# Graphical Passwords for Older Computer Users

**Nancy Carter**
College of William & Mary
Williamsburg, VA 23187 USA
njcarter@cs.wm.edu

**ABSTRACT**
Computers and the internet have been challenging for many computer users over the age of 60. We conducted a survey of older users which revealed that the creation, management and recall of strong text passwords were some of the challenging aspects of modern technology. In practice, this user group based passwords on familiar facts such as family member names, pets, phone numbers and important personal dates. Graphical passwords formed from abstract graphical symbols or anonymous facial images are feasible, but harder for older computers users to grasp and recall. In this paper we describe initial results for our graphical password system based on recognition of culturally-familiar facial images that are age-relevant to the life experiences of older users. Our goals are to design an easy-to-memorize, graphical password system intended specifically for older users, and achieve a level of password entropy comparable to traditional PINs and text passwords. We are also conducting a user study to demonstrate our technique and capture performance and recall metrics for comparison with traditional password systems.

**Author Keywords**
Graphical Passwords; Authentication; Older Adults, Human Factors; Human Cognition; Face Recognition

**ACM Classification Keywords**
H.5.2. [User Interfaces]: User-centered Design.

**INTRODUCTION**
User authentication, through the creation and memorization of strong passwords, poses a challenge for older computer users [3][6]. The sequences of letters, numbers and symbols forming traditional strong passwords can be abstract, with less meaning to the user than a personalized text or image sequence. This project resulted from a survey of older users who revealed that text passwords were challenging to create and use. We have created and are currently evaluating an image-based graphical password technique designed specifically for the over-60 population. In contrast to previous work, which required the user to memorize anonymous facial images, abstract icons, points on a map or works of art, this project allows the user to choose a personally meaningful set of images to form their password.

The images chosen by the user are termed the "target images" and will be selected by the user from the display presentation. Target images are displayed embedded within a set of "decoy images" all on a single screen. All images showing in the display presentation are randomly placed. Figure 1 shows the case of a single four-image sequence that is contained within the representative screen displays. Decoy images are carefully chosen to match the external appearance characteristics of the password image set. Decoy images are drawn from the set of images within our database that are not meaningful to the user. The user typically has decades of familiarity with the subjects in the chosen password images, making those images easier to pick out from the decoy images.

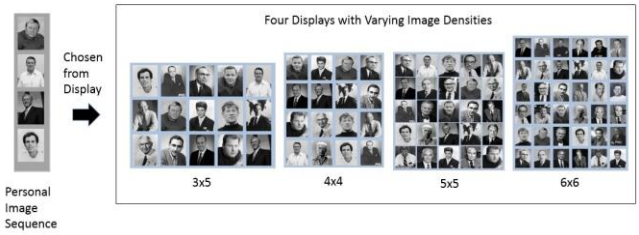


**Figure 1: Graphical password login screens. Left to Right: 4 image personal sequence, 3x5, 4x4, 5x5 and 6x6 displays.**

The selection of decoy images is restricted to images sharing physical characteristics with the target image set. The resulting display presentation is resistant to an in-person guessing attack. An observer looking at the display sees multiple images sharing common physical attributes and cannot identify the password target sequence by looking for unique aspects of the subjects in the images. As an example, a user choosing four males in business attire for their personal sequence will see a display randomly populated with images of males with ties wearing dark suits photographed against a light background.

If the user selects their sequence of personal images in the correct order, that constitutes a successful login. If the


*UIST '15* Adjunct, November 08-11, 2015, Charlotte, NC, USA
ACM 978-1-4503-3780-9/15/11.
http://dx.doi.org/10.1145/2815585.2815593

user is unsuccessful at selecting their sequence, then the login request is considered a failure and the display is refreshed with a re-randomized display of images. Because the arrangement of the images changes with each presentation, a casual observer will not see a geographic pattern to the location of the target images. Re-randomizing the arrangement of images also prevents a pattern from forming on touchscreen surfaces, a defense against a smudge attack [1]. Three successive failures should lock-out the user, providing a further defense against a guessing attack.

During our experiment, volunteers shared that they often developed a mental story to aid recall of their image sequences in the correct order. The mental story is formed from the user's personal association with the subjects in the images. These personal associations are not discoverable from written records or the results of web searching. It is the meaning behind the images that make the images an easily remembered password. Only the user knows which images are meaningful to them personally and therefore constitute the correct image sequence.

## BACKGROUND

Much work has been done with graphical passwords [2] but none with solutions that are personalized to each individual older user. Previous work with graphical password systems was based on images of artwork, computer icons such as emoji, and facial images of anonymous persons [3][7]. All are somewhat abstract and require effort to memorize. Writing down the images or icons required detailed descriptions, enabling anyone with access to the note to execute the described password sequence [4]. Older users are open to creative computing opportunities [8] and have shown they perform better at memorizing age-appropriate materials [4]. Our personalized password technique is also usable with a touchscreen [5] to facilitate those with hand and finger disabilities.

### Survey of Older Computer Users

We conducted an open-ended interview-style technology survey of more than twenty computer users over the age of 60 with the goal of identifying technology areas that could be meaningfully enhanced for this user population. The study revealed a common concern with creating and managing text-based passwords. Some representative comments from study participants are shown in the upper half of Figure 2. Fifteen of the study participants answered more detailed questions focusing on password creation, management and recall. Eleven of the fifteen stated they used a password creation strategy based on such familiar and comfortable components as a child's name, previous phone number, pet name, or spouse's birthdate. None of the surveyed users employed strong passwords meeting the definition of a series of characters including upper/lower case, numbers and symbols that did not contain a meaningful text sequence. Thirteen of the fifteen participants normally wrote down their passwords. Of the remaining two participants, one refused to use more than one password "in order to keep life simple." The other participant refused to use more than two specific passwords in their computing life. Both of these persons accepted the resulting lifestyle limitations on internet and computer use resulting from their password limitation decisions.

Overwhelmingly, older users in our study wrote down their passwords, and were careful to safeguard their written records. They recognized that access to the written passwords potentially resulted in compromise of their important personal online records. In the current situation, loss of the written records constitutes an immediate password compromise.

The study results motivated us to design an easy-to-use password scheme based on personally familiar images that will foster user confidence and increasing acceptance of computing and internet use. By relying on personally meaningful images, we hope that the tendency to write down explicit password image sequence descriptions will be lessened. If a user does write down a list describing image subjects, an attacker will have to understand the description to make a match possible to a specific image subject name. If a subject is identified, the attacker will still have to conduct sufficient research to identify each subject in the display presentation images. For example a music fan may choose images of Kate Smith, Glenn Miller, Dizzy Gillespie and Louis Armstrong for his password sequence images. The attacker finding this list of names will have to look up the names and learn what each person looks like before attempting to select this image sequence as a password.

> ***"It is annoying to create passwords, it is an extra effort and hard to memorize."***
>
> ***"It is hard to make a password that is halfway safe."***
>
> ***"It was easy to quickly recognize my chosen images because I have followed the careers of those individuals all my life."***
>
> ***"It has been a week and I cannot forget my password image sequence."***
>
> ***"This [password image technique] is interesting!"***

**Figure 2: Volunteer Comments.**

### Graphical Password Entropy

One goal of our graphical password technique is to achieve a level of entropy comparable or superior to the traditional text password or PIN code systems. Entropy is the unpredictability of possible values in a password sequence. A system with higher entropy is more resistant to guessing attacks but harder to memorize. A text-based

password, N characters long, using the alphabet a to z, A to Z, 0 to 9 and symbols !@#$&*+%, has 70N possible values. Each character having one of seventy possible values. A graphical password based on images has as many possible values as the choices available on the screen to the user. The more images on the display, the greater the entropy of the password system. Given N images and password length M, our technique's entropy is N^M. As shown in Figure 3, an 8 character text password system with entropy of 5.7 x 10^14 is comparable to an 8 image password sequence chosen from a display with 70 images. Both have greater entropy than a traditional PIN code system.

Our challenges are that increasing the number of images on the display forces each image to be smaller, and therefore harder to see and discern image details. Our display consists of a single screen to eliminate the need for scrolling, a challenge for those with finger and hand disabilities. Longer password sequences result in greater entropy but add to the memorization and recall challenge. The time needed to hunt and select the chosen target password images within the surrounding decoy images increases. The probability of choosing the correct images in incorrect order also increases. One goal of our experiment is to understand how users search the displayed images. Are there techniques available to speed up the visual search pattern for the target images and thereby make the graphical password system faster? Does peripheral vision aid in speeding up the search for the target images? Do users remember the current locations of subsequent target images while searching for the initial members of the target image set? Do target image sequences become too long for effective recall and search? Can display screens have too many or too small images for effective search?

### Graphical Password System Design

We use a laptop computer equipped with a touchscreen and mouse for this project. A large collection of images is organized into categories based upon the occupation of the subject. Participants selected categories based on personal interests and then chose personal image sequences by browsing. One question our experiment hopes to answer is to find out if users who spend more time selecting meaningful target images, perform faster and have better recall than users who spend less time selecting their target images? Each participant identified images which were unknown to them in a separate session. The set of decoy images was chosen from the set of personal unknown images.

Our study participants selected target sequences in lengths of 4, 7 and 10 images. Password sequences were presented in screens of 3x5, 4x4, 5x5, 6x6 and 7x10 images. Each display shows a random image placement to aid in defense against touchscreen smudge attacks [1] and in-person guessing attacks.

### Image Database

The images in the database are carefully chosen of subjects who were famous during the early working years of the over-60 user. All of the images are black and white, focusing on the subject's upper torso or face. Identifying features such as team or corporate logos have been removed. Each image has been coded as to sex, race, posture, attire, foreground color, background color, gaze direction and brightness level. The coding facilitates composing a set of decoy images that match the feature set and color spectrum of the password target images. An attacker cannot guess the password sequence based on visible attributes of the images. Each user's personal history motivated the choice of images for their password target sequence. That motivation is in effect an internal "secret key" to the password image sequence and is unique to each individual.

| Pin Length | 10 Symbol Alphabet |
|---|---|
| 4 | 10E+04 |
| 5 | 10E+05 |
| 6 | 10E+06 |
| 7 | 10E+07 |
| 8 | 10E+08 |
| 9 | 10E+09 |
| 10 | 10E+10 |

**(a)**

| Text Length | 10 Symbol Alphabet |
|---|---|
| 4 | 2.40E+07 |
| 5 | 1.68E+09 |
| 6 | 1.18E+011 |
| 7 | 8.24E+012 |
| 8 | 5.77E+014 |
| 9 | 4.04E+016 |
| 10 | 2.82E+018 |

**(b)**

| | Display Screen Density | | | |
|---|---|---|---|---|
| Sequence Size | 16 | 25 | 36 | 70 |
| 4 | 6.55E+04 | 3.91E+05 | 1.68E+06 | 2.40E+07 |
| 5 | 1.05E+06 | 9.77E+06 | 6.05E+07 | 1.68E+09 |
| 6 | 1.68E+07 | 2.44E+08 | 2.18E+09 | 1.18E+011 |
| 7 | 2.68E+08 | 6.10E+09 | 7.84E+010 | 8.24E+012 |
| 8 | 4.30E+09 | 1.53E+011 | 2.82E+012 | 5.77E+014 |
| 9 | 6.87E+010 | 3.81E+012 | 1.02E+014 | 4.04E+016 |
| 10 | 1.10E+012 | 9.54E+013 | 3.66E+015 | 2.82E+018 |

**(c)**

**Figure 3: Entropy Comparison of Multiple Graphical Password Systems. Clockwise from upper left: PIN Code (a), Text Password (b) and Graphical Password Systems (c).**

### Interim Results

Participants completed a series of exercises that utilized self-chosen 4, 7 and 10 image target sequences. Each experiment recorded timing and success/failure rates for varying sequence lengths of 4, 7 and 10 images, and varying display image densities of 15, 16, 25, 36 and 70 images. Each participant also prepared and typed text-based passwords of varying lengths for comparison purposes. Participants repeated the exercises at intervals of at least a week after choosing their target images to determine recall.

Volunteers are typically able to select their four-image password image sequences easily and quickly in the lower density screen displays. Often they did this more quickly than some volunteers would take to look up, recall and type a text password. Figure 4 provides a comparison of the individual timing differences between the first and last exercises performed by nine volunteers using five display image densities. Volunteers performed no more than two intermediate experiments at each density level. Selection times and group variance improved with this minor amount of experience.

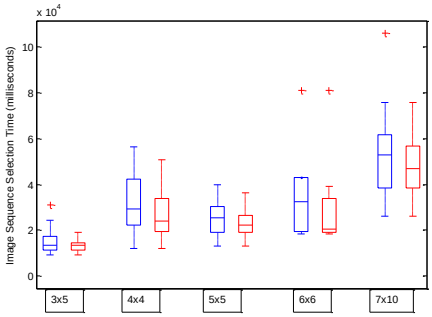


**Figure 4: Login timing data for nine volunteers using a mouse to select a personal four image sequence from display grids of increasing density. From left to right: 3x5, 4x4, 5x5, 6x6 and 7x10 display grids. Blue identifies the first experiment result. Red identifies the last result.**

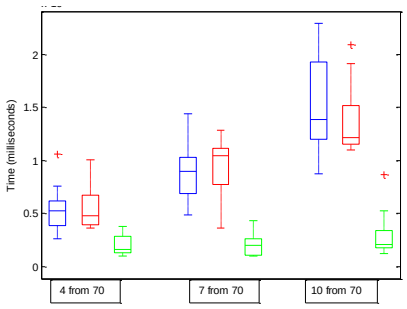


**Figure 5: Average login timing for nine volunteers using a mouse to select an increasing size image sequence from a 7x10 display grids. From left to right: 4, 7 and 10 image sequences. Blue is the first attempt. Red is the last. Green is the comparable size text password result.**

Figure 5 provides a comparison of the median timing differences at a single density of 70 images. In order to compare mouse with touchscreen performance, we used results from 11 volunteers running 138 exercises with their four-image sequences and a 4x4 display. The median time login with the mouse was less than twenty seconds, and less than fifteen seconds using the touchscreen.

Participants often provided positive comments such as those shown in the lower half of Figure 2. Their comments are a marked contrast to the concern many older users associate with the formation, management and use of traditional strong text passwords.

## CONCLUSION

Our initial results show that a culturally-relevant, personally meaningful, image-based graphical password solution is promising as a technically effective, socially accepted and easier-to-use alternative to text-based passwords for older computer users. Our study will continue to evaluate this technique with more volunteers to assess timing and recall effects of peripheral vision, effects of color contrast patterns and image hunting techniques.

## ACKNOWLEDGMENTS

We gratefully acknowledge the contributions of colleagues Ed Novak, Cheng Li, Zhengrui Qin, and Qun Li, along with our volunteer participants who willingly shared their opinions about computing and internet technologies.

## REFERENCES

1. Aviv, A., Gibson, K., Mossop, E., Blaze, M., and Smith, J. Smudge Attacks on Smartphone Touch Screens. In Proc. WOOT 2010, USENIX Assn, Article No. 1-7.

2. Biddle, R., Chiasson, S. and Van Oorschot, P.C. Graphical Passwords: Learning from the First Twelve Years. ACM Computing Surveys (CSUR), Volume 44 Issue 4, August 2012, Article No. 19.

3. Brostoff, S. and Sasse, M. Are Passfaces More Usable Than Passwords? A Field Trial Investigation. In People and Computers XIV-Usability or Else!, SprinkerLink (2000), 405-424.

4. Chowdhury, S., Poet, R. and Mackenzie, L. Passhint: Memorable and Secure Authentication. In Proc. CHI 2014, ACM (2014), 2917-2926.

5. Findlater, L., Froehlich, J., Fattal, K., Wobbrock, J., and Dastyar, T. Age-Related Differences in Performance with Touchscreens Compared to Traditional Mouse Input. In Proc. CHI 2013, ACM (2013), 343-346.

6. Nicholson, J., Coventry, L. and Briggs, P. Age-Related Performance Issues for PIN and Face-Based Authentication Systems. In Proc. CHI 2013, ACM (2013), 323-33.

7. Passfaces Corporation. The science behind Passfaces. http://www.passfaces.com/enterprise/ resources/white_papers.htm accessed April 2015.

8. Waycott, J., Vetere, F., Pedall, S., Kulik, L., Ozanne, E., Gruner, A. and Downs, J. Older Adults as Digital Content Producers. In Proc. CHI 2013, ACM (2013), 39-48