International Journal of Engineering & Technology, 7 (4.39) (2018) 61-64

International Journal of Engineering & Technology

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

Research paper

A New Graphical Password System Using Intersecting Points in a Signature

Gi-Chul Yang

Department of Convergence Software, Mokpo National University, 1666 Youngsan-ro Muan-Gun Jeonnam,58554,Korea
**Corresponding author E-mail: gcyang@mokpo.ac.kr*

Abstract

Background/Objectives: These days the most commonly used method of digital user authentication uses text-based passwords. Security enhancements using text-based passwordsrequire long and complex passwords, but long and complex text-based passwords are hard to remember and inconvenient to use. Therefore, authentication techniques that can replace text-based passwords are necessary. The objective of this paper is developing a user friendly graphical password system with strong security power.
Methods/Statistical analysis: In order to develop a user friendly graphical password system with strong security power, the system developed in this articlecalled PassSign adapts advantages fromthe PassPositions system and signature recognition system. PassPositions system usie relative position information of click points and it is a recognition error free system with high usability. Signature recognition system has strong security power since it is hard to redraw someone else's signature but error prone. PassSign takes signatures as passwords and use relative position information of intersecting points generated in an input signature to identify a certain user's signature for high usability andstrong security.
Findings: There are various existing graphical password systems with there own advantages and disadvantages. Among the existing graphical password systems, signature recognition system has advantages of usability and strong security. It is, however, expensive to implement and error prone. PassPositions system also has advantages of reliability and usability, but has not good enough password space. PassSign system developed in this article removes all the disadvantages of those systems while all the advantages are remain.
Improvements/Applications: This article introduces a new graphical password system called PassSign. PassSign took advantages of existing graphical password systems and it is user friendly and recognition free with strong security power. Also, PassSign is a light and inexpensive user authentication system which is suitable for various mobile devices with relatively small memory space.

Keywords: *Security, Graphical Password, Authentication, Signature Recognition, Mobile Device.*

1. Introduction

In this increasingly complex modern society, the importance of digital security is growing rapidly day by day and the demands of digital security are growing rapidly nowadays. For this digital security, the most commonly used user authentication method uses passwords. The password should be easy for the user to remember and should not be easily exposed to others. However, text-based passwords, which are widely used these days, do not satisfy these conflicting requirements, and general users tend to use short passwords that are easy to remember [1]. This makes the password vulnerable to brute force attacks and dictionary attacks. Therefore users often try to use long passwords. However, long text-based passwords are difficult for users to remember. On the other hand short and simple text-based passwords are easy to be stolen. Text-based passwords are also vulnerable to attacks by using automated programs that generate passwords, shoulder-surfing attacks, or spyware.
Graphical passwords are not using letters or numbers, but pictures or patterns that are easier to remember than text-based passwords [2]. Also, graphical passwords are not as easy to detect as text-based passwords since password spaces of graphical passwords are larger than text-based passwords and it is cumbersome to attack graphical passwords by using automated password-generating programs.
However, graphical passwords have disadvantages compared to text-based passwords in that data transmission costs are high and the systems are weak to shoulder-surfing attacks when the systems are in operation. And in systems using graphical passwords, keyboard input is often inconvenient. Nowadays, the graphical passwords have been developed in various ways. However, there are other problems such as high probability of guessing a correct password in a graphical password system that is authenticated by sequentially selecting (clicking) the exact position of the image displayed on the screen. Therefore, it is necessary to develop a new graphical password system that is easy to use with low possibility of being stolen.
This article introduces a user friendly user authentication system called PassSign, a new graphical password system that took advantages of existing graphical password systems while having strong security power. In next Section, we briefly review on existing graphical password schemes, and Section3 explains the new graphical password system called PassSign in detail. And Section 4 concludes the article.

2. Related Works on Graphical Passwords

First, Graphical passwords are easily remembered by users, and authentication codes are harder for others to recognize than

authentication techniques using text-based passwords. Graphical passwords have evolved rapidly as an authentication technique that can replace text-based authentication techniques since Blonder's idea came out [3]. The graphical password can be divided into a recognition-based graphical password and a recall-based graphical password.

First, recognition-based graphical passwords evolved from the Blonder method. Blonder-style graphical passwords prescribe the image to be used by the system developer and divide the image into specific zones. Depending on the image, regions of the image that are divided into different shapes can be used as selection points. When creating a password, the user selects the regions of the image on the screen in order and selects the same area in the same order for authentication.

Such a Blonder type graphical password is inconvenient because a user must use a personal image and cannot arbitrarily set a selection point because only a predetermined region in the image must be used as a selection point. In other words, if the selection point that the user wants to select is in the boundary of the pre-divided zone and zone, it cannot be used as the selection point in the Blonder type graphical password.

To remedy the drawbacks of this early Blonder-style graphical password scheme, Wiedenbeck and her colleagues have developed PassPoints, a password scheme that allows the use of arbitrary images or photos without predefined boundaries [4]. Therefore, a user who uses PassPoints can select any pixel or selection point regardless of the contents of the picture on the screen when creating a password, and the surrounding pixels at a certain distance around the selected pixel are all recognized as the same selection point. For example, all pixels within a radius of 2 mm or within 3 mm around a selected pixel are regarded as selection points. At this time, if the radius is large, the password is easy to be stolen, and if it is small, it may be inconvenient to use. Also, since the pixels are used as selection points rather than the areas within the image, the on-screen image only helps to remember the selection points. So you do not have to use predefined images and you can use your favorite pictures or images. It can also help prevent password stealing by using different pictures on different systems. Nevertheless, graphical passwords have certain areas that are often used as passwords in a given picture. [Figure 1] shows example images and selection points used in the PassPoints system.

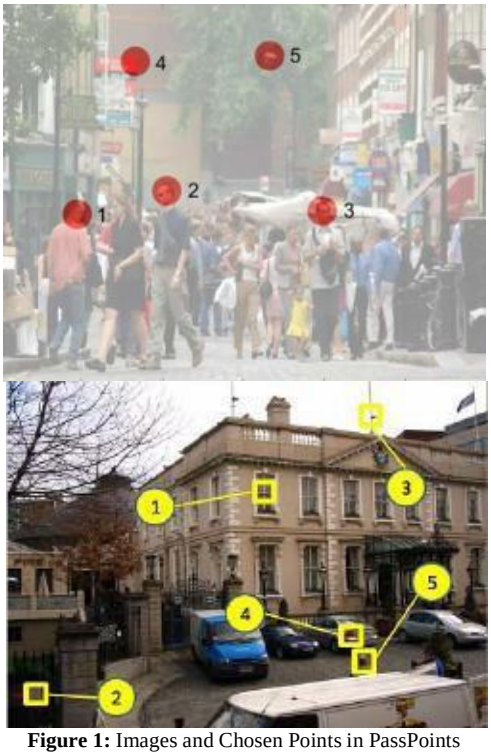

Figure 1: Images and Chosen Points in PassPoints

Dirik and his colleagues studied the possibilities of theft in the PassPoints system [5]. In other words, it is a study on the method of predicting what will be a selection point in a picture when a background is used. There have also been efforts to make graphical passwords difficult to steal or guess [6]. [Figure 2] is an example where many objects are used to make the recognition code difficult to understand even if the graphical password is stolen behind the back.

Figure 2: A Shoulder-Surfing Resistant Graphical Password Scheme

Thorpe and Orschot have studied how to figure out these complex graphical passwords and introduced the concept of 'Graphical Dictionaries' [7]. Next, let's look at the recall-based graphical password. With recall-based graphical passwords, Jermyn and his colleagues introduced a system known as DAS (Draw-A-Secret) [8]. [Figure 3] is a system that can draw a pattern.

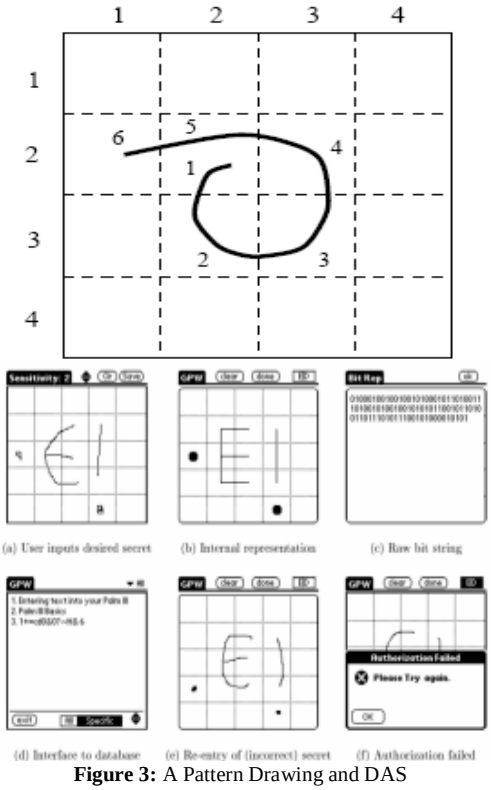

Figure 3: A Pattern Drawing and DAS

In a DAS system, there are sections on the screen and a pattern is drawn as it passes through the sections. As the pattern is drawn, the order of the passing area is memorized and this is the right way to be authenticated. Therefore, the user must remember the pattern that he or she created when creating the password, and in what order the pattern should be drawn in which area, and then reproduce it at the time of authentication.
Then [Figure4] is a system proposed by Syukri and his colleagues to authenticate by drawing a signature with a mouse [9]. Online signature recognition is another topic, so we will not discuss it further here.

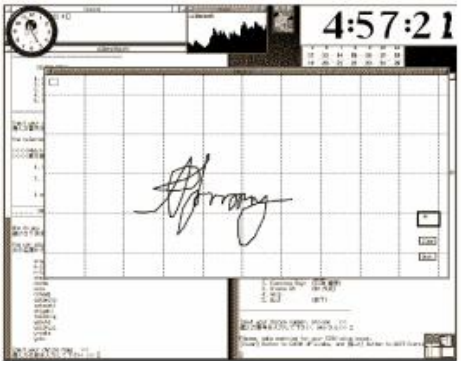

Figure 4: A Signature Recognition System

The system of Syukri and his colleagues have the advantage of easy to remember because they use their own signature and it is difficult for others to steal, but it is difficult to sign using a mouse and the procedure of recognition is complicated. Recently, a technique for using graphical passwords and text-based passwords together has also been introduced. In the next chapter, a new graphical password system PassSign is introduced; PassSign is a graphical password system that is based on this preliminary study and has a low probability of being stolen and is easy to use and reliable.

3. A New Graphical Password System using Intersecting Points

PassSign, a new graphical password system introduced in this section, is advantageous in that it is easy to use and difficult for others to steal since it is hard to redraw someone else's signature. Users of PassSign use their own signature like Signature Recognition System proposed by Syukri and colleagues shown in the previous section. Unlike Syukri and his colleagues' Signature Recognition System, PassSign's signature recognition process is not complicated. This is because the PassSign's signature recognition method uses the relative position information of the intersecting points in a signature like the technique used by PassPositions. It is a newly developed technique adapted in a graphical password system PassPositions, unlike the conventional methods [10].
PassPositions is a graphical password system using Relative Position. Conventional graphical passwords use absolute positions (selection points) using regions or pixels on an image. PassPositions are the same as existing systems in that users select multiple select points in sequence when registering passwords. However, when they are registered in the system, the absolute position of the selection point is not recorded in the system but the relative position is recorded. For example, if a user selects three selection points (a, b, c), PassPositions calculates the absolute position of pixel 'a'. Then, when the second selection point 'b' is entered, the absolute position of 'b' is calculated, and the relative position of 'b' with respect to 'a' is found. That is, whether 'b' is located on top of 'a', beneath, or left or right. Also, if 'c' is entered, the relative position to 'b' for 'c' is found and recorded. Also, in the authentication, the authentication is performed by finding the relative position with respect to the selected points in the same way. With this technique of PassPositions, the user need only select the relative positions on the screen instead of selecting the correct absolute positions [10].
In order to utilize the technique of PassPositions that utilizing the relative position information, PassSign system recognizes the intersecting points generated during a signature drawing and uses the relative position information of the intersecting positions as a password. In other words, PassPositions takes location of click points from the input window to generate a password, but PassSign does not take click points as input or password. It recognizes the intersecting point's locations of the stroke(s) that occur during the signing process to generate a password.
For example, if a user draws a signature like [Figure. 5], intersecting points are generated at location ① and ②. PassSign uses these intersecting points as the click points in PassPositions.

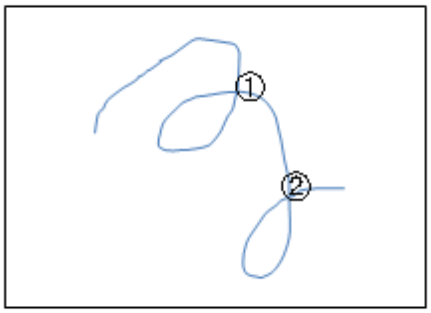

Figure 5: One Stroke Signature of PassSign

The second intersecting point ② is located at the lower right relative to the first intersecting point ①. Therefore, RP-String is generated (RU). These intersecting points can be generated in a single signature, and they function like input points in PassPositions. The stroke line in [Figure 5] is not visible when the system is actually operated, and it makes difficult to steal the signature. [Figure 5] is an example of single stroke signature. However, a PassSign system also can accept signatures with multiple strokes.
[Figure 6] shows an example of a PassSign system that recognizes a multi-stroke signature consisting of a curve and a straight stroke. Here, if you enter the curve stroke first and the straight line later, three intersecting points are created as in [Figure 6]. The first and second intersecting points are generated by the curved stroke itself and the third intersecting point is generated with the second stroke the straight line. PassSign can accept as many strokes as a user use for his/her signature.

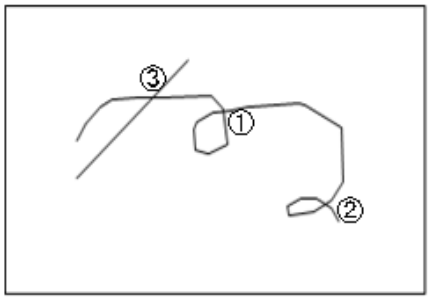

Figure 6: Two Strokes Signature of PassSign

So in this case RP-String is (RD, LU). In other words, PassPositions and PassSign differ only in the password input methods for authentication and the authentication procedure is the same. However, PassSign has the advantages that it is easy for users to remember because they use their own signatures as passwords, and it is hard for others to steal. In addition, unlike existing signature recognition systems, it uses simple positional information of intersecting points, which makes system

implementation easy with low cost. Also, since the size of the system is small, it can be efficiently installed in a small mobile device having a small memory and/or battery capacity.
[Figure7] shows practical examples of PassSign with visualizing stroke lines and intersecting points. PassSign has the option of showing and hiding those things on the input screen.

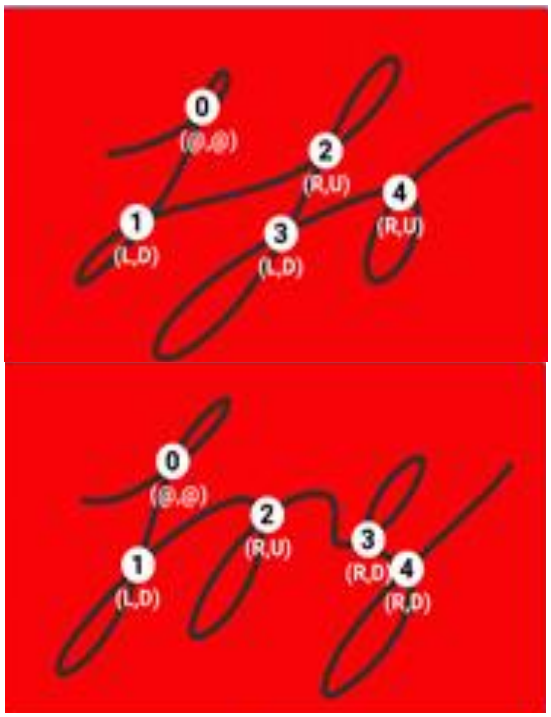

Figure 7: Examples of Implemented PassSign

4. Conclusion

This article introduces a new graphical password system called PassSign. PassSign has advantages in that it is easy to use and difficult for others to steal because users use their own signature like Signature Recognition System proposed by Syukri and colleagues. However, unlike Syukri and his colleagues' Signature Recognition System, PassSign's signature recognition process is simple and errorless. PassSign uses location information of intersecting points in a signature to identify the password as in PassPositions. In this way we can build PassSign simple and easy without recognition error.
PassSign utilizes both Syukri and his colleagues' and Yangs' idea to develop a new graphical password authentication system. PassSign has the advantages that it is easy for users to remember and use because they use their own signatures as passwords, and it is hard for others to steal. In addition, unlike existing signature recognition systems, it uses simple positional information of stroke(s) intersecting points, which makes the system implementation easy with low cost. Even though it uses the relative positional information as used by PassPositions, input mechanism of PassSign is different. The input mechanism of PassSign is a signature rather than click points that strengthens the security.
Also, since the size of the authentication system PassSign is small, efficient installation of the system in small mobile devices is possible. Usually small mobile devices have small memory and/or small battery capacity. So, PassSign will efficiently work with the environments of small mobile devices. PassSign is easy to use and hard to steal. Also, it is cost efficient to use and implementation.

Acknowledgment

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] Dhamija R. and Perrig A., Deja Vu: A User Study Using Images for Authentication, in Proceedings of 9th USENIX Security Symposium, 2000.
[2] Shepard RN, Recognition memory for words, sentences, and pictures, Journal of Verbal Learning and Verbal Behavior, 1967, vol. 6,pp. 156-163.
[3] Blonder, G, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.
[4] Wiedenbeck SJ, Waters JC, Birget A. Brodskiy and Memon N, PassPoints: Design and longitudinal evaluation of a graphical password system, International Journal of Human Computer Studies, 2005. 63, pp. 102-127.
[5] Dirik AE, Memon N, Birget JC. Modeling user choice in the PassPoints graphical password scheme', Symposium on Usable Privacy and Security (SOUPS), at Carnegie-Mellon Univ., Pittsburgh, 2007.
[6] Man SD, Hong, and Mathews M. A shoulder surfing resistant graphical password scheme, in Proceedings of International conference on security and management. Las Vegas, NV, 2003.
[7] Thorpe J, and Oorschot PCv. Graphical Dictionaries and the Memorable Space of Graphical Passwords, in Proceedings of the 13th USENIX Security Symposium. San Diego, USA: USENIX, 2004.
[8] Jermyn IA, Mayer F, Monrose MK, Reiter, and Rubin AD. The Design and Analysis of Graphical Passwords, in Proceedings of the 8th USENIX Security Symposium, 1999.
[9] Syukri AF, Okamoto E. and Mambo M,A User Identification System Using Signature Written with Mouse, in Third Australasian Conference on Information Security and Privacy (ACISP): SpringerVerlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.
[10] Yang G.-C. 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.