Regular paper

Journal of the KIECS. pp. 915-922, vol. 12, no. 5, Oct. 31 2017, t. 85, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2017.12.5.915

D-PASS: 스마트 기기 사용자 인증 기법 연구

정유선* · 최동민**

D-PASS: A Study on User Authentication Method for Smart Devices

You-Sun Jeoung* · Dong-Min Choi**

요 약

모바일 스마트 기기 이용자의 급격한 증가는 스마트 기기의 활동 범위를 크게 확장하는 계기가 되었다. 이러한 스마트 기기는 기존의 모바일 기기와 달리 기기 사용자의 다양한 비밀 정보를 관리·사용하고 있어 높은 보안 요구사항을 갖는다. 그러나 현재 스마트 기기에서 제공하는 인증 기법들은 최근의 스마트 기기를 대상으로 하는 보안 공격 유형들 중 사회 공학 공격에 해당하는 엿보기, 레코딩, 스머지와 같은 공격에 취약하다. 이에 본 연구에서 우리는 사회공학 공격에 강인하면서도 충분히 사용자 편의성을 고려한 새로운 방식의 인증 기법을 제안한다. 제안하는 기법은 그래픽 기반 인증 기법과 텍스트 기반 인증 기법을 혼합 적용하여 보안 안전성이 높으며 여타 그래픽 기반 기법과 달리 암호의 기억이 용이하다.

ABSTRACT

The rapid increase in users of mobile smart devices has greatly expanded their range of activities. Compare to conventional mobile devices, smart devices have higher security requirements because they manage and use various kind of confidential information of the owners. However, the cation schemes provided by conventional smart devices are vulnerable to recent attacks such as shoulder surfing, recording, and smudge attacks, which are the social engineering attacks among the types of security attacks targeting the smart devices. In this paper, we propose a novel authentication method that is robust against social engineering attacks but sufficiently considering user's convenience. The proposed method is robust by using combination of a graphical authentication method and a text-based authentication method. Furthermore, our method is easier to memorize the password compare to the conventional graphical authentication methods.

키워드

Graphical Authentication, Text-Based Authentication, Social Engineering Attack, Dial, Smart Device Authentication Method, User Private Information

그래픽 기반 인증, 텍스트 기반 인증, 사회공학 공격, 다이얼, 스마트 기기 인증 기법, 사용자 개인정보

Ⅰ. 서 론

최근의 스마트 기기 생산 및 사용자의 급격한 증가는 곧 스마트 기기를 이용한 다양한 생산 및 소비 활동의 증가를 가져왔으며 현재 대부분의 Desktop Pc 기반 활동은 스마트 기기를 통해서 처리가 가능하게 될 정도로 우리 일상생활의 한 부분을 차지하고 있다. 데스크탑 기반 보안 기법들 역시 이러한 추세에 맞게 모바일 기기 및 IoT 기기에 적용되고 있으며 모바일 기기 특성을 활용하는 보안 기법들도 제안되고 있다

* 동강대학교 겸임교수 (ys1128f@naver.com)
** 교신저자 : 조선대학교 자유전공학부
· 접 수 일 : 2017. 09. 30
· 수정완료일 : 2017. 10. 07
· 게재확정일 : 2017. 10. 18
· Received : Sep 30, 2017, Revised : Oct 07, 2017, Accepted : Oct 18, 2017
· Corresponding Author : Dong-Min Choi
Div. of Undeclared Majors, Chosun University,
Email : jdmcc@chosun.ac.kr

[1-7]. 보안 기법들 중 패턴 락 기법[8]은 9개의 점과 이를 연결하는 선분의 패턴을 통해 사용자 인증을 수행하는 보안 기법으로써 안드로이드 기반 스마트 기기의 주요 보안 기법으로 사용되고 있다. 그러나 스마트 기기의 특성과 사용자 특성을 공격 대상으로 하는 최근의 공격 유형인 엿보기[9], 레코딩[10], 스머지[11], 그리고 패스워드 추정 공격[12-13]에 취약하다. 이에 우리는 이러한 공격 유형에 강인한 스마트 기기용 사용자 인증 기법을 제안한다. 제안하는 기법은 텍스트 기반 패스워드 입력과 그래픽 기반 패스워드 인증 기법이 혼합된 형태로 기존의 텍스트 기반 기법 대비 보안상 안전하며 금고 다이얼식 비밀번호 입력을 적용하여 사용자에 친숙하다.

II. 보안위협과 대응방안

2.1 Shoulder Surfing

최근의 스마트 기기는 스크린 크기의 증가로 인해 엿보기 공격(Shoulder-Surfing Attack)[9]에 점점 더 취약해지고 있다. 이 공격은 공격자의 직접적인 관찰을 통한 비밀정보 취득을 시도하므로 시각정보 유출에 주의해야 한다.

2.2 Recording

전자식 광학 장비의 발전은 기존의 엿보기 공격을 진보시켰다. 이는 레코딩 공격(Recording Attack)[10]으로 사용자의 비밀정보 취득을 위해 광학 장비를 사용하며 엿보기 공격에 비해 높은 공격 성공률을 갖는다. 이러한 공격은 사용자의 패스워드 입력 행위에 대한 기록 및 반복 재생이 가능하므로, 특정 패턴 또는 정보를 비밀정보로 사용할 경우 이러한 공격에 매우 취약하다.

2.3 Smudge

지문인식 또는 패턴인식을 통한 사용자 인증 기법의 경우 주로 스마트 기기 화면을 통해 비밀정보 입력을 수행하는데 이런 경우 손가락 지문 또는 유분이 기기 스크린에 남아 공격자로 하여금 패스워드 추정 또는 가짜 지문을 이용한 인증이 가능하게 한다. 이는 스머지 공격(Smudge Attack)[11]에 해당하며 이러한 공격 유형에 대응하기 위해 다중 인증 또는 정형화된 패턴을 변화시켜 패스워드 추정이 불가능하도록 해야 한다.

2.4 스마트 기기용 QWERTY 보안 키보드

보안 키보드는 주로 은행에서 사용하는 QWERTY 타입의 보안 키패드를[14] 의미하며 이는 다음의 그림 1과 같다.

그림 1. 모바일 QWERTY 보안 키보드 예시
Fig. 1 Example of mobile qwerty secure keyboard

이 기법은 패스워드 추정을 어렵게 하기 위해 패스워드 입력창 하단의 키패드의 각 키의 위치가 임의의 간격을 두고 다시 배치되는 방식을 취한다. 또한 안전성 향상을 위해 화면 하단의 재배열 버튼을 눌러 재배치 가능하다. 그러나 키의 재배치에 한계가 있어 각 행의 키는 상하 다른 행으로 위치가 변경되지 않아 확률적 패스워드 추정이 가능하다. 따라서 엿보기, 레코딩, 그리고 스머지 공격에 모두 취약하다.

2.4 스마트 기기용 ABC 보안 키보드

QWERTY 타입 이외에도 알파벳 순의 키배치가 이루어지는 ABC타입의 키보드[15] 또한 다음의 그림 2와 같이 키 사이에 임의 개수의 공백이나 마크를 삽입한다. 이 방법은 QWERTY 방식과 달리 사용자에 친숙하지 않아 입력에 시간이 다소 걸리는 점이 있으나 보안의 관점에서 QWERTY 방식에 비해 키 재배치가 자유로워 행간 키 이동이 가능하다. 따라서 QWERTY 기법보다 입력 위치를 추정하기 어렵다. 그러나 여전히 확률적 추정 성공률은 존재하며 엿보기, 레코딩, 그리고 스머지 공격에 모두 취약하다.

그림 2. 모바일 ABC 보안 키보드 예시
Fig. 2 Example of mobile abc secure keyboard

2.5 터치&슬라이드 키보드

기존의 보안 키보드의 입력방법과 달리 이 방법은 기존의 키 배열을 사용하지 않는다[15]. 다음의 그림 3과 같이 숫자키를 제외한 키는 모두 좌에서 우로 순환하여 화면에 표시되는 방식으로 사용자는 원하는 키의 입력을 위해 화면 중앙의 노락색 사각 테두리 안에 입력을 원하는 키를 이동시킨 후 노란색 사각 테두리 안의 글자를 클릭하여 입력을 수행하며 최종적으로 확인 버튼을 눌러 입력을 마친다. 한글의 자음과 모음, 그리고 영문의 대·소문자를 상단의 순환링과 하단의 순환링에 별도로 배치함으로써 입력의 편의성을 고려하였으며 순환 링에 나타나는 초기 입력 문자의 위치가 고정되어 있지 않을 경우 패스워드 추정을 통한 공격이 어렵다. 그러나 직접적인 관찰 또는 광학 장비를 활용한 공격에는 여전히 취약하여 엿보기, 레코딩 공격에 취약하다.

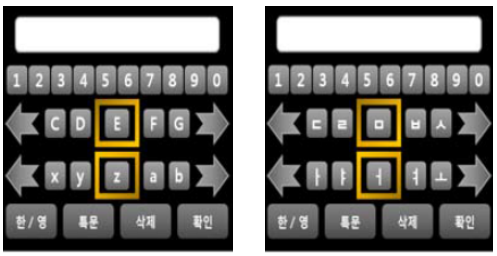

그림 3. 터치&슬라이드 키보드 예시
Fig. 3 Example of touch mobile abc secure keyboard

2.6 SmudgeSafe

이 기법[16]은 이미지 정보가 적용된 패턴 입력 인증 기법으로 패턴의 배경으로 사용되는 이미지의 변화 즉, 임의의 각도 회전 또는 스케일링된 이미지에 대해 패턴을 대응하여 그리는 방법으로 기존의 패턴 기반 인증 기법에 비해 향상된 보안성을 갖으며 특히 스머지 공격에 강인하다. 다음의 그림 4와 같이 이 기법에서 기본적으로 등록된 패턴 'N'은 배경의 이미지 정보와 대응되어 그 좌표가 같이 저장되며, 이 정보가 인증에 사용된다. 따라서 패턴 입력을 통한 사용자 인증 수행 시 배경 이미지의 변형을 패턴의 변화와 함께 고려하여 패턴을 입력 및 사용자 인증을 수행하는 기법이다. 이 기법은 기존의 단순 패턴입력을 통한 인증기법에 비해 보안 안전성은 높으나 패턴 입력에 따른 오류 발생률이 높다. 또한 이 기법은 기존의 텍스트 입력 기반 기법에 비해 엿보기, 레코딩, 그리고 스머지 공격에 상대적으로 안전하나 배경 정보와 패턴 정보가 함께 유출될 경우 여전히 기존의 단순패턴 인증과 동일한 보안 취약성을 갖는다.

그림 4. 터치&슬라이드 키보드 예시
Fig. 4 Example of smudgesafe

III. 제안 기법

제안하는 방법은 다음의 그림 5와 같이 다각형의 중첩된 다양한 크기의 다이얼을 통한 텍스트 기반 패스워드를 입력하는 방식으로써, 기존의 PIN 기반 입력 기법 및 단순 그래픽 기반 사용자 인증 기법을 대체하는 기법으로, 기존의 4-6자리 숫자를 직접 숫자키패드를 통하여 입력하거나 패턴의 직접적인 입력을 통한 사용자 인증 기법을 보완한다.

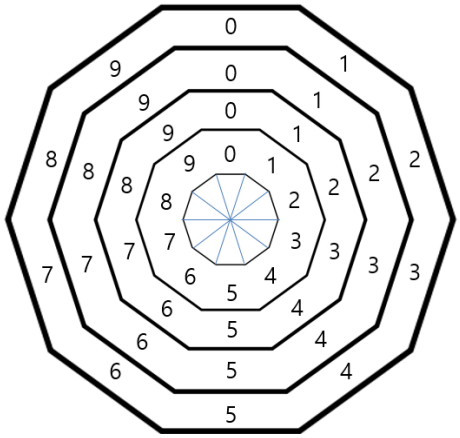

그림 5. 제안 기법의 레이아웃
Fig. 5 Layout of proposed scheme

제안 기법은 위의 그림 4와 같이 기존의 PIN 입력을 위한 키패드 기반 구조와 상이한 구조를 가지고 있다. 기존의 PIN 입력 키패드 기반 기법은 패스워드 입력 과정에서 정보 유출의 우려가 높아 안전한 사용이 어렵다. 제안하는 기법은 스크린에 디스플레이 되는 입체적으로 표시된 다이얼을 마치 금고의 다이얼을 돌리는 것과 같이 좌 방향 또는 우방향으로 회전시켜 다이얼 중앙 최상단의 정보 표시자인 포인터와 순차적으로 일치시키는 방법으로 PIN 코드를 입력하며 제안 기법의 PIN 코드 입력에 대한 예는 다음의 그림 6과 같다.

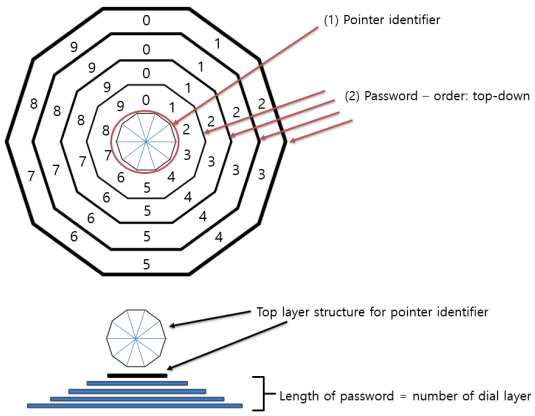

그림 6. 제안 기법 구조
Fig. 6 Structure of proposed scheme

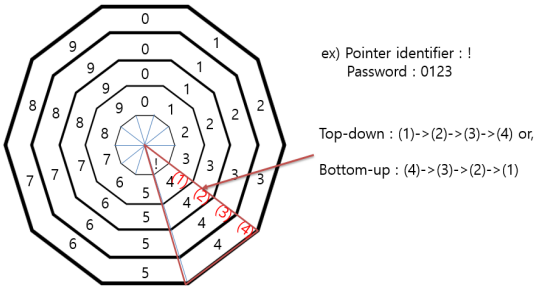

그림 7. 제안 기법의 패스워드 입력 순서
Fig. 7 Password input order of proposed scheme

패스워드 등록에 앞서, 사용자는 최상단 다이얼에 위치하게 될 색 또는 기호 정보를 정의한다. 이 정보는 일종의 포인터와 같은 개념으로 쓰이며, 이 정보와 PIN 코드의 조합으로 사용자 인증이 진행된다. 그림 7은 사용자에 의해 등록된 정보'!'와 PIN 코드 0123에 대한 입력 예시이다. PIN 입력을 위해, 사용자는 스크린에 표시된 그림 6과 같은 입력 다이얼을 키보드와 같은 입력 수단으로 사용하게 되며, 해당 다이얼은 바깥쪽에서 안쪽으로 또는 안쪽에서 바깥쪽으로 순서대로 다이얼을 회전시켜 그림 6의 최상단 다이얼에 표시된 '!' 정보와 같은 방향으로 정렬한다. 이때 최상단에 표시되는 기호 또는 색 정보는 사용자가 선정한 기호 또는 색 정보를 포함하는 10개의 기호 또는 10개의 색 정보가 각 영역에 함께 표시된다. 또한 최상단에 표시되는 정보는 PIN 다이얼의 각 다이얼 정보를 입력할 때마다 매번 위치가 바뀐다. 각 PIN 다이얼의 정보 입력을 위한 버튼은 PIN 최상단 다이얼을 터치함으로 정보입력이 수행된다. 따라서 사용자는 기호정보와 PIN 정보를 기억하면 사용자 인증을 수행할 수 있다. 외부 공격자는 최상단 다이얼의 사용자 선택 정보, 즉 색 또는 기호정보를 알 수 없으면 PIN을 추정하는 것이 불가능하다.

스머지 공격에 대해서도 최상단 다이얼의 위치 정보가 매번 변하므로 PIN 코드 입력시 스크린에 남는 유분 정보가 제각각 다르게 되어 추정이 어렵다. 가속도 및 자이로 센서류를 이용한 패스워드 추정 또는 스크린 터치 좌표 획득을 통한 패스워드 추정, 또는 스크린 캡쳐 공격을 통한 패스워드 추정 공격에 대해서도 값이 매번 다르게 측정되므로 비밀정보 획득이 어렵다. 또한, 패스워드 추정을 더욱 어렵게 하기 위

해 다이얼의 회전을 손가락 터치 및 슬라이드의 감도에 사용자가 가중치를 더하게 함으로써 회전 속도 및 회전 비율을 변경할 수 있다. 추가적으로 사용자 입력의 편의를 위해 최상단을 제외한 각 층의 다이얼은 자신의 다이얼 정보가 입력이 완료되면 다이얼을 삭제하도록 하여 손가락 터치에 따른 잘못된 다이얼 선택을 보완할 수 있으며, 사용자 본인이 입력한 정보의 순서를 추정하도록 할 수 있다.

다음의 그림 8은 PIN 코드 입력이 (1)->(2)->(3)->(4)의 순번으로 동작할 경우 다이얼 삭제를 순차적으로 최상단 다이얼에서부터 최하단의 순으로 나타낸 것이며, (4)->(3)->(2)->(1)의 순번일 경우 그림 8의 역순으로 다이얼 삭제가 진행된다.

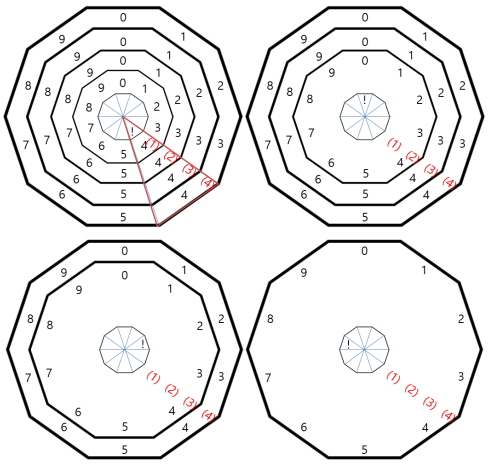

그림 8. 다이얼 삭제 예시
Fig. 8 Example of dial deletions

Ⅳ. 안전성 평가

다음의 표 1은 엿보기, 레코딩, 스머지, 그리고 패스워드 추정 공격에 대한 안전성을 기존의 기법과 비교한 비교표이다.

보통 등급인 'M'을 기준으로 안전성을 높고 'H' 낮음 'L'에 따라 구분하였다. 표에 의하면 QWERTY 기반 기법은 키 입력이 바로 확인 가능하다는 점에서 엿보기, 레코딩, 스머지, 그리고 패스워드 추정 공격에 모두 취약하다. ABC기반 기법의 경우, 키의 재배치가 QWERTY에 비해 조금 자유로운 것 외에 차이점이

표 1. 안전성 비교
Table 1. Security comparison

(H: High, M: Moderate, L: Low)

Type of Attack	User Authentication Method			
	QWERTY Keyboard	ABC Keyboard	Smudge Safe	Proposed
Shoulder Surfing	L	L	L	H
Recording	L	L	L	H
Smudge	L	M	M	H
Password Guessing	L	M	M-H	H

없어 엿보기 및 레코딩 공격에 취약하다. SmudgeSafe의 경우 비밀정보 획득의 용이성으로 인해 엿보기, 레코딩 공격에 취약하며 스머지 및 패스워드 추정 공격에 QWERTY 및 ABC에 비해 강인하다.

제안하는 방법의 경우 직접적으로 누출되는 정보는 직접적인 비밀정보 유출에 관련이 없어 엿보기 공격에 대한 비밀정보 획득 시도에 강인하다. 또한 레코딩 공격에 의한 연속적인 영상 정보의 유출에도 정보 표시자 정보의 유출이 없다면 패스워드 추정을 위한 근거가 되는 정보가 유출되지 않아 보안상 안전하다. 스머지 공격의 경우에도 다이얼 정보의 임의 변경을 통해 회피 가능하여 안전하다고 할 수 있으며, 이를 통해 패스워드 추정 공격에 어려움이 있다.

Ⅴ. 결론 및 향후개선 방향

제안 기법은 기존의 스마트 기기용 텍스트 기반 보안 키보드의 입력에 대한 보안상 문제점과 그래픽 기반 패스워드 입력 기법의 보안상 한계점에 대한 보완 연구로써, 그래픽 기반 패스워드 입력을 적용한 최근의 사회공학 공격에 강인한 텍스트 정보 입력을 제안하였다. 안전성 비교 결과 제안하는 방법은 기존 보안 기법의 문제점이었던 스마트 기기의 화면에 표시되는 정보를 통해 유출 가능한 정보의 누설이 최소화되어 기존 기법들에 비해 안전하다. 향후 우리는 제안 기법의 보안 안전성에 대한 사용자 편의성 확보를 위해 Password registration usability, Login process usability, Easy to remember, Typographical error, Typing speed, Amount of time spent for login process 항목에 대해 개선 방안을 도출하고자 한다.

References

[1] K. Kim, D. Wang, and S. Han, “Home Security System Based on IoT,” *J. of Korea Institute Electronic Communication Science*, vol. 12, no. 1, 2017, pp. 147-154.

[2] S. Agrawal, A. Z. Ansari, and M. S. Umar, “Multimedia Graphical Grid based Text Password Authentication: For Advanced Users,” *2016 Thirteenth Int. Conf. on Wireless and Optical Communications Networks (WOCN),* Hyderabad, India, Jul. 2016, pp. 1-5.

[3] D. Tak and D. Choi, “Layered Pattern Authentication Scheme on Smartphone Resistant to Social Engineering Attacks,” *J. of Korea Multimedia Society,* vol. 19, no. 2, 2016, pp. 280-290.

[4] A. V. D. M. Kayem, "Graphical Passwords – A Discussio,” *2016 30th Int. Conf. on Advanced Information Networking and Applications Workshops (WAINA),* Crans-Montana, Switzerland, Mar. 2016, pp. 596-600.

[5] G. Lee, B. Kim, and J. Lee, “Distributed Hardware Security System with Secure Key Update,” *J. of Korea Institute Electronic Communication Science*, vol. 12, no. 4, 2017, pp. 671-678.

[6] J. Saidov, B. Kim, J. Lee and G. Lee, “Hardware Interlocking Security System with Secure Key Update Mechanisms In IoT Environments,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 12, no. 4, 2017, pp. 671-678

[7] S. Lee and W. Jeong, “A Study on Authentication Algorithm for NFC Security Channel”, *J. of the Korea Institute of Electronic Communication Sciences*, vol. 7, no. 4, 2012, pp. 805-810

[8] M. Shahzad, A. X. Liu, and A. Samuel, "Secure unlocking of mobile touch screen devices by simple gestures: You can see it but you can not do it,” *Proc. of the 19th Annual Int. Conf. on Mobile Computing & Networking, MobiCom '13,* Miami, USA, Sept. 2013, pp. 39-50.

[9] H. Sun, S. Chen, J. Yeh, and C. Cheng, "A Shoulder Surfing Resistant Graphical Authentication System,” *IEEE Trans. Dependable and Secure Computing,* vol. pp, issue 99, 2016, pp.11-16.

[10] T. Takada, "FakePointer: An Authentication Scheme for Improving Security against Peeping Attacks using Video Cameras," *Proc. of Int. Conf. on Mobile Ubiquitous Computing, Systems, Services and Technologies,* Valencia, Spain, Sept. 2008, pp. 395-400.

[11] H. Kim, H. Seo, Y. Lee, T. Park, and H. Kim, "Implementation of Secure Virtual Financial Keypad for Shoulder Surfing Attack,” *Review of Korea Institute of Information Security and Cryptograph (KIISC),* vol. 23, no. 6, 2013, pp. 21-29.

[12] L. Cai and H. Chen, "TouchLogger: Inferring Keystrokes on Touch Screen from Smart-phone Motion,” *Proc. of the 6th USENIX Conf. on Hot Topics in Security,* San Francisco, USA, Aug. 2011, pp.9.

[13] E. Miluzzo, A. Varshavsky, S. Balakrishnan, and R.R. Choudhury, "TapPrints: Your Finger Taps Have Fingerprints,” *Proc. of the 10th Int. Conf. on Mobile Systems, Applications, and Services,* Lake District, UK, Jun. 2012, pp. 323-336.

[14] Y. Lee, "An Analysis on The Vulnerability of Secure Keypads for Mobile Devices,” *J. of Korean Society for Internet Information,* vol. 14, no. 3, 2013, pp. 15-21.

[15] D. Lee, D. Bae, S. You, J. Chae, Y. Lee, and H. Yang, “An Analysis on the Security of Secure Keypads for Smartphone,” *Review of Korea Institute of Information Security and Cryptograph (KIISC),* vol. 21, no. 7, 2011, pp. 30-37.

[16] S. Schneegass, F. Steimle, A. Bulling, F. Alt, and A. Schmidt, “SmudgeSafe : Geometric Image Transformations for Smudge-resistant User Authentication,” *2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing,* SEATTLE, USA, Sept. 2014, pp. 775-786.

저자 소개

정유선(You-Sun Jeoung)

1999년 원광대학교 의상학과 졸업(이학사)
2007년 조선대학교 대학원 컴퓨터공학과 졸업(공학석사)
2013년 조선대학교 대학원 컴퓨터공학과 졸업(공학박사)
2017년 ~현재 동강대학교 보건행정학과 겸임교수
※ 관심분야 : 의료통신시스템, 빅데이터, 센서인식 시스템, 3차원영상처리, U 헬스케어, 생체정보

최동민(Dong-Min Choi)

2003년 경희대학교 공과대학 졸업(공학사)
2007년 조선대학교 정보컴퓨터교육 졸업(교육학석사)
2010년 조선대학교 대학원 컴퓨터공학과 졸업(공학박사)
2013년 조선대학교 컴퓨터공학과 박사후연구원
2014년 ~현재 조선대학교 자유전공학부 조교수
※ 관심분야 : 센서 네트워크, 모바일 센서 응용 기술, VPA 기술, U 헬스케어, 스마트 그리드 홈 네트워크 보안, 정보 윤리, 스마트폰 응용 보안 기술, 모바일 VR/AR 생체정보 보안