ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 9 (2019) No. 4, pp. 1-11
DOI:10.33168/JSMS.2019.0401

Implementing Complex Personal Authentication System by a Biometrics Pattern Algorithm

Daihwan Lim [1]

[1] Computer Engineering of Seokyeong University, Republic of Korea
jpeace1226@gmail.com

Abstract. This paper proposes a complex personal authentication system using multimodal biometrics for advanced personal authentication in a mobile environment. For this, face recognition, fingerprint recognition and OTP type pattern algorithm were selected. Through the proposed algorithm, an improved security authentication system is realized compared with the single authentication algorithm.

Keywords: Certification, Biometric, Identification, Fingerprint, Speech recognition, Eye recognition.

1. Introduction

Recently, the technology of mobile devices in various fields has been developed along with the Internet environment of the objects, and the demand is rapidly expanding. So, the security issues also occur in the mobile device environment. Accordingly, a variety of biometrics (face, fingerprint, voice, etc.) technologies used in the PC environment are being used as biometrics technology for personal authentication of a user even in a mobile environment. Fingerprint, face recognition, and iris recognition are among the most widely used technologies in mobile (Daugman, 1993).

Fingerprint technology, which is mainly used recently, is being used as a method for personal authentication in door lock systems, office access management, advanced mobile devices such as laptops and premium smart phones. In addition, fingerprint recognition technology of mobile devices is used as a personal authentication method in a field such as PINTECH, which has recently become an issue in the financial field. Such biometrics are simpler and more secure than existing authentication systems that use combinations of numbers (Jain et al., 1999).

However, in recent years, such biometric authentication has been frequently

hacked through various methods. Once such biometric data is leaked, it can be more dangerous because it cannot be modified unlike existing passwords or accredited certificates.

In the case of public certificate, complaints of many users are also increasing due to the required complicated two step password input procedure and a complicated authentication method such as an OTP code input and a public I-pin input are required the complaints of many users are also increasing. As a result, recent users are demanding a new authentication method that satisfies both the aspects of security and user convenience.

Therefore, complex biometric authentication technology is emerging as a more secure and reliable user authentication method than the existing complicated and cumbersome method. In the case of complex biometric authentication, unlike the single authentication method, there is no need for the user to remember or possess passwords using various characters, and since the comparison factor is multiplexed, it provides higher security performance than the single authentication method. In this paper, we have developed a complex biometric authentication algorithm for simple authentication procedure and personal authentication with enhanced security as a complex biometric technology and propose an authentication system that satisfies both security and user convenience.

2. Related Research

2.1. Fingerprint

As one of the biometrics technologies, it is a method of recognizing a user through a fingerprint that characterizes each person. To use fingerprint recognition technology, the user must first register his / her fingerprint in the system. The registered fingerprint is stored together with the registered person's name or other personal information. Then, when the user inputs his / her fingerprint, the system compares the previously registered fingerprint with the previously registered fingerprint and recognizes the user. Fingerprint recognition technology is lower in price than other biometrics technology, and recognition speed is fast. Applications range from access control, time and attendance management, building integration systems, financial automation equipment, computer security, e-commerce certification and airport information systems (Reisfeld et al., 1990).

2.2. Eye recognition

The eye recognition system is a security system that follows the fingerprint recognition technology and refers to a technology that recognizes people using iris information of the eye having unique characteristics for each person, or such an authentication system.

A person's eye has characteristics that do not change after completion after 18

months of age. The iris pattern is almost unchanged once it is set, and every person has a different shape. In addition, it has more unique patterns than fingerprints, and can be recognized accurately even when wearing glasses or lenses. It is an advantage that there is no sense of rejection because of non-contact method.

The eye recognition system uses different eye characteristics for each person and applies them to the authentication technology for security. It was first introduced in the United States in the 1980s as an authentication method developed to identify people by analyzing the shape and color of iris and the morphology of retinal capillaries. This is done by coding the iris patterns and converting them into video signals to compare and judge. The general working principle is as follows. First, when the user's eye is aligned with the mirror in the center of the iris recognizer at a certain distance, the infrared camera adjusts the focus through the zoom lens. After the iris camera image, the user's iris as a photo, the iris recognition algorithm analyzes the iris pattern of the iris region to generate iris codes unique to the user. Finally, a comparative search is performed simultaneously to the iris code being registered in the database. In addition, it takes only about 2 seconds to process, and it is evaluated as biometrics technology which is one step advanced than fingerprint or retina recognition technology (Daugman, 1990).

2.3. Speech recognition

Speech recognition technology refers to a technique in which a computer converts an acoustic speech signal obtained through a sound sensor such as a microphone into a word or a sentence.

Generally, speech recognition technology extracts a sound signal and then removes noise. Then, the feature of the speech signal is extracted and compared with the speech model database (DB). Speech recognition technology is also a combination of sensing and data analysis techniques. However, it is known that the data to be measured and analyzed is a form of voice data, so it can be understood easily and accurately (Quatieri, 2001).

Various speech recognition services based on speech recognition technology began to be introduced in the late 2000s. A typical example is Apple's voice-based personal assistant service, Siri, launched in 2011. Siri is a personal secretary service that provides various services such as mobile search, schedule management, dialing, memo, music playback based on voice command of iPhone users. Since the launch of Apple's Siri, Google has launched a personal assistant service based on speech recognition, such as Google Now and Microsoft, Cortana. And NTT DoCoMo of Japan has also launched a foreign language interpretation service called 'Shabetekonsheru'.

In recent years, service devices based on voice recognition technologies such as "NUGU" of SKT and "Genie" of KT have been released.

3. Suggested System

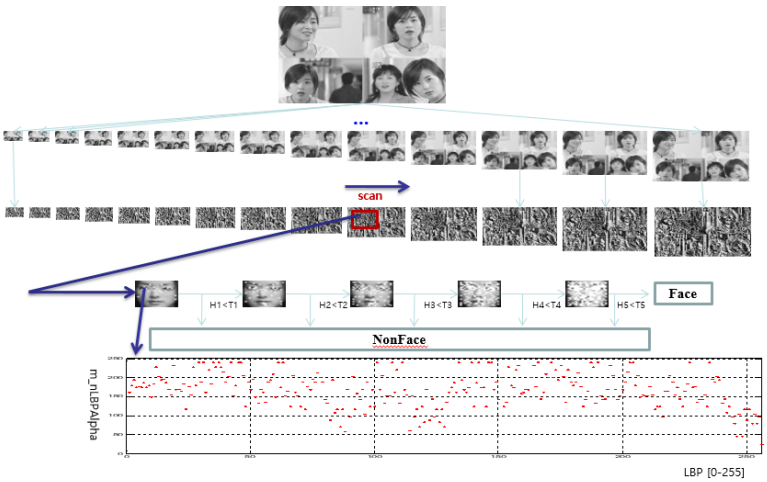
3.1. Development of complex personal authentication system applying biometrics pattern algorithm

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.

Based on these requirements, we designed and developed a simple authentication system that combines biometrics authentication (face, fingerprint, and eye) and PIN authentication. In order to strengthen the authentication system, we applied machine learning algorithm, which is the core of artificial intelligence (AI) technology, which has recently been in the spotlight, to improve versatility, security, and convenience.

Biometrics algorithms such as face recognition algorithm, eye recognition algorithm and fingerprint algorithm have been developed and applied to construct a complex personal authentication system using Biometrics pattern algorithm.

First, the face recognition algorithm is developed as shown in Fig.1 All paragraphs must be indented. All paragraphs must be justified.



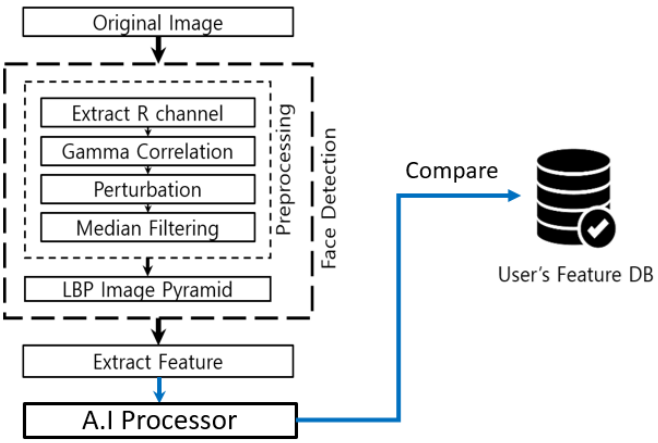


Fig. 1: Face recognition algorithm block diagram

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 databases. In the database constructed for the Face Recognition test, images of backlight, face pose inclination, low illumination, and occlusion were not detected in the RGB channel.

Fig. 2: Result of face detection

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 applied to compare the eye position and eye line of the learned user with the current user. The structure is shown in Fig.3.

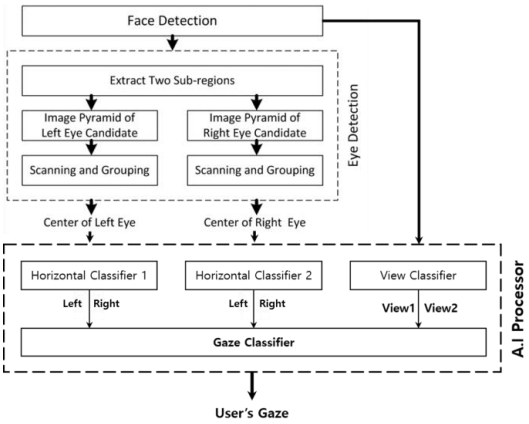


Fig. 3: Eye recognition algorithm block diagram

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) (Kim, 2011).

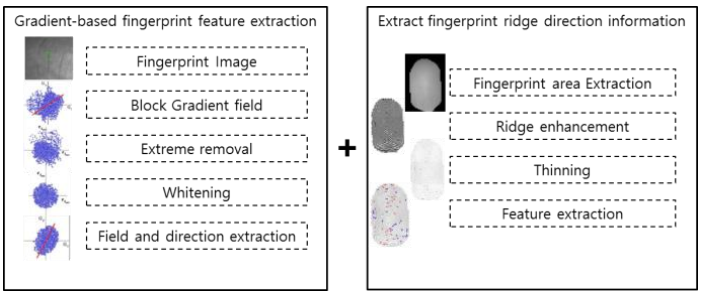


Fig. 4: Fingerprint recognition method

The algorithm used for fingerprint recognition is based on a 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 activated. When the registered fingerprint comparison is matched, the user is authenticated and the authentication is successful.

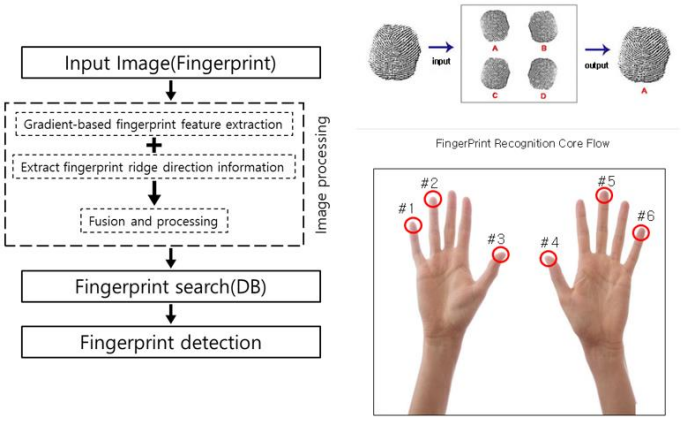


Fig. 5: Fingerprint recognition core flower

In this paper, in order to use the developed authentication system more effectively, we applied intelligent algorithm as shown in Fig.6. The applied A.I Processor learns the user 's biometric information, continuously grasps the feature points and patterns, enhances the accuracy of user authentication and enhances security.

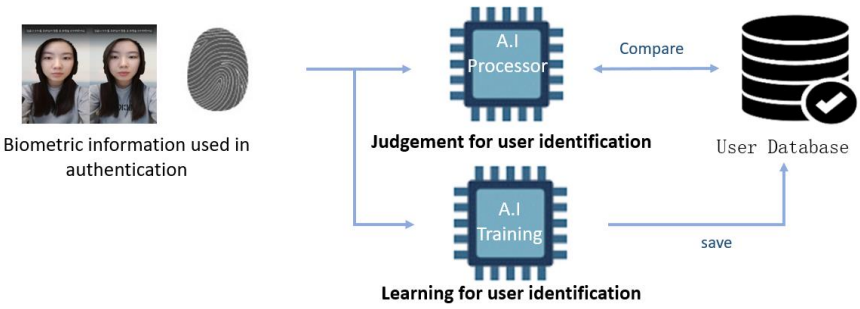


Fig. 6: A.I processor apply

By applying the biometric authentication scheme through the biometric

authentication algorithm (Face recognition, Eye recognition, Fingerprint recognition), which are described above and the PIN authentication method that are commonly used, as shown in Fig.7, a biometric authentication complex authentication algorithm that can perform real-time authentication processing for the first time in the world has been developed.

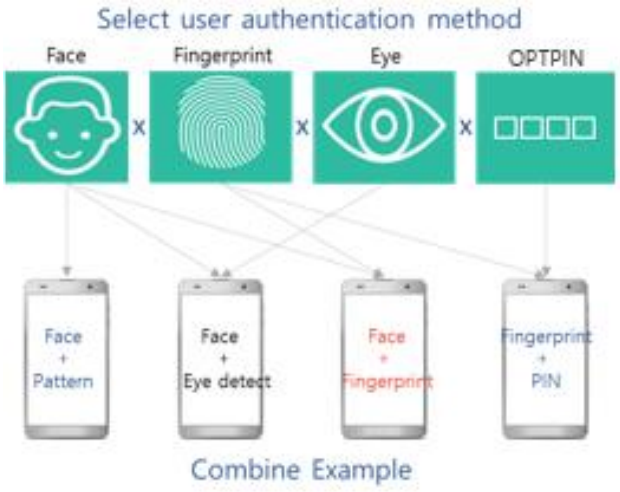


Fig. 7: Method of multimodal biometrics

This authentication system has been applied to Android on mobile basis and has been developed to protect personal information more conveniently, quickly and safely through various account registration. Fig.8 shows the real-time composite authentication screen. This algorithm has been developed so that it can be applied to a device based on Internet of Things. The language used was developed using Java and C.

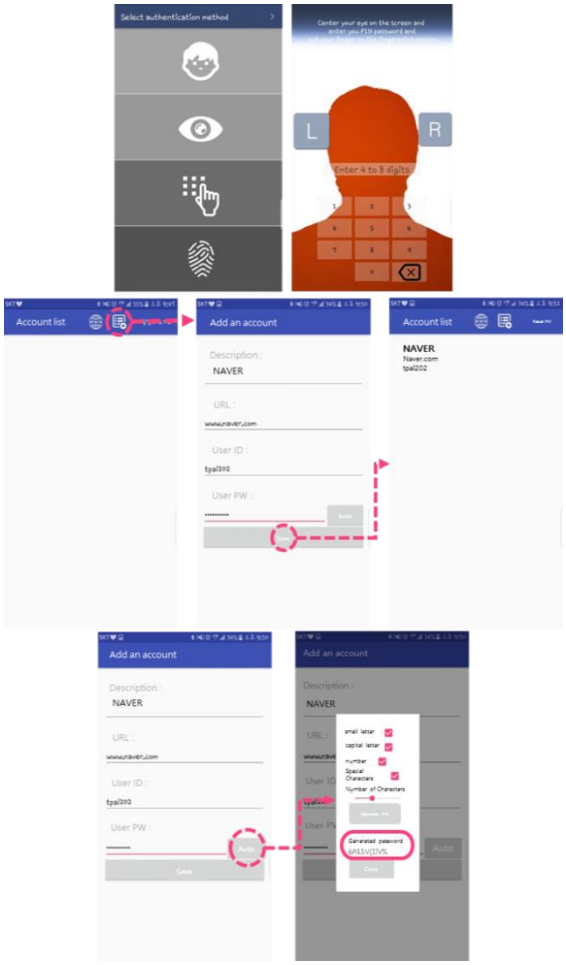


Fig. 8: Multimodal biometrics algorithm

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. Detection speed measurement results are shown in Fig.9. The evaluation environment includes an Intel-based Core ™ i7 CPU, Memory 8.0GB, 1980x1200 Raw Data based Windows OS.

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

Fig. 9: Result of detection speed

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.10.

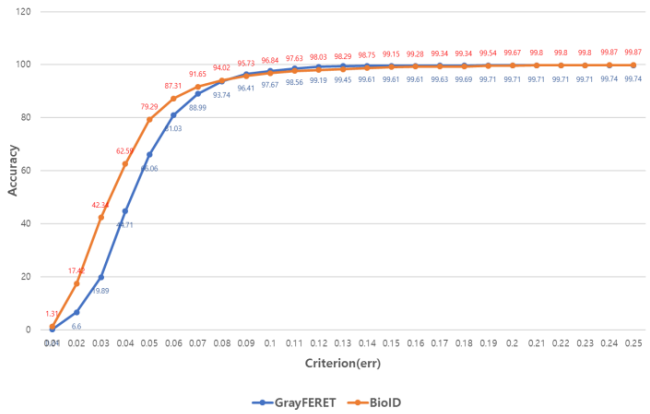


Fig. 10: Result of detection speed

4. Conclusion and Feature Work

The market for biometrics in the world is expected to grow to about 12.6 trillion won in 2016 and to 320 billion in Korea. In addition, the demand for authentication is steadily increasing due to the expansion of mobile functions, the increase of financial non-face authentication service of PINTECH and Internet banking, and the expansion of convergence service of Internet of Things and wearable device. 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. The algorithm developed through this paper can be an alternative to solve this problem. In addition, we will develop a more robust and convenient personal authentication system by installing an intelligent system based on deep learning, which is a recent issue in the artificial intelligence application part, which is finally tried in this paper.

Acknowledgement

This research was supported by Seokyeong University in 2017.

References

A. Jain, R. Bolle and S. Pankanti, Biometrics Personal Identification in Networked, Society, Kluwer Academic Publisher, (1999)

Biometrics Consortium: http://www.biometrics.org.

Dai Hwan Lim, Ki Hun Nam, Jin Young Park , Implement of Complex Personal Authentication System applying Biometrics Pattern Algorithm, *IJSH*, Vol. 13, No. 2 (2019)

D. Reisfeld, H. Wolfson and Y. Yeshrun, Detection of Interest Points Using Symmetry, Proceedings of 3rd ICCV, (1990).

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

J. Daugman, How iris recognition works, *IEEE Transactions on Circuits and Systems for Video technology*, (2004), Vol. 14, No.1. pp. 21-30

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.

Nam-Ho Kim, 2011, “Voice-based OTP Generation Techniques for Mobile Banking”, *KIIT*, 11(5), 2013.5, 113-119 (7 pages)

Thomas F. Quatieri, Discrete Time Speech Signal Processing Principles and Practice, Prentice Hall, (2001).