Computer Science and Information Technologies
Vol. 4, No. 1, March 2023, pp. 1~13
ISSN: 2722-3221, DOI: 10.11591/csit.v4i1.pp1-13

Antispoofing in face biometrics: a comprehensive study on software-based techniques

Vinutha H[1], Thippeswamy G[2]
[1]Department of Computer Science and Engineering, Dr. Ambedkar Institute of Technology, Bengaluru, India
[2]BMS Institue of Technology and Management, Bengaluru, India

Article Info

Article history:

Received Feb 19, 2021
Revised Dec 19, 2022
Accepted Dec 30, 2022

Keywords:

Classification of face anti-spoofing methods
Face spoof detection
Metrics for face anti spoofing system
Software based face anti-spoofing techniques
Vulnerabilities of biometric system

ABSTRACT

The vulnerability of the face recognition system to spoofing attacks has piqued the biometric community's interest, motivating them to develop anti-spoofing techniques to secure it. Photo, video, or mask attacks can compromise face biometric systems (types of presentation attacks). Spoofing attacks are detected using liveness detection techniques, which determine whether the facial image presented at a biometric system is a live face or a fake version of it. We discuss the classification of face anti-spoofing techniques in this paper. Anti-spoofing techniques are divided into two categories: hardware and software methods. Hardware-based techniques are summarized briefly. A comprehensive study on software-based countermeasures for presentation attacks is discussed, which are further divided into static and dynamic methods. We cited a few publicly available presentation attack datasets and calculated a few metrics to demonstrate the value of anti-spoofing techniques.

Corresponding Author:

Vinutha H
Department of Computer Science and Engineering, Dr. Ambedkar Institute of Technology
Bengaluru, India
Email: vinuthah@gmail.com

1. INTRODUCTION

Biometric recognition systems for identifying people have grown tremendously in large scale for population census, controlling workspace access, applying access control to sensitive information, in forensics to identify criminals, while performing online transactions, law enforcement applications, and so on, for either user identification or verification. Biometric recognition is an automated process to authenticate and/or identify any individual using his or her physiological or behavioral traits. Examples of physiological characteristics are fingerprints, palmprints, iris, face, and deoxyribonucleic acid (DNA), and a few examples of behavioral characteristics are gait, voice, handwritten signatures, and key strokes. Biometric identification has various merits compared to the traditional identification system, which uses a smart card and password, as biometrics is a person’s key that can never be lost or forgotten. Biometrics is always attached to the user, and it is not easy to share or forge [1].

As we know now, biometrics utilize a user’s unique biological trait for identity verification. This type of authentication falls under possession-based authentication, which relies on a secret that only you have. The other type relies on a secret that only you know, called knowledge-based authentication. Such a biometric authentication system is vulnerable to spoofing attacks, where a fraudster makes an effort to compromise it. The type of spoofing attacks will change based on the different types of biometric modality, whether the biometric technique uses an iris, a fingerprint, a face, a keystroke, or a voice. Few traits cannot be easily compared to others. And hence, there is a requirement for specifically designed algorithms to identify the spoofs.

Each biometric has its own merits and flaws. For example, a fingerprint is most commonly used for commercial purposes to provide evidence of his or her presence; however, providing the fingerprint impression requires strong user cooperation. Iris is extremely precise, but it is dependent on image quality and requires users to actively participate in the scanning process. Face recognition is favorable in terms of availability and reliability. In this biometric system, a biometric user’s face can be captured without their knowledge or consent, meaning they need not cooperate and recognition can be done from longer distances [2].

Fraudsters take advantage of the vulnerabilities of a secure biometric system. In a spoofing attack, an individual attempts to masquerade as another person to get through a secured biometric recognition system. So, there is a significant requirement for anti-spoofing techniques to secure the biometric recognition systems. We need preventive measures to defend against unauthorized replicas of biometric traits.

Amongst all the biometric systems that are put up for commercial purposes, face biometrics play a pivotal role since they are widely used in national border control, physical or logical access control, forensics, e-commerce, surveillance, and e-governance domains. In a science fiction film, a young man disguised himself as an elderly person to board a plane to Canada, using a silicon mask on his face to fool border control agents [3]. since facial images can be captured in a non-intrusive manner using low-cost sensors [4]. Hence, spoofing as an authorized individual using their information is the biggest threat to biometric systems. Ramachandra and Busch [4] reports a black hat test that reveals the spoofing process in face recognition in laptops from various vendors. These cases demonstrate the loopholes of a real-time face recognition system. The attackers are highly motivated, as they can easily deceive the system by cost-effectively creating the face artifacts. Various video tutorials are now available on the web that provide information on how to create face artifacts [5]. And hence spoofing (including anti-spoofing) is the most urgent problem for researchers to address in the face recognition domain.

2. VULNERABILITIES OF FACE BIOMETRIC SYSTEM

Face recognition in the biometric system consists of two stages: enrollment and authentication. During enrollment, an unknown user's biometric information is recorded and saved as a template in the database of the recognition system. Generally, a biometric recognition system can be utilized for either verification or identification purposes. A biometric verification system does a one-to-one comparison to verify the user's identity. A biometric identification system identifies a user by comparing his biometric template with that of all the other users stored in a database. So biometric identification does a one-to-many comparison to identify a user from among many users who have enrolled their templates [6].

The basic architecture of the face recognition system consists of a sensor module that captures the face image, a feature extraction module that extracts facial features, and a matcher module that matches the input face with already stored templates for authentication. Ramachandra and Busch [4], Ratha *et al.* [7] have identified eight loopholes in a generic biometric system, which are depicted in Figure 1.

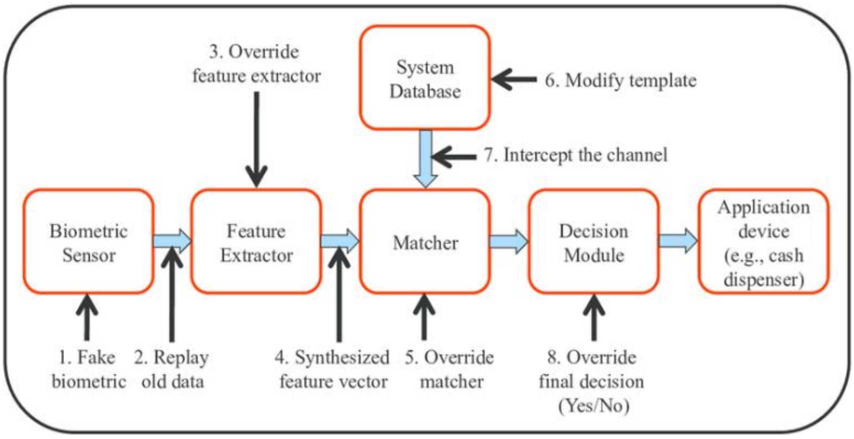

Figure 1. Vulnerabilities of biometric recognition systems

These vulnerabilities are categorized into four groups according to Jain *et al.* [8]:

a. User interface attack: while the sensor is capturing the biometric information attacker presents fake properties such as photos, videos, and masks.
b. Channel attack: the channels between the modules are intruded by replaying the old data, artificially synthesizing a feature vector, intercepting the channels or overriding the final decision.
c. Module attacks: modules are attacked by overriding the feature extractor and the matcher modules, their behavior can be modified.
d. Template database attacks: fraudster modifies a valid user's template in the database by replacing it with his biometrics.

3. FACE SPOOFING METHOD

Spoofing is an attempt to intrude into the normal workings of the biometric system by introducing artificial replicas of biometric traits in an unauthorized manner. A fraudster performs spoofing attacks to mimic a valid individual to bring down an entire biometric recognition system. To deceive a facial biometric system, they use the following spoofing methods: i) **Images and masks**: a fake user produces an authorized user's photograph or wears a mask created using prosthetics to imitate an individual; ii) **Identity manipulation**: the facial image stored by the biometric system is manipulated to match the facial characteristics of an unauthorized user using face morphing software, also biometric technological systems can be tricked either by changing the stored image or by using special makeup; and iii) **Identical twins:** Identical twins can act as spoofs for each other. The methods are used to attack the face recognition system by a fraudster. The face spoof attacks can be classified as given Figure 2 [9].

a. **Printed flat photo attack:** the commonest attack is the usage of flat printed photos against the recognition system without the permission of the original user (Refer to Figure 2(b)).
b. **Cut photo attack: e**yes in the printed copy of the photo is cut off to display blink behavior to get over with the challenge-response antispoofing technique (IDLive Face) (Refer to Figure 2(c)).
c. **Warped photo attack: p**rinted photo is bent in a certain way to simulate the facial movements (Refer to Figure 2(d)).
d. **Video replay attack: a** video is played before the sensor device of a face recognition system using a laptop or a mobile device. In this type of attack, some of the movements like the blinking of eyes, facial expressions, head movements can be performed using phones, tablets or laptops (Refer to Figure 2(e)).
e. **Mask attack: t**wo types of masks are used by any impostor, they are wearable masks and paper cut masks. It is the most difficult type of attack. Mask manufacturing is expensive and it requires three-dimensional (3D) scanning and printing devices too (Refer to Figures 2(f) and (g)).

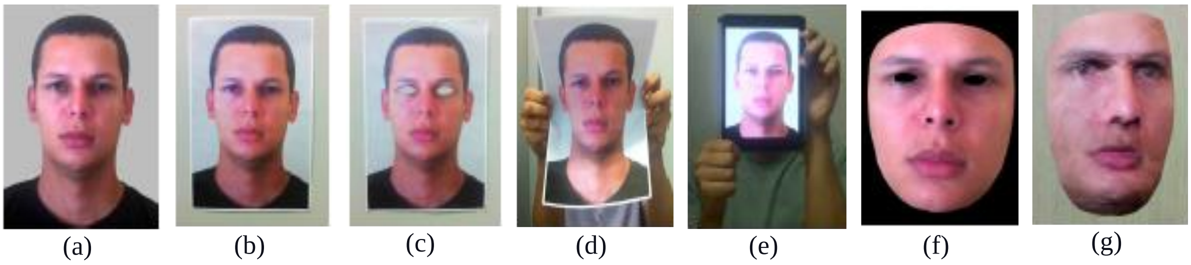

Figure 2. Types of presenation attacks (a) valid user, (b) printed flat photo, (c) eye cut photo, (d) warped photo, (e) video playback, (f) synthetic mask, and (g) paper cut mask [9]

4. FACE SPOOF DETECTION

Face spoof detection, liveness detection of a face, countermeasures against facial spoof attacks and face anti-spoofing are used interchangeably to refer to the methods to identify a fraudster trying to gain access into facial recognition systems by posing him/herself as a genuine user. Liveness detection in a spoofing problem marks the contrast between fake and real faces and hence it is a face recognition problem. The difference is that the face recognition techniques try to look for a face that increases interpersonal variations (differences between two persons) but anti-spoofing techniques strive for a face representation that reduces interpersonal variations thereby increasing intrapersonal variations due to changes in illumination and poses [10].

Liveness detection can be defined is the ability of the biometric system to recognize a living, authorized individual. Here biometric authentication involves verifying that the user who has initially enrolled, is the same person who is appearing for authentication, not a 2D photograph, or digital version of the face [11]. This can be achieved through algorithms that examine the input data collected from biometric sensors.

Liveness detection can be categorized as active and passive: **Active method** asks the person to perform an action that cannot be easily reproduced. That is, asking the user to blink his/her eyes, and raise the eyebrows. These are also called as challenge-response techniques [12]. BioID offers a challenge-response technique to identify a spoof attempt. Here the BioID system challenges the user by giving some random commands, and the response is validated. **The passive method** applies techniques to detect a non-live image without user interference. For this purpose, the biometric data captured during the enrollment stage is used. IDLive [12] a passive facial liveness detection, happens at the backend, which recognizes the spoof attempt without requiring user interaction.

5. CLASSIFICATION OF FACE ANTI-SPOOFING METHODS

Antispoofing methods [13] are categorized into two main groups. They are designated as hardware and software based techniques [2]. These are the most deployed methods of anti-spoofing which are further grouped into various other methods as shown in Figure 3.

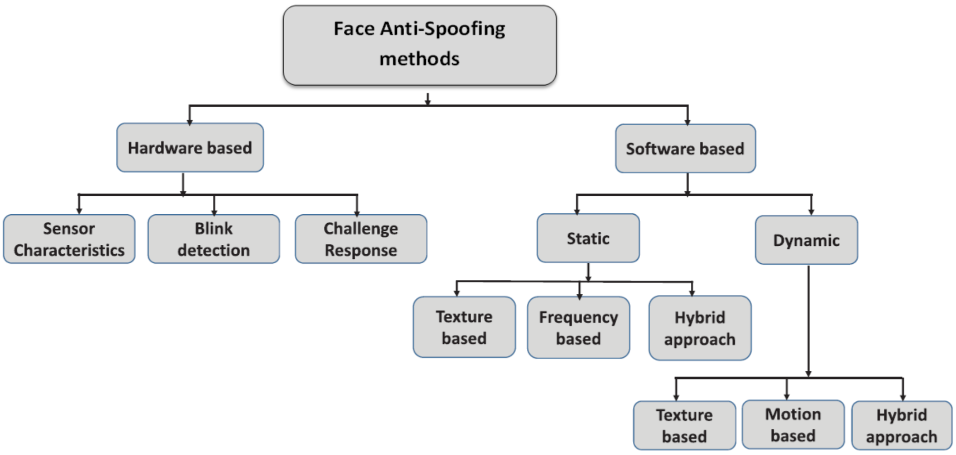

Figure 3. Classification of face anti-spoofing methods

6. HARDWARE-BASED TECHNIQUES

Hardware-based anti-spoofing techniques incorporate special hardware devices in the biometric system to detect fake access. In the literature, authors have used different types of hardware devices in their face biometric set up. These devices utilize different types of imaging technologies such as near-infrared (NIR) images [14], [15], 3D depth images [16], or complementary infrared (CIR). These are captured by comparing the reflectance information of real authenticated faces and the spoof equipments, using light emitting diode (LEDs) and photodiodes set-up at various wavelengths. Thermal imaging has been explored, by acquiring large datasets of thermal images of face using infrared cameras, for real as well as for the spoof attempts in liveness detection [17]. Erdogmus and Marcel [18] used depth information of 2D photographs to discover a 2D attack. Whereas Wang *et al.* [16] recovers a 3D facial information to determine the spoofing attacks using specialized depth cameras. Ng and Chia [19] made use of facial expressions that randomly changed the temporal information thereby verifying the liveness of users.[15] used a near-infrared band for disguise detection.

Subsidiary sophisticated hardware increases the overall cost of the system and also most of the mobile phone cameras and webcams available today are not compatible with it. So, this has motivated the anti-spoofing research fraternity to shift to software-based anti-spoofing techniques which are cheaper and they can be easily installed to the existing face biometric systems. Table 1 gives a brief insight into the hardware-based methods utilized by the researches for spoof detection through the years.

Table 1. Hardware based anti-spoofing techniques

Contributors	Method/Equipment
Pavlidis and Symosek (2000)	Near infrared bands
Ng and Chia [19]	Random temporal cues
Dhamecha *et al.* [17]	Thermal imaging using infrared cameras
Ergdogmus and Marcel [18]	2D depth information
Wang *et al.* [16]	3Dfacial depth information using depth cameras
Z. Zhang *et al.* [14]	Multispectral reflectance distributions
Albakri and Alghowinem [20]	3D depth cameras

7. SOFTWARE-BASED TECHNIQUES

Software-based anti-spoofing techniques make use of an algorithm that detects and categorizes the captured face into either a spoofed face, as a result of any spoofing attacks or a genuine face. These sorts of techniques incur lesser cost, easy to incorporate a piece of code running inside the face recognition system and exhibit higher accuracy. Major advantage is it does not require specialized and higher cost hardware equipment as in hardware-based anti-spoofing techniques and also doesn't user need not co-operate, it can work without the knowledge of the user accessing the face recognition system.

Software-based methods **a**re further categorized into **static** and **dynamic** approaches. **Static approaches** execute on only spatial information without requiring temporal data. Here a single image is considered. If a video is presented and static approach is used then each frame of a video sequence is considered for further processing. A static approach incurs less cost but yields good performance. **Dynamic approaches** utilize spatio-temporal information of the video played before the face recognition system for access control. This approach tends to find the relative motion of the video frames that are run against the face sensor and hence it requires more time and effort compared to static approaches. **State-of-the-art static approaches** are grouped into 3 different groups based on the nature of the algorithms used. They are **texture based**, **frequency-based** and **hybrid approaches** (Refer to Table 2).

Texture based approaches analyze the microtextures of the facial image representation. This is the most popular approach in determining display and photo attacks because this delineates amongst the formation of pigments (formed while printing), specular reflection (due to quality variation) and a shade (arising due to display attack). Määttä *et al.* [21] first came up with a widely used texture-based approach based on local binary patterns (LBPs) and detected photo print attack. Edmunds [10] propose software-based protection methods based on the LBP descriptor to evaluate texture-based anti-spoofing techniques, by focusing on differences between natural and unnatural characteristics present in the face region. Here LBP operator embeds color and contrast information in texture characterization and they combine the images with HSI color model to form a HSI-LBP color texture descriptor which improves texture-based anti-spoofing techniques on Replay Attack for CASIA and MSU databases. Chingovska *et al.* [22] also used the same LBP descriptors to solve the replay video attack on the face recognition system. LBP captures the pigment information on the image which is formed out of printers and also LBP captures the change in reflectance due to the quality variation of the attack equipment.

Frequency-based approaches analyze and quantify the frequency component. Initial work was based on the fourier spectrum analysis to successfully detect a photo attack for face biometric carried out by Li *et al.* [23]. Liu *et al.* [24] also used fourier spectra to detect video replay attacks. There are different works carried out by researchers like [24] those used discrete cosine transforms, Zhang *et al.* [14] made use of difference of Gaussian (DoG) filters, and Peng and Chan [25] used components which are of high frequency.

Hybrid approaches combine more than one property or attribute associated with the spoofed image. Many researchers have tried out their hands in combining various attributes to achieve better recognition between fake and real faces, for example, Raghavendra and Busch [26] combined texture attribute with time-frequency information, Määttä *et al.* [21] fused texture and shape, Komulainen *et al.* [27] incorporated all the context information. Hasan *et al.* [28] fused modified DoG filtering and binary pattern variance to identify photo spoofing, by analyzing both texture LBP and contrast (variance) characteristics. Support vector machine (SVM) was used on the extracted feature vectors and they also prove that LBP-variants (LBPV) with SVM classifier method gives better results compared to SVM and LBP in presentation attack detection. Benlamoudi *et al.* [29] used the Viola-Jones face detection algorithm [30] and pictorial structure model [31] to detect the face and then localize the eye positions; then, the coordinates of the eyes are used to make right the posing of the face. In the multi block (MB) technique [32], face is divided into square blocks and a texture descriptor is applied on each block. Three popular texture descriptors, binarized statistical image features (BSIF), LBP, and local phase quantization (LPQ) are used in multiple levels, forming a multi-level feature descriptors (FD-ML) for feature extraction. ML representation is formed by combining multiple MBs [32]. Finally, Lib-SVM [33] was used to classify the feature vectors as valid or invalid. Table 2 consolidates on software-based static countermeasures by quoting their methods adopted, types of attacks, datasets and performance metrics used.

Table 2. Software based static anti-spoofing methods

Contributors	Types of static method	method	Attack type	Database	EER (%)	HTER (%)
Edmunds [10]	Texture	HSI-LBP color texture descriptor	Print, mobile and ipad	Replay-Attack Casia MSU android MSU laptop	- 30 30 40	44.1 - - -
Määttä *et al.* [21]	Texture	LBP	Photo attack	NUAA Photograph Imposter database	2.8	-
Chingovska *et al.* [22]	Texture	LBP	Replay video attack	Replay-attack	-	15
Li *et al.* [23]	Frequency	Fourier spectrum analysis	Photo attack	NUAA Photograph Imposter database	4.71	1.5
Zhang *et al.* [14]	Frequency	DoG filters	-	-	-	-
Liu *et al.* [24]	Frequency	Fourier spectrum analysis	Replay video attack	Replay-Attack	-	-
Raghavendra and Busch [26]	Texture	Local features-eye (periocular) and nose region, Global features - BSIF and SVM-classification	3D mask attacks	3DMAD	-	0.03
Hasan *et al.* [28]	Texture	LBPV pattern representation and SVM	Photo attack	NUAA Photograph Imposter database	-	0.39
Benlamoudi *et al.* [29]	Representation + texture	LBP, LPQ, BSIF-descriptors Fisher core - sort the features in ascending order SVM-classification	Warped photo attack cut photo attack Video attack	CASIA-FAS MSU-MFS Replay-Attack database	17.46 14.9 -	- - 12.25
Li *et al.* [34]	Spatio temporal	3D convolutional neural network (CNN)		CASIA MSU	1.4 0	- -
George and Marcel [35]	Hybrid	Fully connected neural network-CNN	Replay attack	Replay mobile dataset	-	0
Sharifi [36]	Texture	Fuses CNN and OVLBP	Print attacks Video attacks	OVLBP Print Attack Replay Attack OVLBP+CNN Print Attack Replay Attack	 - - - -	 14.35 15.75 10.40 11.00
Chen *et al.* [37]	Texture	Retinex based LBP and region based CNN ROI pooling	Replay attacks	Replay Attack	0.093	0.206
Pujol (2020) [32]	Texture	Entropy based HOG-EBHOG	Presentation attacks	CASIA FASD MIFS	9.5	-

State-of-the-art dynamic **approaches** are of three kinds: **motion-based**, t**exture based** and h**ybrid schemes** (Refer to Table 3). **Motion-based approaches** employ a structure from facial movements, which in turn yield depth information for features of face. Kollreider *et al.* [38] has proposed a novel liveness awareness framework by estimating face motion for face authentication which utilizes lightweight optical flow and gives a liveness score. A generalized dynamic approach for spoof detection was proposed by Li *et al.* [39] by utilizing pulses extracted from videos, referring to the fact that only a live face can have pulses (motion) in it but not the printed photos or mask. Edmunds and Caplier [40] exploit conditional local neural fields track face's motions and bag-of-words feature extraction method extracts rigid and non-rigid motion features using the fisher vector.

Texture based approaches exploit the characteristic of face representations that discriminate a live face from fake ones. Research community started with relying on LBP patterns and its variants only to fuse different characteristics to form **hybrid schemes** which prove to be more efficient comparatively. Pereira *et al.* [41] extended regular LBP operator to VLB (volume local binary pattern) operator, the so-called spatiotemporal characteristics (dynamic texture), to detect the dynamics of face micro-textures. Liu *et al.* [42] has developed an remote photoplethysmography (rPPG) correlation model which extracts local heartbeat signal patterns that discriminate against a mask and a live face. A confidence map was drawn using signal strength that exploits the characteristics of rPPG distribution on real faces. Buolkenafet *et al.* [43] has considered facial appearance to detect the liveness. They extract features from color spaces and the fisher vector encoding method is applied to these features for liveness detection. They have tested on the following benchmark databases: Casia, Replay-attack, MSU-MFSD and claim that their method outperforms the best methods available.

Table 3. Software based dynamic anti-spoofing methods

Contributor	Types of dynamic method	method	Attack type	Database	EER (%)	HTER (%)
Kollreider *et al*. [38]	Motion	Optical flow	Playback attack	Replay Attack database and proprietary	0.5	-
T. de Freitas *et al*. [41]	Motion	Spatio-temporal extension of LBP	Print attacks and Video attacks	CASIA Replay-Attack	10	- 7.60
Litong Feng *et al*. [44]	Texure and motion	Dense optical flow hierarchical neural network	Print attacks Video attacks Mask attack	Replay Attack and 3D MAD CASIA FASD	0 5.83	0 -
Siqi Liu *et al*. [42]	Heart beat signal	Analyses heart beat signal through rPPG	3D mask attack	Public and self-contained datasets	-	-
Xiaobai Li *et al* [39]	motion	Pulse detection and color texture analysis	Print attacks Video attacks Mask attacks	3DMAD and REALF masks	-	-
Z Boulkenafet *et al.* [43]	Color spaces	Fisher vector encoding on the extracted features of different color spaces	Print attacks Video attacks	CASIA, Replay Attack, MSU-MFSD	-	-
Junying Gan *et al*. [45]	Video frames	3D CNN	Video attacks	Replay Attack CASIA	- -	0.04 10.65
Yaojie Liu *et al*. [46]	Depth and signals	CNN-RNN model for face depth estimation and rPPG signals estimation	Presentation attacks	Proprietary database	-	-
Taiamiti Edmunds and Alice Caplier [40]	Motion	Conditional local neural fields face tracking	Presentation attacks	CASIA FASD, Replay-Attack, MSU-MFSD, 3DMAD	-	-
Lei Li *et al*. [47]	Texture	Deep LBP	print attacks and video attacks	Replay-Attack, CASIA	-	-
Emna Fourati *et al*. [48]	Motion	Image quality assessment	Presentation attacks	Replay-Attack	-	0.024
H. Chen *et al*. [37]	Motion	R-CNN and Improved retinex LBP	Video attacks	Replay-Attack	0.093	0.26
Xin Cheng *et al*. [49]	Texture and motion	Dynamic and texture fusion attention network	Replay and video attacks	CASIA-MFSD Replay Attack	6.9 -	- 2.2

Gan *et al.* [45] have exploited spatio-temporal features of video frames using 3D CNN which have scored half total error rate (HTER) (refer to **metrics for face anti-spoofing system evaluation** section) values of 0.04% and 10.65% for Replay Attack and CASIA databases respectively. Feng *et al.* [44] proposed a hierarchical neural network model for antispoofing by integrating image quality and motion cues and achieving 0% HTER and equal error rate (EER) for both Replay Attack and 3DMAD datasets. In the case of CASIA FASD, the framework has achieved an EER 5.83%. Other than these, Pan *et al.* [50] utilizes conditional random fields (CRF) that will be generated whenever an eye blink occurs in the face for liveness detection. CRF works on context-based phenomena of temporal data.

The earlier works carried out in the literature using static or dynamic approaches make use of handcrafted features like LBP, and scale invariant feature transform (SIFT), to discriminate between the real and fake faces. CNN started gaining popularity, during which it was first used by Yang *et al.* [51] for face anti-spoofing. The following are a few instances where CNN marked its presence assertively.

Nikitin *et al.* [52] fused two deep classifiers, first being used in identifying the presence of spoofing medium and the second classifier is used to analyze the blinking of eyes and checks eyes openness classification per frame. Muhammad *et al.* [53] incorporated a novel, sample learning-based recurrent neural network (SLRNN) anti-spoofing architecture which makes use of the following 3 models: CNN, sparse filtering and long short-term memory (LSTM). Sparse filtering was applied for augmenting the features using residual networks (ResNet). The augmented features formed a sequence and were fed into a LSTM network to construct the final representation. A 3D CNN framework was proposed by Li *et al.* [34] which takes both spatial and temporal information, using the data augmentation method and employs a generalization regularization thereby improving generalization performance. George and Marcel [35] proposes a dense fully connected neural network architecture, trained with pixel-wise binary supervision. Here a single CNN model which uses frame level information without requiring temporal data for detecting the presentation attack with deep pixel-wise supervision. It has achieved HTER of 0% in the Replay Mobile dataset and an ACER of 0.42% in Protocol-1 of OULU dataset. A CNN-RNN (recurrent neural network) combination model was employed by Liu *et al.* [46] for face depth estimation and rPPG signals estimation using pixel-wise and sequence–wise supervision respectively. And depth information and rPPG signals are fused. Li and Feng [47] used SVM to classify between real and fake by extracting handcrafted deep partial features from the convolutional responses. Two sets of feature information extracted out of the CNN model and OVLBP (overlapped histograms of local binary patterns) are fused by Sharifi [36] to form a score vector. A majority voting of CNN, OVLBP, and fused score helps in fake detection. Table 3 summarizes the Software based dynamic anti-spoofing techniques contributed by various researchers.

8. METRICS FOR FACE ANTI-SPOOFING SYSTEM EVALUATION

A spoof detection system can incur two types of errors [9]: i) number of false acceptance (NFA) -it gives the count of fraudsters accepted as authorized users (i.e.), and the probability of its occurrence is known as false acceptance rate (FAR); ii) number of false rejection (NFR) - this is the count of authorized users, who can be considered as fraudsters, and its probability of occurrence is called a false rejection rate (FRR) (Refer to Table 4 for the metrices). FAR and FRR are inversely proportional to each other. A receiver operating characteristics (ROC) curve is drawn by computing all possible pairs of FAR and FRR values, as illustrated in Figure 4.

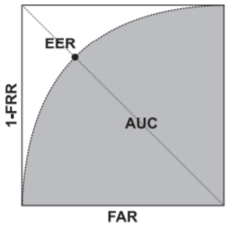

Figure 4. Relationship amongst the metrics on the ROC curve

The area under curve (AUC) metric is obtained by the integral of a ROC, the grey area in Figure 4. EER is the point of interference when FAR equals FRR on the ROC curve, and HTER is the point on the ROC curve where the average of FAR and FRR is minimum. Finally, for overall accuracy (ACC) both authorized users and fraudsters are considered. A variant of ROC called DET (decision error tradeoff) is also used in some cases for showing verification performances. The only difference between ROC and DET is that the primary difference is that the y-axis takes a false rejection rate instead of a true acceptance rate in the DET curve.

For the biometric authentication in Android smartphone, Google recognizes two types of attacks: “impostor” attacks and “spoof” attacks. A fraudster pretends to be an authorized user by disguising his or her features in an impostor attack, but in a spoof attack, a non-live representation of the authorized user such as a photograph or video is used to gain entry. Google sets a threshold of 7% accept rate or less for strong security during attack detection that is the percentage of times an attack is not detected [11]. This is analogous to a biometric “false accept rate”, which represents the likelihood that a person is incorrectly identified as a biometric match. Figure 5 shows the plot of error metrics plotted for different static methods. The X-axis is plotted with the static method (one of texture, frequency, and hybrid) along with the type of attack to which this method is applied and Y-axis measures the EER and HTER values for each method if available.

Table 4. Metrics commonly applied on face spoofing evaluation

Metric	Stand for	Equation	Type
FAR	False Acceptance Rate	FAR = $\frac{NFA}{\#Impostor}$	Error
FRR	False Rejection Rate	FRR = $\frac{NFR}{\#Genuine}$	Error
EER	Equal Error Rate	EER = (FAR= FRR)	Error
HTER	Half Total Error Rate	HTER = $\frac{\text{FAR+ FRR}}{2}$	Error
ACC	Accuracy	100 X (1- $\frac{FAR\ X\ \#Impostor+FRR\ X\ \#\ Genuine}{\#Impostor+\ \#Impostor}$)	Hit
AUC	Area Under Curve	Area = $\int_a^b f(x)\,dx, where\ f : [a,b] \rightarrow R$	Hit

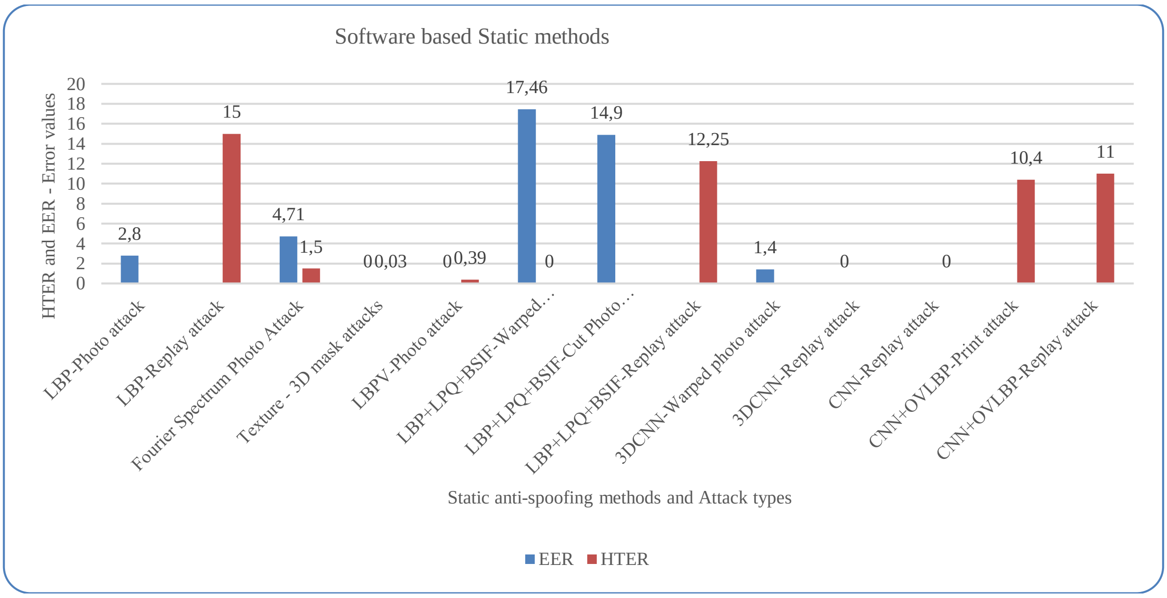

Figure 5. EER-HTER error evaluation for software based static methods

Based on the statistics in the graph it seems that out of all the texture components LBPV offers better spoof recognition with the least error of 0.039 for the photo attacks. For the video attacks, the hybrid approach of 3D CNN has the highest recognition rate of 100% that is 0 error. Raghavendra and Busch [26] has applied texture descriptors for 3D mask attacks. Until now it is known to have the lowest error recorded using texture descriptors. But it is also proved that the same video replay attacks have 0 HTER when CNN are used for recognition. It is observed that hybrid approaches have higher HTER and EER values i.e. when multiple descriptors are applied. So, there is a scope of research in this domain in which two descriptors from texture and frequency-based methods will yield better spoof recognition and lesser error rates.

The error metrics for dynamic methods are plotted in Figure 6 where X-axis depicting one of the three dynamic descriptors (motion, texture, and hybrid) with the attack type. Y-axis carries the HTER and ERR values. Dense optical flow is best suited for identifying the print attacks as it is proven that its HTER and EER values are 0. But if we use spatio-temporal descriptor (hybrid) or a 3D CNN for print attacks, for video frames the captured error rate is 0.04, it incurs error with HTER of around 10, which is not acceptable in anti-spoofing algorithms. 3D CNNs find their use here, that is when they are used. Hence in the literature, the application of texture descriptors over the face image has proven to be a good approach in static methods and dense optical flow works very well for both print and video attacks in dynamic methods. But deep learning is manifesting the face recognition domain too and CNNs, deep neural networks are being extensively used in discriminating amongst the original, valid faces and the spoofed faces.

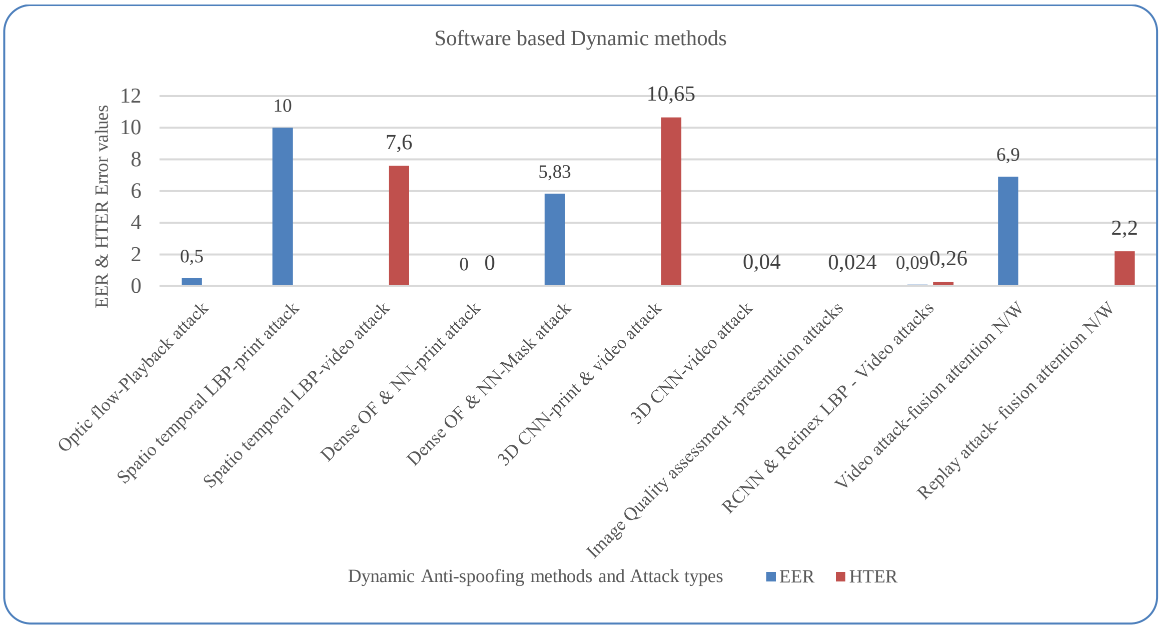

Figure 6. EER- HTER error evaluation for software based dynamic methods

9. FACE ANTI-SPOOFING DATASETS

Face spoof attack databases that are available, play a pivotal role in computing new and better face anti-spoofing techniques. Here few face publicly available databases are discussed. Researchers around the world use extensively, the seven publicly available benchmark data sets to evaluate their anti-spoofing algorithms. NUAA Photograph Imposter [55], replay-attack [22], print-attack [55], CASIA face anti-spoofing[56], MSU-MFSD [57] are the well-known datasets concerned with 2D attacks. For mask attacks, the 3D mask attack dataset [18], [58] dataset are used.

The first and foremost public dataset that was made available for face anti-spoofing was the NUAA Photograph Imposter dataset [55]. Images here were captured by regular webcams in different environments under varied illumination conditions, in three sessions, between each of which with an interval of two weeks were taken. Printed flat and warped attacks are evaluated.

The Print-Attack dataset [55] was the standard dataset used in the first competition for spoof detection. The images were captured by presenting a flat printed photo of an authorized person to the system by hand-held method (*i.e.*, the fraudster holds the photo in the hands) or using a fixed support (*i.e.*, photos are stuck on a fixed stand or wall). Print-Attack dataset was extended to the Replay-Attack dataset [22] for evaluating video and photo attacks. It comprises of 1,300 video clips of video and photo attacks. Here trio attacks modes were considered: i) printed photo and video playbacks, ii) using a low-resolution mobile phone and iii) an iPod screen. CASIA face anti-spoofing data set [56] has seven situations with different image qualities and various attack types. This data set presents warped photo attacks, video playback attacks, and eye-cut photo attacks.

The first public database for mask attacks is 3D mask-attack dataset (3DMAD) [18] and it comprises an RGB-D camera recorded video sequences. ThatsMyFace13 manufactured the masks using the frontal and profile images of an individual. MSU mobile face spoofing dataset (MSU MFSD) [57] has 280 video clips of video and print photo attacks. A color printer printed all the photos of 35 participants used for attacks on a large-sized paper. Each participant’s video playback was taken to perform an attack. MORPHO Company created [58] dataset, which is a paid-mask dataset, using a 3D scanner. To obtain authorized images of face shape and texture, it uses a structured light technology. Then Sculpteo 3D Printing technology manufactures the masks, and are recaptured by the same sensor to get the fraudster images. Face spoof attack databases that are available, play a pivotal role in computing new and better face anti-spoofing techniques. Here few face publicly available databases are discussed. Researchers around the world use extensively, the seven publicly available benchmark data sets to evaluate their anti-spoofing algorithms. NUAA Photograph Imposter [55], replay-attack [22], print-attack [55], CASIA face anti-spoofing [56], MSU-MFSD [57] are the well-known datasets concerned with 2D attacks. For mask attacks, the 3D mask attack dataset [18], Kose and Dugelay's [58] data set are used.

The first and foremost public dataset that was made available for face anti-spoofing was the NUAA Photograph Imposter dataset [55]. Images here were captured by regular webcams in different environments under varied illumination conditions, in three sessions, between each of which with an interval of two weeks were taken. Printed flat and warped attacks are evaluated. The print-attack dataset [55] was the standard dataset used in the first competition for spoof detection. The images were captured by presenting a flat printed photo of an authorized person to the system by hand-held method (*i.e.,* the fraudster holds the photo in the hands) or using a fixed support (*i.e.,* photos are stuck on a fixed stand or wall). Print-attack dataset was extended to the replay-attack dataset [22] for evaluating video and photo attacks. It comprises of 1,300 video clips of video and photo attacks. Here trio attacks modes were considered: i) printed photo and video playbacks, ii) using a low-resolution mobile phone and iii) an iPod screen. CASIA face anti-spoofing dataset [56] has seven situations with different image qualities and various attack types. This data set presents warped photo attacks, video playback attacks, and eye-cut photo attacks.

The first public database for mask attacks is 3D mask-attack dataset (3DMAD) [18] and it comprises an RGB-D camera recorded video sequences. ThatsMyFace13 manufactured the masks using the frontal and profile images of an individual. MSU mobile face spoofing dataset [57] has 280 video clips of video and print photo attacks. A color printer printed all the photos of 35 participants used for attacks on a large-sized paper. Each participant's video playback was taken to perform an attack. MORPHO Company created Kose and Dugelay's [58] dataset, which is a paid-mask dataset, using a 3D scanner. To obtain authorized images of face shape and texture, it uses a structured light technology. Then Sculpteo 3D Printing technology manufactures the masks, and are recaptured by the same sensor to get the fraudster images.

10. CONCLUSION AND FUTURE DIRECTIONS

The biometric system particularly the Face recognition system faces many threats and challenges from the fraudsters due to its vulnerabilities. These challenges were effectively addressed by the researchers from the past by applying different types of Anti-spoofing techniques. These techniques make use of either hardware or software-based solutions. In our review process, we gave an overview of the state-of-the-art of both static and dynamic methods followed in Software-based anti-spoofing techniques. Few performance metrics like FAR, FRR, ROC, HTER, EER, ACC which are used in evaluating face anti-spoofing techniques are discussed as well. We tried to consolidate on few publicly available benchmark databases for 2D presentation attacks, that are available upon which anti-spoofing technique can be applied. A lot of research work has been carried out on the databases where they knew the type of presentation attack and countermeasures for known attacks are devised. But in the real world, we cannot integrate anti-spoofing algorithm for a single particular known type of attack. Fraudsters can attack the same system in different ways either using a mask or by presenting a printed photo or he can run a video replay instead of an authorized user's face, here type of attacks is not known. Though there are few works on unknown attacks in which partial paper cuts and transparent masks are used, much more focus is required in this area. Potential face recognition systems for unknown attacks should be designed to detect the type of attack (also called zero-shot face anti-spoofing) and mitigate it.

REFERENCES

[1] J. Galbally, S. Marcel, and J. Fierrez, "Biometric antispoofing methods: a survey in face recognition," *IEEE Access*, vol. 2, pp. 1530–1552, 2014, doi: 10.1109/ACCESS.2014.2381273.

[2] A. Benlamoudi, "Multi-modal and anti-spoofing person identification," University of Kasdi Merbah, 2018.

[3] "Real face spoofing case1," *Daily Mail*, 2015. http://www.dailymail.co.uk/news/article-1326885/Man-boards-plane-disguised-old-man-arrested-arrival-Canada.html.

[4] R. Ramachandra and C. Busch, "Presentation attack detection methods for face recognition systems: a comprehensive survey," *ACM Computing Surveys*, vol. 50, no. 1, pp. 1–37, Jan. 2017, doi: 10.1145/3038924.

[5] "3D Face Mask," *Face 3D Mask*, 2014. http://www.thatsmyface.com.

[6] P. S. Sudhish, A. K. Jain, and K. Cao, "Adaptive fusion of biometric and biographic information for identity de-duplication," *Pattern Recognition Letters*, vol. 84, pp. 199–207, Dec. 2016, doi: 10.1016/j.patrec.2016.10.011.

[7] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2091 LNCS, Springer Berlin Heidelberg, 2001, pp. 223–228.

[8] K. Nandakumar, A. K. Jain, and A. Nagar, "Biometric template security," *Eurasip Journal on Advances in Signal Processing*, vol. 2008, no. 1, p. 579416, 2008, doi: 10.1155/2008/579416.

[9] L. Souza, L. Oliveira, M. Pamplona, and J. Papa, “How far did we get in face spoofing detection?,” *Engineering Applications of Artificial Intelligence*, vol. 72, pp. 368–381, Jun. 2018, doi: 10.1016/j.engappai.2018.04.013.

[10] T. Edmunds, “Protection of 2D face identification systems against spoofing attacks,” Université Grenoble Alpes, 2017.

[11] “Biometric liveness detection and spoof detection,” *Aware Biometrics Software*, 2020. https://www.aware.com/biometric-liveness-detection-spoof-detection/.

[12] “IDLive® Face passive facial liveness detection,” *IDR&D*. https://www.idrnd.ai/passive-facial-liveness/.

[13] “Biometric Spoofing And Liveness Detection,” *IEVO Ltd.*, 2019. https://ievoreader.com/biometric-spoofing-and-liveness-detection/.

[14] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, “Face liveness detection by learning multispectral reflectance distributions,” in *2011 IEEE International Conference on Automatic Face and Gesture Recognition and Workshops, FG 2011*, Mar. 2011, pp. 436–441, doi: 10.1109/FG.2011.5771438.

[15] I. Pavlidis and P. Symosek, “The imaging issue in an automatic face/disguise detection system,” in *Proceedings IEEE Workshop on Computer Vision Beyond the Visible Spectrum: Methods and Applications*, 2000, pp. 15–24, doi: 10.1109/cvbvs.2000.855246.

[16] T. Wang, J. Yang, Z. Lei, S. Liao, and S. Z. Li, “Face liveness detection using 3D structure recovered from a single camera,” in *International Conference on Biometrics, ICB 2013*, Jun. 2013, pp. 1–6, doi: 10.1109/ICB.2013.6612957.

[17] T. I. Dhamecha, A. Nigam, R. Singh, and M. Vatsa, “Disguise detection and face recognition in visible and thermal spectrums,” in *Proceedings - 2013 International Conference on Biometrics, ICB 2013*, Jun. 2013, pp. 1–6, doi: 10.1109/ICB.2013.6613019.

[18] N. Erdogmus and S. Marcel, “Spoofing attacks in 2D face recognition with 3D masks and anti-spoofing with Kinect,” Sep. 2013, doi: 10.1109/BTAS.2013.6712688.

[19] E. S. Ng and A. Y. S. Chia, “Face verification using temporal affective cues,” in *International Conference on Pattern Recognition (ICPR)*, 2012, pp. 1249–1252.

[20] G. Albakri and S. Alghowinem, “The effectiveness of depth data in liveness face authentication using 3D sensor cameras,” *Sensors (Switzerland)*, vol. 19, no. 8, p. 1928, Apr. 2019, doi: 10.3390/s19081928.

[21] J. Määttä, A. Hadid, and M. Pietikäinen, “Face spoofing detection from single images using micro-texture analysis,” in *International Joint Conference on Biometrics, IJCB 2011*, Oct. 2011, pp. 1–7, doi: 10.1109/IJCB.2011.6117510.

[22] I. Chingovska, A. Anjos, and S. Marcel, “On the effectiveness of local binary patterns in face anti-spoofing,” in *proceedings of the international conference of biometrics special interest group (BIOSIG)*, 2012, pp. 1–7.

[23] J. Li, Y. Wang, T. Tan, and A. K. Jain, “Live face detection based on the analysis of Fourier spectra,” in *Biometric Technology for Human Identification*, Aug. 2004, vol. 5404, pp. 296–303, doi: 10.1117/12.541955.

[24] W. Liu, “Face liveness detection using analysis of fourier spectra based on hair,” in *International Conference on Wavelet Analysis and Pattern Recognition*, Jul. 2014, vol. 2014-Janua, pp. 75–80, doi: 10.1109/ICWAPR.2014.6961294.

[25] J. Peng and P. P. K. Chan, “Face liveness detection for combating the spoofing attack in face recognition,” in *International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR’14)*, Jul. 2014, vol. 2014-Janua, pp. 176–181, doi: 10.1109/ICWAPR.2014.6961311.

[26] R. Raghavendra and C. Busch, “Novel presentation attack detection algorithm for face recognition system: Application to 3D face mask attack,” in *2014 IEEE International Conference on Image Processing, ICIP 2014*, Oct. 2014, pp. 323–327, doi: 10.1109/ICIP.2014.7025064.

[27] J. Komulainen, A. Hadid, and M. Pietikainen, “Context based face anti-spoofing,” in *IEEE 6th International Conference on Biometrics: Theory, Applications and Systems, BTAS 2013*, Sep. 2013, pp. 1–8, doi: 10.1109/BTAS.2013.6712690.

[28] M. R. Hasan, S. M. Hasan Mahmud, and X. Y. Li, “Face anti-spoofing using texture-based techniques and filtering methods,” *Journal of Physics: Conference Series*, vol. 1229, no. 1, p. 12044, May 2019, doi: 10.1088/1742-6596/1229/1/012044.

[29] A. Benlamoudi, K. E. Aiadi, A. Ouafi, D. Samai, and M. Oussalah, “Face antispoofing based on frame difference and multilevel representation,” *Journal of Electronic Imaging*, vol. 26, no. 4, p. 043007, Jul. 2017, doi: 10.1117/1.jei.26.4.043007.

[30] P. Viola and M. J. Jones, “Robust real-time face detection,” *International Journal of Computer Vision*, vol. 57, no. 2, pp. 137–154, 2004, doi: 10.1023/B:VISI.0000013087.49260.fb.

[31] X. Tan, F. Song, Z.-H. Zhou, and S. Chen, “Enhanced pictorial structures for precise eye localization under incontrolled conditions,” in *IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2009)*, Jun. 2009, pp. 1621–1628, doi: 10.1109/cvpr.2009.5206818.

[32] F. A. Pujol, M. J. Pujol, C. Rizo-Maestre, and M. Pujol, “Entropy-based face recognition and spoof detection for security applications,” *Sustainability (Switzerland)*, vol. 12, no. 1, pp. 1–18, Dec. 2020, doi: 10.3390/SU12010085.

[33] C. C. Chang and C. J. Lin, “LIBSVM: a Library for support vector machines,” *ACM Transactions on Intelligent Systems and Technology*, vol. 2, no. 3, pp. 1–27, Apr. 2011, doi: 10.1145/1961189.1961199.

[34] H. Li, P. He, S. Wang, A. Rocha, X. Jiang, and A. C. Kot, “Learning generalized deep feature representation for face anti-spoofing,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2639–2652, Oct. 2018, doi: 10.1109/TIFS.2018.2825949.

[35] A. George and S. Marcel, “Deep pixel-wise binary supervision for face presentation attack detection,” Jun. 2019, doi: 10.1109/ICB45273.2019.8987370.

[36] O. Sharifi, “Score-level-based face anti-spoofing system using handcrafted and deep learned characteristics,” *International Journal of Image, Graphics and Signal Processing*, vol. 11, no. 2, pp. 15–20, Feb. 2019, doi: 10.5815/ijigsp.2019.02.02.

[37] H. Chen, G. Hu, Z. Lei, Y. Chen, N. M. Robertson, and S. Z. Li, “Attention-based two-stream convolutional networks for face spoofing detection,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 578–593, 2020, doi: 10.1109/TIFS.2019.2922241.

[38] K. Kollreider, H. Fronthaler, and J. Bigun, “Non-intrusive liveness detection by face images,” *Image and Vision Computing*, vol. 27, no. 3, pp. 233–244, Feb. 2009, doi: 10.1016/j.imavis.2007.05.004.

[39] X. Li, J. Komulainen, G. Zhao, P. C. Yuen, and M. Pietikainen, “Generalized face anti-spoofing by detecting pulse from face videos,” in *International Conference on Pattern Recognition*, Dec. 2016, vol. 0, pp. 4244–4249, doi: 10.1109/ICPR.2016.7900300.

[40] T. Edmunds and A. Caplier, “Motion-based countermeasure against photo and video spoofing attacks in face recognition,” *Journal of Visual Communication and Image Representation*, vol. 50, pp. 314–332, Jan. 2018, doi: 10.1016/j.jvcir.2017.12.004.

[41] T. D. F. Pereira *et al.*, “Face liveness detection using dynamic texture,” *Eurasip Journal on Image and Video Processing*, vol. 2014, no. 1, Jan. 2014, doi: 10.1186/1687-5281-2014-2.

[42] S. Liu, P. C. Yuen, S. Zhang, and G. Zhao, “3D mask face anti-spoofing with remote photoplethysmography,” in *European conference on Computer Vision*, 2016, vol. 9911, pp. 58–100, doi: 10.1007/978-3-319-46478-7_6.

[43] Z. Boulkenafet, J. Komulainen, and A. Hadid, “Face antispoofing using speeded-up robust features and fisher vector encoding,” *IEEE Signal Processing Letters*, vol. 24, no. 2, pp. 141–145, 2017, doi: 10.1109/LSP.2016.2630740.

[44] L. Feng *et al.*, “Integration of image quality and motion cues for face anti-spoofing: a neural network approach,” *Journal of Visual*

Communication and Image Representation, vol. 38, pp. 451–460, Jul. 2016, doi: 10.1016/j.jvcir.2016.03.019.

[45] J. Gan, S. Li, Y. Zhai, and C. Liu, "3D convolutional neural network based on face anti-spoofing," in *2nd International Conference on Multimedia and Image Processing, ICMIP 2017*, Mar. 2017, vol. 2017-Janua, pp. 1–5, doi: 10.1109/ICMIP.2017.9.

[46] Y. Liu, A. Jourabloo, and X. Liu, "Learning deep models for face anti-spoofing: binary or auxiliary supervision," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, Jun. 2018, pp. 389–398, doi: 10.1109/CVPR.2018.00048.

[47] L. Li and X. Feng, "Face anti-spoofing via deep local binary pattern," in *Deep Learning in Object Detection and Recognition*, Springer Singapore, 2019, pp. 91–111.

[48] E. Fourati, W. Elloumi, and A. Chetouani, "Anti-spoofing in face recognition-based biometric authentication using image quality assessment," *Multimedia Tools and Applications*, vol. 79, no. 1–2, pp. 865–889, Oct. 2020, doi: 10.1007/s11042-019-08115-w.

[49] X. Cheng, H. Wang, J. Zhou, H. Chang, X. Zhao, and Y. Jia, "DTFA-Net: dynamic and texture features fusion attention network for face antispoofing," *Complexity*, vol. 2020, pp. 1–11, Jul. 2020, doi: 10.1155/2020/5836596.

[50] G. Pan, L. Sun, Z. Wu, and Y. Wang, "Monocular camera-based face liveness detection by combining eyeblink and scene context," *Telecommunication Systems*, vol. 47, no. 3–4, pp. 215–225, Aug. 2011, doi: 10.1007/s11235-010-9313-3.

[51] J. Yang, Z. Lei, and S. Z. Li, "Learn convolutional neural network for face anti-spoofing," *arXiv preprint arXiv:1408.5601*, 2014, [Online]. Available: http://arxiv.org/abs/1408.5601.

[52] M. Y. Nikitin, V. S. Konushin, and A. S. Konushin, "Face anti-spoofing with joint spoofing medium detection and eye blinking analysis," *Computer Optics*, vol. 43, no. 4, pp. 618–626, Aug. 2019, doi: 10.18287/2412-6179-2019-43-4-618-626.

[53] U. Muhammad, T. Holmberg, W. C. De Melo, and A. Hadid, "Face anti-spoofing via sample learning based recurrent neural network (RNN)," in *30th British Machine Vision Conference 2019, BMVC 2019*, 2019, p. 113.

[54] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," in *Proceedings of 11th European Conference on Computer Vision (ECCV'10)*, 2010, vol. 6316 LNCS, no. PART 6, pp. 504–517, doi: 10.1007/978-3-642-15567-3_37.

[55] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: a public database and a baseline," Oct. 2011, doi: 10.1109/IJCB.2011.6117503.

[56] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks," in *Proceedings - 2012 5th IAPR International Conference on Biometrics, ICB 2012*, Mar. 2012, pp. 26–31, doi: 10.1109/ICB.2012.6199754.

[57] D. Wen, H. Han, and A. K. Jain, "Face spoof detection with image distortion analysis," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 746–761, Apr. 2015, doi: 10.1109/TIFS.2015.2400395.

[58] N. Kose and J. L. Dugelay, "Shape and texture based countermeasure to protect face recognition systems against mask attacks," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, Jun. 2013, pp. 111–116, doi: 10.1109/CVPRW.2013.24.

[59] Y. Liu, J. Stehouwer, A. Jourabloo, and X. Liu, "Deep tree learning for zero-shot face anti-spoofing," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, Jun. 2019, vol. 2019-June, pp. 4675–4684, doi: 10.1109/CVPR.2019.00481.

[60] O. Nikisins, A. Mohammadi, A. Anjos, and S. Marcel, "On effectiveness of anomaly detection approaches against unseen presentation attacks in face anti-spoofing," in *International Conference on Biometrics, ICB 2018*, Feb. 2018, pp. 75–81, doi: 10.1109/ICB2018.2018.00022.

BIOGRAPHIES OF AUTHORS

Vinutha H is an assistant professor at the Department of Computer Science and Engineering, Dr. Ambedkar Institute of Technology, Karnataka, India, and a research scholar at the Department of Computer Science and Engineering, BMS Institute of Technology and Management, Karnataka, India. She received her B.E. degree in Computer Science and Engineering from Visvesvaraya Technological University, India, in 2007. She received her Master's degree in Computer Science and Engineering from Visvesvaraya Technological University in 2011. She is currently pursuing her Ph.D. in the field of image processing and pattern recognition. She has nearly 8 years of industry, academic, and research experience. She is a member of professional bodies like ISTE and IAENG. Her research interests include pattern recognition, soft computing, machine learning, and artificial intelligence. She can be contacted at email: vinuthah@gmail.com.

Dr. Thippeswamy G is a professor at the Department of Computer Science and Engineering and Dean, Academics, BMS Institute of Technology and Management, Karnataka, India. He received his B.E. degree in computer science and engineering from Bangalore University, India, in 1993. He received his Master's degree in Computer Science from Bangalore University, India, in 1997. He received his Ph.D. degree from Mangalore University, India, in 2012. He has nearly 25 years of academic and research experience. He has presented and published 40 research papers. He was co-principal investigator for a DST-RFBR-sponsored international research project with Moscow State University, Moscow, Russia, twice: on spatial modeling of human faces for real-time analysis and classification during 2009–2011 and on mathematical models and morphological analysis-based algorithms for image comparison and classification in computer vision systems during 2017–2019. He is a member of many professional bodies, like CSI, ISTE, and FIE. He has many international interactions with the Department of Cybernetics and Mathematics at Moscow State University, Moscow, Russia; Lappeenranta University, Finland; the Department of Information Technology at the University of Malaya, Malaysia; the University of Kiel, Germany; and the University of Oulu, Finland. His research interests include computer vision, image processing, and pattern recognition. He can be contacted at email: swamy.gangappa@gmail.com.