International Journal of Internet, Broadcasting and Communication Vol.8 No.2 38-42 (2016)
http://dx.doi.org/10.7236/IJIBC.2016.8.2.38

IJIBC 16-2-4

Face Recognition Authentication Scheme for Mobile Banking System

JongGun Song[1], Young Sil Lee[1], WonTae Jang[2], HoonJae Lee[2], TaeYong Kim[2*]

[1]*Dongseo University*
[2]*Division of Computer Engineering, Dongseo University*
*youngsil.lee0113@gmail.com, noname31@nate.com, {jwtway, hjlee, *tykimw2k}@dongseo.ac.kr*

Abstract

In this paper, we propose 3-factor mobile banking authentication scheme applied to face recognition techniques with existing certificate and OTP. An image of the user's face is captured by smart phone camera and its brightness processing of the contour of a face and background by n of X and Y points. Then, distance between the point of eyes, nose and mouth from captured user's face are compared with stored facial features. When the compared results corresponding to the data that stored in a face recognition DB, the user is authenticated.

Keywords: *Mobile banking, authentication, face recognition, certificate, one time password (OTP)*

1. Introduction

About half the adult global population now owns a smartphone, and by 2020, an estimated 80 percent will have one. Smartphones already have penetrated every facet of daily life [1]. The exponential usage of smartphones is deeply influencing user behavior and preferences. But while the mobile channel now touches every market and vertical, no sector has adopted mobile technology more wholeheartedly than the financial industry. Undoubtedly, mobile banking has changed the way people bank – ease, convenience and flexibility became its synonyms.

However, the challenge is that these mobile banking has also heightened concerns over fraud and data privacy [2]. In fact, rapidly growing the use of mobile banking, but with that growth come a whole new set of threats: mobile malware, third-party apps, access through the unsecured Wi-Fi networks, risky consumer behavior, and so on. It does not matter whether an institution uses a proprietary or third-party mobile banking application – the bank owns the risks [3].

To overcome these security threats, one of the best ways to overcome security concerns is to improve the authentication process. Unfortunately, strong authentication has traditionally meant sacrificing usability [4]. Users either relied on insecure passwords and challenge questions or they carried OTP devices, smartcards and security cards, which are inconvenient for users. However, users demand a balance between security and simplicity. The challenge is to guarantee effective security, without harming the user experience. This is where the use of biometrics comes into the picture by providing faster, easier and more robust authentication in a seamless way [5].

Authentication is the act of confirming a person or device/equipment using person-al identities, which

Manuscript Received: Feb. 10, 2016 / Revised: Feb. 20, 2016 / Accepted: Mar. 15, 2016
Corresponding Author: tykimw2k@ dongseo.ac.kr
Tel: +82-51-320-1738, Fax: +82-51-327-8955
Division of Computer Engineering, Dongseo University

often involves verifying at least one form of identification. There are three major factors to authenticate users based on something the user know (password and challenges response), something the user has (ID, security token, device and equipment), and something the user is (fingerprint, DNA, and other biometric identifiers). Each authentication factor covers a range of elements used to authenticate a person's identity, which can be used to grant the access authorization, approve a transaction request, and sign documents [6]. Among of these, biometric authentication is a well-studied area of research and it has been evaluated against a rich set of metrics that incorporate both performance and usability aspects. Physical biometrics, such as face, voice and signature, are the most commonly used forms [7].

In this paper, we propose a mobile banking authentication scheme applied to face recognition techniques with existing certificate and OTP. A face image is captured by smart phone camera and its brightness processing of the contour of a face and back-ground by n of X and Y points. Then, distance between the point of eyes, nose and mouth from captured user's face are compared with stored facial features. When the compared results corresponding to the data that stored in a face recognition DB, the user is authenticated.

2. Proposed Authentication Scheme

We propose 3-factor authentication scheme applied to OTP and face recognition techniques with existing 1-factor method by using login and certificate.

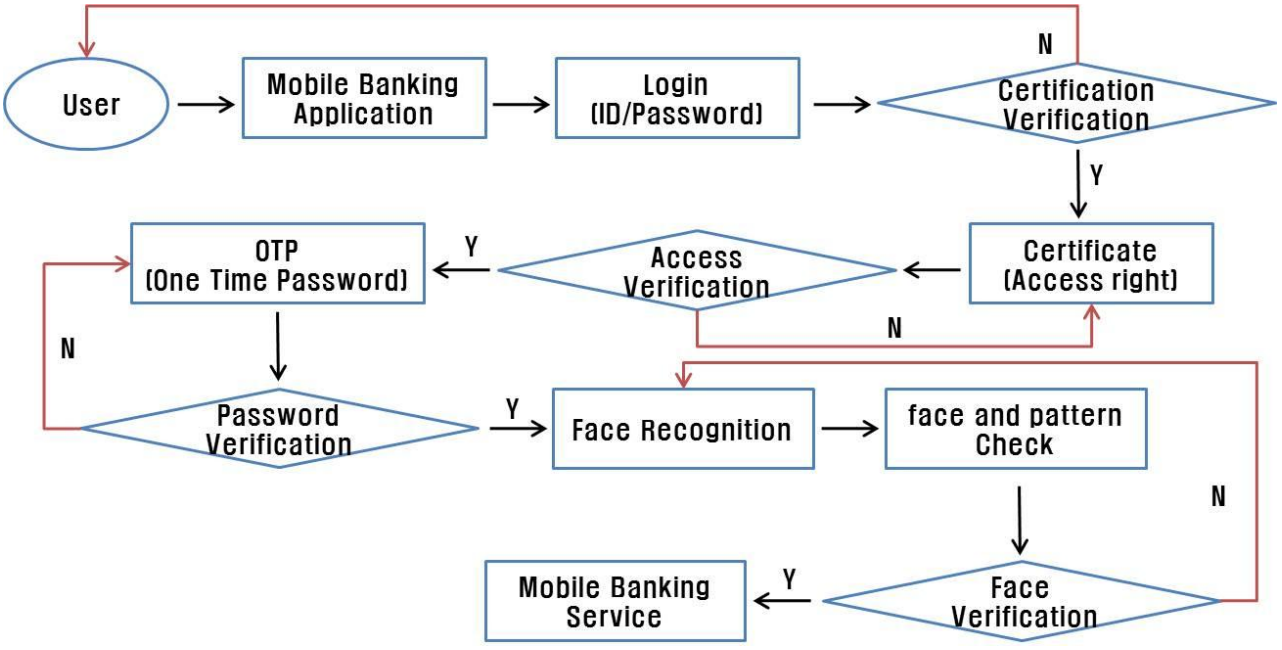

Figure 1. Overall process of proposed scheme

The overall process of authentication through face recognition is implemented as follows: an image of user's face is captured by smart phone camera, and when the extracted results correspond to the data saved in a facial recognition DB (database), the user is authenticated. The recognition system operates by image acquisition, pre-processing, face detection, face standardization and face recognition.

Fig. 2 shows the structure of face recognition technology; in the preprocessing, a user registers one's face to the DB; the first step is brightness processing of the contour of a face and background by X and Y points. The recognition part matches the contour of a face with the registered data on the DB and the service is executed after the user authenticates by matching the parameters such as distance by and between eyes, nose, and the contour of a face.

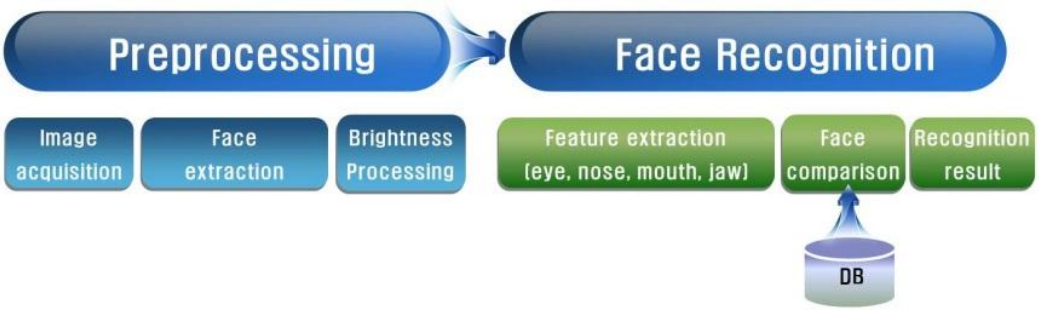

Figure 2. System structure of proposed scheme

First, in Fig. 3 – (a, b, and c) shows the methods of conventional certificate and OTP system: a user accesses a certificate and executes the face recognition through the smart phone camera. (a) When the user enter their login information (i.e., ID, Password, phone number), (b) the 3-digits sync code is transmitted to a smart phone by push notification and 6-digit random code is generated. (c) After verify the OTP code, a user completed their authentication process through a certificates. When the process of initial authentication is completed, user uses the mobile banking service after verification of extracting a feature through the user's face recognition.

Second, in Fig. 3 – (d, e, and f) shows the process of face recognition: (d) to obtain an image of user's face, separately extracting the recognized the contour of a face by automatically focused (green box). (e) It shows the relative position and feature of the main part of the extracted face (i.e., eyes, nose, mouth and jaw) by the re-detection. (f) It extracts the distance between the contours and main part of user's face (yellow box) in accordance with symmetrical structure through dotted dozens of points into a main part of the face. Then stored it in the DB and use the mobile banking authentication systems.

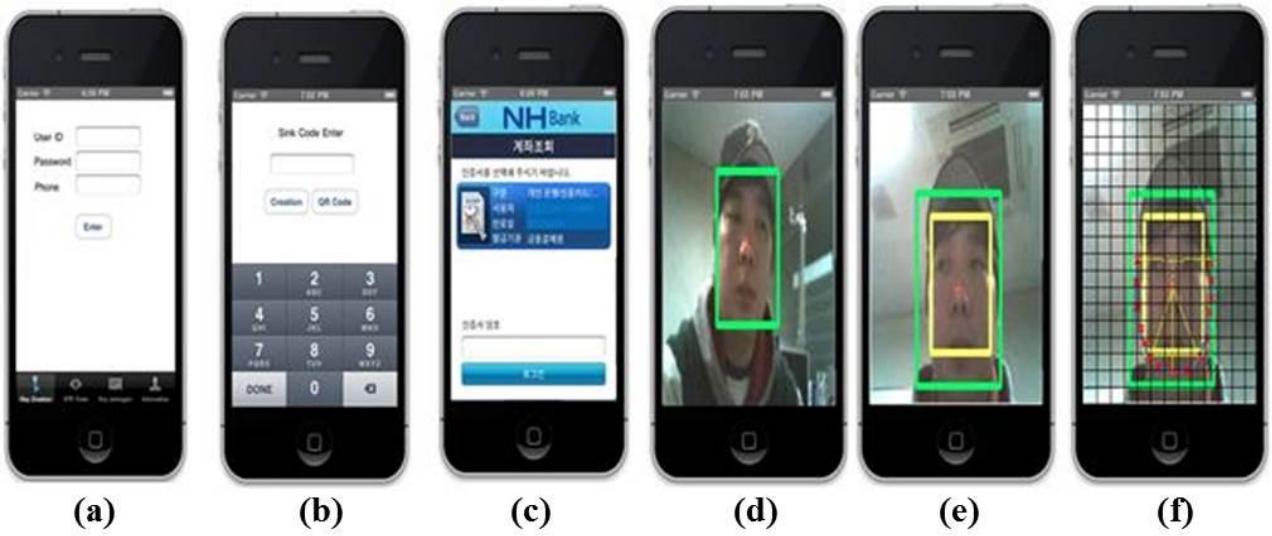

Figure 3. An experimental result of proposed authentication scheme

3. Evaluation of proposed scheme

In this section, we explained our experimental result, especially focused on face recognition. For the evaluation, we divided two categories which are face and main part of user's face and we tested several cases – face only, face & glasses, face & cap, face & glasses & cap, and picture of face as shown in Table 1 below.

Table 1. An experiment result of successful recognition rate

	Case 1. Face only	Case 2. Face & Glasses	Case 3. Face & Cap	Case 4. Face & Glasses & Cap	Case 5. Picture of Face
Step 1. Face	100%	90%	90%	90%	40%
Step 2. Main part of face	100%	80%	80%	50%	0%

The result of experiments in each case targeted 10 peoples: case 1 can reach a 100% of success rate and case 2, 3 and 4 can reach 80% and 50% success rate which means the recognition rate may not be good when the user wearing any elements such as glasses and cap. Furthermore, case 5 is 0% success rate which means proposed scheme is not allowed to recognize picture. This is important because to prevent identity theft through picture of authorized user.

Table 2. The comparison result

Authentication / Element	Existing authentication scheme		Proposed authentication scheme
	Login + Certification	Login + Certification + OTP	
Storage	Mobile device		
Input mode	Mobile Keyboard	Mobile Keyboard	Mobile Keyboard, Camera
Spill methods	Hacking, Theft, Lose		Theft, Lose
Possible attacks	Keyboard Hacking, Backdoor, Remote Control etc.	Memory Hacking, Keyboard Hacking, Phishing	-
Security Element	Authentication	Authentication	Authentication and Forgery prevention
Direction of Authentication	One-way (User →Financial)	One-way (User →Financial)	Two-way (User↔Financial)

Table 2 shows a comparative analysis of proposed authentication scheme with the existing mobile banking authentication scheme, by using biometric method; it is possible to check that the prospects of safety and credibility are strengthened. In addition, our scheme provides a two-way authentication that authenticates the user and the bank unlike existing one-way authentication method that authenticated user only.

4. Conclusion

Since 2010, the smart phone has led the world's users of the mobile phone market. However it has suffered from the loss or unstable security due to malicious codes. At present, smart phone certificates for mobile banking as well as integrated banking application services are under development.

To present an alternative to mitigate the unstable security and vulnerabilities of mobile banking service, we analyzed the problems of existing methods. Based on this, we propose a safe way to the factors of lost and risks. Our proposed scheme adopts a biometric authentication method by using smart phone and seems to be safe in terms of addressing security issues and malicious codes.

5. Acknowledgement

This work was supported by a research program of Dongseo University's Ubiquitous Appliance Regional Innovation Center supported by the grants from Ministry of Knowledge Economy of the Korean government and Busan Metropolitan City (No. B0008352).

References

[1] Ori Bach, Are you Ready for the Mobile Banking Authentication Challenge?, Security Intelligence, May 26, 2015. *https://securityintelligence.com*

[2] Shivani Aggarwal, The New Mobile Banking Password – Your Voice, Global Finance, Oct. 15, 2014. *https://www.gfmag.com*

[3] Tom Wills, Mobile Banking: Emerging Threats, Vulnerabilities and Counter-Measures, Information Security Media Group, 2015. *http://www.bankinfosecurity.com*

[4] Confident Technologies Secure Accessibility, Mobile Banking Security Using Strong Authentication, Confident Technologies, Inc., Jun. 01, 2011. *http://confidenttechnologies.com*

[5] Burcu Cinaz-Arnrich, Will mobile biometric authentication replace today's passwords?, Apr. 24, 2015. *http://www.monitise.com*

[6] Chorng-Shiuh Koon, Tzu-I Yang, and Chien-Chao Tseng, "A User Authentication Scheme Using Physiological and Behavioral Biometrics for Multitouch Devices," *The Scientific World Journal*, pp. 1-12, 2014.

[7] Shari Trewin, Cal Swart, Larry Koved, Jacquelyn Martino, Kapil Singh, and Shay Ben-David, "Biometric Authentication on a Mobile Device: A Study of User Effort, Error and Task Disruption," In *Proc. the 28th Annual Computer Security Applications Conference (ACSAC'12)*, pp.159-168, Dec. 3-7, 2012.