Deepfake Detection For Palmprint Authentication

Min-Jen Tsai[1] and Cheng-Tao, Chang[1,2]
Institute of Information Management, National Yang Ming Chiao Tung University [1]
1001 Ta-Hsueh Road, Hsin-Chu, 300, Taiwan, R.O.C[1]
Broadband Networks Laboratory, Chunghwa Telecom Laboratories[2]
No. 99, Dianyan Rd., Yangmei Dist., Taoyuan City, Taiwan, R.O.C.[2]

***Abstract*—The focus of this paper is palmprint recognition. Using the database of Hong Kong Polytechnic University.** A **method is proposed to generate synthetic palmprint images by using different types of GANs. These images are evaluated by a MesoNet algorithm to achieve an AUC score of 0.66. The results demonstrate the algorithm's accuracy in detecting deepfake palmprints.**

Keywords—Palm print, DCGAN, WGAN, Cycle GAN, Deepfake Detection

I. Introduction

Biometric authentication, which includes fingerprint and facial recognition, has greatly advanced in recent years. Zhang et al. [1] have made notable contributions to palmprint recognition. GANs can generate synthetic data while distinguishing real samples from fake ones using adversarial learning. The GAN network architecture is illustrated in Fig. 1.

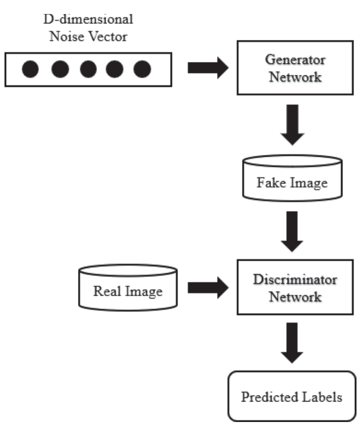


Fig. 1. Architecture of the GAN network.

Shervin et al. [2] proposed a palmprint generation method using Total Variation and analyzed the generation status with the use of an epoch change chart. Zhang et al. [3] exemplified deepfake detection using SURF-based feature point detection to recognize manipulated videos. However, tampering with biometric databases, including palmprint databases, is of growing concern. Therefore, random samples from the Poly-U palmprint database are used in this paper to generate synthetic palmprints by various GANs, such as Deep Convolutional Generative Adversarial Networks (DCGAN) [4], Wasserstein GAN(WGAN) [5], and Cycle GAN [6]. The results are detected by the MesoNet [7] model.

II. Proposed System

This section contains an in-depth description of the technical aspects of the palmprint generation framework, which utilizes GANs and the MesoNet prediction model, as illustrated in Fig. 2. DCGAN is a CNN-based GAN that replaces pooling layers, incorporates Batch Normalization and employs activation functions in both the generator and discriminator [4]. WGAN addresses GANs' training instability by employing Wasserstein distance and enforcing the Lipschitz constraint. Meanwhile, Cycle GAN enables image style transfer without paired training data using two generators and discriminators. The MesoNet architecture comprises convolutional and pooling layers, a dense network with a hidden layer, ReLU activation, and Batch Normalization.

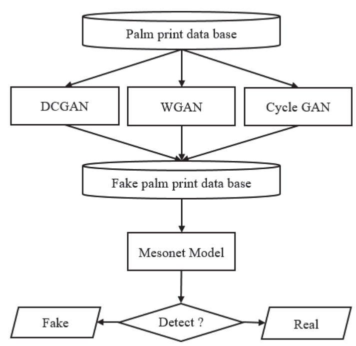


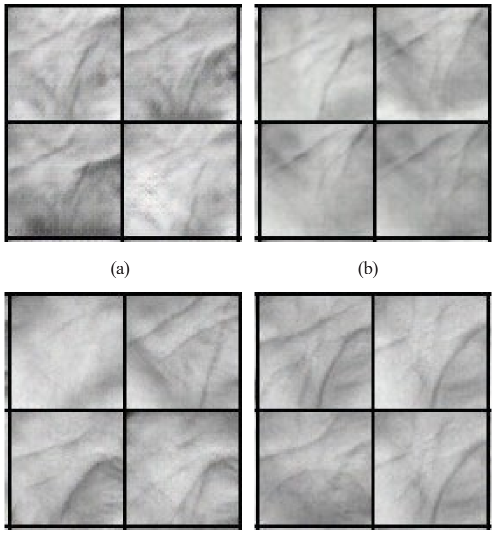
Fig. 2. Prediction of the system of Palm-GANs generation by the MesoNet model.

III. Experimental Results

The results of generating synthetic palmprint images using various GAN techniques with random samples from the Poly-U palmprint database [8] and their detection using MesoNet are discussed in this section.

A. DCGAN

The experimental results of the proposed DCGAN architecture revealed a gradual improvement in the clarity of fake images generated from images Fig. 3(a), 3(b), 3(c), and 3(d) as the training epochs increased, as depicted in Fig. 3.



(a) (b)

(c) (d)

Fig. 3. DCGAN output images show the generated images at different epochs. Specifically, images (a), (b), (c), and (d) were generated at epoch 20, 40, 60, and 80, respectively.

B. WGAN

WGAN demonstrated improved stability and generated high-quality images with reduced mode collapse compared to traditional GANs, as shown in Fig. 4.

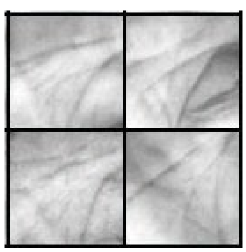


Fig. 4. Results generated by WGAN.

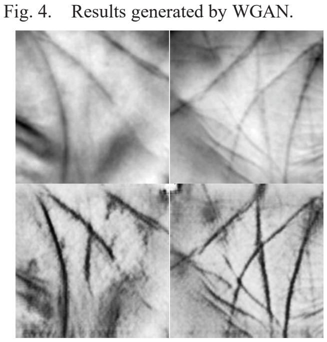


Fig. 5. The top row represents real images, while the bottom row depicts the fake images generated by Cycle GAN.

C. Cycle GAN

This study used the Cycle GAN method to generate the fake palmprint images. Their quality was assessed based on visual appearance, critical feature accuracy, and similarity to real palmprints. The results indicated the evolving nature of the generated images, which exhibited high fidelity and captured essential palmprint features, as shown in Fig 5.

D. MesoNet prediction

MesoNet is a binary classifier built as a relatively shallow Convolutional Neural Network (CNN), trained to classify images into one of two classes. One class refers to "real" images (images of real palmprint), and the other refers to "fake" images (images generated by DeepFake AI). Synthetic palm prints were developed using the Poly-U palmprint database with various GAN methods. The evaluation yielded an AUC value 0.66, indicating that the performance surpassed random guessing (AUC = 0.5), as shown in Fig. 6.

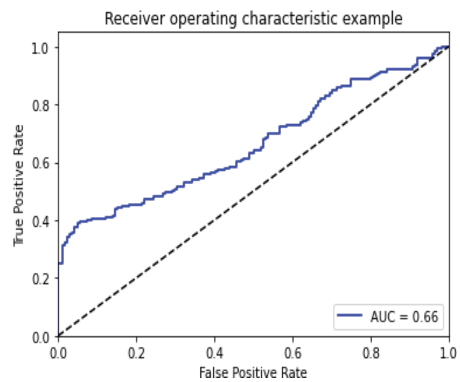


Fig. 6. Results of AUC with MesoNet

IV. CONCLUSION

Adversarial generative networks were used in this paper to generate manipulated biometric features and applied deepfake detection techniques. The MesoNet method proved effective in detecting tampered images, and a proposed solution for determining palmprint image manipulation showed promising results. Future researchers will explore additional deepfake detection methods in this emerging field.

REFERENCES

[1] D. Zhang, W.K. Kong, J. You and M. Wong, "Online Palmprint ldentification," lEEE Transactions on lnstrumentation and Measurement, vol. 25, pp. 1041-1050, 2003.

[2] Shervin Minaee, Mehdi Minaei, Amirali Abdolrashidi "Palm-GAN: Generating Realistic Palmprint lmages Using Total-Variation Regularized GAN," https://doi.org/10.48550/arXiv.2003.10834

[3] Zhang Y, Zheng L, Thing V L L. Automated face swapping and its detection[C]//2017 lEEE 2nd lnternational Conference on Signal and lmage Processing (lCSlP). lEEE, 2017: 15-19.

[4] Radford, Alec, Luke Metz, and Soumith Chintala. "Unsupervised representation learning with deep convolutional generative adversarial networks." arXiv preprint arXiv:1511.06434 (2015).

[5] Arjovsky, Martin, Soumith Chintala, and Leon Bottou. "Wasserstein gan." arXiv preprint arXiv:1701.07875 (2017).

[6] Zhu, Jun-Yan, et al. "Unpaired image-to-image translation using cycle-consistent adversarial networks." Proceedings of the lEEE international conference on computer vision. 2017

[7] D. Afchar, V. Nozick, J. Yamagishi, and l. Echizen. "MesoNet: a compact facial video forgery detection network." ln 2018 lEEE international workshop on information forensics and security (WlFS), pages 1—7. lEEE, 2018.

[8] PolyU Palmprint Database, Multispectral Palmprint Database. [Online]. Available at http://www.comp.polyu.edu.hk/biometrics/