Development Status and Prospects of Graphical Password Authentication System in Korea

Gi-Chul Yang
Department of Convergence Software, Mokpo National University
Muan-gun, Jeonnam 58554 – Korea

Received November 22, 2018; revised January 27, 2019; revised February 23, 2019; accepted April 10, 2019; published November 30, 2019

Abstract

Security is becoming more important as society changes rapidly. In addition, today's ICT environment demands changes in existing security technologies. As a result, password authentication methods are also changing. The authentication method most often used for security is password authentication. The most-commonly used passwords are text-based. Security enhancement requires longer and more complex passwords, but long, complex, text-based passwords are hard to remember and inconvenient to use. Therefore, authentication techniques that can replace text-based passwords are required today. Graphical passwords are more difficult to steal than text-based passwords and are easier for users to remember. In recent years, researches into graphical passwords that can replace existing text-based passwords are being actively conducting in various places throughout the world. This article surveys recent research and development directions of graphical password authentication systems in Korea. For this purpose, security authentication methods using graphical passwords are categorized into technical groups and the research associated with graphical passwords performed in Korea is explored. In addition, the advantages and disadvantages of all investigated graphical password authentication methods were analyzed along with their characteristics.

Keywords: Graphical password, Authentication, Computer security, Security attack.

http://doi.org/10.3837/tiis.2019.11.026 **ISSN : 1976-7277**

1. Introduction

In today's increasingly complex society, the importance of security and the demand for sophisticated authentication techniques are growing. For contemporary digital security, a password is the authentication method most commonly used. Currently, text-based passwords are most often used for authentication. They are popular because they are easy to create and simple to use. Also, any password used for authentication should be easily remembered and should not be easily exposed to others. However, text-based passwords do not satisfy these requirements. Text-based passwords are difficult for users to remember if the password length is long and complicated and easily stolen if they are simple. Most users tend to use short passwords that are easy to remember [1]. This makes the password vulnerable to brute force attacks and dictionary attacks. Text-based passwords are also vulnerable to shoulder-surfing attacks, spyware or automated programs that generate passwords.

Moreover, the number of passwords that users must remember are increasing these days, and it is not easy to use multiple, long and complex text-based passwords. Therefore, people often use a single password for many accounts. Once the password is compromised, so is the integrity of any authentication process that utilizes it. Therefore, authentication techniques that can replace text-based passwords are required today.

To solve the problem of this text-based authentication, various methods of password schemes have been developed so far. Among them, there are biometric passwords, which are using fingerprints or iris recognition, and graphical passwords using images in place of text, and so on. Biometric techniques need special devices and the system construction cost is high and inconvenient. Also, there is a problem such as personal information leakage.

On the other hand, graphical passwords have no problems in biometrics and use images that the users can easily remember rather than text. A graphical password uses images instead of texts. Graphical password research guided by a principle established by psychological research: people remember images better than characters [2]. Even though, it is true that not all the graphical password schemes are better than text-based password schemes, it is possible to develop better password schemes by using graphics rather than texts. And it is true that graphical password scheme has potential applications, especially where text input is hard (e.g., PDAs or ATMs), or in situations where passwords are infrequently used (e.g., web site passwords) [3].

Graphical passwords do not use letters or numbers but images or patterns that are easier to remember than text-based passwords. Graphical passwords are not as easy to detect as text-based passwords since their password spaces are usually larger than text-based passwords. Also, it is hard to attack graphical password systems by using automated password-generating programs. However, graphical password systems have two disadvantages when compared to text-based password systems: data transmission costs are high and the system is vulnerable to shoulder-surfing attacks when operating the system in real situations. Also, inputting data by using a keyboard is often inconvenient for systems using graphical passwords. However, the graphical password authentication scheme is one of the important techniques that can replace the text-based password authentication scheme. Recently, research on graphical passwords has been actively conducted in many places throughout the world. This paper describes the development status and prospects of graphical password authentication systems in Korea.

This paper is organized as follows: Section 2 explores the types of authentication schemes and types of graphical passwords. Section 3 investigates the graphical password schemes developed in Korea. In Section 4, we analyze and compare the advantages and disadvantages of the graphical password schemes investigated in Section 3. Section 5 concludes the paper.

2. Authentication Schemes and Graphical Password Schemes

This section reviews the types of authentication schemes and the types of graphical password schemes. Section 2.1 describes the types of authentication schemes and the types of graphical password schemes are explained in section 2.2.

2.1 Authentication Schemes

There are three types of authentication schemes. The first one is a token-based authentication scheme, the second one is a biometric-based authentication scheme, and the third one is a knowledge-based authentication scheme. **Fig. 1** shows the types of authentication schemes.

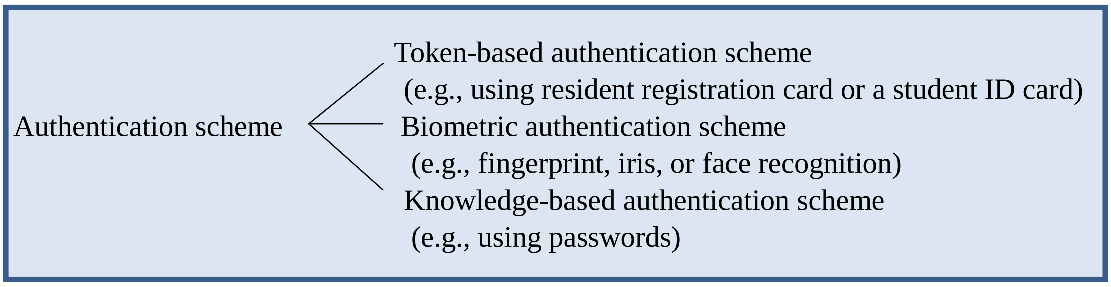

Authentication scheme
Token-based authentication scheme
(e.g., using resident registration card or a student ID card)
Biometric authentication scheme
(e.g., fingerprint, iris, or face recognition)
Knowledge-based authentication scheme
(e.g., using passwords)

Fig. 1. Types of authentication schemes

A token-based authentication scheme is a scheme that processes authentication using something physical, such as a resident registration card or a student ID card. A token-based authentication scheme has the disadvantage of having to carry something that acts like a key.

A biometric authentication scheme recognizes the characteristics of the body, such as a fingerprint, an iris, or a face, and processes the authentication. In a biometric authentication system, it is difficult to steal a password because it uses a characteristic of the body as a password. However, there are some disadvantages: it requires separate, high-priced equipment for biometrics recognition and the user cannot change their password and cannot use the system if it is stolen.

Biometric authentication systems can divided into two categories: those requiring contact with the body and those that do not. A fingerprint recognition system, which is commonly used nowadays, is a system that requires contact with the body, and an iris or face recognition system does not require bodily contact. Such a biometric authentication system has advantages in terms of reliability, response speed, and ease of use. However, there is a disadvantage that it is difficult to construct the system and the operating cost is high.

Finally, a knowledge-based authentication scheme is based on the user's cognitive ability. In a knowledge-based authentication scheme, passwords are used. The passwords must be easy for the user to remember and difficult for others to guess. There are two types: text-based passwords and graphical passwords. The text-based password system is the most commonly used knowledge-based authentication system. Unfortunately, text-based passwords tend to conflict with the requirements of passwords generally: long passwords are hard to remember and short passwords are easy to guess. The authentication system used to overcome these drawbacks is a graphical password system.

2.2 Graphical Password Schemes

The graphical password scheme is an authentication scheme built on the fact that people easily remember pictures rather than letters or numbers. Currently, the graphical password schemes can be divided into four different categories. These categories are recall-based scheme, recognition-based scheme, cued-recall scheme, and hybrid scheme. Fig. 2 shows the types of graphical password.

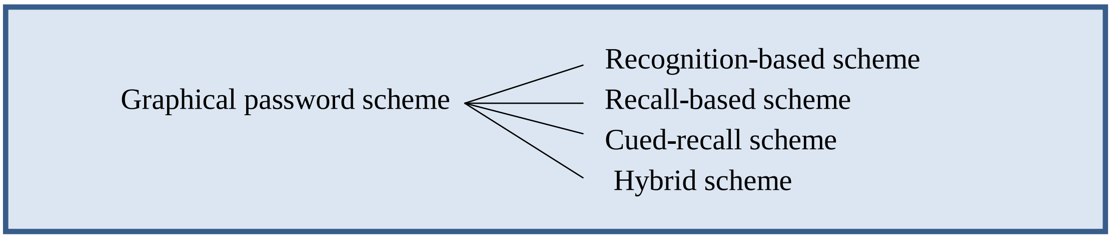


Fig. 2. Types of graphical password schemes

Recall-based graphical password systems handle authentication by comparing input patterns to a registered pattern. This process is comparable to a text-based password system. However, the user must remember the password without any hints. Therefore, users cannot easily use long passwords for a recall-based graphical password system. Hence, the recall-based graphical password system is weak against dictionary attacks.

A recognition-based graphical password system is a system in which various pieces of information are listed and the user chooses the correct password information to obtain authentication. For example, the password prompt for such a system could display a multitude of faces. The user is then authenticated only after selecting the correct, pre-specified face within an allotted number of attempts. This method takes a long time to input a password and there may be various problems, such as communication costs for collecting, storing, and transmitting photographic data necessary for system construction and operation.

A cued-recall type graphical password system receives the password pattern with the help of a background image or other helpful information. The burden of memorization on the user is less than that of a simple, recall-based password system. For example, there is a system that grants authentication after the user clicks on predetermined points in a given image in a specified order [4]. Such a system has advantages, such as quick password input and less burden on a user's memory. However, the drawbacks are the hot spot problem and the requirement of clicking points accurately.

A hybrid graphical password system is a system that uses several kinds of graphical password techniques together. When building a hybrid graphical password system, it is important to think about interaction and maximize the efficiency of the final system.

3. Graphical Password Schemes Developed in Korea

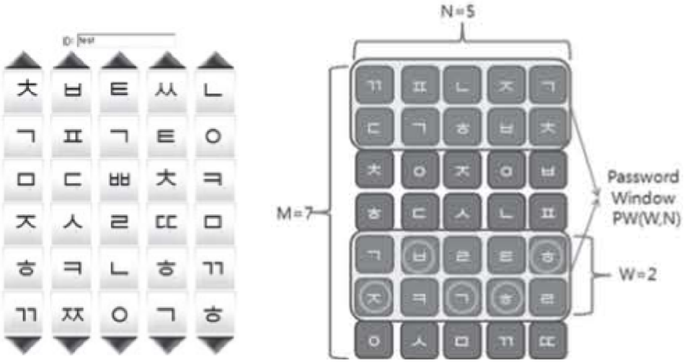
This section is a comprehensive survey of graphical password techniques developed in Korea. This survey uses research contained in the Computer Research Information Center in Korea and papers found on the internet. The research is listed in chronological order. The contents described here may not cover all graphical password research conducted in Korea, but we can track current research status and development directions of the graphical password authentication system in Korea through the work contained in this section.

The R-Point technique, released in 2006, is a graphical password technique that uses a single image and a number *k* as a password [5]. The number *k* indicates the distance according to the number of cells. **Fig. 3** shows images that can be used as a password in the form of a square if the cross-shaped image and number 2 were selected by a user for password registration. That is, if one of the images at a distance of 2 away from the selected image is selected, authentication is granted.

Fig. 3. R-Point technique

The R-Point technique only requires the memorization of a data pair (i.e., a single image and a number *k*), so it is easy to recall the password. Because the R-Point technique randomly displays an array of images each time, the image used as a password changes every time. Therefore, it is immune to a shoulder-surfing attack but is vulnerable to a brute force attack.

The grid-based password system released in 2010 and 2011 is a system that handles authentication by placing user-specified characters in the *M X N* grid of the screen [6, 7].



(a) (b)

Fig. 4. Grid-based password system (The symbol in each grid is a Korean alphabet. It can be replaced for other symbols.)

Fig. 4 (b) shows an improved grid-based password system that sets a password grid of size *W X N* smaller than the input grid of size *M X N* across the screen. The user inputs the specified characters into the password grid to receive authentication. Grid-based password systems (similar to the R-Point technique) can prevent shoulder-surfing attacks, but are vulnerable to brute force attacks and have a longer login time than text-based passwords. The graphical password system, released in 2011 and 2012, is a path-selection authentication system that handles authentication by having the user trace a path through user-specified pictures among several pictures on the screen in the order [8, 9] as shown in **Fig. 5**.

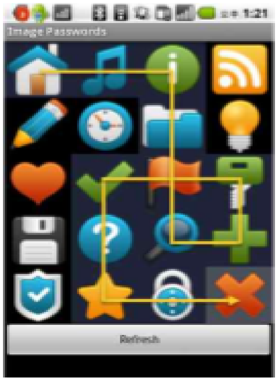
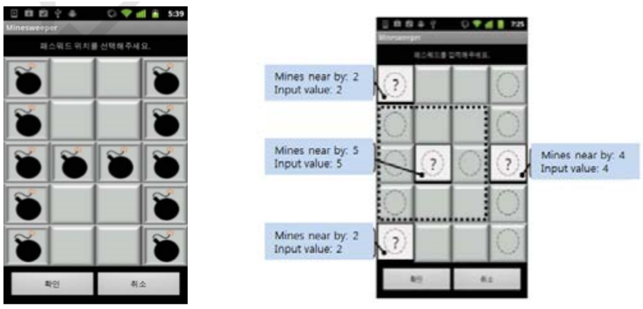


Fig. 5. Path selection authentication system

The user selects a start image, an end image, the pass images, and a mine image when the password is set. When prompted to login, the user begins from the start image and traces a path through the pass images in order to reach the end image. If the path passes through the mine image, the authentication fails. As with R-Point and grid-based systems, path-selection authentication systems can prevent shoulder-surfing attacks but are vulnerable to brute force attacks.

Another graphical password system, also announced in 2012, is derived from the classic Windows game, Minesweeper. [10] As shown in **Fig. 6**(a), the user sets their password by placing mines in a specific configuration. Authentication is achieved by selecting squares containing mines located one cell distance away from cells selected by the system (the cell marked with '?') as shown in **Fig. 6**(b).

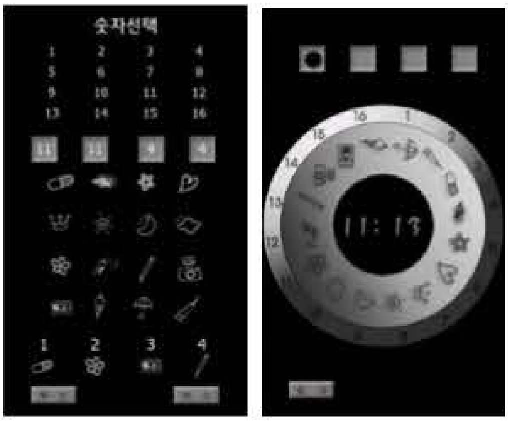


(a) (b)

Fig. 6. Minesweeper password system

This technique is relatively stronger than other systems against shoulder-surfing attacks and brute force attacks, however, it requires users to accurately remember the location of mines and time is required to calculate the number of mines.

The double-ring graphical password scheme, released in 2012, arranges 16 images in an inner ring and 16 numbers in an outer ring. A password is registered by pairing images with numbers. Authentication is granted after the user matches images to the corresponding numbers. [11]. Fig. 7(a) shows the password registration screen and Fig. 7(b) shows the password input screen for authentication.

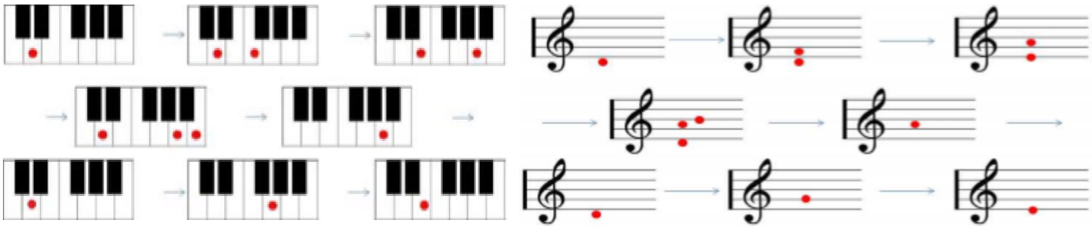


(a) (b)

Fig. 7. Password system using double ring

The double-ring password system, also, can prevent shoulder-surfing attacks, but the password entry space is relatively narrow compared to the previous methods.

The melody-based authentication method is a graphical password scheme that generates a melody by touching a piano key or a musical staff [12]. In this technique, a user touches a key to enter the password as shown in Fig. 8(a), or enters the password by touching locations on a musical staff, as shown in Fig. 8(b).



(a) (b)

Fig. 8. Melody-based authentication technique using keyboard and sheet music

Lengthy passwords can be memorized easily, but this method suffers from the same drawback as the double-ring method: it can be difficult to precisely click the position. Also, the input time of the password may be long.

The Korean-stroke-based graphical password technique is a system that utilizes input strokes of characters to be used as a password. The user generates a password by decomposing and simplifying both Korean consonants and vowel strokes [13]. The strokes used in Hangul are as follows: straight stroke, crossing stroke, diagonal stroke from the right, diagonal stroke from the left and circle stroke.

Straight: ↓
Crossing: →
Right diagonal stroke: ↙
Left diagonal stroke: ↘
Circle: O

These strokes are entered in the input window as shown in Fig. 9.

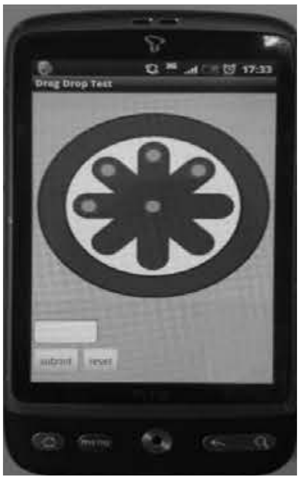


Fig. 9. Korean stroke-based graphical password system

For example, ' ' consists of a crossing stroke and a straight stroke. The Korean-stroke-based graphical password technique is easy to use but vulnerable to shoulder-surfing attacks.

Authentication technology using numerical patterns is a technique to enhance password security by inputting a numeric shape as a pattern [14]. The user memorizes four numbers as a password and draws the shape of each number in the input window and stores the password sequence. The password sequence of the left side pattern of Fig. 10 is "2-3-6-5-4-7-8", and the password sequence of the right side pattern is "1-2-5-4-7-8". This same number '2' is recognized as different passwords depending on the pattern, and because it is a pattern-based password, it is possible to construct a password through the path of the pattern. In this way, it is difficult to guess the password by inputting a combination of numbers as a pattern, which greatly improves security [14].

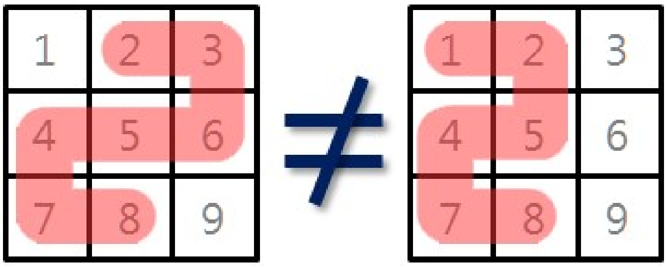
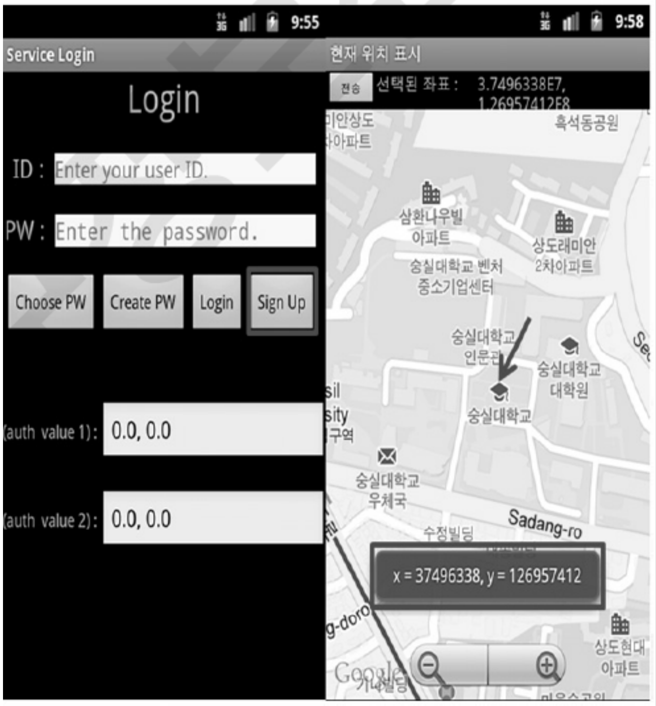


Fig. 10. Pattern-based numeric password

In a pattern-based numeric password authentication system, the user achieves authentication with a long pattern sequence to enhance security. The system uses a number shape instead of numeric entry to strengthen the security of the password. However, this method of authentication can be easily compromised by shoulder surfing.

The GPS-based graphical password scheme, released in 2013, uses GPS location information generated by smart phones [15]. This technique uses two authentication values. One value tracks the position of the mobile phone, and the other is the GPS coordinate value registered by the user. Since the GPS-based graphical password system requires the user to input the location information on the screen as shown in Fig. 11, it is difficult to select the exact location, and the current location information cannot serve as the password but the device ID can be used as a password.



Service Login

Login

ID : Enter your user ID.

PW : Enter the password.

(auth value 1): 0.0, 0.0

(auth value 2): 0.0, 0.0

현재 위치 표시

선택된 좌표 : 3.7496338E7, 1.26957412E8

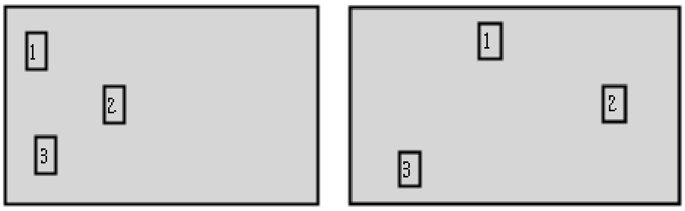
x = 37496338, y = 126957412

Fig. 11. GPS-based graphical password system

Character-based graphical password systems, first devised in 2014, utilize titles on book covers in a novel way. [16] The user registers several characters as passwords, the same as a text-based password system. The authentication process begins by displaying nine book covers. The user then selects a book cover containing the first character of the password. This process is repeated until the entire password is entered and authenticated. This system is vulnerable to brute force attacks because the password space is not large enough. Also, the password input process can be lengthy.

PassPositions, a graphical password system released in 2014, is a new graphical password system that uses the relative position information of selected points [17]. The PassPositions system is similar to the PassPoints system [4, 18] in that you enter the password by clicking anywhere in the input window in order. However, PassPoints uses the absolute position information of the clicked points as passwords, while PassPositions use the relative position information of clicked points as passwords.

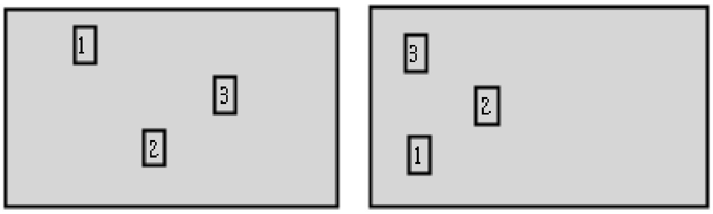
This is how it works: a user selects a point, ‘a’, by clicking on the input window. PassPositions determines the absolute position of ‘a’. Next, the user clicks on a second point, ‘b’. The absolute position of ‘b’ is determined and the position of ‘b’ relative to ‘a’ is calculated. That is, the system determines if it is above, below, or to the left or right of ‘a’. When ‘c’ is input, the system does the same thing: it determines the absolute position of ‘c’ and the relative position of ‘c’ to ‘b’. The pattern of relative positions is compared to the registered pattern in the system and authentication is granted or denied. The users only need to select points that will distinguish their relative positions. **Fig. 12** shows two cases where the relative positions of selection points are the same. The number in the selection points is the selection order.



(a) (b)

Fig. 12. Cases with the Same Relative Positions

The order of selection points $\boxed{1}$, $\boxed{2}$, $\boxed{3}$, is the same in **Fig. 13** (a) and **Fig. 13** (b). Their absolute positions are different. However, their relative positions are the same. In both cases, $\boxed{2}$ is at the lower right of $\boxed{1}$ and $\boxed{3}$ is at the bottom left of $\boxed{2}$. In the Passpoints system, the patterns represented in **Fig. 12** (a) and **Fig. 12** (b) would be considered different, but in PassPositions they are treated as the same pattern. By contrast, **Fig. 13** (a) and **Fig. 13** (b) would be treated as different passwords



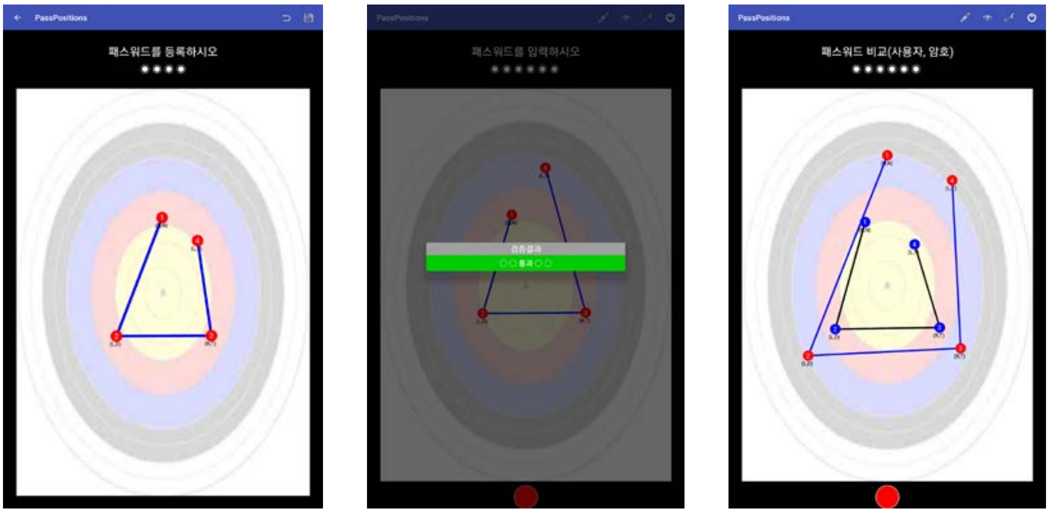
(a) (b)

Fig. 13. Cases with Different Relative Positions

In PassPoints, authentication is granted only by clicking exactly the same (absolute) positions specified during password registry, whereas PassPositions uses the relative position information of the clicked points for authentication. Therefore, even if you click different absolute positions than the ones you clicked at the time of registry, authentication is completed as long as the relative positions are entered in the correct order. Therefore, people who have difficulties clicking on precise locations can use PassPositions easily. Also, the people who use PassPositions can enter passwords faster than the people using PassPoints. Furthermore, PassPositions’ security against shoulder-surfing attacks is stronger than PassPoints, because users don't need to click exactly the same location each time you enter the password. The one minor drawback is the reduced password space available in PassPositions.

PassPositions can be made even more practical when used in mobile devices that operate directly using the touch pad with hands. When using a tool, such as a mouse or an electronic fan, it is relatively easy to select a narrow area more accurately than when using a finger. PassPositions also allows users to freely select images for your background as you would in the PassPoints system. Alternately, users can opt to have no background picture. That is to say: the user can customize their password entry system.

Recently, the PassPositions system was adapted to the Android platform. **Fig. 14**(a) shows the input window of PassPositions system, and **Fig. 14**(b) shows the case of successful authentication. **Fig. 14**(c) is a function to compare the registered information with the input information, and it is not used in actual system operation. (The solid lines and dots in the window in **Fig. 14**(a) are not visible when operating the system. This is to prevent shoulder-surfing attacks.)



(a) **(b)** **(c)**

Fig. 14. PassPositions system

PassPositions II, released in 2017, improves upon the previous PassPositions system. It provides a larger password space and is more user-friendly than the first PassPositions system [19]. The relative position calculation in PassPositions II is different from PassPositions. Whereas the first version tracked the relative positions sequentially (e.g., ‘b’ to ‘a’, then ‘c’ to ‘b’, then ‘d’ to ‘c’), PassPositions II tracks the relative position of newly-entered points by comparing its position to all previously entered points (‘b’ to ‘a’, ‘c’ to ‘a’ and ‘b’, ‘d’ to ‘c’, ‘b’, and ‘a’, etc.).

In the old PassPositions system, if a new click occurred on the same vertical or horizontal axis as the previous click, it caused an error. Furthermore, it was difficult for the user to accurately discern whether a new click was on the same axis or not. In order to overcome these disadvantages, PassPositions II extended the width of the lines extending vertically and horizontally to enhance the usability.

4. Comparison and Analysis of the Graphical Password Schemes Developed in Korea

The comparison of graphical password schemes investigated in the previous section is presented in this section. There are many criteria to compare graphical password schemes, but we compare the schemes using three general categories: characteristics, security and usability **Table 1** shows the list of graphical password schemes along with their types, strong points, weak points, and year points, and years of release.

Table 1. Characteristics of the graphical password schemes

Scheme	Type	Strong points	Weak points	Year
①R-Point technique	Cued-recall	Shoulder-surfing attack	Brute force attack	2006
②Grid-based password system	Recognition	Shoulder-surfing attack	Brute force attack	2010 and 2011
③Path selection authentication system	Recognition	Shoulder-surfing attack	Brute force attack	2011 and 2012
④Password system applying minesweeper game	Recall	Shoulder-surfing attack & Brute force attack	Login time & Memorability	2012
⑤Password system using double ring	Recognition	Shoulder-surfing attack	Brute force attack	2012
⑥Melody-based authentication technique	Cued-recall	Memorability	Input accuracy & time	2012
⑦Korean stroke-based graphical password	Recall	Easy to use	Shoulder-surfing attack	2012
⑧Pattern-based numeric password	Recall	Easy to use	Shoulder-surfing attack	2012
⑨GPS-based graphical password system	Cued-recall	Shoulder-surfing attack	Hard to use	2013
⑩Character-based graphical password	Cued-recall	Advertising tool	Brute force attack & Login time	2014
⑪PassPositions	Recall/ Cued-recall	Easy to use	Brute force attack	2014
⑫PassPositions-II	Recall/ Cued-recall	Easy to use & Security	Memorability	2017

A few points are worth noting: research began around 2006. There was a noticeable uptick in graphical password research beginning in 2010 and extending through 2014. Among the graphical password systems developed in Korea since 2006, there were more recall-based systems than recognition-based systems. They tried to overcome shoulder-surfing attacks while achieving strong security. If they are weak to brute force attacks, it means their password space is not large enough. Although the number of studies on graphical password systems in Korea is low, there are some studies and they are at a level comparable to other countries.

Security is the *raison d'etre* of authentication systems. Their sole reason for existence is to grant access only to approved users. Hence, they should prevent a user's credentials from being compromised by attacks. A brief discussion of attack types is in order.

Attacks are classified as guessing attacks, capture attacks, and task-performing attacks. For example, brute-force attacks and dictionary attacks. Capture attacks are exemplified by shoulder-surfing and reconstruction attacks. Social engineering attacks and malware attacks require the performance of extra tasks and are hence classified as task-performing attacks. **Fig. 15** shows the types of attacks.

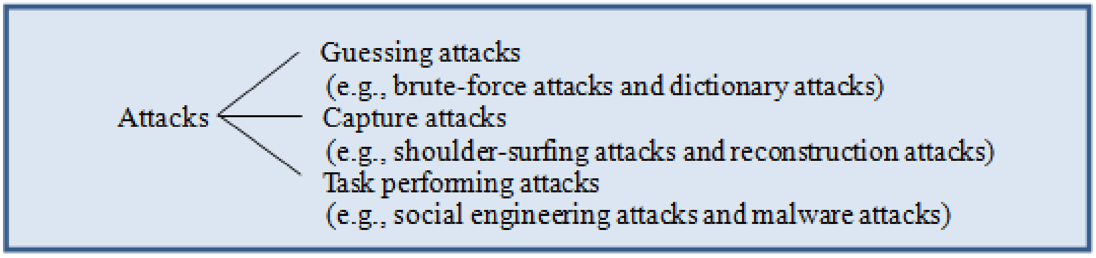

Attacks
Guessing attacks
(e.g., brute-force attacks and dictionary attacks)
Capture attacks
(e.g., shoulder-surfing attacks and reconstruction attacks)
Task perfoming attacks
(e.g., social engineering attacks and malware attacks)

Fig. 15. Types of attacks

The first one is brute force attacks. Brute force attacks use trial and error exhaustively attempt input combinations until hitting upon the correct one. A full search of very large password spaces for brute force attacks is limited by time. Hence, in order to minimize the threat of brute force attack, the theoretical password space should be too large to search. Usually, a recognition-based system is susceptible to brute force attacks.

A dictionary attack is an attack method by guessing passwords from a dictionary (i.e., list of high probability candidate passwords) which is prepared by collecting data on a user's behavior. A dictionary modeled collectively as a probable password space. To minimize the threat of dictionary attacks, the dictionary (effective password space) must be too large to search.

Shoulder-surfing attacks try to gain login information by observing the user entering the password directly or by recording the user's behavior. A reconstruction attack pools together information gathered from observing several logins. Many graphical password schemes, which tried to avoid shoulder-surfing attacks, have drawbacks on usability.

There are various types of task-performing attacks. Malware attacks use software, such as a Trojan horse, to gather and transmit a user's information without their permission. Phishing and pharming attacks try to trick users into using fraudulent websites. Social engineering attacks attempt to deceive a user into voluntarily disclosing their credentials by gaining their confidence in person-to-person contact. One common method is a "social engineer" pretending to call from a help desk. The unsuspecting victim then believes they are giving their information to a trusted authority. Finally, a smudge attack uses the residual oils from a finger left on a touchscreen device, such as a cell phone or tablet computer. Oily residues and/or smudges generated by touching on a touch screen can be used to infer recently and frequently touched locations. Attackers may inspect the smudges and attempt to extract user's sensitive information. A research result shows that Android password patterns were able to break 68% of the time under proper conditions [20].

There are many aspects to consider in order to measuring the security of graphical password schemes, but we select three important types of attacks to compare security stability levels of the graphical password schemes presented here: shoulder-surfing attack, brute force attack, and smudge attack.

Table 2. Comparison of security stability levels

Scheme	Shoulder-surfing attack	Brute force attack	Smudge attack
R-Point technique	Middle	Low	High
Grid-based password system	High	Low	High
Path selection authentication system	High	Middle	High
Password system applying minesweeper game	Middle	High	High
Password system using double ring	Low	Low	High
Melody-based authentication technique	Middle	High	High
Korean stroke-based graphical password	Middle	High	Middle
Pattern-based numeric password	Low	High	Middle
GPS-based graphical password system	Middle	Middle	Middle
Character-based graphical password	Middle	Low	High
PassPositions	Middle	Low	High
PassPositions-II	Middle	High	High

Table 2 compares the security stability levels of shoulder-surfing attacks, brute force attacks and smudge attacks. ‘High’ indicates the highest level of security and ‘Low’ indicates the lowest. ‘Middle’ indicates the mid-level of security stability.

Most graphical password schemes investigated here are not able to prevent the various attacks simultaneously. However, it might be possible to create a graphical password scheme that can prevent various attacks simultaneously if we take advantages from various graphical password schemes presented here.

While the security stability level is one of the important factors of a graphical password system, usability is another. Since there has essentially been no accepted standard for evaluating the usability of graphical password systems, most systems have been tested using different criteria. There are three important factors used to investigate the usability of graphical password schemes presented here: memorability, login time, and ease of use.

Memorability is one of greatest advantages that graphical password systems have over text-based password systems. According to psychology studies, human memory is far better at recognizing and recalling visual information than textual information [21, 22]. Ease of login, including the time to create a password and the time to complete a login, is the most frequently examined usability standard. The login should be quick and simple since it is the most frequently performed task by users of an authentication system. Memorability issues are strongly related to login performance since memorability is a main factor determining login success. Also, memorability depends on whether passwords can be remembered over short- and long-term and with varying login frequencies.

Table 3 shows the usability level of each scheme according to memorability, login time, and ease of use. High memorability means that it is easy to memorize the password and high login time means that it takes long time to login. Also, high ease of use means it is easy to use the system.

Table 3. Usability level of each scheme

Scheme	Memorability	Login time	Ease of use
R-Point technique	Middle	Middle	Middle
Grid-based password system	Low	High	Middle
Path selection authentication system	Low	High	Middle
Password system applying minesweeper game	Low	High	Middle
Password system using double ring	Middle	Low	High
Melody-based authentication technique	Middle	High	Middle
Korean stroke-based graphical password	Middle	High	Middle
Pattern-based numeric password	Middle	Middle	Middle
GPS-based graphical password system	Middle	Middle	Middle
Character-based graphical password	Middle	Middle	High
PassPositions	High	Low	High
PassPositions-II	Middle	Middle	High

The usability of PassPositions is ideal for the graphical password system. However, achieving both strong security and high usability concomitantly is an important goal for the development of a graphical password system with higher levels of maturity and usefulness. **Fig. 16** shows the relative position of each graphical password schemes investigated so far according to security and usability.

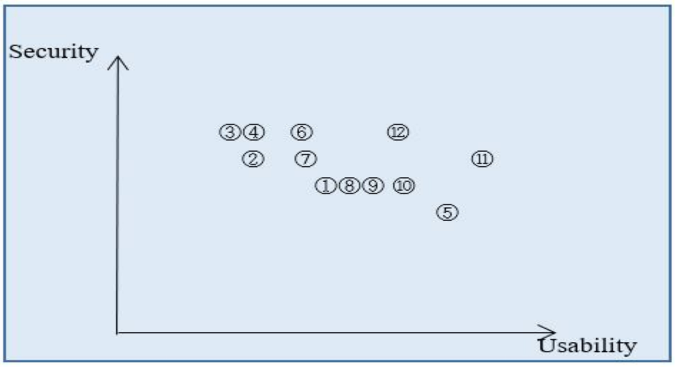


Fig. 16. Security and usability

Each number in **Fig. 16** indicates a graphical password scheme listed in Table 1. The graphical password schemes ③④ and ①⑧⑨ are located in the same position in **Fig. 16**. Located in the upper right corner of **Fig. 16** is the ideal graphical password system which can be designed by increasing security and usability simultaneously. Most graphical password systems investigated in this paper have trade-offs, where increased security implies decreased usability. However, according to our analysis of graphical password schemes, research efforts could trend toward an increase in both security and usability as research and development continue. As we investigated so far, graphical Password schemes developed towards to increase the security while maintaining good usability. However, there is no one perfect password system everybody agreed on yet. It is a good point that recently developed graphical password systems are better than the systems developed earlier in terms of achieving the goal for both security and usability together in one system. There are efforts still on going to develop more sophisticated graphical password systems, even though there is trade off between security and usability and it is cumbersome to achieve both in one password system. The development speed of graphical password system in Korea is fast enough to catch up and lead the global state of the art research on graphical password system in the near future.

5. Conclusion

Graphical password authentication techniques are one of the major authentication schemes actively researched around world and have received much recent attention. In this paper, the development status and prospects of graphical password authentication systems in Korea were presented. To do this, a comprehensive survey of existing graphical password research results was culled from the papers contained in the Computer Research Information Center in Korea and on the internet. The research results were described in chronological order. The current graphical password techniques can be classified into four categories: recognition-based, recall-based, cued-recall and hybrid techniques. A comparison of investigated graphical password techniques was presented in Tables 1, 2, and 3.

The research began around 2006. Graphical password research sharply increased beginning in 2012. There have been more recall-based systems than recognition-based systems developed in Korea since 2006. Surprisingly, there were no hybrid graphical password systems among those investigated. They primarily aimed at overcoming shoulder-surfing attacks while maintaining strong security. Although the number of studies on graphical password systems in Korea is relatively low, it is comparable to that of other countries.

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (2017R1D1A1B04032968).

References

[1] A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," *Communications of the ACM*, vol. 42, pp.40–46, 1999. Article (CrossRef Link)

[2] R. N. Shepard, "Recognition memory for words, sentences and pictures 1," *Journal of Verbal Learning and Verbal Behavior*, vol. 6, pp.156–163, 1967. Article (CrossRef Link)

[3] Aviv, Adam J. Gibson, Katherine, Mossop, Evan, Blaze, Matt, Smith, Jonathan M., "Smudge Attacks on Smartphone Touch Screens," in *Proc. of 4th USENIX Workshop on Offensive Technologies*. Article (CrossRef Link)

[4] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *International Journal of Human Computer Studies*, vol. 63, pp. 102-127, 2005. Article (CrossRef Link)

[5] T. Seong, G.-W. Park and Y.-S. Byun, "A Study on Graphical Passwords," in *Proc. of 26th KIPS Fall Conference*, vol. 13, no. 2, 2006. Article (CrossRef Link)

[6] J.-W. Kim, S.-H. Kim, K. Kim and H.-G. Cho, "A Shoulder-Surfing Resistant Graphical Password Using Hangul Choseong," in *Proc. of KISS Fall Conference*, vol. 37, no. 2(A), pp. 95-96, 2010. Article (CrossRef Link)

[7] J.-W. Kim, S.-H. Kim, K. Kim and H.-G. Cho, "Improvement of the Grid-based Password System Resistant to Shoulder-Surfing Attacks, "*Journal of KISS*, vol. 17, no. 4, 2011. Article (CrossRef Link)

[8] G. Moon, J. Kim and M. Hong, "A Graphic Password Scheme using Eulerian Path," in *Proc. of the Korea Computer Conference*, vol. 38, no. 1(D), 2011. Article (CrossRef Link)

[9] G. Moon, J. Kim and M. Hong, "A Graphical Password Scheme Resistant to Shoulder-Surfing Attack in Mobile Environments," *Journal of KISS*, vol. 18, no. 1, 2012. Article (CrossRef Link)

[10] T. Kim, S. Kim, E. Park and J.H. Yi, "Minesweeper Game Based Password Authentication Scheme Resistant to Shoulder-Surfing Attack," in *Proc. of 37th KIPS Spring Conference*, vol. 19, no. 1, pp. 654-657, 2012. Article (CrossRef Link)

[11] G. Park, A. Kim and S.-H. Lee, "A Graphic Password Scheme based on Structure of Double Rings Resistant to Smudge and Shoulder Surfing Attack," in *Proc. of the Korea Computer Conference*, vol. 39, no. 1(C), 2012. Article (CrossRef Link)

[12] J. An, S. Kim, A. Kim and S.-H. Lee, "A Melody-based Authentication Scheme by using Piano Key and Score," in *Proc. of the Korea Computer Conference*, vol. 39, no. 1(C), 2012.

[13] T. Ko, T. Shon and M. Hong, "A Study on the Korean-Stroke based Graphical Password Approach," *Journal of KIISC*, vol. 22, no. 2, pp. 189-200, 2012. Article (CrossRef Link)

[14] S.-H. Ju and H.-S. Seo, "A study on User Authentication Technology of Numeric based Pattern Password," *Journal of the Korea Society of Computer and Information*, vol. 17, no. 9, pp. 65-73, 2012. Article (CrossRef Link)

[15] T.E. Kim, H.H. Kim and M.S. Jun, "A study on the SmartPhone GPS based Graphical Password Approach," *KIPS Transactions on Computer and Communications System*, vol. 2, no. 12, pp. 525-532, 2013. Article (CrossRef Link)

[16] H. Jeong, A. Kim and S.-H Lee, "A Text-based Graphical Password by Using Titles on Book Covers," in *Proc. of the Korea Computer Conference*, vol. 41, no. 1, pp. 2000-2002, 2014. Article (CrossRef Link)

[17] G.-C. Yang and H. Kim, "A New Graphical Password Scheme Based on Universal Design," *Journal of Digital Convergence*, vol. 12, no. 5, pp. 231-238, 2014. Article (CrossRef Link)

[18] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in *Proc. of Human-Computer Interaction International (HCII 2005), Las Vegas*, *NV*, 2005.

[19] G.-C. Yang, "PassPositions: A Secure and User-Friendly Graphical Password Scheme," in *Proc. of the 4th International Conference on Computer Applications and Information Processing Technology (CAIPT) 2017*, *Bali*, 2017. Article (CrossRef Link)

[20] Rachna Dhamija, Adrian Perrig, Déjà Vu, "A User Study Using Images for Authentication," in *Proc. of the 9th USENIX Security Symposium, Denver, Colorado, USA*, August 14-17, 2000. Article (CrossRef Link)

[21] Kirkpatrick, E. A., "An experimental study of memory," *Psychological Review*, 1, 602–609, 1894. Article (CrossRef Link)

[22] S. Madigan, "Picture memory," *In J. Yuille, editor, Imagery, Memory, and Cognition: Essays in Honor of Allan Paivio, chapter 3*, pages 65–89, Lawrence Erlbaum Associates, 1983.

Gi-Chul Yang received his M.S. degree from Department of Computer Science, the University of Iowa, USA in 1986 and PhD degree in Computer Science and Telecommunications Program from the University of Missouri, USA in 1993. Currently, he is a Professor at Mokpo National University, where he has been working since September 1993. He was also a Director of Information & Computing Institute, School of Information Engineering at Mokpo National University. His research interests include Artificial Intelligence (AI) and Human Computer Interaction (HCI). He was a Visiting Scholar at Heriot-Watt University and University of Hamburg in 2002 and 2015, respectively. He collaborated with professors at Linkoping University, University of Zurich, University of Missouri, University of Auckland, and Drexel University. He is an author of several books (written in Korean) and was an editor of Springer's Transactions of Engineering Technologies.