

A study on slim optical fingerprint sensor for fake fingerprint detection on mobile environment

Young-Hyun Baek*, Byunggeun Kim, Seok-han Kim and Jong-woo Ahn

Research Institute, UNION COMMUNITY Co., Ltd. Seoul, South Korea

*Email: neural76@unioncomm.co.kr

Abstract. We propose a slim optical fingerprint sensor for fake fingerprint detection on mobile environment. The sensor proposed in this paper is compact size and slim thickness. Also, it can be used by only the power of smart phone without battery or external power. This sensor has a new lens design and optical path to minimize distortion. This sensor shows detailed images of ridges and valleys characteristic of fingerprints and has a characteristic of being resistant to moisture. The proposed sensor can detect various kinds of fake fingerprint (Paper, rubber, silicone, etc.). Simulations show that the slim optical fingerprint sensor has an effective performance on the results of the fake fingerprint detection rate.

1. Introduction

In the recent years, biometric technologies have gained increasing attention in the various field. The fingerprint recognition is a well-known biometric technology. There various techniques have been used in the optical, capacitive, radio frequency, ultrasound, and thermal methods [1-5]. Among them, the most common sensors are optical and capacitive fingerprint method. Optical fingerprint sensor is to offer greater durability and reliability, providing lower cost and longer life. Capacitive fingerprint sensor is to offer lower durability and providing higher cost.

In this paper, we propose a slim optical fingerprint sensor for mobile environment. This paper is organized as follows. In section 2, we proposed the slim optical structure and design. section 3 presents the simulations results. And section 4 is conclusions.

2. Proposed slim optical fingerprint sensor design

2.1. Optical fingerprint sensor

Figure 1 shows the Optical fingerprint sensor structure. The light is reflected at the fingerprint (as they pass through(valleys) or reflect off objects(ridges)). The sensor is to offer greater durability and reliability, providing lower cost and longer life, but they cannot be miniaturized due to optical characteristic (the distance between the prism and the image sensor) [3-6].

2.2. Fingerprint recognition system

This section provides a basic introduction to fingerprint recognition systems and their main parts, including a brief description of the most widely used techniques and algorithms. Figure 2 shows main modules of a fingerprint recognition system. Data capture(fingerprint sensing), in which the fingerprint of an individual is acquired by a fingerprint scanner to produce a raw digital representation. Next



preprocessing, in which the input fingerprint is enhanced and adapted to simplify the task of feature extraction. Fingerprint feature extraction, in which the fingerprint is further processed to generate discriminative properties, also called feature vectors. Final step matching, in which the feature vector of the input fingerprint is compared against one or more existing templates. The templates of approved users of the biometric system, also called clients, are usually stored in a database. Clients can claim an identity and their fingerprints can be checked against stored fingerprints.

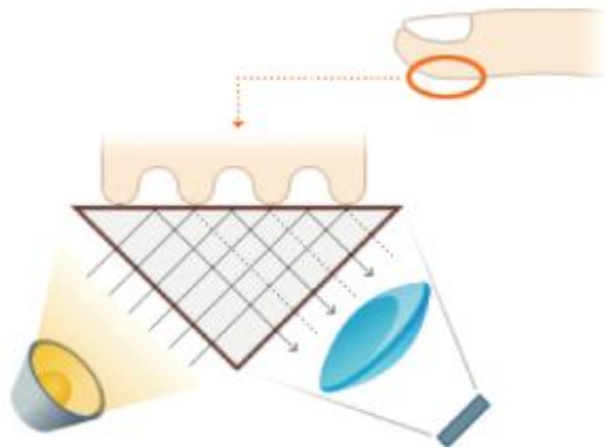


Figure 1. Optical capture method.

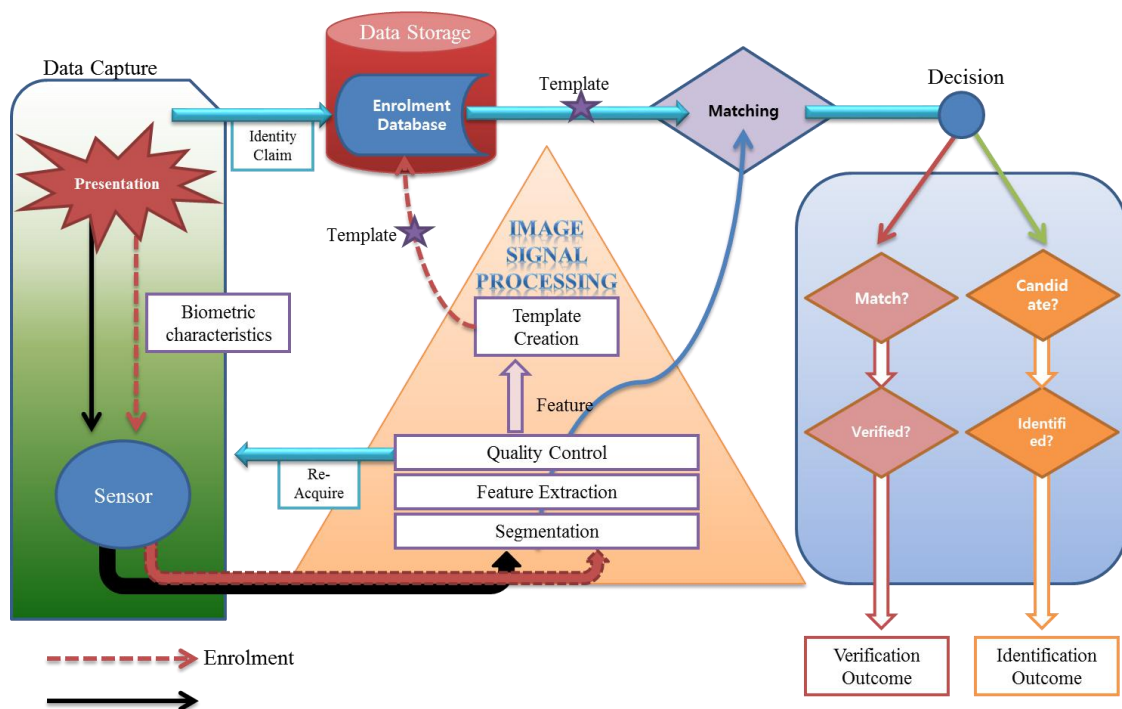


Figure 2. Main modules of fingerprint recognition system.

2.3. Definition of fake fingerprint

The fake fingerprint generally refers to a fake access by an illegal user into fingerprint biometric system by using a fake fingerprint reproducing that one of an unauthorized user. These artifacts are made from various materials like silicon, clay, rubber, paper, etc (figure 3). The whole process of creation of fake fingerprints can be done with or without co-operation and get easy access to highly authenticated society. We can countermeasure against such attacks using liveness check.

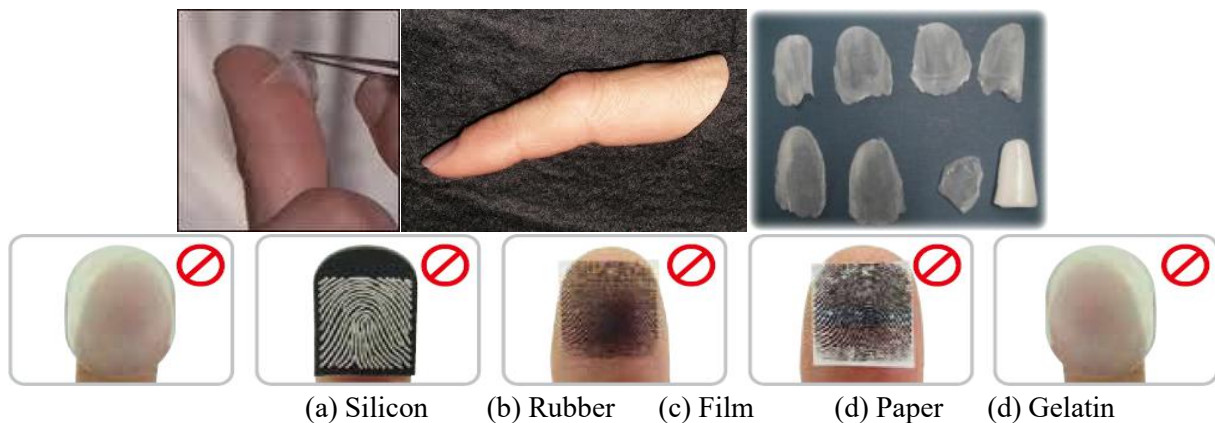


Figure 3. A kind of fake fingerprint.

2.4. Proposal slim optical lens design

The figure 4 is the slim optical design output applying the spherical lens to satisfy the standard FBI PIV Spec. In order to satisfy the PIV must be able to decompose the line of 0.05mm prism fingerprint surface. 0.05mm line of the prism surface is reduced through the image formation lens system to the image sensor there is in early value to be dismantled should enter the one line to a pixel of the image sensor. But consider that the line of machining tolerances and tolerances enclosures, an assembler 1line differential is 1 pixel is put in danger. It is most desirable to enter the 1 line to 2 pixel. If 1 line is designed to fall into the 3 pixel image. This is because the larger the angle of incidence to the micro-lens over each pixel in the image CMOS sensor. The prism surface is at least 0.05mm to be suitable for the more than 2.8 μ m, 5.6 μ m or less, when incident on the image sensor through the lens system. At this time, the ratio of the line is between 0.112 times 0.056 times. To enter the 1 line 21 pixel image differs, so the vertical direction is 25mm cis shall be imaged by 2.8mm. Figure 4 is applying a spherical lens design.

The prism is set to start because it should be separated so that they are at the wet. In addition, the surface of the fingerprint image without being affected by the external light source should be uniform.

Ability to separate water and silicon in all areas of active area:

- Minimum angle of 59.9 ° to distinguish water from silicon
- The angle of the active area is 60.2 ° (figure 5), which is greater than 59.9 °.

2.5. Slim fingerprint internal configuration

Figure 6 shows the configuration of the proposed slim fingerprint sensor.

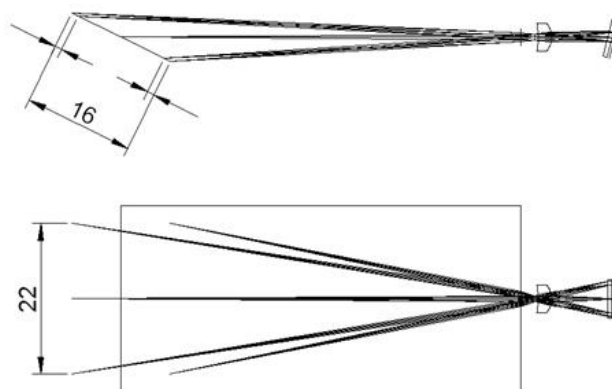


Figure 4. New spherical lens design (Active area in prism : 22 *16mm).

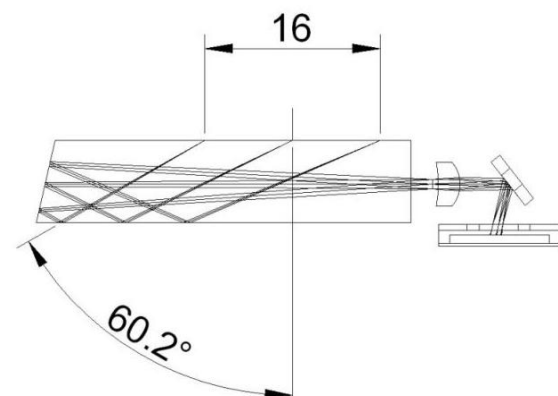


Figure 5. The prism design in slim moisture fingerprints.

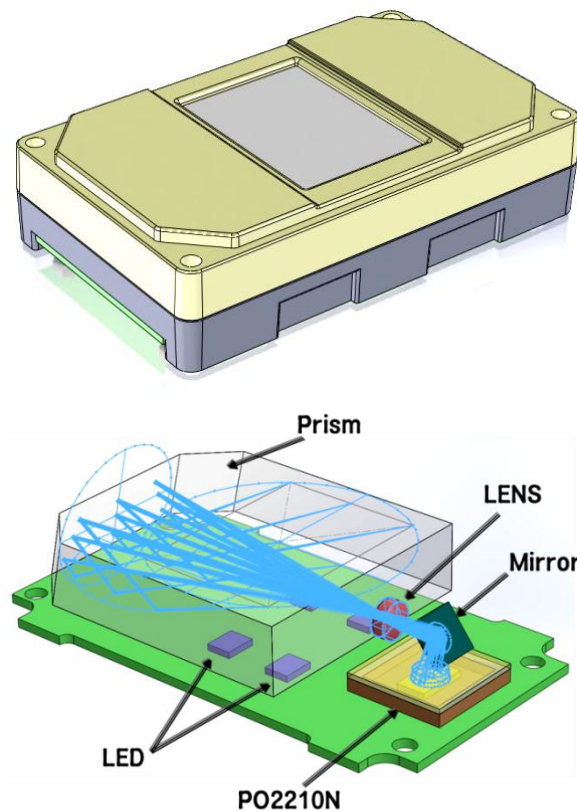


Figure 6. The device design in slim optical fingerprints.

3. Simulations

This section focuses on evaluating the proposed sensor. We start by describing the test optical simulation data. Then, the experiment results of the proposed slim optical sensor is presented for fake fingerprint detection rate.

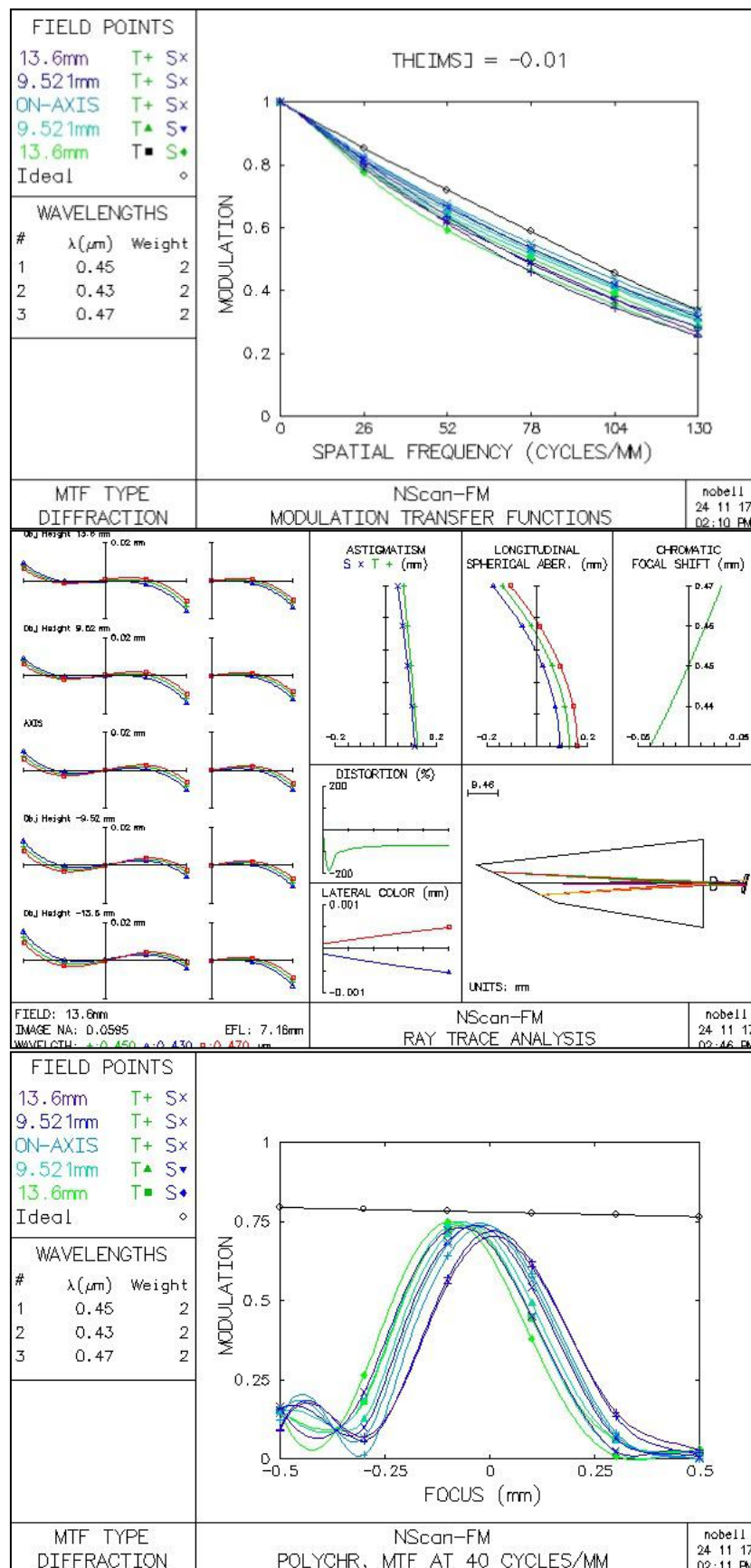
Table 1 shows the comparison results when the result shows the high performance in all fake feature type. As can be seen in table 1, the fake fingerprint detection a 97.25% accuracy in the make fake fingerprint 100 set.

Table 1. The comparison results (100set).

	Fake Detection(detect/try)	Detection rate(%)
Real Finger	0/100	Pass
Paper	100/100	100%
Rubber	98/100	98%
Film	100/100	100%
Silicon	91/100	91%

4. Conclusion

The performance of the slim optical sensor with mobile environment is shown in figure 7. As a result, we succeeded in overcoming the limitation of optical design and implementing optical type fingerprint sensor with slim structure. The proposed system tested on the real finger and fake fingers. And The table 1 results show that the fake fingerprint detection accuracy has been 97.25% which proves that our system has a performance. In future works, we will need to variety of material fake fingerprint testing.



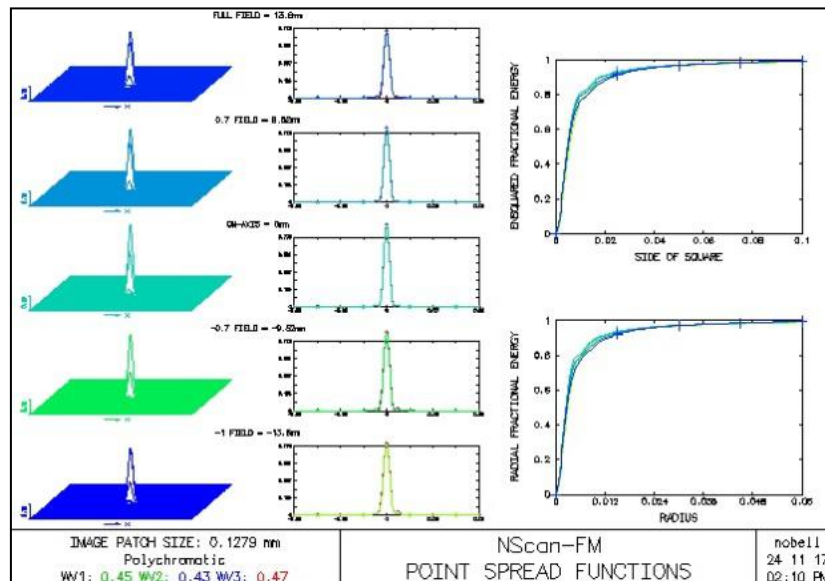


Figure 7. The Optical system design / Optical system simulation result.

Acknowledgments

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

References

- [1] A. Al-Ajlan, "Survey on fingerprint liveness detection", In International Workshop on Biometrics and Forensics, pp 1-5, 2013
- [2] D., Maio, D., Jain, A.K., Prabhakar, S.: "Handbook of Fingerprint Recognition", Springer-Verlag, New York, 2003
- [3] Qinzhi Zhanga, Hong Yan, "Fingerprint classification based on extraction and analysis of singularities and pseudoridges", Pattern Recognition, vol.37, pp 2233-43, 2004
- [4] J. W. Lee, D. J. Min, J. Y. Kim and W. C. Kim, "A 600-dpi Capacitive Fingerprint Sensor Chip and Image-Synthesis Technique", IEEE J. of Solid-state circuits, vol. 34, no. 4, (1999) April, pp 469-75
- [5] S. -M. Jung, J. -M. Nam, D. -H. Yang and M. K. Lee, "A CMOS Integrated Capacitive Fingerprint Sensor with 32-bit RISC Microcontroller", IEEE Journal of Solid-state Circuit, vol. 40, no. 8, (2005), pp 1745-50
- [6] 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 2558-67, 2008