadi, A.; George, A.; Bourlai, T.; Marcel, S.; Schuckers, S.; et al. Face Liveness Detection Competition (LivDet-Face)—2021. *IEEE Int. Jt. Conf. Biom. IJCB* **2021**, 1–10. [CrossRef]
32. Kowalski, M. A Study on Presentation Attack Detection in Thermal Infrared. *Sensors* **2020**, *20*, 3988. [CrossRef]
33. Ghaffar, I.A.; Mohd, M.N.H. Presentation attack detection for face recognition on smartphones: A comprehensive review. *J. Telecommun. Electron. Comput. Eng.* **2017**, *9*, 33–38.
34. Kenneth, M.O.; Sulaimon, B.A.; Abdulhamid, S.M.; Ochei, L.C. A Systematic Literature Review on Face Morphing Attack Detection (MAD). *Illum. Artif. Intell. Cybersecur. Forensics* **2022**, *109*, 139–172. [CrossRef]
35. A Bibliometric Analysis of Face Presentation Attacks based on Domain Adaptation. Available online: https://digitalcommons.unl.edu/libphilprac/5454/ (accessed on 18 December 2022).
36. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *BMJ* **2009**, *339*, 332–336. [CrossRef]
37. Panic, N.; Leoncini, E.; de Belvis, G.; Ricciardi, W.; Boccia, S. Evaluation of the Endorsement of the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) Statement on the Quality of Published Systematic Review and Meta-Analyses. *PLoS ONE* **2013**, *8*, e83138. [CrossRef]
38. Rathgeb, C.; Drozdowski, P.; Busch, C. Detection of Makeup Presentation Attacks based on Deep Face Representations. *Int. Conf. Pattern Recognit. (ICPR)* **2021**, 3443–3450. [CrossRef]
39. Boulkenafet, Z.; Komulainen, J.; Li, L.; Feng, X.; Hadid, A. OULU-NPU: A mobile face presentation attack database with real-world variations. In Proceedings of the 2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017), Washington, DC, USA, 30 May–3 June 2017; pp. 612–618. [CrossRef]
40. On the Effectiveness of Local Binary Patterns in Face Anti-Spoofing. Available online: https://www.semanticscholar.org/paper/On-the-effectiveness-of-local-binary-patterns-in-Chingovska-Anjos/30648c20ffa148e2d15cb705abfb8a1650f652df (accessed on 18 December 2022).
41. Agarwal, A.; Yadav, D.; Kohli, N.; Singh, R.; Vatsa, M.; Noore, A. Face Presentation Attack with Latex Masks in Multispectral Videos. *IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops* **2017**, 275–283. [CrossRef]
42. Erdogmus, N.; Marcel, S. Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect. In Proceedings of the IEEE 6th International Conference on Biometrics: Theory, Applications and Systems, BTAS, Arlington, VA, USA, 29 September 2013; pp. 1–6. [CrossRef]

43. Tan, X.; Li, Y.; Liu, J.; Jiang, L. Face liveness detection from a single image with sparse low rank bilinear discriminative model. In Proceedings of the European Conference on Computer Vision, Heraklion, Greece, 5–11 September 2010; pp. 504–517. [CrossRef]
44. de Souza, G.B.; Papa, J.P.; Marana, A.N. On the Learning of Deep Local Features for Robust Face Spoofing Detection. In Proceedings of the 31st Conference on Graphics, Patterns and Images, SIBGRAPI, Paraná, Brazil, 29 October–1 November 2018; pp. 258–265. [CrossRef]
45. Li, J.; Zhang, X.; Zhang, Y.; Wang, H.; Yang, F. Face Liveness Detection Based on Multiple Feature Descriptors. In Proceedings of the 2019 International Conference on Technologies and Applications of Artificial Intelligence, TAAI, Kaohsiung, Taiwan, 21–23 November 2019; pp. 1–5. [CrossRef]
46. Shilpa, S.; Sajeena, A. Hybrid Deep Learning Approach for Face Spoofing Detection. In Proceedings of the International Conference on Intelligent Computing and Control Systems, ICCS, Madurai, India, 15–17 May 2019; pp. 412–416. [CrossRef]
47. Chen, B.; Yang, W.; Wang, S. Generalized Face Antispoofing by Learning to Fuse Features from High- and Low-Frequency Domains. *IEEE MultiMedia* **2021**, *28*, 56–64. [CrossRef]
48. Nguyen, D.T.; Pham, T.D.; Baek, N.R.; Park, K.R. Combining Deep and Handcrafted Image Features for Presentation Attack Detection in Face Recognition Systems Using Visible-Light Camera Sensors. *Sensors* **2018**, *18*, 699. [CrossRef]
49. Perumal, R.S.; Santosh, K.C.; Chandra Mouli, P.V.S.S.R. Learning Deep Feature Representation for Face Spoofing. In *Recent Trends in Image Processing and Pattern Recognition. RTIP2R 2018. Communications in Computer and Information Science*; Springer Nature: Singapore, 2019; Volume 1035, pp. 178–185.
50. Song, X.; Zhao, X.; Fang, L.; Lin, T. Discriminative representation combinations for accurate face spoofing detection. *Pattern Recognit.* **2019**, *85*, 220–231. [CrossRef]
51. Zuo, Y.; Gao, W.; Wang, J. Face Liveness Detection Algorithm based on Livenesslight Network. In Proceedings of the 2020 International Conference on High Performance Big Data and Intelligent Systems, HPBD and IS, Shenzhen, China, 23 May 2020; pp. 1–5. [CrossRef]
52. Wen, D.; Han, H.; Jain, A.K. Face Spoof Detection With Image Distortion Analysis. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 746–761. [CrossRef]
53. Chen, B.; Yang, W.; Li, H.; Wang, S.; Kwong, S. Camera Invariant Feature Learning for Generalized Face Anti-Spoofing. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 2477–2492. [CrossRef]
54. Cai, R.; Li, H.; Wang, S.; Chen, C.; Kot, A.C. DRL-FAS: A Novel Framework Based on Deep Reinforcement Learning for Face Anti-Spoofing. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 937–951. [CrossRef]
55. Guo, J.; Zhu, X.; Xiao, J.; Lei, Z.; Wan, G.; Li, S.Z. Improving Face Anti-Spoofing by 3D Virtual Synthesis. In Proceedings of the 2019 International Conference on Biometrics (ICB), Crete, Greece, 4–7 June 2019. [CrossRef]
56. Zhang, Z.; Yan, J.; Liu, S.; Lei, Z.; Yi, D.; Li, S.Z. A face antispoofing database with diverse attacks. In Proceedings of the 2012 5th IAPR International Conference on BIOMETRICS (ICB), New Delhi, India, 29 March–1 April 2012; pp. 26–31. [CrossRef]
57. Li, H.; Wang, S.; He, P.; Rocha, A.D.R. Face Anti-Spoofing with Deep Neural Network Distillation. *IEEE J. Sel. Top. Signal Process.* **2020**, *14*, 933–946. [CrossRef]
58. Yang, J.; Lei, Z.; Yi, D.; Li, S.Z. Person-Specific Face Antispoofing with Subject Domain Adaptation. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 797–809. [CrossRef]
59. Transfer Learning Using Convolutional Neural Networks for Face Anti-Spoofing. Available online: https://doi.org/10.1007/978-3-319-59876-5_4 (accessed on 8 December 2022).
60. Vareto, R.H.; Diniz, M.A.; Schwartz, W.R. Face De-spoofing: Anti-spoofing via Noise Modeling. Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications. CIARP 2019. *Lect. Notes Comput. Sci.* **2019**, *11217*, 187–197. [CrossRef]
61. Liu, Y.; Stehouwer, J.; Jourabloo, A.; Liu, X. Deep Tree Learning for Zero-Shot Face Anti-Spoofing. *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.* **2019**, 4675–4684. [CrossRef]
62. Vareto, R.H.; Schwartz, W.R. Face spoofing detection via ensemble of classifiers toward low-power devices. *Pattern Anal. Appl.* **2020**, *24*, 511–521. [CrossRef]
63. Zhang, B.; Tondi, B.; Barni, M. Adversarial examples for replay attacks against CNN-based face recognition with anti-spoofing capability. *Comput. Vis. Image Underst.* **2020**, *197–198*, 102988. [CrossRef]
64. Rehman, Y.A.U.; Po, L.M.; Liu, M. Deep learning for face anti-spoofing: An end-to-end approach. Signal Processing—Algorithms, Architectures, Arrangements, and Applications Conference Proceedings, SPA. *IEEE* **2017**, 195–200. [CrossRef]
65. Ying, X.; Li, X.; Chuah, M.C. LiveFace: A Multi-task CNN for Fast Face-Authentication. In Proceedings of the 17th IEEE International Conference on Machine Learning and Applications, ICMLA, Orlando, FL, USA, 17–20 December 2018; pp. 955–960. [CrossRef]
66. Nikitin, M.Y.; Konushin, V.S.; Konushin, A.S. Face anti-spoofing with joint spoofing medium detection and eye blinking analysis. *Comput. Opt.* **2019**, *43*, 618–626. [CrossRef]
67. Chen, H.; Hu, G.; Lei, Z.; Chen, Y.; Robertson, N.M.; Li, S.Z. Attention-Based Two-Stream Convolutional Networks for Face Spoofing Detection. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 578–593. [CrossRef]
68. Erdogmus, N.; Marcel, S. Spoofing Face Recognition With 3D Masks. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 1084–1097. [CrossRef]
69. Te, G.; Hu, W.; Guo, Z. Exploring Hypergraph Representation On Face Anti-Spoofing Beyond 2d Attacks. In Proceedings of the IEEE International Conference on Multimedia and Expo (ICME), London, UK, 6–10 July 2020; pp. 1–6. [CrossRef]

70. Agarwal, A.; Singh, R.; Vatsa, M. Face anti-spoofing using Haralick features. In Proceedings of the 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), Niagara Falls, NY, USA, 6–9 September 2016. [CrossRef]
71. Bousnina, N.; Zheng, L.; Mikram, M.; Ghouzali, S.; Minaoui, K. Unraveling robustness of deep face anti-spoofing models against pixel attacks. *Multimedia Tools Appl.* **2021**, *80*, 7229–7246. [CrossRef]
72. Mehta, S.; Uberoi, A.; Agarwal, A.; Vatsa, M.; Singh, R. Crafting A Panoptic Face Presentation Attack Detector. In Proceedings of the 2019 International Conference on Biometrics, ICB 2019, Crete, Greece, 4–7 June 2019. [CrossRef]
73. Tu, X.; Zhang, H.; Xie, M.; Luo, Y.; Zhang, Y.; Ma, Z. Deep transfer across domains for face antispoofing. *J. Electron. Imaging* **2019**, *28*. [CrossRef]
74. Chen, B.; Yang, W.; Wang, S. Face Anti-Spoofing by Fusing High and Low Frequency Features for Advanced Generalization Capability. In Proceedings of the 3rd International Conference on Multimedia Information Processing and Retrieval, MIPR 2020, Guangdong, China, 6–8 August 2020; pp. 199–204. [CrossRef]
75. Shao, R.; Lan, X.; Li, J.; Yuen, P.C. Multi-Adversarial Discriminative Deep Domain Generalization for Face Presentation Attack Detection. In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, San Juan, PR, USA, 17–19 June 1997; pp. 10015–10023. [CrossRef]
76. Patel, K.; Han, H.; Jain, A.K. Secure Face Unlock: Spoof Detection on Smartphones. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 2268–2283. [CrossRef]
77. Wang, G.; Han, H.; Shan, S.; Chen, X. Improving Cross-database Face Presentation Attack Detection via Adversarial Domain Adaptation. In Proceedings of the 2019 International Conference on Biometrics, ICB, Crete, Greece, 4–7 June 2019. [CrossRef]
78. Muhammad, U.; Hadid, A. Face Anti-spoofing using Hybrid Residual Learning Framework. In Proceedings of the 2019 International Conference on Biometrics, ICB, Crete, Greece, 4–7 June 2019. [CrossRef]
79. Nagpal, C.; Dubey, S.R. A Performance Evaluation of Convolutional Neural Networks for Face Anti Spoofing. In Proceedings of the International Joint Conference on Neural Networks, Budapest, Hungary, 14–19 July 2019. [CrossRef]
80. Sun, Y.; Xiong, H.; Yiu, S.M. Understanding deep face anti-spoofing: From the perspective of data. *Vis. Comput.* **2021**, *37*, 1015–1028. [CrossRef]
81. Patel, K.; Han, H.; Jain, A.K. Cross-Database Face Antispoofing with Robust Feature Representation. Available online: https://doi.org/10.1007/978-3-319-46654-5_67 (accessed on 8 December 2022).
82. Galbally, J.; Satta, R. Three-dimensional and two-and-a-half-dimensional face recognition spoofing using three-dimensional printed models. *IET Biom.* **2016**, *5*, 83–91. [CrossRef]
83. Steiner, H.; Kolb, A.; Jung, N. Reliable face anti-spoofing using multispectral SWIR imaging. In Proceedings of the 2016 International Conference on Biometrics, ICB, Halmstad, Sweden, 13–16 June 2016. [CrossRef]
84. Jia, S.; Guo, G.; Xu, Z. A survey on 3D mask presentation attack detection and countermeasures. *Pattern Recognit.* **2020**, *98*, 107032. [CrossRef]
85. de Freitas, T.; Komulaine, J.; Anjos, A.; De Martino, J.M.; Hadid, A.; Pietikäinen, M.; Marcel, S. PereiraFace Liveness Detection using Dynamic Texture. *EURASIP J. Image Video Process* **2014**, *2*, 1–15. Available online: https://jivp.eurasipjournals.com/content/2014/1/2 (accessed on 8 December 2022).
86. Liu, S.; Yang, B.; Yuen, P.C.; Zhao, G. A 3D Mask Face Anti-Spoofing Database with Real World Variations. In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, Las Vegas, NV, USA, 26 June–1 July 2016; pp. 1551–1557. [CrossRef]
87. Li, X.; Wan, J.; Jin, Y.; Liu, A.; Guo, G.; Li, S.Z. 3DPC-Net: 3D Point Cloud Network for Face Anti-spoofing. In Proceedings of the IJCB 2020—IEEE/IAPR International Joint Conference on Biometrics, Houston, TX, USA, 28 September–1 October 2020. [CrossRef]
88. Xu, Z.; Li, S. Learning temporal features using LSTM-CNN architecture for face. In Proceedings of the 2015 IAPR Asian Conference on Pattern Recognition, Kuala Lumpur, Malaysia, 3–6 November 2015; pp. 141–145.
89. Thepade, S.; Jagdale, P.; Bhingurde, A.; Erandole, S. Novel Face Liveness Detection Using Fusion of Features and Machine Learning Classifiers. In Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies, ICIoT, Doha, Qatar, 2–5 February 2020; pp. 141–145. [CrossRef]
90. Manjani, I.; Tariyal, S.; Vatsa, M.; Singh, R.; Majumdar, A. Detecting Silicone Mask-Based Presentation Attack via Deep Dictionary Learning. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 1713–1723. [CrossRef]
91. Jia, S.; Hu, C.; Guo, G.; Xu, Z. A Database for Face Presentation Attack Using Wax Figure Faces. In Proceedings of the Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Trento, Italy, 9–10 September 2019; pp. 39–47. [CrossRef]
92. Sun, W.; Song, Y.; Chen, C.; Huang, J.; Kot, A.C. Face Spoofing Detection Based on Local Ternary Label Supervision in Fully Convolutional Networks. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3181–3196. [CrossRef]
93. Bhattacharjee, S.; Marcel, S. What You Can't See Can Help You—Extended-Range Imaging for 3D-Mask Presentation Attack Detection. In Proceedings of the 2017 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 20–22 September 2017; pp. 1–7. [CrossRef]
94. Liu, Y.; Jourabloo, A.; Liu, X. Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision. In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA, 18–23 June 2018. [CrossRef]

95. Ito, K.; Kimura, A.; Aoki, T. Performance Evaluation of Face Anti-Spoofing Method Using Deep Metric Learning from a Few Frames of Face Video. In Proceedings of the 2020 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, APSIPA ASC 2020, Auckland, New Zealand, 7–10 December 2020; pp. 1414–1419.
96. Li, X.; Wu, W.; Li, T.; Su, Y.; Yang, L. Face Liveness Detection Based on Parallel CNN. *J. Phys. Conf. Ser.* **2021**, *1549*, 042069. [CrossRef]
97. Liu, A.; Tan, Z.; Wan, J.; Escalera, S.; Guo, G.; Li, S.Z. CASIA-SURF CeFA: A Benchmark for Multi-modal Cross-ethnicity Face Anti-spoofing. In Proceedings of the 2021 IEEE Winter Conference on Applications of Computer Vision (WACV), Waikoloa, HI, USA, 3–7 January 2021; pp. 1178–1186. [CrossRef]
98. Liu, A.; Tan, Z.; Li, X.; Wan, J.; Escalera, S.; Guo, G.; Li, S.Z. Static and dynamic fusion for multi-modal cross-ethnicity face anti-spoofing. *arXiv* **2019**, arXiv:Abs/1912.0, 2019.
99. Liu, A.; Zhao, C.; Yu, Z.; Wan, J.; Su, A.; Liu, X.; Tan, Z.; Escalera, S.; Xing, J.; Liang, Y.; et al. Contrastive Context-Aware Learning for 3D High-Fidelity Mask Face Presentation Attack Detection. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 2497–2507. [CrossRef]
100. Arashloo, S.R. Unseen Face Presentation Attack Detection Using Sparse Multiple Kernel Fisher Null-Space. *IEEE Trans. Circuits Syst. Video Technol.* **2021**, *31*, 4084–4095. [CrossRef]
101. Peixoto, B.; Michelassi, C.; Rocha, A. Face liveness detection under bad illumination conditions. In Proceedings of the 2011 18th IEEE International Conference on Image Processing, Brussels, Belgium, 11–14 September 2011; pp. 3557–3560. [CrossRef]
102. Hassanien, A.E. Advances in Intelligent Systems and Computing 723 Mohamed Mostafa Editors. In Proceedings of the the International Conference on Advanced Machine Learning Technologies and Applications (AMLTA2018) 2020, Cairo, Egypt, 22–24 February 2018.
103. Li, H.; Li, W.; Cao, H.; Wang, S.; Huang, F.; Kot, A.C. Unsupervised Domain Adaptation for Face Anti-Spoofing. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 1794–1809. [CrossRef]
104. Ghofrani, A.; Toroghi, R.M.; Tabatabaie, S.M. Attention-Based Face AntiSpoofing of RGB Camera using a Minimal End-2-End Neural Network. Iranian Conference on Machine Vision and Image Processing, MVIP. In Proceedings of the Iranian Conference on Machine Vision and Image Processing, MVIP, Qom, Iran, 18–20 February 2020. [CrossRef]
105. Liu, W.; Wei, X.; Lei, T.; Wang, X.; Meng, H.; Nandi, A.K. Data-Fusion-Based Two-Stage Cascade Framework for Multimodality Face Anti-Spoofing. *IEEE Trans. Cogn. Dev. Syst.* **2021**, *14*, 672–683. [CrossRef]
106. George, A.; Mostaani, Z.; Geissenbuhler, D.; Nikisins, O.; Anjos, A.; Marcel, S. Biometric Face Presentation Attack Detection With Multi-Channel Convolutional Neural Network. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 42–55. [CrossRef]
107. Amir Mohammadi, S.M.; Bhattacharjee, S. Domain Adaptation for Generalization of Face Presentation Attack Detection in Mobile Settengs with Minimal Information. In Proceedings of the ICASSP 2020–2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Barcelona, Spain, 4–8 May 2020; pp. 1001–1005. [CrossRef]
108. Nikisins, O.; George, A.; Marcel, S. Domain Adaptation in Multi-Channel Autoencoder based Features for Robust Face Anti-Spoofing. In Proceedings of the 2019 International Conference on Biometrics, ICB, Crete, Greece, 4–7 June 2019. [CrossRef]
109. Yu, Z.; Wan, J.; Qin, Y.; Li, X.; Li, S.Z.; Zhao, G. NAS-FAS: Static-Dynamic Central Difference Network Search for Face Anti-Spoofing. *IEEE Trans. Pattern Anal. Mach. Intell.* **2020**, *43*, 3005–3023. [CrossRef]
110. Komulainen, J.; Hadid, A.; Pietikainen, M. Face spoofing detection from single images using texture and local shape analysis. *IET Biom.* **2012**, *1*, 3–10. [CrossRef]
111. Boulkenafet, Z.; Komulainen, J.; Hadid, A. Face anti-spoofing based on color texture analysis. In Proceedings of the International Conference on Image Processing, ICIP, Bordeaux, France, 16–19 October 2015; Volume 2015, pp. 2636–2640. [CrossRef]
112. Lu, L.; Yu, J.; Chen, Y.; Liu, H.; Zhu, Y.; Liu, Y.; Li, M. LipPass: Lip Reading-based User Authentication on Smartphones Leveraging Acoustic Signals. In Proceedings of the IEEE INFOCOM, Honolulu, HI, USA, 16–19 April 2018; pp. 1466–1474. [CrossRef]
113. Singh, A.K.; Joshi, P.; Nandi, G.C. Face recognition with liveness detection using eye and mouth movement. In Proceedings of the 2014 International Conference on Signal Propagation and Computer Technology, ICSPCT, Rajasthan, India, 12–13 July 2014; pp. 592–597. [CrossRef]
114. Smiatacz, M. Liveness Measurements Using Optical Flow for Biometric Person Authentication. *Metrol. Meas. Syst.* **2012**, *19*, 257–268. [CrossRef]
115. Li, J.; Wang, Y.; Tan, T.; Jain, A.K. Live face detection based on the analysis of Fourier spectra. *Biom. Technol. Hum. Identif.* **2004**, *5404*, 296–304. [CrossRef]
116. Kollreider, K.; Fronthaler, H.; Bigun, J. Non-intrusive liveness detection by face images. *Image Vis. Comput.* **2009**, *27*, 233–244. [CrossRef]
117. Ning, X.; Li, W.; Wei, M.; Sun, L.; Dong, X. Face Anti-spoofing based on Deep Stack Generalization Networks. In Proceedings of the 7th International Conference on Pattern Recognition Applications and Methods—ICPRAM 2018, Funchal, Portugal, 16–18 January 2018; pp. 317–323. [CrossRef]
118. Li, L.; Feng, X.; Boulkenafet, Z.; Xia, Z.; Li, M.; Hadid, A. An original face anti-spoofing approach using partial convolutional neural network. In Proceedings of the 2016 6th International Conference on Image Processing Theory, Tools and Applications, IPTA, Oulu, Finland, 12–15 December 2016. [CrossRef]
119. Tirunagari, S.; Poh, N.; Windridge, D.; Iorliam, A.; Suki, N.; Ho, A.T.S. Detection of Face Spoofing Using Visual Dynamics. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 762–777. [CrossRef]

120. Liu, S.-Q.; Lan, X.; Yuen, P.C. Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection. In *Computer Vision—ECCV 2018. ECCV 2018. Lecture Notes in Computer Science*; Ferrari, V., Hebert, M., Sminchisescu, C., Weiss, Y., Eds.; Springer: Cham, Swizterland, 2018; Volume 11220, pp. 577–594. [CrossRef]
121. Yang, J.; Lei, Z.; Li, S.Z. Learn Convolutional Neural Network for Face Anti-Spoofing. 2014. Available online: https://arxiv.org/abs/1408.5601 (accessed on 15 September 2022).
122. Wang, G.; Han, H.; Shan, S.; Chen, X. Unsupervised Adversarial Domain Adaptation for Cross-Domain Face Presentation Attack Detection. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 56–69. [CrossRef]
123. Wang, Z.; Zhao, C.; Qin, Y.; Zhou, Q.; Qi, G.; Wan, J.; Lei, Z. Exploiting Temporal and Depth Information for Multi-Frame Face Anti-Spoofing. 2018. Available online: https://arxiv.org/abs/1811.05118 (accessed on 10 October 2022).
124. 3D Mask Face Anti-Spoofing with Remote Photoplethysmography. Available online: https://doi.org/10.1007/978-3-319-46478-7_6 (accessed on 10 October 2022).
125. Li, H.; Wang, S.; Kot, A.C. Face spoofing detection with image quality regression. In Proceedings of the 2016 6th International Conference on Image Processing Theory, Tools and Applications, IPTA, Oulu, Finland, 12–15 December 2016. [CrossRef]
126. Singh, A.K.; Joshi, P.; Nandi, G. Face liveness detection through face structure analysis. *Int. J. Appl. Pattern Recognit.* **2014**, *1*, 338–360. [CrossRef]
127. George, A.; Marcel, S. Deep Pixel-wise Binary Supervision for Face Presentation Attack Detection. In Proceedings of the 2019 International Conference on Biometrics, ICB, Crete, Greece, 4–7 June 2019. [CrossRef]
128. Jatain, R.; Jailia, M. Authentication and Facial Expression Analysis System using Deep Transfer Learning Approach. In Proceedings of the 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), Tamil Nadu, India, 29–31 March 2022; pp. 1209–1214. [CrossRef]
129. Muhammad, U.; Yu, Z.; Komulainen, J. Self-supervised 2D face presentation attack detection via temporal sequence sampling. *Pattern Recognit. Lett.* **2022**, *156*, 15–22. [CrossRef]
130. Li, Z.; Cai, R.; Li, H.; Lam, K.-Y.; Hu, Y.; Kot, A.C. One-Class Knowledge Distillation for Face Presentation Attack Detection. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 2137–2150. [CrossRef]
131. Li, H.; He, P.; Wang, S.; Rocha, A.; Jiang, X.; Kot, A.C. Learning Generalized Deep Feature Representation for Face Anti-Spoofing. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2639–2652. [CrossRef]
132. Zhou, F.; Gao, C.; Chen, F.; Li, C.; Li, X.; Yang, F.; Zhao, Y. Face Anti-Spoofing Based on Multi-layer Domain Adaptation. In Proceedings of the 2019 IEEE International Conference on Multimedia & Expo Workshops, Shanghai, China, 8–12 July 2019; pp. 192–197. [CrossRef]
133. Qin, Y.; Zhang, W.; Shi, J.; Wang, Z.; Yan, L. One-class adaptation face anti-spoofing with loss function search. *Neurocomputing* **2020**, *417*, 384–395. [CrossRef]
134. Sun, W.; Song, Y.; Zhao, H.; Jin, Z. A Face Spoofing Detection Method Based on Domain Adaptation and Lossless Size Adaptation. *IEEE Access* **2020**, *8*, 66553–66563. [CrossRef]
135. Liu, Y.; Liu, X. Physics-Guided Spoof Trace Disentanglement for Generic Face Anti-Spoofing. *arXiv* **2020**, *14*, 1–16. Available online: https://arxiv.org/abs/2012.05185 (accessed on 12 November 2022).
136. Jia, Y.; Zhang, J.; Shan, S.; Chen, X. Single-Side Domain Generalization for Face Anti-Spoofing. In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Washington, DC, USA, 16–18 June 2020; pp. 8481–8490. [CrossRef]
137. Saha, S.; Xu, W.; Kanakis, M.; Georgoulis, S.; Chen, Y.; Paudel, D.P.; Van Gool, L. Domain Agnostic Feature Learning for Image and Video Based Face Anti-spoofing. *IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops* **2020**, *2020*, 3490–3499. [CrossRef]
138. Tu, X.; Ma, Z.; Zhao, J.; Du, G.; Xie, M.; Feng, J. Learning Generalizable and Identity-Discriminative Representations for Face Anti-Spoofing. *ACM Trans. Intell. Syst. Technol.* **2020**, *11*, 5. [CrossRef]
139. Deb, D.; Jain, A.K. Look Locally Infer Globally: A Generalizable Face Anti-Spoofing Approach. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 1143–1157. [CrossRef]
140. Kotwal, K.; Bhattacharjee, S.; Abbet, P.; Mostaani, Z.; Wei, H.; Wenkang, X.; Yaxi, Z.; Marcel, S. Domain-Specific Adaptation of CNN for Detecting Face Presentation Attacks in NIR. *IEEE Trans. Biom. Behav. Identit Sci.* **2022**, *4*, 135–147. [CrossRef]
141. Perez-Cabo, D.; Jimenez-Cabello, D.; Costa-Pazo, A.; Lopez-Sastre, R.J. Deep Anomaly Detection for Generalized Face Anti-Spoofing. *IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognition. Work.* **2019**, 1591–1600. [CrossRef]
142. Li, Z.; Li, H.; Lam, K.-Y.; Kot, A.C. Unseen Face Presentation Attack Detection with Hypersphere Loss. In Proceedings of the ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing, Barcelona, Spain, 4–8 May 2020; Volume 2020, pp. 2852–2856. [CrossRef]
143. Koshy, R.; Mahmood, A. Enhanced Deep Learning Architectures for Face Liveness Detection for Static and Video Sequences. *Entropy* **2020**, *22*, 1186. [CrossRef]
144. Fatemifar, S.; Arashloo, S.R.; Awais, M.; Kittler, J. Client-specific anomaly detection for face presentation attack detection. *Pattern Recognit.* **2021**, *112*, 107696. [CrossRef]
145. Nikisins, O.; Mohammadi, A.; Anjos, A.; Marcel, S. On Effectiveness of Anomaly Detection Approaches against Unseen Presentation Attacks in Face Anti-spoofing. In Proceedings of the 2018 International Conference on Biometrics, ICB, Gold Coast, Australia, 20–23 February 2018; pp. 75–81. [CrossRef]

146. Baweja, Y.; Oza, P.; Perera, P.; Patel, V.M. Anomaly Detection-Based Unknown Face Presentation Attack Detection. In Proceedings of the IJCB 2020—IEEE/IAPR International Joint Conference on Biometrics, Houston, TX, USA, 28 September–1 October 2020. [CrossRef]
147. Shao, R.; Perera, P.; Yuen, P.C.; Patel, V.M. Federated Generalized Face Presentation Attack Detection. *Comput. Vis. Pattern Recognit.* **2021**, *14*, 1–13. Available online: https://arxiv.org/abs/2104.06595 (accessed on 22 November 2022). [CrossRef]
148. Nguyen, D.T.; Pham, T.D.; Batchuluun, G.; Noh, K.J.; Park, K.R. Presentation Attack Face Image Generation Based on a Deep Generative Adversarial Network. *Sensors* **2020**, *20*, 1810. [CrossRef] [PubMed]
149. Liu, A.; Tan, Z.; Wan, J.; Liang, Y.; Lei, Z.; Guo, G.; Li, S.Z. Face Anti-Spoofing via Adversarial Cross-Modality Translation. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 2759–2772. [CrossRef]
150. Wang, J.; Zhang, J.; Bian, Y.; Cai, Y.; Wang, C.; Pu, S. Self-Domain Adaptation for Face Anti-Spoofing. *Proc. Conf. AAAI Artif. Intell.* **2021**, *35*, 2746–2754. [CrossRef]
151. Jia, Y.; Zhang, J.; Shan, S. Dual-Branch Meta-Learning Network with Distribution Alignment for Face Anti-Spoofing. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 138–151. [CrossRef]
152. Cai, R.; Li, Z.; Wan, R.; Li, H.; Hu, Y.; Kot, A.C. Learning Meta Pattern for Face Anti-Spoofing. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 1201–1213. [CrossRef]
153. Perez-Cabo, D.; Jimenez-Cabello, D.; Costa-Pazo, A.; Lopez-Sastre, R.J. Learning to Learn Face-PAD: A lifelong learning approach. In Proceedings of the 2020 IEEE International Joint Conference on Biometrics (IJCB), Houston, TX, USA, 28 September–1 October 2020; pp. 1–9. [CrossRef]