Fake Fingerprint Detection Biometric System Using Neural Network Algorithm

Young-Hyun Baek, Byunggeun Kim, and Seock-Han Kim
Unioncommunity Co., Ltd, Seoul, Korea
Email: neural76@unioncomm.co.kr, {byunggni, hanny33}@unioncomm.co.kr

***Abstract*—The fingerprint recognition system is the most used among various biometric methods. Biometric systems are vulnerable to fake attacks, and many studies have been done to solve it. Therefore, in this paper, we propose a fake fingerprint detection method using neural network. To evaluate the proposed method, we have evaluated the fake fingerprint detection method using various materials. Experimental results show that the detection rate for fake fingerprint is 97.6% on average, which proves an effective detection method.**

***Index Terms*—fingerprint, neural network, biometric, fake fingerprint**

I. Introduction

Biometrics is a technology that recognizes various features, such as fingerprint, face, iris, and vein that use physical features. Behavioral features include voice, gait, signature recognition and etc. The biometric system is divided into enrollment, which extracts and stores the features of the user, verification, which identifies the registered information and the identification of the user depending on the matching method, and identification to identify the user among many people. Many studies are done about fake fingerprint extraction method in the fake fingerprint recognition system [1]-[3]. In this paper, we propose a method to detect the fake fingerprints by using its own features and difference of various materials (silicon, gelatin, rubber, paper and film).

This paper is organized as follows. Section II describes the biometric system. Section III describes the definition of fake fingerprints. Section IV shows the experiments results of the proposed method, and final conclusions are made in Section V.

II. Biometric System

The biometric system has a vulnerability as shown in Fig. 1 and can be divided into 8 attack points as shown below [3].

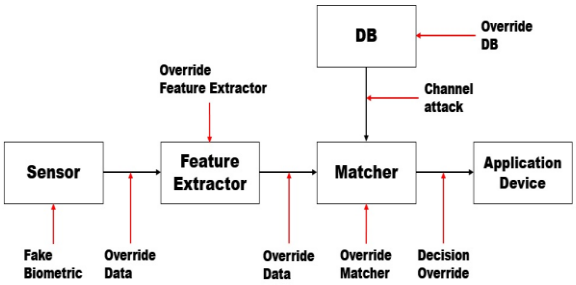


Figure 1. The attack point of biometric system.

1) *Biometric input device attack*
2) *Attack on data transmission*
3) *Attack on data extraction*
4) *Attack from the extracted data*
5) *Comparative data attack*
6) *The stored data attack*
7) *Attack on the stored data transmission*
8) *Attack in matching results*

The biometric system has a various of attack points as above. We have studied how to detect the fake fingerprint in the biometric input device, which is the first attack point.

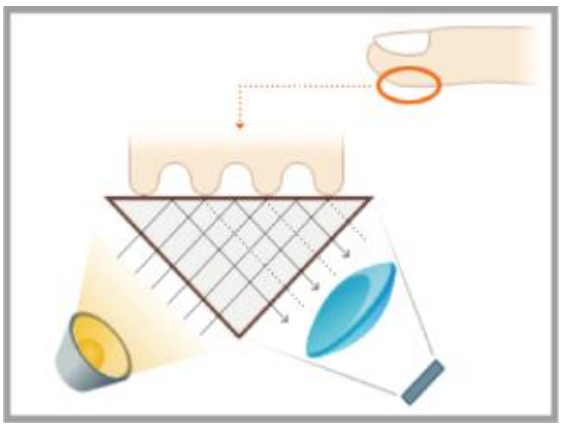


Figure 2. The attack point of biometric system.

The biometric system uses a various of technologies such as fingerprint, face, and iris and the most common one is the fingerprint recognition technology. The fingerprint recognition technology can be captured by

Manuscript received September 15, 2018; revised December 6, 2018.

doi: 10.18178/ijsps.6.4.27-30

various methods such as optical method, semiconductor method, and ultrasonic method and Fig. 2 is a method of capturing the fingerprint by optical method [4], [5].

The optical fingerprint capture acquires the fingerprint image by using the absorption and reflection of the ridges and valleys of the fingerprint by using a light source. At this time, the difference between the real and fake fingerprint occurs.

III. Biometric System

Fake fingerprints can be made with the various materials and can be made from silicon, rubber, OHP film, paper, and gelatin as shown in Fig. 3.

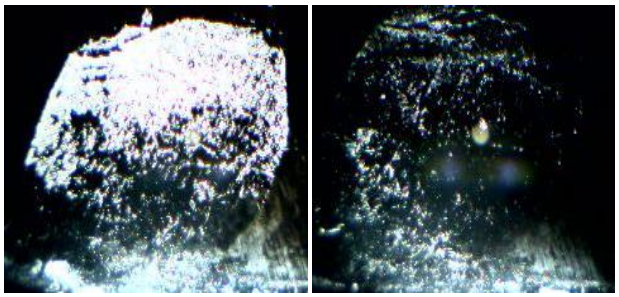
Figure 3. The various materials of fake fingerprint.

Fig. 4 shows a real production example about a fake fingerprint. The fake fingerprint can be affected by the quality of material and features of materials and made with blur, crushing ridges, and hole.

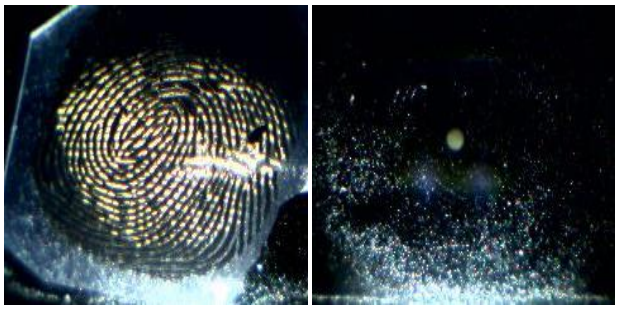
Figure 4. The various materials of fake fingerprint.

Fig. 5 shows the fingerprint image that captures the real fingerprint and a various of fake fingerprints by the optical method. Fig. 5(a) shows the image that captures the real fingerprint and Fig. 5(b, c, d, e, f) shows a variety of fake fingerprint images, which are paper, film, rubber, silicon, and gelatin, respectively. Fig. 5(a) is the real fingerprint, which is reddish in the center compared to the surrounding area. Fig. 5(b) is a fake fingerprint image made by paper. When a fingerprint is reflected by water, a ridge is not shown. Also, when a white object appears or no water, the image is not shown well. Fig. 5(c) is a fake fingerprint image made by film. When a fingerprint is reflected by water, a ridge is shown and no other images appears. Fig. 5(d) is a fake fingerprint image made by rubber, in which ridges are cut off or the hole appears depending on the fingerprint production quality. Also, the value of ridges shows equally. Fig. 5(e) is a fake fingerprint image made by silicon. The values of ridges are generally high and it can show the crushing of ridges and hole. Fig. 5(f) is a fake fingerprint image made by gelatin, which shows the same color with 5(a) and can show the ridge crushing, and hole depending on the production quality.

(a) Real fingerprint



(b) Paper fake fingerprint



(c) Film fake fingerprint

(d) Rubber fake fingerprint

(e) Gelatin fake fingerprint

Figure 5. Image that captures the read and fake fingerprint.

IV. The Proposed Method

The proposed method is to extract the real and fake fingerprint using the reflection and absorption in color light source. Thus, it consists of two major modules. Fig. 6 shows the structure of the proposed fake fingerprint detection, which can be divided into feature extraction module and classification module using neural network. The module for extracting the features are to extract the parameters to input to the neural network and can be divided into 4 method. The feature extraction step extracts the parameters to be input to the neural network in 4 ways. The first extracts the color change, the second extracts the histogram of the RGB channel, the third extracts the ridge width, and finally the hole. The neural network classification step classifies real and fake fingerprints using the training data [6]-[9].

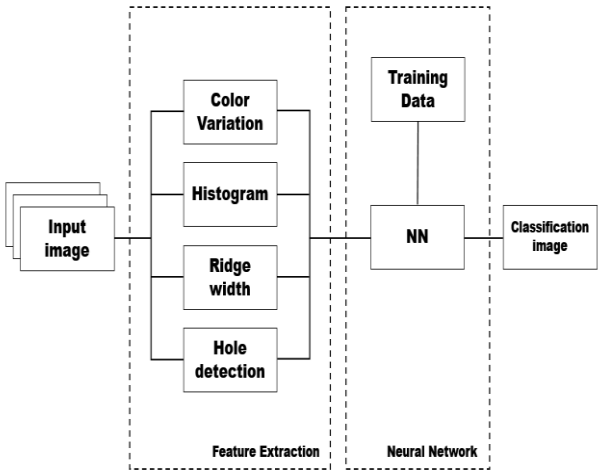


Figure 6. The proposed detection biometric system

Table I shows the experimental results. As shown in Table I, the proposed method showed an average detection rate of 97.5%.

TABLE I. Type Sizes for Camera-Ready Papers

Fake Type	Try (#)	Success (#)	Fail (#)
Paper	100	100	0
Film	100	100	0
Rubber	100	99	1
Silicon	100	97	3
Gelatin	100	92	8
Total value	500	488	12
Average [%]	-	97.6%	2.4%

Fake fingerprints made of paper and film among the materials of fake fingerprints could be detected at 100%. Other rubber, silicon, and gelatin fake fingerprints showed 99%, 97%, and 92% detection performance, respectively. Gelatin was able to acquire images similar to real fingerprints, and had similar elasticity, color, and features of real fingerprints, resulting in a lower detection performance than other fake fingerprints.

V. Conclusion

In this paper, we propose a detection method using a neural network to detect fake fingerprints of various materials. To evaluate the performance of the proposed reconstruction method, we used images of silicon, gelatin, rubber, film, and paper. As a result, an average of 97.6% was detected in various fake fingerprints, proving to be efficient. Future research will be conducted to improve the performance of gelatin fake fingerprints.

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No. 2017-0-00154, Mobile based biometrics performance and liveness detection technology development).

References

[1] C. Sousedik and C. Busch, “Presentation attack detection methods for fingerprint recognition systems: A survey,” *IET Biometrics*, vol. 2, pp. 1-15, 2014.

[2] A. Al-Ajlan, “Survey on fingerprint liveness detection,” in *Proc. 2013 International Workshop on Biometrics and Forensics (IWBF)*, 2013.

[3] S. S Kulkarni and H. Y Patil, “Survey on fingerprint spoofing, detection techniques and databases,” in *Proc. IJCA Proceedings on National Conference on Advances in Computing*, 2015, pp. 30-33.

[4] D. Maltoni *et al*., *Handbook of Fingerprint Recognition*, Springer, 2009.

[5] Q. Zhanga *et al*., “Fingerprint classification based on extraction and analysis of singularities and pseudoridges,” *Pattern Recognition*, vol. 37, pp. 2233-2243, 2004.

[6] J. Chang and K. Fan, “A new model for fingerprint classification by ridge distribution sequences,” *Pattern Recognition*, vol. 35, pp. 1209-1223, 2002.

[7] S. Kulkarni, “Fingerprint feature extraction and classification by learning the characteristics of fingerprint patterns,” *Neural Network World*, pp. 219-226, 2011.

[8] R. Collobert and J. Weston, “A unified architecture for natural language processing,” in *Proc. International Conference on Machine Learning*, 2008, pp. 160-167.

[9] R. Socher *et al*., "Dynamic pooling and unfolding recursive autoencoders for paraphrase detection," in *Proc. International Conference on Neural Information Processing Systems*, 2011, pp. 801-809.

Young-Hyun Baek is Chief Technology Officer (CTO) of Unioncommunity R&D Center. He received his B.S. and M.S. degrees in Electronic Engineering from Wonkwang University, Korea, in 2002 and 2004, respectively and his Ph.D. in Electronic Engineering from the University of Wonkwang in 2007. Dr. Baek was Assistant Professor of the Division of Electronic & Control Engineering at the Wonkwang University. He served or currently serving as a reviewer and Technical Program Committee for many important Journals, Conferences, Symposiums, Workshop in Biometrics, Image Processing, Optical Device area. His research interests include Fingerprint Sensor, Biometrics Security System, Fake finger Technology. He is a member of the IEEE, IEEK, TTA, KISA Technical pool.

Byunggeun Kim received his M.S. degree in Advanced Technology Fusion from Konkuk University, Korea, in 2010. Currently, he worked at the Unioncommunity R&D Center as a Senior Research Engineer. His research interests include Pattern Recognition, Face Recognition, Image Processing, Live Finger Detection, Fingerprint Classification and High Performance Fingerprint Recognition Systems.

Seock-Han Kim received his M.S. degree in Electronic and Electrical Engineering from Dankuk University, Korea, in 2010. Currently, he worked at the Unioncommunity R&D Center as a Senior Research Engineer. His research interests include Fingerprint Algorithm, Live Fingerprint Detection, Fingerprint Classification, Fingerprint Recognition Systems.