Pegem Journal of Education and Instruction, Vol. 13, No. 4 , 2023 (pp. 624-643)

RESEARCH ARTICLE WWW.PEGEGOG.NET

FACE SPOOFING DETECTION BASED ON MULTI-SCALE COLOR INVERSION DUAL-STREAM CONVOLUTIONAL NEURAL NETWORK

B.Prashanthi[1], Aluri Harshitha [2], Sharanya Deekonda[3],Likhitha[4]

[1] Assistant Professor, Department of Information Technology, Sridevi Women's Engineering College, Hyderabad
teachingprashanthi@gmail.com

[2, 3, 4] Department of Information Technology, Sridevi Women's Engineering College,
Hyderabad

ABSTRACT Facial recognition technology (FRT) is becoming standard issue. Face spoofing detection (also known as face liveness detection or face anti-spoofing) technology has been developed in response to the extraordinary issues faced by FRT as a result of the misuse of personal face images on social media. Low accuracy and generalizability may be issues with traditional face spoofing detection algorithms since they often rely on manually extracted attributes to differentiate between actual and phony faces. Moreover, changes in light impact the efficacy of current approaches. In order to tackle these problems, we provide MSCI-DSCNN, a multi-scale color inversion dual-stream convolutional neural network. Before feeding the MSCI photos into the enhanced MobileNet to extract face reflection features, one stream of the suggested model grayscales the input RGB images and performs multi-scale color inversion to get the MSCI images. In order to extract face color characteristics, the enhanced MobileNet is fed RGB photos straight from the other stream of the network. At last, face spoofing detection makes use of the combined characteristics obtained from the two branches. Results from our evaluation of the suggested framework on CASIA-FASD, REPLAY-ATTACK, and OULU-NPU—three datasets that are open to the public—are encouraging. Our MSCI-DSCNN technique is shown to be very successful in large cross-database studies, which further assess the generalization capabilities of the proposed strategy.

KEYWORDS: Face spoofing detection, Anti-spoofing, CASIA-FASD, REPLAY-ATTACK, Convolutional neural network.

1. INTRODUCTION

In order to verify an individual's identification, most modern electronic device systems employ facial recognition technology, while other biometrics like fingerprints and iris scans are also often used. As useful as facial recognition apps are in our everyday lives, they also provide hackers with chances to steal sensitive data from law-abiding citizens (Birla & Gupta, 2022). It is possible for criminals to bypass facial recognition systems by obtaining user-posted personal images and presenting them to face

How to cite this article: B.Prashanthi1, Aluri Harshitha 2, Sharanya Deekonda3,Likhitha4. FACE SPOOFING DETECTION BASED ON MULTI-SCALE COLOR INVERSION DUAL-STREAM CONVOLUTIONAL NEURAL NETWORK
.Pegem Journal of Education and Instruction, Vol. 13, No. 4, 2023, 624-643
Source of support: Nil **Conflicts of Interest:** None.
DOI: 10.48047/pegegog.13.04.74
Received: 12.10.2023
Accepted: 22.11.2023 **Published:** 24.12.2023

capture equipment. Consequently, research into technologies that can identify face spoofing has exploded in popularity, with studies cited from both academics and businesses (Chang and Yeh, 2022; Rehman et al., 2020). Unauthorized users may compromise facial recognition systems in three primary ways: print, replay, and mask attacks (Yan et al., 2022). The term "print attack" describes the practice of printing out user images with their consent in order to trick facial recognition systems into thinking they are someone else. A replay attack occurs when an attacker uses a mobile device to show a video of themselves in an attempt to fool a face certification system. When perpetrators use 3D masks to fool facial recognition software, they are committing a mask assault. The primary goals of this paper's study are print and replay assaults, which are the most popular attack techniques because to their cheap cost and ease of execution. As a pre-processing step in a face recognition system, face spoofing detection (or face liveness detection) is often used to confirm the authenticity of the collected face picture. Consequently, detecting face faking is often seen as a task involving binary classification. Some of the most common approaches to traditional face spoofing detection rely on physiological data or texture analysis. Since the secondary imaging medium's texture characteristics vary from the actual face's, texture-based approaches take this into account. Face spoofing detection methods that rely on LBP, HOG, and DOG to extract hand-crafted features often have limited cross-dataset generalizability (Chen et al., 2019, Chingovska et al., 2012, Shu et al., 2021, 2022), according to publications such as Komulainen et al. (2012), Yang et al. (2013), and Zhang et al. (2012). Though computationally demanding, physiologically-based approaches mainly use motion characteristics such eye blinks (Pan et al., 2007) and mouth movements (Kollreider et al., 2007) as important signals to differentiate between genuine and synthetic faces. deep learning-based techniques, in contrast to conventional methods' low-level representation of hand-crafted features, may extract high-level semantic feature expressions. These approaches are primarily categorized into two types: methods based on single disparity cues and methods based on multiple disparity cues. Image quality, rPPG, spatial-temporal information, and other signals are all part of the picture. Because issues including color distribution distortion, haziness, the Moire effect, and other similar issues might arise from secondary imaging of artificial faces, techniques based on image quality have been suggested (Li, Feng, Boulkenafet, Xia, & Li, 2016). This sort of approach often requires very high-quality input photos and isn't very good at distinguishing between various types of false faces across datasets. Although rPPG-based approaches enhance detection performance by integrating rPPG signals with neural network characteristics (Hernandez-Ortega et al., 2018), they are light-sensitive and need stable lighting. By combining geographical and temporal data, approaches based on spatial-temporal information may identify face spoofing (Asim et al., 2017), which in turn improves the capacity to withstand print and replay assaults. The number of parameters and calculation costs are significantly raised due to the use of two characteristics in this kind of procedure. There are still issues with face spoofing detection, despite the many suggested approaches. These include a high number of parameters, light sensitivity, and low generalizability across datasets. A study of Retinex theory prompted the issue of lighting conditions. We present a multi-scale color inversion dual-stream convolutional neural network (MSCI-DSCNN) with an MSCI stream and an RGB stream to solve the aforementioned problems. The face color characteristics are extracted using the RGB stream, while the reflection features are extracted using the MSCI stream. In the end, face anti-spoofing is achieved by adaptively integrating these two types of traits. Here are the key points from this paper:

(1) To enhance the accuracy of face spoofing detection, a multi-scale color inversion algorithm is suggested. (2) To further enhance the MobileNet, a paralleled convolutional block attention module (PCBAM) is designed and integrated into the improved MobileNet.

(3) The method has been thoroughly tested in three publicly available databases, and the experimental results demonstrate the effectiveness of MSCI-DSCNN. Furthermore, we also do cross-database testing and get good results, which means the proposed MSCI-DSCNN is

very generalizable. Conventional approaches that rely on ML

Face spoofing detection in traditional approaches, such as those based on texture and physiological information, often makes use of characteristics that are hand-crafted. To start with, Chingovska et al. (2012) investigated the impact of texture features based on local binary pattern (LBP) on three different kinds of assaults, specifically addressing texture feature-based approaches. A method was suggested by Zhang et al. (Zhang & Xiang, 2020) to link the LBP histograms of the discrete wavelet transform (DWT) blocks horizontally.

2. MATERIALS AND METHODS:

Face anti-spoofing (FAS) has lately attracted increasing attention due to its vital role in securing face recognition systems from presentation attacks (PAs). As more and more realistic PAs with novel types spring up, early-stage FAS methods based on handcrafted features become unreliable due to their limited representation capacity. With the emergence of large-scale academic datasets in the recent decade, deep learning based FAS achieves remarkable performance and dominates this area. However, existing reviews in this field mainly focus on the handcrafted features, which are outdated and uninspiring for the progress of FAS community. In this paper, to stimulate future research, we present the

first comprehensive review of recent advances in deep learning based FAS. It covers several novel and insightful components: 1) besides supervision with binary label (e.g., _0‘ for bonafide versus _1‘ for PAs), we also investigate recent methods with pixel-wise supervision (e.g., pseudo depth map); 2) in addition to traditional intra-dataset evaluation, we collect and analyze the latest methods specially designed for domain generalization and open-set FAS; and 3) besides commercial RGB camera, we summarize the deep learning applications under multi-modal (e.g., depth and infrared) or specialized (e.g., light field and flash) sensors. We conclude this survey by emphasizing current open issues and highlighting potential prospects.

DUE to its convenience and remarkable accuracy, face recognition technology [1] has been applied in a few interactive intelligent applications such as checking-in and mobile payment. However, existing face recognition systems are vulnerable to presentation attacks (PAs) ranging from print, replay, makeup, 3D-mask, etc. Therefore, both academia and industry have paid extensive attention to developing face anti-spoofing (FAS) technology for securing the face recognition system. As illustrated in Fig. 1, FAS (namely _face presentation attack detection‘ or _face livenessdetection‘) is an active research topic in computer vision and has received an increasing number of publications in recent years. In the early stage, plenty of traditional handcrafted feature [2], [3], [4], [5], [6] based methods have been proposed for presentation attack detection (PAD). Most traditional algorithms are designed based on human liveness cues and handcrafted features, which need rich task-aware prior knowledge for design.

In term of the methods based on the liveness cues, eye-blinking [2], [7], [8], face and head movement [9], [10] (e.g., nodding and smiling), gaze tracking [11], [12] and remote physiological signals (e.g., rPPG [3], [13], [14], [15]) are explored for dynamic discrimination. However, these physiological liveness cues are usually captured from long-term interactive face videos, which is inconvenient for practical deployment. Furthermore, the liveness cues are easily mimicked by video attacks, making them less reliable. On the other hand, classical handcrafted descriptors (e.g., LBP [4], [16], SIFT [6], SURF [17], HOG

[5] and DoG [18]) are designed for extracting effective spoofing patterns from various color spaces (RGB, HSV, and YCbCr). It can be seen from Table-A 1 (in Appendix), available online, that the FAS surveys before 2018 mainly focus on this category. Subsequently, a few hybrid (handcrafted+deep learning) [19], [20], [21], [22] and end-to-end deep learning based methods [13], [23], [24], [25], [26], [27], [28] are proposed for both static and dynamic face

PAD. Most works [29], [30], [31], [32], [33], [34], [35] treat FAS as a binary classification problem (e.g., _0‘ for live while _1‘ for spoofing faces, or vice versa) thus supervised by a simple binary cross-entropy loss. Different from other binary vision tasks, the FAS is a self-evolving problem (i.e., attack versus defense develop iteratively), which makes it more challenging. Furthermore, other binary vision tasks (e.g., human gender classification) highly rely on the obvious.

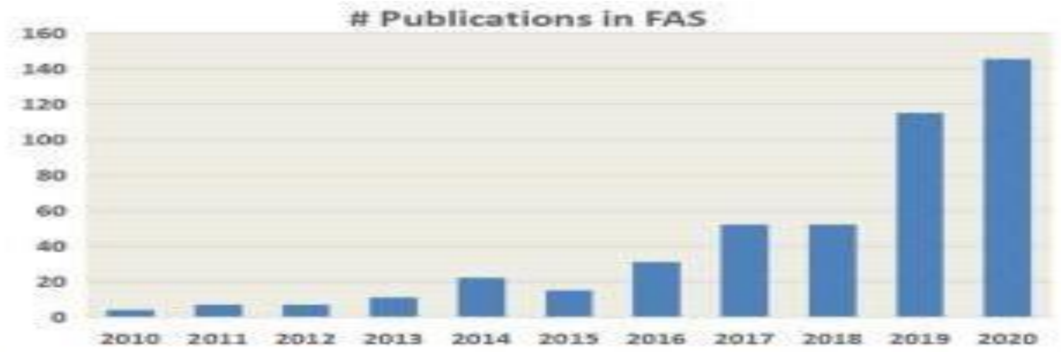


Fig. 1. The increasing research interest in the FAS field, obtained through Google scholar search with key-words: allintitle: "face anti-spoofing", "face presentation attack detection", and "face liveness detection".

appearance-based semantic clues (e.g., hair style, wearing, facial shape) while the intrinsic features (e.g., material and geometry) in FAS are usually content-irrelevant (e.g., not related to facial attribute and ID), subtle and with finegrained details, which are very challenging to distinguish by even human eyes. Thus, convolutional neural networks (CNNs) with single binary loss might reasonably mine different kinds of semantic features for binary vision tasks like gender classification but discover arbitrary and unfaithful clues (e.g., screen bezel) for spoofing patterns. Fortunately, such intrinsic live/spoof clues are usually closely related with some position-aware auxiliary tasks. For instance, the face surface of print/replay and transparent mask attacks are usually with irregular/limited geometric depth distribution and abnormal reflection, respectively.

Based on these physical evidences, recently, pixel-wise supervision [13], [24], [26], [32], [36], [37] attracts more attention as it provides more fine-grained context-aware supervision signals, which is beneficial for deep models learning intrinsic spoofing cues. On one hand, pseudo depth labels [13], [26], reflection maps [24], [36], binary mask label [32], [38], [39] and 3D point cloud maps [40] are typical pixel-wise auxiliary supervisions, which describe the local live/spoof cues in pixel/patch level. On the other hand, besides physical-guided auxiliary signals, a few generative deep FAS methods model the intrinsic spoofing patterns via relaxed pixel-wise reconstruction constraints [33], [41], [42], [43].

As shown in Table-A 1 (in Appendix), available in the online supplemental material, the latest FAS surveys from 2018 to 2020 investigate limited numbers of deep learning based methods, which hardly provide comprehensive elaborations for the community researchers. Note that most datadriven methods introduced in previous surveys are supervised by traditional binary loss, and there is still a blank for summarizing the arisen pixel-wise supervision methods. Meanwhile, the emergence of large-scale public FAS datasets with rich attack types and recorded sensors also greatly boosts the research community. First, the datasets with vast samples and subjects have been released. For instance, CelebA-Spoof [44], recorded from 10177 subjects, contains 156384 and 469153 face images for bonafide and PAs, respectively. Second, besides the common PA types (e.g., print and replay attacks), some up-to-date datasets contain richer challenging PA types (e.g., SiW-M [38] and

WMCA [45] with more than 10 PA types). However, we can find from Table-A 1 (in Appendix), available in the online supplemental material, that existing surveys only investigate a handful of old and small-scale FAS datasets, which cannot provide fair benchmarks for deep learning based methods. Third, in terms of modality and hardware for recording, besides commercial visible RGB camera, numerous multimodal and specialized sensors benefit the FAS task. For example, CASIA-SURF [28] and WMCA [45] show the effectiveness of PAD via fusing RGB/depth/NIR information while dedicated systems with multispectral SWIR [46] and four-directional polarized [47] cameras significantly benefit for spoofing material perception. However, previous surveys mostly focus on single RGB modality using a commercial visible camera, and neglect the deep learning applications on the multimodal and specialized systems for high-security scenarios.

From the perspective of evaluation protocols, traditional _intra-dataset intra-type‘ and _cross-dataset intra-type‘ protocols are widely investigated in previous FAS surveys (see Table-A 1 in Appendix, available in the online supplemental material). As FAS is actually an open-set problem in practice, the uncertain gaps (e.g., environments and attack types) between training and testing conditions should be considered. However, no existing reviews consider the issues about unseen domain generalization [48], [49], [50], [51] and unknown PAD [38], [52], [53], [54]. Most reviewed FAS methods design or train the FAS model on predefined scenarios and PAs. Thus, the trained models easily overfit on several specific domains and attack types, and are vulnerable to unseen domains and unknown attacks. To bridge the gaps between academic research and real-world applications, in this paper, we fully investigate deep learning based methods under four FAS protocols, including challenging domain generalization and open-set PAD situations. Compared with existing literatures, the major contributions of this work can be summarized as follows: To the best of our knowledge, this is the first survey paper to comprehensively cover deep learning methods for both single- and multi-modal FAS with generalized protocols.

Compared with previous surveys only considering the methods with binary loss supervision, we also elaborate on those with auxiliary/generative pixel-wise supervision. As opposed to existing reviews [56], [57], [58] with only limited numbers of small-scale datasts, we show detailed comparisons among past-to-present 35 public datasets including various kinds of PAs as well as advanced recording sensors. This paper covers the most recent and advanced progress of deep learning on four practical FAS protocols (i.e., intra-dataset intra-type, cross-dataset intratype, intra-dataset cross-type, and cross-dataset crosstype testings). Therefore, it provides the readers with state-of-the-art methods with different application scenarios (e.g., unseen domain generalization and unknown attack detection). Comprehensive comparisons of existing deep FAS methods with insightful taxonomy are provided in Tables-A 5, 6, 7, 8, 9, 10, and 11 (in Appendix),

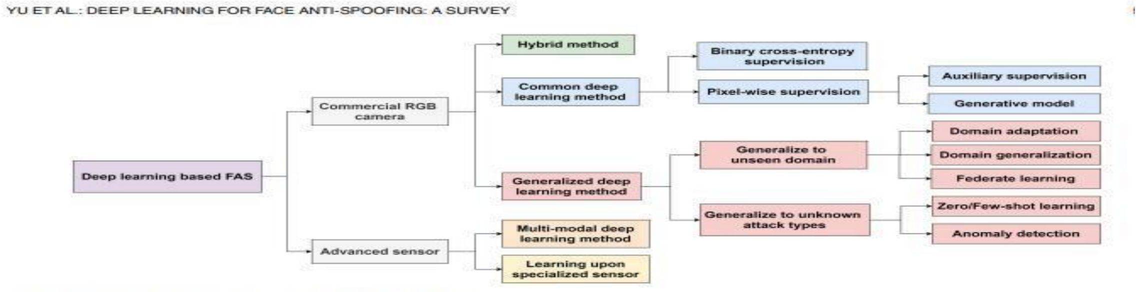

YU ET AL.: DEEP LEARNING FOR FACE ANTI-SPOOFING: A SURVEY
Deep learning based FAS
Commercial RGB camera
Advanced sensor
Hybrid method
Common deep learning method
Generalized deep learning method
Multi-modal deep learning method
Learning upon specialized sensor
Binary cross-entropy supervision
Pixel-wise supervision
Generalize to unseen domain
Generalize to unknown attack types
Auxiliary supervision
Generative model
Domain adaptation
Domain generalization
Federate learning
Zero/Few-shot learning
Anomaly detection

Fig. 2. Topology of the deep learning based FAS methods.

available in the online supplemental material, with brief summaries and discussions being presented. We summarize the topology of deep learning based FAS methods with the commercial monocular RGB camera and advanced sensors in Fig. 2. On one hand, as commercial RGB camera is widely used in many real-world applicational scenarios (e.g., access control system and mobile device unlocking), there are richer research works based on this branch. It includes three main categories: 1) hybrid learning methods combining both handcrafted and deep learning features; 2) traditional end-to-end supervised deep learning based methods; and 3) generalized deep learning methods to both unseen domain and unknown attack types. Besides the commercial RGB camera, researchers have also developed sensor-aware deep learning methods for efficient FAS using specialized sensors/hardwares. Meanwhile, as multi-spectrum imaging systems with acceptable costs are increasingly used in realworld applications, multi-modal deep learning based methods become hot and active in the FAS research community.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. 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. 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.The widespread deployment of facial recognition-based biometric systems has made facial presentation attack detection (face anti-spoofing) an increasingly critical issue. This survey thoroughly investigates facial Presentation Attack Detection (PAD) methods that only require RGB cameras of generic consumer devices over the past two decades. We present an attack scenario-oriented typology of the existing facial PAD methods, and we provide a review of over 50 of the most influenced facial PAD methods over the past two decades till today and their related issues. We adopt a comprehensive presentation of the reviewed facial PAD methods following the proposed typology and in chronological order. By doing so, we

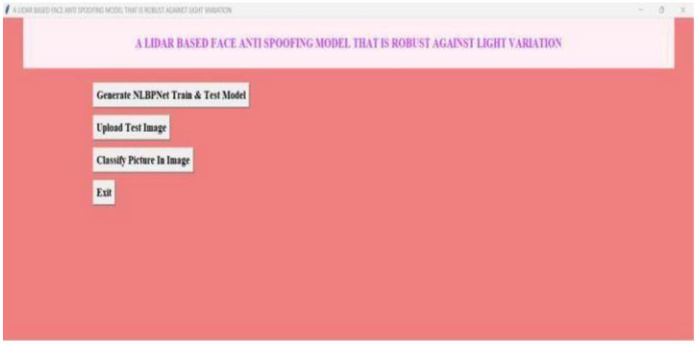
depict the main challenges, evolutions and current trends in the field of facial PAD and provide insights on its future research. From an experimental point of view, this survey paper provides a summarized overview of the available public databases and an extensive comparison of the results reported in PAD-reviewed papers.In the past two decades, the advancement of technology in electronics and computer science has provided access to top-level technology devices at affordable prices to an important proportion of the world population. Various biometric systems have been widely deployed in real-life applications, such as online payment and e-commerce security, smartphone-based authentication, secured access control, biometric passport and border checks. Facial recognition is among the most studied biometric technologies since the 90s [1], mainly for its numerous advantages compared to other biometrics. Indeed, faces are highly distinctive among individuals and facial recognition can be implemented even in nonintrusive acquisition scenarios or from a distance.Recently, deep learning has dramatically improved the state-of-the-art performance of many computer vision tasks, such as image classification and object recognition [2,3,4]. With these significant progresses, facial recognition has also made great breakthroughs such as the success of DeepFace [5], DeepIDs [6], VGG Face [7], FaceNet [8], SphereFace [9] and ArcFace [10]. One of these spectacular breakthroughs occurred between 2014 and 2015, when multiple groups [5,8,11] approached and then surpassed human-level recognition accuracy on very challenging face benchmarks, such as Labeled Faces in the Wild (LFW) [12] or YouTube Faces (YTF) [13]. Thanks to their convenience, excellent performances and great security levels, facial recognition systems are among the most widespread biometric systems in the market compared to other biometrics such as iris and fingerprint recognition [14].However, given facial authentication systems‘ popularity, they became primary targets of Presentation Attacks (PAs) [15]. PAs are performed by malicious or ill-intentioned users who either aim at impersonating someone else‘s identity (impersonation attack) or at avoiding being recognized by the system (obfuscation attack). However, compared to face recognition performances, the vulnerabilities of facial authentication systems to PAs have been much less studied.The main objective of this paper is to present a detailed review of face PAD methods that are crucial for assessing the vulnerability/robustness of current facial recognition-based systems towards ill-intentioned users. Given the prevalence of biometric applications based on facial authentication, such as online payment, it is crucial to protect genuine users against impersonation attacks in real-life scenarios. In this survey paper, we will focus more on impersonation detection. However, at the end of the paper, we will discuss obfuscation detection as well.A face-based authentication system has become an important topic in various fields of IoT applications such as identity validation for social care, crime detection, ATM access, computer security, etc. However, these authentication systems are vulnerable to different attacks. Presentation attacks have become a clear threat for facial biometric-based authentication and security applications. To address this issue, we proposed a deep learning approach for face spoofing detection systems in IoT cloud-based environment. The deep learning approach extracted features from multicolor space to obtain more information from the input face image regarding luminance and chrominance data. These features are combined and selected by the Minimum Redundancy Maximum Relevance (mRMR) algorithm to provide an efficient and discriminate feature set. Finally, the extracted deep color-based features of the face image are used for face spoofing detection in a cloud environment. The proposed method achieves stable results with less training data compared to conventional deep learning methods. This advantage of the proposed approach reduces the time of processing in the training phase and optimizes resource management in storing training data on the cloud. The proposed system was tested and evaluated based on two challenging public access face spoofing databases, namely, Replay-Attack and ROSE-Youtu. The experimental results based on these databases showed that the proposed method achieved satisfactory results compared to the state-of-the-art methods based on an equal error rate (EER) of 0.2% and 3.8%, respectively, for the Replay-Attack and ROSE-Youtu databases. Nowadays, the Internet of Things (IoT) affects human lives in a wide range of technology from smart homes to smart cities. An enormous number of IoT devices are utilized for collecting and analyzing information for different reasons, such as healthcare, security, and management. According to the estimation of scientifics, around 90% of storing data would be useless [1]. Therefore, the researchers proposed [1] utilizing the edge devices in the architecture of applications or services for cloud computing. In this way, the data can be analyzed and filtered in edge devices and send more enhanced data for processing in the cloud. For example, the deployed sensors for traffic monitoring can be also utilized for fire detection with low-cost and low-performance devices. However, IoT-based systems are faced with different problems such as security threats from the Internet. For instance, let us consider an IoT-based healthcare application which contains critical information such as blood sugar level and blood pressure. The authentication system for data communication through wireless channels should be secured for protecting critical information of clients. Biometric authentication can be utilized for identifying a person in wireless communication. This authentication requires using personal attributes, such as speech, face, fingerprints, palmprint, gait, and iris [2]. This kind of authentication is based on a comparison between the physical aspect of the client that is collected with the help of different sensors and a copy that was stored. The physiological information of clients is more reliable when compared to knowledge-based or token-based methods because this information is unique and not shareable. For this reason, IoT-based cloud computing systems for authentication of clients applied their biometric information. For instance, Kumari and Thangaraj [3] proposed a feature selection technique in biometric authentication using a cloud framework. In another similar study, Shakil et al. [4] proposed a biometric authentication system and data management application for security of healthcare data in the cloud. Also, Vidya and Chandra [5] proposed a multimodal biometric authentication system based on entropy-based local binary pattern feature description technique for cloud computing. Additionally, Masud et al. [6] proposed a deep learning-based approach for face recognition in IoT environments. Face recognition systems have achieved significant interest in many applications such as cell phones‘ and laptops‘ authentication or registration systems at places such as online exam centers and airports [1]. These kinds of security systems in the Big Data analytics platform are a topic of concern for real-time applications. Consider the scenario when a person is to be recognized in an airport for registration or a student is attending an online exam. In these scenarios and other similar conditions, the camera captures images of the face continuously and sends these data for processing in the cloud environment. Based on meaningful information of face image, a certain person can easily be identified. Nevertheless, these kinds of authentication and registration systems are vulnerable to different types of attacks. For improving the security of biometric authentication systems, various methods and models are proposed. For example, Ali et al. [1] proposed a multimodal biometric authentication system using an encryption method for protecting the privacy of biometric information in the IoT-based cloud environment. In another study, Gomez-Barrero et al. [2] proposed a framework for the protection of the privacy of multibiometric templates with an encryption method. However, the aforementioned methods are designed for protection based on man-in-the-middle attacks in wireless communication. According to the literature, face spoofing attacks in IoT cloud environments are not discussed and studied yet. The main objective of this study is to present an IoT cloud-based framework for protecting client‘s information from face spoofing attacks. In a face spoofing attack, the intruder bypasses the authentication system by presenting a fake face of the victim. Due to this threat, robust and stable face Presentation Attack Detection (PAD) methods must be developed and designed. Face spoofing attacks may be classified into four main groups: print, display, replay, and mask attacks [7]. According to the types of sensors for detection of these kinds of attacks, different algorithms are proposed [9–11]. Generally, light field camera sensors are more popular compared to other sensors such as infrared and thermal ones [8] or multibiometric fusion systems [9] because this additional equipment increases the cost of authentication systems. In this case, many researchers investigate feature-based methods. These kinds of spoofing detection methods attempt to extract discriminative features to recognize the genuine user from a fake face. For example, in print, display, and mask attacks, facial liveness features such as lip movement, head movement, and eye blinking can help recognize spoofing attacks. Furthermore, detection of replay attacks is more challenging because they contain this kind of liveness feature [7]. In some cases, the intruder applies liveness features in a mask attack by cropping the lip and eye area from a mask, which shows that liveness features alone cannot detect spoofing attacks properly. Replay display and printed attack images contain some noise and defects because of recapturing of information by a camera. During recapturing of information, the fake face loses the high-frequency information by getting affected in terms of the texture and color information of images, and these features can help distinguish a genuine person and a recaptured face image. Especially in printing and displaying attacks, during recapturing of information, some defects and noises appear in the spoofing face image. These artifacts lead to inadequate color reproduction in comparison to real biometric samples [10]. RGB is the commonly employed color space for sensing and displaying color images on many devices. Nevertheless, this color space in image analysis is inadequate due to the high correlation between the red, green, and blue color components and incomplete separation of the luminance and chrominance information [11]. Therefore, a different color space may help extract discriminative features for extraction of liveness cues of skin tones for detection of live and fake images. Therefore, image texture analysis based on different color spaces has attracted the consideration of research areas in the field of face spoofing attacks [11, 12]. By the success of deep learning algorithms in the field of computer vision and multimedia analysis, deep texture analysis-based algorithms have been employed in face spoofing problems. Nevertheless, deep learning-based face spoofing detection algorithms are faced with some problems such as few numbers of spoofing data and lack of diversity of scenarios which make it difficult to train a deep network [13, 14]. Additionally, IoT-based authentication systems encountered several difficulties such as storing or processing in a real-time manner [6]. To address these problems, we presented a novel approach based on hybrid convolutional neural network (CNN) models on different color spaces for IoT-based cloud computing. The proposed deep learning approach utilized three pretrained models in different color spaces for extracting luminance and chrominance information which are useful in recognition of spoofing face images. Due to extracted robust and discriminative features from a single image, this proposed model can achieve satisfactory results with less training dataset. This advantage of the proposed approach helps to decrease the storing training data in cloud computing which tackles one of the major problems of cloud computing systems. To the best of our knowledge, for the first time, in this paper, an IoT security framework is proposed for face spoofing detection. Extensive experimental analysis was conducted based on two challenging public access spoofing databases with their predefined evaluation protocols for comparison of our proposed approach against state-of-the-art methods. These experimental results show that our proposed approach outperforms all existing deep-based methods among state-of-the-art methods based on benchmark databases. In addition, experimental results show that the proposed approach can achieve stable results with less training dataset compared to benchmark deep learning models. In light of this information, the main contributions of this paper are presenting an IoT security framework for face spoofing detection which achieved significant results compared to the state of algorithms based on two public databases. Also, the proposed approach achieved stable results with less training dataset compared to benchmark deep learning models**.**

3. DISCUSSIONS:

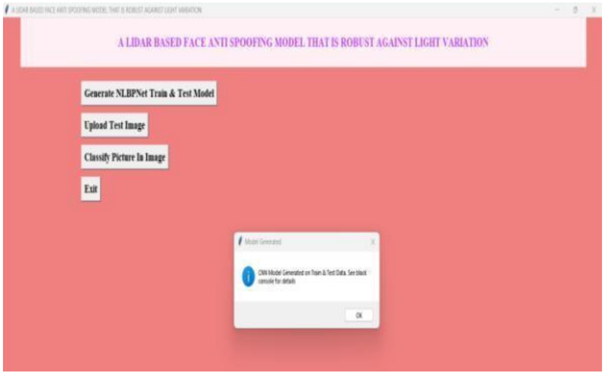
Since most current face spoofing detection systems only work with visible light photos, illumination fluctuations have a significant impact on detection effectiveness, even if deep learning approaches can extract high-level semantic information. Given that real-world lighting circumstances are seldom static, we provide a novel approach based on the Retinex theory: a dual-stream deep convolutional neural network—to adapt to these ever-changing illuminations. In the first place, our

4. RESULT:

Utilizing the Tensorflow toolkit, the suggested MSCI-DSCNN is trained and evaluated on a personal computer outfitted with a GeForce GTX 1080 Ti GPU. We start by providing a quick overview of the three benchmark datasets that are accessible to the public: OULU-NPU (Boulkenafet, Komulainen, Li, & Feng, 2017), REPLAY-ATTACK (Chingovska et al., 2012), and CASIA-FASD (Zhang et al., 2012). The assessment criteria will be detailed after this. We conclude by presenting the experimental findings, both intra- and cross-dataset, obtained from the three datasets.To run this project double click on _run.bat‘ file to get below screen

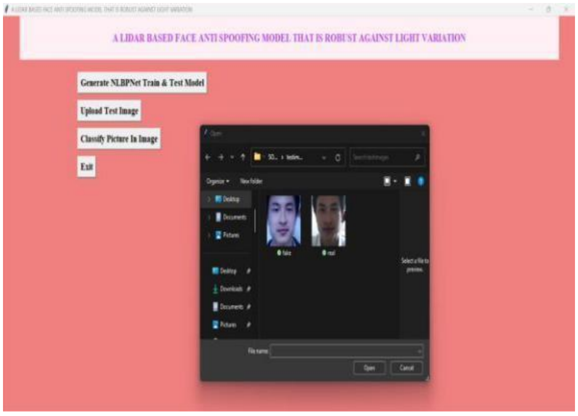

A LIDAR BASED FACE ANTI SPOOFING MODEL THAT IS ROBUST AGAINST LIGHT VARIATION
A LIDAR BASED FACE ANTI SPOOFING MODEL THAT IS ROBUST AGAINST LIGHT VARIATION
Generate NLBPNet Train & Test Model
Upload Test Image
Classify Picture In Image
Exit

In above screen click on _Generate NLBPNet Train & Test Model‘ button to generate CNN model using LBP images contains inside LBP folder.

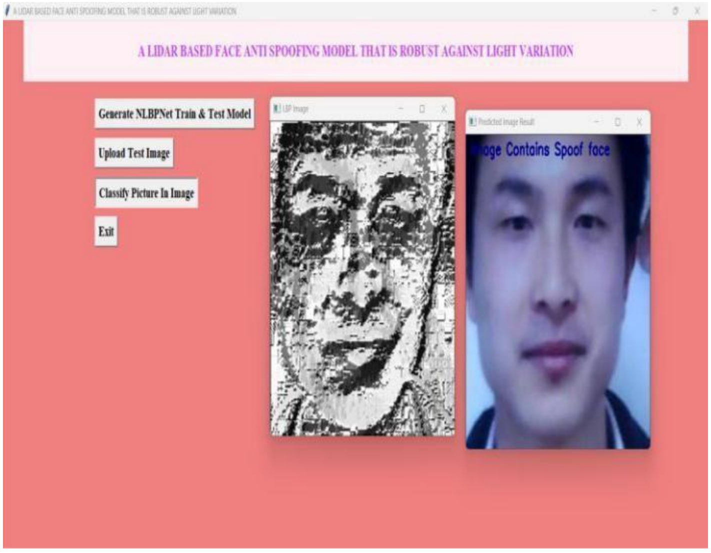

A LIDAR BASED FACE ANTI SPOOFING MODEL THAT IS ROBUST AGAINST LIGHT VARIATION
Generate NLBPNet Train & Test Model
Upload Test Image
Classify Picture In Image
Exit
Model Generated
OK

CNN Model Generated on Train & Test Data. See black console for details

In above screen we can see CNN LBPNET model generated. Now click on _Upload Test Image‘ button to upload test image

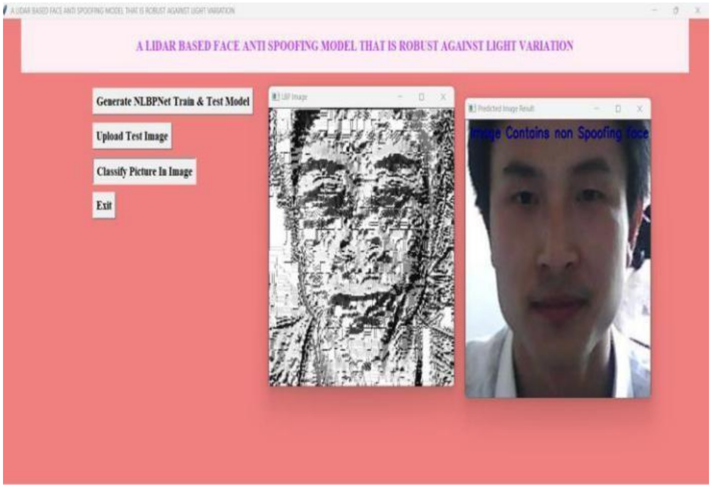

A LIDAR BASED FACE ANTI SPOOFING MODEL THAT IS ROBUST AGAINST LIGHT VARIATION
Generate NLBPNet Train & Test Model
Upload Test Image
Classify Picture In Image
Exit
Open
Organize
New folder
Desktop
Documents
Pictures
fake
real
Downloads
Select a file to preview.
File name:
Open
Cancel

In above screen we can see two faces are there from same person but in different appearances. For simplicity I gave image name as fake and real to test whether application can detect it or not. In above screen I am uploading fake image and then click on _Classify Picture In Image‘ button to get below result


A LIDAR BASED FACE ANTI SPOOFING MODEL THAT IS ROBUST AGAINST LIGHT VARIATION
Generate NLBPNet Train & Test Model
Upload Test Image
Classify Picture In Image
Exit
LBP Image
Predicted Image Result

age Contains Spoof face

In above screen application display message on image as it contains spoof face and I am displaying LBP format image also. Now we I will upload real image Below are the result for uploaded image


A LIDAR BASED FACE ANTI SPOOFING MODEL THAT IS ROBUST AGAINST LIGHT VARIATION
Generate NLBPNet Train & Test Model
Upload Test Image
Classify Picture In Image
Exit
LBP Image
Predicted Image Result

age Contains non Spoofing face

In above screen application display message on image as it contains non-spoofing face. You can use other image also available inside data folder. This data folder contains fake and real faces in separate folders. You can upload from that folder also for testing

5. CONCLUSION

under order to identify face spoofing under varying lighting circumstances, we present a dual-stream convolutional neural network called multi-scale color inversion dual-stream convolutional neural network (MSCI-DSCNN). We present the multi-scale color inversion (MSCI) approach and suggest incorporating it into one stream of the network so it may extract additional discriminative reflection characteristics.

6. REFERENCES AND CITATION

- L. Birla *et al.* **PATRON: Exploring respiratory signal derived from non-contact face videos for face anti-spoofing** **Expert Systems with Applications** (2022)
- H.-H. Chang *et al.* **Face anti-spoofing detection based on multi-scale image quality assessment** **Image and Vision Computing** (2022)
- V.L. da Silva *et al.* **Residual spatiotemporal convolutional networks for face anti-spoofing** **Journal of Visual Communication and Image Representation** (2023)
- R. Huang *et al.* **Face anti-spoofing using feature distilling and global attention learning** **Pattern Recognition** (2023)
- Y.A.U. Rehman *et al.* **SLNet: Stereo face liveness detection via dynamic disparity-maps and convolutional neural network** **Expert Systems with Applications** (2020)
- C. Wang *et al.* **A Learnable Gradient operator for face presentation attack detection** **Pattern Recognition** (2023)
- C. Wang *et al.* **An adaptive index smoothing loss for face anti-spoofing** **Pattern Recognition Letters** (2022)
- W. Zhang *et al.* **Face anti-spoofing detection based on DWT-LBP-DCT features** **Signal Processing: Image Communication** (2020)
- A. Alotaibi *et al.* **Deep face liveness detection based on nonlinear diffusion using convolution neural network** **Signal, Image and Video Processing** (2017)
- Face liveness detection using convolutional-features fusion of real and deep network generated face images q
- LiveNet: Improving features generalization for face liveness detection using convolution neural networks
- X. Song *et al.* Discriminative representation combinations for accurate face spoofing detection