Journal of Convergence for Information Technology
Vol. 12. No. 3, pp. 38-45, 2022
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2022.12.03.038

핀테크 환경에서 그룹핑을 이용한 이중 터치 기반의 위치 차단이 가능한 보안 키패드 설계

문형진
성결대학교 정보통신공학부 조교수

Design for Position Protection Secure Keypads based on Double-Touch using Grouping in the Fintech

Hyung-Jin Mun
Assistant Professor, Dept. of Information & Communication Engineering, Sungkyul University

요 약 핀테크 기술의 발전으로 인해 스마트폰을 이용한 금융거래가 활성화되고 있다. 금융거래시 사용자 인증을 위한 비밀번호는 스마트 폰의 터치 스크린 상에 보여지는 가상 키패드를 통해 입력된다. 비밀번호를 터치할 때 공격자가 높은 해상도를 가진 카메라로 촬영하거나 어깨 너머로 훔쳐보는 방식으로 사용자가 입력한 비밀번호를 알아낼 수 있다. 이런 공격을 막기 위해 보안이 적용된 가상 키패드는 크기가 작은 터치 스크린에 입력하기 어렵고, 훔쳐보기 공격에 취약점이 여전히 존재한다. 본 논문에서는 전체 키패드를 몇 개의 그룹으로 나누고 작은 화면에 표시하여 입력할 문자가 속해 있는 그룹을 터치하고, 그룹 내에서 해당 문자를 터치하는 방식으로 입력할 문자를 쉽게 찾을 수 있다. 제안기법은 입력할 문자가 속한 그룹을 선택하며 해당 그룹에 키패드를 10개 이내로 작은 스크린에 보여주기 때문에 키패드의 크기를 기존 방법보다 2배 이상 확대가 가능하고, 위치를 랜덤하게 배치하여 터치한 위치를 통한 공격을 차단할 수 있다.

주제어 : 핀테크, 보안 키패드, 그룹핑 패드, 어깨너머공격, 가상 키패드, 비밀번호, 이중 터치

Abstract Due to the development of fintech technology, financial transactions using smart phones are being activated. The password for user authentication during financial transactions is entered through the virtual keypad displayed on the screen of the smart phone. When the password is entered, the attacker can find out the password by capturing it with a high-resolution camera or spying over the shoulder. A virtual keypad with security applied to prevent such an attack is difficult to input on a small touch-screen, and there is still a vulnerability in peeping attacks. In this paper, the entire keypad is divided into several groups and displayed on a small screen, touching the group to which the character to be input belongs, and then touching the corresponding character within the group. The proposed method selects the group to which the character to be input belongs, and displays the keypad in the group on a small screen with no more than 10 keypads, so that the size of the keypad can be enlarged more than twice compared to the existing method, and the location is randomly placed, hence location of the touch attacks can be blocked.

Key Words : Fintech, Secure Keypads, Grouping Pads, Shoulder Surfing Attack, Virtual Keypads, Password, Double touch

*Corresponding Author : Hyung-Jin Mun(jinmun@gmail.com)
Received February 14, 2022
Revised March 6, 2022
Accepted March 20, 2022
Published March 28, 2022

1. 서론

ICT 발달로 스마트폰의 기하급수적인 사용으로 이어져 다양한 서비스가 스마트폰 기반 서비스로 전환되고 있다. 특히, 핀테크 기술의 발전으로 스마트 폰을 이용하여 빈번하게 거래 및 결제가 이루어지고 있다. 스마트 폰에서 작은 디스플레이에서 정보를 제공하고 터치를 기반으로 입력받고 있지만 이로 인해 문제점을 가지고 있다. 금융 거래의 활성화로 PC 환경에서의 공격이 모바일 단말기에서 그대로 이루어지고 있다[1,2]. 스마트폰에서 SNS 및 SMS를 통한 피싱, 파밍, 스미싱 공격이나 어깨너머 공격(Shoulder surfing attack)과 같은 사회공학기법 공격이 주를 이루고 있다[3-6].

스마트 폰에서 SMS 나 SNS 등을 이용한 사회적공학기법을 이용한 바이러스 감염 및 불법 파일로 인한 멜웨어 설치, 키로깅 공격 등 다양한 공격이 가능하여 이를 이를 막기 위한 연구들이 이루어지고 있다[3-7].

핀테크에서 모바일 단말기의 급증으로 스마트폰을 이용한 금융거래가 많아지고 있다[8,9]. 스마트폰을 이용한 금융거래의 안전한 거래를 위해 다양한 인증 기법이 제시되고 있다. 스마트 폰으로 전달된 SMS를 기반으로 인증하거나 FIDO(Fast Identity Online)기술을 활용한다. FIDO 기술은 온라인 환경에서 ID 인증 없이 스마트폰을 이용한 지문이나 홍채, 안면인증 등 생체인증을 활용하여 편리하고 안전하게 인증하는 방식이다[10].

몰래 엿보는 공격을 어깨너머 공격이라고 하고, 고해상도 촬영이 가능한 카메라로 사용자의 입력하는 손동작을 촬영하거나 입력하는 것을 엿보는 공격으로 입력정보를 유추할 수 있다[6,11,12].

스마트 폰에서 안전한 금융거래를 위해 보안 키패드가 제공되어 인증서 비밀번호 및 계좌 비밀번호를 입력한다. 금융기관에서는 쉽게 입력하기 위해 PC자판(PC keyboard)과 같은 배열을 가진 QWERTY 키패드를 제공하거나 알파벳 순서로 배치된 ABC 키패드를 제공한다[13,14]. 하지만, 스마트 폰의 터치 스크린의 크기가 작아 터치가 어렵고, 다른 문자를 터치하는 실수 많아지는 단점을 가진다. 또한, 공격자가 입력하는 PIN를 탈취하기 위해 스마트 폰에 키로거(Keylogger)를 몰래 설치한 상태에서 사용자가 터치한 위치(좌표 값)이 탈취할 경우 보안 키패드에 입력되는 정보를 유추할 수 있다[7,14].

고해상도의 카메라를 이용한 촬영이나 어깨 너머 훔쳐보기 공격으로부터 사용자의 입력 정보의 노출을 막기 위한 연구들이 진행되고 있다. 키패드 모양을 변경하거나 키패드의 위치를 랜덤하게 배치하는 방법이 제시되었지만 입력 문자를 찾는 데 어려움이 있거나 터치에 불편함이 있다.

촬영이나 훔쳐보기의 공격을 막을 수 있는 보안 키패드를 설계하기 위해 다음과 같은 요구사항이 요구된다.

키패드의 크기를 보장하여 사용자가 터치할 때 잘못 터치하는 실수를 줄어야 한다.

입력할 키패드의 위치를 빠르게 찾아서 터치할 수 있어야 한다.

입력한 문자가 맞는지 확인하기 위해 사용자에게 보여줄 경우 훔쳐보기 공격을 회피할 방안이 필요하다.

2. 관련 연구

2.1 가상 키패드

사용자는 스마트 폰에서 비밀번호를 터치 스크린에 제공되는 가상 키패드로 입력한다. 하지만 터치 스크린에 실수없이 쉽게 PIN를 입력해야 하지만 스마트 폰의 터치 공간의 제약으로 가상 키패드 생성시 여러 가지 사항을 고려해야 한다. 많이 사용되는 가상 키패드는 QWERTY 키패드와 ABC 키패드가 있고, Fig. 1는 QWERTY 키패드이고, Fig. 2는 ABC 키패드이다[15].

1	2	3	4	5	6		7	8	9	0
q		w	e	r	t	y	u	i	o	p
a	s		d	f	g	h		j	k	l
↑	z	x	c	v		b	n	m	↵	
#+=			SPACE					OK		

Fig. 1. QWERTY Keypads

a	b	c	d		e	f	g		h
i		j		l	m	n	o	p	q
r	s	t	u	v	w	x		y	z
Shift			?123		←			CLOSE	

Fig. 2. ABC Keypads

현재, QWERTY 키패드와 ABC 키패드는 일반적으로 많이 사용되지만 왼쪽이나 오른쪽 측면의 키패드가 고정되어 있고, 그 이외의 키패드는 한 칸이나 두 칸만 이동되어 노출된 터치 정보를 활용하여 PIN를 유추하

거나 이미 알아낸 PIN 정보를 활용하여 유추할 수 있다. 예를 들어, 사용자의 PIN이 “asdfgh” 일 때 공격자가 “asecgh”를 알아낸 경우 ec가 df라고 유추하거나 각 문자에 대한 예상 문자를 도출하여 후보가 될 PIN를 계속적으로 입력하는 방식으로 알아낼 수 있다.

2.2 단순한 보안 키패드

QWERTY 키패드와 ABC 키패드는 터치하는 위치를 파악할 경우 PIN이 노출될 가능성이 높아 이를 해결하기 위해 키패드 위치를 변경하는 기법이 제시되고 있다.

QWERTY 키패드에서 각 열 마다 반 칸의 공백을 추가하거나 각 열의 키패드를 재배치하는 형태의 물결형 보안 키패드(Ripple type)가 있다[15,16]. 열 마다 반 칸 채우는 방식은 QWERTY 키패드와 비슷하여 입력 편리성은 좋으나 입력 위치를 통한 공격은 기존 키패드와 비슷하다.

QWERTY 키패드의 4개 행에서 임의의 행을 선택하여 복사하여 추가하는 클론 키패드(clone)는 QWERTY 키패드과 비슷하여 키패드의 위치를 찾기 쉽고 중복된 행의 키패드에 대해 공격이 상대적으로 안전하지만 한 개의 행이 추가되어 키패드가 전체적으로 작아지는 단점이 있다.

ABC 보안 키패드 기반으로 한 키패드의 화살표를 터치하여 좌우로 키패드를 이동시키거나 슬라이드를 이용하여 입력한 문자를 찾고 터치를 통해 PIN을 입력하는 좌우 슬라이드 보안 키패드(touch & slide)가 있지만 ABC 방식이라 PC자판에 익숙하지 않는 사용자에게 편리하지만 원하는 문자가 나올 때까지 이동시키거나 슬라이드하여 PIN 입력해야 한다.

2.3 개선된 보안 키패드

2.3.1 시작 위치 랜덤 배치 보안키패드

서화정이 제안한 보안 키패드는 Fig. 3과 같이 QWERTY 키패드에서 “1”의 위치를 임의의 위치에 배치한 변경한 QWERTY 키패드이다. 사용자가 먼저 “1”의 위치를 찾은 후, “1”를 기준으로 QWERTY 자판을 기억해야 입력할 문자를 찾을 수 있기때문에 다른 키패드보다 입력하기 어렵다[13,17]. 또한, ‘1’의 위치가 매번 변경되어 위치에 의한 공격에 안전하지만 QWERTY 자판의 배열에 익숙하지 않을 경우 사용하기 어렵다.

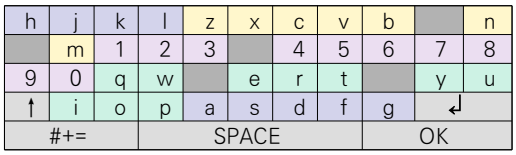


Fig. 3. Keypads proposed by Seo

2.3.2 테트리스 모양 보안 키패드

가상 키패드를 테트리스 모양으로 생성하여 QWERTY 기반의 배치한 보안 키패드이다[18-20].

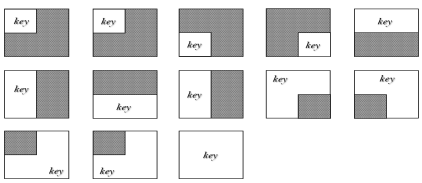


Fig. 4. Number of cases arranged in quadrisection

테트리스 모양의 키패드는 기존 키패드보다 작은 형태로 Fig. 4와 같이 13개의 형태를 가지며 테트리스 형태로 연결한 보안 키패드이다. 테트리스 모양의 키패드는 기존 키패드보다 작고, 테트리스 게임처럼 연결상태를 가질 수 있어 많은 여백을 확보하여 기존 보안 키패드보다 위치 기반 공격에 강하다. 13개의 테트리스 형태 키패드를 영문자 입력에서 적용된 사례는 Fig. 5와 같다. 더 많은 여백이 확보되어 사용자가 왼쪽이나 오른쪽을 문자 키패드를 배치하지 않을 수 있기 때문에 기존 기법에서 왼쪽과 오른쪽 터치시에 가지는 취약점으로부터 안전하다.

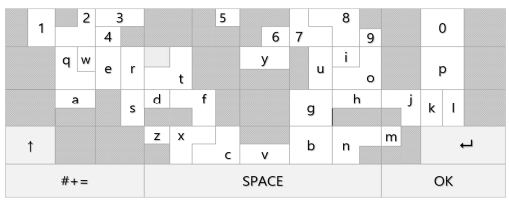


Fig. 5. Example of secure keypad with tetris type

하지만, 테트리스의 특성으로 문자 간에 여백이 많아 위치에 대한 보안 안전성을 높일 수 있지만 기존 키패드의 1/4, 1/2, 3/4, 1크기로 인해 터치시 실수가 많은 단점을 가진다[17-19].

2.3.3 이중 터치 기반 숫자 보안 키패드

Fig. 6은 숫자 키패드에 2개의 숫자를 입력할 수 있는 형태이다. Fig. 6은 어깨너머 공격, 무차별 대입 공격(Brute force attack), 키로깅 공격(keylogging attack) 등의 취약점을 해결하기 위해 키패드마다 각각 2개의 숫자(n/M)로 이루어진 키패드이다.

3/7	2/4	5/1
4/5	1/9	7/6
6/8	8/2	0/3
	9/0	OK

Fig. 6. Numeric keypad example with double touch

하나의 키패드에 2개의 숫자를 표시하되, 왼쪽은 작은 크기로, 오른쪽은 큰 크기의 숫자가 표시하여 키패드를 1초 이상 터치하면 왼쪽 숫자가 입력되고 1초 미만 터치하면 오른쪽 숫자가 입력되는 방식이다. 훔쳐보기 공격에 강하지만 숫자 키패드만 가능한 방법으로 알파벳을 적용하기 어렵다[20].

2.4 어깨 너머 공격을 회피 개선기법

사용자가 터치된 문자가 터치 스크린에 *로 표시되어 입력한 문자를 확인하기 위해 터치한 마지막 문자는 보여준다. 하지만 촬영이나 훔쳐볼 수 있다는 취약점을 가진다.

2.4.1 4색 정리

4색 정리(Four Color Theorem)은 평면의 유한 개의 부분으로 나누어 색을 표시할 때 서로 경계선 부분을 다른 색으로 표시가 가능하다는 정리이다. 즉, 키패드의 주변을 4개 컬러로 모든 키패드로 표현할 수 있다[21]. 즉, 사용자가 ⓓ를 터치할 경우 ⓓ의 주변 키패드인 s, e, f, c가 터치될 수 있다. 잘못 터치하는 것을 막기 위해 각 키패드에 색을 표시하여 색을 확인하여 잘못 터치한지를 확인할 수 있다.

2.4.2 마지막 입력 확인

서화정은 PIN을 모두 입력하기 전까지 입력된 숫자나 문자를 모두 *로 표시되고, 입력이 완료되었을 때 입력된 비밀번호를 출력하는 기법을 제안하였다[22]. PIN을 입력하는 과정에서의 비밀번호를 노출하지 않지만 마지막에 입력이 완료된 상태에서 비밀번호 전체가 노출되는 단점을 가진다. 비밀번호를 입력하는 모습을 촬영할 경우 비밀번호 전체를 노출된다.

3. 제안기법

제안 기법은 가상 키패드에 보여지는 모든 문자를 4~6개의 그룹으로 나누고, 처음에는 그룹을 선택하고, 그 다음 단계는 선택된 그룹에서 그룹의 문자를 랜덤하게 배치하여 입력할 문자를 터치하는 방식이다.

3.1 더블 터치 가상 보안 키패드

제안한 보안 키패드는 PC자판을 그룹핑하여 보여주고, 처음에는 그룹을 선택하고, 선택된 문자를 두 번째 키패드를 보여주는 방식의 보안 키패드이다.

가상 키패드는 PC자판 형태로 10개 숫자 키패드, 26개의 영문자 키패드, 32개의 특수문자 키패드로 구성되어 있다. Fig. 7은 제안 기법에서 하나의 예시로 4개의 그룹으로 나눈 상태로 첫 화면(Fig. 7(a))에 제시한다.

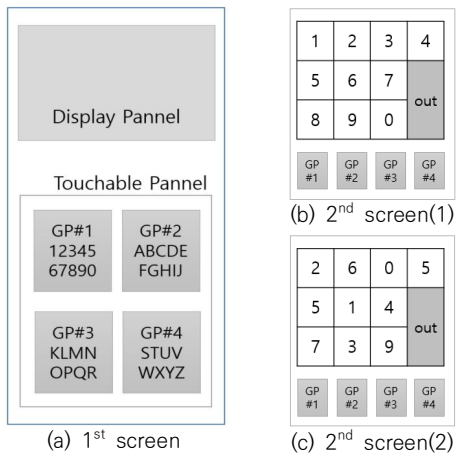


Fig. 7. Secure keypad screen of the proposed Method

원하는 그룹을 선택하면 해당 그룹의 모든 키패드를 다음 단계에서 제공된다. Fig. 7(b)과 Fig. 7(c)와 같이 GP#1를 선택한 경우 “1 2 3 4 5 6 7 8 9 0” 숫자를 한번에 보여준다. 사용자는 입력할 문자를 터치하면 디스플레이에서 터치한 문자에 해당되는 색을 표시하여 입력된 문자가 맞는지 확인한다. 두번째 문자가 같은 그룹에 있을 경우 다시 추가적으로 입력한다. 두번째

문자가 같은 그룹에 있지 않을 경우 첫 화면으로 바로 가거나 그룹의 번호를 알 경우 바로 그 그룹번호를 터치하여 바로 해당 그룹 키패드로 넘어간다. 해당 그룹에서 원하는 문자를 터치하여 입력한다.

처음 터치는 그룹을 선택하고, 두 번째 터치는 그룹에서 원하는 문자를 택하는 방식이기 때문에 원하는 문자를 쉽게 터치할 수 있고, 위치도 랜덤하게 배치하기 때문에 위치기반공격에 강한 키패드이다.

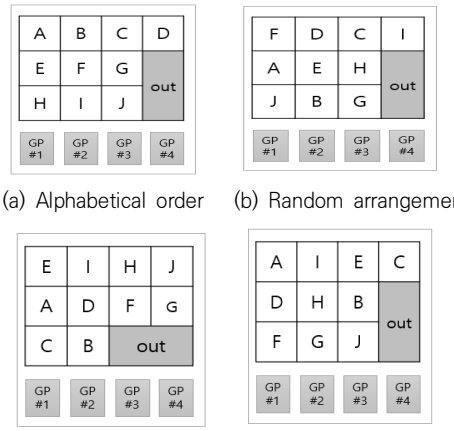
사용자는 입력할 비밀번호가 있는 그룹을 선택하고, 선택된 그룹이 두 번째 화면에 디스플레이에 선택된 그룹에 속한 모든 자판을 보여준다.

그 그룹의 선택된 키패드를 랜덤하게 배치하여 보여준다. 그 보여준 키패드를 터치하여 비밀번호를 입력한다. 즉, 원하는 문자를 2번 터치하여 입력한다.

그룹을 선택한 후 두 번째 단계 화면에서 그룹의 키패드를 배치하는 방법은 다양하게 존재한다. Fig. 7에서 숫자를 선택했을 때 예시는 Fig. 8과 같다.

- 알파벳 순이나 수의 오름차순으로 배치하는 방법 : Fig. 8(a)과 같이 그룹에 있는 키패드 간에 순서를 정하고, 배치하는 방법으로 키패드를 찾기 쉽다. 위치가 고정되어 터치한 위치를 파악할 경우 유추 가능성이 존재하지만 그룹내 자판을 이동하여 공격으로 회피할 수 있다.
- 랜덤하게 배치하는 방법 : Fig. 8(b)과 같이 키패드의 순서를 섞어서 배치하는 방법으로 원하는 키패드를 찾는 데 어려움은 존재하지만 10개 이내이므로 어렵지 않게 찾을 수 있다. 매번 터치할 때마다 랜덤하게 변경할 수 있어 터치한 위치에 대한 공격에 강하다.
- PC자판과 같은 방식으로 배치하는 방법 : Fig. 8(c)과 같이 PC자판에 익숙한 사용자에게는 빠르게 키패드를 찾을 수 있어 입력 편리성이 있지만 위치가 고정되는 부분이 있어 터치한 위치를 파악할 경우 유추 가능성이 존재한다. 그룹내 자판을 이동하여 공격으로 회피할 수 있다.
- 영어 사전에 많이 사용된 빈도수에 따라 배치하는 방법 : Fig. 8(d)과 같이 고전 암호학에서 빈도분석을 이용한 공격으로 해독하는 기법으로 사용자가 많이 사용되는 문자를 기반으로 배치하여 원하는 문자를 쉽게 찾을 수 있다. 영어 사전의 많이 사용되는 알파벳의 빈도수에 따라 4개의 그룹을 1)EARIOTN 2)SLCUDPMH 3)GBFYWKV 4)XZJQ 로 나눌 수 있다.

Fig. 8은 첫화면에서 그룹(GP#2)를 선택한 후, 두 번째 단계에서 (a)는 빈도수가 높은 문자를 알파벳순으로 배치한 모습이고, (b) 랜덤하게 배치된 모습이고, (c)는 알파벳순으로 배치된 모습이다. (d)는 PC자판 2번째 행의 문자를 순서대로 첫줄에 배치하고, 3번째 행의 문자를 2번째 줄에 배치하고, 4번째 행의 문자를 3번째 줄에 배치하되, 공간이 부족한 경우 남는 곳에 배치하는 방식이다.

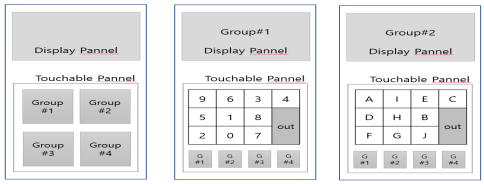


(a) Alphabetical order (b) Random arrangement

(c) PC keyboard order (d) Frequency basis

Fig. 8. Method of Keypad Generated in the 2nd stage

사용자가 입력하는 편리성과 안전성을 고려하여 선택하는 방식으로 운영이 가능하다. 다음 문자를 입력할 때 같은 그룹에 속하는 경우에는 첫화면으로 이동하지 않고, 바로 입력이 가능하고, 다른 그룹에 속하는 문자일 경우 하단의 그룹 버튼을 클릭하거나 “out” 버튼을 이용하여 해당 그룹으로 이동한다.



(a)1st step (b) 2nd step (c) 2nd* step

Fig. 9. PIN input process

Fig. 9는 PIN를 입력하는 절차를 보여주고 있다. 숫자 7를 입력할 때 처음 화면(a)에서 그룹을 선택하면 두번째 단계(b)로 넘어간다. 여기에서 원하는 문자를

입력하고, 입력이 완료된 상태에서 그 다음 ⑨ 라면 같은 그룹(b)에 있으면 보여지는 화면에서 해당 키패드를 터치한다. 같은 그룹에 없을 경우 ⑩ 를 터치하여 (a)로 넘어가거나 해당 문자가 속하는 그룹을 알 경우 해당 그룹을 선택한다. (c)는 G#2를 터치하여 해당 그룹으로 바로 들어간 모습이다. 만약에 모를 경우 첫화면(a)로 이동하여 해당 그룹을 찾아 선택한다.

4. 제안 기법의 분석 및 평가

디스플레이가 작은 스마트폰에서는 2가지 측면을 고려하여 보안 키패드를 설계해야 한다. 비밀번호 입력시 사용자의 입력 편리성을 높이기 위해 키패드의 쉽게 찾을 수 있어야 한다. 비밀번호 터치하는 시간을 줄이면 어깨 너머 공격 등과 같은 훔쳐보기를 차단하는 효과가 있다. 공격자가 훔쳐볼 수 있는 상황이라면 키패드의 위치를 변경시켜 비밀번호 유추를 어렵게 해야 한다.

4.1 터치 위치를 이용한 비밀번호 유추 방법

Fig. 10는 QWERTY 키패드의 첫 번째 행에 배치되는 문자열을 보여준다. Fig. 10에서 보듯이 6번째 공간을 터치했을 때 나올 수 있는 경우의 수는 공백(□), 5나 6이므로 공백이면 터치하지 않기 때문에, 5나 6으로 유추할 수 있다[6].

location	1	2	3	4	5	6	7	8	9	10	11
number of cases	□ 1	□ 1 2	□ 2 3	□ 3 4	□ 4 5	□ 5 6	□ 6 7	□ 7 8	□ 8 9	□ 9 0	□ 0

Fig. 10. Key types that is possible to be inserted in the first row

Fig. 11는 PC자판의 QWERTY 키패드에서 각 위치를 터치했을 때 예상되는 키의 값에 대한 확률을 나타낸 것이다[6,13,18]. Fig. 11에서 2행 4열(2 row, 4 col)를 터치가 했다면 e일 확률은 30%이고, r 일 확률이 70%이고, 3행에서는 경우의 수가 3개의 문자가 된다.

4.2 기존 기법과의 비교분석 및 논의

제안기법은 먼저 그룹을 터치한 후 그룹내에 원하는 문자를 터치하는 방식으로 서론에서 제시된 요구사항을 만족하고 있다.

제안기법에서 키패드의 크기를 보장하고 있다. 한번에 보여지는 문자의 개수는 10개 이하라서 크기조절이 가능하다.

그룹을 4~6개로 묶어서 손쉽게 선택하고 다음 단계에서 10개 이하의 문자를 사용자가 선정된 방식으로 다양하게 배치하여 쉽게 찾을 수 있다.

제안기법은 2번째 단계에서 터치한 문자의 컬러를 디스플레이에서 제시하여 오터치여부를 확인이 가능하다.

제안 기법에서 그룹 키패드를 터치한 후 그룹내의 키패드를 터치해야 하기 때문에 터치횟수가 늘어날 수 있는 단점을 가진다. 하지만, 비밀번호로 많이 사용되는 “password1”인 9개 문자에 대해 제안기법에서 터치할 경우 선택된 그룹의 번호는 324443321이므로 15번 터치하여 “password1”를 입력할 수 있다. 즉, 입력할 문자의 2배가 아닌 평균적으로 1.5배 정도의 터치만으로 원하는 비밀번호를 입력할 수 있다. 터치 횟수에 따른 불편함과 안전성 및 입력 편리성을 trade off 가능하다.

location / row	1 col	2 col	3 col	4 col	5 col	6 col	7 col	8 col	9 col	10 col	11 col
1 row	1 100%	1 10% 2 90%	2 20% 3 80%	3 30% 4 70%	4 40% 5 60%	5 50% 6 50%	6 60% 7 40%	7 70% 8 30%	8 80% 9 20%	9 90% 0 10%	0 100%
2 row	q 100%	q 10% w 90%	w 20% e 80%	e **30%** r **70%**	r 40% t 60%	t 50% y 50%	y 60% u 40%	u 70% i 30%	i 80% o 20%	o 90% p 10%	p 100%
3 row	a 100%	a 20% s 80%	a 2% s 36% d 62%	s 7% d 47% f 47%	d 13% f 53% g 33%	f 22% g 56% h 22%	g 33% h 53% j 13%	h 47% j 47% k 7%	j 62% k 36% l 2%	k 80% l 20%	l 100%
4 row	z 100%	z 14% x 86%	x 29% c 71%	c 43% v 57%	v 43% b 57%	b 29% n 71%	n 14% m 86%	m 100%			

Fig. 11. Key leak probability of secure keypad for each location

5. 결론

스마트폰의 발달과 급격한 보급으로 다양한 분야에서 스마트폰을 이용하고 있다. 특히, 핀테크 기술의 발달로 인해 스마트 폰을 이용한 금융거래에서 비밀번호를 터치하는 방식의 인증기법이 보편화 되어 있다. 하지만, 스마트 폰의 작은 디스플레이에서 사용자가 원하는 비밀번호를 터치하기 어렵고, 고해상도의 카메라의 촬영이나 어깨 너머로 훔쳐보는 공격에 취약하다. 스마트 폰의 터치한 위치를 탈취하여 입력한 PIN을 알아내는 공격으로부터 안전하게 보호하기 위한 많은 보안 키패드가 제안되었지만 입력할 문자를 찾기 어렵거나 터치하기 어려운 단점을 가지고 있다.

본 연구는 그룹핑된 이중 터치 보안키패드를 제안하여, 사용자가 터치할 키패드를 10개 이내로 제한하여 키패드의 크기를 확대하고 다양한 방법으로 재배치하여 위치 기반의 공격으로부터 안전하다. 향후 연구는 제안기법에서 그룹핑하는 방법과 두 번째 단계에서 배열방법에 따른 사용자의 경험과 편리성, 안정성 분석에 대한 연구가 필요하다.

REFERENCES

[1] E. J. Choi, W. C. Jung. & S. Y. Kim. (2015). Attacks and Defenses for Vulnerability of Cross Site Scripting. *Journal of Digital Convergence, 13(2),* 177-183.
DOI :10.14400/JDC.2015.13.2.177

[2] C. Nayak, M. Parhi & S. Ghosal. (2014). Robust virtual keyboard for online banking. *International Journal of Computer Applications*, *107(21),* 36-38.
DOI : 10.5120/19142-0530

[3] B. S. Yu & S. H. Yun. (2011). The Design and Implementation of Messenger Authentication Protocol to Prevent Smartphone Phishing. *Journal of the Korea Convergence Society, 2(4),* 9-14.
DOI : 10.15207/JKCS.2011.2.4.009

[4] D. Y. Kim & S. M. Cho. (2015). A Proposal of Smart Phone App for Preventing Smishing Attack. *Journal of Security Engineering, 12(3),* 207-220.

[5] J. H. Kim, J. Y. Go. & K. H. Lee. (2015). A Scheme of Social Engineering Attacks and Countermeasures Using Big Data based Conversion Voice Phishing. *Journal of the Korea Convergence Society, 6(1),* 85-91.
DOI : 10.15207/JKCS.2015.6.1.085

[6] S. H. Kim, M. S. Park. & S. J. Kim. (2014). Shoulder Surfing Attack Modeling and Security Analysis on Commercial Keypad Schemes. *Journal of the Korea Institute of Information Security & Cryptology, 24(6),* 1159-1174.
DOI : 10.13089/JKIISC.2014.24.6.1159

[7] G. O. Baik, C. H. Lim & J. G. Shon. (2010). A Virtual Keyboard System for Preventing Keylogging. *Journal of Security Engineering, 7(4),* 319-334.

[8] S. W. Choi & Y.J. Shin. (2015). Economy Effects of IT Industry on Financial and Insurance Services. *Journal of Digital Convergence, 13(1),* 191-203.
DOI : 10.14400/JDC.2015.13.1.191

[9] J. O. Park & B. W. Jin. (2015). A Study on Authentication Method for Secure Payment in Fintech Environment. *The Journal of the Institute of Internet, Broadcasting and Communication, 15(4),* 25-31.

[10] C. J. Chae, H. J. Cho & H. M. Jung. (2018). Authentication Method using Multiple Biometric Information in FIDO Environment. *Journal of Digital Convergence, 16(1),* 159-164.
DOI : 10.14400/JDC.2018.16.1.159

[11] Q. Yue, Z. Ling, X. Fu, B. Liu, W. Yu & W. Zhao. (2014). My google glass sees your passwords!. *Proceedings of the Black Hat USA.*

[12] H. J. Seo & H. W. Kim. (2016). Design of Security Keypad Against Key Stroke Inference Attack. *Journal of the Korea Institute of Information Security & Cryptology, 26(1),* 41-47.
DOI : 10.13089/JKIISC.2016.26.1.41

[13] Y. H. Lee. (2013). An Analysis on the Vulnerability of Secure Keypads for Mobile Devices. *Journal of Korean Society for Internet Information, 14(3),* 15-21.
DOI : 10.7472/jksii.2013.14.3.15

[14] J. S. Song, M. W. Chung, S. H. Seo & S. H. Lee. (2015). Security vulnerability analysis of Simple Mobile Payments Services. *The Korea Information Processing Society Fall Conference, 22(2),* 817-820.

[15] D. H. Lee, D. H. Bae, S. L Yoo, J. Y. Chae, Y. Lee & H. G. Yang. (2011). Analysis of safety in secure keypads for smartphone. *REVIEW of The Korea Institute of Information Security and Cryptology, 21(7),* 30-37.
DOI : KIISC.2011.21.7.30.

[16] W. G. Pak, S. Yeo, Y. R. Cha. (2015). A Secure

Virtual Keypad for Mobile devices. *Proceeding of KOREA INFORMATION SCIENCE SOCIETY,* 875-876.

[17] H. J. Mun. (2017). Virtual Keypads based on Tetris with Resistance for Attack using Location Information. *Journal of the Korea Convergence Society, 8(6),* 37-44.
DOI : 10.15207/JKCS.2017.8.6.037

[18] H. J. Mun & K. H. Han. (2018). Tetris security keypads design with higher security using alignment and padding. *International Journal of Engineering & Technology, 7(2.33),* 11-14.
DOI : 10.14419/ijet.v7i2.33.13838

[19] H. J. Mun, S. Y. Kang & C. Shin. (2020). Implementation of Secure Keypads based on Tetris-Form Protection for Touch Position in the Fintech. *Journal of Convergence for Information Technology, 10(8),* 144-151.
DOI: 10.22156/CS4SMB.2020.10.08.144

[20] J. Song, M. W. Jung, J. I. Choi & S. H. Seo. (2018). Proposal and Implementation of Security Keypad with Dual Touch. *KIPS Transactions on Computer and Communication Systems, 7(3),* 73-80.
DOI : 10.3745/KTCCS.2018.7.3.73

[21] H. J. Kim, H. J. Seo, Y. C. Lee, T. H. Park & H.W. Kim. (2013). Implementation of virtual finace keypads with resistance for shoulder surfing attack. *REVIEW The Korea Institute of Information Security and Cryptology(KIISC), 23(6),* 21-29.
DOI : KIISC.2013.23.6.21.

[22] H. J. Seo & H. W. Kim. (2014). Secure Keypad with Encrypted Input Message. *Journal of the Korea Institute of Information and Communication Engineering, 18(12),* 2899-2910.
DOI : 10.6109/jkiice.2014.18.12.2899

문 형 진(Hyung-Jin Mun) **[종신회원]**

· 1996년 2월 : 충남대학교 수학과 (이학사)
· 2008년 2월 : 충북대학교 전자계산학(이학박사)
· 2009년 3월 ~ 2012년 8월 : 중국 연변과학기술대학교 컴퓨터전자통신학부 조교수, 부교수
· 2017년 3월 ~ 현재 : 성결대학교 정보통신공학부 조교수
· 관심분야 : 정보보호, 네트워크 보안, Fintech 보안, 사용자인증
· E-Mail : jinmun@gmail.com