A Study of Graphical Password for Mobile Devices

Xiaoyuan Suo

Department of Math and Computer Science,
Webster University,
Saint Louis, MO, USA
xiaoyuansuo51@webtser.edu

Abstract. The objective of this project is to conduct a comprehensive research into the usability; design and security of graphical password on touch screen devices. We address the design limitation of touch screen devices and possible solutions. We also propose a simple graphical password scheme designed specifically for touch screen devices. Further, expert reviews and usability studies were used to explore user interactions in order to gain a more complete understanding on the potentials to improve the graphical password design for touch screen mobile devices.

Keywords: Graphical password, iPad/iPhone app, Mobile app design, Mobile.

1 Introduction

Mobile device, especially touch screen interface designs have attracted rising attention in recent years; devices such as ATM (automated teller machines), ticket machine, PDA (personal digital assistant), have been widely used in various occasions. Lately, touch screen devices are technologically becoming more accurate, usable and popular in any size; such as smart phones, or Apple's iPad, iPhone, and iPod touch [1] etc. Media report estimates that touch screen devices will account for more than 80 percent of mobile sales in North America by 2013[2].

Graphical passwords have been proposed as a possible alternative to text-based schemes, motivated partially by psychological studies [3] that show human can remember pictures better than text. Graphical password techniques include recall-based click password (e.g. imposing background image so user can click on various locations on the image), and recognize-based selection password (e.g. selecting images or icons from an image pool). In particular, recall-based click passwords have received much more attention in recent years[4]. However, very little studies have been done on graphical password on touch screen mobile devices.

In this work, we propose a novel graphical password scheme designed specifically for touch screen devices. Since touch screen devices dominate the mobile world, this project has the potential to influence design of mobile user experiences. The project is built on iOS platform using Objective C, and deployed as an iPad/iPhone application. This application is designed for research purposes only. To our knowledge, this is the first attempt in studying graphical password design scheme on touch screen devices.

G. Memmi and U. Blanke (Eds.): MobiCASE 2013, LNICST 130, pp. 202–214, 2014.

This study directly concerns user experiences and effective designs of touch screen applications.

Further, expert reviews and usability studies were used to explore user interactions in order to gain a more complete understanding on the following:

a. *Approaches to overcome limitations of a touch screen computer for graphical password designs.*
Touch screens have special limitations such as: user's finger, hand and arm can obscure part of the screen; and the human finger as a pointing device has very low "resolution". It is also difficult to point at targets that are smaller than the users' finger width.

b. *The relationship between user password choices and the complexity of the background image.*
The complexity of an image is defined as a combinational quantitative measure of the number of objects presented, the number of major colors, and the familiarity of the image to users and other factors. Careful selected background images can enhance effective graphical password design. The study highlights the vulnerability of click based graphical passwords. As a result, we discuss several graphical password attacking methods based on the choice of pictures. This study aims to achieve better balance between security and usability of click based graphical passwords through better choices of background images.

c. *The relationship between background image choice and successful authentication rate.*
Successful rate, in this case, is defined as the number of successful authentications versus the number of trials within a critical time frame.

d. *The relationship between tolerance rate and successful rate.*
The tolerance rate is defined as a number of pixels permitted to be selected around the original selection. A properly selected tolerance rate has direct impact on user experiences.

e. *Security concerns of using graphical password for touch screen devices*
Although graphical password theoretically provides a large amount of password space, usability studies showed the number of "usable clicks" are significantly less.

f. *Assess the future of graphical password for touch screen devices.*
This process involves preliminary assessment of potential for using graphical password on touch screen devices.

2 Touch Screen Mobile Device Design Limitations

One difficulty for interface design on mobile devices is lack of screen space caused by their small size [5]. Small displays and multiple inputs, especially with the presence of a figure, require users to register click-based password with pinpoint accuracy.

2.1 Screen Precision

The Touch-Screen device size and the Touch-Screen's effective area affect the Touch-Screen keyboard design. The device sizes can be small, medium, or large.

Small Touch-Screen devices[6], such as mobile and smart phones, Personal Digital Assistants (PDAs), and handheld computers, have a smaller Touch-Screen area and smaller onscreen objects. Finger use has become more popular in the research community since Apple's iPhone and iPod touch were released. In the recent years, researchers started to examine text entry specifically for tabletop displays [7].

The work by Parhi et al. [6]is presented to determine optimal target sizes for one-handed thumb use of mobile handheld devices equipped with a touch screen using a two phase study. The study primarily focused on small sized screen. Phase 1 of this study is intended to determine size recommendation for widgets used for single-target tasks, such as activating buttons, radio buttons and checkboxes; and phase 2 is trying to evaluate required key sizes for widgets used for text or numeric entry. The study concluded that no key size smaller than 9.6mm would be recommended for serial tapping tasks, such as data or numeric entry. A 9.2 mm target size for discrete tasks would be sufficiently large for one-handed thumb use on touch screen devices.

Investigations by Sears, A., et al. [8] showed the effect keyboard size has on typing speed and error rates for touch screen keyboards using the lift-off strategy. A cursor appeared when users touched the screen and a key was selected when they lifted their finger from the screen. Four keyboard sizes were investigated ranging from 24.6 cm to 6.8 cm wide. Results indicated novice users can type approximately 10 words per minute on smallest keyboard and 20 words per minute on the largest. Experienced users improved to 21 words per minute on smallest keyboard and 32 words per minute.

Work by Colle and Hiszem [9] estimates the smallest key size that would not degrade performance or user satisfaction. The results showed participants entry times were longer and errors were higher for smaller key sizes, but no significant differences were found between key sizes of 20-25mm. participants also preferred 20 mm keys to smaller keys, and they were indifferent between 20 and 25 mm keys. The work concludes a key size of 20 mm was found to be sufficiently large for land-on key entry. [9]

Three experiments conducted by Lee and Zhai focused on the operation of soft buttons (either using a stylus or fingers). The study showed button size affects performance, particularly when buttons are smaller than 10 mm. Styli can more accurately handle smaller buttons and they depend less on synthetic feedback than fingers do, but they can be lost easily and require an acquisition step that bare fingers do not. The two types of touch sensors explored, capacitive and resistive, afford very different behavior but only subtle performance difference. The first can be operated by fingers with very sensitive response, but is more error prone. [10]

Work by Brewster [5] describes a small pilot study and two formal experiments that investigate the usability of sonically-enhanced buttons of different sizes. An experimental interface was created that ran on a 3Com Palm III mobile computer and used a simple calculator-style interface to enter data. The buttons of the calculator were changed in size between 4x4, 8x8 and 16x16 pixels and used a range of different types of sound from basic to complex. Results showed that sounds significantly improved usability for both standard and small button sizes – more data could be entered with sonically-enhanced buttons and subjective workload reduced.

More sophisticated sounds that presented more information about the state of the buttons were shown to be more effective than the standard Palm III sounds. The results showed that if sound was added to buttons then they could be reduced in size from 16x16 to 8x8 pixels without much loss in quantitative performance. This reduction in size, however, caused a significant increase in subjective workload. Results also showed that when a mobile device was used in more realistic situation (whilst walking outside) usability was significantly reduced (with increased workload and less data entered) than when used in a usability laboratory. These studies show that sound can be beneficial for usability and that care must be taken to do testing in realistic environments to get a good measure of mobile device usability.

2.2 Techniques to Improve Screen Input Precision

When using a touch screen device, the user's finger, hand and arm can obscure part of the screen. Also, the human finger as a pointing device has very low "resolution". These limitations have been realized and tackled before--mostly notably by Sears, Shneiderman and colleagues [8, 11]. Their basic technique, called *Take-Off*, provides a cursor above the user's fingertip with a fixed offset when touching the screen. The user drags the cursor to a desired target and lifts the finger (takes off) to select the target objects. They achieved considerable success with this technique for targets between finger size and 4 pixels. Instead of using a bare finger, in some cases the user may use a stylus (pen) to interact with touch screens. A stylus is a much "sharper" pointer than a fingertip, but its resolution may still not be as good as a mouse cursor.

Work by Diller [12] studied various techniques to improve input areas of touch screen mobile devices; in this work, multiple approaches and studies were discussed. While these studies were limited to relatively large targets, Garwin and Levine reported single pixel accuracy when using a laser scanned touch screen. Selection time and error rate data were not reported. [13]

The goal of our work is to introduce a graphical password design for touch-screen devices and provide a study on the usability of such an application design. We hope to provide fellow researchers and practitioners in the field with a more complete guidance to achieve more usable touch screen device designs. Our work differs from this work by having a more comprehensive discussion and classification of techniques to increase accuracy of touch screen devices.

In addition to analyzing properties of tabletop displays and summarizing existing text entry methods for tabletop use; Work by Go et al. [14] also proposed a new keyboard design. In addition to the new design, the work primarily discussed touch screen keyboard use for finger typing; the analysis is from five aspects: screen size, touch screen keyboard types, number of keys, typing devices, and technique. Our work will focus more on the precision of Touch-Screen input.

Many researchers have shown the benefits of tactile feedback for touch screen widgets in all metrics: performance, usability and user experience [15-22]. Koskinen et. al, [22] showed people perceive some tactile feedbacks more pleasant than others when virtual buttons are pressed with fingers on a touch screen.

3 A Novel Scheme of Graphical Password on Touch Screen Mobile Device

The architecture of our novel graphical password scheme is shown in figure 1. The flow chart is based on two main logic paths, namely, registration and authentication. Users are given a database of images to select from; the images are categorized into different sections to improve user experiences.

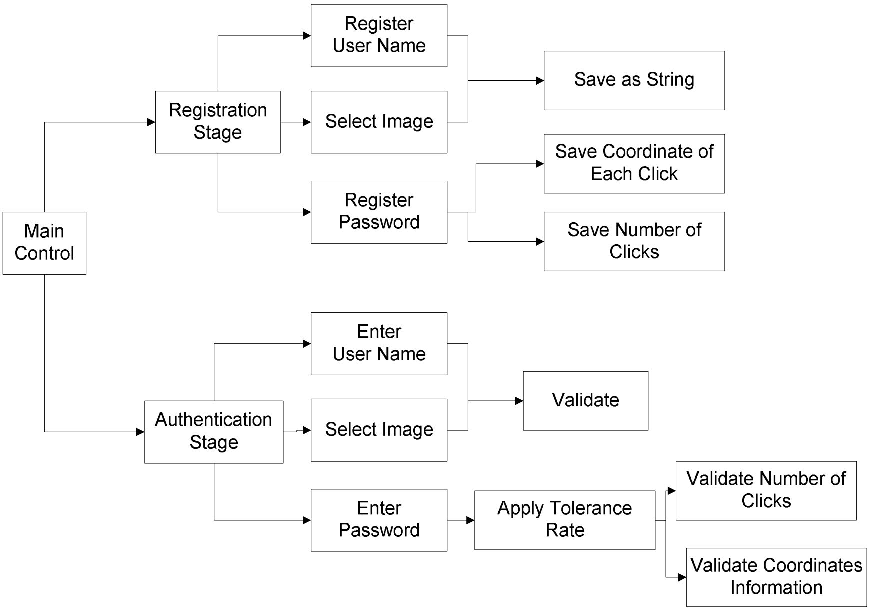

Fig. 1. Registration and authentication process

In the screenshot shown in figure 2, two categories are shown: personal images and natural images. The user is also given the choice of importing images from the personal collections.

During the registration stage, user is required to enter a user name and select an image first. The size of each image is adjusted to fit into the screen. After the image is loaded onto the screen, user will be asked to click on various places on the image. The sequence of clicks, with an X and Y coordinates, is recorded and saved along with the user name and choice of image into our database.

During the authentication stage, user will first be asked to enter a user name and select their registered image. Unless the user name and the choice of images match those in the database, the authentication will fail. When the image is loaded, user will be allowed to tap the image to authenticate. During this process, user will be allowed to select a tolerance rate, which means they can tap within a circle of pixels rather than the specific pixel they pre-selected.

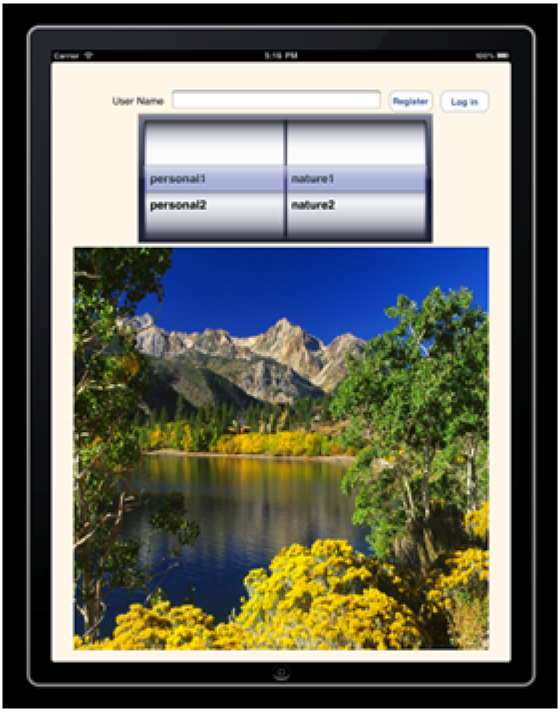

Fig. 2. Screen shot of graphical password on iPad

4 Analysis and Lessons Learned from User Studies

In usability experiments conducted with a group of 25 users recruited from information technology or IT education related fields, the successful authentication rate of our scheme is more than 80%.

4.1 Click Recognition

We encourage each user to register at least 5 different clicks to increase security measures of a particular graphical password. Each click has a few asscociated values, namely, tolerrance rate and coordinate.

In figure 4, the 5 dots represent 5 different clicks. The three authentication-clicks, A, A_2 and A_f represents two accepted authentications and one failure authentication respectively. It is quite obvious that $A_2(x_{a2}, y_{a2})$ belongs to the tolerance region of P2. However, $A(x_a, y_a)$ could potentially belong to either P1 or P2. The calculation is done using the logic shown in the figure below. In this particular case, since $D_1 < D_2$, $A(x_a, y_a)$ is a match to pre-registered click point-P_1.

$$D_1 = \sqrt{(x_1 - x_a)^2 + (y_1 - y_a)^2}$$
$$D_2 = \sqrt{(x_2 - x_a)^2 + (y_2 - y_a)^2}$$

```
$if\ (D_1 > D_2)||(D_1 < T_1)$
    $P_2$
$else$
    $P_1$
```

Fig. 3. Method to determine the authentication, when a particular authentication click falls into both regions

$A_f(x_f, y_f)$ is a false click in this case, since it's not within the tolerance region of either pre-registered click.

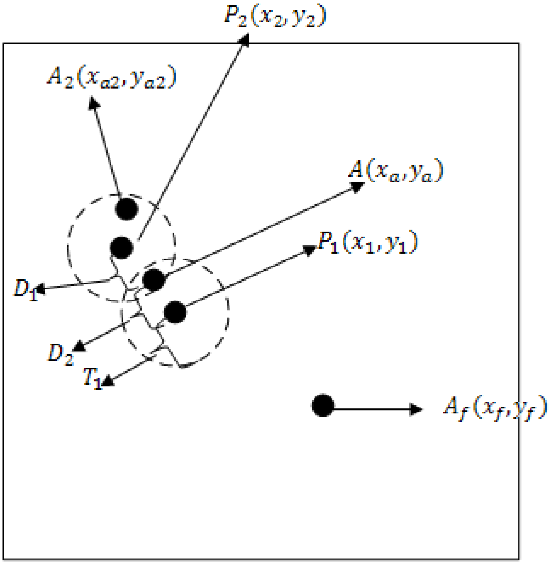

Fig. 4. P1 and P2 are the pre-registered clicks. $A_2(x_{a2}, y_{a2})$, $A(x_a, y_a)$ and $A_f(x_f, y_f)$ are the authentication clicks. D values represent the distance between two clicks. The dashed circular regions represent the tolerance regions. T1 represents the radius of the circular tolerance region.

4.2 The Choice of Tolerance Rate

The tolerance rate is defined as a number of pixels permitted to be selected around the original selection. A properly selected tolerance rate has direct impact on user experiences. The bigger the tolerance rate, the easier the user task is. At the same time, a bigger tolerance rate permits a bigger chance of educated guess. To balance security and usability, it is noted that a better tolerance rate is essential. After a brief user study, we found a tolerance rate bigger than 30 pixels is preferred among all users. When the tolerance rate is set below 30 pixels, the failure rate significantly increases. The following figure demonstrates how different tolerance rate affect the authentication failure rate.

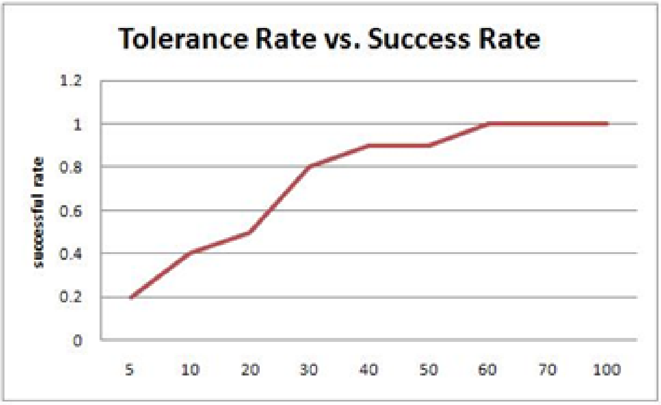

Fig. 5. As the tolerance rate increases, the percentage of successes also increases

4.3 Effective Password Space Analysis

In this section, we introduce a term “Effective Password Space”. In a touch pad or similar electronic devices that rely on finger touches or a hand-held tool for input, effective password space should be smaller than the touch pad screen size. Touch screens have special limitations such as: user’s finger, hand and arm can obscure part of the screen; and the human finger as a pointing device has very low “resolution”. It is also difficult to point at targets that are smaller than the users’ finger width. It is generally assumed that touch input cannot be accurate because of the fat finger problem, i.e., the softness of the fingertip combined with the occlusion of the target by the finger [12]. In the experiment conducted; we required user to register 5 non-overlapping points as their graphical password.

Studies have shown using a stylus pen or computer aided input device would potentially achieve an ideal accuracy of 1 pixels square [14], but the usability of such an approach remains a question. In particular, selection time and error rate data were not reported under this scheme and this mechanism was reported to be impractical to carry out in regular users’ daily life.

It also should be noted that “tolerance rate” is also a key factor in determination of effective password space. As shown from the previous section, a tolerance area should be set to accommodate the usability of the system. In the equation below,

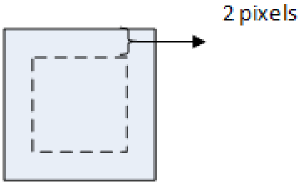

Fig. 6. Total effective password space for a touch screen, assuming the pressing area is 4 pixels square

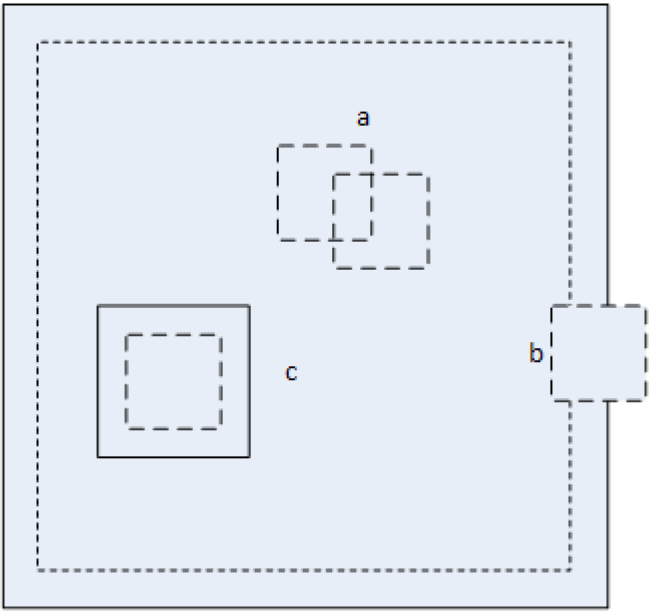

Fig. 7. Different touches on a touchpad

password space or the number of possible clicks can be defined in two possibilities (where n and m are the length and width of a particular screen in number of pixels):

$$password\ space = \begin{cases} 1, & if\ n \leq 4\ or\ m\ \leq 4 \\ (n-4)*(m-4), & if\ n > 4\ or\ m > 4 \end{cases}$$

There are typically three different cases for user touches, the first case, as shown in the figure above (a), two touches are overlapped. This is an illegal case of selection, since the overlapped region can belong to either touch. The second case (b) is very unlikely to happen, since part of the touch area would be outside of the touch screen. As a result, we conclude that the effective password space would be the inner dashed region, in another word, the difference of the actual touch screen size and the 2 pixels width side along each side. (c) is a legal registration in this case; the solid lines represents tolerance regions.

In the case of iPad, which became a popular hand-held touch pad device since April 2010, the screen size is $1024 \times 768\ pixels$. In a short experiment we conducted with users, we chose a simply designed screen of 16 rows and 12 columns, representing a total of 192 pixels; we can make the following calculations:

1. The first figure press can happen almost everywhere on the screen, except the edge areas as we discussed previously. Therefore, the possibility is 140—minus the edge pixels.
2. To calculate the second finger press possibility, we wrote a very simple program to statistically calculate the overall-possibility based on the first press's location.

As we mentioned before, first press has 140 possibilities. After measuring 140 different possibilities, the possibility of second press is close to 131 possible locations in average.

3. The third finger press is relatively harder to calculate. There should be four different types finger presses in general. The likelihood of each finger press is similar. After a brief calculation, we found122 possible areas for the third finger press in average (as shown in figure 6).
4. When the similar rules applied, 113 possible areas are found for the fourth finger press. And 104 possible areas are found for the fifth finger press.
5. In total, we had a possibility of $140 \times 131 \times 122 \times 113 \times 104$ password space—fairly large, but not sufficiently large enough to prevent brutal force search. After all, 2.6×10^{10} is still a finite number that can be cracked by brutal force attack.

In fact, applications for touch screen devices all suffer "fat-finger" problem. We performed an experiment with our users on a 850×650 screen with simple white background, and no assistance from any commercial software. We then measured the pixel size of 41 sparsely distributed finger presses made by our users. The average size was 67.9 pixels; the smallest pixel size was 6 and the largest was 213; with most sizes found between 10 and 100.

While these studies were limited to relatively large targets, In an extreme case, where user can achieve the minimal figure pressing area of 4 pixels square, the effective password space has been significantly reduced, although not dramatically. In the average case of user selecting 5 different regions as their graphical password, none of the 5 regions should have overlap. Studies have shown using a stylus pen or computer aided input device would potentially achieve an ideal accuracy of 1 pixels square [13], but the usability of such approach remains to be a question. In particular, Selection time and error rate data were not reported under this scheme, other than the fact this mechanism is impractical to carry out in regular users' daily life. It also should be noted that "tolerance rate" is also a key factor in determination of effective password space. Typically, a tolerance area should be set to accommodate the usability of the system, when tolerance rates are too high, users end up with less effective password space, and vice versa.

With all factors discussed, effective graphical password space for touch screen devices is indeed very small.

4.4 Background Image Selection vs. User Experiences

The complexity of an image is defined as a combinational quantitative measure of the number of objects presented, the number of major colors, and the familiarity of the image to users and other factors. Careful selected background images can enhance effective graphical password design. The study highlights the vulnerability of click based graphical passwords. As a result, we discuss several graphical password attacking methods based on the choice of pictures. This study aims to achieve better balance between security and usability of click based graphical passwords through better choices of background images. Successful rate, in this case, is defined as the number of successful authentications versus the number of trials within a critical time frame.

Users were given the option of using their personal pictures for background. In the presence of a background image, it is arguable if the password space will remain its complete full-size. Users do have significant preference when it comes to different background images. In another word, background images reduce password space; yet regular users cannot live without background images. [23]

Complexity of the background image directly affects the usability of the graphical password. Some of the factors that define the image complexity are listed below:

1. Colors: We cannot always provide the user with meaningful pictures. When the graphical password is generated in a semi-automatic fashion, color can play a practical role.
2. Objects: Objects in the image are another. Face recognition [24] is one type of graphical password that uses objects as its main theme. Depend on the size of the object and the proportions the object occupancy compared to the entire image, user may only able to focus on one or a very limited number of objects at a time.
3. Location and Shapes: There can be two types of shapes in a graphical password images: the shape of the objects in an image, or the shape formatted by patterns of clicks.

4.5 Security Concerns

Relatively little study of usability has been done for graphical passwords. In addition, as Cranor, et al.[25] noted, little work has been done to study the security of graphical passwords as well as possible attacking methods. In fact, some recent studies have shown that there are in fact unintentional patterns in user created graphical passwords. In reality, security and usability[23, 26]of graphical passwords are often at odds with each other, but both factors are critical to all authentication systems.

Chiasson et, al [27] found out that click-based passwords follow distinct patterns; and patterns occurs independently of the background image. Our brief user study showed user passwords do not always fall into patterns; click patterns actually occur only when the complexity of an image is higher than the tolerance. In fact, user studies proved patterns occur much less frequently than the other factors we mentioned above.

Some other [28-31] work suggested hot-spots occurs in click-based password. The hot-spot analysis work by Julie Thorpe [31] suggested that by using an entirely automated attack based on image processing techniques, 36% of user passwords within 2^{31} guesses (or 12% within 2^{16} guesses) can be broken in one instance, and 20% within 2^{33} guesses (or 10% within 2^{18} guesses) can be broken in a second instance. We believe semi-automatic methods with the help from human will enhance the attack.

5 Conclusion

Expert review of the system revealed graphical password for mobile touch screen devices to be effective and promising. During the debriefing following the experiment, experts proposed improving graphical targets through a variety of design innovations that may be avenues for future research. Expert reviews and usability experiments indicate graphical passwords have potentials to work well with touch screen devices.

Through experimental examination of touch sizes, tolerance areas and recall basked passwords, our scheme produced successful authentication rates of greater than 80%. This study contributes additional data to the field of graphical password research.

References

1. Apple, `http://www.apple.com`
2. Gartner, Gartner Says Touchscreen Mobile Device Sales Will Grow 97 Percent in 2010 (2010), `http://www.gartner.com/it/page.jsp?id=1313415`
3. Shepard, R.N.: Recognition memory for words, sentences, and pictures. Journal of Verbal Learning and Verbal Behavior, 156–163 (1967)
4. Wiedenbeck, S., et al.: PassPoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human Computer Studies (to appear)
5. Brewster, S.: Overcoming the Lack of Screen Space on Mobile Computers. Personal and Ubiquitous Computing 6(3) (2002)
6. Parhi, P., Karlson, A., Bederson, B.: Target Size Study for One-Handed Thumb Use on Small Touchscreen Devices. In: MobileHCI 2006, Helsinki, Finland (2006)
7. Hinrichs, U., et al.: Examination of Text-Entry Methods for Tabletop Displays in Horizontal Interactive Human-Computer Systems. In: Second Annual IEEE International Workshop on TABLETOP 2007, Newport, RI, pp. 105–112 (2007)
8. Sears, A., et al.: Investigating Touchscreen Typing: The effect of keyboard size on typing speed. Behaviour & Information Technology 12, 17 (1992)
9. Colle, H., Hiszem, K.: Standing at a kiosk: Effects of key size and spacing on touch screen numeric keypad performance and user preference. Ergonomics 47(13), 17 (2004)
10. Lee, S., Zhai, S.: The Performance of Touch Screen Soft Buttons. In: CHI 2009, Boston, MA (2009)
11. Sears, A.: Improving Touchscreen Keyboards: Design issues and a comparison with other devices. Interacting with Computers 3(3), 253 (1991)
12. Diller, F.: Target Practice: Current Efforts to Improve Input Areas on Touchscreen Mobile Devices (2010)
13. Garwin, R.L., Levine, J.L.: Light-sensitive pen to substitute for finger in laser-scanned touch screen. IBM Technical Disclosure Bulletin 32(3B), 11 (1989)
14. Go, K., Endo, Y.: Touchscreen Software Keyboard for Finger Typing. Advances in Human-Computer Interaction (2008)
15. Poupyrev, I., Maruyama, S.: Tactile interfaces for small touch screens. In: 16th Annual ACM Symposium on User Interface Software and Technology, New York, NY (2003)
16. Lee, J.C., et al.: Haptic pen: a tactile feedback stylus for touch screens. In: 17th Annual ACM Symposium on User Interface Software and Technology (2004)

17. Fukumoto, M., Sugimura, T.: Active click: tactile feedback for touch panels. In: CHI 2001 Extended Abstracts on Human Factors in Computing (2001)
18. Nashel, A., Razzaque, S.: Tactile virtual buttons for mobile devices. In: CHI 2003 Extended Abstracts on Human Factors in Computing Systems (2003)
19. Brewster, S., Chohan, F., Brown, L.: Tactile feedback for mobile interactions. In: SIGCHI Conference on Human Factors in Computing Systems (2007)
20. Hoggan, E., Brewster, S.A., Johnston, J.: Investigating the effectiveness of tactile feedback for mobile touchscreens. In: Annual SIGCHI Conference on Human Factors in Computing Systems (2008)
21. Poupyrev, I., Maruyama, S., Rekimoto, J.: Ambient touch: designing tactile interfaces for handheld devices. In: 15th Annual ACM Symposium on User Interface Software and Technology (2002)
22. Koskinen, E., Kaaresoja, T., Laitinen, P.: Feel-good touch: finding the most pleasant tactile feedback for a mobile touch screen button. In: 10th International Conference on Multimodal Interfaces (2008)
23. Suo, X., Zhu, Y., Owen, G.S.: The Impact of Image Choices on the Usability and Security of Click Based Graphical Passwords. In: Bebis, G., et al. (eds.) ISVC 2009, Part II. LNCS, vol. 5876, pp. 889–898. Springer, Heidelberg (2009)
24. Davis, D., Monrose, F., Reiter, M.K.: On user choice in graphical password schemes. In: Proceedings of the 13th Usenix Security Symposium, San Diego, CA (2004)
25. Cranor, L., Garfinkel, S.: Secure or Usable? Security & Privacy 2(5), 2 (2004)
26. Suo, X., Zhu, Y., Owen, G.S.: Graphical Password: A Survey. In: Proceedings of Annual Computer Security Applications Conference (ACSAC), Tucson, Arizona. IEEE (2005)
27. Chiasson, S., et al.: User interface design affects security: Patterns in click-based graphical passwords (2008)
28. Chiasson, S., et al.: A Second Look at the Usability of Click-based Graphical Passwords. In: SOUPS (2007)
29. Dirik, A.E., Menon, N., Birget, J.C.: Modeling user choice in the PassPoints graphical password scheme. In: SOUPS. ACM (2007)
30. Gołofit, K.: Click Passwords Under Investigation. In: Biskup, J., López, J. (eds.) ESORICS 2007. LNCS, vol. 4734, pp. 343–358. Springer, Heidelberg (2007)
31. Thorpe, J., van Oorschot, P.C.: Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords. In: 16th USENIX Security Symposium, Boston, MA (2007)