Secure Virtual Keypad for Smartphones against Shoulder Surfing Attacks

Dongmin Choi[1], Cheolheon Baek[1], Jian Shen[2], and Ilyong Chung[1]*
[1]Chosun University, Gwangju, Korea
{jdmcc, iyc}@chosun.ac.kr
[2]Nanjing University of I.S.T, Jiangsu Province, Nanjing, China
s_shenjian@126.com

Abstract

Currently, cryptographic security of financial applications that run on mobile devices is considered a main feature. Thus, financial institutions develop novel secure solutions that are cryptographically secure. However, in terms of social engineering attacks, financial applications are vulnerable because most mobile devices have a display screen that is easily visible to attackers; they can easily look over your shoulder to see your password as you input it using the screen keypad. Therefore, we focused on securing the mobile keypad against shoulder surfing attacks. In this paper, we modified the previous 4-color based keypad that supports color blindness, and made it more secure against multiple attackers.

Keywords: Color blindness, Mobile virtual secure keypad, Shoulder surfing attack

1 Introduction

Mobile banking is a banking service involving transactions, such as account inquiry, cash withdrawal, and cash transfer, done from a mobile device. Mobile banking comes with an inherent security risk of financial information exposure due to data being transferred between mobile devices and servers. This risk is increased with the usage of smart phones since a majority of them run on embedded open source operating systems. Anonymous software developers freely develop smart phone applications, and users can install these applications in their smart phones via wireless internet connection. These softwares are difficult to trust, and so even though smart phones have a prevention feature built in, it still have a fatal weakness in the security. Thus, financial institutions develop prevention tools and algorithms, such as secure keypads [1-3] and malware detectors, to keep their services safe [4]. The virtual secure keypad is one such technology that offers software reliability and security. However, it is still vulnerable to social engineering attacks. For the user's convenience and to relieve typographical errors, the input data display window for a secure keypad shows the last input character of the password without masking it with an asterisk (*) or other characters. However, this convenience causes security vulnerabilities leading to social engineering attacks such as shoulder surfing attacks [5]. As shown in Figure 1, the shoulder surfing attack occurs when direct observation techniques, such as peeping over someone's shoulder or video recording, are employed to maliciously obtain passwords, PINs, and other sensitive personal information [6].

H. Kim's research [7] proposed a 4-color theorem-based [8] keypad method to guard against this kind of attack. However, their solution does not consider users with color blindness. Therefore, in our research, we propose a secure mobile keypad solution to provide advanced functionality for users

Research Briefs on Informaiton & Communication Technology Evolution (ReBICTE), Vol. 1, Article No. 10 (January 15, 2015)

*Corresponding author: Department of Computer Engineering, Choun University, Gwangju, Korea. Tel: +82-(0)62-230-7712

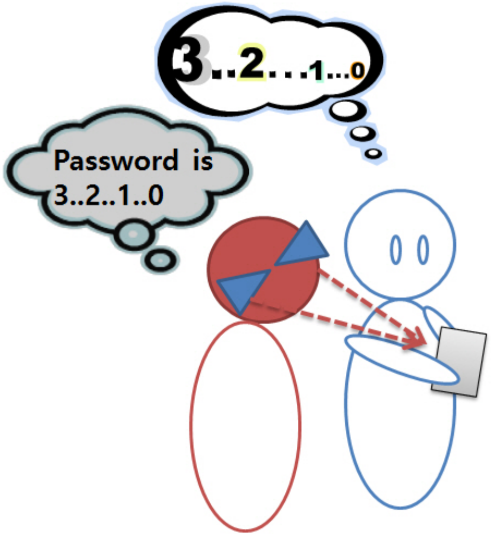


Figure 1: Example of shoulder surfing attack

with color blindness. We modified the previous 4-color based keypad to support color blind users, and improved its security against multiple shoulder surfing attacks. Compared with methods in previous research, our method offers increased security against multiple shoulder surfing attacks to all users, including those with color blindness. It does so without sacrificing typing speed and accuracy. The remainder of this paper is organized as follows: In Section 2, we describe related works. In Section 3, we explain our proposed scheme. Finally, we conclude the paper in Section 4.

2 Related Works

2.1 Security Threats

Mobile banking with a smartphone is a type of e-banking service, and security threats to this service can occur at three stages: the design and development, installation and use, and system and management stage. A shoulder surfing attack occurs in the installation and use stage. The components of a smartphone e-banking service application include the smartphone (device/platform), the e-banking service application (application), and mobile communication (network/wireless network). A shoulder surfing attack is aimed at the smartphone component. Hence, we need to prevent shoulder surfing attacks on smartphone devices. However, recent smartphone devices have large screens measuring over 5 inches that are more vulnerable to shoulder surfing attacks. Of course, larger screen sizes have several advantages. Two of them are higher typing accuracy and typing speed. Using these features, smartphone users input their secret information with higher speed and lower errors using an enlarged secure keypad [9]. However, even if the attacker is does not use his own eyes to obtain the information, other devices, such as camcorders or CCTV, can still be used, rendering these features useless. Therefore, it is crucial that we develop new methods to secure against shoulder surfing attacks.

2.2 Color Blindness Ratio and its Awareness

According to D. Mclntyre's report [10] on color blindness, approximately 8.5% of the world's population is color blind. A smartphone is currently a worldwide bestseller. Most people use smartphones for maintaining their lifestyle. Thus, for the 8.5% who are color blind, it is mandatory to develop a method that allows them to exploit the full functionality of their smartphones. In several games, a colorblind mode is available to support users who cannot recognize specific colors. When this option is enabled, the colors of several parts are changed to be recognizable by the colorblind. Some popular games, such as League of Legends, World of Tanks, and World of Warcraft already include a colorblind mode. In Korea, a mobile game named Modue Game also has a colorblind mode. Figure 2 below shows examples of colorblind mode options.

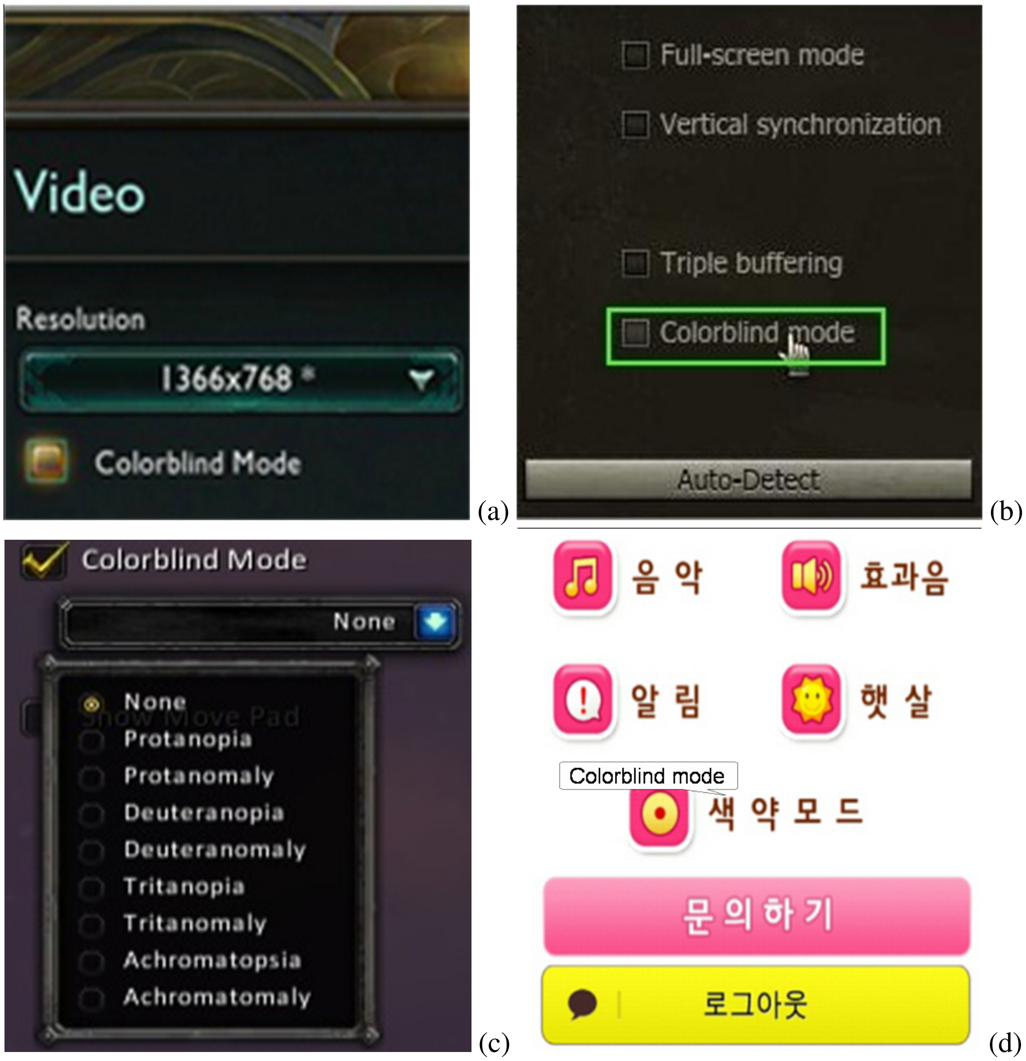


Figure 2: Examples of colorblind mode in three popular games and a Korean mobile game: (a) League of Legends, (b) World of Tanks, (c) World of Warcraft, and (d) Modue Game, respectively.

2.3 Comparison of Previous Methods

Figure 3(a) shows existing methods of secure password input/indication and (b) shows H Kim's method.

Figure 3(a) demonstrates an existing secure keypad that allows the user to see the last keystroke without the last letter being masked with an asterisk (*). However, this method is vulnerable to shoulder surfing attacks with a 68% attack success. To overcome this weakness, H. Kim's method uses a color

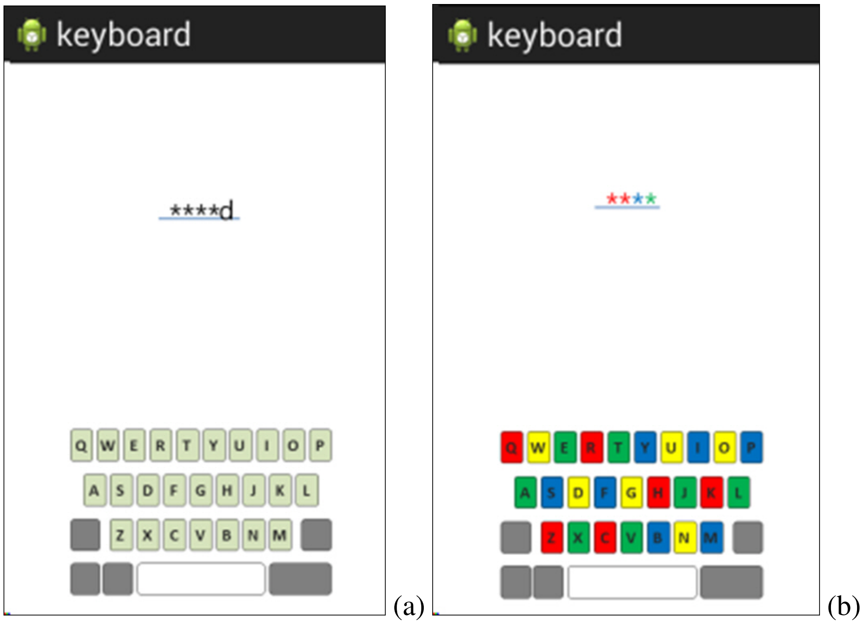


Figure 3: Comparison of existing method and H. Kim’s method

masking scheme, as shown in in Figure 3(b). In this method, each virtual key is masked by one of four colors, and this color is randomly selected by the algorithm. When a user taps the keys, the key masking color information is displayed only by the masking character (*) instead of tapping a key character. This method reduces the attack success to 0%, meaning it is theoretically safe. However, a colored asterisk symbol is tiny and may be too small to read. Moreover, in the case of multiple attacks, the attacker can estimate the color pattern of the keypad by combining partial information since the color masked keypad information is never changed when a color is randomly assigned. Figure 4 shows an example of multiple shoulder surfing attacks.

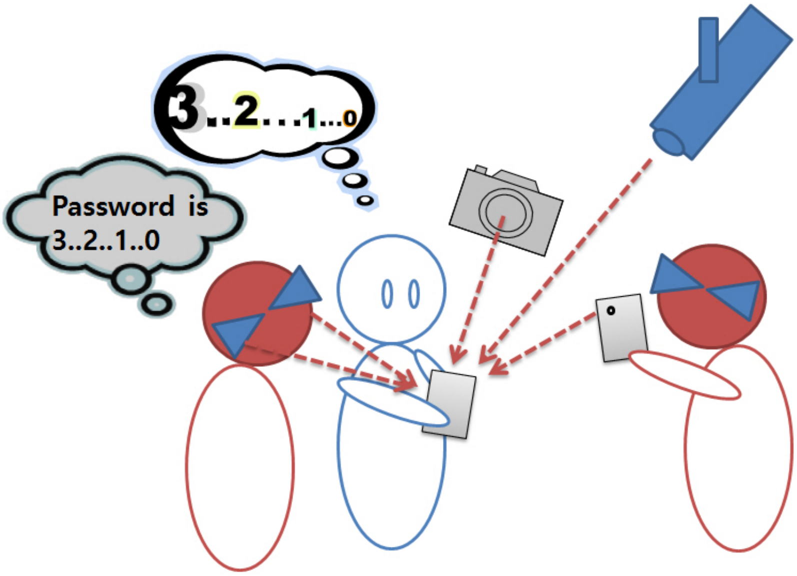


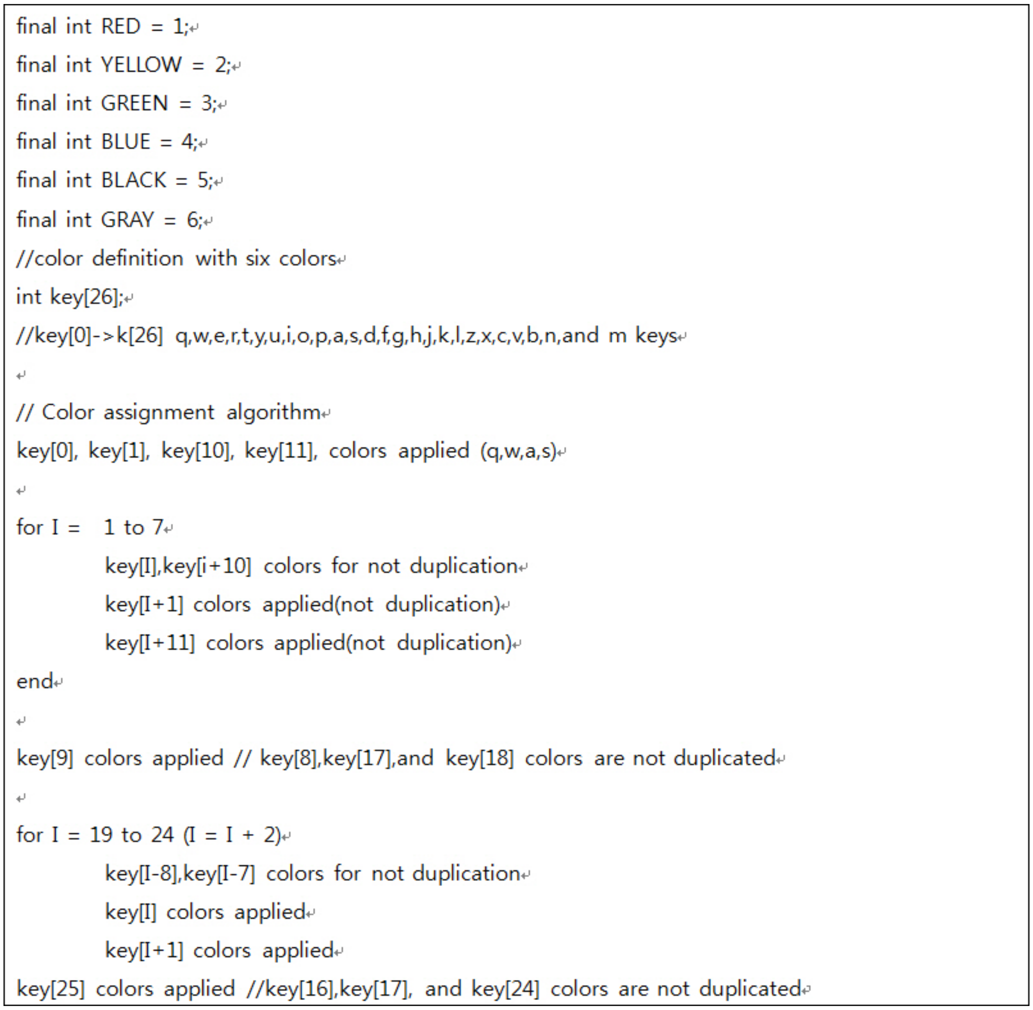
Figure 4: Example of multiple shoulder surfing attacks

3 Proposed Method

In this paper, we propose a secure keypad with a colorblind option to secure smartphones against shoulder surfing attacks. This method is a modification of H. Kim's color display algorithm. We also applied a random key color-changing algorithm to guard against multiple shoulder surfing attacks. Therefore, our method offers user convenience and increased security against multiple attackers.

3.1 Keypad and Masking Color-Changing Algorithm

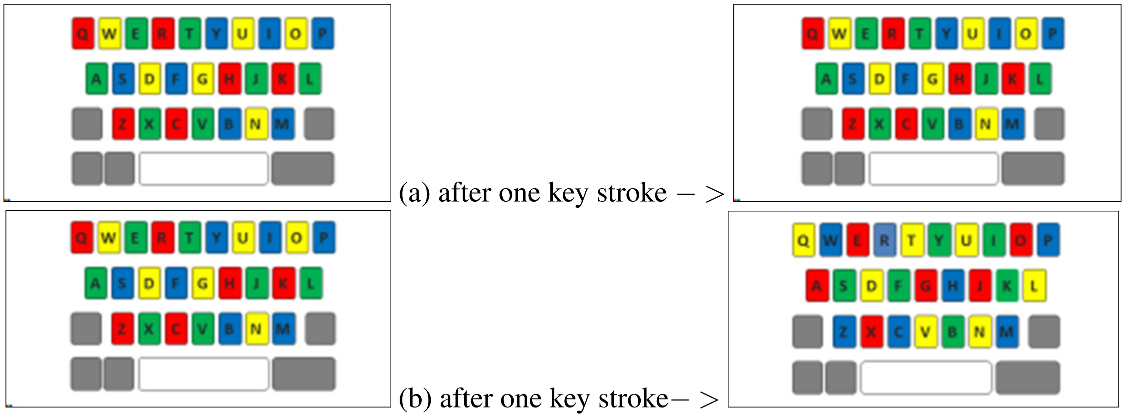
The basic scheme for the keypad and color generation is similar to H. Kim's method. However, to guard against multiple attackers, we added a new component to the color-changing algorithm. Figure 5 shows the pseudo code of key color generation and re-generation algorithm.



```
final int RED = 1;↵
final int YELLOW = 2;↵
final int GREEN = 3;↵
final int BLUE = 4;↵
final int BLACK = 5;↵
final int GRAY = 6;↵
//color definition with six colors↵
int key[26];↵
//key[0]->k[26] 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,and m keys↵
↵
// Color assignment algorithm↵
key[0], key[1], key[10], key[11], colors applied (q,w,a,s)↵
↵
for I =   1 to 7↵
          key[I],key[i+10] colors for not duplication↵
          key[I+1] colors applied(not duplication)↵
          key[I+11] colors applied(not duplication)↵
end↵
↵
key[9] colors applied // key[8],key[17],and key[18] colors are not duplicated↵
↵
for I = 19 to 24 (I = I + 2)↵
          key[I-8],key[I-7] colors for not duplication↵
          key[I] colors applied↵
          key[I+1] colors applied↵
key[25] colors applied //key[16],key[17], and key[24] colors are not duplicated↵
```

Figure 5: Pseudo code of key color generation & re-generation algorithm

As shown in Figure 6, the difference between the previous method (a) and the proposed method is the continuous changing of colors at every keystroke. For example, in Figure 6(b), the Q key in red is changed to yellow after one keystroke. As shown in the example, the color of each key changes randomly, and is never the same as that of neighboring key colors.



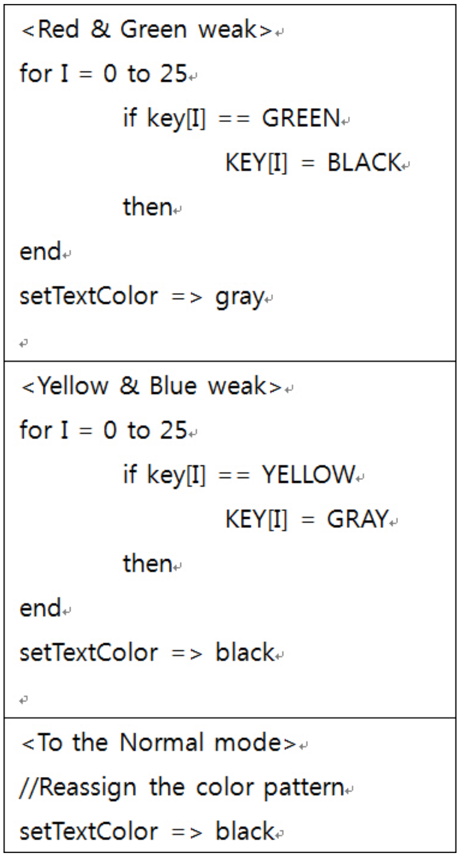
(a) after one key stroke – >

(b) after one key stroke– >

Figure 6: Comparison of H. Kim's static color keypad, and proposed dynamic color keypad

3.2 Colorblind Mode

For users with color blindness, we modified the key color pattern-changing algorithm and added a function key. The previous method applied a 4-color theorem to protect the user's secret information input via virtual keypad. However, the 4-color theorem uses red, yellow, blue, and green colors that are hard to distinguish for the colorblind. Thus, we added a colorblind mode to change several colors for them. Figure 7 shows the pseudo code of the colorblind mode in the proposed method.



```
<Red & Green weak>
for I = 0 to 25
        if key[I] == GREEN
                KEY[I] = BLACK
        then
end
setTextColor => gray

<Yellow & Blue weak>
for I = 0 to 25
        if key[I] == YELLOW
                KEY[I] = GRAY
        then
end
setTextColor => black

<To the Normal mode>
//Reassign the color pattern
setTextColor => black
```

Figure 7: Pseudo code of colorblind mode

Moreover, as shown in Figure 8, we added a colorblind mode button and pop-up menu as features of the proposed method to conveniently enable colorblind mode. The colorblind mode has two options: red & green weak mode and yellow & blue weak mode.

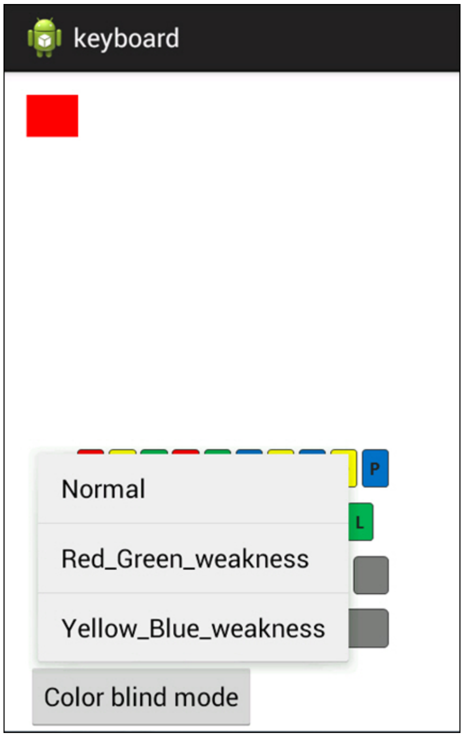


Figure 8: Color blind mode button and popup menu

The red &green weak mode is a green-to-black color changing mode, and the yellow & blue weak mode is a yellow-to-gray color changing mode. This method allows those who find it difficult to detect color differences to conveniently use a secure keypad.

3.3 User Keystroke Information Display Method

The previous method uses a black asterisk (*) to display secret keystroke information, and H. Kim's method uses a colored asterisk. However, the size of the asterisk is too small for the user to recognize exact color. Therefore, we used a space character instead of an asterisk to easily recognize the color, as shown in Figure 9.

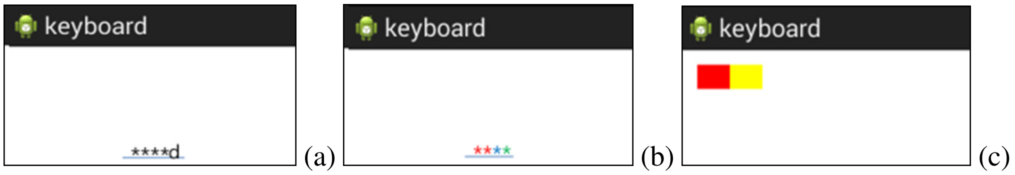


Figure 9: Comparison of color information display method

4 Conclusion

In this paper, we demonstrated a virtual keypad that offers strong privacy and higher level of user convenience. With smartphone manufacturers developing products with the screen sizes up to 7 inches that require virtual screen keypads, it was necessary to develop a virtual keypad that is secure against different types of shoulder surfing attacks. Our proposed method is secure even in the case of multiple attacks, and it offers a mode for colorblind and partially sighted persons.

References

[1] Mayank Agarwal, Mahendra Mehra andR Pawar, and deven Shah. Secure authentication using dynamic virtual keyboard layout. In *Proc. of the 2011 International Conference* & *Workshop on Emerging Trends in Technology (ICWET'11), New York, NY, USA*, pages 288–291. ACM, February 2011.

[2] Dieter Jungnickel. *Graphs, Networks and Algorithms*. Springer, 2013.

[3] Hyun-Jin Kim, Hwa-Jeong Seo, Yeon-Chul Lee, Tae-Hwan Park, and Ho-Won Kim. Implementation of secure virtual financial keypad for shoulder surfing attack. *Korea Institute of Information Security and Cryptography*, 23(6):21–29, December 2013.

[4] Okazaki Laboratory. shoulder-surfing Attack Resistant Authentication Methods. http://knowledgecenter.comarch.com, September 2014.

[5] Arash Habibi Lashkari, Samaneh Farmand, and Rosli Saleh. Shoulder surfing attack in graphical password authentication. *International Journal of Computer Science and Information security*, 6(2):145–154, November 2009.

[6] Dongkyu Lee. Mobile payment: Innovative trends, implications. Technical Report 7, Bank of Korea, 2013.

[7] Soo-Min Lim, Hyiung-Joong Kim, and seong Kee Kim. Designing password input system resistant on shoulder surfing attack with statiscal analysis. *Journal of the Institute of Electronics Engineers of Korea*, 49(9):215–224, September 2013.

[8] Donald Mclntyre. *Colour Blindness: Causes and Effects*. Dalton Publishing, 2002.

[9] DawHun Nyang, Aziz Mohaisen, and Jeonil Kang. Keylogging-resistant visual authentication protocols. *IEEE Transactions on Mobile Computing*, 13(11):2566–2579, November 2014.

[10] YoungLok Park and MyungKeun Yoon. Distributed one-time keyboard systems. *IEICE Transactions on Informations and Systems*, E96-D(12):2870–2872, December 2013.

Author Biography

Dongmin Choi received his B.E. degree from the Kyunghee University in 2003 and M.S. and Ph.D. degrees in computer Science from Chosun University in 2007 and 2011, respectively. Since 2014, he has been a Professor in College of General Education, Gwangju, Korea. His research interests are in information security, sensor network systems, mobile ad-hoc systems, smart grid home network systems and internet ethics.

Cheolheon Baek received his B.E. degree from Chosun University in 2014.He is currently working toward the M.S. degree in the department of computer science at Chosun University.his major research insterested are mobile ad-hoc networks, wireless sensor networks.

Jian Shen received the B.E. degree from Nanjing University of Information Science and Technology, Nanjing, China, in 2007 and the M.E. and Ph.D. degrees in Computer Science from Chosun University, Gwangju, South Korea, in 2009 and 2012, respectively. Since late 2012, he has been a faculty member in the School of Computer and Software at Nanjing University of Information Science and Technology, Nanjing, China. Currently, he is a full professor and the academic leader in the School of Computer and Software at Nanjing University of Information Science and Technology. His research interests include computer networking, security systems, mobile computing and networking, ad hoc networks and systems, and ubiquitous sensor networks.

Ilyong Chung received the B.E. degree from Hanyang University,Seoul, Korea, in 1983 and the M.S. and Ph.D. degrees in Computer Science from City University of New York, in 1987 and 1991, respectively. From 1991 to 1994, he was a senior technical staff of Electronic and Telecommunication Research Institute (ETRI), Dajeon, Korea. Since 1994, he has been a Professor in Department of Computer Science, Gwangju, Korea. His research interests are in computer networking, security systems and coding theory.