International Journal of Smart Home
Vol. 13, No. 2 (2019), pp.17-24
http://dx.doi.org/10.21742/ijsh.2019.13.2.03

Implement of Complex Personal Authentication System applying Biometrics Pattern Algorithm

Dai Hwan Lim[1], Ki Hun Nam[2], Jin Young Park[3]

Dept. Computer Engineering Seokyeong Univ, GoQba technology corp,
[1]jpeace1226@gamil.com, [2]namkh@skuniv.ac.kr, [3]2goqba@goqba.com

Abstract

We propose a complex personal authentication system that enhances user convenience and security to meet the increasing demand for authentication in IOT, wearable devices, mobile services and non-face environments. This system is a complex personal authentication system that can perform authentication processing in real time by combining a biometric authentication method (face, line of sight, fingerprint) and PIN authentication method, which are highly discriminating and difficult to forge and falsify. We also introduced an artificial intelligence processor (Machine Learning) to learn biometric information of the user and increase the accuracy of authentication. This has resulted in a complex personal authentication system that is enhanced against a single authentication algorithm. In future, we intend to develop a more robust and convenient personal authentication system by incorporating deep learning based intelligent system into this system.

Keywords: *Biometrics, Complex authentication, IoT, PIN, Intelligence processor.*

1. Introduction

In addition to the IOT environment, there is an increasing demand for security services for mobile devices. Biometric authentication algorithms are simpler and more secure than existing authentication systems, but cannot be modified when authentication data is leaked. Therefore, simple mobile devices require strict security authentication procedures and cause inconvenience to users. We have implemented and developed an authentication system that guarantees convenience and versatility and enhanced security through complex biometric authentication technology[1][2][3][4].

2. Related Research

2.1 Fingerprint Recognition

One of the biometrics technologies that is cheaper and faster than other biometric devices is to recognize users through fingerprints that are characteristic of each individual[5].

2.2 Iris Recognition

By analyzing the shape and color of the iris and the morphology of the retinal capillaries, it is possible to recognize people by using the iris information of the eyes with different shapes

Article history:
Received （January 14, 2019), Review Result (June 21, 2019), Accepted (July 22, 2019)

Print ISSN: 1975-4094, eISSN: 2383-725x IJSH

for each person. Even if wearing glasses or lenses, accurate recognition is possible. The iris authentication system is faster and more accurate than fingerprint authentication, but it requires additional equipment and is expensive[6].

2.3 Speech Recognition

Speech recognition is a technique that converts the acoustic signals obtained through the sound sensor into words or sentences, and extracts the characteristics of the speech signals and compares them with the speech model database. Currently, various services such as voice recognition personal assistant and artificial intelligent speaker are being launched using such technology[7].

3. Suggested System

Biometric authentication is a universal authentication method for simple authentication because it is highly discriminative and difficult to counterfeit and modulate. However, authentication technology faces a new problem that needs to meet market competitiveness such as versatility, convenience, security and so on. In this paper, we designed and developed a simple authentication system that combines biometric (Face, Fingerprint, Eye) authentication and PIN authentication based on these requirements. First, the face recognition algorithm is robust against illumination changes and can be processed at high speed using LBP Image pyramid and Adaboost algorithm. The structure is shown in Fig 1.

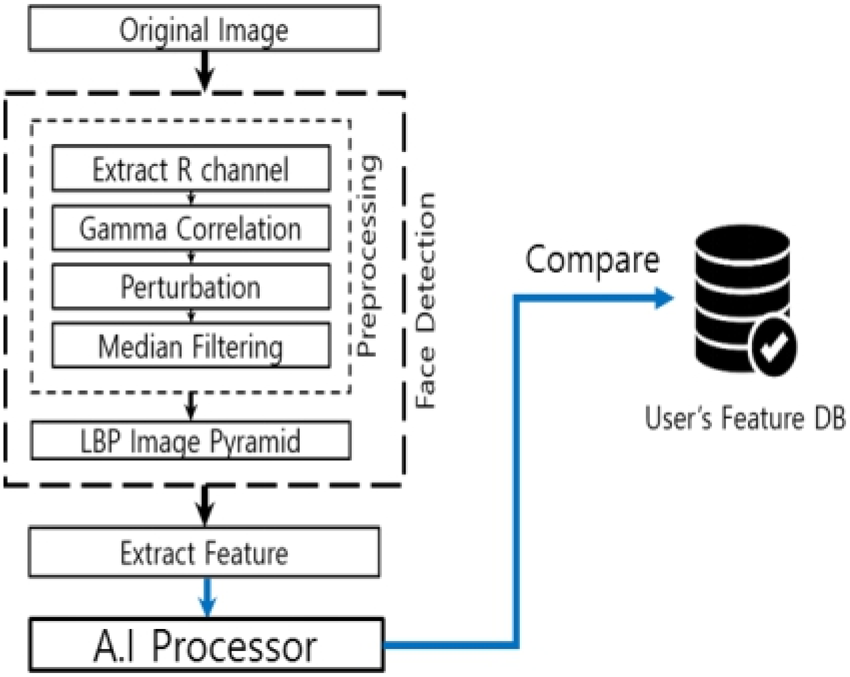


Figure 1. Face Recognition Algorithm Block Diagram

Images that have undergone a preprocessing process for image enhancement are subjected to face scanning through the LBP Image pyramid. LBP value is image processing which is strong against illumination change unlike gray value. It is composed of 8 neighbor pixels based on the center pixel (M) and expressed by 8 bits. Fig 2 shows the result of Face Recognition designed in this paper. The test database was evaluated using a total of 84 database. In the database constructed for the Face Recognition test, images of backlight, face pose inclination, low illumination, occlusion were not detected in the RGB channel.

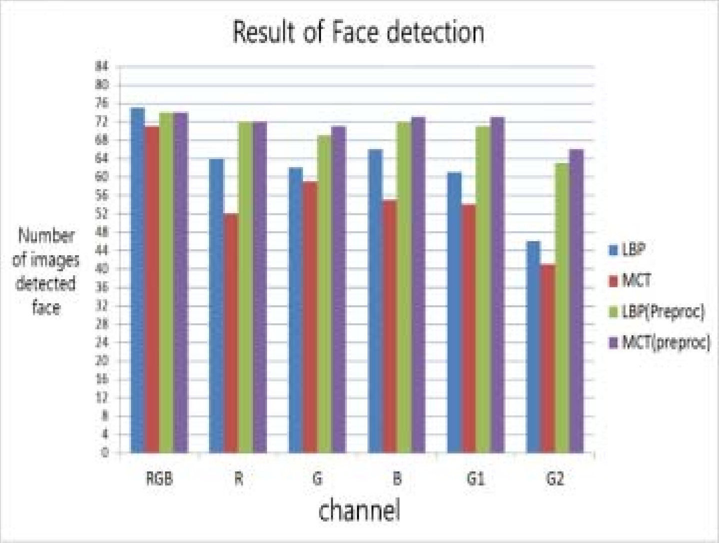


Figure 2. Result of Face Detection.

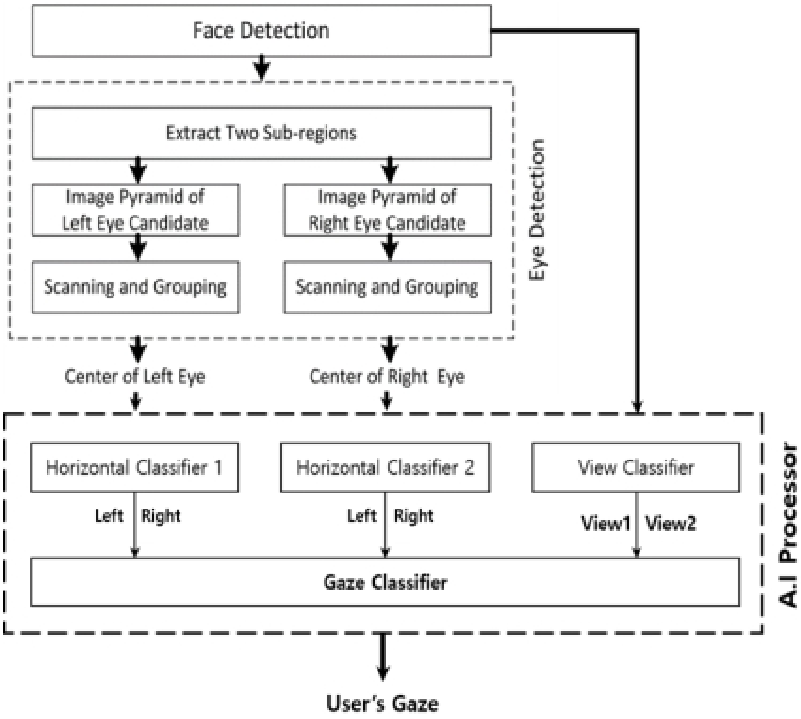


Figure 3. Eye Recognition Algorithm Block Diagram

In this study, we constructed LBP + Adaboost for face detection, robust against illumination changes, and able to process at high speed. For learning data, 400,000 positive images and 600,000 negative images were used. The learning took about one day. Cascade is composed of four stages, and the feature number of each stage is [26, 60, 144, 360]. FDDB was used for the evaluation, and the performance was superior to the previous studies.

The Eye Detection algorithm is a method of authenticating the position and gaze of the learned user's eyes by comparing with the current user. This algorithm uses a normal camera, not expensive iris camera, it is possible to prevent the risk of hacking, because the eye is detected in real time. The structure is shown in Fig 3.

Finally, the fingerprint recognition algorithm is developed as shown in Fig 4 In particular, fingerprint recognition developed in this paper uses OTP (One Time Password) which is one of the user authentication methods that use one-time passwords randomly generated for effective authentication, to overcome various vulnerabilities. First, the camera fingerprint recognition and the fingerprint OTP S / W are used to register several fingerprints. Next, when the authentication is requested, random fingerprint information is requested and then finally the fingerprint ID requested is confirmed (security of the existing method)[8].

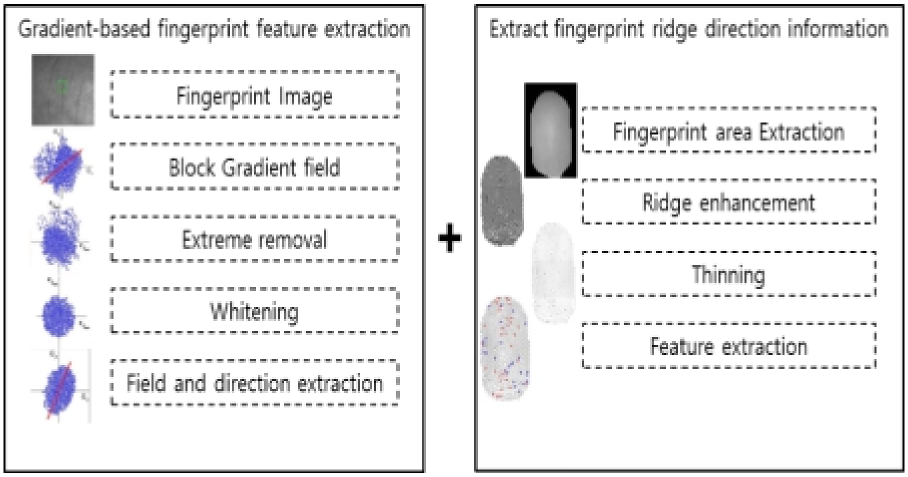

Gradient-based fingerprint feature extraction
Fingerprint Image
Block Gradient field
Extreme removal
Whitening
Field and direction extraction
+
Extract fingerprint ridge direction information
Fingerprint area Extraction
Ridge enhancement
Thinning
Feature extraction

Figure. 4 Fingerprint recognition method

The algorithm used for fingerprint recognition is based on gradient-based fingerprint recognition algorithm. The fingerprint area and features are extracted. The main process for identifying the required fingerprint ID is as shown in Fig.5. At this time, when the registration fingerprint is inconsistent, the second random registration fingerprint is requested. If the registration fingerprint is inconsistent more than 3 times, the automatic locking function is performed. When the registered fingerprint comparison is matched, the user is authenticated and the authentication is succeeded.

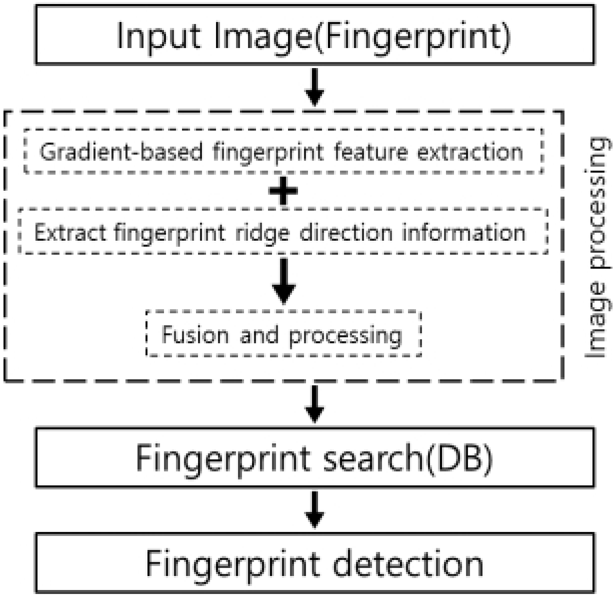
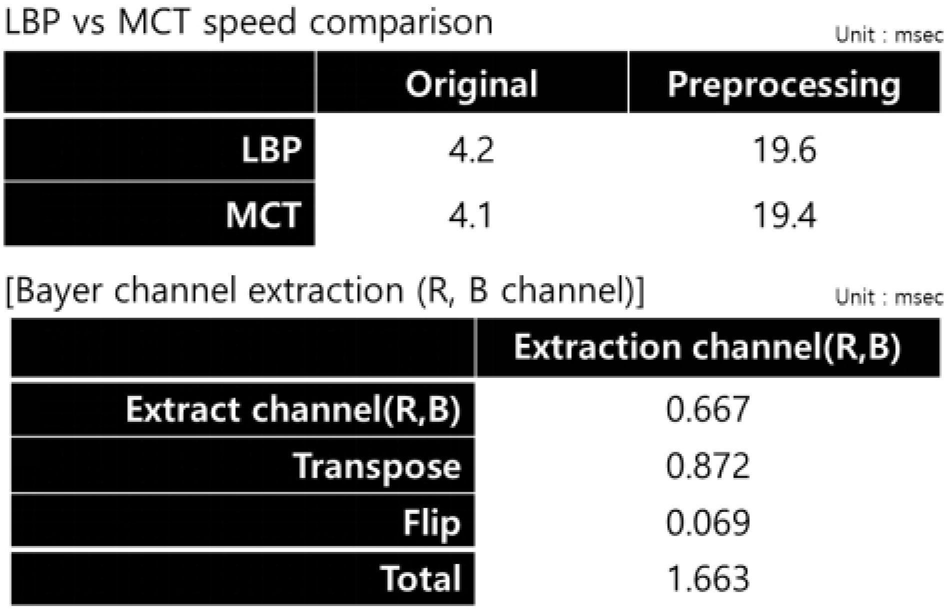


Figure 5. Fingerprint Recognition Core Flower



LBP vs MCT speed comparison

Unit : msec

	Original	Preprocessing
LBP	4.2	19.6
MCT	4.1	19.4

[Bayer channel extraction (R, B channel)]

Unit : msec

	Extraction channel(R,B)
Extract channel(R,B)	0.667
Transpose	0.872
Flip	0.069
Total	1.663

Figure 6. Result of Face Detection

In order to effectively use the above algorithm, an intelligent algorithm is applied. This intelligent algorithm learns the user's biometric information, enhances the accuracy of authentication and enhances security. In addition, biometrics authentication methods and commonly used pin authentication methods are applied. The world's first complex personal authentication algorithm has been developed that can process 16 combinations in real time.

Performance evaluation showed good results in terms of face detection processing speed, and eye detection performance was good regardless of channel.

4. Conclusion and Future Work

In the algorithm developed in this paper, the performance evaluation was performed on the face detection processing speed part and the performance part of the eye detection part. Face detection measurement results are shown in Figure 6. The evaluation environment includes an Intel-based Core ™ i7 CPU, Memory 8.0GB, 1980x1200 Raw Data based Windows OS.

As shown in the measurement results, it was judged to have excellent results in terms of speed. In the case of eye detection, the test was performed on the RGB / R / G / B / G1 / G2 channels and resulted in good performance on all channels as shown in Fig.7.

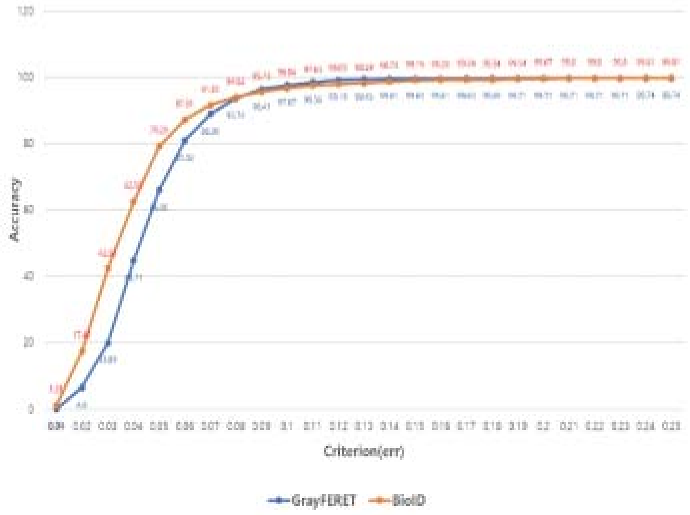


Figure 7. Result of Eye Detection

IOT, wearable device, mobile service and non-face authentication market growth, biometric market size is expected to expand further and certification demand will increase accordingly. Through this system, biometric authentication in the security market will be an alternative satisfying market competitiveness. In addition, we intend to develop a more robust and convenient authentication system by incorporating a deep learning based intelligent system, which is a recent issue.

References

[1] J. Daugman, “High Confidence Visual Recognition of Persons by a Test of Statistical Independence”, IEEE Trans. On Pattern Analysis and Machine Intelligence, **(1993)**, Vol. No.11. pp. 1148-1161. [DOI: 10.1109/34.244676]

[2] Biometrics Consortium: http://www.biometrics.org.

[3] http://thenextweb.com/google/2011/11/11android-4-0-face-unlock-feature-defeated-using-a-photo-video/.

[4] A. Jain, R. Bolle and S. Pankanti, “Biometrics Personal Identification in Networked”, Society, Kluwer Academic Publisher, **(1999)**

[5] D. Reisfeld, H. Wolfson and Y. Yeshrun, "Detection of Interest Points Using Symmetry", Proceedings of 3rd ICCV, **(1990)**. [DOI: 10.1109/ICCV.1990.139494]

[6] J. Daugman, "How iris recognition works", IEEE Transactions on Circuits and Systems for Video technology, **(2004)**, Vol. 14, No.1. pp. 21-30 [DOI: 10.1016/B978-0-12-374457-9.00025-1]

[7] Thomas F. Quatieri, "Discrete Time Speech Signal Processing Principles and Practice", Prentice Hall, **(2001)**.

[8] Nam-Ho Kim, "Voice-based OTP Generation Techniques for Mobile Banking", Journal of KIIT, Vol.11, No. 5, pp. 113-119, (**2013)**

Authors

Dai Hwan Lim
2006 : PhD degree in Computer Science, Hanyang University.
2006~2009 : SKTeclcom senior researcher
2009~2015 : Adjunct Professor, Computer Engineering, konkuk University.
2008~2015 : LG Electronics Team Leader.
2016~Present : Assistant Professor, Computer Engineering, Seokyeong

Ki Hun Nam
2006 : PhD degree in Computer Science, Seokyeong University.
2006~2009 : Research Engineer, Information Display Research Institute, Hanyang University.
2009~2010 : Principle Researcher, BK21, Chungbuk University.
2011~2016 : Adjunct Professor, Computer Engineering, Seokyeong University.
2017~Present : Assistant Professor, Computer Engineering, Seokyeong University.

Jin young Park
2017~ : Graduate School of Global Entrepreneurship
2017~ : GoQba technology CEO
2017 : Next Planning I