IEIE Transactions on Smart Processing and Computing, vol. 6, no. 2, April 2017
https://doi.org/10.5573/IEIESPC.2017.6.2.071

Smart Optical Fingerprint Sensor for Robust Fake Fingerprint Detection

Young-Hyun Baek

Research Institute, Union Community Co., Ltd. / Seoul, Korea neural76@unioncomm.co.kr

Received October 17, 2016; Revised January 5, 2017; Accepted February 23, 2017; Published April 30, 2017

** Short Paper*

** Review Paper: This paper reviews the recent progress possibly including previous works in a particular research topic, and has been accepted by the editorial board through the regular reviewing process.*

***Abstract*:** In this paper, a smart optical fingerprint sensor technology that is robust against faked fingerprints. A new lens and prism accurately detect fingerprint ridges and valleys that are needed to express a fingerprint's intrinsic characteristics well. The proposed technology includes light path configuration and an optical fingerprint sensor that can effectively identify faked fingerprint features. Results of simulation show the smart optical fingerprint sensor classifies the characteristics of faked fingerprints made from silicone, gelatin, paper, and rubber, and show that the proposed technology has superior detection performance with faked fingerprints, compared to the existing infrared discrimination method.

***Keywords*:**

1. Introduction

Fingerprint recognition technology is one of the most widely deployed and developed biometrics technologies. The first step in performing fingerprint recognition is to acquire an image. In conventional fingerprint image acquisition, ink is applied to the fingers and the fingers pressed onto paper. Currently, a fingerprint image is acquired directly from a sensor device, such as an optical fingerprint sensor, a semiconductor fingerprint sensor, or an ultrasonic fingerprint sensor. Although the various fingerprint sensor technologies are convenient, there is a problem in that fingerprint quality changes depending on the environment, and is inconsistent. Causes of the problem include the difference between a dry finger and a wet finger, finger surface damage, contact failure between finger and sensor, and sensitivity differences depending on the external light source and moisture [1, 2]. This paper addresses the problems of the most widely used optical sensors, and proposes smart optical sensor technology that is robust against faked fingerprints. The optical system consists of a prism, a lens, and a complementary metal-oxide semiconductor (CMOS) sensor [3].

In the image acquisition method, a fingerprint is pressed on a prism, and the CMOS acquires the region where the light emitted from the light source is diffused and absorbed by the prism. Fig. 1 shows the basic structure of light source, prism, and lens.

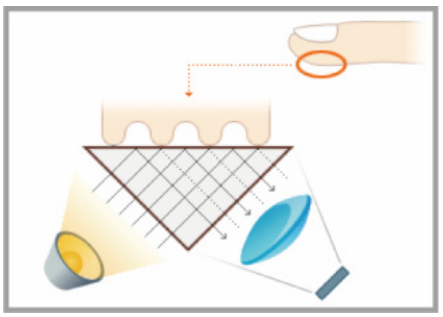


Fig. 1. The basic structure of an optical system.

The optical sensor has an advantage in that the authentication rate is higher than other sensors, because it provides a good-quality image and can collect fingerprint information from a wide area. However, when the distance between the prism and CMOS sensor is close, it is difficult to downsize the image because the optical distortion is large in the obtained image. It has another disadvantage in that it is vulnerable to faked fingerprints from using the photography method. We proposes an optical design technique that can effectively defend against and detect faked fingerprints. Since the proposed technology cannot

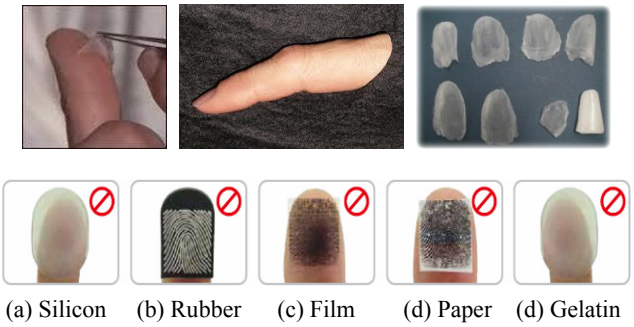


Fig. 2. Fake fingerprint samples.

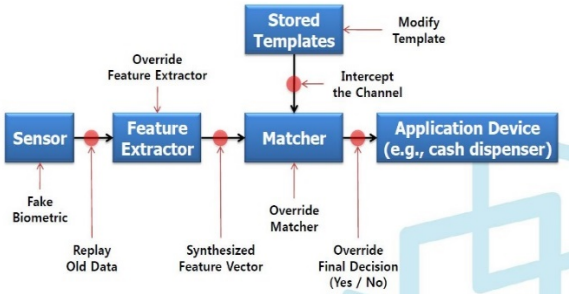


Fig. 3. Eight points of weakness for attacks against a biological system.

contain moisture due to the characteristics of faked fingerprints, an optical design technique analyzes the properties of moisture. Section 2 of this paper describes the definition of faked fingerprints and the characteristics of the light sources used. Section 3 presents an optical design technique that is robust to moisture characteristics. Simulation and data analysis are discussed in Section 4, and then the paper is concluded.

2. Definition of Fake Fingerprint and Characteristics of Light Source

2.1 Definition of Fake Fingerprint

A fake fingerprint attack refers to an unauthorized user creating a false fingerprint and illegally using it to engage a biometric system. Fake fingerprints can be made of various materials, as shown in Fig. 2, with paper, rubber, silicone, and gelatin the most commonly used materials [4, 5].

The reason for the increase in fake fingerprint attacks is that the user is directly vulnerable through the eight weak points of the biosecurity systems shown in Fig. 3, where the sensor serves as a doorway to the system. In a general door lock system, by the same logic, if the door is strong, accidents can be reduced accordingly [6, 7].

2.2 The Characteristics of the Light Source

We uses a blue light source of 400~450 nm to optimize the optical design. For this wavelength, the blue in red, green, and blue is high, and the green and red are treated as

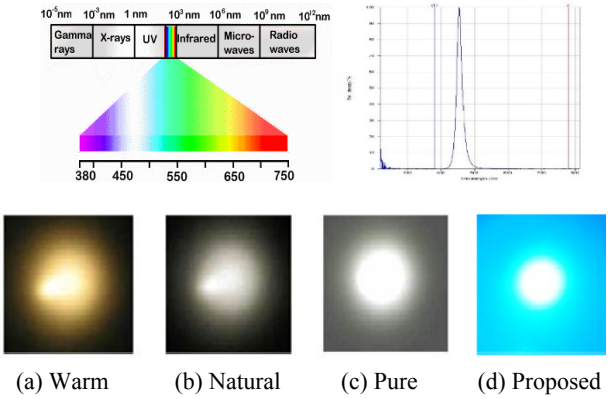


Fig. 4. Light source distribution depending on light temperature.

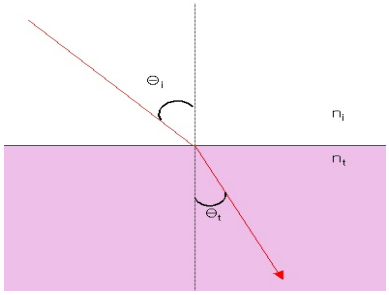


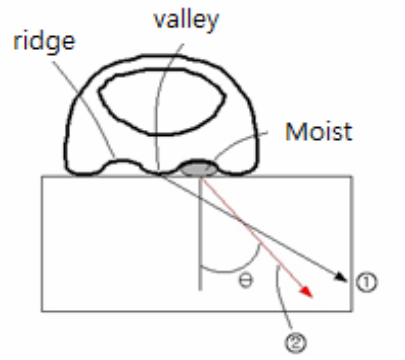
Fig. 5. The refraction of the prism.

noise, so that only the blue band is advantageous when designing the optical path. Also, due to the characteristics of the blue wavelengths, the amount of light absorbed and reflected by the skin has a distinct difference, comparing human and non-human fingerprints. Fig. 4 shows the temperature of the light by wavelength.

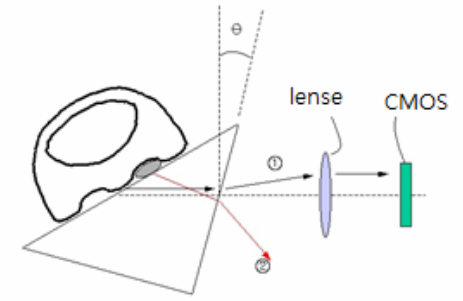
3. Optical Design Technology Robust to Moisture Characteristics

What is important in optical design is the magnification of the size of the image sensor and the fingerprint input window that you want to use. The lens can be composed of a plurality of lenses to increase the resolution, but the minimum number is set to show the required performance. The key point of an optical design that is robust to the proposed moisture characteristics is the prism, which enables fingerprint image acquisition even when water is on the hand. As shown in Fig. 5, incident light θ_i is refracted by θ_t at the interface of the medium. Therefore, you cannot see the image above the border at angles greater than θ_t. For example, if n_i is water and n_t is the prism, you cannot see the water image in an area more than θ_t.

In Fig. 6, when a finger is placed on the prism, the valley that becomes the fingerprint comes out through the □ path, and the moisture like water between the ridge comes out as the ▪ path.



(a) Fingerprint on prism



(b) Angle change of the prism

Fig. 6. The capture method.

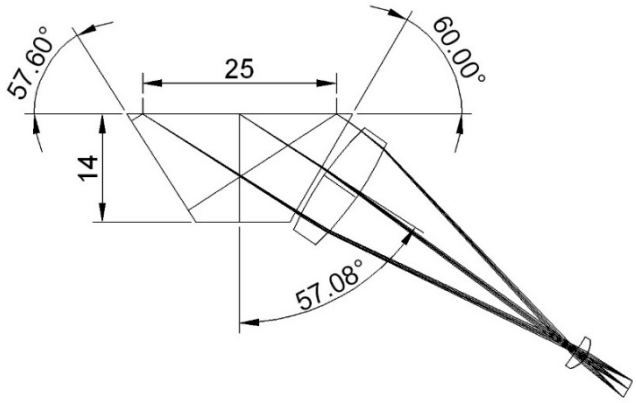


Fig. 7. Prism angle.

Therefore, if you hold the prism angle and the optical axis of the lens, as shown in Fig. 7, you can obtain pure images, even if you have water or sweat on the hands. The material of the prism is SF4. Since the refractive index is 1.755, by $n_i : \sin\theta_i = n_i : \sin\theta_2$, $n_i = 1.33$ (water), $\theta_2 = \sin^{-1}\frac{n_i}{n_2} = 49.29°$.

Therefore, you cannot see the water if refractive index θ_2 is more than 50°. So the prism is designed so that the angle of incidence is more than 50° in SF4. Of course, prism angle θ_2 does not need to be 60°. However, when the angle of refraction increases, the water becomes indistinguishable, and when the angle becomes smaller, the ratio of the rectangle increases. Therefore, as shown in Fig. 7, the background angle of the prism fingerprint

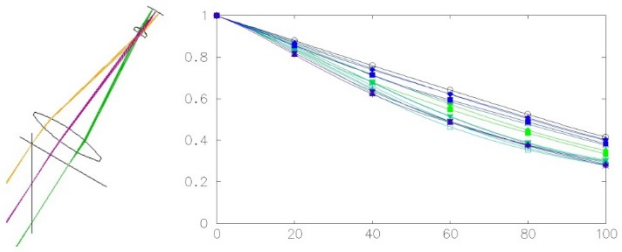


Fig. 8. MTF graph for the light path design.

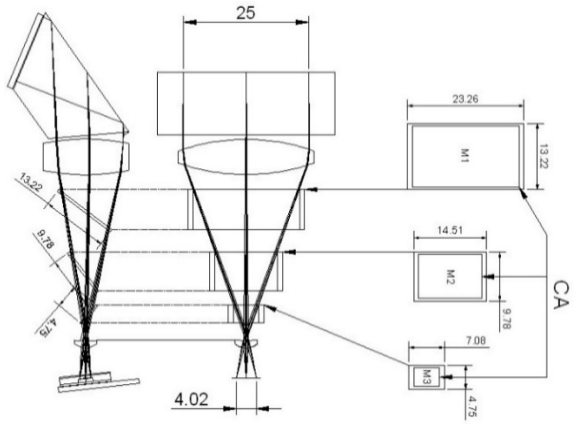


Fig. 9. The drawing of the proposed optical design result.

connection surface is fixed at 57.6°.

An MTF(Modulation Transfer Function) graph for the light path design of Fig. 7 is the same as Fig. 8. At this time, the modulation is designed to satisfy 100 lines from 30%.

When the prism fingerprint input area is square, the image becomes a rectangle. This is because the virtual image generated inside the prism has a rectangular ratio. Fig. 9 shows the clear area (CA), which is designed as the clean area required for image formation. A clear area(CA) is an area where a mirror is not contaminated or the path is blocked by the mechanism. At this time, the lens is designed so that the lens is not contaminated or the path blocked by the mechanism.

4. Simulation

The simulation for performance evaluation of the proposed optical design was as follows. First, various types of fake fingerprints were prepared for use in the test. By using the prepared samples and an actual fingerprint, image acquisition was performed with the proposed sensor and another optical sensor. The experiment consisted of 200 real fingerprints and 200 fake fingerprints. Fake fingerprints were made by using silicone, rubber, gelatin, film, and paper, and a fake fingerprint database was created, as shown in Fig. 10. This database is composed of images at 260x300 and an accumulation of 24-bit fingerprint images.

Fig. 11 is an image of test results by material. As seen

(1) Green (healthy skin prints), (2) Black (paper), (3) Black (film), (4) Bright Ocean (rubber), (5) Dark Blue (silicon), and (6) Ocean (gelatin)

Fig. 10. The manufactured fake fingerprint color light database.

(1) Real Fingerprint

(2) Silicon Fake Fingerprint

(3) Gelatin Fake Fingerprint

(4) Rubber Fake Fingerprint

(5) Film Fake Fingerprint

(6) Paper Fake Fingerprint

Fig. 11. Test result images by material.

Table 1. The comparison results (200set).

Type (ingredient)	Fake detection (Detect/Try time)	Detection rate
Silicon(body double)	200/200	100%
Film (ohp)	200/200	100%
Paper(cellulose)	200/200	100%
Rubber(latex)	187/200	93.5%
Gelatin(granular)	192/200	96.0%
Total average detection rate		97.9%

in the figure, it can be confirmed that the image including the brightness difference of light for each material shows a different result.

As shown in Table 1, 200 fingerprints were found to be detect for the silicon type, film type, Paper type fake fingerprints. In the case of the fingerprints, the fingerprints were 97.9% defective. However, there are no certified samples, so performance differences may occur depending on the sample to be produced.

5. Conclusion

The smart optical fingerprint sensor proposed in this paper can enhance the detected characteristics of real fingerprints by including moisture. With faked fingerprint materials, the distribution of water is weak, or there are many differences in reflectance and absorption rate compared to real human fingerprints from using water or oil from the outside. Future work includes faking fingerprints from various samples, more easily learning the characteristics of each material, and studying a stronger faked fingerprint sensor.

Acknowledgement

This research was supported by an Advanced Technology Center (ATC) grant funded by the Korean government (Ministry of Trade, Industry and Energy) (No. 10051484).

References

[1] Sarat C. Sousedik and C. Busch, "Presentation attack detection methods for fingerprint recognition systems: A survey", IET Biometrics, vol.2, no.1, pp.1-15, 2014. Article (CrossRef Link)

[2] Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: "Handbook of Fingerprint Recognition", Springer-Verlag, New York, 2003. Article (CrossRef Link)

[3] S. -J. Kim, K. -H. Lee, S. -W. Han and E. Yoon, "A CMOS Fingerprint System-on-a-Chip With Adaptable Pixel Networks and Column-Parallel Processors for Image Enhancement and Recognition", Journal of Solid-state Circuit, vol. 43, no. 11, (2008), pp. 2558-2567, 2008. Article (CrossRef Link)

[4] S. S Kulkarni and H. Y Patil. Article: Survey on Fingerprint Spoofing, Detection Techniques and Databases. IJCA Proceedings on National Conference on Advances in Computing NCAC 2015(7):30-33, December 2015. Article (CrossRef Link)

[5] A. Al-Ajlan, "Survey on fingerprint liveness detection", In International Workshop on Biometrics and Forensics, pp. 1-5, 2013. Article (CrossRef Link)

[6] M. Tico, P. Kuosmanen, "A multiresolution method for singular points detection in fingerprint images", Proceedings of IEEE International Symposium on Circuits and Systems, vol. 4, p.183-186, 1999. Article (CrossRef Link)

[7] J. Zhou, F.L Chen, J.W. Gu, "A novel algorithm for detecting singular points from fingerprint image", IEEE Transactions on Pattern Analysis and Machine Intelligence, 31(7), p.1239-1250, 2009. Article (CrossRef Link)

[8] J. Chang and K. Fan, "A new model for fingerprint

classification by ridge distribution sequences", Pattern Recognition, 35:1209–1223, 2002. Article (CrossRef Link)

[9] S Yadav, M Mathuria, "Fingerprint Recognition based on Minutiae Information", International Journal of Computer Applications, vol.120, 2015. Article (CrossRef Link)

Young-Hyun Baek is Chief Technology Officer (CTO) of the Union Community R&D Center. He received his BSc and MSc in Electronic Engineering from Wonkwang University, Korea, in 2002 and 2004, respectively, and a PhD in Electronic Engineering from the University of Wonkwang in 2007. Dr. Baek was an Assistant Professor in the Division of Electronic & Control Engineering at Wonkwang University. He has served as, or is currently serving as, a reviewer and on the Technical Program Committee for many important journals, conferences, symposiums, and workshops in biometrics, image processing, and optical device areas. His research interests include fingerprint sensors, biometrics security systems, and fake-finger technology. He is a member of the IEEE, IEEK, TTA, and KISA Technical pool.