Multimed Tools Appl (2016) 75:15171–15183
DOI 10.1007/s11042-014-2208-7

An effective locking scheme of smart multimedia devices with convenience and enhanced security

Young-Sik Jeong · Hyun-Woo Kim · Jong Hyuk Park

Received: 15 January 2014 / Revised: 10 July 2014 / Accepted: 20 July 2014 /
Published online: 7 August 2014

Abstract The touch screen, the fruit of recent IT development, is incorporated into many applications through a variety of touch screen smart multimedia devices (e.g., digital cameras, TVs, door-lock systems, smart phones, tablet PCs and so on). For smart multimedia devices, it provides convenient use of time and space for many people by replacing many desktop PC functions. Although this convenience has gained popularity among the public, the security is usually neglected. In addition, the miniaturization of smart devices provides easy portability, but it also leads to more chances of being lost or stolen. Inherent features are generalized, but the features also increase risk of exposing personal information. As a result, smart multimedia devices provide a variety of locking features to protect personal information. The features include simple hiding of the screen, password buttons, and pattern locks. Although password and pattern lock features exhibit some degree of security, they are vulnerable to shoulder surfing or smudging. In this paper, vulnerable security points of smart multimedia devices are complemented and the locking system for enhanced security (LSES), in which intuitive user interface provides convenience, is proposed. LSES reduces exposure risk factors with various input methods for the lock pattern.

Keywords Smart multimedia device · Smart phone · Touch screen · Locking system · Security · Secure smart multimedia device

1 Introduction

The first touch screen, an electric touch interface, was invented by Samuel C. Hurst in 1971, and since then, it has eventually evolved into the touch screen of today. Currently, the touch

Y.-S. Jeong · H.-W. Kim
Department of Multimedia Engineering, Dongguk University, Seoul, Republic of Korea

Y.-S. Jeong
e-mail: ysjeong@dongguk.edu

H.-W. Kim
e-mail: z4538@nate.com

J. H. Park (✉)
Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul, Republic of Korea
e-mail: parkjonghyuk1@hotmail.com

screen is used in various areas of smart multimedia devices, and many applications have been developed for user convenience. From general user perspective, smart multimedia devices should not only carry out basic functions, such as schedule management, memo, phone book, phone, and alarm, but also various additional content, including Internet navigation, Augmented Reality (AR), Social Networking Service (SNS), e-mail, and network games, to increase convenience in everyday life. From a business perspective, a mobile office is found to be effective in increasing work efficiency and reducing costs [1–4, 9, 10, 12]. For these reasons, smart multimedia devices have become a daily necessity for many individuals.

Most users store important personal information on these compact multimedia devices as they would a desktop PC. Though they may be physically small, they can store a lot of information, which is precisely why various locking systems are built in for data security. Locking systems include motion, drag, face recognition, face and voice recognition, patterns, personal identification numbers (PINs), and passwords. However, in spite the various available locking systems, the security function is minimal or the input method is inconvenient. Even if the locking system has a security function, it may not be safe from shoulder surfing or smudge attacks, calling for a new approach to the locking system [5–8, 11].

In this paper, a locking system for enhanced security (LSES) is proposed to protect the information stored on smart multimedia devices. LSES, via an intuitive interface, can easily disable the lock screen. In addition, through a variety of methods, it can prevent others with malicious intent from inferring the pattern. In LSES, the pattern lock is not restricted to the areas of the touch screen but can use and reuse all areas, which increases the strength of the secret pattern and provides enhanced security.

The rest of the paper is organized as follows. In Chapter 2, the built-in smart multimedia device locking systems and touch screen-based representative ways to attack smart multimedia device unlock look are discussed. In Chapter 3, the pattern setup method of the proposed LSES and various recognition methods to unlock are described. The design and implementation of LSES, existing locking systems, and evaluation of performance are explained in Chapters 4, 5, and 6, respectively. Lastly, Chapter 7 summarizes the overall conclusions and future work.

2 Related works

This paper first examines the screen locking function currently built into touch screen-based smart multimedia devices. Then it discusses malicious users' common attack methods aimed at inferring the secret pattern of a locked screen.

2.1 Previously developed locking systems

Common locking systems in smart multimedia devices include drag, motion, face and voice recognition, patterns, PINs, and passwords. In general, these locking systems are used to turn off the screen automatically and reactivate the screen using a power button after the screen has been turned off. Table 1 shows the names of the locking systems built into smart multimedia devices and explains their functions [1–4, 6, 9–12].

2.2 Representative methods of attack against screen locking

Even though many screen locking systems exist, the security that they offer is fundamentally vulnerable. During the act of unlocking the locked screen, the touch screen input is exposed.

Table 1 Diverse locking systems built into smart multimedia devices and their functions

Embedded locking systems	Lock functions
Drag	Drag is a common locking system. It is basically a screen defined by the user for the purpose of hiding the content on the smart multimedia device. To unlock the locked screen, the user drags a certain area with a random starting point on the touch screen, or presses a certain button displayed and then drags to a certain area. Since only a certain area is dragged, anyone can unlock the screen, including malicious persons; therefore, it is a very vulnerable security option.
Motion	The recognition of motion depends on the smart multimedia device, and it is not frequently used. To unlock the locked screen, the smart multimedia device is tilted while the user touches the touch screen. It is convenient because it has a simple interface, like drag, but it offers low security because anyone can unlock the locked screen.
Face recognition	This security setting demands that the user be at a certain distance and present the precise focal point of the face. Having to similarly display the facial expression set by the user to unlock the locked screen is also inconvenient, and inconsistency may occur, depending on the recognition distance. In addition, since other people with a similar face may unlock the locked screen, face recognition does not offer high security.
Face and voice recognition	Face and voice recognition is a method that adds voice recognition to the face recognition method to remove the risk of similar looking people unlocking the locked screen. However, when the user speaks to the smart multimedia device to activate the voice recognition, his/her voice may be easily exposed to others, and if someone else can mimic the tone or intonation of the voice, this makes it possible for that person to unlock the locked screen. Therefore, this security method is very vulnerable. In addition, if there are problems with recognition, the user must try again, possibly numerous times, which is inconvenient.
Pattern	Pattern is a common locking system, similar to drag. It is composed of a 3×3 grid and access is granted by dragging each point. The number of recognized patterns is limited, and the security strength depends on the locking pattern set by the user. Screen locking through a pattern provides an easy interface and security.
PIN	To unlock the locked screen, the user can input a PIN. The PIN is composed of a combination of numbers, and the weaker the relationship between the numbers and the user, the higher the security. However, since the PIN it is made up of only numbers, its security strength is weaker than that of a password, and it is not easy to unlock the screen swiftly.
Password	Password is the most commonly used screen locking method. It can be composed of numbers, letters, special characters, or a combination of these. It offers very strong security, but inputting a password to unlock the locked screen also poses a risk of leakage through screen exposure. In addition, a complex combination inclined toward high security may result in the user forgetting the password or slow down the unlocking process.

The two most common methods of attack to unlock a locked screen using a touch screen are shoulder surfing and smudging.

A shoulder surfing attack is simple and may allow the attacker to steal information easily. In this attack method, a malicious person watches or records with a hidden camera when a user inputs a secret pattern to unlock a locked touch screen. Smart multimedia devices with inbuilt pattern, PIN, and password unlocking functions are very vulnerable to this attack method.

Since the numbers are aligned, PIN has an even stronger vulnerability than the other screen unlocking methods. Although pattern is expected to offer strong security, due to the large space for movement, the area for input is limited to a 3×3 grid, and since the secret pattern points are all accessible through dragging, this method does not offer high security.

A smudge attack literally utilizes a smudge. When a user inputs a secret pattern to unlock the locked touch screen, a fingerprint or trace remains on the touch screen. Smudging uses that generated trace to find out the secret pattern. Unless the user is meticulous about maintaining the cleanliness of the touch screen, which he/she uses frequently, it can be exploited by a malicious person to launch an attack.

3 Locking system of LSES

LSES provides two locking systems with built-in directionality: continuous draw direction path (CDDP) and draw sequential direction (DSD). CDDP and DSD both provide eight common directions for cognition (north, northwest, northeast, south, southwest, southeast, west, and east), as shown in Fig. 1.

3.1 CDDP

CDDP extends a limited number of existing patterns for a pattern lock. The 3×3 type of pattern lock provides simple convenience to users with its nine fixed access points, but the limited number of patterns is a vulnerable point in security. To deal with this problem, using direction, instead of access points, enables the creation of a greater number of varied patterns.

Cognition of eight directions is activated at the first touch spot in CDDP. If moved by dragging, seven directions, excluding the last moving part, are activated. Since the touch screen area used by dragging is reusable, it is difficult to infer the secret pattern. Fig. 2 shows the cognition procedure for the east and southwest directions. ① from Fig. 2 show the activation of all eight directions at first touch. ② shows the activation of seven directions, excluding the cognized direction upon dragging to the east when touched, and ③ shows the activation of seven directions, excluding the cognized direction, after being dragged from ② to the southwest.

3.2 DSD

The starting point of DSD is anywhere within the touch screen. Cognition of direction starts as soon as one moves outside the circle area created at the starting point. Similar to CDDP, it recognizes only the direction so the touch screen can be reused many times for various

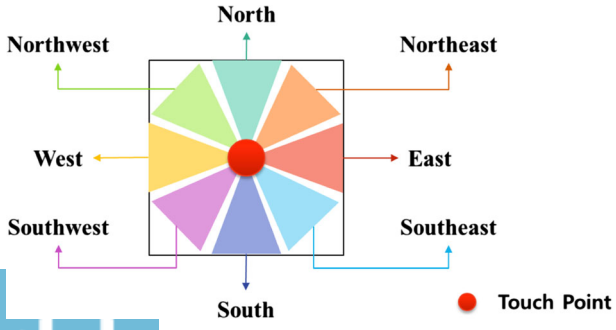


Fig. 1 LSES direction cognition

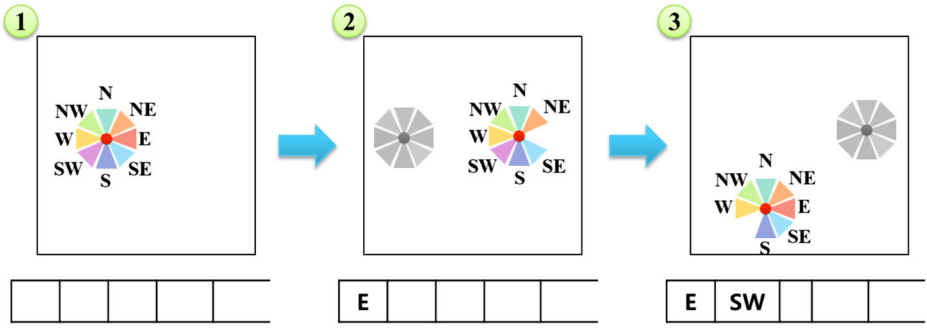


Fig. 2 Direction cognition of CDDP in LSES

patterns. In addition, different areas become starting points through new touches. Even when first cognized outside the circular area, it can still be recognized again by coming in and out of the circular area. Figure 3 shows the process of cognition in the southwest.

① from Fig. 3 show the first touch. ② shows dragging to the east from the starting point, and cognition is being made outside the circle. As shown in ③, the new input can be made by re-entering the circular area while still pressing the screen. ④ shows cognition outside the circle for input to the southwest. This makes it possible to input additional directions. These cognitions enhance security by providing variety in the secret patterns and in the ways to input the same pattern.

LSES provides systematic random directionality to negate the user's vulnerability to shoulder surfing and smudge attacks. For random directionality, when a user inputs all set patterns, the directionality generated in the system should be input. For the directionality generated in the system, the current time is applied as a seed value to prevent overlapping. The number of directionalities generated in the system is provided so that the user or the system can determine the maximal length. Therefore, it will be difficult for shoulder surfing to determine the secret pattern that the user has set. Moreover, it is difficult for a smudge attack to judge whether the trace is a pattern set by the user or a systematic pattern resulting from the systematic directionality provided by LSES, thereby heightening security.

4 LSES design

The LSES design proposed in this paper is largely composed of a user interface that receives input from the user; a point path trace that pursues the input; a direction (D)-manager that manages the

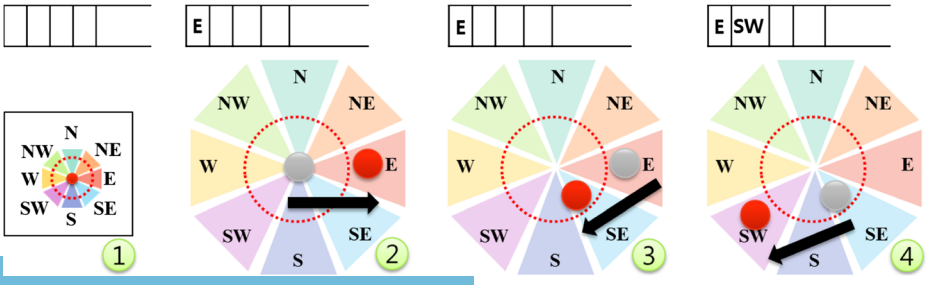


Fig. 3 Direction cognition of DSD in LSES

input directionality; an intelligent direction pattern (IDP)-manager that manages the systematic directionality; a database (DB)-manager that stores and manages the input directionality; a lock (L)-service that provides services for screen locking; a coordinate converter that converts the input directionality to show it to the user; and an activity to show the LSES setting and locked screen to the user. Figure 4 shows a structural map of the overall functions of LSES.

The user interface consists of a direction, setting, and mode. The direction perceives the user's movements north, northeast, northwest, south, southeast, southwest, west, and east. The perceived directionality is sent to the IDP-manager and D-manager. The setting sets up the background color of the lock screen and the range of the DSD circle. The mode has two types of lock pattern provided by LSES, and one can select either DSD or DCCP. The point path trace plays the role of calculating the distance from the point the user pressed to the point where the user moved in the user interface. This calculated distance is sent to activity and may be viewed on a real-time basis.

The D-manager is composed of M-check (mode-check), which checks the selected lock pattern mode in the user interface; DSD analysis, which analyzes direction in case of DSD depending on the check result; DSD-C (DSD-check), which checks whether the same pattern has been input for direction pattern setup; and DSD-S (DSD-save), which sends index of direction to the DB-manager when the patterns are the same. If the selected mode from M-check is CDDP, CDDP analysis analyzes direction, CDDP-C checks whether the same pattern has been input, and CDDP-S sends the index of direction to the DB-manager.

The IDP-manager operates according to whether the user set. It stores the data produced from the point path trace and compares the distances moved to unlock the locking and directionality and the direction pattern set by the user. Using the compared data, to reduce attacks by malicious persons, it demands that the user input a random direction pattern. The random direction pattern is induced to input directionality with low frequency in the user's input to unlock the locked screen. This may heighten the security strength against smudge attacks.

The DB-manager consists of D-analysis that analyzes the data conveyed and stores them in SQLite, update that revises a previously set directional pattern, insert that inputs a new directional pattern when it is executed for the first time, and s-check that checks whether the stored direction pattern exists and allows the user to select the mode to unlock the screen.

L-service is comprised of lock analysis that analyzes whether screen locking has been executed, unlock and lock that are executed according to the lock analysis, and screen check

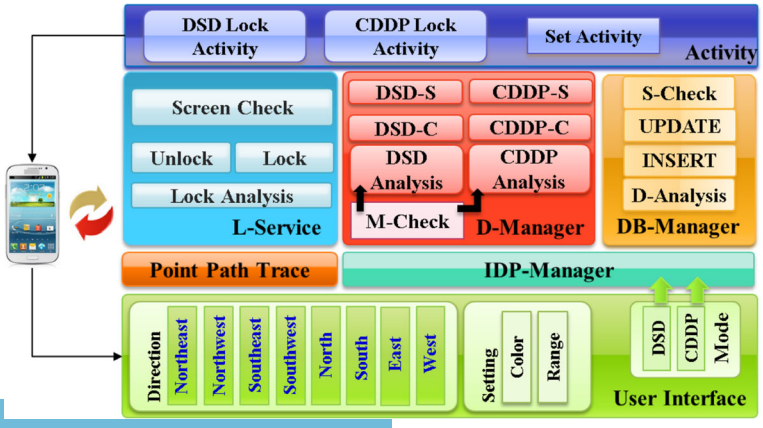


Fig. 4 LSES architecture

that is intended to perform a test of the movement direction when screen locking is performed. In screen check, when the input directionality differs from the stored directionality, the input directionality is initialized. The user may determine the number of initializations, and they are used as the number of attempts to unlock the screen.

Activity consists of set activity, which sets up the pattern the user is going to use in the lock screen, and DSD lock activity or CDDP lock activity, which appears when the user sets up the lock and the smart multimedia device or the screen is turned off. Depending on the mode selected in the user interface, either DSD or CDDP lock activity is executed.

5 LSES implementation

When LSES is executed for the first time, no information on the secret pattern using directionality is available. Therefore, the user must input a directional pattern whose locking will be set. Figure 5 shows a screen where LSES has been executed for the first time. The screen consists of a touch area for inputting the pattern, a cancel button for canceling the pattern, a revise button to revise when a directional pattern has been wrongly input, and a continue button to perform the next progression after inputting the directionality.

Figure 6 displays a screen that has perceived the directionality of the user who touched it. When each direction—north, northeast, east, southeast, south, southwest, west, and northwest—is perceived, it is shown to the user as an icon at the selected starting point.

Like Figs. 6 and 7 shows a screen when a total of ten directions—north, south, north, south, east, west, east, west, north, and south—are input through the perception of directionality. By

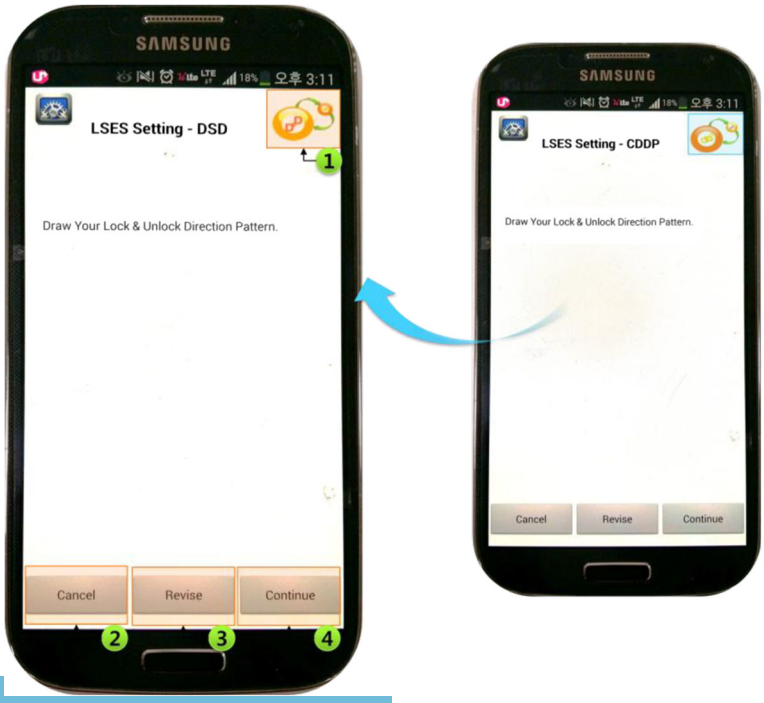


Fig. 5 LSES initial execution screen

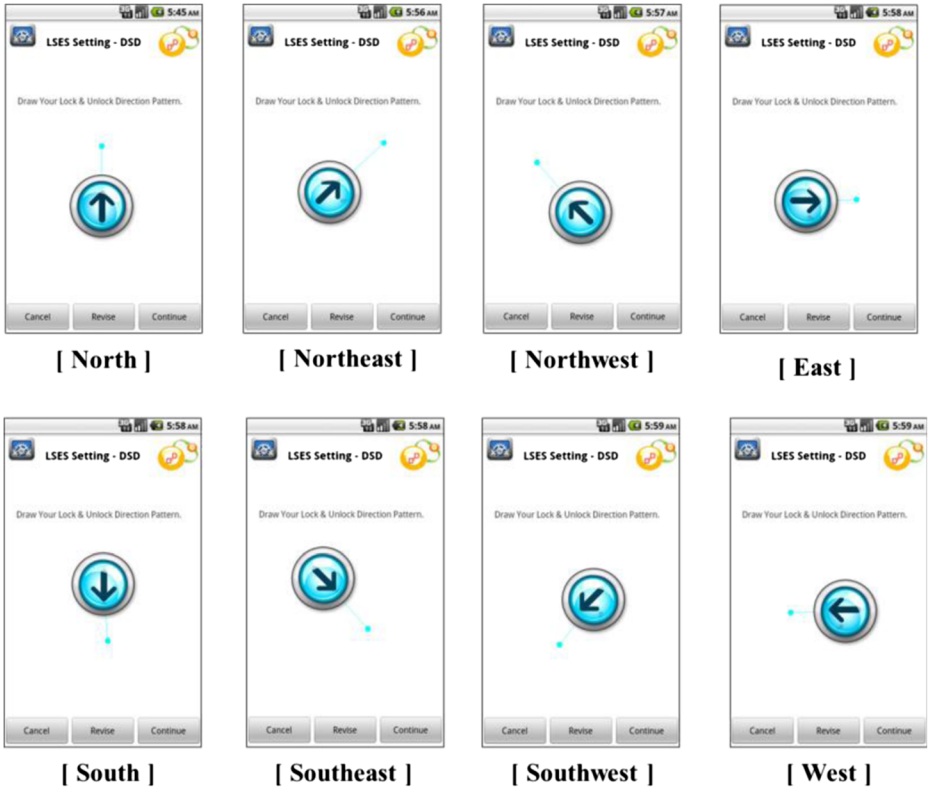


Fig. 6 Screen displaying the perception of directionality

showing the input directionality to the user, he/she may verify it, and when the user wishes to revise it, he/she may do so using the revise button at the bottom of the screen. Pressing continue activates the confirmation screen, and then pressing the OK button, saves the direction pattern. In this way, the user can save as many direction patterns as he/she chooses, within the limits of the smart multimedia device's memory.

Figure 8 shows the unlocking process of the lock screen in LSES-DSD mode, using the direction pattern in Fig. 7 as the secret pattern. Anywhere in the touch screen can be used as the starting point, and it can be completed by one touch or dragging. In addition, if the user runs out of space while inputting the pattern, he/she may restart from anywhere in the screen. Since the screen is able to cognize only the direction, it is very easily reusable.

Figure 9 shows the lock screen in CDDP mode of LSES. Similar to Fig. 8, the direction pattern in Fig. 7 is used. As an overlapping direction path is possible, the vulnerability to shoulder surfing is complemented.

6 Performance evaluation

Among the generally used locking systems, pattern locks are more secure than drag locks. A pattern lock has limited number of lock pattern it is restricted to 3×3 access points. Figure 10 compares the number of possible patterns in the pattern lock and in DSD and CDDP of LSES

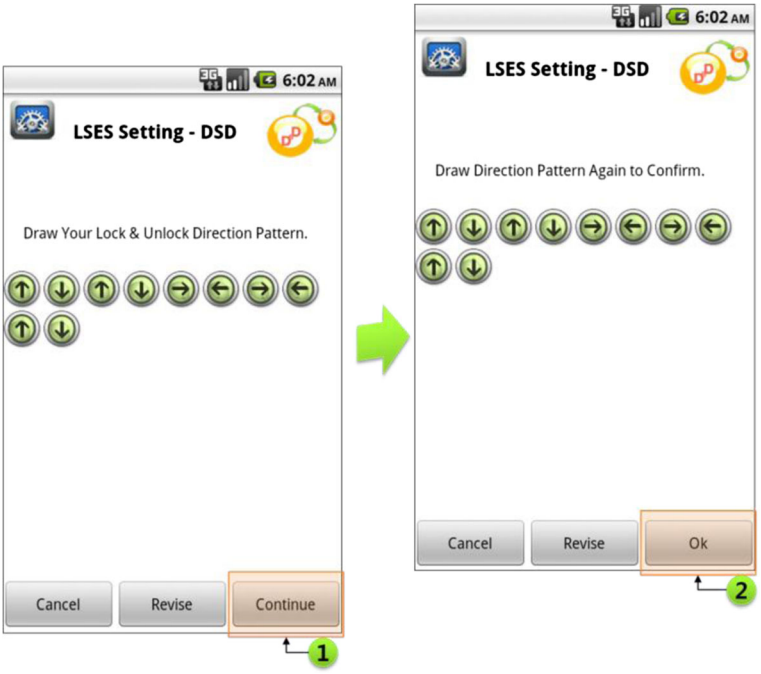
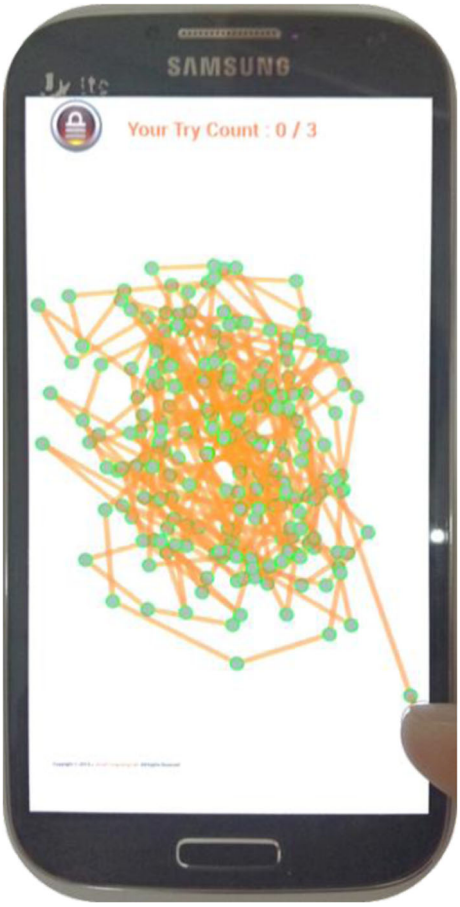


Fig. 7 Screen upon receiving ten directions from user

discussed in this paper. In the pattern lock, more than four patterns need to be input to set up the lock, and maximum of nine access point can be used. The number of patterns, excluding the repeated access point (from 1 to 3, the pattern automatically passes by 2), is 389,112. On the other hand, since DSD and CDDP of LSES consider the direction, continuous input of eight directions is possible. In Fig. 10, when the input value is 7, there is not much difference

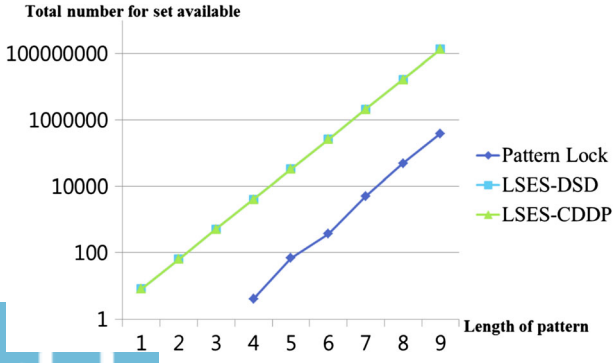
Fig. 8 DSD mode of LSES

Fig. 9 CDDP mode of LSES



in the number of patterns. However, the number of patterns created by eight inputs in the pattern lock is very different from the number of patterns created by using all access points. In addition, if the lock pattern is created by inputting nine times, in the case of DSD and CDDP, more than 10,000,000 patterns can be created, which enhances security by making it harder

Fig. 10 Total number of patterns depending on the input value



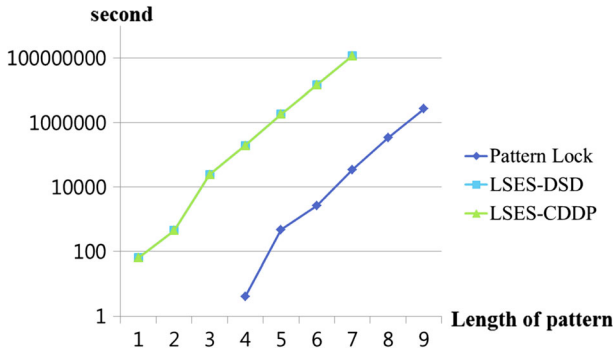


Fig. 11 Input time for all possible patterns depending on pattern length

and more time consuming to unlock. If inputting time is increased like this, for n number of inputs, 8^n patterns are created in DSD and CDDP.

Figure 11 compares the time to input all possible patterns in pattern lock, DSD, and CDDP, assuming that one pattern takes 1 s to input. When a pattern is incorrectly inputted, for five wrong trials, 30 s of waiting time is applied in pattern lock.

In case of pattern lock, it took 2,723,784 s to input 389,112 patterns, which converts into 31~32 days of security strength. In contrast, DSD and CDDP of LSES require 939,524,096 s to input 134,217,728 possible patterns. This is equivalent to 10,874 days and 339 times stronger security strength than pattern lock.

7 Conclusion

Touch screen-based smart multimedia devices are utilized by many different people due to their portability and many inbuilt functions. As the storage capacity of these smart multimedia devices increases, they can be used to store more data related to tasks, as well as personal data. As a result, they offer increased convenience. However, the number of malicious persons and the risk of losing data have also increased. In particular, if a smart multimedia device's touch screen is frequently exposed, the smart multimedia device may become a target for malicious persons.

LSES addresses the vulnerability of touch screens to shoulder surfing and smudge attacks. LSES perceives directionality and, therefore, the touch screen may be reused, enabling the setting of a screen lock with many directional patterns. When the screen is locked, LSES provides several methods for unlocking it that differ from the previous method of inputting the same pattern; therefore, it is difficult for a malicious person to infer the pattern. In addition, to increase security against smudge attacks, systematic random directions were provided. Through systematic random directions, the inference of traces becomes all the more difficult, and the inconvenience of having to polish the touch screen every time is resolved, allowing the user to use the smart multimedia device with ease.

In the future, we intend to converge LSES with an algorithm so the neural network can derive systematic random directions more intelligently. In addition, the researcher aims to study a middleware that may transmit the location of the smart multimedia device to a contact number set by the user. This middleware will be installable in all smart multimedia devices and other digital devices that enable mail and Internet access, so that the user may use it conveniently.

Acknowledgments This research is supported by the MSIP (Ministry of Science, ICT and Future Planning), Republic of Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2014-H0301-14-1021) supervised by the NIPA (National IT Industry Promotion Agency).

References

1. Alberts CJ, Dorofee AJ (2002) Managing information security risks: the OCTAVE approach. Addison-Wesley Professional, pp 1–471
2. Aviv AJ, Gibson K, Mossop E, Blaze M, Smith JM (2010) Smudge attacks on Smartphone touch screens. Proceedings of the 4th USENIX Conference on Offensive Technologies, No. 1, No. 7, pp 1–10
3. Chin E, Felt AP, Sekary V, Wagner D (2012) Measuring user confidence in Smartphone security and privacy. The 2012 Symposium on Usable Privacy and Security (SOUPS), No. 1, pp 1–16
4. Gong YI (2010) Implications and agreement of Smartphone. Korea Inf Soc Dev Inst 22(4)
5. Hyeong-Il K, Yong-Ki K, Jae-Woo C (2013) A grid-based cloaking area creation scheme for continuous LBS queries in distributed systems. J Converg 4(1)
6. ITU-T (2010) Security aspects of mobile phones. T09 SG17 100407 TD PLEN 1012
7. Junho A, Richard H (2012) An indoor augmented-reality evacuation system for the Smartphone using personalized Pedometry. Human-centric Comput Inf Sci 2(18)
8. Kim C-s, Yoon S-b, Lee M-k (2010) Shoulder-surfing resistant password input method for mobile environment. J Korea Inst Inf Secur Cryptol 20(3):93–104
9. Mulliner C, Vigna G, Dagon D, Lee W (2006) "Using labeling to prevent cross-service attacks against smart phones" DIMVA 2006. LNCS 4064:91–108
10. Park M (2011) The evolution of the mobile phones with touchscreen and the prospect of future: focused on the SRI-tech. Master Thesis, Incheon University
11. Peng K (2013) A secure network for mobile wireless service. J Inf Process Syst 9(2):247–259
12. Wang G, Zhou W, Yang LT (2013) Trust, security and privacy for pervasive applications. J Supercomput 64(3):661–663

Young-Sik Jeong is a professor in the Department of Multimedia Engineering at Dongguk University in Korea. His research interests include multimedia cloud computing, mobile computing, ubiquitous sensor network (USN), and USN middleware. He received his B.S. degree in Mathematics and his M.S. and Ph.D. degrees in Computer Science and Engineering from Korea University in Seoul, Korea in 1987, 1989, and 1993, respectively. Since 1993, he has been serving as an IEC/TC 100 Korean Technical Committee member, as the IEC/TC 108 Chairman of Korean Technical Committee, and as an ISO/IEC JTC1 SC25 Korean Technical Committee member. He is Editor-in-Chief of Journal of Information Processing Systems and Associate Editor of International Journal of Communication Systems, Journal of Internet Technology and International Journal of Grid and Utility Computing. In addition, he has been serving as a Guest Editor for international journals by some publishers: Springer, Elsevier, John Wiley, Oxford Univ. Press, Hindawi, Emerald, Inderscience and so on. He is also is a member of the IEEE.

Hyun-Woo Kim received the B.S in Computer Engineering WonKwang Univ. in 2012. He is a Ph.D. student of the Department of Multimedia Engineering, Dongguk University. His research interests include multimedia cloud computing, mobile computing, ubiquitous sensor network (USN), USN middleware and Big-Data Processing Scheme.

Jong Hyuk Park received his Ph.D. degree in Graduate School of Information Security from Korea University, Korea. From December, 2002 to July, 2007, Dr. Park had been a research scientist of R&D Institute, Hanwha S&C Co., Ltd., Korea. From September, 2007 to August, 2009, He had been a professor at the Department of Computer Science and Engineering, Kyungnam University, Korea. He is now a professor at the Department of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech), Korea. Dr. Park has published about 100 research papers in international journals and conferences. He has been serving as chairs, program committee, or organizing committee chair for many international conferences and workshops. He is a president of the Future Technology Research Association International (FTRA) and Korea Information Technology Convergence Society (KITCS). He is editor-in-chief of Human-centric Computing and Information Sciences (HCIS) by Springer, International Journal of Information Technology, Communications and Convergence (IJITCC) by InderScience, and Journal of Convergence (JoC) by FTRA Publishing. He is Associate Editor/Editor of 14 international journals including eight journals indexed by SCI(E). In addition, he has been serving as a Guest Editor for international journals by some publishers: Springer, Elsevier, John Wiley, Oxford Univ. Press, Hindawi, Emerald, Inderscience. His research interests include security and digital forensics, Human-centric ubiquitous computing, context awareness, multimedia services, etc. He got the best paper awards from ISA-08 and ITCS-11 conferences and the outstanding leadership awards from IEEE HPCC-09, ICA3PP-10, IEEE ISPA-11, and PDCAT-11. Dr. Park' s research interests include Digital Forensics, Security, Ubiquitous and Pervasive Computing, Context Awareness, Multimedia Service, etc. He is a member of the IEEE, IEEE Computer Society, KIPS, KICS, KIISC, KMMS, KDFS and KIIT.