Attacking Face Recognition With T-Shirts: Database, Vulnerability Assessment, and Detection

AUTHORS: MATHIAS IBSEN,CHRISTIAN RATHGEB, FABIAN BRECHTEL, RUBEN KLEPP, KATRIN PÖPPELMANN, ANJITH GEORGE ,SÉBASTIEN MARCEL AND CHRISTOPH BUSCH

Published Date:5/06/2023
Published in IEEE Access.
Type: Journal

Presented by: Rohit Kumar
Scholar No: 24204041120
Course: M. Tech in Agile Software Engineering

Contents

Introduction to Face Recognition and Presentation Attacks (PAs)

- **Face Recognition:** It widely used in personal, industrial, and governmental security applications.
- **Presentation Attacks (PAs):** Attempts to deceive recognition systems by presenting modified or artificial input (e.g., masks).
- **Challenge:** Performance can drop with changes in lighting, angles, or low image quality, making it difficult to recognize faces consistently.

T-Shirt Presentation Attack

- **Concept:** Using T-shirts with printed faces to fool face recognition systems.
- **Motivation:** Such T-shirt-based attacks are low-cost, easy to conceal, and can bypass face recognition systems.
- **Goal of Study**: Estimate the vulnerability of face recognition systems to T-shirt PAs and propose detection methods.

T-Shirt Presentation Attack

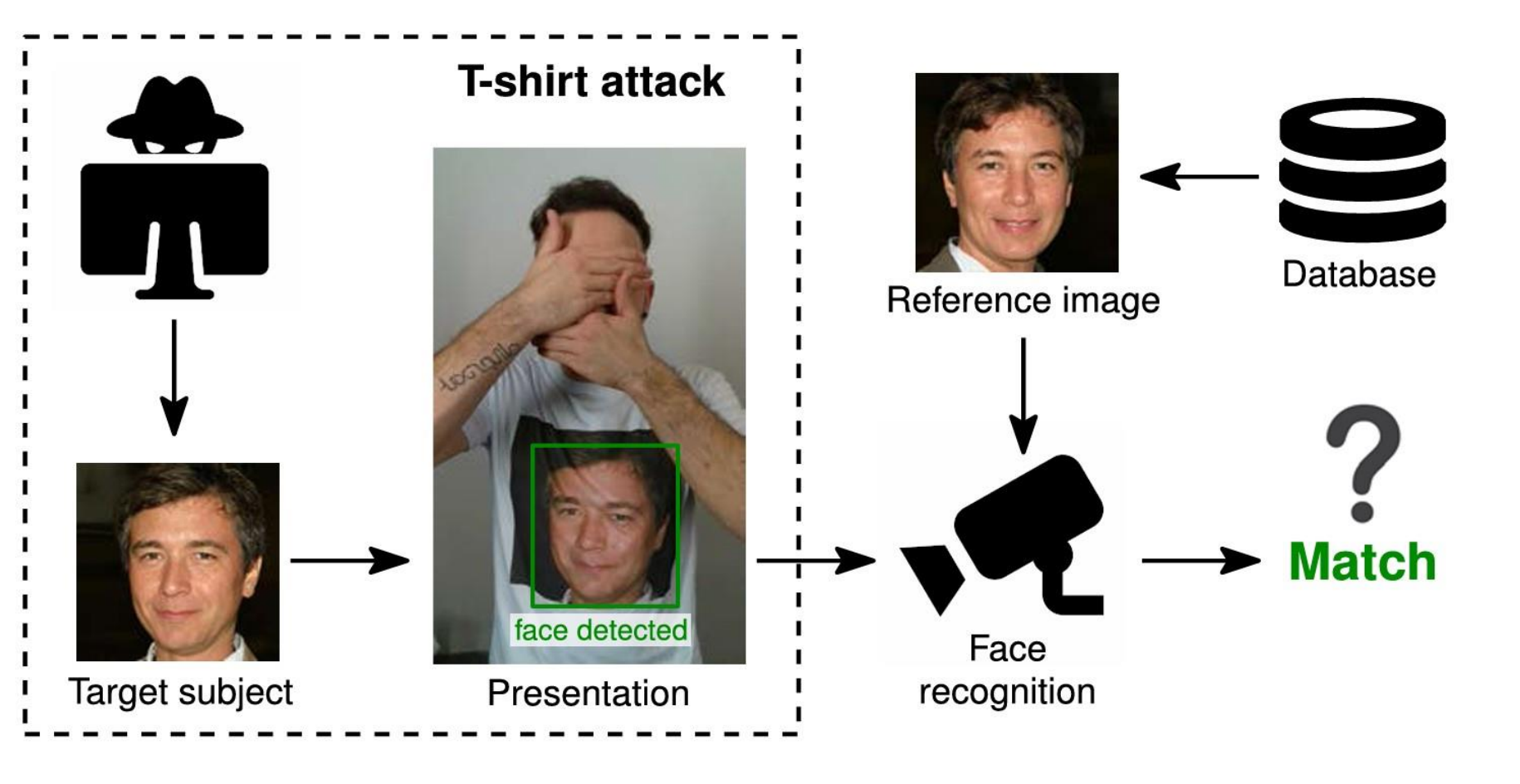

Figure 1. Can T-shirts with faces printed on them be used to attack face recognition systems?

T-Shirt Face Presentation Attack (TFPA) Database

Database Details

Capturing Scenarios

Significance

Database Details

Property	Description
Attack type:	Impersonation attack
Attack creation:	Synthetic face printed on T-shirt
Face generation methods:	StyleGAN & InterFaceGAN
No. of spectrums:	2 (visible, depth)
No. of attacks:	1608
No. of PAIs:	100
No. of subjects:	Real (8), generated (100)
Capturing device:	Intel RealSense Depth Camera D435
Environment:	Controlled indoor with white background

Table 1. An overview of the proposed T-shirt face presentation attack (TFPA) database.

Capturing Scenarios

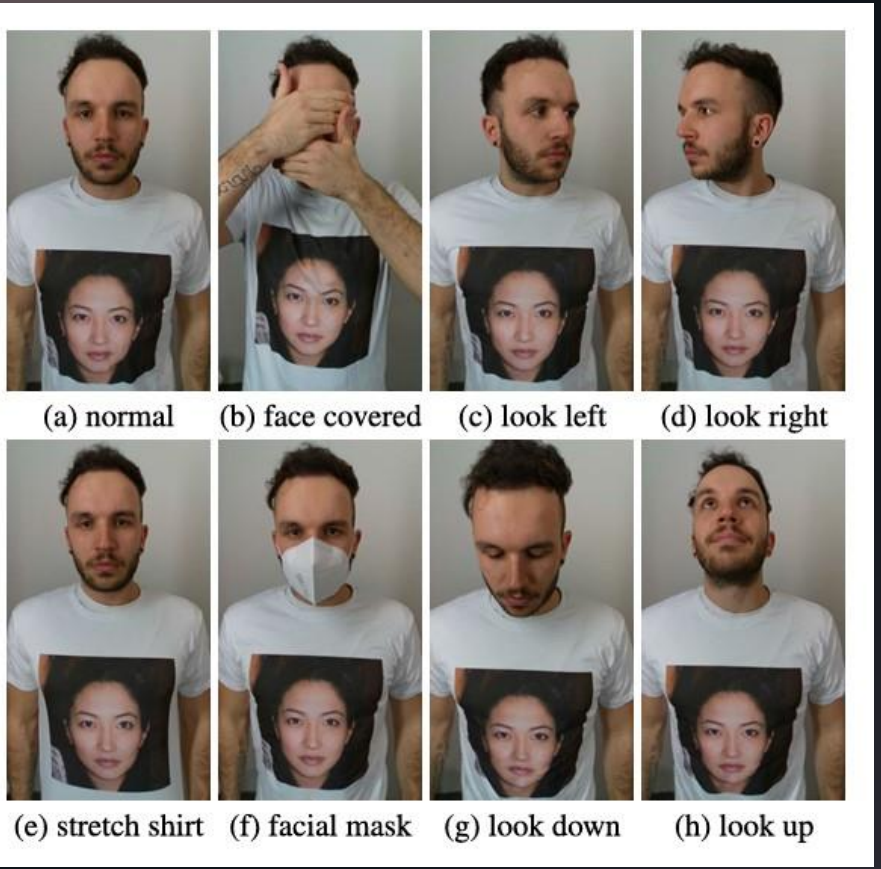

FIGURE 2. The eight different capturing scenarios.

Results:

- To evaluate this, three open-source algorithms were used, namely RetinaFace [6], MTCNN [7], and dlib [5]

- The results show that the T-shirt faces are successfully detected in almost all cases with an average estimated detection rate for the three algorithms > 99% across all eight poses.

		dlib		MTCNN		RetinaFace		Avg.
Scenario	Face type	Success %	Avg. score	Success. %	Avg. score	Success %	Avg. score	Success %
Normal	real	100	0.60	100	1.00	100	0.98	100
	T-shirt	100	0.56	100	1.00	100	0.98	100
Face covered	real	0.50	0.01	10.45	0.41	11.94	0.67	7.63
	T-shirt	98.01	0.50	99.50	1.00	100	0.97	99.17
Look left	real	88.56	0.30	100	1.00	100	0.98	96.19
	T-shirt	100	0.52	100	1.00	100	0.98	100
Look right	real	95.02	0.43	100	1.00	100	0.98	98.34
	T-shirt	100	0.53	100	1.00	100	0.98	100
Stretch T-shirt	real	100	0.59	100	1.00	100	0.97	100
	T-shirt	100	0.60	100	1.00	100	0.98	100
Facial mask	real	92.04	0.17	100	1.00	100	0.98	97.35
	T-shirt	99.50	0.56	100	1.00	100	0.98	99.83
Look down	real	88.56	0.34	100	1.00	100	0.98	96.19
	T-shirt	100	0.56	100	1.00	100	0.98	100
Look up	real	89.55	0.31	99	0.99	100	0.99	96.18
	T-shirt	100	0.55	100	1.00	100	0.98	100

Table 2. Detection accuracy and average detection scores across algorithms and capturing scenarios for T-shirt and real faces.

Vulnerability Assessment of Face Recognition Systems

- Many face detection algorithms can detect faces on T-shirts as real faces.
- IAPMR > 92.6% [9]
- Both open-source and commercial systems show high vulnerability, especially in scenarios where attackers conceal their real faces.

Proposed Detection Methods

- Depth Map Analysis
- Anomaly Detection
- Fusion Approach

Experimental Setup and Matrics

Training and Testing: DV and AD models were trained on controlled reference images and more uncontrolled probe images from the FRGCv2 [8] database.

Matrics

- **Attack Presentation Classification Error Rate (APCER)**: Measures the proportion of attacks incorrectly classified as real. means system incorrectly detect fake face is real.
- **Bona Fide Presentation Classification Error Rate (BPCER)**: Measures the proportion of real images wrongly classified as attacks. Its recognize real face is fake.

Results:

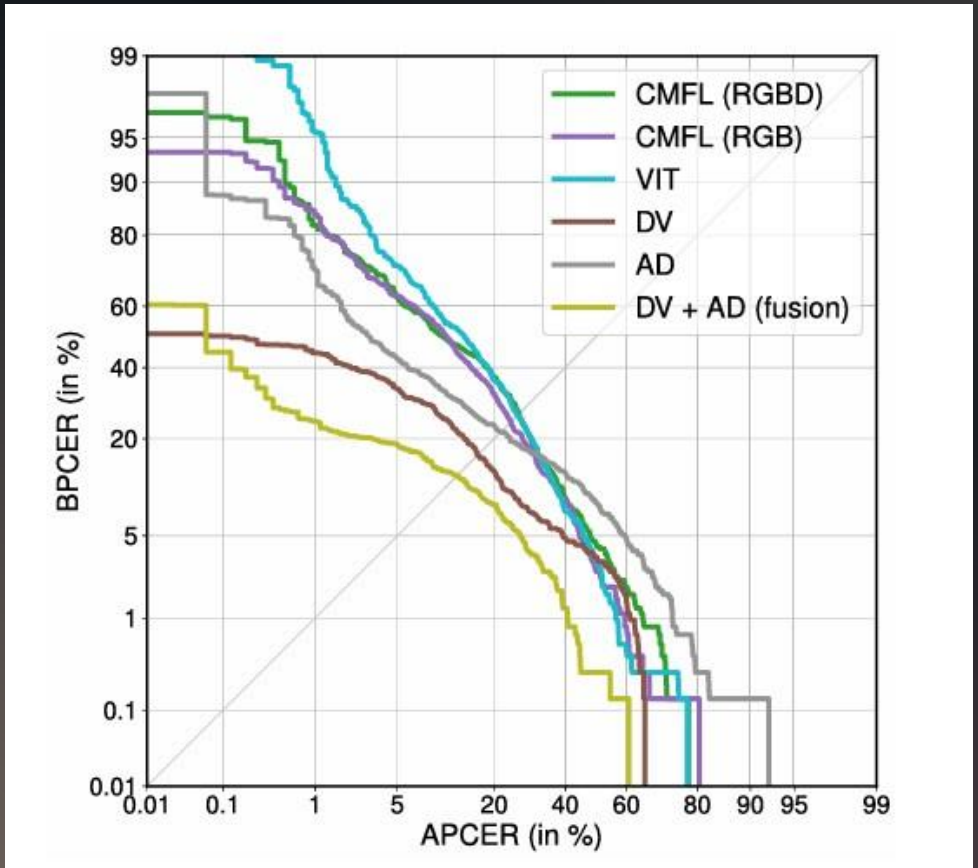

FIGURE 3. DET curves showing PAD performance on TFPA.

TABLE 2. D-EER, BPCER10, and BPCER20 in % for the different PAD algorithms.

PAD Algorithm	D-EER	BPCER10	BPCER20
CMFL (RGBD)	26.14	50.41	62.77
CMFL (RGB)	24.18	52.34	63.32
VIT	25.82	56.59	72.25
DV	16.34	25.55	33.52
AD	21.70	33.24	42.72
DV + AD (fusion)	**12.52**	**13.46**	**18.54**

Conclusion

- **Summary**: T-shirt PAs present a serious risk to face recognition systems, which are highly vulnerable without adaptive PAD methods.
- **Key Contribution**: Introduction of a T-shirt PA database and new detection methods.
- **Potential Future Solutions**: Explore new datasets and more adaptive PAD systems

Reference

[1] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, ''ArcFace: Additive angular margin loss for deep face recognition,'' in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2019, pp. 4685–4694.

[2] Q. Meng, S. Zhao, Z. Huang, and F. Zhou, ''MagFace: A universal representation for face recognition and quality assessment,'' in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2021, pp. 14220–14229.

[3] R. Raghavendra, K. B. Raja, and C. Busch, ''Presentation attack detection for face recognition using light field camera,'' IEEE Trans. ImageProcess., vol. 24, no. 3, pp. 1060–1075, Mar. 2015.[23]

[4] C.Chen,A.Dantcheva,T.Swearingen,andA.Ross,"Spoofingfacesusing makeup: An investigative study,'' in Proc. IEEE Int. Conf. Identity, Secur. Behav. Anal. (ISBA), Feb. 2017, pp. 1–8. [36]

[5] D. King, ''Dlib-ml: A machine learning toolkit,'' J. Mach. Learn. Res., vol. 10, pp. 1755–1758, Dec. 2009. [51]

[6] J. Deng, J. Guo, E. Ververas, I. Kotsia, and S. Zafeiriou, ''RetinaFace: Single-shot multi-level face localisation in the wild,'' in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2020, pp. 5202–5211. [53]

[7] K.Zhang,Z.Zhang,Z.Li,andY.Qiao,''Jointfacedetectionandalignment using multitask cascaded convolutional networks,'' IEEE Signal Process. Lett., vol. 23, no. 10, pp. 1499–1503, Oct. 2016. [52]

[8] P. J. Phillips, P. J. Flynn, T. Scruggs, K. W. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Worek, ''Overview of the face recognition grand challenge,'' in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2005, pp. 947–954. 54

[9] Information Technology Biometric Presentation Attack Detection—Part 3: Testing and Reporting, Standard ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 30107-3, International Organization for Standardization, 2017. [56]

[10] C. Lugaresi, J. Tang, H. Nash, C. McClanahan, E. Uboweja, M. Hays, F. Zhang, C.-L. Chang, M. G. Yong, J. Lee, W.-T. Chang, W. Hua, M. Georg, and M. Grundmann, ''MediaPipe: A framework for perceiving and processing reality,'' in Proc. 3rd Workshop Comput. Vis. AR/VR IEEE Comput. Vis. Pattern Recognit. (CVPR), Jun. 2019, pp. 1–4. [57]

THANK YOU

Questions