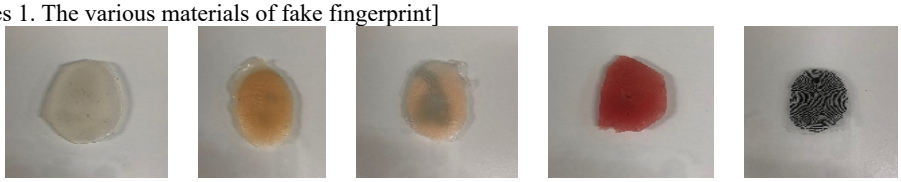
A Novel Fake Fingerprint Detection Algorithm Using A Triple-Wavelengths Computation Method Based On Heart Rate Variability (HRV)

UnionCommunity Research Center, 127, Beobwon-ro, Songpa-Gu, 12F, Daemyung Valeon Bldg., Seoul, 05836, Republic of Korea;
*Young-Hyun Baek, Seock-Han Kim, Dong-Ho Lee, Byunggeun Kim, Sun-Dong Kim
e-mail: neural76@unioncomm.co.kr

Abstract. Biometric systems are an emerging technology that enables the authentication of an individual based on physiological characteristics including face, fingerprint, iris, hand geometry, palm, or behavioral characteristics including voice, gait, keystroke dynamic and handwriting signature, etc. There number attacks and there remedial solutions discussed in the literature on different modules of biometrics system and communication links among them. But still the researchers are not able to secure every module of a biometric system against these attacks[1~3]. Recently, research has shown that it is possible to spoof a variety of fingerprint scanners using some simple techniques with molds made from paper, rubber, silicon or gelatin materials. In this paper, we propose a new algorithm that detect fake fingerprints by acquiring the properties of three inherent wavelengths from the heart rate variability using the red, green and infrared LEDs, and performing composite computation. To accomplish this goal, we begin with a heart rate variability factors and a waveform acquisition device design method to construct these components with data signal processing. The next step measures the peak change in heart rate. The peak of the blood flow changes according to the heart rate variability. It is analyzed using red, green, and infrared LED wavelengths. At this time, the acquired data is not a heart rate of the owner. It is the acquired data of absorbed & reflected wavelength in the real human skin and the blood flow changes. In case of real fingerprints, the average IR LED data is 38,823 PPG signal, red led data 40,996 PPG signal, green led data 5,570 PPG signal. Fake fingerprints show a big difference for each material. The silicon material fake fingerprints indicate IR LED 8,146 PPG signal, red led 10,186 PPG signal, green led 1,289 PPG signal. The gelatin material fake fingerprints are IR LED 16,851 PPG signal, red led 13,726 PPG signal, green led 2,690 PPG signal. The film material fake fingerprints indicate IR LED 7,566 PPG signal, red led 9,523 PPG signal, green led 908 PPG signal. Then, the obtained data is computed in units of 1 second. And performs a task of converting analog data into digital data. The next step is to compare the wavelengths of the enrolled real fingerprint with that of the detected fake fingerprint. Finally, compare the properties difference with the learned fake fingerprint material wavelengths. When the learning error rate threshold value is exceeded, the computation is completed. Simulations show that the proposal algoritm has an effective performance on the results of the fake fingerprint detection rate.

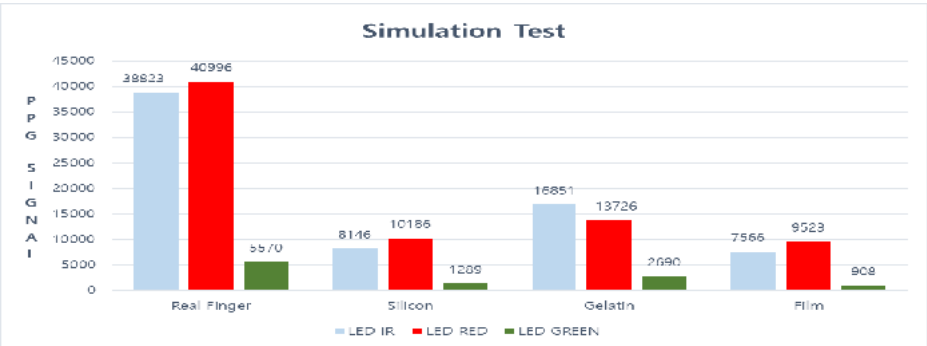
Key words: heart rate variability (HRV), fake fingerprint, biometric, spoof recognition, signal processing, pattern analysis

[Test References 1. The various materials of fake fingerprint]



Slicon 1 Slicon 2 Gelratin 1 Gelratin 2 Filim

[Test References 2. Simulation test result]



[References]

[1] Bozhac Tan and Stephanie Schuckers, “Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise”, Pattern Recognition 2010, vol. 43, pp. 2845-2857.

[2] Young-Hyun Baek, Byunggeun Kim and Seock-Han Kim, “ Fake Fingerprint Detection Biometric System Using Neural Network Algorithm”, 2018, 7th International Conference on Knowledge Discovery ICNIT 2018, pp 17.

[3] S. S Kulkarni and H. Y Patil, “Survey on Fingerprint Spoofing, Detection Techniques and Databases”, IJCA Proceedings on National Conference on Advances in Computing, 2015, pp. 30-33.