Presentation Attack Detection for Face Recognition on Smartphones: A Comprehensive Review

Idris Abdul Ghaffar, Mohd Norzali Haji Mohd
Embedded Computing Systems (EmbCos) Research Group,
Biomedical Modelling and Simulation (BIOMEMS) Research Group,
Faculty of Electrical and Electronics Engineering, University Tun Hussien Onn Malaysia,
86400 Parit Raja, Batu Pahat, Johor, Malaysia
idris@kumpul.info

***Abstract*—Even though the field of Face Presentation Attack Detection (PAD) has been around for quite a long time, but still it is quite a new field to be implemented on smartphones. Implementation on smartphones is different because the limited computing power of the smartphones when compared to computers. Presentation Attack for a face recognition system may happen in various ways, using photograph, video or mask of an authentic user's face. The Presentation Attack Detection system is vital to counter those kinds of intrusion. Face presentation attack countermeasures are categorized as sensor level or feature level. Face Presentation Attack Detection through the sensor level technique involved in using additional hardware or sensor to protect recognition system from spoofing while feature level techniques are purely software-based algorithms and analysis. Under the feature level techniques, it may be divided into liveness detection; motion analysis; face appearance properties (texture analysis, reflectance); image quality analysis (image distortion); contextual information; challenge response. There are a few types of research have been done for face PAD on smartphones. They also have released the database they used for their testing and performance benchmarking.**

***Index Terms*—Anti-spoofing; Face Recognition; Presentation Attack Countermeasures; Presentation Attack Detection.**

I. INTRODUCTION

Personal authentication using biometrics technologies have nowadays evolved into getting as a way of life. It is getting important in every aspect of our life. One of the essential expect in our life is our smartphone. We do everything on our smartphone. Protecting smartphones using biometrics such as fingerprint and face unlock are available now. The ability to use our smartphone for mobile payment using biometric fingerprint is also possible now with the Apple Pay and Samsung Pay. In the future, there will be much more security critical application will run on our phone and require our biometric traits. With this advancement, there is a possibility these systems may be fooled or spoofed. The need to protect the system from spoofing is also increasingly important and should be looked into thoroughly. ISO/IEC JTC 1/SC 37 overlooked the biometric since 2002. In 2016, they introduced a new standard for anti-spoofing. It is officially known as ISO/IEC 30107-1:2016 Information technology -- Biometric presentation attack detection -- Part 1: Framework.

Presentation Attack Detection for face authentication on a smartphone has recently been attracting researchers and begin to get traction. This is the future way to go. It is not just for phone unlocking only, but apps using it as well. This paper will be looking into what kind of presentation attack detection for face authentication on smartphones has been researched all this while.

II. PRESENTATION AND THE PRESENTATION ATTACK INSTRUMENTS

Generally, in a biometric system, presentation is a process of presenting the user trait to the sensor. For a face recognition system, this is a process of presenting the face of a person to the camera. When a genuine user presented his/her face to the camera, the system will allow access for that user. However, an unauthorized user may try to access the system by trying to impersonate a real genuine user. This is known as presentation attack. Presentation attack may be carried out by various means. All those means are to fool the system into thinking that the genuine user is accessing the system. Presentation Attack Instruments (PAI) are the tools used to attack the face recognition system. PAI is classified into two: Artificial or Human. Figure 1 breaks down all the PAI for a face recognition system.

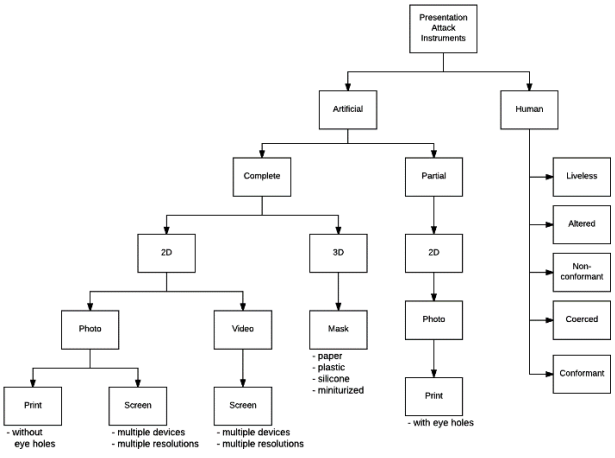

Figure 1: Presentation Attack Instruments for Face Recognition System

A. Artificial Presentation Attack Instruments

Under the Artificial PAI, classification can be made as Complete or Partial. Partial include using 2D photo print-out with eye holes. For Complete Artificial PAI, it can be either 2D or 3D.

B. Photo Presentation Attack Instruments

These attacks are carried out using a photograph of a real user. By far, this is the most common kind of attack

considering that it is easier to source for a photo of the real user. The photograph is shown to the camera in order to fool the system into thinking that the real user is present in front of the camera. The photograph of the real user may be taken by the attacker using a digital camera or easily obtained on online social media such as Facebook, Instagram, Twitter, etc [1].

The photograph of the real user then can either be printed onto a piece of paper or displayed on a screen of digital devices such as mobile phone, tablets, and laptop [2][3].

The life-size face print-out can be put on the imposter's face. Cutting through around the eyes of the print-out will make eye blinking detection possible [4]. Figure 2(a) shows how a presentation attack using a photo print-out.

C. Video Presentation Attack Instruments

Instead of using still photos, an imposter may attack the system by playing back a recorded video of a real user. The video can be played on mobile screen, tablet, or laptop and ultrabooks. This method is also known as replay attacks. [4] [5] [6]. Figure 2(b) shows how a presentation attack using a video replay.

D. Mask Presentation Attack Instruments

A more challenging kind of attack is the mask attack. Mask can be produced from various kind of material. It will replicate the face of a real user. A real face can also be produced by a 3D printer. This is also considered as mask attack [7] [8] [9]. Anybody can have a face mask of another person by having that person's frontal photo and side photos. This service is provided by thatmyface.com [10]. Figure 2(c) shows how a presentation attack using a mask.

(a) (b) (c)

Figure 2: (a) An example of presentation attack using a print-out photo. Photo from IDIAP website. (b) An example of presentation attack using video replay on a mobile device [8]. (c) An example of a mask used for face spoofing. Photo from University Oulu, Finland website

E. Human Presentation Attack Instruments

Human PAIs are very difficult and might be impossible to detect. The following falls under the Human PAI category:

- *Lifeless* – Using the actual face of the dead person or cadaver
- *Altered* – Make use of plastic surgery to alter/modify an imposter face to look like the real user face.
- *Non-Conformant* – facial expression/extreme.
- *Coerced* –The real genuine user is unconscious, under duress
- *Conformant* – zero effort impostor attempt

The Human PAI is out of the scope of this paper and will not be discussed any further.

III. Presentation Attack Detection

Presentation Attack Detection (PAD) is the countermeasure to detect and defeat presentation attacks to a biometric system. For a face recognition system, the presentation attack detection will try to detect and defeat all of the attacks as mentioned previously. In general, PAD will try to differentiate between access by a real genuine user and an imposter trying to access the system by using other means.

PAD does not work on its own, it is used in conjunction with a face recognition system. It is to authenticate the face used by the recognition process is a real person face and not fake faces. Figure 3 shows the PAD and Face Recognition system working together.

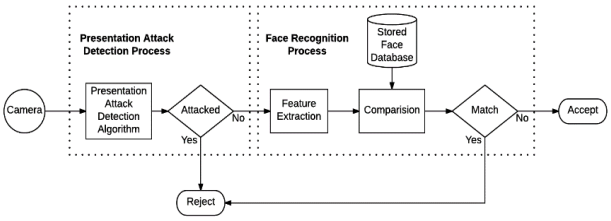

Figure 3: Combination of PAD and face Recognition system to make a complete system

IV. Category Presentation Attack Detection

Many types of research have been done by various groups in this area and may method and algorithms has been proposed. Out of all the method proposed and developed, it is categorized into two very basic categories: sensor-level and feature-level. See Figure 4.

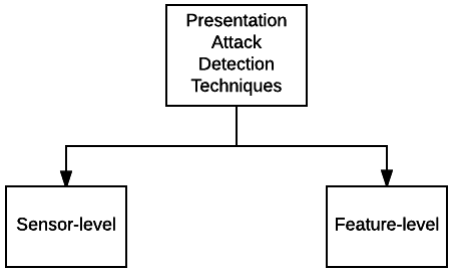

Figure 4: The Basic Presentation Attack Detection Techniques

Sensor-Level Techniques. It is also known as hardware-based techniques. This technique will require additional sensor besides a camera in order to detect another trait of a user. This may include facial thermogram, blood pressure, fingerprint sweat, gait etc. For an example, please refer [11] and [12].

Feature-Level Techniques. It is also known as software-based techniques. It will rely on algorithms to detect presentation attack and does not include any additional sensor beside the standard camera.

This article will focus on the Feature-Level Techniques of PAD because a standard smartphone is equipped with cameras (front and back) only. It does now have any other sensor.

V. Feature-Level Presentation Attack Detection Techniques

These are basically the face presentation attack detection techniques which purely rely on algorithm and software:

- liveness detection
- motion analysis

- face appearance properties (texture analysis, reflectance)
- image quality analysis (image distortion)
- contextual information
- challenge response

A. Liveness Detection

This kind of PAD technique is utilised in [4], [13], [14]. This is the most elementary and common technique. It will try to detect physiological signs of life in the face captured by the camera. Detection includes eye blinking, facial expression changes, head movement and mouth movements [15]. This technique may be best dealing with photograph based spoofing but not very suitable for video playback spoofing since it can be replicated in a video.

B. Motion Analysis

In general, this technique will try to detect spontaneous movement clues generated when 2D spoof photo or video are presented to the camera. [16]

The analysis is based on series of images captured by the camera and to compare the movement of planar objects such as photographs and video playback which is different with a real face. Assuming that facial parts in real faces do not move the same as on photographs, the optical flow-based method can capture and track the subtle relative movements between different facial parts to determine spoofing [17].

C. Facial Appearance Properties

This presentation attack detection technique will analyse facial appearance properties such as the face reflectance and the face texture. The reflectance and texture of a real face are different compared to a spoof face.

D. Image Quality Analysis

This technique will try to detect the presence of image distortion usually found in the spoofed face.

Colour Distortion. Colour distribution may be different between face printed on a paper, face displayed on mobile devices and a real face [18]. Those differences can be analysed to determine face spoofing.

Moiré Pattern. During various image acquisition and image display process, undesired aliasing of images was produced. Moiré patterns are actually pattern produced when two or more patterns are overlapping on top of each other, which will result in the appearance of the new third pattern. Photo of a face printed using CYMK, photos and videos displayed on mobile devices display will exhibit this Moiré patterns [19]. Figure 5 displays the Moiré pattern produced.

Face Shape Deformation. This is especially true in the case of print attacks. The photo might be bend while an imposter holding it and this may skew the shape of the spoof face.

E. Contextual Information

When trying to detect presentation attack, it is also important to analyse the scene and the environment as well. This technique will look for any abnormality within the scene, in particular, a person holding a mobile device or a piece of paper with a photo of a face [20].

Figure 5: Example of Moiré patterns due to the overlapping of digital grids. (a) Portion of the Lena test image. (b) Photograph of (a) on a 13-inch MacBook Pro screen and shot by an iPhone 4 camera without any compression artifacts. (c)-(d) Details of (a)-(b), respectively

F. Challenge Response

This technique of PAD requires the user to respond to the "challenge" instructed by the system. The system may request the user to "blink left eye" or "rotate the head clockwise".

VI. Presentation Attack Detection on Smartphones

While there has been a lot of research in this area of Presentation Attack Detection, not many were emphasized for smartphone and mobile devices. Only in the last couple of years, research based on smartphone and mobile device PAD are gaining popularity.

Many different algorithms have been developed and these algorithms are tested to gauge the performance level. Besides the finding or the outcome of the research, the researchers also release database or dataset that they used during their test. These databases are publicly available and can be used by other researchers to gauge their own algorithm performance

This section will look at those research that has been done, the techniques and methods they use, the performance of their algorithm and the database they have released.

A. MSU Mobile Face Spoofing Database (MSU MFSD)

This database is produced as part of research in [18]. It proposed the use of Image Distortion Analysis techniques in detecting presentation attack. Specifically, it will detect presentation attack by analysing for the following:

- Specular Reflection Features
- Blurriness Features
- Chromatic Moment Features Recaptured
- Color Diversity Features Another

The techniques employed here are based on Image Quality Analysis category. In this case, it will look for spoofing by detecting for any distortion in the image as mentioned above.

The publicly available MSU MFSD Database for face spoof attack consists of 280 video clips of photo and video attack attempts to 35 clients.

For data collection for this database, two type of cameras that were used:

i. built-in webcam in MacBook Air 13" (640x480);
ii. front-facing camera in the Google Nexus 5 Android phone (720x480)

For this database, three types of spoofing attack medium are used:

i. iPad
ii. iPhone
iii. printed photo

Information on how to obtain the MSU Mobile Face Spoofing Database is available from the Michigan State University website [21].

B. MSU Unconstrained Smartphone Spoof Attack Database (MSU USSA)

This database is produced as part of research [22]. It proposed the following methods:

- reject options using Interpupillary Distance (IPD) constraint and bezel detection
- fusion of Local Binary Pattern (LBP) and Colour Moments

The techniques employed here are a combination of texture analysis and image analysis techniques. It also includes IPD calculation in order to detect spoofing, because a person holding a printed photography might accidentally bend the photo making the pupil distance between the two eyes not equal. It will also detect for any bezel that might have a printed photograph.

The main purpose of this MSU USSA database is to simulate spoof attacks on smartphones. The MSU USSA database makes sure that it contains a mixture of environments, image qualities, image capture devices and subject diversity. A total of 1,000 live subject images of celebrities from the Weakly Labeled Face Database are selected. Therefore, the public set of the MSU USSA database for face spoofing all together consist of 9,000 images (1,000 live subject and 8,000 spoof attack) of the 1,000 subjects.

For data collection for this database, two type of cameras that were used:

i. Front-facing camera in the Google Nexus 5 Android phone (1280 × 960).
ii. Rear-facing camera in the Google Nexus 5 Android phone (3264 × 2448).

Information on how to obtain the MSU Unconstrained Smartphone Spoof Attack Database (MSU USSA) is available from the Michigan State University website [23].

C. IDIAP Replay-Mobile Database

This database is produced as part of [24] research. It proposed the following methods:

- Image Quality Measures
- Using Gabor-jets texture-descriptor

The techniques used are combinations of the Image Quality Analysis category and combined with Texture Analysis. The image is analysed with various quality measures to determine spoofing.

The Replay-Mobile Database contains spoof attacks with a total of 1190 video clips of photos and videos under different lighting conditions to 40 clients. Those videos were recorded with using an iPad Mini2 running iOS and an LG-G4 smartphone running Android. The IDIAP Replay-Mobile Database is available for download from the Idiap Research Institute [25].

D. MSU Replay-Attack for Smartphones (RAFS)

This database is part of research in [7]. The proposed method used in the research is the Moiré Pattern Analysis with the following:

- Multi-scale LBP (MLBP)
- Densely Sampled SIFT (DSIFT)
- Combination of MLBP and DSIFT

The research utilises Texture Analysis methods. Image are analyse using MLBP, DSIFT and combination of both.

The RAFS (Replay-Attack for Smartphones) is an extension of MSU Mobile Face Spoofing Database (MFSD) by capturing replay attacks using smartphones. It contains 165 videos from 55 subjects. From the total 165 videos, 55 videos are live face videos from the MSU MFSD that are captured using the front-facing camera on a Google Nexus 5 in a controlled background environment. The remaining 110 (2×55) videos are spoofed face videos which are captured by showing the live face videos on a MacBook screen (1280×800), and recapturing the face videos using the built-in rear camera of Google Nexus 5 and built-in rear camera of iPhone 6, respectively.

VII. Evaluation of Presentation Attack Detection

There are two types of error can be produced in a face PAD system: False Acceptance (FA) and False Rejection (FR).

The False Acceptance Rate, or FAR, is the probability that the anti-spoofing system will mistakenly accept an access attempt by an imposter using a spoof face. FAR is the equivalence to the ratio of the number of False Acceptances (FA) divided by the total number of spoofing attacks.

The False Rejection Rate, or FRR, is the probability that the biometric security system will mistakenly reject an access attempt by a real user. FRR is the equivalence to the ratio of the number of False Rejections (FR) divided by the total number of genuine access.

Table 1
Relation Between False Acceptance, False Rejection, Spoofing Attack, Genuine Access and Face Presentation Attack Detection System Acceptance And Rejection

	Presentation Attack/ Fake Face	Genuine Access/ Real Face
System Accept	False Acceptance (FA)	True Acceptance (TA)
System Reject	True Rejection (TR)	False Rejection (FR)

Two commonly indicator to measure the performance is to use the Half Total Error Rate (HTER) and Equal Error Rate (EER).

Half Total Error Rate (HTER) is the average of False Acceptance Rate (FAR) and False Rejection Rate (FRR).

Equal Error Rate (EER) is the rate at which the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) are the same. This value is a single number that is sometimes used to compare matching performance between systems [26][27].

Besides the traditional False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), and Half Total Error Rate (HTER) used for evaluation, there are newer PAD evaluations based on ISO/IEC 30107-3 specifications: Attack Presentation Classification Error Rate (APCER), Bona Fide Presentation Classification Error Rate (BPCER) and Average Classification Error Rate (ACER).

Attack Presentation Classification Error Rate (APCER) is the proportion of attack presentations using the same PAI

species incorrectly classified as bona fide presentations in a specific scenario.

Bona Fide Presentation Classification Error Rate (BPCER), also known as Normal Presentation Classification Error Rate (NPCER) is proportion of bona fide presentations incorrectly classified as attack presentations in a specific scenario.

Average Classification Error Rate (ACER) is the mean of APCER and BPCER. To gauge the performance and effectiveness of a PAD algorithm, it is tested against the publicly available database. Besides the four databases that are already mentioned in the previous section, there are other databases which are not specific for smartphones but are used as a benchmark as well. Testing and benchmarking a PAD algorithm and method are usually done using intra-database itself and also cross-database with others.

E. Intra-database Testing

The PAD algorithm and method are both trained and tested using the same database. The training and testing will most likely use the same spoof media, same camera, same environment, same lighting condition and same subjects.

F. Cross-database Testing

In cross-database testing, the PAD algorithm and method are trained using one database and tested using another different database. The training and testing will most likely use different spoof media, different camera, different environment, different lighting condition and different subjects. Cross-database performance result is close to the real-world application, where a PAD algorithm needs to detect spoof media condition which it has not been trained for.

Table 2
Presentation Attack Detection on Smartphone - Performance Result

DB	Method/Techniques	Intra-database Test			Cross-database Test			
		IDIAP [5] HTER (%)	CASIA [6] ERR (%)	MFSD ERR (%)	IDIAP [5] (TRAIN) MFSD (TEST)		MFSD (TRAIN) IDIAP [5] (TEST)	
					TPR@FAR=0.1	TPR@FAR=0.01	TPR@FAR=0.1	TPR@FAR=0.01
MSU MFSD	Image Distortion Analysis	7.41	13.3 (30FRMS) 12.9 (75FRMS)	8.58 (35 SUBJECTS) 5.82 (55 SUBJECTS)	75.5	29.8	73.7	38.6

DB	Method/Techniques	Intra-database Test			Cross-database Test		
	Interpupillary Distance (IPD) constraint and bezel detection	IDIAP [5] HTER (%)	CASIA FASD [6] ERR (%)	MFSD ERR (%)	USSA (TRAIN) TEST		
					MSU MFSD	IDIAP [5]	CASIA FASD [6]
MSU USSA	Local Binary Pattern (LBP) and Colour Moments	Original Protocol			9.27% HTER	3.50% HTER	2.00% HTER
		14.6	5.88	8.41			
		Smartphone Unlock for face unlock					
		0	1.67	2.67			

DB	Method/Techniques	Intra-database Test			
		HTER (%)	ACER (%)	APCER (%)	BPCER (%)
IDIAP REPLAY-MOBILE	IQM	7.8	13.64	19.87	7.40
	Gabor	9.13	9.53	7.91	11.15

DB	Method/Techniques	Intra-database Test			Cross-database Test		
	Multi-scale LBP (MLBP)	IDIAP [5] HTER (%)	CASIA[6] HTER (%)	RAFS HTER (%)	IDIAP [5] HTER (%)	CASIA [6] HTER (%)	RAFS HTER (%)
MSU RAFS	Densely Sampled SIFT (DSIFT)	3.3%	0.0	11.3	18.0	49.0	11.4

VIII. Performance of Presentation Attack Detection on Smartphones

Table 2 summarized the performance results of PAD algorithms on a smartphone that have been presented in the earlier section.

From all we have seen, still, there isn't single method that can claim it is superior to the other methods. While some performed good with a certain database, it may not be performing well with others. Some method gets a good result in an intra-database testing but did not get a good result in a cross-database testing environment. Even for an intra-database testing, different results are obtained with testing with a different database.

IX. Conclusion

A lot of research has been done in this field of face presentation attack detection in general. Face presentation attack detection for a smartphone is quite new and has now been the focus of many research groups. Different techniques and methods have been introduced.

This paper has presented the various research that have been done for presentation attack detection on smartphones and explained their techniques and method.

From the result comparison, it shows that a lot of research in presentation attack detection countermeasure is still needed.

All of the research presented are tested with images of subjects taken mostly in controlled environment. We do not know how those methods will perform in the real world used by the real users as a complete biometrics system and used in different scenarios and environment.

The cross-database testing is a close representation of a real-world scenario usage. In a real-world scenario, it is impossible for us to train our algorithm with each and every different spoof material scenario (different camera, different environment, different lighting condition and different subjects).

ACKNOWLEDGMENT

This paper was partly sponsored by the Center for Graduate Studies UTHM. The research also received funding from the Office for Research, Innovation, Commercialization and Consultancy Management (ORICC), UTHM with the GPPS grant number U796.

REFERENCES

[1] Y. Li, K. Xu, Q. Yan, Y. Li, and R. H. Deng, "Understanding OSN-based facial disclosure against face authentication systems," *Proc. 9th ACM Symp. Information, Comput. Commun. Secur. - ASIA CCS '14*, pp. 413–424, 2014.

[2] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," *2011 Int. Jt. Conf. Biometrics, IJCB 2011*, 2011.

[3] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face Liveness Detection from A Single Image with Sparse Low Rank Bilinear Discriminative Model," in *Computer Vision – ECCV 2010*, 2010.

[4] G. Pan *et al.*, "Eyeblink-based Anti-Spoofing in Face Recognition from a Generic Webcamera," *11th IEEE ICCV, Rio Janeiro, Brazil, Oct.*, vol. 14, p. 20, 2007.

[5] I. Chingovska, A. Anjos, and E. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," *Int. Conf. Biometrics Spec. Interes. Gr.*, pp. 1–7, 2012.

[6] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A Face Antispoofing Database with Diverse Attacks," in *IAPR International Conference on Biometrics (ICB)*, 2012, pp. 2–7.

[7] K. Patel, H. Han, A. K. Jain, and G. Ott, "Live face video vs. spoof face video: Use of moiré patterns to detect replay video attacks," *Proc. 2015 Int. Conf. Biometrics, ICB 2015*, pp. 98–105, 2015.

[8] S. Bharadwaj, S. Member, T. I. Dhamecha, and S. Member, "Face Anti-spoofing via Motion Magnification and Multifeature Videolet Aggregation," no. ii, pp. 1–12.

[9] N. Kose and J. L. Dugelay, "Mask spoofing in face recognition and countermeasures," *Image Vis. Comput.*, vol. 32, no. 10, pp. 779–789, 2014.

[10] "ThatsMyFace." [Online]. Available: http://www.thatsmyface.com/.

[11] M. N. H. Mohd, M. Kashima, K. Sato, and M. Watanabe, "Internal state measurement from facial stereo thermal and visible sensors through svm classification," *ARPN J. Eng. Appl. Sci.*, vol. 10, no. 18, pp. 8363–8371, 2015.

[12] M. Mohd, M.N.H., Kashima, M., Sato, K., Watanabe, "A non-invasive facial visual-infrared stereo vision based measurement as an alternative for physiological measurement," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2015, pp. 684–697.

[13] M. De Marsico, M. Nappi, D. Riccio, and J. L. Dugelay, "Moving face spoofing detection via 3D projective invariants," *Proc. - 2012 5th IAPR Int. Conf. Biometrics, ICB 2012*, pp. 73–78, 2012.

[14] K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun, "Real-Time Face Detection and Motion Analysis With Application in ' Liveness ' Assessment," *Analysis*, vol. 2, no. 3, pp. 548–558, 2007.

[15] G. Pan, Z. Wu, and L. Sun, "Liveness Detection for Face Recognition," in *Recent Advances in Face Recognition*, 2008, pp. 109–124.

[16] Z. Akhtar and G. L. Foresti, "Face Spoof Attack Recognition Using Discriminative Image Patches," *J. Electr. Comput. Eng.*, vol. 2016, 2016.

[17] K. Kollreider, H. Fronthaler, and J. Bigun, "Non-intrusive liveness detection by face images," *Image Vis. Comput.*, vol. 27, no. 3, pp. 233–244, 2009.

[18] D. Wen, H. Han, and A. K. Jain, "Face Spoof Detection with Image Distortion Analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 4, pp. 746–761, 2015.

[19] D. C. Garcia and R. L. De Queiroz, "Face-Spoofing 2D-Detection Based on Moiré-Pattern Analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 4, pp. 778–786, 2015.

[20] D. C. . Garcia and R. L. De Queiroz, "MOIRE-PATTERN-BASED FACE-SPOOFING DETECTION," *Int. Conf. Image Process.*, vol. 1, pp. 4843–4847, 2015.

[21] "The MSU Mobile Face Spoofing Database (MFSD)." [Online]. Available: https://www.cse.msu.edu/rgroups/biometrics/Publications/Databases/MSUMobileFaceSpoofing/index.htm.

[22] W. Arti, B. Swapnil, B. Ashwini, and V. Mohini, "Secure Face Spoof Detection on Smartphone," *Int. Res. J. Eng. Technol.*, vol. 3, no. 10, pp. 167–170, 2016.

[23] "Unconstrained Smartphone Spoof Attack Database (USSA)." [Online]. Available: http://biometrics.cse.msu.edu/Publications/Databases/MSU_USSA/.

[24] A. Costa-pazo, S. Bhattacharjee, E. Vazquez-fernandez, and S. Marcel, "The REPLAY-MOBILE Face Presentation-Attack Database," in *Proceedings of the International Conference on Biometrics Special Interests Group (BioSIG)*, 2016.

[25] "Replay-Mobile Database." [Online]. Available: https://www.idiap.ch/dataset/replay-mobile.

[26] S. Bengio and J. Mariethoz, "A Statistical Significance Test For Person Authentication," in *ODYSSEY04 - The Speaker and Language Recognition Workshop, Toledo, Spain*, 2004, no. 2.

[27] M. E. Schuckers, *Computational Methods in Biometric Authentication: Statistical Methods for Performance Evaluation*. Springer-Verlag London, 2010.