A database for face presentation attack using wax figure faces*

Shan Jia[1,2][0000−0001−7503−8378], Chuanbo Hu[2][0000−0003−1165−5005], Guodong Guo[2][0000−0001−9583−0055], and Zhengquan Xu[1][0000−0002−7130−2992]

[1] Wuhan University, Wuhan, 430072, China
[2] West Virginia University, Morgantown, 26505, USA
{jias,xuzq}@whu.edu.cn
{chuanbo.hu,guodong.guo}@mail.wvu.edu

Abstract. Compared to 2D face presentation attacks (e.g. printed photos and video replays), 3D type attacks are more challenging to face recognition systems (FRS) by presenting 3D characteristics or materials similar to real faces. Existing 3D face spoofing databases, however, mostly based on 3D masks, are restricted to small data size or poor authenticity due to the production difficulty and high cost. In this work, we introduce the first wax figure face database, WFFD, as one type of super-realistic 3D presentation attacks to spoof the FRS. This database consists of 2200 images with both real and wax figure faces (totally 4400 faces) with a high diversity from online collections. Experiments on this database first investigate the vulnerability of three popular FRS to this kind of new attack. Further, we evaluate the performance of several face presentation attack detection methods to show the attack abilities of this super-realistic face spoofing database.

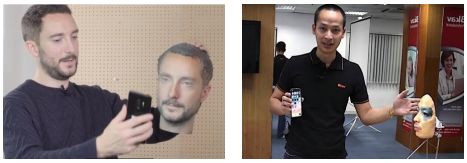
Keywords: Wax figure face · Face presentation attack · Face recognition

1 Introduction

With the widespread face recognition technologies, the security and privacy risks of face recognition systems (FRS) have been increasingly become as a critical issue in both academia and industry. Face presentation attacks are one of the most easily realized threats by presenting an artificial object or a copy or synthetic pattern of faces to the biometric data capture subsystem [6]. Based on the way to generate the face artifact, face presentation attacks can be classified into 2D modalities (which present printed/digital photographs or recorded videos on the mobile/tablet), and 3D type (by wearing a mask or presenting a synthetic model).

Because of the simplicity, efficiency, and low cost of making 2D type attacks, current systems and research pay more attentions to 2D face presentation attacks. However, with similiar 3D structures or materials to real faces, 3D face

* Supported by Wuhan University.



(a) (b)

Fig. 1: Examples of 3D presentation attack cases. (a) Android phones fooled by a 3D-printed head, (b) iPhone X face ID unlocked by a 3D mask.

presentation attacks are more hyper-realistic, and therefore, more powerful to attack the FRS while more difficult to detect. For example, as shown in Figure 1, even some systems, which have already taken presentation attack detection (PAD) into consideration, can be fooled by the 3D face presentation attacks.

Existing 3D presentation attacks are mostly based on wearable face masks. 3D facial mask spoofing was previously thought impossible to become a common practice in the literature [17], because compared to 2D type attacks, 3D masks are much more difficult and high-cost to manufacture, requiring special 3D devices and materials. In recent years, the rapid advancement of 3D printing technologies and services has made it easier and cheaper to make 3D masks. Several 3D mask attack databases have been created based on the third-party services [8, 12], by self-manufacturing [10], or from online resources [14]. However, they are restricted to small data sizes (mostly less than 30 subjects) or low mask qualities. This will not only limit the attack abilities of these fake faces, but also limit research works in reporting robust detection performance against 3D presentation attacks.

To address this problem, we take advantage of the popularity and publicity of numerous celebrity wax figure museums in the world, and collect a large number of wax figure images to form the new Wax Figure Face Database (WFFD). These life-size wax figure faces are all carefully designed and made in clay with wax layers, silicone or resin materials, so that they are super-realistic and similar to real faces. With the development of wax figure manufacture technologies and services, we think the easily obtainable and super-realistic wax figure faces will pose threat to the face recognition systems. Therefore, we introduce these wax figure faces as a new challenging type of 3D face presentation attacks in this paper, and analyze their impact on face recognition.

To the best of our knowledge, this is the first wax figure face database, also with a large data size and high diversity. Altogether, the WFFD consists of 2200 images of 450 subjects (with both real and wax figure faces, totally 4400 faces), which are diversified in subject age, ethnicity, face pose, facial expression, recording environment, and cameras, and therefore closer to the practical situation. Based on the new database, we first investigate the vulnerability of three popular face recognition systems to these super-realistic presentation attacks, and further evaluate the performance of several popular face PAD methods to show the attack ability of this 3D face spoofing database.

2 Related work

Most existing 3D face presentation attack databases create attacks by presenting wearable face masks, which are made of different materials with similar 3D face characteristics to the real faces. 3DMAD [8] is the first publicly available 3D mask database. It used the services of ThatsMyFace[3] to manufacture 17 masks of users, and recorded 255 video sequences with an RGB-D camera of Micsoft Kinect device for both real access and presentation attacks. This database is widely used by providing color images, depth images, and manually annotated eye positions of all face samples.

With the development of 3D modeling and printing technologies, from 2016, more mask databases were created. 3DFS-DB [10] is a self-manufactured and gender-balanced 3D face spoofing database. They made 26 printed models using two 3D printers: the ShareBot Pro and the CubeX[4], which are relatively low-cost and worth about 1000 and 2000 €, respectively. Acrylonitrile Butadiene Styrene (ABS) plastic material is used to generate the physical artifacts. HKBU-MARs [12] is another 3D mask spoofing database with more variations to simulate the real world scenarios. It generated 12 masks from two companies (ThatsMyFace and REAL-F[5]) with different appearance qualities. 7 camera types and 6 typical lighting settings are also included to form totally 1008 videos. To include more subjects, the SMAD database [14] collected and compiled videos of people wearing silicone masks from online resources. It contains 65 genuine access videos of people auditioning, interviewing, or hosting shows, and 65 attacked videos of people wearing a complete 3D structure (but not customized) mask around the head which fits well with proper holes for the eyes and mouth.

Besides, there have been some 3D mask spoofing databases with special lighting information for more effective detection. The MLFP database [2] (Multispectral Latex Mask based Video Face Presentation Attack database) is a unique multispectral database for face presentation attacks using latex and paper masks. It contains 1350 videos of 10 subjects in visible, near infrared (NIR), and thermal spectrums, which are captured at different locations (indoor and outdoor) in an unconstrained environment. Similarly, the ERPA database [5] also provides the RGB and NIR images of both bona fide and 3D mask attack presentations captured using special cameras. This is a small dataset with frame images of 5 subjects stored. The depth information is also provided. Both rigid resin-coated masks and flexible silicone masks are considered.

These databases have played a significant role in designing multiple detection schemes against 3D face presentation attacks. However, they still face the problems of small database size, low diversity, or poor authenticity, which will certainly limit the development of effective and practical detection schemes.

[3] http://thatsmyface.com/.
[4] https://www.sharebot.it. and http://www.cubify.com.
[5] http://real-f.jp/en_the-realface.html.

(a) (b)

Fig. 2: Examples of images of WFFD database. (a) Protocol I, (b) Protocol II.

3 The wax figure face database

To address the issues in existing 3D face presentation attack databases, we introduce the new WFFD database with a large size and high diversity as super-realistic 3D presentation attacks. The details of the data collection process, and the evaluation protocols are presented in this section.

This Wax Figure Face Database is based on numerous celebrity wax figure images from online resources. These user-customized and life-size wax figure faces are all carefully designed and made in clay with wax layers, silicone or resin materials, so that they are super-realistic. We first downloaded multiple celebrity wax figure faces as attacks with a high diversity in subject age, ethnicity, face pose, expression, recording environment, and cameras, and then collected the corresponding celebrity images as real access attempts. For each subject, the wax figure face and real face were finally grouped in one image to show the high authenticity, as the examples shown in Figure 2(a).

Further, we introduce one more challenging scenario where the wax figure face and real face were originally recorded together, as shown in Figure 2(b). With the same recording environment, and even the same face poses and facial expressions, these images are more difficult to distinguish.

Altogether, the WFFD consists of 2200 images with both real and wax figure faces of 470 subjects, totally 4400 faces. Table 1 compares the characteristics of WFFD with six existing 3D face presentation attack databases. To evaluate the performances of the face PAD methods on the WFFD database, we further designed three protocols. 1) Protocol I contains images grouped manually, which means the wax figure faces and real faces came from different recording devices and environment. 2) Protocol II contains the wax figure faces and real faces recorded in the same environment with the same cameras. 3) Protocol III combines previous two protocols to simulate the real-world operational conditions. More details about the images used in each protocol are shown in Table 2.

4 Experiments

In this section, we first investigate the vulnerability of three popular face recognition systems to these super-realistic 3D presentation attacks, and then evaluate the performance of several popular face PAD methods on the proposed database.

Table 1: Comparison of 3D face presentation attack databases

Database	Year	#Sub	#Sam	Format	Material	Image description
3DMAD [8]	2013	17	255	video	paper, resin	2D, 2.5D
3DFS-DB [10]	2016	26	520	video	plastic	2D, 2.5D, 3D
HKBU-MARs [12]	2016	12	1008	video	/	2D
SMAD [14]	2017	/	130	video	silicone	2D
MLFP [2]	2017	10	1350	video	latex, paper	multispectral
ERPA [5]	2017	5	86	image	resin, silicone	multispectral, depth
WFFD (proposed)	2019	470	2200	image	wax figure	2D

Table 2: Number of images in each evaluation protocol

Protocol	#Training	#Development	#Testing	#Total
Protocol I	600	200	200	1000
Protocol II	720	240	240	1200
Protocol III	1320	440	440	2200

* Note that the three subsets have no overlap.

4.1 Performance evaluation metrics

Based on the ISO/IEC metrics, for the evaluation of the vulnerability of FRSs, the Impostor Attack Presentation Match Rate (IAPMR) metric was used to report the results, which can be considered as an indication of the attack success chances if the FRS is evaluated regarding its PAD capabilities. It is defined as the proportion of impostor attack presentations using the same Presentation Attack Instrument (PAI) species in which the target reference is matched in a full-system evaluation of a verification system. For the detection performance evaluation, we reported the results using the Attack Presentation Classification Error Rate (APCER), the Bona Fide Presentation Classification Error Rate (BPCER), and the Average Classification Error Rate (ACER).

4.2 Vulnerabilities of face recognition systems

Three FARs were considered to show the vulnerability towards detecting fake faces using the proposed WFFD database, so that the attack abilities of the super-realistic database can be demonstrated. They are two publicly available FRSs: OpenFace [3] and Face++ [9], and a commercial system Neurotechnology VeriLook SDK [15]. Using the thresholds recommended by these FRSs, we calculated the IAPMR values on three protocols of the WFFD database, as presented in Table 3.

Table 3 shows that over 92% of the images in the three protocols of the WFFD were successfully compared using the Openface and Face+, which means the high attack success chances of the proposed WFFD database on these two face recognition systems. However, lower values of the IAPMR can be seen when the VeriLook SDK was employed on the three protocols. This is attributed to the fact that some faces with special poses or low qualities cannot be identified by the VeriLook SDK, therefore, leading to less successful matches.

Table 3: IAPMR of three Face Recognition Systems

Protocol	Openface	Face++	VeriLook
Threshold	0.99*	1e-5†	36**
Protocol I	93.29%	92.60%	76.14%
Protocol II	96.73%	96.22%	88.12%
Protocol III	95.25%	94.72%	81.75%

* Using a squared L2 distance threshold; †Using the confidence threshold at the 0.001% error rate; ** Using the matching score when FAR=0.1%.

In addition, by comparing the results for Protocol I and Protocol II, we can observe that higher IAPMR values were achieved for images in Protocol II, where the fake faces and real faces were recorded in the same scenarios with the same cameras. This leads to the higher attack abilities of images in Protocol II.

4.3 Detection performance of face PAD algorithms

Several face PAD methods were evaluated on the WFFD database to show how they can work for the proposed super-realistic 3D presentation attacks. These PAD methods were based on different features, including the multi-scale LBP [8], the color LBP [7], the Haralick features [1], the reflectance properties [11], the multi-level Local Phase Quantization (LPQ) [4], deep features based on the ResNet-50 model [16] and VGG-16 model [13]. They all achieved high detection performance against 2D spoofing attacks or 3D mask attacks.

In this experiment, for each image in the WFFD database, the two face regions were first detected, cropped and normalized into 64×64 pixel images. Based on different PAD methods, features were extracted from the face images, and then fed into a Softmax classifier with a cross-entropy loss function.

The detection results on Protocol I and Protocol II of the proposed WFFD are shown in Table 4. For the Protocol I, we can see that existing seven face PAD methods achieved high detection error rates, ranging from 17% to 46%. We attribute the poor performances to the high diversity and super-realistic attacks in the WFFD database, therefore, making it difficult to detect real faces from wax figure faces recorded in different scenarios.

Table 4: Detection error rates (%) on Protocol I and Protocol II of the WFFD

Method	Protocol I				Protocol II			
	EER	APCER	BPCER	ACER	EER	APCER	BPCER	ACER
Multi-scale LBP [8]	33.17	31.22	31.22	31.22	36.62	37.32	33.45	35.39
Color LBP [7]	33.17	30.24	36.10	33.17	37.32	36.62	41.90	39.26
Haralick features [1]	32.19	25.85	37.07	31.46	38.38	41.55	24.65	33.10
Reflectance [11]	41.95	40.00	52.19	46.10	44.37	50.70	44.37	47.53
Multi-level LPQ [4]	24.88	24.88	25.36	25.12	33.10	35.56	22.89	29.22
ResNet-50 based [16]	**17.07**	**20.49**	**18.04**	**19.27**	**20.42**	**19.37**	**24.29**	**21.83**
VGG-16 based [13]	45.85	50.73	41.95	46.34	48.94	40.14	52.82	46.48

Comparing the two groups of results in Table 4, we can see that most error rates for Protocol II are higher than the values for Protocol I. Such results are reasonable since recording the real faces and wax figure faces in the same scenarios with the same cameras results in less differences of the faces. Therefore, it is more difficult to detect the presentation attacks in this protocol, also meaning the higher attack abilities, which reached a similar conclusion with the results in Table 3. Overall, due to the highly discriminative features learned by the ResNet-50 models, the method [16] achieved the best results for both the two protocols. The multi-level LPQ [4] based method also performed relatively well, with the ACER under 30%.

The overall results of the seven evaluated PAD methods on the WFFD database are shown in Table 5. The ACER values ranged from 20.04% to 47.24%, showing the poor detection performance of these methods against the proposed wax figure face presentation attacks, and therefore, the strong attack abilities of the WFFD database in face recognition.

Table 5: Detection error rates (%) on Protocol III of the WFFD

Methods	EER	APCER	BPCER	ACER
Multi-scale LBP [8]	34.56	33.33	32.92	33.13
Color LBP [7]	36.81	35.38	35.79	35.58
Haralick features [1]	36.81	36.40	32.92	34.66
Reflectance [11]	44.78	46.01	46.22	46.11
Multi-level LPQ [4]	28.63	29.45	25.15	27.30
ResNet-50 based [16]	**18.81**	**19.43**	**20.65**	**20.04**
VGG-16 based [13]	48.67	45.19	49.28	47.24

5 Conclusion

To address the limitations in existing 3D face presentation attack databases, we have proposed a new database, WFFD, composed of wax figure faces with high diversity and large data size as super-realistic face presentation attacks. The database will be made publicly available in order to help the development and fair evaluation of different PAD algorithms. Extensive experiments have demonstrated the vulnerability of popular face recognition systems to these attacks, and the performance degradation of several existing PAD methods in detecting real faces from wax figure faces, showing the challenges when wax figure face are used for 3D attacks.

Some motion based methods, such as head movement and blink detection based may seem quite effective in detecting wax figure fake faces if the faces are recorded in videos. However, nowadays the high-tech wax figure technologies have realized the intelligent wax figures, which can not only move but also sense people and change its behaviour based on its surroundings. Therefore, it is demanding to investigate more discriminative and powerful methods to detect these new challenging 3D face presentation attacks in the future.

References

1. Agarwal, A., Singh, R., Vatsa, M.: Face anti-spoofing using haralick features. In: Biometrics Theory, Applications and Systems (BTAS), 2016 IEEE 8th International Conference on. pp. 1–6. IEEE (2016)
2. Agarwal, A., Yadav, D., Kohli, N., Singh, R., Vatsa, M., Noore, A.: Face presentation attack with latex masks in multispectral videos. In: Computer Vision and Pattern Recognition Workshops. pp. 275–283 (2017)
3. Amos, B., Ludwiczuk, B., Satyanarayanan, M., et al.: Openface: A general-purpose face recognition library with mobile applications. CMU School of Computer Science (2016)
4. Benlamoudi, A., Samai, D., Ouafi, A., Bekhouche, S., Taleb-Ahmed, A., Hadid, A.: Face spoofing detection using multi-level local phase quantization (ml-lpq). In: Proc. of the First Int. Conf. on Automatic Control, Telecommunication and signals ICATS15 (2015)
5. Bhattacharjee, S., Marcel, S.: What you cant see can help you–extended-range imaging for 3d-mask presentation attack detection. In: Proceedings of the 16th International Conference on Biometrics Special Interest Group. No. EPFL-CONF-231840, Gesellschaft fuer Informatik eV (GI) (2017)
6. Biometrics, I.J.S..: Information technologybiometric presentation attack detectionpart 1: Framework. international organization for standardization (2016)
7. Boulkenafet, Z., Komulainen, J., Hadid, A.: Face anti-spoofing based on color texture analysis. In: Image Processing (ICIP), 2015 IEEE International Conference on. pp. 2636–2640. IEEE (2015)
8. Erdogmus, N., Marcel, S.: Spoofing in 2d face recognition with 3d masks and anti-spoofing with kinect. In: Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on. pp. 1–6. IEEE (2013)
9. Face++: Face compare sdk. `https://www.faceplusplus.com/face-compare-sdk/`
10. Galbally, J., Satta, R.: Three-dimensional and two-and-a-half-dimensional face recognition spoofing using three-dimensional printed models. IET Biometrics **5**(2), 83–91 (2016)
11. Kose, N., Dugelay, J.L.: Reflectance analysis based countermeasure technique to detect face mask attacks. In: Digital Signal Processing (DSP), 2013 18th International Conference on. pp. 1–6. IEEE (2013)
12. Liu, S., Yang, B., Yuen, P.C., Zhao, G.: A 3d mask face anti-spoofing database with real world variations. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops. pp. 100–106 (2016)
13. Lucena, O., Junior, A., Moia, V., Souza, R., Valle, E., Lotufo, R.: Transfer learning using convolutional neural networks for face anti-spoofing. In: International Conference Image Analysis and Recognition. pp. 27–34. Springer (2017)
14. Manjani, I., Tariyal, S., Vatsa, M., Singh, R., Majumdar, A.: Detecting silicone mask-based presentation attack via deep dictionary learning. IEEE Transactions on Information Forensics and Security **12**(7), 1713–1723 (2017)
15. Neurotechnology: Verilook sdk. `http://www.neurotechnology.com/verilook.html`
16. Tu, X., Fang, Y.: Ultra-deep neural network for face anti-spoofing. In: International Conference on Neural Information Processing. pp. 686–695. Springer (2017)
17. Zhang, Z., Yan, J., Liu, S., Lei, Z., Yi, D., Li, S.Z.: A face antispoofing database with diverse attacks. In: Biometrics (ICB), 2012 5th IAPR international conference on. pp. 26–31. IEEE (2012)