International Journal of Engineering & Technology, 7 (2.33) (2018) 11-14

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Tetris security keypads design with higher security using alignment and padding

Hyung Jin Mun [1] *, Kun-Hee Han [2]

[1] Assistant Professor, Dept. of Information & Communication Engineering, Sungkyul University, 14097, Anyang-city, Republic of Korea
[2] Dept. of Information Communication & Engineering, Baekseok University, 31065, Cheonan-city, Republic of Korea
**Corresponding author E-mail: jinmun@gmail.com*

Abstract

Background/Objectives: With the development of ICT, there has been a rapid increase of demand on convenient services for users to make financial transactions on smartphone. User authentication is made by inputting password on smartphone.
Methods/Statistical analysis: Banks or fintech service providers receive password using a security keypads, but attackers take a peep at passwords by various ways such as Google Glass or shoulder surfing attack. Because the locations of keypads are almost fixed and the size of keypads is almost the same, they are vulnerable to attacks using the touched location or shoulder surfing attacks.
Findings: To protect security and safety from various attacks such as the stealing of touched location using Google Glass, shoulder surfing attack, or malware, this study proposes to diversify the size of keypads, connect the keys as a Tetris game but randomly align them to left or right, and add paddings in-between the keypads so that it is difficult to infer a password by the information of touched location.
Improvements/Applications: Since a different letter is entered even if the same key is touched, it will be difficult for the attacker to infer the password through this proposed technique. It will be possible to block the attacker from peeping at a user's touched location information or the shoulder surfing attack.

Keywords: *Virtual Keypads; Password, Secure Keypads; Tetris Form Keypads; Shoulder Surfing Attack; Password Guess Attack.*

1. Introduction

Recently, the use of mobile devices such as smartphone has become more universalized. Mobile devices provide many conveniences to users' daily life, and fintech service using smartphone is growing rapidly. However, Malwares have also been rising quickly to 6 billion a year, due to the increase in the number of mobile device users and automatic malware creation toolkit [1]. Key-logger attacks occur frequently, in which an attacker secretly saves and leaks the keypad information a user entered for authentication [2].
Due to the advancement of fintech service and popularity of online banks, demand for technology to increase convenience by using mobile devices has been increasing [3]. Especially, as the demand for electronic transactions online has risen due to the popularization of smartphone, users have demanded for more financial transactions using smartphone. Thus, smartphones and financial service providers have made user authentication in various ways [4 - 6].
However, due to the limited size of mobile devices, it is difficult to enter a password. English Keypads must be arranged on the same location as a keyboard because of the habit of PC users. To reduce the time for finding letters, English characters except the numbers must be arranged on three lines and keypads must be arranged horizontally on a vertical-shaped smartphone screen, which is inconvenient.
Many banks or card companies use security keypads to enhance security, but the keypads touched by a user can be easily known by taking a video of it with Google Glass or looking at it over the shoulder when the user is entering a password. To prevent this, many financial institutions create keyboards with security keypads for users to enter their passwords safely.
QWERTY Alphabet Keypads are arranged in the same way as a PC keyboard, and the space of 1 ~ 2 keypads are divided into 1 ~ 4 arranged on a random location. (Figure 1).

(A) Method with Spacing as the Size of Keypad

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					Rearrange		

(B) Method With Spacing In Half Of The Size Of Keypad

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					Rearrange		

Fig. 1: QWERTY Keypads for Alphabets.

When only numbers are entered, a number keypad is a security keypad on which 10 keys are arranged on random locations, as in

Copyright © 2018 Hyung Jin Mun, Kun-Hee Han. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Figure 2 in which numbers are entered. It is used to enter an account or card password during a financial transaction.

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

Fig. 2: QWERTY Keypads for Number Keypads.

A mobile device is exposed more easily to malware than a PC through SMS or Apps. By hacking or using malware, an attacker can steal the smartphone root authority and infer the password entered by a user's touched location information. Presently, financial institutions have applied security keypads to prevent the leakage of passwords using touched location information, but since the keypads are arranged on fixed locations, they are still vulnerable as an attacker can figure out part of the password entered by the user with the location information touched.

Research has been conducted on security keypads that flexibly rearrange locations [7 – 9] as well as to improve the problems of fixed-size keypads [10]. Through a research improving QWERTY Keypads, it is possible to prevent and attack the attach of stealing a password with the user's touch information. However, it is easy to infer a password on a mobile device in which an attacker obtained root authority if the password is consisted of keys on both sides such as Q, A, Z, P, L, and M. Even without hacking, a part of password entered by a user can be figured out through a shoulder surfing attack or through a user's socio-engineering technique. That is, the arrangement of keypad locations or security keypads with various sizes is still insufficient for responding to attacks.

In the proposed technique, various sizes and shapes of keypads are created in a Tetris form and are connected to reduce spaces; instead several paddings are put in for the remaining spaces to block the inferring of a password based on a touched location as well as an shoulder surfing attack due to keypads with different sizes.

This study is consisted as follows. Chapter 2 introduces the password guessing attack using the location touched by a user as well as the existing security keypads, and Chapter 3 proposes a security keypad that has enhanced security through left-and-right alignment and adding more padding. Finally, Chapter 4 analyzes the proposed technique, and Chapter 5 draws a conclusion.

2. Related work

2.1. Guessing attack on a touched password using location information

In Figure 1, numbers 1 to 0 are arranged in order on the first line of QWERTY keypad. If the very left keypad is touched, 1 has definitely been touched. If the second keypad is touched, this means that 1 or 2 has been touched. Thus, a keypad exists only in 4 shapes: □12, 1□2, 123, 12□. In the first line, 10 number keypads are arranged on 11 spaces, and even when arranged randomly, □ 1 2 and 1 □ 2 have only one case respectively. 123 has eight cases and 12□ has only one case as well [11-12]

Figure 3 shows that keypads that can come out on the 5th are 4,5, and a gap (□).

	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. 3: Key Types That Is Possible to Be Inserted in the First Row.

One gap is used for English letters in the 12th line. The keypads arranged on the 2nd line, 3rd row is w, e, and □. Next, 'w' is arranged in 2 forms: q□w or □qw, and English letters are fixed for the rest. 'e' has one shape in 'qwe', but has 8 cases because 1 gap can be arranged on a

random location. □is also possible, but since a user does not touch □ so the total number of cases is 10. That is, the probability of having 'w' is 20% and 'e' is 80% [11,12]. <Table 1> shows the probability of keys by location on a QWERTY keyboard.

Table 1: Key Probability of Secure Keypad for Each Location

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

2.2. Safe security keypad to location information guessing attack

2.2.1. Ripple-type keypad

Ripple keypads makes padding on the top and bottom of a row to arrange keypads as in Figure 3 [7]. (Figure 4)

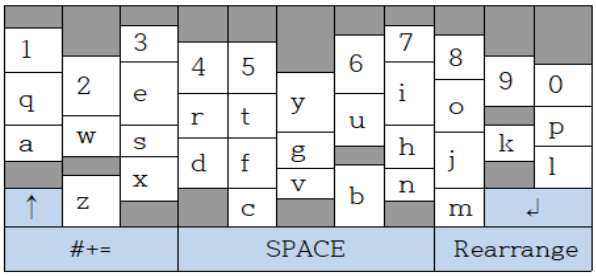


Fig. 4: Keypads Technique by Lee - Ripple Type Keypad.

2.2.2. Column-based exchange-type keypad

In the column-based exchange keypads, keys are exchanged between the top and bottom of a row in a QWERTY keyboard [8].

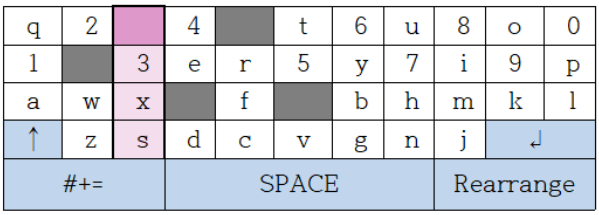


Fig. 5: Keypads Technique by Pak – Keypads Exchanged Based on Column.

Figure 5 shows the arrangement of 3□sx on the 3rd row into □3xs; however, it is even difficult for a user familiar with a PC keyboard to find the keys s/he will touch when the top and bottom are switched.

2.2.3. Clone keypad

Clone keypads can have different location values even when the same letter is touched, because one of the four lines of QWERTY keyboard is copied and arranged on the very top line [7]. (Figure 6) This means that when 'w' is entered, the keypads can be touched in 2 ways: (line 1, row 2) and (line 3, row 2), and it is difficult to guess a password using location information

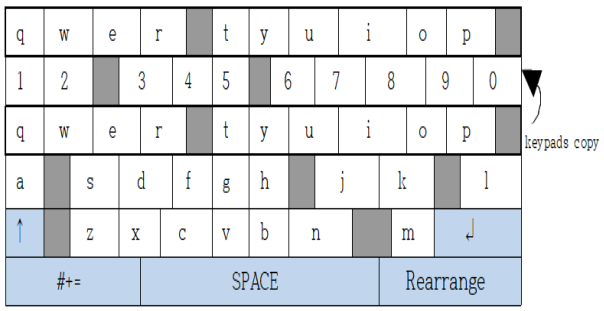


Fig. 6: Keypads Technique by Lee - Clone Keypad.

2.2.4. Keypad based on random pad

In Seo's keypad technique, a random keypad is chosen and 4 lines (line '1', line 'q', line 'q', and line 'z') are chosen randomly; then a random key is chosen from the first chosen line to arrange based on the keypad [9]. Figure 7 shows the arrangement of line 'a' followed by line '1', line 'q', and line 'z' in order by choosing letter 'd' as the starting key, and the arrangement of 'a' and 's' on line 'a'.

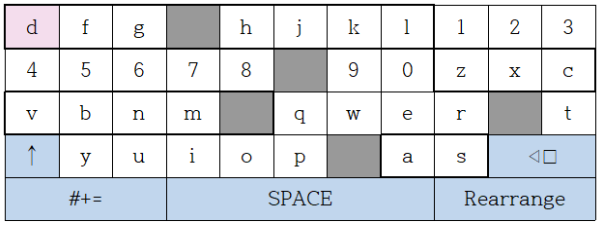


Fig. 7: Keypads Technique by Seo.

3. Proposed model

3.1. Virtual security keypad based on tetris

Password guessing attack using a touched location has been avoided by inserting padding or changing the alignment order because the keypads are square-shaped, but this causes difficulties or inconvenience for users to find the appropriate letters when entering a password [10]. To improve, 13 Tetris-shaped keypads were created and attached. Figure 8 shows Tetris-shaped security keypads in 13 forms. While there is one letter on one key in the previous security keypads and 'q' and 'w' are arranged differently, the two separate letters 'q' and 'w' are arranged on one keypad area in the Tetris-shaped security keypad; thus, safety is improved since even when the same keys are touched, they are entered as different letters. Despite of this, when the key on left or right ends on each line, i.e., '1', 'q', 'l', and 'z' are touched, it becomes possible to guess the password. Furthermore, there are too many spaces on the right.

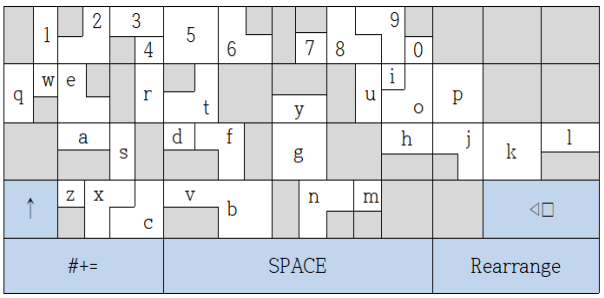


Fig. 8: Example of Secure Keypads with Tetris Type.

3.2. Improved tetris security keypad using padding and alignment

The proposed technique can decrease the possibility for a user to touch the keys on far left, by arranging the left-aligned keys of the Tetris-shaped security keypad randomly on left or right for each line. Since the possibility of touching the very ends, however, still remains when the keys are aligned on the left or right end, 1, 1.5, and 2 blocks of spaces of keypads should be added randomly on left and right; this can completely block the possibility for a user to touch the far left when entering a password and avoid arranging the keypads on only one side.

Figure 9 shows the padding of Tetris-shaped keypads on left and right and the alignment of security pads on left and right. Since the "Num" keypads must be entered separately on the existing keypad, the overall size of keypads can be increased

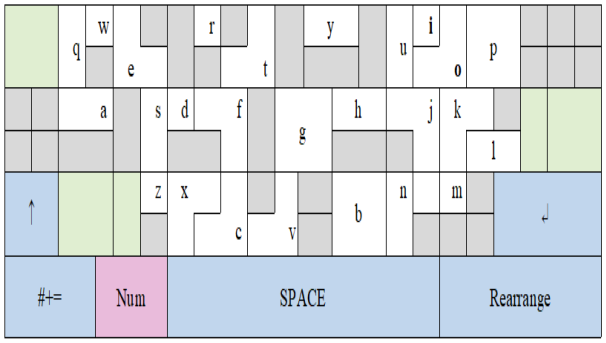


Fig. 9: Tetris Security Keypads with Padding and Alignment.

Figure 9 shows that the first line is in left alignment, 1 key is padded, and several keypads are padded in the middle. The second line is in right alignment and 2/3 keys are padded. Finally, the third line is in left alignment and 1.5 keys are padded.

4. Algorithm and analysis of the proposed technique

The proposed technique has improved the safety of the existing Tetris security keypads. The next one is a pseudo-code to realize the proposed technique. Since the size of connected Tetris-shaped keypads is 2 less than the number of the letters on each line, it was made difficult to guess the touched letters by forming some spaces.

1) Let isAlign[i] is LeftAlign or RightAlign.
2) Let be CountKeypads[i]={10,9,7}
3) for(i=0;i<3;i++) {

```
for(j=0;j<CountKeypads[i];j++){
do{
Tetris Keypad[j] = random (Tetrix)
Paste Keypad (tetrixKeypad, RandomKeypad)
 //RandomKeypad : 1.0, 1.5, 2.0
lengthKeypads=len(pasteKeypad)
} while(0<=CountKeypads[i]-lengthKeypads<2)
}
if(LeftAlign) paddingLeft()
else paddingRight()
}
```

As seen in Figure 9, ‘w’ is generally smaller than the size of keypad so it is safer from shoulder surfing attacks. Also, ‘i’ and ‘o’ are safe from shoulder surfing peek attacks because they are arranged on one area of the existing keypad and are perceived as different letters depending on the location it is touched. Therefore, when the same space is touched twice on the existing keypads, an attacker can infer it is the same letter even though s/he does not know what has been touched. Since the keypads are formed in a Tetris shape, 1 to 4 keys can be put on one keypad space and touching the same keypad space can be touching different letters, so it becomes difficult for the attacker to infer the password. The proposed technique has also solved the issue of having many unnecessary spaces on the right of the existing Tetris security keypads.

An attacker can check immediately when ‘l’ or ‘q’, ‘l’ is touched as in Figure 8. However, it is safer than the existing Tetris-form security keypads by randomly choosing alignment, padding the spaces of a random size on both ends, and adequately padding in-between the keypads, which decreases the possibility of a user to touch the both ends.

5. Conclusion

As a considerable number of bank accounts have opened with the start of Kakao Bank, an internet bank system, many banks have been struggling not to lose customers because internet banks such as Kakao Bank provides convenience to users as they can make financial transactions on smartphone.

However, safety must also be improved as the user convenience increases on various online transactions. Using devices such as Google Glass, an attacker can find out the keypads touched by a user through a zoomed-in screen or by taking a video of user touching the keys.

It is difficult to touch keypads on smartphone due to its vertical shape, so it is necessary to show horizontal-shaped security keypads on an app that runs the keys and to create keypads of various shapes and sizes other than 13 types. In the future, it will be crucial to conduct a research on security keypad that cannot be identified when looked from the side.

References

[1] AV-TEST | Antivirus & Security Software & AntiMalware Reviews. https://www.av-test.org/en/ Date accessed: 11/29/2017.

[2] Roland M, Langer J, Scharinger J, Practical Attack Scenarios on Secure Element-Enabled Mobile Devices, *4th International Workshop on Near Field Communication*, 2012, pp. 19-24.

[3] Kim Y, Park Y J, Choi J, Yeon J, An Empirical Study on the Adoption of “Fintech” Service: Focused on Mobile Payment Services. *Advanced Science and Technology Letters*, 2015, 114(26), pp. 136-140.

[4] Kang B S, Lee K H, 2-Channel authentication technique using cardiac impulse based OTP. *Journal of Computer Virology and Hacking Techniques*, 2016, 12(3), pp. 163-167.

[5] Park J O, Jin B W, A study on authentication method for secure payment in Fintech environment. *The Journal of the Institute of Internet, Broadcasting and Communication*, 2015, 15(4), pp. 25-31.

[6] Kim D R, A Study on the OTP Generation Algorithm for User Authentication, *Journal of the Korea Convergence Society*, 2015, 13(1), pp. 283-288.

[7] Lee D H, Bae D H, Yoo S L, Chae J Y, Lee Y H, Yang H G, Analysis of safety in secure keypads for smartphone, *REVIEW OF KIISC*, 2011, 21(7), pp. 30-37. http://www.ndsl.kr/ndsl/search/detail/article/articleSearchResultDetail.do?cn=JAKO201111436232012 Date accessed: 11/29/2017.

[8] Pak W G, Yeo S K, Cha Y R, A Secure Virtual Keypad for Mobile devices, *Proceeding of Korea Information Science Society*, 2015, pp. 875-876. http://www.dbpia.co.kr/Journal/ArticleDetail/NODE06602558 Date accessed: 11/29/2017.

[9] Seo H J, Kim H W, Design of Security Keypad Against Key Stroke Inference Attack, *Journal of the Korea Institute of Information Security & Cryptology*, 2016, 26(1), pp. 41-47.

[10] Mun H-J, Virtual Keypads based on Tetris with Resistance for Attack using Location Information. *Journal of the Korea Convergence Society*, 2017, 8(6), pp. 37-44.

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

[12] Lee Y H, An Analysis on the Vulnerability of Secure Keypads for Mobile Devices, *Journal of Korean Society for Internet Information*, 2013, 14(3), pp. 15-21.