A Multimodal Password System based on Graphics and Text

Gi-Chul Yang, *Member, IAENG*

ABSTRACT—Password systems should be secure and easy to use. However, text-based systems require passwords that can be difficult to remember, while graphical systems require passwords with lengthy input times. In addition, shoulder-surfing attacks are a difficulty common to both. This paper discusses a multi-modal password system called GTPass. GTPass uses both graphics and text to capitalize on the advantages and eliminate the drawbacks of both systems. GTPass introduces a new password input scheme called TIS (Transformed Input Scheme) to solve existing problems in graphical password systems and text-based password systems. GTPass users can memorize the password easily and the passwords require very little time to enter. TIS can potentially be used to generate large password spaces. Accordingly, GTPass will be easy to use and highly resistant to a variety of attacks.

Index Terms—Graphical password, shoulder-surfing attack, security, authentication

I. INTRODUCTION

NOWADAYS a user may have multiple secured accounts. Ideally, each account will have a unique and suitably long password with diverse alphanumeric characters to strengthen the security. However, long, text-based passwords are hard to remember. Since it can be cumbersome to utilize all different passwords for each account, a user may use the same password for all accounts. Using one password for many accounts is a very dangerous habit: if just one account is compromised, then they are all compromised. Due to this dangerous but natural response to the demands of text-based passwords, there is a trend to replace text-based password systems with graphical password systems. There are also various developments for authentication and security [1, 2]. Graphics are easier to memorize than text [3, 4]. This makes graphical password systems more user-friendly. But it also makes them more vulnerable to shoulder-surfing attacks, since others can remember graphics easily, too.

A shoulder-surfing attack occurs when an attacker acquires a target's credentials by simply looking over their shoulder. The defense of a user's credentials from shoulder-surfing attacks is one of the biggest and most general problems that any password system faces. This problem is worse in graphical password systems because they are easier to remember.

The Transparent Image Moving (TIM) schema currently provides one of the best solutions to the problem of shoulder-surfing attacks [5]. In TIM, a user can move the password images up, down, left, or right without touching the image directly. Hence, an attacker would not be able to acquire a user's password by observing the login process. TIM introduced an excellent method to prevent shoulder-surfing attacks.

Chiasson and her colleagues raised an interesting research question for text-based passwords:

> "Can cueing mechanisms be (safely) added to text passwords in order to achieve the same memorability advantages seen in click-based graphical passwords?" [6].

In light of the strengths and flaws of both kinds of system, this question should be re-posed as, "Can a password system have both advantages of graphical passwords and text-based passwords while avoiding their drawbacks?" This paper answers that question in the affirmative by introducing an efficient password system called 'GTPass' (Graphic & Text based Password system). GTPass uses graphics and text to adopt the advantages of both types of password. A user needs to select and memorize images to set the password and type numbers to login. An important feature of GTPass is input variability: each login requires the user to input different numbers for the password, since password images will appear in random locations on the interface grid.

GTPass is strongly secure and easy to use. GTPass provides a robust defense against various attacks, including shoulder-surfing attacks, since it uses the Transformed Input Scheme (TIS) for password input. TIS is an password input scheme that makes it possible to input a password without indicating the password entity directly. For example, a user's password entity is an image, but the login procedure uses a number to submit the image as a password. The corresponding relation between the image and the number is not one-to-one. It varies each login, so it is difficult to acquire a user's password entity. Also, GTPass requires a relatively short login time, since a user types numbers instead of moving images to login.

The next section explains three recent developments. GTPass is described in detail in section 3. Section 4 concludes the paper.

Manuscript received May 29, 2019; revised July 05, 2019. This research was supported by basic science research program through the national research foundation of Korea (NRF) and funded by the ministry of education, science and technology (2017R1D1A1B04032968).

G.-C. Yang is with the Mokpo National University, Mokpo, Korea. (Corresponding author to provide phone: +82-61-450-2355; fax: +82-61-450-2358; e-mail: gcyangr@ mokpo.ac.kr).

.

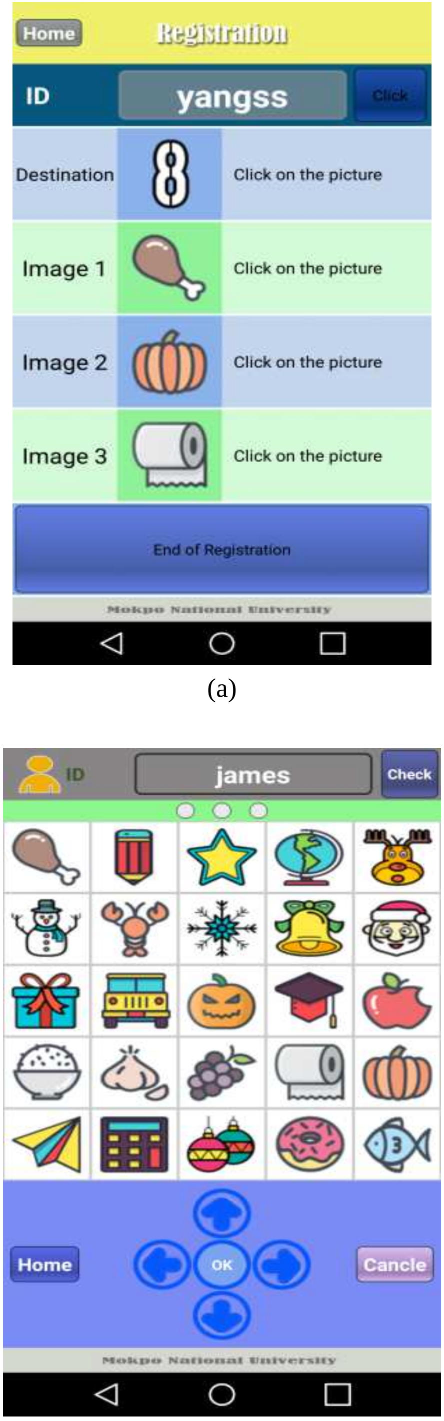
II. RECENT DEVELOPMENTS

Research in graphical password schemes, which increase security and usability, has accelerated over the last five years. It is generally difficult to compare different approaches because they vary in the selection of features. The wide range of previous approaches can be seen in the comprehensive survey in [7, 8]. Further complicating comparisons between different studies is the fact that authentication performance depends on how the authentication system is designed and the experimental methods used to evaluate usability. Unfortunately, a set of universal testing standards does not exist. Hence, this section describes three current graphical password schemes, but lacks an in-depth comparison. However, the information presented will be sufficient to show how the GTPass system introduced in this paper is an improvement over existing systems.

The graphical password was first proposed by G. Blonder [9]. Instead of alpha-numeric codes, it uses pre-selected small regions in an image to compose a password. The user has to choose some of these regions as a password, and the user must click in each one of the chosen regions in the correct order to login. One example is the graphical password scheme PassPoints. It allows any image to be used, and does not require artificial, pre-defined click regions with well-marked boundaries [10]. A different system, PassPositions, is a graphical password authentication scheme which uses relative positions of the click points [11]. PassPositions remembers the relative positions of the chosen points. The relative position indicates the direction of the current chosen point according to the previously chosen point. Both PassPoints and PassPositions use the locations of click points as a password entity. However, this password input scheme is vulnerable to shoulder surfing attacks, since others can possibly catch a user's click points by observation.

Alternately, the TIM scheme is a form of security authentication that obtains an authentication through the movement of a number of images to a pre-determined position [5]. The images appear in a grid-like window displayed on an input device (for example, a touch-based input device). **Fig. 1(a)** shows a registration screen choosing 8 as a destination and a drumstick, a pumpkin, and a toilet paper roll as the password images.

In the password authentication step, the selected password images are moved in order to the selected destination positions one by one through the interface shown in **Fig. 1(b)**. The authentication is performed by confirming the final position of the selected image(s), regardless of the path taken to the selected destination. The images can be manipulated by a direction key, a touch pad, a mouse, or other similar methods and devices. The TIM technique solves the problem of shoulder-surfing attacks; However, TIM does have a longer login time than text-based password systems.



ID yangss

Destination 8 Click on the picture

Image 1 Click on the picture

Image 2 Click on the picture

Image 3 Click on the picture

ID james

(a)

(b)

Fig. 1. Authentication processing steps of TIM

The goal is to develop a graphical password authentication system which has the highest security and the highest usability. A new, multi-modal password authentication system called GTPass was designed to meet both criteria. GTPass improves existing transparent password entity designation schemes, speeding up password input times while maintaining strong security. This system will be described in section 3.

III. A PASSWORD SYSTEM BASED ON GRAPHICS & TEXT

GTPass uses graphics and text simultaneously to utilize the advantages of graphical passwords and text-based passwords. Images are used when registering their password, and numbers are used when logging in. Images are easier to memorize than text (including numbers) and numeric login provides a shorter login time than using image movement. It is an innovation that can solve many problems in existing password schemes.

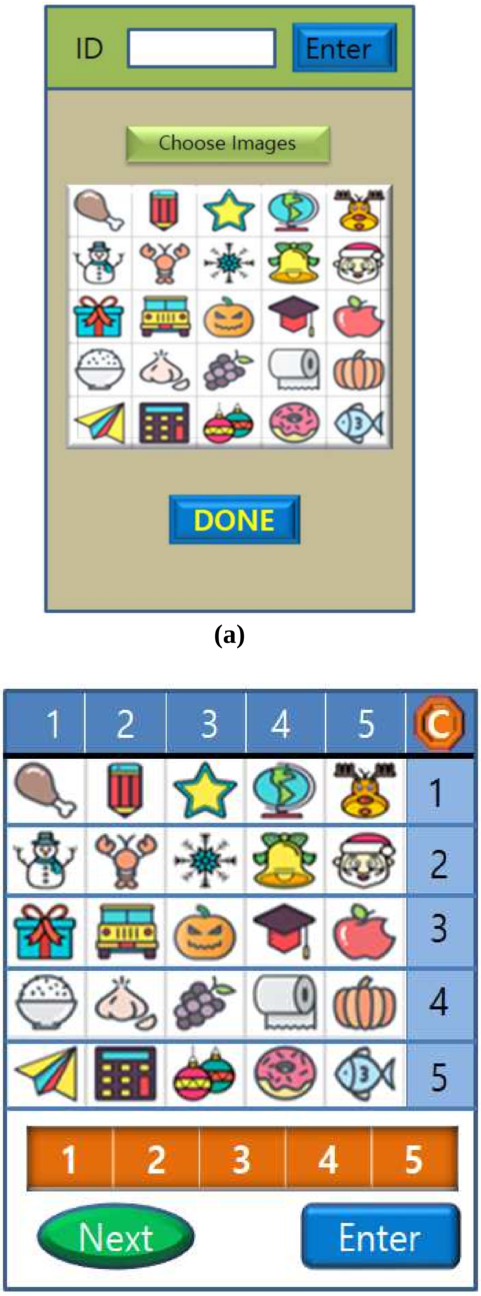
A user memorizes images to set the password. To login, the user types numbers that appear on the interface to login. The user does not need to memorize the numbers. Images are the real password entities, but the numeric symbols are used to submit a password for login. This kind of password input scheme is the Transformed Input Scheme (TIS) of password input introduced in this paper.

TIS is a password input scheme that makes it possible to avoid indicating the password entity directly. If a password system uses TIS, then a user can submit the password to the system without manipulating the real password entity. This makes it difficult to identify the password entity. TIS also increases the usability by allowing users to memorize images rather than text and reduces the login time by using numbers for password input. TIS makes the password system secure and easy to use.

A. GTPass System

GTPass has a secure and efficient password authentication scheme. The important feature of GTPass is the use of graphics and numbers for authentication. GTPass uses graphics and numbers together but do not require memorizing numbers. Users just need to memorize chosen graphics only for their password. In addition, GTPass utilizes location information along with TIS to prevent shoulder-surfing attacks and speed up the login time. **Fig. 2** shows the interfaces of GTPass. The interfaces shown in **Fig. 2** use 25 images. Those images can be changed to others as needed. The number of images can be changed also. For example: we can use 7 x 7 image grid instead of 5 x 5 to increase the security.

GTPass proceeds in two steps: password registration and password authentication. At the password registration step, a user makes an ID and chooses as many image(s) as desired from **Fig. 2(a).** After the user selects the desired number of images, they click 'DONE'. Later, at the password authentication step, a user types two numbers for each image selected at the registration step. The two numbers indicate the column and row number of the image appearing on the interface as shown in **Fig. 2(b).** To select each image, the user types the number on top first and the number on the right side second.



(a)

(b)

Fig. 2. GTPass interfaces

The number on top indicates column and the number at the right hand side indicates row of the selected image. For example, if a user's password image is the star in **Fig. 2(b),** then the user types a '3' and a '1'. Then, the user clicks the 'Next' button to proceed to the next image. This process will be repeated for every image the user registered. The images on the interface are randomly redisplayed each time the user clicks the 'Next' button. After submitting the numbers that correspond to all of the password images, the user clicks the 'Enter' button to complete the authentication.

An example: a user selects the star, the garlic bulb, and the fish as password images to register. Then, they click 'Done'. When the user authenticates their password, they will first need to enter '31' for the star (as in **Fig. 2(b)**) and then click 'Next'. After that, the user will need to enter '24' for the garlic bulb and click 'Next' again (Note: For simplicity in this example, we are assuming that the display does not change the order of the images. However, the order of the images on the authentication screen can change configuration.) Finally, the user will enter a ‘55’ for the fish and click ‘Enter’. This will complete the authentication process. Alternately, GTPass can be configured to allow the user to enter a single number that corresponds to the sequence of their registered image locations on a single screen. In this alternate configuration, the user would just enter ‘312455’ and then click ‘Enter’ to complete the authentication process.

In either case, since the image locations change on each login attempt, the user will enter different numbers. Inputting different numbers for the same image makes it difficult for an attacker to compromise the user’s password. TIS adds cueing mechanisms for numeric passwords to GTPass in order to achieve the same memorability advantages seen in click-based graphical passwords. In addition, GTPass enlarges the number of possible numeric password permutations. It thereby increases the password space.

As we can see here, the actual entity of a password (i.e., an image) is transformed into a number when submitted to the system for authentication. TIS can prevent shoulder-surfing attacks and shorten login time. As explained above, GTPass authenticates the user in two steps. Here is the process in an abbreviated format:

Registration Step:

(1) A user creates his/her profile by entering a username.
(2) The user selects an image.
(3) The user repeats (2) as many times as necessary to create the desired password.
(4) The user completes the registration step by pressing the ‘DONE’ button.

Authentication Step:

(1) The GTPass system prompts the user for their username. The user enters the username.
(2) The user inputs two-digit numbers corresponding to the column and row location of each image (either in sequence or all at once).
(3) After the inputting all the numbers, the user presses the ‘ENTER’ button to login.

B. The Password Space of GTPass

GTPass provides a strong defense against brute force and guessing attacks, as well as shoulder-surfing attacks and others. GTPass uses TIS to prevent shoulder-surfing attacks. It is also difficult to guess the password because it has a larger password space than a standard numeric password.

For GTPass, the password space is calculated as follows:

The number of possible passwords that can be generated by three selections from 25 images will be:

$$25 * 25 * 25 = 15{,}625 \qquad (1)$$

(1) shows the password space of GTPass demo system described in the previous sub-section. If N is the number of password images selected from 25 images, then the password space P for GTPass is:

$$P = 25^{N} \qquad (2)$$

The general password space for GTPass can be calculated by the formula

$$P = (X * Y)^{N} \qquad (3)$$

where X is the number of columns and Y is the number of rows and N is the number of password images selected. For example, consider a grid of seven columns and seven rows with a password of eight images. The password space is

$$P = (7 * 7)^{8} = 33{,}232{,}930{,}569{,}601 \qquad (4)$$

Clearly, GTPass can generate a very large password space. Thus, it can provide a strong defense against brute force attacks. Most graphical passwords are vulnerable to shoulder surfing attacks, but GTPass provides strong security against them by using the TIS scheme. At every login, the positions of the images will vary. The randomness of image placement in the interface grid confuses potential attackers trying to memorize the password details. Thus, it is more difficult for any attacker to guess or crack GTPass passwords by observation. In this way, GTPass is highly resistant to shoulder-surfing attacks.

IV. Survey On The System

We conducted a survey of novice users to reveal their general impressions of the usability and security of the GTPass system. A total of 59 participants answered the survey questions after hearing an explanation of the system. These participants were male and female university students and had no prior experience with the GTPass password system. The answer choices used a Likert scale ranging from 0 to 10.

Regarding usability, we asked three questions. The first question was, “How long will it take to log in?” Participants answered based on their expected average login time. The second question was, “What is the rate of login failure?”. Participants answered based on the expected rate of login failure. The third question was, “How easy is it to use the system?”. Participants answered based on their general judgments of the usability of the GTPass system. We asked about security of the GTPass system for the last question. ″How easy do you think it is to gain someone else's password by watching the login process?”

The result of the first question on login time is shown in **Fig. 3**. Here, a ‘0’ indicates the shortest time and a ‘10’ indicates the longest time.

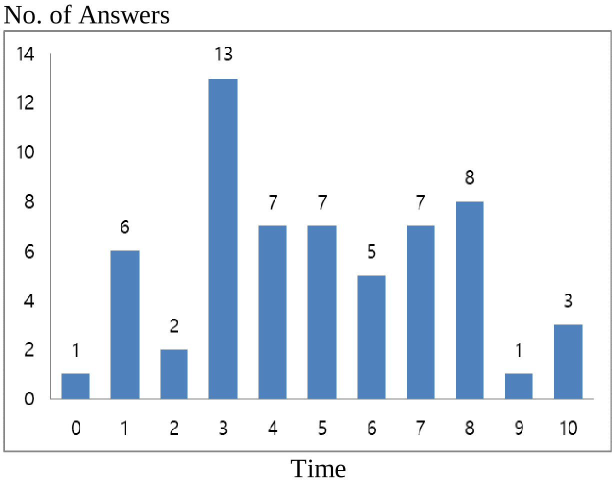


Fig. 3. Answer distribution on login time.

The answer distribution of the first question indicates that the GTPass system is not different from current alphanumeric password systems.

The result of the second question on the rate of login failure is shown in Fig. 4. Here, a ‘0’ indicates no failure and a ‘10’ indicates the highest possible rate of login failure.

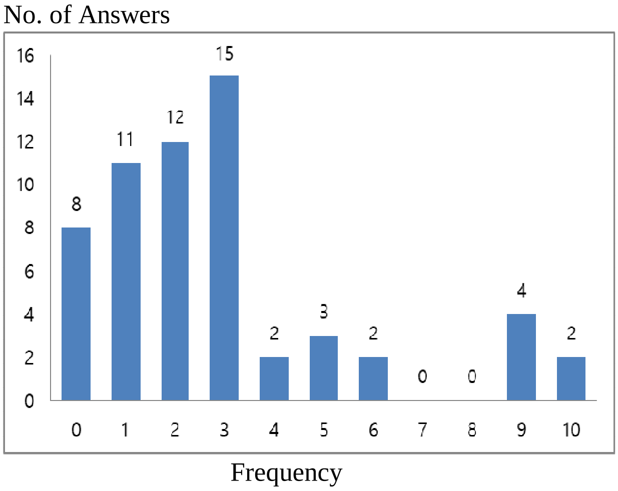


Fig. 4. Answer distribution on error rate.

The answer distribution of the second question indicates clearly that the GTPass system has a strong defense against errors.

The result of the third question on convenience of usage is shown in Fig. 5. Here, a ‘0’ indicates that it is very easy to use the system and a ‘10’ indicates that it is very difficult to use the system. The answer distribution of the third question indicates that the usability of the GTPass system is marginal.

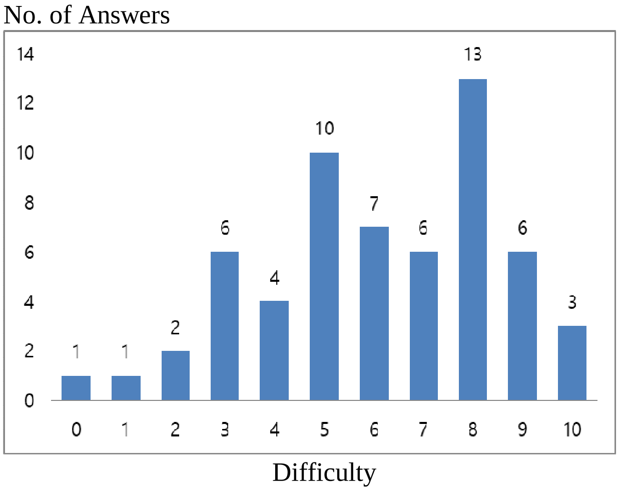


Fig. 5. Answer distribution on convenience.

Regarding security, we asked, “How easy do you think it is to gain someone else's password by watching the login process?” The result is shown in **Fig. 6**. Here, a ‘0’ indicates that gaining someone’s password is very easy and a ‘10’ indicates that gaining someone’s password is very difficult.

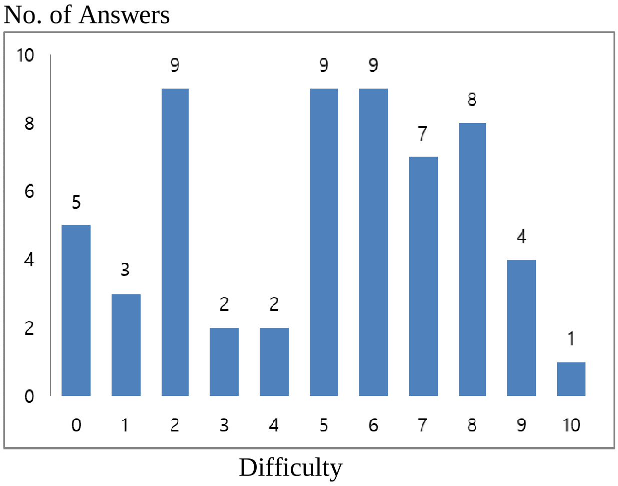


Fig. 6. Answer distribution on security.

The answer distribution of the security question indicates that the GTPass system is very secure. About 77% of the participants answered ‘5’ or above on the question. We can say that below 5 indicates that it is easy to attack and over 5 indicates that it is hard to attack. Overall, the survey showed that the GTPass system is easy to use and has strong security.

V. Conclusion

The past decade has seen a growing interest in using graphical passwords as an alternative to traditional text-based passwords. One alternative is graphical passwords, which have memorability advantages over text-based passwords. However, graphical passwords have drawbacks of their own. They usually require a longer login time than traditional text-based passwords. TIS combines the memorability of graphical passwords with the rapid entry of text-based passwords. It joins cueing mechanisms to text passwords in order to achieve the same memorability advantages seen in click-based, graphical passwords. This reduces the risk of shoulder-surfing attacks. It also creates large password spaces that can defeat guessing attacks. GTPass utilizes TIS to ultimately create a more usable and secure multi-modal authentication system.

ACKNOWLEDGMENT

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

REFERENCES

[1] W. R Simpson and Kevin E. Foltz, “Secure Identity for Enterprises” *IAENG International Journal of Computer Science*, vol. 45, no.1, pp 142-152, 2018.

[2] S. Boonkrong and C. Somboonpattanakit, “Dynamic Salt Generation and Placement for Secure Password Storing” *IAENG International Journal of Computer Science*, vol. 43, no. 1, pp 27-36, 2016.

[3] R. N. Shepard, "Recognition memory for words, sentences, and pictures," *Journal of Verbal Learning and Verbal Behavior*, vol. 6, pp 156-163, 1967.

[4] A. Paivio, T.B. Rogers, P.C. Smythe, “Why are pictures easier to recall then words?” *Psychonomic Science*, vol. 1, no. 4, pp 137–138, 1976.

[5] G.-C. Yang, “Shoulder-Surfing Resistant Graphical Authentication Using Transparent Image Moving Scheme”, *The 13th Asia Pacific International Conference on Information Science and Technology (APIC-IST)*, 2018.

[6] Sonia Chiasson, Alain Forget, Elizabeth Stobert, P.C. van Oorschot, Robert Biddle, “Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords”, *Proceedings of the 16th ACM conference on Computer and communications security*, pp 500-511, 2009.

[7] R. Biddle, S. Chiasson, and P.C. van Oorschot,.”Graphical passwords: Learning from the First Twelve Years” *ACM Computing Surveys, vol. 44, no. 4, pp 1-41.* Technical Report TR-09-09, School of Computer Science, Carleton University, Ottawa, Canada, 2009.

[8] Xiaoyuan Suo Ying Zhu G. Scott. Owen, “Graphical Passwords: A Survey”, *21st Annual Computer Security Applications Conference (ACSAC 2005)*, Tucson, AZ, USA, 2005.

[9] G. Blonder, "Graphical passwords," *in Lucent Technologies, Inc.*, Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.

[10] 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, no. 1-2, pp 102-127, 2005.

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

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.