A Review on Face Anti-Spoofing

Rizky Naufal Perdana[1], Igi Ardiyanto[2], Hanung Adi Nugroho[3]

***Abstract*—The biometric system is a security technology that uses information based on a living person's characteristics to verify or recognize the identity, such as facial recognition. Face recognition has numerous applications in the real world, such as access control and surveillance. But face recognition has a security issue of spoofing. A face anti-spoofing, a task to prevent fake authorization by breaching the face recognition systems using a photo, video, mask, or a different substitute for an authorized person's face, is used to overcome this challenge. There is also increasing research of new datasets by providing new types of attack or diversity to reach a better generalization. This paper review of the recent development includes a general understanding of face spoofing, anti-spoofing methods, and the latest development to solve the problem against various spoof types.**

***Keywords*—Image Processing, Biometric System, Face Spoof.**

I. INTRODUCTION

In the last few years, there has been an increase in control access based on the biometric system using unique personal biometric information from a human [1]. The main reasons for developing a biometric system are security breaches or false transactions in non-biometric systems, which tend to be cracked due to certain weaknesses. Biometrics can use physical or human characteristics for identification using palm/fingerprint, voice, eyes, and face. The face turns out to be one of the good options for an application because most mobile devices can be equipped with a camera; it can be used in a smartphone or social media access control.

Face recognition for security systems is widely used [2], but face recognition systems are vulnerable to counterfeiting attacks or so-called face spoofing using the presentation and replay attack. Therefore, face anti-spoofing has a goal to decide the face recognition system's captured image, whether it is real or fake. Even though it is difficult, it is very important to protect the face biometric systems from false authorization, especially with technology development to produce various kinds of attacks.

Face spoofing comes with many difficult challenges with the system itself and outside demand in a real-world application. The face spoofing technique trend tends to be in high computational models in order to achieve better accuracy without considering the memory or power cost [3]. The fact that new hardware development is improving each year will provide high computational power and memory to make these systems able to run with real-time performance. Furthermore, another trend is that biometric systems are now shifting to mobile devices or embedded systems [4], making the anti-spoofing system compact with low computation and storage costs.

One of many surveys in face spoofing discusses extensive detail [3], making it difficult for newcomers to understand the basic understanding of face spoof. On the contrary, this review discusses general information about face spoofing and the challenge in order to understand the basic knowledge of several approaches to address the spoofing problem. A short review of the seven new novelty is presented to see how far the latest methods have been developed. A comparison of the eight latest large databases of face spoof is presented to see the diversity and development of spoof type, which goal is to help any future research choosing a certain category to reach better generalization.

II. FACE ANTI-SPOOFING

A. Face Spoof

A face spoofing case is that a person tries to present fake evidence to the biometric system or face recognition to get the authorization in order to gain resources inside the system in the wrong way [3]. Face spoofing can be implemented by several methods with the help of photographs and videos. Good photographs can easily be obtained due to social network media with high-quality print, so do videos. Videos can be recorded from any mobile phone or some other digital device with a high specification camera. The last is mask replicating the real face.

Therefore, in face spoofing, many types of attacks can be performed. These spoofs are classified into photo attacks, video attacks, and mask attacks used to deceive the recognition system.

1) Photo Attack: A spoofing attack happens by showing a genuine user photograph to a biometric system. The attacker can use the photograph from the user's social media or use a digital camera or mobile phone to capture the photograph. The image is printed on paper; the attacker can also use a photographic mask. It is another way to face spoofing in which high-quality printed photographs are used. Then, the eyes and mouth area are cut out to make it more recognizable. The attacker then displays an image of the genuine user's face on the device's screen to the area capture of the camera or stands behind with the printed photo so that eye blinking and lip movement can be reproduced at the time.

2) Video Attack: Video attacks are more progressive versions of photo attacks. The attacker prepared videos of a genuine user by using devices that can record high-quality viedos. By the time of spoofing, the attacker replays the recorded video of the genuine user in the camera's area of capture. Due to the precise movement of a face in the video, it becomes very hard to detect it as spoofing.

[1,2,3] *Department of Electrical and Information Engineering, Faculty of Engineering, Universitas Gadjah Mada, Jln. Grafika No. 2, Kampus UGM, Yogyakarta, 55281, INDONESIA (Tel. +62-274-552305, email:* [1]*rizky.naufal.p@mail.ugm.ac.id,* [2]*igi@ugm.ac.id,* [3]*adinugroho@ugm.ac.id)*

3) Mask Attack: This kind of attack takes place when the attacker makes a face mask based on a genuine user face with a very similar shape and characteristics of the real face. It is a further advanced version of printed attack and video attack because the mask is created using real materials that can mimic a face, such as plastic or silicone, to achieve depth cues. In face spoofing, mask attacks are not easy to be detected. However, these attacks are less common than photos and video attacks because the budget for this kind of attack is expensive.

B. Anti-Spoofing Methods

Face anti-spoofing is a security method to solve the problem before reaching the recognition phase [3]. The objective of anti-spoofing is to secure the biometric system from any users with illegal authorization. Usually, face detection and recognition systems do not have this kind of security; they work very poorly. The face anti-spoofing system must recognize whether the input image is acceptable or not. If the processed input is detected as a genuine user, it will continue to the next phase; otherwise, it will reset the system from the beginning. Anti-spoofing methods also need to meet some basic requirements such as the methods should not require excessive interaction, user-friendly, and fast; the cost should be low; the efficiency should be high. Several methods in face spoofing detection have been introduced are categorized into:

1) Texture: Texture-based methods concentrate on the shape, size, color, arrangement, and density of an image by identifying the texture in images [5]. The texture descriptors identified the texture differences and patterns like print failures and blurriness to spot spoofing. It is mainly based on differentiating between a genuine face and a spoof in texture features like shape and detailedness characteristics. This type of approach is the most widely used approach. However, it has a weakness in generalization ability.

2) Motion: This kind of method compares or detects the motion pattern from the genuine or spoof face in the image that has been captured [6]. Based on the opinion, the movement of 2D like print photo objects is totally different from the movements of real human faces since it is a 3D object. This method can distinguish between the genuine face and spoofing through eye blinking, mouth movement, and head rotation. By using motion analysis, spoofing by 2D face spoof becomes very hard as the motion analysis requires a video. If the video has low quality or motion activity, it becomes difficult to spoof. At the same time, it also has a weakness if a video with high quality is used.

3) Image Quality: This method aims to differentiate the image quality between genuine face and spoof [7]. This approach is based on spoofing, and genuine images have differences in quality captured by the system. Features like a blur, chromatic moment, specular reflection can be used to measure the quality of an image to differentiate the spoof from a real face.

4) Frequency: The frequency-based method is using noise signals in the captured image or video to differentiate between the genuine face and spoof attacks [8]. It is based on the opinion that there will be a variation in frequency in captured images or videos. This method is based on frequency analysis to detect face spoofing because the content of a spoofing image stands out more sharply in certain regions of the 2D Fourier spectra. Therefore, it is enough to use the information about the regions to classify the input video or image as genuine or spoof.

5) Deep Learning: Because of its popularity, deep learning techniques are also considered effective in solving the issue of building an anti-spoofing system. In the deep learning technique, a convolution neural network is used to detect spoofing attacks [9]. The process takes an input image, a process that consists of neurons that have a function of weight, bias, and activation, then classify it into certain categories. The 3D depth and infrared images or any multimodal databases can also improve the learning process of spoof detection using deep learning.

C. Face-Spoofing Dataset

The main reason for developing a spoof dataset is the anti-spoofing system needs datasets that have both quantity and diversity [10]–[17]. A human face consists of many features that vary in shape and color. Researchers around the world need a large-scale database for face anti-spoofing to overcome this challenge. Several types of the dataset are categories into:

1) Single Modal: The dataset consists of images and videos that are generated by having genuine persons trying to access a recognition system or by presenting photos or videos recording of the persons. The variety of datasets is usually separated into different protocols to build many types of spoofs or under different quality and lighting conditions, but only in one type of visual image such as RGB.

2) Multimodal: The multimodal dataset consists of different types of visual images such as RGB, IR, heat, and depth. The goal of a multimodal dataset is to increase the diversity of anti-spoofing research since the algorithms that are trained in a specific modality can mostly only be implemented in the same type.

3) Wild Spoof: This type of dataset consists of images and videos collected in the wild or a real environment in a biometric system. It is specifically designed for unknown attacks to increase diversity; therefore, the trained algorithm can be used in the real scene.

III. Application & Architecture

Each year the latest technology became more powerful, software and hardware became more adaptable to each other; one of them is applications of the face biometric system that can be used for many purposes. The main purpose of the development is to increase safety, and because of that, it has become an important function in devices for some industries or

governments [3]. Building such a way of securing access inside systems to ensure one's safety are important. It is built to prevent an act of crime such as stealing with the identities of authorized users. Hence, it can decrease the crime rates. The applications using the biometric system can be put into two categories by type.

D. Single Modal

The single modal system uses only one biometric characteristic to detect the spoof. The system can be dependable and accurate, but it faces some issues such as:

- the noise of biometric input can make false information for the system;
- the system becomes non-universal because of the specific data training; and
- vulnerable to variation of spoofing attacks.

E. Multimodal/Fusion

The multimodal or fusion becomes more accessible and more common due to the hardware development and the current research. One example of a fusion biometric system is its feature face, eyes/iris, and ear to recognize the user. Combining different traits will eliminate the weakness of single-modal and make the system have advantages such as:

- increase success rate by eliminating individual weaknesses; and
- increase versatility for various spoofing.

F. Architecture

In the face spoofing system, sensors/cameras are used to capture the image of a face. The system then preprocesses the image, such as resize, noise removal, conversion, etc. After the image has been processed, the feature extraction can be performed using any available technique which can distinguish between a genuine face and a spoof. It can be more than one method, the so-called multimodal system using the same or entirely different input to improve the result. After that, the system will decide to enter the next phase or not. The overview process of face anti-spoofing can be seen in Fig. 1.

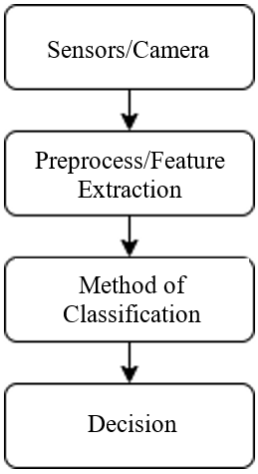


Fig. 1 General architecture in face anti-spoofing system.

IV. Recent Development

In this section, there will be a short review of some related works of anti-spoof methods and datasets.

A. Methods

1) Spoof Trace Disentanglement Network (STDN): This research proposes a novel network named Spoof Trace Disentanglement Network (STDN) to solve the challenging problem of disentangling spoof traces from faces into a hierarchical representation [18]. The research reconstructed the live counterpart and synthesized a new spoof from the live one using the spoof traces. By using a 3D warp layer to deform traces, it corrects the geometric discrepancy in synthesizing new spoof and enhances the training. The disentanglement technique improves in known and unknown spoofing, and it can also provide visual evidence to help the model making a decision.

2) Multi-Channel Convolutional Neural Network: This research proposes a novel framework for Presentation Attack Detection (PAD) using a one-class classifier and Multi-Channel Convolutional Neural Network learned from the representation [19]. Using the loss function makes the network forced to learn a compact embedding yet effective for genuine class while differentiating from the representation of spoofs and using one-class Gaussian Mixture Model on top of the embeddings for the PAD. The proposed framework introduced a new approach to learn a solid PAD system to spot genuine face and spoof classes. The system was evaluated using publicly known databases. The result showed better performance and effectiveness in unknown spoof protocols.

3) Zero-shot Face Anti-Spoofing: This research proposes a method by using the novel Deep Tree Network (DTN) to route the unseen attacks to the most proper leaf node named Zero-Shot Face Anti-spoofing (ZSFA) [12]. Zero-shot object recognition, or more commonly known as zero-shot learning, has a goal to recognize the objects from complex or unknown cases. Previous ZSFA research only studies a few spoofs like print and replay, limiting the insight on the real issue. This research studied the ZSFA issue with 13 types of spoofs, including print, video, mask, etc. The Network would classify any spoof samples into sub-area, dealing with them in an unsupervised way. When an input sample entered the system, either known or unknown spoof, DTN would treat it with the most similar case area and decide.

4) Central Difference Convolutional Network: This research proposes a novel anti-spoofing method based on Central Difference Convolution (CDC) to solve the spoofing challenge [20]. The method could capture detailed patterns with amount intensity and gradient information; then, the designed model was named Central Difference Convolutional Network (CDCN) based on CDC. It was also introduced CDCN++ by a specifically designed CDC search area. It then utilized Neural Architecture Search (NAS), discovering a more powerful

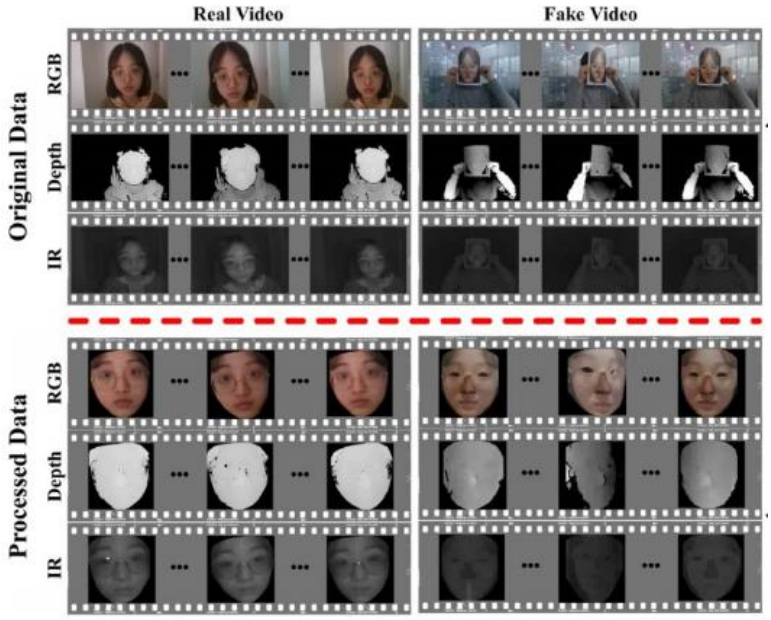


Fig. 2 The CASIA-SURF dataset sample before and after preprocess with different modalities [13].

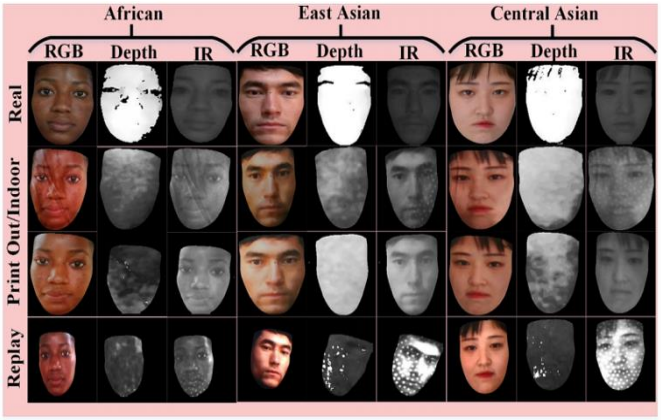


Fig. 3 The CASIA-SURF-CeFA dataset sample of 3 different ethnicities and modalities [14].

network structure, consisting of a searched CDC backbone and Multiscale Attention Fusion Module (MAFM) to reach a better result. Comprehensive experiments were tested using the proposed methods showing the system performed better in the intra-test and the cross-test dataset.

5) Deep Spatial Gradient and Temporal Depth Learning: This research proposes a novel method that utilized fine-grained Spatio-temporal information for facial depth estimation [21]. The approach to spot spoofs from multiple frames based on detailed distinctions information between genuine faces and spoofs might be discarded through stacked vanilla convolutions. The movement of genuine faces provided specific information in spotting the spoof by making use of Residual Spatial Gradient Block (RSGB) to find more detailed distinctions. At the same time, Spatio-Temporal Propagation Module (STPM) efficiently encoded spatio-temporal information. It also presented Contrastive Depth Loss (CDL) to improve the PAD generality for more accurate depth supervision.

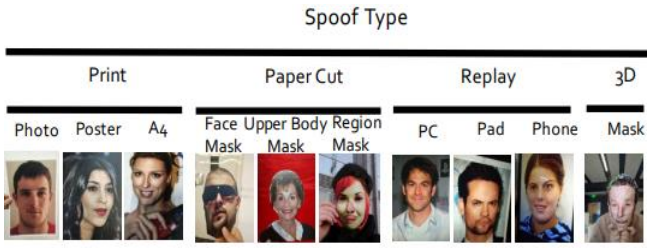
6) Learning Generalizable and Identity-Discriminative Representations: This research proposes two novelties, Total Pairwise Confusion (TPC) loss, simple but effective for Convolutional Neural Network (CNN) training to enhance generalization of PAD [22]. Then, the CNN model and the Fast Domain Adaptation (FDA) component were combined to lessen the negative effects of domain changes. The model, called Generalizable Face Authentication CNN (GFA-CNN), had goal to support generalization and applicational. The model also worked in a multi-task way meaning that the model would work with face recognition simultaneously. The GFA-CNN model's performance achieved good results in the cross-test dataset and high accuracy in face recognition.

7) Convolutional Neural Networks as Light as Feather: This research proposes a light CNN architecture to solve the issue of high computation and storage cost called FeatherNet [9]. Since the network had a thin stem, it would make the computational cost less. A new architecture named as Streaming Module, a Global Depthwise Convolution layer, showed better results than using the Global Average Pooling approach. It also introduced a novel fusion process using ensemble+cascade structure and showed better performance in the single model classifiers.

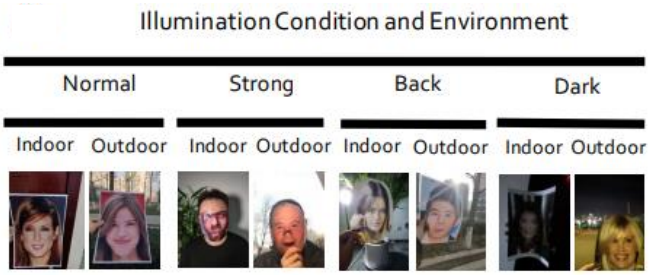
Table I shows a short review of related works of anti-spoof methods and datasets used in each study.

B. Dataset

1) CASIA Databases: In the development of face anti-spoofing datasets throughout the year, most datasets have a limited number not only in subjects but also in modalities; this is one of the reasons why development cannot go much further. To help future research in face anti-spoofing, CASIA-SURF has been introduced as a large-scale multimodal database that has multiple modalities and a huge number of subjects [13].



(a)



(b)

Fig. 4 The CelebA-Spoof dataset sample with rich annotation, (a) type of attacks, (b) sessions [15].

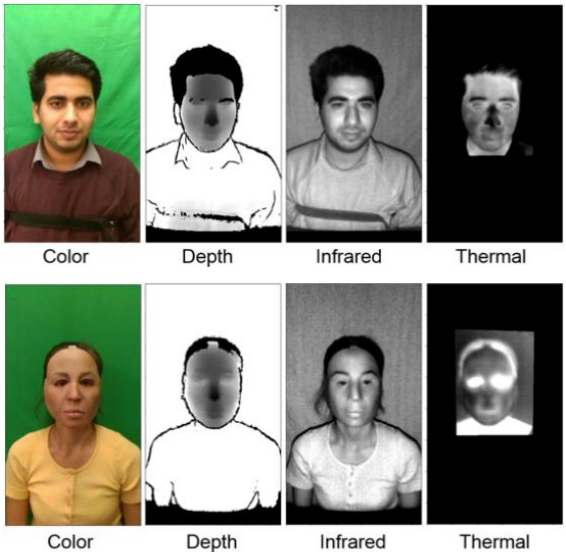


Fig. 5 The WMCA dataset sample of four different modalities [16].

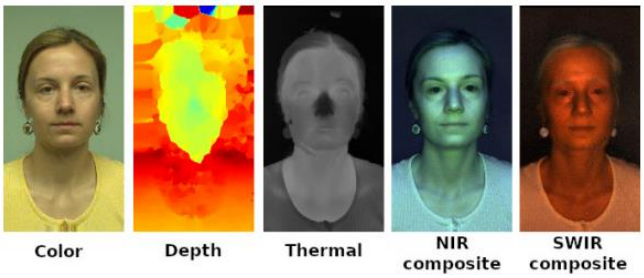


Fig. 6 The HQ-WMCA dataset sample of five different modalities [17].

The dataset consists of three types of modalities in RGB, Depth, and IR samples, each with 1,000 subjects and 21,000 videos.

The CASIA database has been developed further and increases the diversity briefly named CASIA-SURF Cross-

Fig. 7 The SiW dataset sample of genuine faces (top) and spoof (bottom) videos [11].

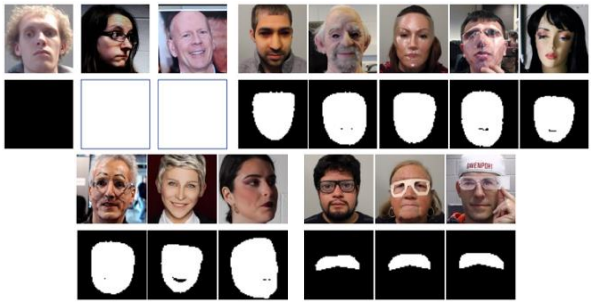


Fig. 8 The SiW-M dataset sample of the one genuine face and 13 types of spoof with ground truth [12].

Fig. 9 The OULU-NPU dataset sample with 6 different sensors/cameras [10].

ethnicity Face Anti-spoofing (CeFA) consisting of multi ethnicities (Africa, East Asia, and Central Asia), three types of modalities, 1,607 subjects, and 2D as well as 3D spoofs [14]. Some samples of CASIA-SURF can be seen in Fig. 2 and CASIA-SURF-CeFA in Fig. 3.

2) CelebA-Spoof Database: The existing methods still struggle with solving complex and unknown spoof to generalize real-case scenarios. Datasets need both quantity and diversity to help further research. CelebA-Spoof contains 625,537 pictures of 10,177 subjects [15]. By capturing the spoofing image from eight scenes (2 environments × 4 illumination conditions) with more than ten sensors will increase the diversity of datasets. The dataset also has ten types of spoof annotations and 40 attribute annotations inherited from its predecessor. Some samples of CelebA-Spoof are shown in Fig. 4.

3) WMCA Databases: The use of multiple channels makes the biometric systems more difficult to spoof. Wide Multi-Channel Presentation Attack (WMCA) database has 72 different subjects consists of multimodal 2D spoofs using print or replay and 3D spoofs like masks (paper, silicone, rigid, transparent), non-medical eyeglasses, and mannequins for both impersonation and obfuscation [16]. The database has different channel images like color/RGB, depth, IR, and thermal to help further research in face anti-spoofing.

TABLE I
SUMMARY OF RECENT FACE SPOOF METHOD

Ref.	Method	Databases	Novelty
[18]	Spoof Trace Disentanglement Network	OULU-NPU, SiW, SiW-M	Spoof Trace Classification
[19]	Multi-Channel Convolutional Neural Network	WMCA, MLFP, SiW-M	Loss Function, Multi-Channel One-Class Classifier
[12]	Zero-shoot Face Anti-Spoofing	CASIA, Replay-Attack, MSU-MFSD, SiW-M	Deep Tree Network with Unsupervised Learning
[20]	Central Difference Convolutional Network	OULU-NPU, SiW, CASIA-MFSD, Replay-Attack, MSU-MFSD, SiW-M	Central Difference Convolution
[21]	Deep Spatial Gradient and Temporal Depth Learning	OULU-NPU, SiW, CASIA-MFSD, Replay-Attack, DMAD	Depth Supervised Spatio-Temporal Network
[22]	Learning Generalizable and Identity-Discriminative Representations	CASIA-FASD, Replay-Attack, MSU-MFSD, Oulu-NPU, SiW	Total Pairwise Confusion + Fast Domain Adaptation
[9]	Convolutional Neural Networks as Light as Feather	CASIA-SURF, MMFD	Ensemble + Cascade Fusion Architecture

TABLE II
COMPARISON OF RECENT FACE SPOOF DATABASES (V: VIDEO & I: IMAGE)

Ref.	Database	Year	Modality	Subject	Data	Sensor	Pose Range	Type & Complexity
[10]	OULU-NPU	2017	RGB	55	5,940 (V)	6	Frontal	Print, Replay (Multi-session with few ethnicities)
[15]	CelebA-Spoof	2020	RGB	10,177	625,537 (I)	> 10	Frontal	Print, Replay, 3D Mask, Paper Cut (Multi-session with few ethnicities)
[11]	SiW	2018	RGB	165	4,620 (V)	2	[-90°,90°]	Print, Replay (Multi-session with various ethnicity)
[12]	SiW-M	2019	RGB	493	1,628 (V)	4	[-90°,90°]	Print, Replay, 3D Mask, Make up, Partial (Multi-session with various ethnicity)
[13]	CASIA-SURF	2019	RGB/IR/Depth	1,000	21,000 (V)	1	Frontal	Print, Replay (Few sessions with few ethnicities)
[14]	CASIA-SURF-CeFA	2020	RGB/IR/Depth	1,607	23,538 (V)	1	Frontal	Print, Replay, 2D/3D Mask (Multi-session with various ethnicity)
[16]	WMCA	2019	RGB/IR/Depth/ Thermal	72	6,716 (V)	2	Frontal	Print, Replay, 2D/3D Mask (Multi-session with various ethnicity)
[17]	WMCA-HQ	2020	RGB/IR/Depth/ Thermal/NIR/SWIR	51	2,904 (V)	5	Frontal	Print, Replay, 2D/3D Mask, Makeup, Partial, Wigs, Mannequin (Multi-session with various ethnicity)

In the latest development named High-Quality Wide Multi-Channel Attack (HQ-WMCA), it developed much further of multimodal or multi-channel such as color/RGB, depth, thermal, IR (spectra), and short-wave (spectra) [17]. The databases consist of 555 genuine and 2,349 spoofs from 51 subjects. Some samples of WMCA can be seen in Fig. 5 and HQ-WMCA in Fig. 6.

4) SiW Databases: The development of anti-spoofing methods resulting in a new way of spoof that has been created to bypass the biometric system. A database, the so-called Spoof in The Wild (SiW), has been developed to test the existing face anti-spoofing methods to overcome the challenge of unknown spoof [11]. The Database consists of 165 subjects, 6 spoofing mediums, and 4 sessions in variations of poses, illuminations, expressions (PIE), and camera distance. Some samples of SiW can be seen in Fig. 7.

In the latest development, the so-called Spoof in the Wild database with Multiple Attack Types (SiW-M) has more diversity considering a scenario of spoof recognition as someone else called impersonation and removing the attacker's

own identity called obfuscation [12]. It consists of 968 videos with 13 different types of spoofs and 680 videos of 493 live subjects with addition in ethnicity and age to increase diversity. Some samples of SiW-M can be seen in Fig. 8.

5) OULU-NPU Database: Introduced as OULU-NPU [10], a face PAD database has developed to evaluate the generalization of face anti-spoof technique in real case scenarios to increase diversity so the trained algorithm can be implemented in real life. It consists of videos with an unknown environment which is three different illumination and background areas. The videos are recorded using six different smartphone front cameras with two types of spoofs: prints attack and videos attack. The database consists of 5,940 videos and 55 subjects. Some samples of OULU-NPU can be seen in Fig. 9. Table II shows the comparison of complexity between the database in each study.

V. Conclusion

Spoofing attacks have been proved to be a significant threat for face biometric systems. Thus, researchers have proposed various anti-spoofing methods. Despite the trend in better generalization with various spoofs, most research does not calculate or show whether certain aspects, such as the system, run with high computational and storage costs or not. Therefore, most of the methods still have limitations for real-case applications. However, many researchers have searched for further development in many fusion methods and created diverse databases. Each development makes a transition to fill the gap between academic purpose to real-case application. This paper presents an overview of face spoof and recent development in spoofing methods and datasets, which can be used for future research.

References

[1] J. Stehouwer, A. Jourabloo, Y. Liu, and X. Liu, "Noise Modeling, Synthesis and Classification for Generic Object Anti-Spoofing," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, 2020, pp. 7292–7301.

[2] M.O. Oloyede, G.P. Hancke, and H.C. Myburgh, "A Review on Face Recognition Systems: Recent Approaches and Challenges," *Multimed. Tools Appl.*, Vol. 79, No. 37–38, pp. 27891–27922, 2020.

[3] L. Souza, L. Oliveira, M. Pamplona, and J. Papa, "How Far did We Get in Face Spoofing Detection?" *Eng. Appl. Artif. Intell.*, Vol. 72, pp. 368–381, 2018.

[4] Y. Liu, J. Stehouwer, A. Jourabloo, Y. Atoum, and X. Liu, *Presentation Attack Detection for Face in Mobile Phones*, New York, USA: Springer International Publishing, 2019.

[5] R. Shao, X. Lan, and P.C. Yuen, "Joint Discriminative Learning of Deep Dynamic Textures for 3D Mask Face Anti-Spoofing," *IEEE Trans. Inf. Forensics Secur.*, Vol. 14, No. 4, pp. 923–938, 2019.

[6] H.E. Utami and H. Nugroho, "Face Spoof Detection by Motion Analysis on the Whole Video Frames," *Proc. 2017 5th Int. Conf. Instrumentation, Commun. Inf. Technol. Biomed. Eng. ICICI-BME 2017*, 2017, pp. 213–218.

[7] C.H. Yeh and H.H. Chang, "Face Liveness Detection Based on Perceptual Image Quality Assessment Features with Multi-scale Analysis," *Proc. - 2018 IEEE Winter Conf. Appl. Comput. Vision, WACV 2018*, 2018, pp. 49–56.

[8] B. Chen, W. Yang, and S. Wang, "Face Anti-Spoofing by Fusing High and Low Frequency Features for Advanced Generalization Capability," *Proc. - 3rd Int. Conf. Multimed. Inf. Process. Retrieval, MIPR 2020*, 2020, pp. 199–204.

[9] P. Zhang, F. Zou, Z. Wu, N. Dai, S. Mark, M. Fu, J. Zhao, and K. Li, "FeatherNets: Convolutional Neural Networks as Light as Feather for Face Anti-Spoofing," *IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Work.*, 2019, pp. 1574–1583.

[10] Z. Boulkenafet, J. Komulainen, L. Li, X. Feng, and A. Hadid, "OULU-NPU: A Mobile Face Presentation Attack Database with Real-World Variations," *Proc. - 12th IEEE Int. Conf. Autom. Face Gesture Recognition*, 2017, pp. 612–618.

[11] Y. Liu, A. Jourabloo, and X. Liu, "Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, 2018, pp. 389–398.

[12] Y. Liu, J. Stehouwer, A. Jourabloo, and X. Liu, "Deep Tree Learning for Zero-Shot Face Anti-Spoofing," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, 2019, pp. 4675–4684.

[13] S. Zhang, A. Liu, J. Wan, Y. Liang, G. Guo, S. Escalera, H. Escalante, and S. Li, "CASIA-SURF: A Large-Scale Multimodal Benchmark for Face Anti-Spoofing," *IEEE Trans. Biometrics, Behav. Identity Sci.*, Vol. 2, No. 2, pp. 182–193, Apr. 2020.

[14] A. Liu, Z. Tan, X. Li, J. Wan, S. Escalera, G. Guo, and S. Li, "CASIA-SURF CeFA: A Benchmark for Multimodal Cross-Ethnicity Face Anti-Spoofing," *arXiv:2003.05136*, pp. 1–17, 2020.

[15] Y. Zhang, Z. Yin, Y. Li, G. Yin, J. Yan, J. Shao, and Z. Liu, *CelebA-Spoof: Large-Scale Face Anti-Spoofing Dataset with Rich Annotations*, ser. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), Vol. 12357 LNCS, pp. 70–85, 2020.

[16] A. George, Z. Mostaani, D. Geissenbuhler, O. Nikisins, A. Anjos, and S. Marcel, "Biometric Face Presentation Attack Detection with Multi-Channel Convolutional Neural Network," *IEEE Trans. Inf. Forensics Secur.*, Vol. 15, No. 1, pp. 42–55, 2020.

[17] G. Heusch, A. George, D. Geissbühler, Z. Mostaani, and S. Marcel, "Deep Models and Shortwave Infrared Information to Detect Face Presentation Attacks," *arXiv:2007.11469*, Vol. 14, No. 8, pp. 1–12, 2020.

[18] Y. Liu, J. Stehouwer, and X. Liu, "On Disentangling Spoof Trace for Generic Face Anti-Spoofing," *arXiv:2007.09273*, pp. 1-17, 2020.

[19] A. George and S. Marcel, "Learning One Class Representations for Face Presentation Attack Detection Using Multi-Channel Convolutional Neural Networks," *IEEE Trans. Inf. Forensics Secur.*, Vol. 16, pp. 361–375, 2021.

[20] Z. Yu, C. Zhao, Z. Wang, Y. Qin, Z. Su, X. Li, F. Zhou, and G. Zhao, "Searching Central Difference Convolutional Networks for Face Anti-Spoofing," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, 2020, pp. 5294–5304.

[21] Z. Wang, Z. Yu, C. Zhao, X. Zhu, Y. Qin, Q. Zhou, F. Zhou, and Z. Lei, "Deep Spatial Gradient and Temporal Depth Learning for Face Anti-Spoofing," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, 2020, pp. 5041–5050.

[22] X. Tu, Z. Ma, J. Zhao, G. Du, M. Xie, and J. Feng, "Learning Generalizable and Identity-Discriminative Representations for Face Anti-Spoofing," *ACM Trans. on Intel. Sys. and Technol.*, Vol. 11, No. 5, pp. 1-19, 2020.