Journal of Korea Multimedia Society Vol. 18, No. 3, March 2015(pp. 368-375)
http://dx.doi.org/10.9717/kmms.2015.18.3.368

사회 공학적 공격에 대응하는 색 기반 스마트폰 가상 키보드

최동민[†], 백철헌[††], 정일용[†††]

Virtual Keyboard against Social Engineering Attacks in Smartphones[1)]

Dongmin Choi[†], Cheolheon Baek[††], Ilyong Chung[†††]

ABSTRACT

Nowaday, financial institutions provide secure mobile keyboard solutions to keep their mobile banking services safe. However, these are still vulnerable to attacks, such as shoulder surfing attack. Especially, in the case of handicapped person such as visual impairment and blindness, they are more vulnerable than ordinary person because of inconvenience of secure information input. Among them, we focused on the color blind. For the color blind, 4-color based secure keyboard method causes more inconvenience to notify exact color. Thus, we propose a secure mobile keyboard solution to provide advanced functionality for the color blind users. Our method is based on 4-color theorem to support color blind users. In addition, our scheme is robust against shoulder surfing attack. According to the evaluation result, our method offers increased security against shoulder surfing attack compare with existing methods.

Key words: Virtual Keyboard, Color Blind, Shoulder Surfing Attack

1. 서 론

모바일 뱅킹은 휴대폰 등 모바일 기기를 통해 이루어지는 계좌정보조회, 현금인출, 자금이체 등의 은행서비스를 의미하며, 모바일 뱅킹은 모바일 기기 상호간, 모바일기기와 서버간 및 모바일 기기와 PC간 통신이 이루어지고 있어 금융 정보 유출의 우려가 있다. 특히 스마트폰의 경우 개방형 운영체제를 탑재하여 불특정 다수의 개발자가 만든 어플리케이션이 설치되며, 무선통신을 이용한 인터넷 연결이 빈번하게 이루어지므로 해킹 및 바이러스에 대한 노출 위험이 높다. 이러한 취약점에 대응하여 금융기관들은 운영체제 위·변조 검사, 악성코드 검사, 보안 키패드[1-3] 등 다양한 보안기술[4]을 적용하고 있으며 바이오메트릭스 기술[5]의 적용도 진행되고 있다. 이러한 보안 기술 중 모바일 뱅킹에서 사용되는 가상 키패드 보안 솔루션은 소프트웨어 안전성은 갖추고 있으나 사회 공학적 공격 기법에는 취약한 면이 있다. 가상 키패드 보안 솔루션에서 비밀정보를 입력하는 사용자의 입력 편의를 위해 제공되는 입력 키 정보 표시 창은 사용자 입력 오류 방지를 위해 최종 입력 값을 별(*) 표시 없이 그대로 공개하고 있다. 이는

※ Corresponding Author : Ilyong Chung, Address: (501-759) Chosun Univ., Seoseok-dong, Dong-gu, Gwangju, Korea, TEL : +82-62-230-7712, FAX : +82-62-230-7754, E-mail : iyc@chosun.ac.kr
Receipt date : Dec. 24, 2014, Revision date : Jan. 22, 2015
Approval date : Jan. 29, 2015
[†] Division of Undeclared Majors, Chosun University (E-mail : jdmcc@chosun.ac.kr)
[††] Department of Computer Engineering, Chosun University (E-mail : guhoot@nate.com)
[†††] Department of Computer Engineering, Chosun University
※ This study was supported by research fund from Chosun Univeristy, 2014
1) An earlier version of this paper was presented at the International Workshop on Managing Insider Security Threats, Seoul, south Korea, November 21-22, 2014.

사회 공학적 공격 기법 중 하나인 shoulder surfing attack[6]에 취약하며, 공격자는 이를 통해 모바일 뱅킹 사용자가 입력하는 비밀 정보를 비교적 쉽게 알아낼 수 있다. 이에 H. Kim[3]은 보안 키패드에 4색 이론[7]을 조합한 입력 방법을 제안하였다. 그러나 이 방법은 색맹 및 색약자의 경우 색 구분에 어려움이 있어 적용이 어렵다. 이에 우리는 색맹 및 색약에 적용이 가능한 보안 키패드 입력 기법을 제안한다. 제안하는 방법은 4색 이론이 적용된 보안 키보드이면서 색맹 및 색약도 사용이 가능하며 기존에 비해 보안 안전성이 향상되었다.

본 논문의 구성은 다음과 같다. 제 2장에서는 관련 연구로서 모바일 뱅킹 보안 기술에 관련된 취약점에 대해 고찰한다. 제 3장에서는 제안하는 기법의 동작 알고리즘에 대해 기술한다. 제 4장에서는 제안기법을 기존 기법과 비교하여 평가하며, 마지막으로 5장에서는 본 연구의 결론 및 향후 연구 과제에 대해 논의한다.

2. 관련연구

2.1 모바일 뱅킹 취약점

스마트 폰을 이용한 모바일 뱅킹은 스마트폰 전자금융서비스에 해당하며 해당 서비스에서 발생할 수 있는 보안위협은 설계 및 개발 단계에서 발생하는 보안위협과 설치 및 이용 단계에서 발생하는 보안위협, 그리고 시스템 및 관리 단계에서 발생하는 보안위협으로 분류할 수 있다. 이 중 shoulder surfing attack의 경우 설치 및 이용 단계에서 발생하는 보안위협에 해당하며 스마트폰 전자금융서비스 어플리케이션 이용을 위한 구성요소인 스마트폰(단말/플랫폼), 전자금융서비스 어플리케이션(어플리케이션), 그리고 이동통신망 및 무선 네트워크(네트워크) 중 스마트폰에 해당한다[8]. 즉, shoulder surfing attack은 스마트폰 단말차원에서 대응하여야 함을 의미한다. 그러나 최근의 스마트폰 단말은 대화면 제품이 주류를 이루고 있어 shoulder surfing attack 에 더욱 취약할 수 밖에 없는 환경을 제공하고 있다. 물론 대화면일수록 키패드의 크기도 크게 되어 입력 오류율이 낮아지므로 입력속도가 증가하며 이를 통해 shoulder surfing attack에 어느 정도 대응이 가능하다[9]. 그러나 공격자가 사람이 아닌 고해상도 캠코더나 CCTV, 또는 스마트폰을 이용한 동영상 녹화일 경우 고속 입력으로 인한 이점은 없으며 오히려 대화면으로 인한 취약성만 증가하게 된다. 따라서 대화면 스마트폰 사용자가 모바일 뱅킹 서비스를 이용할 경우에도 shoulder surfing attack에 대응이 가능한 방법이 필요하다.

2.2 색맹 및 색약 비율과 색약 모드

D. Mclntyre [10]의 보고서에 의하면 전 세계 인구의 8.5%가 색맹 또는 색약으로 보고되고 있다. 따라서 대중적인 스마트폰 단말의 사용에 있어 색맹 및 색약을 고려한 방법이 반드시 필요하다고 할 수 있다. 몇몇 게임사에서 제공하는 색약 모드[11]는 일부 색상을 변환시켜 색약도 게임을 즐기기에 편하도록 하는 기능이며, 다수의 게임이 이러한 색약 모드를 지원한다. 외국에서 개발된 게임의 경우 League of Legends[12], World of Tanks[13], World of Warcraft[14] 등의 게임이 이러한 색약 모드를 지원하며 국내 개발 게임으로 모바일 게임인 모두의 게임[15]이 색약 모드를 지원하고 있다. 다음의 Fig. 1은 색약 모드에 대한 예시이다.

2.3 이전 연구 비교

다음의 Fig. 2는 기존에 사용되고 있는 보안 문자 입력 및 표시 방법을 나타낸 것이다.

Fig. 2의 방법은 사용자 입력의 편의를 제공하기 위해 보안입력문자의 마지막 문자를 별표로 가리지

Fig. 1. Example of color blind mode appeared in world of warcraft.

Fig. 2. Secure keyboard solution of basic method [16].

않고 그대로 화면에 나타내는 기존의 방법을 나타낸다. 이 방법은 마지막 문자를 화면에 어떠한 암호화 조치 없이 표시하므로 shoulder surfing attack과 같은 유형의 공격에 매우 취약하며, 이전 연구[3]에 의하면 약 68%의 공격 성공률을 보이고 있다.

이러한 취약점을 극복하기 위해 제안된 H. Kim의 방법[3]은 4색 이론[7]에 근거한 키보드 색 마스킹 방법을 제안하였으며 이는 다음의 Fig. 3과 같다.

Fig. 3. Secure keyboard solution of H. Kim's method [3]

이 방법은 기존의 방법과 달리 사용자의 모든 키보드 입력에 별표로 마스킹 처리를 하였고 사용자 입력과 오입력 확인 및 수정의 편의 및 보안성 강화를 위해 키보드의 각 키를 4색 중 하나로 마스킹 처리를 하였다. 따라서 이 방법이 적용된 키보드를 사용하는 사용자는 4색이 적용된 키를 입력하며, 상단의 입력 확인창의 별표의 색을 확인하여 오 입력을 인지하고 쉽게 수정할 수 있도록 하였다. 이 방법의 장점은 외부 공격자가 입력된 킷값을 알 수 없어 shoulder surfing attack과 같은 사회공학적 공격 기법에 강인하다는 것이다.

그러나 이 방법에는 두 가지 문제가 있다. 첫째로 4색 이론이다. 4색은 각각 빨강, 노랑, 파랑, 노란색을 의미하며 이 색은 색맹이나 색약의 경우 구분이 어려운 색에 속한다. 따라서 사용자가 색 구분에 어려움이 있을 경우 자신이 입력한 키의 값이 올바른지 알 수 없어 보안 문자 입력에 큰 어려움을 갖게 될 수 있다. 둘째로 4색으로 마스킹 된 키보드의 색이 변동이 없다는 것이다. 이는 shoulder surfing attacker가 사용자 입력을 추정할 수 있게 하므로 보안상 취약점을 갖게 된다.

3. 제안 방법

본 연구에서는 shoulder surfing attack에 강인하며 저시력자 및 색맹, 색약을 고려한 보안 키패드 입력 방법을 제안한다. 제안하는 방법은 H. Km의 방법의 색 표시 방법을 수정하였고 color blind mode를 구현하였으며, 키패드 색 랜덤 변환을 사용하여 사용자의 입력 편의성 및 공격자에 대한 보안성을 향상시켰다.

3.1 키 패드 색 결정

키 패드 생성 및 색상 선정 알고리즘은 기존의 H. Kim의 방법과 같다. 그러나 다수의 공격자에 의한 색상 및 입력 위치 추정에 대한 대응 방법으로써 기존의 방법에 키를 입력할 때마다 키의 색상이 랜덤으로 변환하는 함수를 추가하였다. 다음의 Fig. 4의 pseudo code는 보안 키패드 생성과 키패드 색상에 대한 처리를 나타낸다.

아래의 Fig. 4와 같이 제안 방법은 키패드 생성

Initialize : /keyboard & key-color generating process

1. generate(qwerty_keyboard)
2. generate(random_color masking) / by 4-color theorem
   color definition with 4-colors
   neighbor key colors are not duplicated each other.

Main Processing: /color masking process by 4-color theorem after each key stroke

1. input(user_key_stroke) / by users
2. regenerate(qwerty_keyboard)
3. reassignment(random_color masking with {Key_color, Key_position}) / by 4-color theorem
   color definition with 4-colors
   neighbor key colors are not duplicated each other.

Fig. 4. Pseudo code of secure keyboard generation & color assignment.

후, 각각의 키에 색을 결정할 때 기존의 방법과 같이 4색 이론의 키 색을 적용하여 키보드를 생성한다. 그러나 제안 방법은 사용자의 키 입력을 감지하여 각각의 키 입력마다 키보드에 할당된 키 색을 랜덤하게 변경하는 알고리즘을 추가하여 외부 공격자의 지속적인 관찰로 인한 키보드 색 추정이 불가능하게 한다. 다음의 Fig. 5는 제안하는 방법의 초기 키보드 색상 배열과 1번의 키 입력 후 변경된 키보드 색상 배열을 나타낸다.

3.2 색약 모드

우리는 기존의 방법에 기존과 다른 색 변환 알고리즘과 색약 모드를 적용하였다. 기존의 방법은 4색 이론을 적용하여 이용자가 색깔을 이용하여 입력 정보 노출을 차단하였으나 기존의 색은 각각 빨강, 노랑, 파랑, 노란색으로 색맹이나 색약의 경우 구분이 어려우므로 우리는 기존의 방법에 더하여 색약 모드를 추가함으로써 색약자가 인지하기 어려운 색을 제외한 다른 색을 사용할 수 있도록 보완하였다. 다음의 Fig. 6은 제안하는 방법의 색약 모드 알고리즘의 pseudo code이다.

다음의 Fig. 7은 제안하는 방법에서 색약 모드를 사용했을 경우를 나타내는 예시이다. Color blind mode는 두 가지로 구분되며, Red & Green weak모드는 Green을 검은색으로 표현하는 모드이고 Yellow & Blue weak 모드는 Yellow를 회색으로 표현하는 모드이다. 이를 통해 기존의 사용자와 색약자 모두 색 기반 보안 키보드를 사용할 수 있다.

3.3 입력 정보 표현

기존의 방법은 입력된 정보를 표현하는데 별표를 사용하였으며, H. Kim의 방법은 별표에 색상 정보를 입혀서 표시하였다. 그러나 이 방법들은 색맹 및 색약, 그리고 저시력자의 경우 문자의 형태와 크기가 색 판독에 어려운 점이 있어 사용자가 입력한 비밀 문자의 색 정보를 비교하기 어렵다. 이에 우리는 다음의 Fig. 8과 같이 기존의 별표에 색상 정보를 포함하여 표시하던 것을 수정하여 공백 문자를 사용함으로써 사용자가 쉽게 색상 정보를 확인할 수 있도록 하였다.

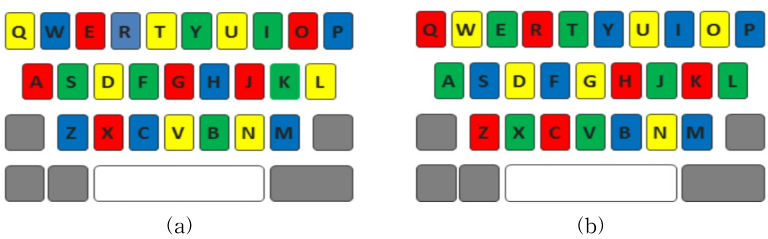

Fig. 5. color pattern re-assignment of proposed method (a) color pattern of initial stage (b) color pattern of one key stroke.

Initialize : /keyboard & key-color generating process

1. generate(qwerty_keyboard)
2. generate(random_color masking) / by 4-color theorem
   color definition with 4-colors
   neighbor key colors are not duplicated each other.

Main Processing: /color blind mode process

1. push(color_blind_mode button) / by users
2. choose(color_blind_mode_option) / by users
3. regenerate(qwerty_keyboard_color_masking)
   generate(substitution_color masking) / green-to-black, yellow-to-gray
4. reassignment(random_color masking with {Key_color(including_substitution_color), Key_position}) / by 4-color theorem
   color definition with 4-colors
   neighbor key colors are not duplicated each other.

Fig. 6. Pseudo code of color blind mode & color assignment.

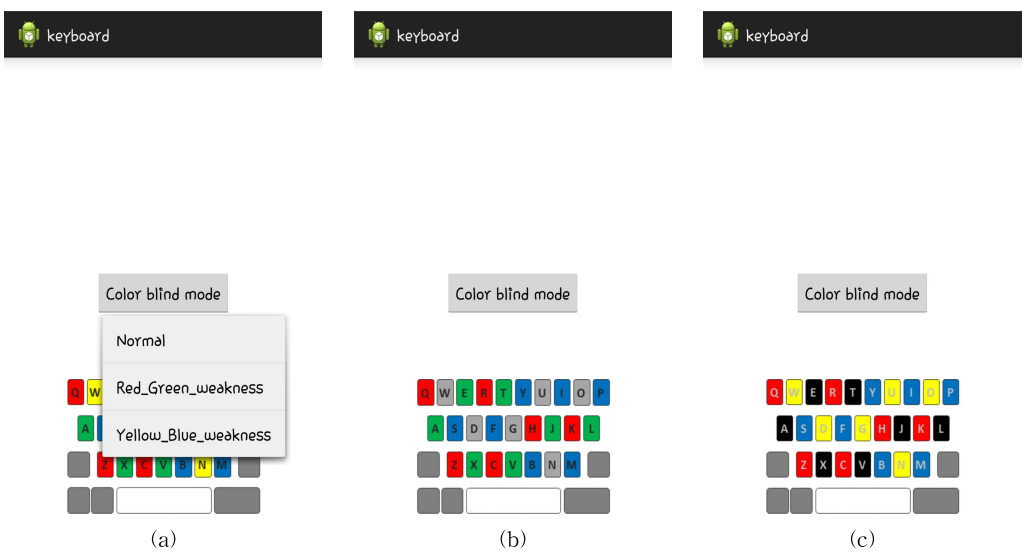

Fig. 7. Example of color blind mode (a) color blind mode button (b) yellow_blue weakness (c) red_green weakness.

4. 성능 평가

이 장에서 우리는 단순 shoulder surfing attack과 지속적인 관찰에 의한 continuous shoulder surfing attack에 대한 실험을 진행하였다. 실험에는 다음의 Table 1과 같은 3종의 모바일 폰이 사용되었으며 단순 shoulder surfing attack은 공격자가 사용자 모바일 폰 상단의 입력문자 확인 창만 볼 수 있게 하였다. 지속적인 관찰에 의한 continuous shoulder surfing attack에서는 공격자가 사용자 모바일 폰의 가상 키보드의 일부를 볼 수 있도록 하였다. 사용자가 비밀 정보를 입력하는 시간은 연령별로 다양하므로 해당실험에서는 모두 동일한 입력 속도(100타/분)를 갖는 것으로 사전에 정의하여 성능 평가를 진행하였다. 성능 평가를 위해 우리는 기존의 3가지 방법인 모든 문자가 별표로 마스킹 되는 secure virtual keyboard 방법과, 사용자 편의를 위해 마지막 문자가 마스킹되지 않는 방법인 modified basic virtual keyboard, 그리고 H. Kim에 의해 제안된 4색 기반의 4-color based virtual keyboard를 비교대상으로 하

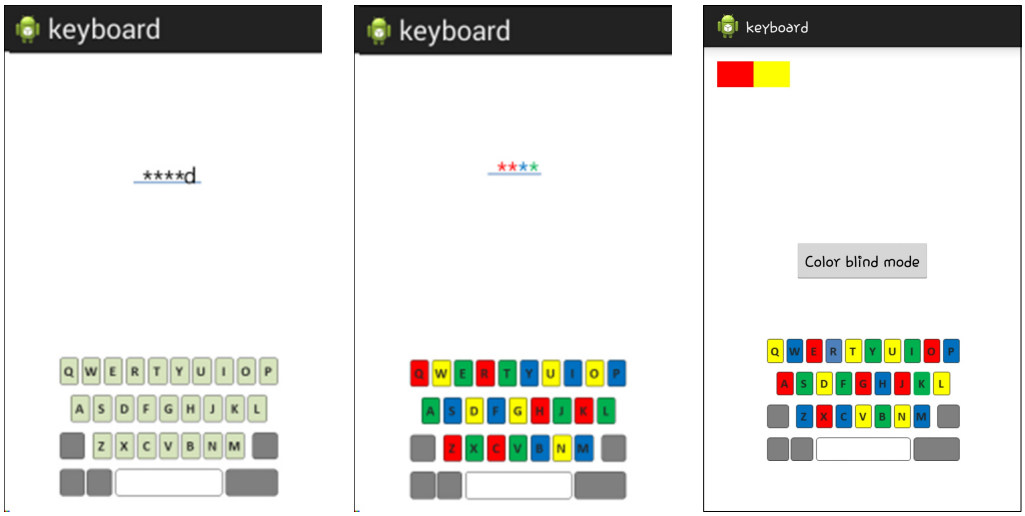

Fig. 8. Comparison of indicating method for user keystroke. (a)basic secure keyboard, (b) H. Kim's secure keyboard, and (c) proposed secure keyboard.

Table 1. Device specifications

Specification	Samsung galaxy S2	Samsung galaxy S3	Samsung galaxy S4
Resolution (px)	480 × 800	720 × 1280	1920 × 1080
Screen size (inches)	4.3	4.8	5
Key size (cm)	0.5*0.8	0.6*0.75	0.6*0.85
Screen brightness	50%	50%	50%

여 성능평가를 수행하였다.

4.1 단순 Shoulder Surfing Attack에 대한 안전성

다음의 Fig. 9는 단순 shoulder surfing attack에 의한 사용자입력정보의 유출 비율을 나타낸다.

단순 shoulder surfing attack은 모바일 폰 상단의

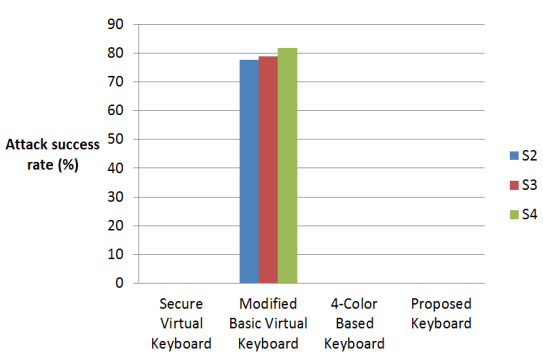

Fig. 9. Comparison of robustness against simple shoulder surfing attacks.

사용자 입력문자 확인 창만을 볼 수 있으므로 사용자 입력문자의 마지막 문자가 마스킹되지 않는 basic virtual keyboard를 제외한 모든 방법이 공격자로부터 안전하다. 그리고 비밀문자 입력 속도를 동일하게 할 경우 변인으로 작용하는 화면 크기가 공격에 어느 정도 취약한 부분이 있음을 실험 결과로부터 도출할 수 있다. 따라서 화면 크기는 공격 성공률에 영향을 크게 미치는 요인으로 작용하고 있으며 큰 화면은 곧 큰 가상 키보드의 크기와 입력 정보 확인창의 입력문자의 크기가 커지게 되어 일반적인 경우 큰 화면을 갖는 스마트폰은 보다 더 공격에 취약하다고 볼 수 있다.

4.2 지속적인 관찰에 의한 Continuous Shoulder Surfing Attack에 대한 안전성

다음의 Fig. 10은 지속적인 관찰에 의한 continuous shoulder surfing attack에 의한 사용자 입력정보의 유출 비율을 나타낸다.

Table 2. comparison result of typographical errors about color blind users

User Convenience	Secure Virtual Keyboard	Modified Basic Virtual Keyboard	4-Color Based Keyboard	Proposed Keyboard
Typographical Errors	Low	Lowest	High	Lowest

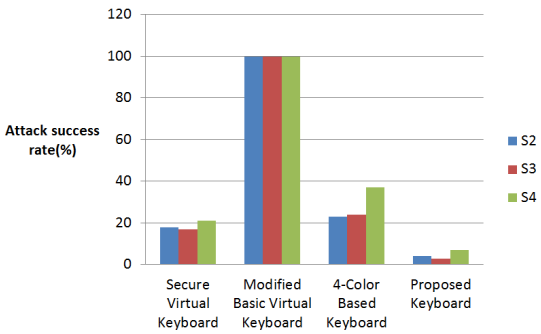

Fig. 10. Comparison of robustness against continuous shoulder surfing attacks.

지속적인 관찰에 의한 continuous shoulder surfing attack은 사용자가 입력하는 키보드의 일부를 관찰 할 수 있으므로 입력값에 대한 추정이 가능하다. 색을 적용하지 않는 기존의 두 가지 방법들 중 모든 입력값을 별표로 마스킹 하는 경우 사용자가 입력하는 키보드 문자의 일부를 볼 수 있으므로 입력값에 대한 추정을 할 수 있어 공격 성공률 단순 공격에 비해 높게 측정되었으며, 마지막 입력값을 마스킹하지 않는 경우 매우 높은 확률로 입력값의 추정이 가능하여 모든 비밀 정보가 유출되는 결과를 보였다. 기존의 4색 이론을 적용한 방법의 경우 키보드에 입힌 색이 고정되어 있어 공격자 측면에서 볼 때 오히려 첫 번째 방법에 비해 상대적으로 높은 확률로 입력값에 대한 추정이 가능하여 일부의 비밀 정보가 유출되는 결과를 보였다. 제안하는 방법의 경우 기존의 4색이론이 적용된 방법보다 화면에 표시되는 색깔 정보를 분명히 확인할 수 있음에도 매 입력마다 랜덤하게 변화하는 키 색깔로 인해 공격자가 혼동을 일으키는 경우가 자주 발생하여 입력값의 추정이 힘들어지는 결과를 보였다.

4.3 사용자 입력 편의성

색약 사용자 입력 편의에 대한 평가로 입력오류 발생률을 측정한 결과, 제안하는 방법은 색약 모드를 지원하는 점으로 인해 기존의 4색 이론이 적용된 방법에 비해 매우 낮은 수준의 입력에러가 발생하였다. 다음의 Table 2는 입력에러 발생률에 대한 결과를 나타낸다.

5. 결론 및 향후 연구

본 연구에서 우리는 색약 사용자의 입력 편의성을 고려하면서 외부 공격에 안전한 가상 키보드를 제안하였다. 최근의 스마트폰은 화면 크기가 대형화되어 가면서 shoulder surfing attack 과 같은 유형의 공격으로부터 사용자 비밀정보의 유출이 증가하는 추세에 있다. 따라서 대화면 단말 사용자 환경에서 사용자 입력을 안전하게 보호할 수 있는 보안 키보드의 개발은 필요불가결하다. 실험 결과에 의하면 제안방법은 기존방법에 비해 단순공격뿐만 아니라 지속공격에도 강인한 결과를 보였으며 색약과 같은 사회적 약자에게도 충분한 입력 편의성을 제공하는 결과를 보였다. 향후 연구에서는 사용자의 상태를 고려한 더욱 발전된 입력편의성을 보장하며 내·외부의 공격에 안전한 가상키보드를 제안하고자 한다.

REFERENCE

[1] M. Agarwal, M. Mehra, R. Pawar, and D. Shah, “Secure Authentication using Dynamic Virtual Keyboard Layout,” *Proceeding of the International Conference & Workshop on Emerging Trends in Technology*, pp. 288-291, 2011.

[2] Y. Park and M. Yoon, “Distributed One-Time Keyboard Systems,” *IEICE Transactions on Information and Systems,* Vol. E96-D, No. 12, pp. 2870-2872, 2013.

[3] H. Kim, H. Seo, Y. Lee, T. Park, and H. Kim, “Implementation of Secure Virtual Financial Keypad for Shoulder Surfing Attack,” *Korea Institute of Information Security and Cryp-*

tography, Vol. 23, No. 6, pp. 21-29, 2013.
[4] Okazaki Laboratory shoulder-surfing Attack Resistant Authentication Methods(2014), http:// knowledgecenter.comarch.com (accessed Dec. 24, 2014).
[5] S. Choi, K. Jeong, and H. Moon, "Enhancement of Authentication Performance based on Multimodal Biometrics for Android Platform," *Journal of Korea Multimedia Society,* Vol. 16, No. 3, pp. 302-308, 2013.
[6] A.H. Lashkari, S. Farmand, O.B. Zakaria, and R. Saleh, "Shoulder Surfing Attack in Graphical Password Authentication," *International Journal of Computer science and Information Security,* Vol. 6, No. 2, pp. 145-154, 2009.
[7] D. Jungnickel, *Graphs, Networks and Algorithms,* Springer, Berlin Heidelberg, 2013.
[8] D. Lee, *Mobile Payment: Innovative Trends, Implications,* Technical Report 7, Bank of Korea, 2013.
[9] D. Nyang, A. Mohaisen, and J. Kang, "Keylogging-resistant Visual Authentication Protocols," *IEEE Transactions on Mobile Computing*, Vol. 1, No. 8, pp. 2566-2579, 2014.
[10] D. Mclntyre, *Colour Blindness: Causes and Effects*, Dalton Publishing, UK, 2002.
[11] Color Blind Mode(2014), https://support.riotgames.com/hc/en-us/articles/201752844 (accessed Dec., 23, 2014).
[12] League of Legends(2014), http://forums.na.leagueoflegends.com/board/showthread.php?p=33632375 (accessed Dec., 23, 2014).
[13] World of Tanks(2014), http://forum.worldoftanks. com/index.php?/tags/forums/Colorblind/ (accessed Dec., 23, 2014).
[14] World of Warcraft(2014), https://us.battle.net/support/en/article/color-blind-mode (accessed Dec., 23, 2014).
[15] Modue Game(2014), https://play.google.com/store/apps/details?id=com.hotdog.tinybattle&hl=ko (accessed Dec., 23, 2014).
[16] TouchEn mTranskey(2014), http://touchen.raonsecure.com/mobile/mobile_02.php (accessed Dec., 23, 2014).

최 동 민

2003년 경희대학교 공과대학 졸업(공학사)
2007년 조선대학교 교육대학원 졸업(교육학석사)
2012년 조선대학교 일반대학원 컴퓨터공학과(공학박사)
2012년~2013년 조선대학교 BK사업팀 연구교수
2014년~현재 조선대학교 자유전공학부 조교수
관심분야 : 정보 보안, 센서 네트워크, 모바일 애드혹 네트워크

백 철 헌

2014년 조선대학교 전자정보공과대학 졸업(공학사)
2014년 조선대학교 일반대학원 컴퓨터공학과(석사)
관심분야 : 센서 네트워크, 정보 보안, 안드로이드 통신

정 일 용

1983년 한양대학교 공과대학 졸업(공학사)
1987년 City University of New York 전산학과(전산학석사)
1991년 City University of New York 전산학과(전산학박사)
1991년~1994년 한국전자통신연구소 선임연구원
1994년~현재 조선대학교 컴퓨터공학부 교수
관심분야 : 네트워크 보안, 병렬 알고리즘, 모바일 애드혹 네트워크