Synthesizing Fingerprint from Pattern Type Analysis Features using cGAN

Samuel Lee, Jae-Gab Choi, Jin-Ho Park, Gye-Young Kim[1]

School of Software, Soongsil University, 378, Sangdo-ro, Dongjak-gu, Seoul, Republic of Korea
{lsme8821, kor03, j.park, gykim11}@ssu.ac.kr

Abstract. This paper proposes a kind of cGAN (Conditional Generative Adversarial Nets), FingerNet. FingerNet automatically generates synthesized fingerprint images using features of fingerprint pattern type.

Keywords: Biometric, Fingerprint, Deep Neural Nets, Conditional Generative Adversarial Nets

1 Introduction

The fingerprints of a person are unique for other persons, therefore, fingerprint recognition technologies have been developing by a lot of companies and research centers for the purpose of identifying and authenticating the person in financial and security. However, due to the immutability of the fingerprint, it can cause a problem when the fingerprint image is leaked. In order to cope with this, the fingerprint image is stored as a template of pattern type analysis features (like left, right, whorl, arch, tent arch) or a line analysis features (like minutiae) without storing the fingerprint image as it is. Since the template also includes the main features of the fingerprint, when the template information is leaked to the outside, it can be synthesized from the template information to the fingerprint at the time of registration [1][2]. However, since the existing fingerprint synthesis methods use only the line analysis features of the fingerprint, the pattern type analysis features are not considered. In this paper, we propose a fingerprint synthesizer using the neural nets (Conditional GAN) from the pattern type analysis features rather than the line analysis features, and show the vulnerability of the fingerprint recognizer using the pattern type analysis features.

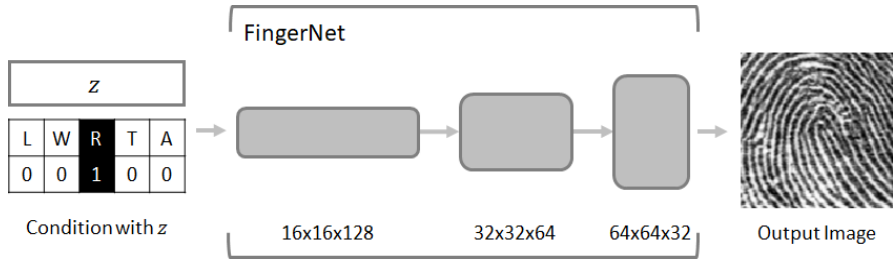
2 Synthesizing Fingerprint using cGAN

The proposed deep neural networks based fingerprint synthesizer structure and the neural network structure used in this paper are shown in “Fig 1”. We use a conditional GAN that can generate images according to a given condition rather than a general GAN that generates an arbitrary image for generation of a fingerprint image

[1] Corresponding Author

corresponding to the pattern type analysis features. The neural network structure used in the conditional GAN uses FingerNet. FingerNet uses 1x105 sized data includes 100-dimensional noise vector (z) with 5-dimensional one-hot encoded pattern type analysis features vector (x) as input and generates an 8 bits 1 channel 128x128 sized image. And FingerNet consists of 1 fully-connected layer and 3 convolutional layers. All layers in the networks perform batch normalizing and use the Rectified Linear Unit (ReLU) as an activation function except for an output layer using Sigmoid as an activation function.

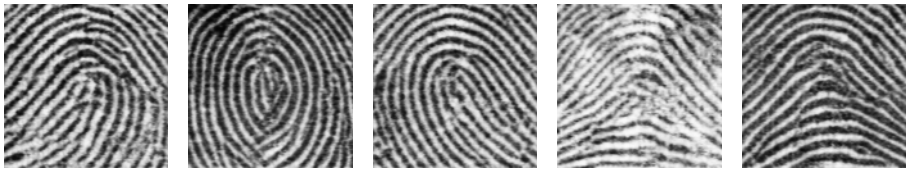
Fig. 1. The Architecture of Fingerprint Synthesizer using Conditional GAN with FingerNet.



3 Experimental Results

In this experiment, NIST Special Database 4 fingerprint database [5] is used for learning of the FingerNet, and the fingerprint images is scaled down to 75% size and then normalized to 128x128 image centered on the fingerprint core point. The fingerprint image synthesized using cGAN with pre-trained FingerNet is shown in "Fig. 2", and the pattern type accuracy of the synthesized fingerprint image is 89.59%. In the case of the fingerprint recognizer using the pattern type analysis features, the accuracy of the fingerprint image is sufficient enough to disable the fingerprint recognizer.

Fig. 2. Synthesized Fingerprints using Conditional GAN with FingerNet.



Acknowledgments

This work was supported by the National Research Foundation of Korean (NRF) grant funded by the Korea government (MSIP; Ministry of Science, ICT & Future Planning) (No. NRF-2016K1A3A1A19945935).

References

1. C. J. Hill, "Risk of masquerade arising from the storage of biometrics", B.S. thesis, Dept. Comput. Sci., Austral. Nat. Univ. Canberra, ACT, Australia, (2001).
2. J. Feng, "Fingerprint Reconstruction: From Minutiae to Phase", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 33, No. 2, 209-223p, (2011).
3. I. J. Goodfellow, "Generative adversarial nets", In Proceedings of NIPS, Advances in Neural Information Processing Systems 27, 2672–2680p, (2014)
4. M. Mirza, "Conditional Generative Adversarial Nets", https://arxiv.org/abs/1411.1784, (2014).
5. C. I. Watson, "NIST Special Database 4", National Institute of Standards and Technology, Advanced Systems Division, Image Recognition Group, (1992).

Appendix: Pre-trained weights and sources codes for replication

Download pre-trained weight file and source codes used in this paper from https://github.com/prodeveloper0/UniquePrintV1