Journal of Multimedia Information System VOL. 9, NO. 2, June 2022 (pp. 103-112): ISSN 2383-7632 (Online)
https://doi.org/10.33851/JMIS.2022.9.2.103

Presentation Attacks in Palmprint Recognition Systems

Yue Sun[1], Changkun Wang[2*]

Abstract

Background: A presentation attack places the printed image or displayed video at the front of the sensor to deceive the biometric recognition system. Usually, presentation attackers steal a genuine user's biometric image and use it for presentation attack. In recent years, reconstruction attack and adversarial attack can generate high-quality fake images, and have high attack success rates. However, their attack rates degrade remarkably after image shooting. Methods: In order to comprehensively analyze the threat of presentation attack to palmprint recognition system, this paper makes six palmprint presentation attack datasets. The datasets were tested on texture coding-based recognition methods and deep learning-based recognition methods. Results and conclusion: The experimental results show that the presentation attack caused by the leakage of the original image has a high success rate and a great threat; while the success rates of reconstruction attack and adversarial attack decrease significantly.

Key Words: Presentation Attack, Reconstruction Attack, Adversarial Attack, Palmprint Recognition.

I. INTRODUCTION

In recent years, biometric recognition has been widely concerned and applied. Biometric recognition includes palmprint [1], face [2-3], gesture [4], and other modalities. Palmprint recognition is a non-invasive recognition method with stable recognition, low equipment cost [5], high user-friendliness, and high privacy, so it can be used in a wide range of applications [6]. The palmprint is representative and has a variety of feature types. Many palmprint features are also applicable to other biological feature modes. Therefore, the present attack is studied on palmprint recognition systems.

Presentation attack is common in the physical world. The attacker only needs to use printed images or videos placed at the front end of sensors to deceive the biometric identification system, typically such as printed photos, electronic displays, rubber molds, etc. Typically, presentation attacks use original biometric images. In addition to using the original biometric images, fake images produced by reconstruction attacks and adversarial attacks can also be used to present attacks.

In Reconstruction attacks, attackers reconstruct users biometric images by obtaining leaked information or vulnerabilities by identification systems, such as feature templates stored in databases and decision information of identification systems. Reconstructed images can impersonate the target user (victim user) and fool the recognition system.

In recent years, deep learning trained models have achieved good results in the field of computer vision [7]. However, some researchers have found that although the deep learning model has a high accuracy rate, it is fragile and vulnerable to attack by adversarial samples. Adversarial attacks add a minor perturbation to a clean image that the human visual system can't detect, but the deep learning model can alter its original classification results, give false results, and even control what kind of results it makes.

Reconstruction attacks and adversarial attacks both have high attack success rates, but they are input to the attacked system in the form of digital images and occur at the back of the sensor. The presentation attack is carried out in front of the sensor, which requires a lower level of authority and goes through a complete identification process, posing a huge threat to the security of the identification system. If the reconstruction attack and adversarial attack can be carried out in front of the sensor like the presentation attack, more attention should be paid to their threat to the biometric recognition system.

This paper analyzes the threat of presentation attacks to palmprint recognition systems by using the original image,

Manuscript received May 21, 2022; Revised June 1, 2022; Accepted June 2, 2022. (ID No. JMIS-22M-05-020)
Corresponding Author (*): Changkun Wang, +86-791-83953463, wangckun991@126.com
[1]School of Software, Nanchang Hangkong University, Nanchang, China, 1916085212108@stu.nchu.edu.cn
[2]School of Information Engineering, Nanchang Hangkong University, Nanchang, China, wangckun991@126.com

adversarial attack, and reconstruction attack. The main contributions are as follows:

(1) For the original images, adversarial attack images, and reconstruction attack images, through two physical display carriers, i.e. photo and monitor, after reimaging at the front of the acquisition device, six palmprint presentation attack datasets were produced.
(2) The experiment analyzed the success rate of presentation attacks by using stolen original palmprint images.
(3) The threat to the palmprint recognition system is analyzed experimentally in the case of reconstruction attack and adversarial attack.

The rest of this paper is organized as follows. Section 2 revisits the related works. Section 3 specifies the methodology. Section 4 are the experiments and discussions. Finally, the conclusions are drawn in Section 5.

II. RELATED WORKS

Presentation attack is a common attack method. The steps of presenting attacks are relatively simple, usually using different carriers to present biological features and establishing a new dataset of presentation attacks. Research on presentation attack focuses on its defense methods, such as in liveness detection. Reconstruction attacks and adversarial attacks can generate fake biometric images. These fake images may be attacked in a similar manner to the presentation attack, which is fed into the system from the sensor. This section introduces the research status of reconstruction attack, adversarial attack and palmprint recognition.

2.1. Reconstruction Attack

Reconstruction attack means that the attacker reconstructs the biometric image of the attacked user. Some palmprint recognition systems protect templates in databases. There are two common methods, such as biometric template protection [8-9] and cancelable biometric [10-11]. However, reconstruction attacks can still generate reconstructed images by matching scores in the recognition system.

In terms of fingerprint modal, Uludag et al. [12] proposed to reconstruct fingerprint mitutia point template with hill-climbing algorithm and divide mitutia image into grid to avoid over-dense detail points in reconstructed image.

In terms of face modes, Andy et al. [13] continuously superimposed face feature images on a face image to modify face features until they were verified by the recognition system. Galbally et al. [14] reconstructed face images with bayesian hill-climbing algorithm. Andy et al. [15] proved that quantized matching scores cannot defend against reconstruction attacks by using hill-climbing algorithm. Marta et al. [16] used uphillsimplex method to generate reconstructed images more efficiently.

In terms of iris mode, Rathgeb et al. [17] optimized the hill-climbing algorithm by simultaneously modifying the pixels within a block. The size of the block depends on the size of the filter of the recognition system, which can reduce the number of modifications and generate reconstructed images faster. Galbally et al. [18] reconstructed iris images with genetic algorithm. Many iris images are synthesized with iris synthesizer as the initial individual, and then the initial individual is divided into blocks, and each block is the individual gene. By continuously producing new offspring until there is an individual verified by the recognition system. The verified individuals are embedded into the real iris image in a small proportion to improve the image quality.

In the palmprint mode, Wang et al. [19] attacked the palmprint recognition system with brute force. This method uses DCGAN to generate a large number of palmprint images, which are continuously input into the recognition system for verification until the palmprint images that pass verification are found. Sun et al. [20] proposed two reconstruction attack methods based on Hill-climbing algorithm, Modified Constraint within Neighborhood (MCwN) and Batch Member Selection (BMS). These two attack methods can quickly generate high-quality reconstructed images.

2.2. Adversarial Attack

Deep neural network trained models have excellent effects on many tasks in the field of computer vision, but Szegedy et al. [21] first discovered the fragile characteristics of neural networks. Whitebox adversarial attacks can be divided into three categories, namely gradient-based, optimization-based and GAN-based methods.

2.2.1. Gradient-Based Methods

Goodfellow et al. [22] believed that the high-dimensional linearity of neural networks led to the appearance of adversative samples, and based on this assumption, they proposed Fast Gradient Sign Method (FGSM). Kurakin et al. [23] extended FGSM and proposed a Basic Iterative Method (BIM), also known as I-FGSM(Iterative FGSM).

2.2.2. Optimization-Based Methods

Carlini et al. [24] limited the L_0, L_2 and L_∞ norms to make the adversarial perturbation smaller and harder to detect, and could break through the protection of the model by defensive distillation. Moosavi et al. [25] proposed DeepFool. In this method, the decision boundary of classification is assumed first, then the minimum norm adversarial perturbation is generated continuously by iterative calculation

method, and the image within the classification boundary is gradually pushed out of the boundary until the wrong classification occurs.

2.2.3. GAN-Based Methods

Xiao et al. [26] first used generative adversarial network (GAN) to generate adversarial samples and proposed AdvGAN. Mangla et al. [27] proposed AdvGAN ++ on the basis of AdvGAN, which improved the success rate of attack.

2.3. Palmprint Recognition

Palmprint recognition is a promising and representative biometric modality. Palmprint recognition methods can be roughly categorized into subspace-based [28-29], statistical-based [30-31], deep-learning-based [32], and coding-based [33-34] methods. deep-learning-based and coding-based methods are popular for palmprint recognition.

2.3.1. Deep-Learning-Based Methods

In recent years, deep learning has achieved tremendous development and remarkable achievements in various fields of computer vision [35-37]. Zhong and Zhu [38] designed a new loss function for palmprint recognition, which can make the distance distribution of Inter-class more concentrated, while the distance distribution of intra-class more dispersed. Matkowski et al. [39] proposed a palmprint recognition method suitable for low-constraint scenarios, which uses a cascading network structure consisting of two sub-networks to perform ROI segmentation and feature extraction tasks respectively. Liang et al. [40] proposed CompNet, which uses CNN to learn the parameters of Gabor filter and effectively utilizes the direction information in palmprint through special Softmax and channel convolution operations. CompNet has lower equal error rate compared with the existing methods, and has fewer parameters in the network, so it is easy to train. Wu et al. [41] realized multi-spectral palmprint fusion, and reduce the variance between intra-class score and inter-class score [42]. Moreover, this method saves storage space and matching computation. Xu et al. [43] Combine with soft biometrics to improve model accuracy.

2.3.2. Coding-Based Methods

Coding-based palmprint recognition method uses hand-designed filters to extract palmprint features. Compared with deep learning-based methods, such methods have faster matching speed, less storage space, and no training is required. The feature extraction of coding-based palmprint recognition method can be divided into cooperative and competitive methods.

The cooperative approach usually fuses multiple feature templates extracted from the palmprint at the feature level or score level. The related works include PalmCode [44], BOCV [45], OrdinalCode [46] and FusionCode [47].

Competition usually selects the index of the maximum/minimum response as the final template. The related works include CompCode [48], RLOC [49], DOC [50] and DRCC [51].

III. METHODOLOGY

3.1. Monitor Presentation Attack

Monitor presentation attack displays palmprint images on the Monitor and retakes them with the camera. Input the re-shot image into the palmprint recognition system to test whether it can pass the verification. In this way, it simulates the attacker using an monitor to display the stolen palmprint image and impersonates the stolen user, to test the security of the palmprint recognition system in this scenario.

To improve the efficiency of the experiment, the screen displays 15 images of the palmprint at a time. The monitor model used in the experiment is DELL U2419HS with a size of 24 inches and a resolution of 1,920×1,080. The original ROI of each palmprint is 128×128 in size, so displaying 15 palmprint images can also fully show the details of the palmprint images. The camera is iPhone XS. The camera is positioned horizontally with the screen and shot under indoor light. The shooting scene is shown in Fig. 1. The image taken is shown in Fig. 2. It can be found that due to the interaction between the camera and the display, the retaken palmprint image will appear moire fringe.

Next, each palmprint image is cut out from the shot image and reduced to the input size set by the recognition system. Since the position between the camera and the monitor does not change, it is possible to quickly crop out the palmprint image. The angle between camera position and display

Fig. 1. Monitor presentation attack shooting scene.

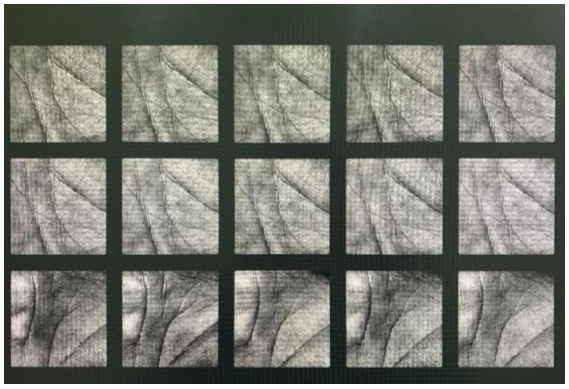


Fig. 2. Images of monitor presentation attack captured by camera.

(a) Original palmprint images

(b) Monitor presentation attack images

Fig. 3. Comparison between original palmprint images and monitor presentation attack images.

is horizontal, thus avoiding image distortion. Since the images taken are RGB images and most palmprint recognition systems use grayscale images for recognition, it is necessary to grayscale each palmprint image. Fig. 3 shows the comparison between the original palmprint image, and the image displayed by a monitor.

3.2. Paper Presentation Attack

Paper presentation attack prints palmprint images with a printer. One piece of paper can hold 9 palmprint images. The paper printed with palmprint images is placed on the desktop, and the camera is at a horizontal angle to the paper. The printer is Lenovo M101DW and the camera is iPhone XS. The image taken is shown in Fig. 4. The palmprint image for the presentation attack was obtained after clipping, shrinking, and graying the shot image. Fig. 5 shows a comparison of the original palmprint image with the image rendered on paper.

IV. EXPERIMENTS

4.1. Experimental Environment And Datasets

The experimental hardware environment is described as

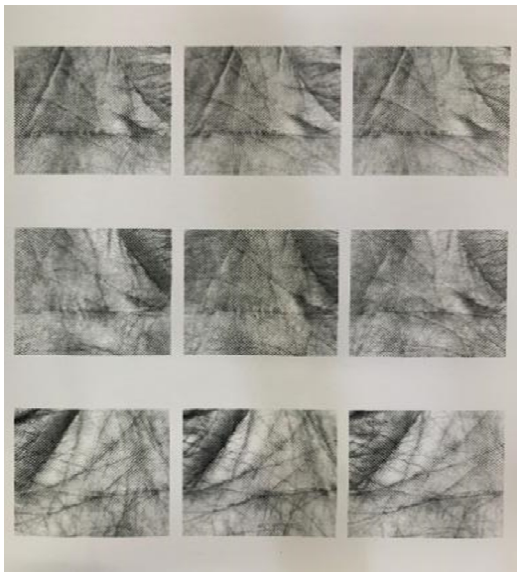
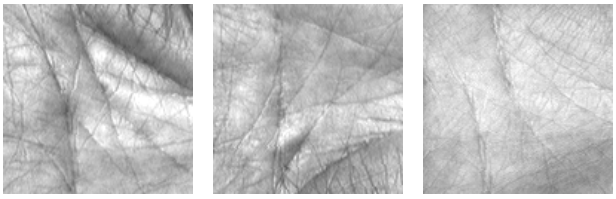
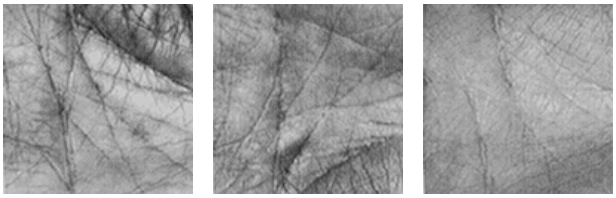


Fig. 4. Paper presentation attack images captured by camera.



(a) Original palmprint images



(b) Paper presentation attack images

Fig. 5. Comparison between original palmprint images and Paper presentation attack images.

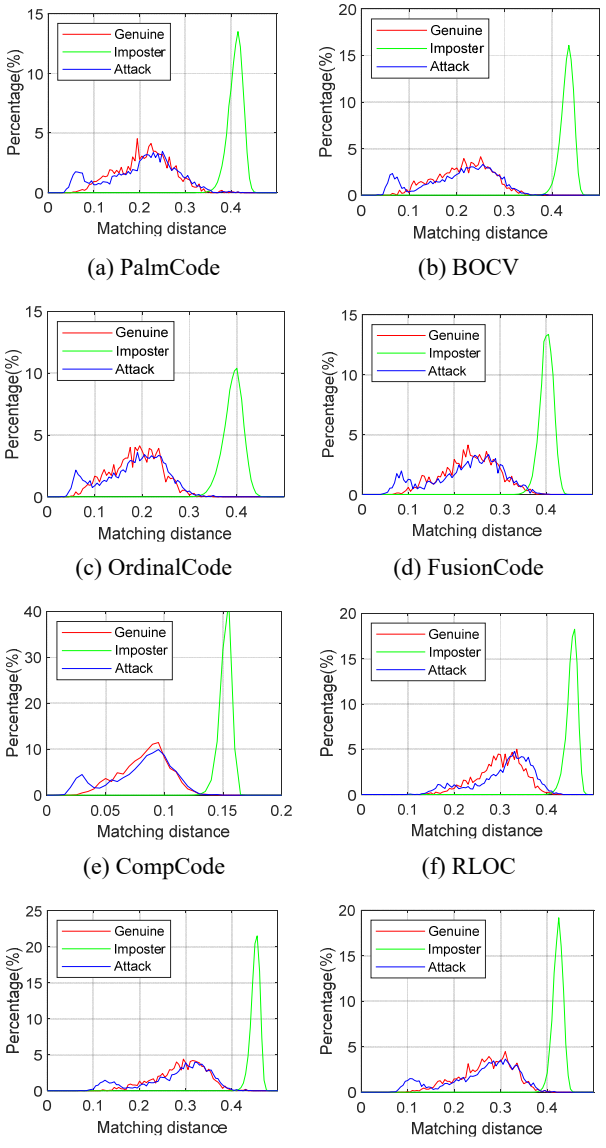
follows: Intel Xeon(R) W-2145 CPU @ 3.70GHz ×16, GeForce GTX 1080 Ti, 64GB memory. The used programming languages are MATLAB and Python. The presentation attack dataset was made based on three palmprint datasets: real palmprint dataset, reconstructed image dataset, and adversarial sample dataset. The real palmprint dataset is a PolyU which contains 600 images. The reconstructed image dataset is the reconstructed images generated by the BMS, which contains 300 images. The adversarial sample dataset contains 400 adversarial samples generated by FGSM against CompNet [40]. At the same time, two kinds of presentation attack datasets should be made based on these three datasets, namely, monitor presentation attack dataset and paper presentation attack data set. Therefore, there are six presentation datasets, Reconstruction_Monitor, Reconstruction_Paper, Adversarial_Monitor, Adversarial _Paper, PolyU_Monitor and PolyU_Paper.

4.2. Presentation Attack on Coding-Based Palmprint Recognition

Attack coding-based palmprint recognition methods with PolyU_Monitor and PolyU_Paper. The simulated scenario is an attacker using the stolen original palm print image displayed on a monitor or paper, input into the palm print recognition system, and trying to impersonate a legitimate user. The distance distribution between the presentation attack dataset and the attacked palmprint image (the original image of making the presentation attack dataset) was calculated.

Fig. 6 shows presentation attack on 8 coding-based palmprint recognition methods using PolyU_Monitor. The red and green lines are intra-class distance and Inter-class distance distribution respectively. The blue lines are the distance distribution between the image in PolyU_Monitor and the palmprint image of the corresponding target user in PolyU. It can be found that there is a small peak on the left of the blue line because PolyU_Monitor matches the corresponding original image in PolyU. The original image has only been displayed and reshot, so the matching distance between them is very small.

Fig. 7 shows presentation attack on 8 coding-based palmprint recognition methods using PolyU_Paper. The blue line also moves slightly to the right compared to the red line, but the small mountain on the left is hard to see and there is a small bump behind it. This is because, compared to the monitor, the printer printing resolution is lower, so the printed palmprint image details are blurry. In particular, some images with high brightness are difficult to be clearly displayed on white paper, so the occurrence of small matching distance will be reduced. In addition, a small part of the



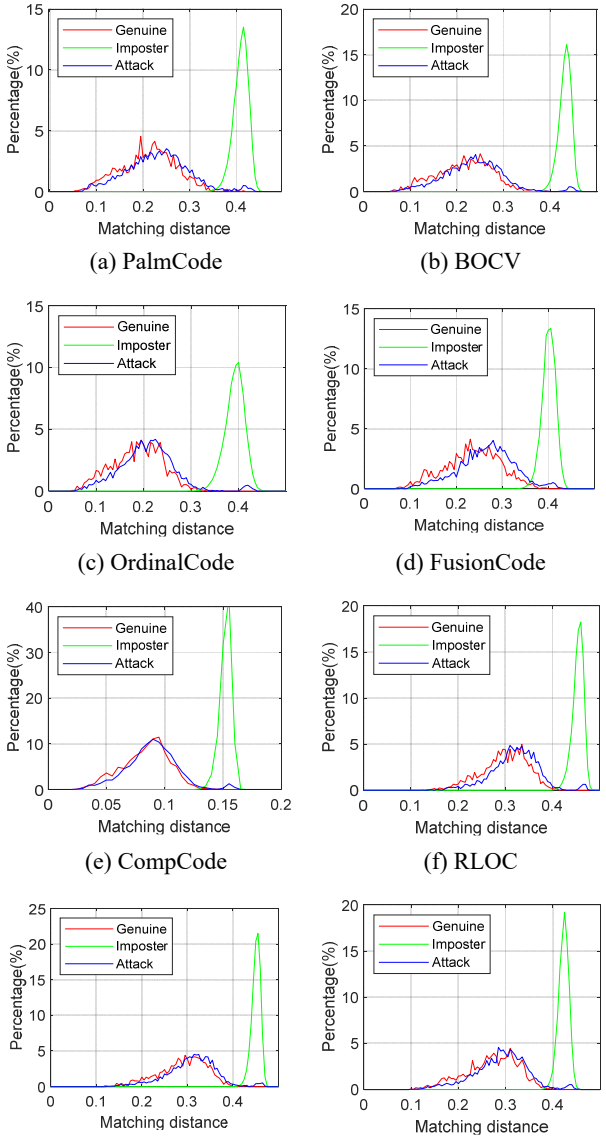
(a) PalmCode (b) BOCV

(c) OrdinalCode (d) FusionCode

(e) CompCode (f) RLOC

(g) DOC (h) DRCC

Fig. 6. Presentation attack on 8 coding-based palmprint recognition methods using PolyU_Monitor.



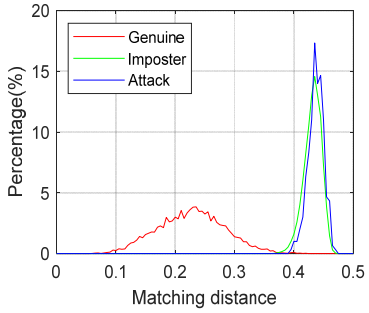
(a) PalmCode (b) BOCV

(c) OrdinalCode (d) FusionCode

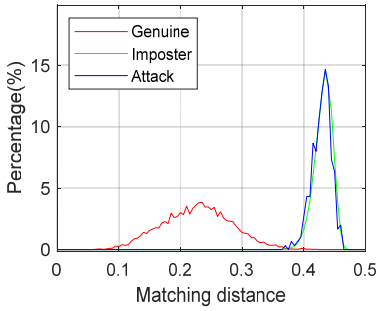
(e) CompCode (f) RLOC

(g) DOC (h) DRCC

Fig. 7. Presentation attack on 8 coding-based palmprint recognition methods using PolyU_Paper.



(a) Reconstruction_Monitor



(b) Reconstruction_Paper

Fig. 8. Presentation attack on PalmCode with reconstructed images.

paper is bent when being shot, which leads to the deformation of the palmprint image and appear some large matching distance. In general, the overlap area of blue line distribution and red line distribution is very large, and the paper presentation attack has a very high success rate.

BMS makes minor modifications on the original palmprint images to generate reconstructed images. After the reconstructed images are displayed on a monitor or paper, the camera collects them and feeds them into the recognition system to test whether they can be successfully authenticated. The experiment calculated the matching distance between images in presentation attack datasets and corresponding target images, and then counted the proportion in each matching distance interval. The experimental results are shown in Fig. 8. The blue line shows the distribution of attack matching distance. As can be seen from the figure, the overall regular of Reconstruction_Monitor and Reconstruction_Paper are similar, and the blue line and the green line basically coincide. This means that after the reconstructed image is reshot on the monitor or paper, the modification of BMS is destroyed and it is not capable of presentation attack.

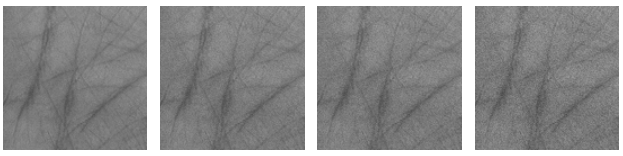
4.3. Presentation Attack on CompNet

CompNet uses a neural network to learn Gabor filter parameters and establishes a competitive mechanism to efficiently utilize the direction information of palm print. Since most neural network models use accuracy rate (ACC) as the model evaluation standard, the accuracy rate is also used to describe the model recognition accuracy in experiments.

Attacks on CompNet using PolyU_Monitor and PolyU_Paper were found to be 100% accurate, while for PolyU_Paper it was slightly lower at 97.4%. The accuracy of the identification system is also the success rate of the attack, which indicates that CompNet has a high success rate in both monitor and paper presentation attack.

Adversarial_Monitor and Adversarial_Paper are made on the basis of adversarial sample generated on CompNet to simulate the attack scene of adversarial sample in front of the camera. These images are targeted adversarial samples generated by FGSM. They can be classified into specific categories to impersonate legitimate users. Adversarial_Monitor and Adversarial_Paper each contain 400 images, which are divided into 4 categories with different ε values, 100 images for each. The higher the ε value is, the better the attack performance is, and the more obvious the forgery trace is. Adversarial samples with different ε values are shown in Fig. 9.

The experimental results of Adversarial_Monitor and Adversarial_Paper for the adversarial attack against CompNet are shown in Fig. 10. The experimental results show that the overall attack success rate is not high, because the targeted adversarial samples not only require the model to be misclassified, but also to be classified into the specified categories. When the ε value is low, the success rate of attack is very low, but with the increase of ε value, the success



(a) $\varepsilon = 0.02$ (b) $\varepsilon = 0.03$ (c) $\varepsilon = 0.04$ (d) $\varepsilon = 0.05$

Fig. 9. Adversarial samples with different $\boldsymbol{\varepsilon}$ values.

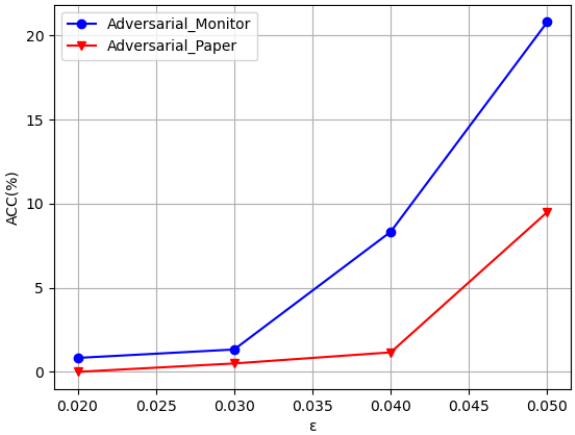


Fig. 10. Presentation attack on CompNet with adversarial samples.

rate also has an increase. This is because when the ε value is small, the added adversarial perturbation is small, and the noise is of high frequency. In the process of monitor or paper presentation and camera shooting, high-frequency noise is easy to be destroyed. With the increase of ε, the added perturbation becomes more obvious and is not easy to be destroyed. Compared with monitor adversarial attack and paper adversarial attack, monitor adversarial attack has a higher attack success rate.

V. CONCLUSIONS

In this paper, six presentation attack datasets are made, and the presentation attack experiments are carried out against coding-based palmprint recognition method and CompNet. The experimental results show that presentation attack caused by palmprint image leakage has a high success rate and poses a great threat to palmprint recognition system. The palmprint image presented by the display will appear moire fringe after re-shooting, but it has little influence on presentation attack. As the resolution of the printer is generally not high, the palmprint image presented on the paper is a little bit blurred and the details are not highly clear. In addition, the paper material is soft and easy to bend, which will lead to the deformation of the printed palmprint image. The experimental results show that monitor presentation attack has a higher attack success rate than paper presentation attack. Adversarial attack and reconstruction attack have a low success rate when they are conducted in front of the camera sensors. BMS does not have the ability to carry out presentation attack on PalmCode, because the BMS changes the initial image too little and it is easy to destroy. Similarly, adversarial attack is difficult to pose a threat to CompNet when the ε value is low.

ACKNOWLEDGEMENT

This research was supported by Innovation Foundation for Postgraduate Student of Nanchang Hangkong University (YC2020124), National Natural Science Foundation of China (61866028), Technology Innovation Guidance Program Project (Special Project of Technology Cooperation, Science and Technology Department of Jiangxi Province) (20212BDH81003).

REFERENCES

[1] A. B. J. Teoh and L. Leng, "Special issue on advanced biometrics with deep learning," *Applied Sciences*, vol. 10, no. 13, p. 4453, Jun. 2020.

[2] S. J. Park, B. G. Kim, and N. Chilamkurti, "A robust Facial expression recognition algorithm based on multi-rate feature fusion scheme," *Sensors*, vol. 21, no. 21, p. 6954, Oct. 2021.

[3] D. Jeong, B. G. Kim, and S. Y. Dong, "deep joint spatio-temporal network (DJSTN) for efficient facial expression recognition," *Sensors*, vol. 20, no. 7, p. 1936, Mar. 2020.

[4] J. H. Kim, G. S. Hong, B. G. Kim, and D. P. Dogra, "Deepgesture: Deep learning-based gesture recognition scheme using motion sensors," *Displays*, vol. 55, pp. 38-45, Dec. 2018.

[5] L. Leng, F. Gao, Q. Chen, and C. Kim, "Palmprint recognition system on mobile devices with double-line-single-point assistance," *Personal and Ubiquitous Computing*, vol. 22., no. 1, pp. 93-104, Dec. 2018.

[6] L. Leng, A. B. J Teoh, M. Li, and M. K. Khan, "A remote cancelable palmprint authentication protocol based on multi-directional two-dimensional PalmPhasor-fusion," *Security and Communication Networks*, vol. 7, no. 11, pp. 1860-1871, Nov. 2014.

[7] D. Kondratyuk, L. Yuan, Y. Li, L. Zhang, M. Tan, and M. Brown, et al., "Movinets: Mobile video networks for efficient video recognition," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 16020-16030, Jun. 2021.

[8] L. Leng, A. B. J. Teoh, and M. Li, "Simplified 2DPalmHash code for secure palmprint verification," *Multimedia Tools and Applications*, vol. 76, no. 6, pp. 8373-8398, Apr. 2017.

[9] L. Leng, A. B. J. Teoh, M. Li, and M. K. Khan, "Analysis of correlation of 2DPalmHash Code and orientation range suitable for transposition," *Neurocomputing*, vol. 131 pp. 377-387, May 2014.

[10] L. Leng and A. B. J. Teoh, "Alignment-free row-co-occurrence cancelable palmprint fuzzy vault," *Pattern Recognition*, vol. 48, no. 7, pp. 2290-2303, Jul. 2015.

[11] L. Leng and J. Zhang, "Dual-key-binding cancelable palmprint cryptosystem for palmprint protection and information security," *Journal of Network and Computer Applications*, vol. 34, no. 6, pp. 1979-1989, Nov. 2011.

[12] U. Uludag and A. K. Jain, "Attacks on biometric systems:a case study in fingerprints," in *Security, Steganography, and Watermarking of Multimedia Contents VI*, California, pp. 622-633, Jun. 2004.

[13] A. Adler, "Images can be regenerated from quantized biometric match score data," in *Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No.04CH37513)*, Niagara Falls, pp. 469-472, May 2004.

[14] C. Kauba, S. Kirchgasser, V. Mirjalili, A. Uhl, and A. Ross, "Inverse biometrics: Generating vascular images

From binary templates," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 3, no. 4, pp. 464-478, Apr. 2021.

[15] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, "On the vulnerability of face verification systems to hill-climbing attacks," *Pattern Recognition*, vol. 43, no. 3, pp. 1027-1038, Mar. 2010.

[16] M. Gomez-Barrero, J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Face verification put to test:a hill-climbing attack based on the uphill-simplex algorithm," in *5th IAPR International Conference on Biometrics (ICB)*, New Delhi, pp. 40-45, Apr. 2012.

[17] C. Rathgeb and A. Uhl, "Attacking iris recognition:An efficient hill-climbing technique," in *20th International Conference on Pattern Recognition*, Istanbul, pp. 1217-1220, Oct. 2010.

[18] J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez and J. Ortega-Garcia, "Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms," *Computer Vision and Image Understanding*, vol. 117, no. 10, pp. 1512-1525, Oct. 2013.

[19] F. Wang, L. Leng, A. B. J. Teoh, and J. Chu, "Palmprint false acceptance attack with a generative adversarial network (GAN)," *Applied Sciences*, vol. 10, no. 23, p. 8547, Nov. 2020.

[20] Y. Sun, L. Leng, Z. Jin, and B. G. Kim, "Reinforced palmprint reconstruction attacks in biometric systems," *Sensors*, vol. 22, no. 2 p. 591, Jan. 2022.

[21] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. J. Goodfellow, and R. Fergus, "Intriguing properties of neural networks," in *International Conference on Learning Representations (ICLR)*, Banff, Apr. 2014.

[22] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," in *International Conference on Learning Representations (ICLR)*, San Diego, May 2015.

[23] A. Kurakin, I. Goodfellow, and S. Bengio, Adversarial Machine Learning at Scale," https://arxiv.org/abs/1611.01236, Feb. 2017.

[24] N. Carlini and D. Wagner, "Towards Evaluating the Robustness of Neural Networks," in *2017 IEEE Symposium on Security and Privacy (SP)*, San Jose, pp. 39-57, Jun. 2017.

[25] S. M. Moosavi-Dezfooli, A. Fawzi, and P. Frossard, "Deepfool: A simple and accurate method to fool deep neural networks," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, Las Vegas, pp. 2574-2582, Jun. 2016.

[26] C. Xiao, B. Li, J. Y. Zhu, W. He, M. Liu, and D. Song, Generating adversarial examples with adversarial networks, https://arxiv.org/abs/1801.02610, 2018.

[27] S. Jandial, P. Mangla, S. Varshney, and V. Balasubramanian, "Advgan++: Harnessing latent layers for adversary generation," in *Proceedings of the IEEE/CVF International Conference on Computer Vision Workshops*, Seoul, Oct. 2019.

[28] X. Bai, N. Gao, Z. Zhang, and D. Zhang, "3D palmprint identification combining blocked ST and PCA," *Pattern Recognition Letters*, vol. 100, no. 2017, pp. 89-95, Dec. 2017.

[29] L. Leng, J. Zhang, M. K. Khan, X. Chen, and K. Alghathbar, "Dynamic weighted discrimination power analysis: A novel approach for face and palmprint recognition in DCT domain," *International Journal of Physical Sciences*, vol. 5, no. 17, pp. 2543-2554, Dec. 2010.

[30] L. Leng, M. Li, and C. Kim, "Dual-source discrimination power analysis for multi-instance contactless palmprint recognition," *Multimedia Tools and Applications*, vol. 76, no. 1, pp. 333-354, Nov. 2017.

[31] L. Fei, J.Wen, Z. Zhang, K. Yan, and Z. Zhong, "Local multiple directional pattern of palmprint image," in *International Conference on Pattern Recognition (ICPR)*, Cancun, pp. 3013-3018, Dec. 2016.

[32] Y. Liu and A. Kumar, "Contactless palmprint identification using deeply learned residual features," *IEEE Transactions on Biometrics*, *Behavior, and Identity Science*, vol. 2, no. 2, pp. 172-181, Apr. 2020.

[33] Lu. Leng, Z. Yang, and W. Min, "Democratic voting downsampling for coding-based palmprint recognition," *IET Biometrics*, vol. 9, no. 6, pp. 290-296, Aug. 2020.

[34] Z. Yang, L. Leng, and W. Min, "extreme downsampling and joint feature for coding-based palmprint recognition," *IEEE Transactions on Instrumentation and Measurement,* vol. 70, pp. 1-12, Nov. 2021.

[35] Z. Yang, J. Li, W. Min, and Q. Wang, "Real-time preidentification and cascaded detection for tiny faces," *Applied Sciences*, vol. 9, no. 20, p. 4344, Oct. 2019.

[36] Y. Liu, H. Yuan, Z. Wang, and S. Ji, "Global pixel transformers for virtual staining of microscopy images," *IEEE Transactions on Medical Imaging*, vol. 39, no. 6, pp. 2256-2266, Jun. 2020.

[37] L. Leng, Z. Yang, C. Kim, and Y. Zhang, "A lightweight practical framework for feces detection and trait recognition," *Sensors*, vol. 20, no. 9, p. 2644, May. 2020.

[38] D. Zhong and J. Zhu, "Centralized large margin cosine loss for open-set deep palmprint recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 6, pp. 1559-1568, Jun. 2020.

[39] W. M. Matkowski, T. Chai, and A. W. K. Kong, "Palmprint recognition in uncontrolled and uncooperative environment," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1601-1615, Oct. 2020.

[40] X. Liang, J. Yang, G. Lu, and D. Zhang, "CompNet: Competitive neural network for palmprint recognition using learnable gabor kernels," *IEEE Signal Processing Letters*, vol. 28, pp. 1739-1743, Aug. 2021.

[41] T. Wu, L. Leng, M. K. Khan ,and F. A. Khan, "Palmprint-palmvein fusion recognition based on deep hashing network," *IEEE Access*, vol. 9, pp. 135816-135827, Sep. 2021.

[42] L. Leng and J. Zhang, "Palmhash code vs. palmphasor code," *Neurocomputing*, vol. 108, no. 2, pp. 1-12, May 2013.

[43] H. Xu, L. Leng, A. B. J. Teoh, and Z. Jin, "Multi-task pre-training with soft biometrics for transfer-learning palmprint recognition," *Neural Processing Letters*, pp. 1-18, Apr. 2022.

[44] D. Zhang, W. K. Kong, J. You, and M. Wong, "Online palmprint identification," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 9, pp. 1041-1050, Sep. 2003.

[45] Z. Guo, D. Zhang, L. Zhang, and W. Zuo, "Palmprint verification using binary orientation co-occurrence vector," *Pattern Recognition Letters*, vol. 30, no. 13, pp. 1219-1227, May.2009.

[46] Z. Sun, T. Tan, Y. Wang, and S. Z. Li, "Ordinal palmprint represention for personal identification," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)*, San Diego, pp. 279-284, Jun. 2005.

[47] A. Kong, D. Zhang, and M. Kamel, "Palmprint identification using feature-level fusion," *Pattern Recognition*, vol. 39, no. 3, pp. 478-487, Aug. 2005.

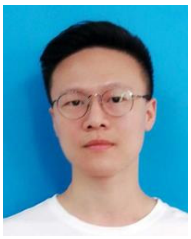
[48] A. K. Kong and D. Zhang, "Competitive coding scheme for palmprint verification," in *Proceedings of the 17th International Conference on Pattern Recognition (ICPR)*, Cambridge, pp. 520-523, Aug. 2004.

[49] W. Jia, D. S. Huang, and D. Zhang, "Palmprint verification based on robust line orientation code," *Pattern Recognition*, vol. 41, no. 5, pp. 1504-1513, Oct. 2007.

[50] L. Fei, Y. Xu, W. Tang, and D. Zhang, "Double-orientation code and nonlinear matching scheme for palmprint recognition," *Pattern Recognition*, vol. 49, pp. 89-101, Aug. 2015.

[51] Y. Xu, L. Fei, J. Wen, and D. Zhang, "Discriminative and robust competitive code for palmprint recognition," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 2, pp. 232-241, Feb. 2018.

AUTHORS



Yue Sun received his BS degrees in Nanjing Forestry University, Nanjing, China, in 2018. He is now pursuing his M.S. degree in Nanchang Hangkong University, Nanchang, China. His research interests include pattern recognition, image processing, and deep learning.

Changkun Wang obtained his M.E. degree from Harbin Institute of Technology, P. R. China. He is currently an associate professor of School of Information Engineering, Nanchang Hangkong University.
He has presided over 30 engineering subjects and published over 20 papers. His research interests include control theory, control engineering and automatics.