Similarity Analysis of Actual Fake Fingerprints and Generated Fake Fingerprints by DCGAN

Seoung-Ho Choi¹ and Sung Hoon Jung²

¹Department of Electronics and Information Engineering, Hansung University, Seoul, Korea

²Division of Mechanical and Electronics Engineering, Hansung University, Seoul, Korea

ljfis

Abstract

This paper proposes a verification method whether fake fingerprints generated by DCGAN are similar to actual fake fingerprints in order to augment fake fingerprint data. The first method to verify is to compare the distributions of the mean and standard deviation of fake fingerprints generated by deep convolutional generative adversarial network (DCGAN) with those of actual fake fingerprints. In the second method, the mean Hamming distance, which is a method of evaluating the similarity of images, is used for measuring the similarity between the generated fake fingerprints and the actual fake fingerprints. The third method is to obtain the histograms of the generated fake fingerprints and actual fake fingerprints and measure the similarity by calculating Pearson correlation of the histograms. The fourth method is to calculate intersection of union, which is a method of evaluating the shape similarity of images, between generated fake fingerprints and actual fake fingerprints. From extensive experiments it was confirmed that fake fingerprints generated by DCGAN could be used to augment fake fingerprint data because generated fake fingerprints are similar to actual fake fingerprints in terms of four similarity measures.

Keywords: DCGAN, Fake fingerprint generation, Fake fingerprint augmentation, Similarity measure

1. Introduction

Recently, biometrics technology with the activation of PinTech is attracting attention as the authentication technology. Biometrics is a method for recognizing human biological characteristics, such as signature, iris, and fingerprint recognition. Although these biometric technologies are widely used in electronic financial transactions, financial damages are also increasing due to fake biometric information. In order to solve this problem, various methods for discriminating fake biometric information have been recently developed [1–8]. Especially, as the successful applications of recent deep learning are increasing, some methods for discriminating fake biometric information using deep learning are being studied [1, 3–8].

Convolutional neural networks (CNN), which are major methods of image information processing, are mainly used for fake fingerprint discrimination methods using deep learning [3–6]. In these methods, about 5 to 7 convolutional layers are used for high fake discrimination performances and they require thousands to tens of thousands of training images. However, it takes a lot of time and cost to acquire real fingerprints and fake fingerprints. In addition, each

Received: Jan. 7, 2019
 Revised : Mar. 18, 2019
 Accepted: Mar. 20, 2019

Correspondence to: Sung Hoon Jung
 (shjung@hansung.ac.kr)
 ©The Korean Institute of Intelligent Systems

©This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

time a fingerprint sensor is changed, a large amount of new data must be acquired. This situation occurs in most cases of applying to deep learning. In certain applications, it is very difficult to obtain data even at a lot of time and cost. To solve the above problem, some methods have been devised to acquire augmenting data using the acquired training data. One of such methods is to rotate, move, or scale up/down the acquired learning data. However, this method is a simple modification not to make a lot of additional training data, so it is difficult to improve the performances [7–9]. In this paper, we propose a similarity verification method for augmenting training data between generated fake fingerprints by deep convolutional generative adversarial networks (DCGAN) and actual fake fingerprints. To make augmenting data, we use the DCGAN, which has been applied to various fields recently. After training actual fake fingerprints in DCGAN, we generate fake fingerprints using the generator of DCGAN.

In order to use the generated fake fingerprints to augment training data, generated fake fingerprints made by the DCGAN must maintain the characteristics of the actual fake fingerprints. Otherwise, the performances of the fake fingerprint discriminator using generated fake fingerprints made by the DCGAN may be lowered. Therefore, in this paper, we show through various experiments how similar the fake fingerprints made by DCGAN are to the actual fake fingerprints. We compare the distribution of the mean and standard deviation of the fake fingerprints generated by the DCGAN with those of the actual fake fingerprints as a first way to verify. In the second method, the mean Hamming distance (MHD), which is one method of evaluating the similarity of images, is used for measuring the similarity between the generated fake fingerprints and the actual fake fingerprints. The third method is to obtain the histograms of the generated fake fingerprints and the actual fake fingerprints and measure the similarity by calculating Pearson correlation of the two group of histograms. The fourth method is to calculate intersection of union (IOU) between the generated fake fingerprints and actual fake fingerprints. IOU is a method of evaluating the shape similarity of images.

To evaluate the above methods, we trained DCGAN using actual fake fingerprints and generated fake fingerprints using the generator of trained DCGAN. For experiments, four data settings are provided with a combination of generated fake fingerprints and actual fake fingerprints that are not trained to DCGAN. We tested similarity between generated fake fingerprints and actual fake fingerprints on these four data settings with four similarity measures. Experimental results showed that

the generated fake fingerprints made by DCGAN are similar to the actual fake fingerprints in most verification methods. This means that the generated fake fingerprints could be used to augment fake fingerprint data for training deep learning.

This paper is organized as follows: first, Section 2 explains the existing fake discrimination and generation methods. In Section 3, we describe the proposed method in this paper and the data generation method. Section 4 describes the experimental environment, experimental methods, and experimental results of the proposed method. Finally, Section 5 explains the conclusion and future research.

2. Related Works

Fingerprint recognition has been studied for a long time in various ways. The fingerprint of a person is acquired through the fingerprint sensor and the features of the fingerprint are extracted from the acquired image, and the features of the fingerprint are compared with the stored features to determine whether the fingerprint is the person. However, since the fingerprint is extracted through the image obtained from the sensor, there is a problem that actual fake fingerprints can't be distinguished from the fake fingerprints that are made of various materials. Various methods have been devised to prevent this problem [2–8]. There are hardware methods and software methods for fake fingerprint discrimination. The hardware approach requires additional sensors to extract features such as blood pressure [10] and skin deformity [11]. Most software methods make a decision by extracting and determining arbitrarily defined characteristics through an algorithm with fingerprint images obtained from a sensor.

In the software-based fake fingerprints discrimination method, Dhriti and Kaur [2] detect the fake fingerprints using KNN after feature extraction with Gabor filters. The research of fake fingerprint discrimination using CNN has been performed recently [3–8]. Marasco et al. [3] used the deep Siamese network to classify fake fingerprints. As a result, it showed robust classification performance according to the material of the fake fingerprints. However, the result of fake discrimination according to the sensor change showed weakly performance. Choi and Jung [4] showed that sequential images can be combined into a single image to include spatio-temporal information and CNN-LSTM can improve the performance of fake fingerprints discrimination. Park et al. [5] obtained a number of patches from fingerprint images and classified them into fake/real/background images by CNN.

Figure 1. Overall process of proposed method.

In the fake fingerprints discrimination using deep learning, many training data are needed for the fake fingerprints discrimination methods to show good performance. If the data is small, an overfitting occurs and the performances are good only for the training data. Furthermore, every time a fingerprint sensor is changed, a large amount of new data must be acquired, which is costly and time consuming. Moreover, there are many areas where it is difficult to obtain a large amount of data. For this purpose, a method of transforming data acquired in the past and using it as training data is also widely used. Methods of transforming existing data include rotating the image, reducing or enlarging the scale, or moving the position.

However, these methods can make only small transforming data because the transforming method is not various. Therefore, it is necessary to augment a large number of training data using existing data. In order to use the generated data as the augmentation data, it is necessary to verify whether the generated data is similar to the existing data. In this paper, we propose four methods to measure similarity between generated data and existing data.

3. Proposed Method

We propose four similarity measures to verify that the generated data by DCGAN can be used as augmented data. Figure 1 shows the overall structure of the fake fingerprint generation and evaluation methods proposed in this paper. In step 1 of Figure 1, fingerprint data is classified into four qualities for training by each quality and by all quality. Step 2 of Figure 1 shows the generation method of fake fingerprints data by

DCGAN. In order to investigate whether there is a difference between two training methods, DCGAN is trained by quality and by all quality. Step 3 is to measure the degree of similarity between fake fingerprints made by DCGAN and actual fake fingerprints. It is necessary to verify whether the fake fingerprint data made by DCGAN is similar to the actual fake fingerprint data. In order to evaluate the similarity of the generated fake fingerprints to the actual fake fingerprints, we proposed four similarity measures.

Firstly, the mean and standard deviation of images are calculated and compared between the generated fake fingerprint images and actual fake fingerprint images. Comparing the similarity with the mean and the standard deviation makes it possible to check the overall distribution of the images but not the detailed comparison of the images. Secondly, similarity was measured using the MHD developed as a method of measuring the similarity of two images. Thirdly, for comparison at the image histogram level, histograms of generated fingerprints and actual fake fingerprints were obtained and Pearson correlation between the histograms of the two data were obtained. Finally, shape similarity was measured using the IOU developed as a method of measuring the similarity of two images.

The method of generating fake fingerprints using DCGAN is as follows. We first obtain actual fake fingerprint images from the material of fake fingerprint generation such as silicon or clay. At this time, the quality of actual fake fingerprints may vary due to the state of the material or the shaking of the hand when the fingerprint image is acquired. That is, fake fingerprint images with bad quality are obtained if the material is too stiff to properly contact the measurement sensor. We divide the

actual fake fingerprint data with four qualities to see if there is a difference according to the quality of fake fingerprints. The quality of the actual fake fingerprint is classified into four levels. Q1 is the best quality, clean overall. Q2 is fake fingerprints that the outline or part of those is whitened. Q3 is worse than Q2, and Q5 is the case where only a part of the fingerprint is acquired. In order to generate fake fingerprint images, DCGAN is trained by quality or by all quality together. After training the DCGAN, the generator of DCGAN generates new fake fingerprints images by applying random latent z to the generator of DCGAN. The DCGAN structure used in our experiments is the same as that proposed by Radford et al. [9].

4. Experimental Results

4.1 Fake Fingerprints Generated by DCGAN

The DCGAN for generating fake fingerprints was implemented using TensorFlow developed by Google. Figure 2 shows the actual fake fingerprint samples for each of the four qualities. Fake fingerprints in Figure 2(a) are very accurate because there are no cracks in the fingerprints and no problem in acquiring the actual fake fingerprints. Figure 2(b) shows actual fake fingerprints with cracks. Fake fingerprints in Figure 2(c) are partially whitening fingerprints with cracks due to poor pressure on fingerprint acquisition. Figure 2(d) shows that the fingerprint acquisition did not work properly, resulting in a lot of white areas.

The DCGAN generator generates fingerprints that are similar to trained fake fingerprints as training progresses using the characteristics of fake fingerprints. Figure 3 shows the fake

Figure 2. DCGAN training data by quality: (a) Q1, (b) Q2, (c) Q3, (d) Q5.

Figure 3. DCGAN training process. At the beginning of training (a), during the middle of training (b), and the end of training.

fingerprints generated by the generator during the training process. Figure 3(a), 3(b), and 3(c) are generated images by the generator at the beginning of training, during the middle of training, and at the end of training, respectively. As you can see in Figure 3, the more the training progresses, the more and more similar fingerprints to the characteristics of the training fake fingerprints are created.

If DCGAN is trained enough, it will generate fingerprints that are quite similar to the actual fake fingerprints. Figure 4 shows the fake fingerprints generated by the DCGAN generator after training. As shown in the Figure 4, it can be seen that they are similar enough to be indistinguishable from the actual fake fingerprints. As shown in Figure 4(c) and 4(e), it can be seen that cracks and white parts occur similarly to the characteristics of the training fake fingerprints. As a result, the generator of DCGAN fully reflects the training data and generates fake fingerprints.

We should verify the similarity of generated fake fingerprints to actual fake fingerprints with four measures. When the similarity is verified with four measures, the generated fake fingerprints by DCGAN can be used as training data for augmenting training data. In the verification method with four measures, we use four data settings to see if the similarity depends on the quality of the fake fingerprints. Table 1 shows four data settings for verification of the similarity according to generated data by DCGAN and actual data. In data setting I, there are no generated fake fingerprints and 1,000 actual fake fingerprints. In data setting II, 600 actual fake fingerprints are trained for each quality in DCGAN, then 200 fake fingerprints are generated by DCGAN for each quality, and 200 actual fake fingerprints are combined to make 1,000 total fake fingerprints. In data setting III, DCGAN learns 2,400 actual fake fingerprints without

Figure 4. Generated Fake Fingerprint Data by DCGAN

Table 1. Data settings for verification of fake fingerprints

Data setting	DCGAN		Actual	Total
	Trained	Generated		
I (Original Quality)	0	0	1000	1000
II (Each Quality)	600 * 4	200 * 4	200	1000
III (All Quality)	2400	800	200	1000
IV (All Quality)	2400	1000	0	1000

distinguishing quality and generates 800 fake fingerprints, and combined to 200 actual fake fingerprints. The data setting IV is the same as the third one, but it generates 1,000 fake fingerprints. Therefore, data setting I and IV are composed of only actual fake fingerprints and only generated fake fingerprints, respectively. In these data settings, all data sets were used after normalization process.

4.2 Similarity Analysis

To analyze whether the fake fingerprints generated by DCGAN are similar to the actual fake fingerprints, our analyzes were performed. In this analysis, we compared them according to the four training data sets as shown in Table 1. This is because that it would be more meaningful to compare the generated fake fingerprints according to the methods of using them as training data.

First, the pixel value of the image was used to calculate and compare the mean and standard deviation of the image. In

Figure 5. Plot of mean and standard deviation of four data sets.

other words, the averages and standard deviations of images of four data sets are shown on the two-dimensional coordinates in order to compare the similarity of four data sets. Figure 5(f) and 5(g) shows the results of the mean and standard deviation of four data sets. First, the data set II, III, and IV, which use fake fingerprints generated by DCGAN, are slightly larger than the data set I in average, which use only actual fake fingerprints. This is probably because DCGAN generates a crack or a white part in the actual fake fingerprints with low quality.

In the data set II and III, since many generated fake fingerprints are included, we can see that the result is almost similar. It can be seen that there is almost no difference in terms of mean and standard deviation in the case of generating by quality and by all quality together. As you can see in Figure 5, data set IV composed of only generated fake fingerprints are overlapped to the data set I composed of only actual fake fingerprints. This indicates that the generated fake fingerprints by DCGAN are similar to the actual fake fingerprints in terms of the distribution of mean and standard deviations.

As a result, from the viewpoint of average and standard de-

Table 2. Analysis of various similarity methods.

	Data set			
	I-I	I-II	I-III	I-IV
Mean Hamming distance [12]	5955.69	6463.39	6446.29	6550.22
Pearson correlation of histogram [15]	0.682 ± 0.219	0.151 ± 0.272	0.272 ± 0.245	0.180 ± 0.111
Intersection of union [13]	0.50	0.45	0.55	0.53

viation analysis, they can be used to augment fake fingerprints. However, the mean and standard deviation represent the overall characteristics of the image and can not be used to measure the similarity of the image in detail. Therefore, three additional analyzes were performed to analyze the detailed characteristics. The MHD used in Sixt et al. [12] was used for the analysis of four data sets. The Hamming distance is increased when the reference pixel value is different from the comparison pixel value. All the extracted Hamming distances are added and divided by the number of pixels, then the total average Hamming distance is obtained.

Table 2 shows the MHD results between two data sets based on data set I. Hamming distance is obtained over all data pairs in two data sets and averaged. The smaller the MHD is, the more similar the two sets of images are. MHD of data set I-I is the smallest because they calculate themselves. The next best thing is data set I-III made by combining all qualities and then data set I-II made by quality. However, the difference between the two sets is very small, so there is no big difference. The worst case is comparison data set I-IV, where all the fake fingerprints were generated by the DCGAN. Although DCGAN produces something that is very similar to an actual fake fingerprint, it shows that it produces something slightly different from the actual fake fingerprint.

Finally, to analyze the similarity of the distribution of brightness values of images, each image is represented by histogram and analyzed by Pearson correlation of histogram for each data set. In other words, all pairs are generated from two sets of images and the Pearson correlation is obtained from each pair. As shown in Table 2, all results show positive correlation results. That is, the histogram of the generated fake fingerprints are similar to the histogram of the actual fake fingerprints. Experimental results show similar tendency to MHD measurement results. These results show that DCGAN can produce similar results to the brightness distribution of training data.

Table 2 shows the IOU results. IOU, a quantitative representation of overlapping parts of object detection [13, 14], has been

used as an evaluation of segmentation [16]. In this paper, we used the IOU as a similarity measure of two data sets through the full combination of the data of each data set based on the data setting I. For examples, I-II column in Table 2 shows the similarity of data set I and II, and shows the lowest value of similarity analysis in comparison data set I-II. Since data set II is made by each quality, the similarity of generated fake fingerprints is not totally followed much of fake fingerprints. In the case of comparison data set I-III and I-IV, it can be confirmed that the methods generated by whole quality are more similar to each other than those made by each quality. The difference between comparison data set I-III and I-IV is 0.02, which appears to be a difference in the experimental method depending on the presence or absence of 200 actual fake fingerprints. Through the four similarity measurement methods, it was shown that the fake fingerprint generated by DCGAN is similar to the actual fake fingerprint and they can be used for augmenting training data.

5. Conclusions

In this paper, we analyzed similarity of actual fake fingerprints and generated fake fingerprints by DCGAN with four similarity measures for augmenting training data. Experimental results showed that fake fingerprints generated by DCGAN are made by combining the features of training actual fake fingerprints and confirmed that the characteristics of the generated fake fingerprint are substantially similar to those of the actual fake fingerprints. From these results, we could conclude that the generated fake fingerprints by DCGAN were used for augmenting training data. These results are useful in the case where training data is costly and time-consuming to acquire, especially in areas where acquisition of training data is very difficult. As a further work, we will directly test the performance improvements of CNN and DNN using the augmenting training data by DCGAN.

Conflict of Interest

No potential conflict of interest relevant to this article was reported.

Acknowledgments

This research was financially supported by Hansung University.

References

- [1] S. H. Choi and S. H. Jung, "Performance improvement of fake discrimination using time information in CNN-based signature recognition," *Journal of Digital Contents Society*, vol. 19, no. 1, pp. 205-212, 2018. <https://doi.org/10.9728/dcs.2018.19.1.205>
- [2] Dhriti and M. Kaur, "K-nearest neighbor classification approach for face and fingerprint at feature level fusion," *International Journal of Computer Applications*, vol. 60, no. 14, pp. 13-17, 2012.
- [3] E. Marasco, P. Wild, and B. Cukic, "Robust and interoperable fingerprint spoof discrimination via convolutional neural networks," *Proceedings of IEEE Symposium on Technologies for Homeland Security*, Waltham, MA, 2016, pp. 1-6. <https://doi.org/10.1109/THS.2016.7568925>
- [4] S. H. Choi and S. H. Jung, "Analysis of the effect of space-time information on CNN-based fake fingerprint discrimination," *Proceedings of 2017 the Korea Software Congress*, 2017, pp. 1968-1970.
- [5] E. Park, W. Kim, Q. Li, and H. Kim, "Fingerprint liveness detection using patch-based convolutional neural networks," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 27, no. 1, pp. 39-47, 2017. <https://doi.org/10.13089/JKIISC.2017.27.1.39>
- [6] E. Park, W. Kim, Q. Li, H. Kim, and J. Kim, "Fingerprint liveness detection using CNN features of random sample patches," *Proceedings of 2016 International Conference of the Biometrics Special Interest Group*, Darmstadt, Germany, 2016, pp. 1-4. <https://doi.org/10.1109/BIOSIG.2016.7736923>
- [7] S. H. Choi and S. H. Jung, "Performance comparison of patch and non-patch method in fake fingerprint generation using auto-encoder," *Proceedings of 2017 the Korea Software Congress*, 2017, pp. 981-982.
- [8] S. H. Choi and S. H. Jung, "Generation for fake fingerprint data through GAN for detecting fake fingerprint by deep learning methods," *Proceedings of 2017 the Institute of Electronics and Information Engineers (IEIE) Conference*, 2017, pp. 965-966.
- [9] A. Radford, L. Metz, and S. Chintala, "Unsupervised representation learning with deep convolutional generative adversarial network," 2016, Available <https://arxiv.org/pdf/1511.06434.pdf>
- [10] P. Lapsley, J. Lee, D. Pare, and N. Hoffman, "Anti-fraud biometric scanner that accurately detects blood flow," US Patent 5737439, 1998.
- [11] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake finger detection by skin distortion analysis," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 3, pp. 360-373, 2006. <https://doi.org/10.1109/TIFS.2006.879289>
- [12] L. Sixt, B. Wild, and T. Landgraf, "RenderGAN: generating realistic labeled data," 2017, Available <https://arxiv.org/pdf/1611.01331.pdf>
- [13] S. Tang and Y. Yuan, "Object detection based on convolutional neural network," Stanford University, Stanford, CA, 2015.
- [14] A. Borji, "Pros and cons of GAN evaluation measures," *Computer Vision and Image Understanding*, vol. 179, pp. 41-65, 2019.
- [15] A. Sanborn and J. Skryzlin, "Deep learning for semantic similarity," Stanford University, Stanford, CA, 2015.
- [16] K. Regmi and A. Borji, "Cross-view image synthesis using conditional GANs," *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, Salt Lake City, UT, 2018, pp. 3501-3510. <https://doi.org/10.1109/CVPR.2018.00369>
- [17] J. Wang and L. Perez, "The effectiveness of data augmentation in image classification using deep learning," 2017, Available <https://arxiv.org/pdf/1712.04621.pdf>

- [18] S. K. Lim, Y. Loo, N. T. Tran, N. M. Cheung, G. Roig, and Y. Elovici, "Doping: generative data augmentation for unsupervised anomaly detection with GAN," *Proceedings of 2018 IEEE International Conference on Data Mining (ICDM)*, Singapore, 2018, pp. 1122-1127. <https://doi.org/10.1109/ICDM.2018.00146>
- [19] M. Podduturi, "Data augmentation for supervised learning with generative adversarial networks," Master's thesis, Iowa State University, Ames, IA, 2018.

Seoung-Ho Choi is a Bachelor's graduated at Department of Electronics and Information Engineering, Hansung University, Korea, in 2018. He majored in artificial neural network in his Bachelor's research. He has been working on research related to deep learning, geometry, probability and statistics, interpretable & explainable theory, and graph theory.

E-mail: jcn99250@naver.com

Sung Hoon Jung received his B.S.E.E. degree from Hanyang University, Korea, in 1988 and M.S. and Ph.D. degrees from KAIST, in 1991 and 1995, respectively. He joined the Department of Information and Communication Engineering at the Hansung University in 1996, where he is a professor. His research interests are in the fields of intelligent systems and systems biology. He is a member of the Korean Institute of Intelligent Systems (KIIS) and Institute of Electronics Engineers of Korea (IEEK).

E-mail: shjung@hansung.ac.kr