A Hybrid Password Authentication Scheme Based on Shape and Text

Ziran Zheng
School of Management & Economics
Shandong Normal University, Jinan, China
Email: zzrnature@gmail.com

Xiyu Liu
School of Management & Economics
Shandong Normal University, Jinan, China
Email: zzrnature@gmail.com

Lizi Yin
School of Science
University of Jinan, Jinan, China
Email: ss_yinlz@ujn.edu.cn

Zhaocheng Liu
Department of Management
Jinan Railway Polytechnic, Jinan, China
Email: liuzhch100@163.com

***Abstract*—Textual-based password authentication scheme tends to be more vulnerable to attacks such as shoulder-surfing and hidden camera. To overcome the vulnerabilities of traditional methods, visual or graphical password schemes have been developed as possible alternative solutions to text-based password schemes. Because simply adopting graphical password authentication also has some drawbacks, schemes using graphic and text have been developed. In this paper, we propose a hybrid password authentication scheme based on shape and text. It uses shapes of strokes on the grid as the origin passwords and allows users to login with text passwords via traditional input devices. The method provides strong resistant to hidden-camera and shoulder-surfing. Moreover, the scheme has high scalability and flexibility to enhance the authentication process security. The analysis of the security level of this approach is also discussed.**

***Index Terms*—first term, second term, third term, fourth term, fifth term, sixth term**

I. INTRODUCTION

How to increase the level of authentication security has become an important problem in the age of information. The most general authentication methods in computers and other devices require the submissions of the users' names and their passwords. The most serious problem about textual password is the vulnerabilities to various attacks. Due to the fact that this type of scheme is based on the characters, the login passwords are quite easy to guess and if the passwords get longer, they become harder to remember for the users themselves. To overcome the vulnerabilities of textual passwords, visual or graphical password schemes have been developed as possible alternative methods to the traditional authentication process. The main idea of graphical passwords is to use the images or shapes to replace the text, since graphical signs are easier to remember than pure characters [1].

Although graphical password schemes have been considered as alternatives to traditional text password, they also have some drawbacks. For example, some of them have vulnerabilities to shoulder-surfing because of the users' direct actions upon the input screen. And some schemes will require users to input the password for several times. In addition, most of the graphical schemes have far more complexity in the implementation of the application.

This work is proposed to make a bridge between the graphic and text password. Since the shape as the password have larger space and easier to remember, we take the advantage of the shape as the users' original passwords. To make the implementation easy and avoid direct interaction appeared between the user and screen, a grid with characters is adopted to construct the new system. With this new authentication scheme, users can only just remember the shapes and strokes they like as their passwords. However, the system authenticates the shape passwords just with text on the grid and their input order during the process.

What we focus on the design of the scheme are as follows: (1) Using shapes and strokes on the grid as the original password, since the shape of stroke can be easier

doi:10.4304/jcp.5.5.765-772

to remember than text. (2) Text-based login process, which supports keyboard as the input device. (3) Strong resistant to shoulder-surfing and hidden camera. (4) It has large password space and robust mechanism against the brute force attack.

This paper is organized as follows. In the next section the background and related work about the graphical scheme are introduced. In the section after that the basic and further description of our approach is presented. The next section discusses and analyzes the security level of the scheme. The conclusion and future work are presented in the last section.

II. Back Ground and Related Work

A graphical password scheme, in which a password is generated through asking the user to click on a graphic or an image provided by the system, is designed by Blonder [2]. When creating a password, the user is asked to choose four images of human faces from a face database as their own password. In the authentication stage, users must click on the approximate areas of those locations. This method is considered as a more convenient password scheme than textual scheme, for the image can help users to recall their own passwords. Wiedenbeck, et al. [3] extended the approach and proposed a system called "PassPoint". It allows users to click on any locations on the image to create the passwords. The system will calculate a tolerance around each pixel which has been chosen. The users must click within the tolerance of the chosen pixels.

Jansen [4-6] proposed a graphical password scheme for mobile devices. During enrollment, a user is asked to choose the theme consists of photos in thumbnail size and set a sequence of pictures as a password. In the authentication stage, a user must input the registered images in the correct order. Each thumbnail image is assigned a numerical value, thus the sequence of the chosen ones will create a numerical password. Because the number of picture is limited to 30, the password space of this scheme is not large.

Jermyn, et al [7] proposed a technique call "Draw a Secret (DAS)". This system allows users to create their own passwords by drawing something on a 2D grid. When a user finishes the drawing, the system stores the coordinates of the grids occupied by the picture. During authentication, users must re-draw the picture which had been created by them. The user will be authenticated if the drawing touches the same gird in the right order. The password space of this scheme is proved to be larger than the full text-based password space.

Thorpe and van Oorschot [8] analyzed the memorable password space of the DAS. Graphical dictionaries were introduced and possibilities of a brute-force attack using dictionaries are studied. They showed that a significant fraction of users will choose mirror symmetric password, since people recall symmetric images better than asymmetric images. Thorpe and van Oorschot [9] also studied the impact of password length and stroke-count as a complexity property of the DAS scheme. In order to improve the security, a "Grid Selection" technique is proposed. It allows users to select a rectangle region as the drawing grid, in which they may input the password. This method increases the DAS password space significantly. Further research was studied by Nali and Thorpe [10].

To overcome the shoulder-surfing problem, many techniques were proposed. Zhao and Li [11] proposed a shoulder-surfing resistant scheme "S3PAS" The main idea of the scheme is as follows. In the login stage, they must find their original text passwords in the login image and click inside the invisible triangle region. The system integrates both graphical and textual password scheme and has high level security. Man, et al, [12] proposed another shoulder-surfing resistant technique. In this scheme, a user chooses many images as the pass-objects. The pass-objects have variants and each of them is assigned to a unique code. In the authentication stage, the user must type the unique codes of the pass-objects variants in the scenes provided by the system. Although the scheme shows perfect results in resisting hidden camera, it requires the user to remember code with the pass-object variants. Further research based on this method was conducted in [13].

Luca, et al. [14] proposed a stroke based shape password for ATMs. They argued that using shapes will allow more complex and more secure authentication with a lower cognition load.

More graphical password schemes have been summarized in a recent survey paper [15].

III. Hybrid Password Scheme

The hybrid password scheme based on shape and text is designed not only for the traditional computers but can be used in the mobile devices. The basic idea of our scheme is to make a map from shape to text with strokes of the shape and a grid with text. The map could be constructed quite simple and straight-forward. This mapping not only guides the user to master this scheme with ease, but makes the whole system easy to implement.

Fig. 1 shows the idea of this work. Users should just think some personal shapes and its strokes as their origin password and enter character in the authentication as the login password.

The whole process includes two main steps: the password creation step, and the login step. In the basic scheme, we take a simple example to descript the two stages. Variants of the scheme will be introduced in the further description.

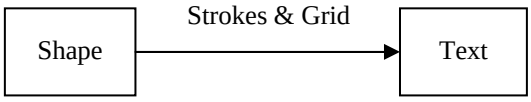

Figure 1. Mapping from shape to text through strokes and grid

A. Notations of the Scheme

The following notations, which are used throughout the paper, are defined to help the presentation and analysis of the scheme.

- U: The set of elements appeared in the grid in the interface.
- V: Input passwords vector, which consists of elements in U.
- $|V|$: Size of the V. It also represents the length of the input passwords, or the strokes' size.
- g: the size of the grid.
- S: Shape of the password. For example, it could be "N", "1", "&"or any other forms. S* means the number of different types of the shape S.
- $|S|$: Number of strokes of the password.
- H: The password space. H_t and H_s represent the text-based and stroke-based password space respectively.

B. Basic Scheme

In the first step, the user is asked to select a group of elements on the grid shown in the interface as the original password. In this example, we use $g = 5 \times 5$ gird to show the process. The password-set interface is shown in Fig. 2.

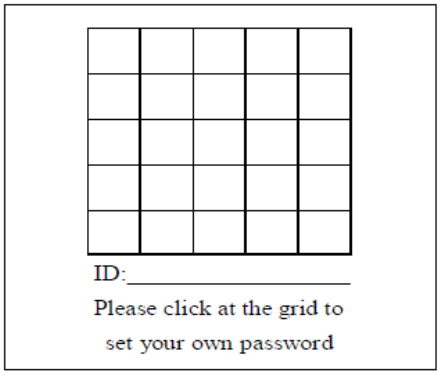

Figure 2. Password set interface

Note that the size or the grid (g) can be different to meet the certain requirements and it could affect the security level of the scheme. More descriptions about this will be explained in the next section.

Firstly, a user is proposed to pick a shape S such as a number shape, a geometric shape, a character shape or even a random shape as his(or her) own original password. The criterion of choosing the shape is as easy to remember as possible for the users themselves. Though the number of the shapes could vary, it is not the key factor to the scheme. Thus we use one shape to describe this instance for the sake of convenience.

After the password shape is selected in their mind, the user should click on the grid in the interface following the shapes' stroke sequence. The system will store the shape and the order with the grid as the user's mapped text password.

Note that, this process doesn't have the same level of security than the login step, since the direct action between the user and the screen. And if the input device is the keyboard like the ATM, the password set process will reflect the original password of the user, if this process is recorded by the camera, the whole password and this scheme will not work. However, this disadvantage can be overcome by a multi-set process, which will be described in detail in next section.

Go back to the example, the user John chooses one of characters of his name "N" as the shape of the password. Suppose the sequence of the stroke "N" is in a simpler order than normal as the shape's stroke order.

When the shape and the order setting are finished, John could design the stroke on the grid as he likes (this is a mechanism to level up the security level. Even if the shape is known by the hacker in some way, the hacker would not be sure the shape's shape on the grid specifically). Here, we suppose that the shape is drawn fully at the grid. After that, the user clicks on the grid to form "N" as the original password. The set procedure can be seen more clearly in the Fig. 3.

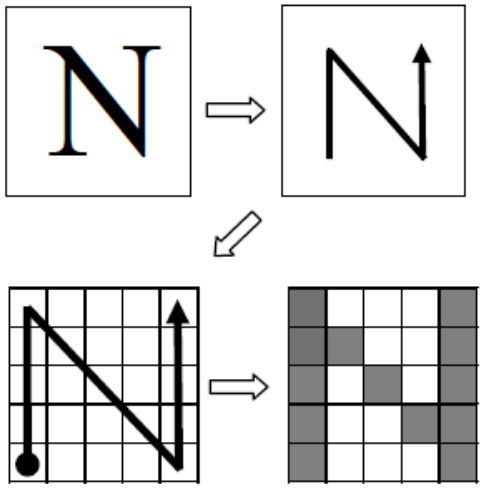

Figure 3. Password set procedure

Fig. 3 not only shows the procedure of the setting password, but also provides the idea of mapping from a simple shape into a grid. The shape is finally represented by a number of blocks on the grid.

In the login step, the interface is presented with a different style. The grid is filled with some similar symbols such as some numbers or characters. The feature of the approach here is to use quite a few numbers of the symbols, which consists of U. Since the less we use, the faster and more secure of the authentication process will be. Here we use the number "0" and "1" to show the example, which means $U = \{0, 1\}$. Note that the system will choose the symbol randomly from U to fill every grid. The login interface is shown in Fig. 4.

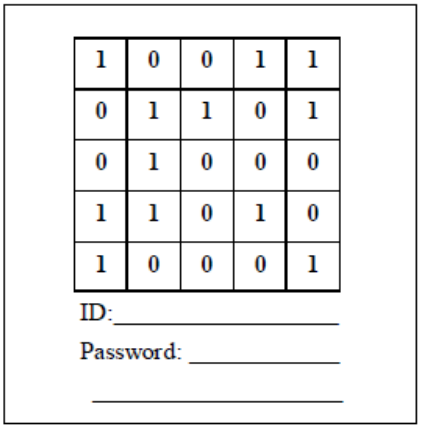

Figure 4. Login interface

During the authentication stage, the user John was asked to enter the password. He will use the keyboard with only "0"and"1" keys to input the password. The order and content of the password is entering the number in the grid following the original password shape's strokes which he has chosen in the password-set step.

Fig. 5 shows the image appeared in the John's mind, which is not the action or the image in the authentication scheme. It just helps to understand what the users would recall and think in the login step.

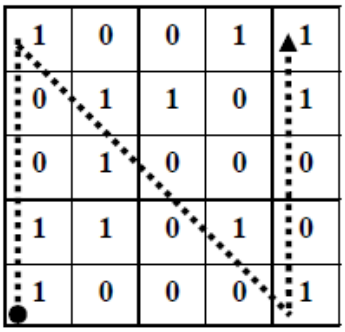

Figure 5. Original stroke on the interface

While looking at the number filled in the grid of the original shape, John should enter numbers in the right order. Thus, the password is as follows: 1100110110011, where *V*=[1,1,0,0,1,1,0,1,1,0,0,1,1].

The system will check if the input vector matches the numbers appeared in John's original sequence of the grid upon the interface created by the system. Because the texts with which the user enters are only using two keys, the login process is quite convenient. It is very useful to shorten the login process. More importantly, the act of inputting with only two keys can effectively resistant to the shoulder surfing.

If the password entered is not correct, then the system will generate another login interface grid for the user with characters randomly selected again. The symbols from U appeared in the grid varies at each login step, which means that the shape and the sequence of shape will not vary but the mapped text will not be the same at different interfaces. It also means the text passwords the user will input are not the same one at different login times. If hackers record the text the user input exclusively, they would get nothing about the information of any user's original password. Thus the text-based brute force attack with the "1"s and"0"s are useless.

The main idea of the scheme is making the stroke shape as the password using the textual input. And we use this mechanism to resist the spy attack. The basic scheme is quite simple. To enhance the scheme, there are some points to explain in details.

IV. Further Descrition

The basic scheme can be extends from different respects. Some of them are made the system easy to use for the users and some are designed to improve the security of the whole system.

A.Shapes Choosing

At the set step, the shape S as the original password can be of quite different types. Users not only can choose the character but can also adopt the geometric shapes, the number shapes, the symbol shapes and even the arbitrary shapes as the preferred password shape. Fig. 6 shows several different kinds of shape: triangle, cube, number"1" and some discrete plots. This mechanism is to offer various alternatives for users.

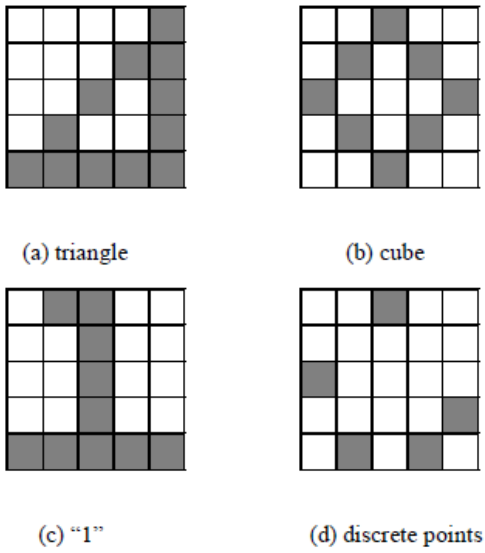

Figure 6. different original shapes

One shape also can have different styles, which means a conceptual shape will generate various specific styles. This description will be provided in the security analysis section.

Essentially, the shape that appeared in the user's mind is the blocks on the grid for the system. Theoretically, any boxes in the grid can be adopted as the user's original shape and the shape or shapes can have no meaning at all

except for the user himself. Any unique shape with personality is considered as the better option than the normal shape with meanings.

B.Shokes Choosing

Even for the same shape, the password shape space is very large since it considers the sequence of the stroke and the number of the strokes |*S*| during the shape creating step.

Take the triangle shape for example. The stroke of the shape could have several variants, which are shown in Fig. 7. Black point means the start of the stroke and the arrow means the end. The shape triangle can be divided into several strokes. Also, these four figures are not all the variants.

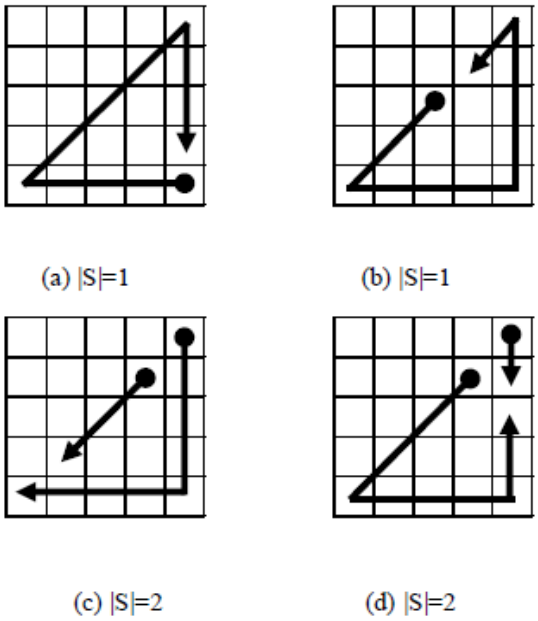

Figure 7. Stroke variants of triangle

Just like the shapes choosing, users could select any order and number of the strokes of their original shape password.

C.Different Interface

At the login step, the characters appeared in the grid can be in any form preferred by the designer or the user. In addition, the number in each grid could vary at the same time.

For example, Fig. 8 shows the variants of the login form.

11	01	0	1	10
0	1	10	0	11
01	10	0	0	01
1	1	00	1	0
11	0	01	0	1

aa	sa	s	a	as
s	a	as	s	aa
sa	as	s	s	sa
a	a	ss	a	s
aa	s	sa	s	a

Figure 8. Other forms of login interface

No matter what appears in the grid, the method of the authentication does not change. John's password now is: *V*=[11, 1, 01, 0, 11, 1, 0, 1, 1, 0, 01, 11, 10],or *V*=[aa, a, sa, s, aa, a, s, a, a, s, sa, aa, as].

Although this kind of change would increase the login time for the user, it also increases the security level of the process. Because of that, the length of the text password changes at each login step and the text password space increases.

D.Different Input Style

Because of the high resistant to the shoulder surfing of the keyboard, the input device could be hidden. We can expand the input style of the system by adding the soft keyboard onto the interface. The mechanism can be used in mobile devices or other screen-based input environment. Although the input process can be easily recorded, the scheme has strong resistance to this kind of attack. Fig. 9 shows the example.

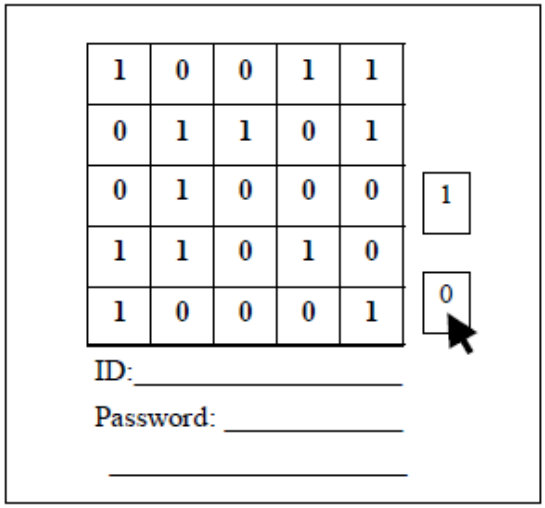

Figure 9. Interface without keyboard

IV. SECURITY ANALYSIS

A. Resistant to Shoulder Surfing

Because the login step does not reflect the shape password directly, this hybrid password scheme is highly resistant to shoulder-surfing. In the login step, the only method to obtain the original shape password is that the attackers must record the whole finger process and the certain grid form of that login process. In addition, if a hidden camera has recorded the whole process of the login step, it is not easy to crack the system either.

Take the password used above for example. We suppose that the attacker has obtained the interface and the password number at the login step using a hidden recorder. The interface is shown in Fig. 10 (the same as the basic scheme shown in the previous example) and the password vector is V=[1100110110011]. Since the scheme is based on the stroke, the attackers had to guess the accordant stroke with the numbers. It is apparent that one password vector could represent many stroke variants. Figure 9 shows the example of three shapes compared to the former "N".

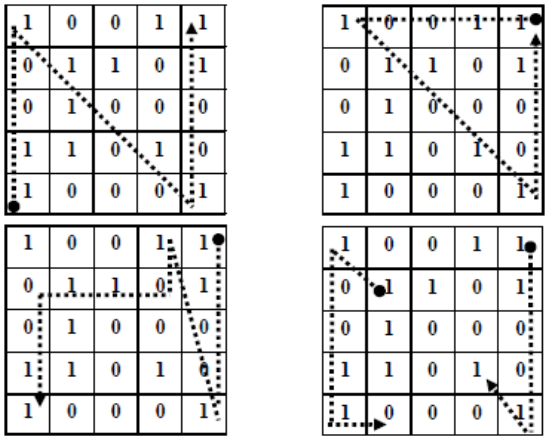

Figure 10. Stroke variants

Because the stroke can be any form of shape, the number of the stroke of one vector is as follows: suppose f_1 means the number of "*1*" and f_2 means the number of "*0*" in the interface, and f_1 = m , f_2 = n , $|V|$= 13 (the size of the shape of V), $H_s = m^8n^5$. In this example, f_1 = 12, f_2 = 13, $H_s = 12^8 13^5 = 1.6 \times 10^{14}$.

B. Resistant to Brute Force

There are two categories of brute force attack: the text-based and the stroke-based.

For the text-based brute force attack, the text space of this password Ht scheme is not large. However, the login passwords required are not the same string in each time when users login. For the string tried by the attackers in parts of the password space may become correct in any time, this method does not have the effect to this scheme.

Another brute force attack is based on the stroke or the shape on the grid. This can be seen more effective than textual-based one. The attacker could try the shape and its stroke on the grid without considering the character appeared in the grid. It is difficult to guess the shape and the stroke of user's password. Moreover, one shape can have different kinds of stroke sequence, and can have different region in the grid. More importantly, an original password could be composed of several strokes of any shape. All of its mechanism larges the password shape space.

Because the login step does not require user to click on the screen directly, the stroke-based textual scheme is highly resistant to shoulder-surfing. The attackers must record the whole finger process and the certain grid form in order to obtain the password. In addition, if a hidden camera has recorded the two scenes of login, it is not easy to crack the system either.

One type of brutal force attack is trying all of the strokes on the grid, assuming that the attacker does not know any information about the stroke's S, $|S|$ and $|V|$. Thus the attackers have to try all of the shapes with any length. The password space Hs is as follows:

$$H_s = g\,|V| \qquad (1)$$

In this example, $H_s = 25^{13} = 1.5 \times 10^{18}$ .More advanced stroke-based brutal force attack is that the attacker would try the certain stroke, assuming that the attacker has known the shape of the password. For example, the attacker uses the character N to attack the scheme. Without considering the stroke dividing of the same shape, the single shape "N" could have variants, as shown in Fig 11.

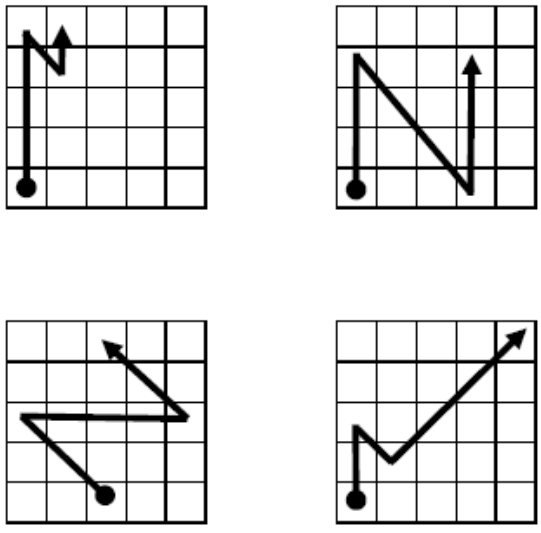

Figure 11. Shape variants of *N*

$H_s = \sum_{m=1}^{|S|} S^* 2^m$, where S^* can only be specified for the certain shape. To this example, we suppose the S^* = 20, $|S|$= 5 , and H_s = 1240 . Although the space is not large enough, it is on the premise that the shape S is fixed.

C. Resistant to Random Click Attack

Because the number of kinds of character in the login step is only 2, random clicking with the two keys may become a more effective method to attack the system. Again considering John's password, where $|V|$=13. The possibility of guessing the right string is $1/2^{13} \approx 0.000122$. And if the attacker does not know the length of the password, then the possibility will become less than that. Furthermore, the number of kinds of text appeared in the grid during authentication can be added to 3, thus it is more difficult to get the correct password through random clicking.

D. Multi-step Login

Multi-step login means: users can choose more shapes than one as their original passwords. Different shapes will be inputted according to different interface grid. To avoid increasing the login time, this method is appropriate for the interface with small size grid. In this situation, user's original passwords are a sequence of shaped, can they se and login with them in the same way like the basic scheme.

V. Conclusion and Future work

In this paper, a hybrid password scheme based on shape and text is proposed. The scheme has salient features as a secure system for authentication immune to shoulder-surfing, hidden camera and brute force attacks. It also has variants to strengthen the security level through changing the login interface of the system.

However, the system still has some drawbacks. Firstly, this method is relativity unfamiliar to the general public so that the users may adopt the simple and weak strokes as their passwords. If the shapes chosen by the use have normal meaning, the attacker will have more chance to attack the password. Thus, teaching the user to use this scheme and select the original shape password carefully is very crucial to this new system.

Secondly, the most vulnerable step of this scheme is the password creating step, since the users have to tell the system the original shapes and stokes. If this process is recorded by the attackers, the whole system will be attacked easily. Therefore, proposing a more secure method to replace the set step can enhance the whole system effectively.

Thirdly, the login process is longer than other graphical schemes. And if the input process is not familiar to the user, the text input will be clicked by mistaken if not carefully.

In addition, although some researchers have do some analysis about the memorability of the shape as the password should be investigated deeply and thoroughly [16][17], so that this kind of password scheme can be accepted by the users.

To address these issues, we should design more advanced authentication system to improve this method.

Acknowledgment

This work is carried out under the "Taishan Scholar" project of Shandong China. The research is also supported by the Natural Science Foundation of China (No.60873058, No.60743010), the Natural Science Foundation of Shandong Province (No. Z2007G03), and the Science and Technology Project of Shandong Education Bureau.

The authors wish to thank A, B, C. This work was supported in part by a grant from XYZ.

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. 41-46, 1999.

[2] G. E. Blonder, "Graphical passwords," in United States Patent, vol. 5559961, 1996.

[3] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in *Human-Computer Interaction International (HCII2005)*. Las Vegas, NV, 2005.

[4] W. Jansen, "Authenticating Mobile Device User Through Image Selection," in *Data Security*, 2004.

[5] W. Jansen, "Authenticating Users on Handheld Devices," in *Proceedings of Canadian Information Technology Security Symposium*, 2003.

[6] W. Jansen, S. Gavrila, and V. Korolev, "A Visual Login Technique for Mobile Devices," in *National Institute of Standards and Technology Interagency Report NISTIR 7030*, 2003.

[7] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.

[8] J.Thorpe and P. C. v. Oorschot, "Graphical dictionaries and the memorable space of graphical passwords," in *Proceedings of the 13th USENIX security Symposium*, San Deigo,CA, 2004.

[9] J.Thorpe and P. C. v. Oorschot, "Towards secure design choices for implementing graphical passwords," in *Proceedings of the 20the Annual Computer Security Applications Conference*. Tucson, Arizona,2004.

[10] D. Nali and J. Thorpe, "Analyzing user choice in graphical passwors.," in *Technical Report School of Information Technology and Engineering*, University of Ottawa, Canada, 2004.

[11] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07)*, vol. 2. Canada, 2007, pp. 467-472.

[12] S.Man, D. Hong, and M.Mathews, "A shouldersurfing resistant graphical password scheme," in *Proceedings of International conference on security and management. Las Vergas*, NV, 2003.

[13] D. Hong, S. Man, and B. Hawes, "A password scheme strongly resistant to spyware," in *Proceedings of International conference on security and management*. Las Vergas, NV, 2002.

[14] A. D. Luca, R. Weiss, and H. Hussmann, "PassShape: stroke based shape passwords," in *Proceedings of the 2007 conference of the computer-human interaction special interest group (CHISIG) of Australia on Computer-human*

interaction: design: activities, artifacts and environments. Australia 2007, pp. 239-240.
[15] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," *21st Annual Computer Security Applications Conference (ASCSAC 2005)*. Tucson, 2005.
[16] R. N. Shepard, "Recognition memory for words, sentences, and pictures," *Journal of Verbal Learning and Verbal Behavior*, vol. 6, pp. 156-163, 1976.
[17] R. Weiss, A. D. Luca, "PassShape – Utilizing Stroke Based Authentication to Increase Password Memorability," *NordiCHI*, 2008.

Ziran Zheng was born on Decemeber 15, 1981, in Jinan, China. In 2007, he received the Master degree in computer software and theory in Shandong Normal University. Currently he is a PhD student at Shandong Normal University. His major field is computer-aided design, information security.