Graphical passwords for older computer users

Nancy Carter*, Cheng Li and Qun Li

Department of Computer Science,
College of William & Mary,
Williamsburg, VA 23187, USA
Email: njcarter@email.wm.edu
Email: cli04@cs.wm.edu
Email: liqun@cs.wm.edu
*Corresponding author

Jennifer A. Stevens

Department of Psychological Sciences,
College of William & Mary,
Williamsburg, VA 23187, USA
Email: jastev@wm.edu

Ed Novak

Department of Computer Science,
Franklin and Marshall College,
Lancaster PA 17604, USA
Email: ed.novak@fandm.edu

Zhengrui Qin

School of Computer Science and Information Systems,
Northwest Missouri State University,
Maryville MO 64468, USA
Email: zqin@nwmissouri.edu

Abstract: Traditional text password authentication is widely used to gain access to computing resources. Not all users possess the same cognitive and manual dexterity skills required to easily create, recall, and enter strong text passwords. We interviewed a group of older users, over the age of 60, and identified user challenges with recall and typing of strong text passwords. We developed and evaluated our graphical password user password system based on familiar facial images embedded randomly among unfamiliar, yet similar images. It assists older users through use of culturally familiar, and age-relevant images forming personalised password image sequences. Our usability study with 19 older volunteers measured recall, and timing with varying password image sequence lengths, increasing display complexity, and two input modalities, touchscreen and mouse. Our graphical password technique demonstrated a recall rate of 97%, password entropy superior to short PINs, and authentication time comparable to short text passwords.

Keywords: authentication; security; graphical passwords; human computer interaction; older users.

Reference to this paper should be made as follows: Carter, N., Li, C., Li, Q., Stevens, J.A., Novak, E. and Qin, Z. (xxxx) 'Graphical passwords for older computer users', *Int. J. Security and Networks*, Vol. X, No. Y, pp.xxx–xxx.

Biographical notes: Nancy Carter received her BS in Computer Science from the University of Maryland, College Park Maryland, and MS in Electrical Engineering from the Naval Postgraduate School, Monterey, California. She is currently a PhD candidate at the College of William & Mary in Williamsburg, Virginia. Her research interests are in human-computer interaction and the internet of things.

Cheng Li received his BS in Computer Science from Nankai University, and MS in Computer Science from the Harbin Institute of Technology. He is currently a PhD candidate at the College of William & Mary in Williamsburg, Virginia. His research interests include software-defined networking, network security, social networks, machine learning, Bitcoin, smart contracts, and the internet of things.

Qun Li is a Professor of Computer Science at the College of William & Mary. He is the recipient of an NSF Career Award and has been recognised as an IEEE fellow. He received his PhD from Dartmouth College. His research interests focus on wireless, mobile, embedded systems and pervasive computing.

Jennifer A. Stevens is an Associate Professor in the Department of Psychological Sciences at the College of William & Mary. She received her BA in Psychology and Philosophy from Ohio State University. She received her MA and PhD from the Department of Psychology at Emory University. Her research interests are in cognitive neuroscience investigating representation, perception, and execution of action.

Ed Novak is an Assistant Professor of Computer Science at Franklin and Marshall College. He earned his BA from the Monmouth College. He received his MS and PhD from the College of William & Mary. His research interests focus on the digital privacy and security of mobile devices, and the internet of things paradigm.

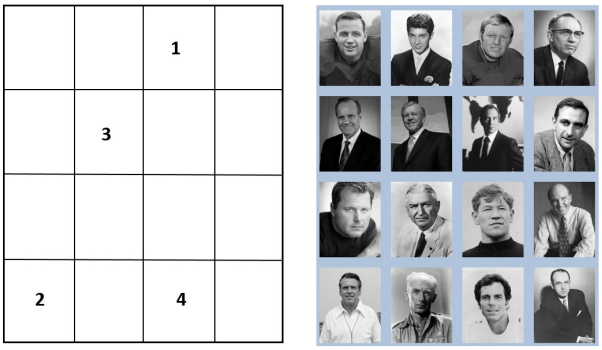
Zhengrui Qin is an Assistant Professor in the School of Computer Science and Information Systems, Northwest Missouri State University. He received his PhD from the College of William & Mary. His current research interests include cyber security and mobile computing.

This paper is a revised and expanded version of a paper entitled ‘Graphical passwords for older computer users’ presented at the Fifth ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb 2017), San Jose, CA, USA, 14 October 2017.

1 Introduction

User authentication through keyboard entry of text passwords is a daily activity for most users. Yet not all portions of the user population find this to be an easy task. After interviewing a group of older volunteers about their human-computer interactions, we confirmed that creating, recalling, and managing strong text passwords were very challenging tasks (Brostoff and Sasse, 2000; Nicholson et al., 2013). We were motivated to design a new password authentication mechanism specifically for older users, a system that would be cognitively and physically easy to use, and also foster feelings of user well-being and competence. our graphical password system enables the user to choose a personally meaningful set of black and white facial images as their personal password sequence, known as the target image set (Carter et al., 2015). A set of unfamiliar, yet similar images, known as the decoy image set, are appended to the user’s target image set to form the displayed image set. The complete set of displayed images are randomised for each presentation to the user. Each user recognises and selects their personal target image sequence from within the randomised display using either the mouse or their finger applied directly to the touchscreen. The image identifier numbers associated with the target and decoy images constitute the graphical password definition within the computing system. An example of a 16-image display is shown on the right in Figure 1. The numbered grid cells on the left of Figure 1 indicate this user’s correct image selection sequence to successfully authenticate, for this instance of the randomised user display presentation.

Figure 1 Graphical password example (see online version for colours)



Our technique leverages the unique cognitive and neural abilities that humans have for processing and recognising faces. The fusiform face area (FFA) in the temporal region of the brain is dedicated to the processing of faces (Kanwisher, 2010), beginning from infancy (Farzin et al, 2012). The neural processing of faces in the FFA has been extensively documented via MRI studies (Van Balen and Wang, 2015; Liu et al., 2010; Gauthier et al., 2000). The built-in human ability to recognise faces from an individual’s personal past history is an easier cognitive task than recollecting memorised sequences of text, symbols or anonymous facial images (Calvo and Peters, 2014; Rogers et al., 2011).

The US population is aging, and having difficulty using computer technology. By 2030, more than 20% of the US population will be 65 and older, contrasted with 13% in 2010 (United States Census Bureau, 2014). In 2013, 41% of

the US adults aged 65 and older did not use the internet and one-third of these felt that the internet was not very easy to use (Pew Research Center, 2014). Among users aged 77 or older, fully 62% do not use the internet (Pew Research Center, 2013). As more of society's functions move online, it is important to study and facilitate older user engagement with computing and the internet (Lindley et al., 2008; Haris et al., 2014).

During our interview study, volunteers indicated that typing strong text passwords was physically challenging because text passwords require good vision to search computer keys for required letters and symbols. Finger, hand, and arm mobility issues can also impair fine motor skills needed for successful typing. Our graphical password system eliminates the need to enter text entirely.

Keyboard entry-based systems such as ten-digit keypads on automated teller machines (ATMs) or symbol grids on smart phone unlock screens require users to memorise abstract number or symbol sequences, and do not vary number or symbol positions, increasing vulnerability to shoulder surfing. These smaller keyboards are harder for the visually impaired to see. Limited symbol sets constrain potential password choices. Subsection 3.3 discusses the improved entropy afforded by increased symbol sets in password construction. Section 6 provides an analysis of current smart phone unlock mechanisms and comparison with our graphical password technique.

Recently, fingerprint sensors have emerged as a popular biometric authentication technique. Unfortunately, the normal process of aging can make skin thinner, and fingerprints therefore become difficult or impossible to scan or recognise (Harmon, 2009). Additionally, certain medical conditions or treatments may render fingerprints unreadable. Older users with health issues resulting in palsy, or shaking, of the hands, fingers or arms may not be able to hold still for a fingerprint scan. Our graphical password system eliminates the need to enter text entirely, and accommodates bodily changes encountered through aging.

The password strength or entropy of our graphical password system is comparable to short text passwords and superior to PINs. Increasing the entropy of our system is possible by increasing the number of images on the display, and increasing the number of images in the user's chosen target sequence. Increasing entropy potentially results in increased authentication time, and reduced recall performance as users search among a larger set of images or strive to recall a longer personal sequence.

Previous work and our volunteer interviews revealed that users often kept written notes of text passwords to aid recall. Unfortunately, loss of the note constituted an immediate password compromise. Written descriptions of our graphical password sequences are not literal physical descriptions. User notes may cite subject names or occupations. Such information may not be recognisable to an adversary gaining possession of the note. Users of our system can create personalised sequences of images that are very meaningful. Some of our volunteers shared that they did not need to keep notes because their chosen sequences had strong personal associations, making them hard to forget.

We conducted a usability study to measure recall and timing performance of our graphical password design. We assembled a database of 550 black and white images, coded as to physical attributes of the image, and occupation of the image subject. We created an image sequence selection tool so each user could efficiently browse the database based on occupation of the image subject. Each volunteer chose three personal target image sequences in lengths of four, seven, and ten images. A series of authentication exercises was created to measure recall rates and elapsed password sequence selection times with varying display image densities, password image sequence lengths, image arrangement patterns, and input device modalities. Additional exercises measured text entry time using the keyboard for comparison purposes. Exercises were repeated to measure user improvement through training experience.

Section 2 of this paper presents a survey of the current literature on graphical password systems. Section 3 presents our graphical password system design including motivations realised from our interview-style survey of older computer users. Section 4 describes our usability study. Results of our usability study are presented in Section 5. We compare our graphical password system with current smartphone unlock techniques in Section 6. Conclusions are presented in Section 7.

2 Related work

Previous graphical password work has been categorised as either recall-based, recognition-based, or cued-recall. *Recall-based* systems such as draw a secret (DAS) and background draw a secret (BDAS) (Dunphy and Yan, 2007) require the user to recreate a previously produced digital drawing. GridMap (Van Balen and Wang, 2015) requires precision finger touching along a series of points on a map presentation. DAS, BDAS and GridMap would be challenging for a user with hand or finger disabilities. *Recognition-based* systems require the user to memorise sequences of abstract images such as emoji, icons, or anonymous faces (Brostoff and Sasse, 2000; Passfaces Corporation, 2015). These sequences are later chosen from amid larger displays containing similar decoy images. *Cued-recall* systems such as Passpoints (Wiedenbeck et al., 2005), require the user to memorise a set of specific points within an image and to later accurately re-select the same point sequence. All of these tasks require significant manual dexterity and drawing skills, and significant memorisation of abstract patterns. Biddle's survey (Biddle et al., 2012) reveals none of the previous work were implemented with solutions personalised to the history of each individual older user.

Komanduri and Hutchings (2008) propose a system requiring the matching of pictures with accompanying text, both shown simultaneously on a display screen. Users transcribe text shown below their assigned images using the keyboard to form the password. While they achieve an

entropy superior to theoretical text password entropy, transcription poses an additional cognitive task, and challenges those with vision or hand-finger impairments.

Users in previous work created written notes describing image, drawing or icon password sequences. Anyone with access to the note could then execute the described password sequence (Chowdhury et al., 2014). User notes describing the subjects in our graphical password personal sequences are not immediately useable. Attackers with access to the note would have to recognise the subject names and their corresponding images in order to match displayed images with the written description.

In practice, users often simplified their text (Florencio and Herley, 2007) and graphical passwords, resulting in a reduction of the practical entropy level of the system. Bonneau and Preibusch (2010) note that Passfaces Corporation (2015) results showed predictable user image choices. Passfaces users often chose faces of self-similar race or gender, or chose faces of those deemed especially beautiful. DAS, BDAS and GridMap users tended to make simple, symmetric, or centred pattern choices. Florencio and Herley (2007) showed that users also often reduce the practical entropy of their text passwords by choosing simplified text passwords. Our design re-randomises image placement at each presentation and requires all images to be unique within a personal sequence, eliminating the possibility of entropy reduction.

Passfaces (Brostoff and Sasse, 2000) required users to navigate multiple screen displays, choosing one facial image on each display. This additional cognitive task requires the user to remember current logical position within a sequence of displays. Our graphical password design presents all image information on a single display screen.

Older users are open to creative computing opportunities (Waycott et al., 2013) and have shown they perform better at memorising age-appropriate materials (Chowdhury et al., 2014). Our graphical password system is personalised to the older user, with a large selection of images available in our database reflecting notable individuals from the prime working years of the over-60 user.

Vision and manual dexterity impairments may render the keyboard challenging to use, resulting in higher errors with such techniques as tap re-authentication (Hao and Li, 2016), and video interpretations of external virtual keyboards (Yin et al., 2016). Our graphical password system enables use of the mouse and touchscreen. Both devices are faster than the keyboard for selecting sequences. The touchscreen has been shown to speed up older adult movement tasks by 35% when compared to the mouse (Findlater et al., 2013).

3 System design

3.1 Design motivation

We conducted an open-ended interview-style technology survey with twenty-six computer users over the age of 60 with the goals of understanding their computing concerns and motivations, and identifying technology areas for enhancement tailored to this user population. Strong text password creation, management, and recall emerged as a major user issue. Some older volunteers deliberately chose to limit their use of technology in order to avoid accumulating more passwords. Other volunteers only used one or two passwords at multiple internet sites. Volunteer comments are listed in Table 1.

Table 1 User interview comments

User comment	*Comment topic*
It is annoying to create passwords, it is an extra effort and hard to memorise.	Password creation
It is hard to make a password that is halfway safe.	Password creation
I only use one password in order to keep life simple.	Password usage

Nineteen of the interview-style study participants answered more detailed questions focusing on password creation, management, and recall strategies. None of the 19 personally used strong passwords meeting the classic definition of a series of characters including upper/lower case, numbers, and symbols, without personally meaningful text sequences. All but one of our volunteers prepared text passwords containing character sequences with strong personal associations such as a child's name, previous phone number, pet name, or spouse's birth date. Such information may be easily findable by an adversary using the internet.

All but two of our volunteers routinely wrote down passwords, making them available to anyone with access to the written record. Two volunteers refused to use more than two passwords and accepted the resulting lifestyle limitations on internet and computer use.

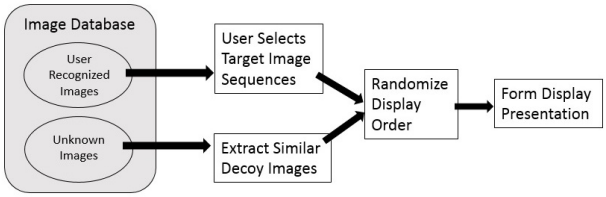
We were motivated to design a new password mechanism specifically for older users, a system that would be physically easy to use and foster feelings of well-being by enabling user competence, and relatedness to their past memories (Calvo and Peters, 2014). By relying on personally meaningful images, we hope the tendency to write down explicit password descriptions will be lessened. It would be hard for users to hand draw accurate image reproductions to make a personal note. If a user does write down a list describing image subjects, an attacker must understand the description to make a match possible to an image subject name. As an 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 the list of names 'Kate, Glenn, Diz and Louis' will have to understand the names and research each person's appearance before attempting their attack.

Using a single display screen for the entire authentication process reduces the need for users to remember selections from previous screens and reduces the number of hand and finger actions.

3.2 Design components

Our design components consist of a collection of black and white images, software for user selection of target images forming personal user sequences, software to facilitate selection of user decoy images, laptop computer equipped with touchscreen and mouse, and usability study software to display varying configurations of images, accept user inputs from the touchscreen or mouse, and record user action elapsed times and results.

Figure 2 Graphical password display construction



The graphical password display screen is formed from the user's target image set and their decoy image set as shown in Figure 2. Once these two image sets are defined, they are merged into one set of images, and their display order is randomised before constructing the display presentation to the user. The user proceeds to select their personal image sequence by either directly touching the touchscreen, or using the mouse to click on selected images. After the complete personal image sequence is selected, the user indicates they are finished and the user's selection is validated. If the user was correct in selecting the proper sequence, then a success is registered. If the user was incorrect in selecting the proper sequence, an error is recorded, the set of images is re-randomised and re-presented to the user.

Each image has a unique image identifier number. The complete graphical password is formed by the set of target image identifier numbers in correct sequence appended to their personalised set of decoy image identifier numbers. Each user's personal target image sequence, chosen based on strong personal memories from the past, forms a 'secret key', unique to each individual. Only the user recognises their personal sequence when viewing all the images on the display. Existing websites or software may incorporate our graphical password system by substituting the user's unique set of target and decoy image identifiers for the traditional text password characters. The complete graphical password is stored by the computer in association with the user's account username, comparable to storage of a traditional text password. This system substitutes an image for each character of the replaced password. Longer password sequences may be implemented by increasing the user's personal image sequence, and adapting the onscreen display presentation to display increased numbers of images. User authentication software would access an image database to retrieve the correct images for display and selection by the user. The image database could either be installed locally or accessed from a web service over the internet via a secure channel.

User amenities such as password hints, password managers, and password reset features could also be adapted for use with graphical passwords. Password managers store and retrieve text passwords as needed to perform user authentications. Expanding the password manager software to discriminate between text and graphical passwords will require each user account to identify associated password type. Storage must increase to accommodate sets of image identifiers in place of text characters. Password managers must serve up the graphical password image identifier numbers in correct order to successfully authenticate. Some password managers create new text passwords upon demand with no user involvement. Since graphical passwords rely on facial recognition to facilitate successful human recall, the user will need to select new graphical password sequences.

3.3 Entropy analysis

A goal of our graphical password design is to achieve a level of entropy, or password strength, comparable or superior to traditional text password or PIN code systems (Password Strength, 2016). Entropy is characterised as the unpredictability of possible values in a password sequence. A password system with higher entropy is more resistant to guessing or brute force attacks but may become harder to memorise or recognise due to increased symbol complexity, increased password sequence length, or increased user display density. Higher entropy configurations in the graphical password system may increase user authentication time as users search for more password sequence images from among higher density displays.

The entropy of our approach is described from three perspectives. First, the information entropy of the symbol set formed by our image database is characterised. Second, the password strength of our system from the perspective of an attacker with direct access to a user system is described. Third, the entropy of a client-server graphical password configuration is described from the perspective of an outside attacker emulating a user. For comparison purposes, equal length text and image password sequences are described from each perspective.

Information entropy is defined as the binary log of the number of possible passwords, provided that each symbol in the password is independent (Password Strength, 2016). The entropy of a random password *H*, is defined

$$H(A,b) = b \times \left(\log_2 (|A|)\right), \tag{1}$$

Given a symbol set *A* serving as the source repository for password symbols, and a chosen password of length *b* symbols, the entropy is the product of the cardinality of *A* and the length of the chosen password sequence. For comparison purposes, assume text passwords are drawn from a set of case-sensitive alphanumeric symbols a–z, A–Z and 0–9 with 62 possible symbols available for each character. The binary log of 62 is 5.95. Graphical password symbols in our usability study are drawn from a repository of 550 images. Repeating images is not permitted, therefore

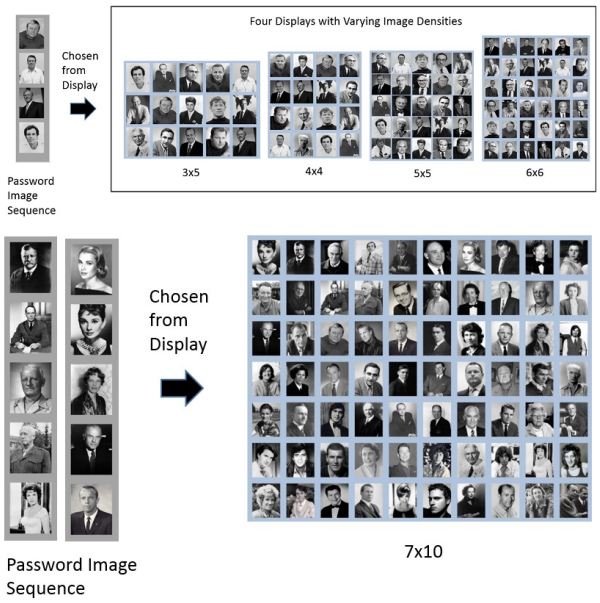
one less image is available for each subsequent choice. For comparison purposes, the binary log of the range 550 to 540 is rounded to 9.1. Comparing equal length text and graphical passwords, each consisting of eight symbols,

$$H_{text}(62, 8) = 8 \times (\log_2(62)) = 47.6 \text{ bits} \quad (2)$$

$$H_{graphical}(550, 8) = 8 \times 9.1 = 72.8 \text{ bits} \quad (3)$$

$H_{graphical}(550, 8)$ is shown to be a 53% improvement over $H_{text}(62, 8)$.

Figure 3 Configuration examples (see online version for colours)



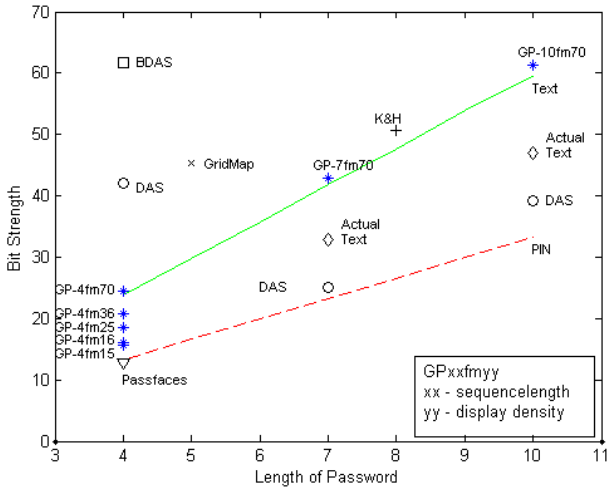
Our usability study demonstrated that longer graphical passwords were difficult for our volunteers to use. A four-image password chosen from a 6 × 6 display configuration was demonstrated as practical in our study. Currently, there is a trend towards requiring longer user text passwords in real-world systems. Comparing a ten-character text password with a four symbol graphical password,

$$H_{text}(62, 10) = 10 \times (\log_2(62)) = 59.5 \text{ bits} \quad (4)$$

$$H_{graphical}(550, 4) = 4 \times 9.1 = 36.4 \text{ bits} \quad (5)$$

$H_{graphical}(550, 4)$ is shown to be a 39% decrease from $H_{text}(62, 10)$ Increasing the image repository to 30,060 images would raise the entropy of the graphical password system equivalent to this text system. In practical application, such a large image repository may require software tools to facilitate user selection of personal target image sequences, and system selection of decoy images. The second perspective is that of an attacker with direct access to a user's personal computer. Faced with attempting to enter a four-character text password, there are N^M possible combinations where N = 62 possible valid text characters and M = 4 choices to be made. To exhaustively try all possible text combinations will take 62^4 = 14,776,336 attempts. Facing a graphical password display of 16 images and choosing the correct permutation of four images will take $N!/(N - M)!$ = 43,680 attempts. In this case, exhaustively trying a text password will take longer than a graphical password image sequence. As with text and PIN systems, graphical password systems may apply system-imposed timeouts after sequential unsuccessful authentication attempts. As an example, with three attempts per minute before a graphical password system-imposed timeout of ten minutes, it will still take 111 days of non-stop attempts to exhaust all possibilities. In comparison, a four-digit numeric PIN offers 10,000 possible combinations. A common touchscreen password mechanism requires the user to select the correct symbol sequence from a grid of identical static symbols such as dots. A configuration requiring the user to select the correct sequence of four non-repeating symbols from a grid of 16 symbols would have a entropy of 43,680 possible variations. Since the correct symbol sequence does not vary in location, a smudge pattern could develop on the touchscreen surface that could aid an attacker. Our approach eliminates the possibility of a smudge pattern by randomising each display presentation.

Figure 4 Entropy comparison (see online version for colours)



The third perspective is that of an attacker attempting to log into a user account on a website from the attacker's personal computer. In this scenario, if a user had a valid four-character text password already stored at the website, the attacker must submit a correct four-character password. As described previously in the second perspective, there are 62^4 = 14,776,336 attempts to be made by the attacker to exhaust all possible combinations. With the graphical password design implemented in a client-server configuration, website servers would already possess a pre-existing record of all 16 images forming the user's display along with a record of the user's valid four image sequence. Each authentication attempt with the graphical password system requires the attacker's client to submit to the server, via a secure channel, 16 symbols representing the chosen image numbers of the user-selected sequence along with the unchosen decoy images. An attacker with no knowledge of

any of the images in the user's display must submit the correct combination of 16 image numbers in addition to the correct permutation of four image numbers forming the user's chosen target sequence. Assuming the attacker knows that the database is currently limited to 550 images, there are 2.69×10^{30} possible combinations of the 16 images that must be attempted, *each* combination with 43,680 possible four image permutations.

The entropy of the graphical password design may be increased by either increasing the number of images in the display or increasing the length of the password image sequence. Our usability study was designed to measure the effects of increasing entropy on user authentication success and timing.

Figure 3 illustrates many of the configurations that were implemented in the usability study described in Section 4. Figure 3 shows the four and ten image sequences, along with the 15, 16, 25, 36, and 70 image density displays. We were able to measure the effects on user recall and elapsed time as entropy increased. Results of the usability study are presented in Section 5.

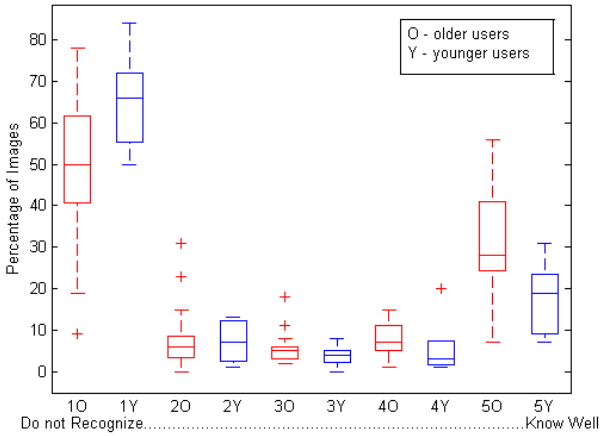
Figure 4 provides a comparison of the graphical password entropy under six configurations of password sequence length and display image density. Each configuration is denoted within Figure 4 by GP-xxfmyy where xx is the sequence length and yy is the display density. Entropy levels of varying PIN, text, and actual text (Florencio and Herley, 2007) systems are also plotted along with notable graphical password systems described in the literature review of Section 2. Entropy is expressed as the bit strength or binary log of the number of possible guessing attempts for the listed password system configuration. While our four-image configuration is comparable to short text passwords and superior to four-digit PINs, the client-server design implementation offers the potential for higher entropy than traditional text passwords of length eight characters.

3.4 Image database

We collected, processed and coded 550 black and white facial images of notable figures from the past. These subjects were prominent in many areas of the US culture during the early-to-mid working years of the over-60 user. While our system could be used by those of any age or cultural background, we deliberately chose images familiar to our older the US study volunteers to leverage the cognitive advantages offered by the FFA. For future work, a production version of the graphical password system could permit the user to identify their age and cultural heritage, and then offer candidate target images that are likely to resonate with the user's cultural background.

It is important that images appear to be similar on the screen to defend against shoulder surfing attack. We converted all collected images to black and white. Images were then digitally manipulated to remove noticeable identifying team logos, military insignia or corporate markings from clothing and backgrounds. Prominent features noticeable from a distance such as large jewellery or boutonnieres were also digitally removed. Images were cropped down to one of three sizes: head and shoulder, head to waist, and full body.

Figure 5 User image recognition (see online version for colours)



Each image has been coded as to subject body size, sex, race, gaze direction, attire, image foreground colour, background colour, and brightness level. Attire codes indicate if image subjects are wearing glasses, hats or notable accessories. Foreground and background colouring is coded as white, black or gray. Gaze direction indicates if the image subject is looking straight ahead into the camera or to the right or left. Brightness level is a description of the overall image tone and is coded as light, medium or dark. By selecting decoy images similar in appearance to target images, an attacker is challenged to guess the password sequence based on gross visible image attributes. Attackers must be physically close to the display to discern finer differences in image details. For future work, colour profiles and brightness levels may be quantified through image spectrum analysis and serve as inputs to a decoy image selection model.

For the graphical password technique to be effective, it is necessary that decoy images be unfamiliar to the usability study subjects. To assess the suitability of our image collection to serve as a source for decoy images we asked volunteers to evaluate the images for familiarity. 16 older (over-60, average age 71.9 years) volunteers and five younger (under-60, average age 37.2 years) volunteers manually reviewed each image. Volunteers assigned image recognition ratings from a 5 point scale. The scale ranged from 1 = do not recognise to 5 = know well.

Figure 6 Image selection tool

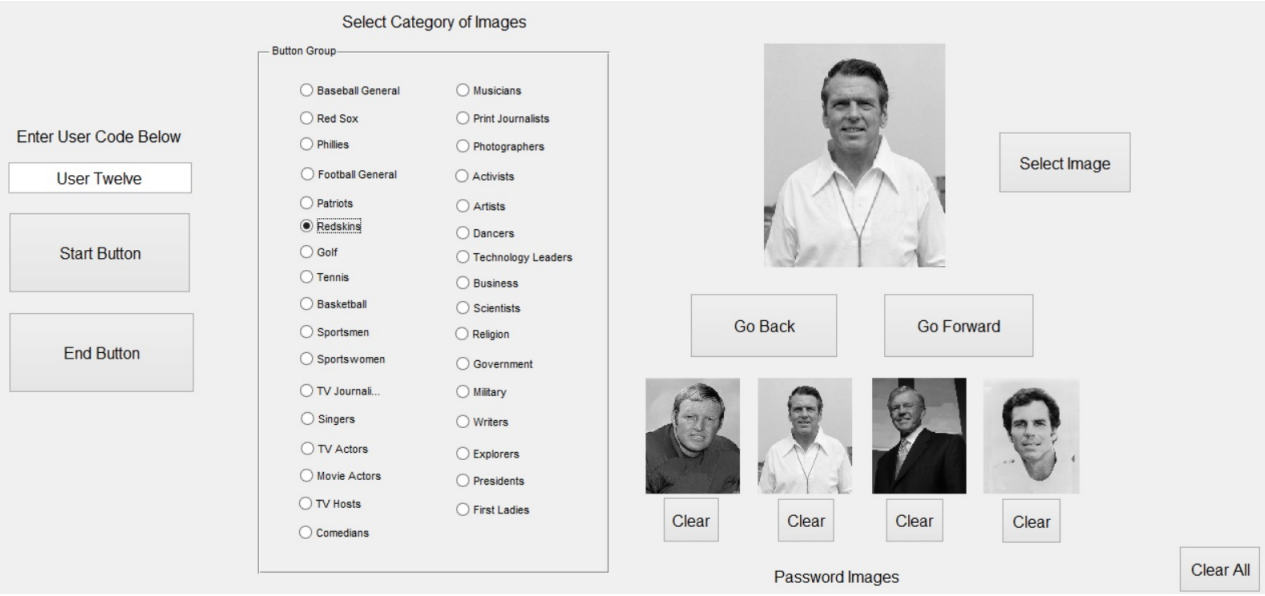


Figure 5 illustrates the results of this review with over-60 users shown in red and the younger group shown in blue. A mean of greater than 50% of images were rated as 'not recognised' by both groups. This provided evidence that the database has enough images to form strong decoy image sets. Figure 5 also illustrates the younger (blue) user rate of non-recognition of images is 19.2% higher than older (red) users, and younger users strongly recognised 14.4% less than older users. This provides evidence that this set of images is more recognisable by our target population of over-60 people.

3.5 Target image selection tool

The MATLAB image selection software tool enables older users to efficiently select personally meaningful images based upon their unique personal interests. As shown in Figure 6, the user interface presents a series of radio buttons enabling selection of a specific category of images based on image subject occupation. Some examples of occupations are actors, football players, golfers, writers, and Presidents. Users could choose their personal image sequences from just one category or choose each image from a separate category. Image categories reflect a wide range of the US cultural interests such as sports, entertainment, journalism, politics, industry, etc. Relying on images from a single category to form a personal sequence increases the risk of an attacker successfully performing a thematic analysis on the images in the display presentation. A security policy to address this risk could require users to select images from more than one occupational category.

Users form their personal target password sequences by browsing among the 33 categories of images. Users cycle through each category by using the 'go back' or 'go forward' buttons shown on the right side of Figure 6. Once the user has selected an image for their personal sequence, that image was displayed at the bottom of the screen in the order chosen. The tool allows users to change selected images if desired. The tool measured level of effort expended by users in choosing their personal images by capturing elapsed time to choose each image and number of images examined by each user. For our study, each user chose three sequences of length four, seven, and ten images. Longer sequences were built upon shorter sequences. As an example, a user's seven image sequence consisted of their four image sequence with three additional images appended. During the usability study, we observed that each user enjoyed the image sequence selection experience, often reminiscing about personal associations as familiar images appeared on the screen. Each user was careful to choose images with strong personal associations.

The decoy images that accompany the target images are chosen based on the user's unfamiliarity with subjects within each decoy image. As discussed in Subsection 3.3, volunteers previously evaluated each image in the database as part of the effort to ensure that a sizeable pool of unrecognised images were available for the study. For the purposes of the usability study described in Section 4, project personnel selected decoy images that were unknown to the user and possessed physical characteristics similar to the user's target images. As an example, a user selecting images of blond women for their personal target password sequence will find that the decoy images are also of blond women. The coding in the image database facilitated the identification of suitable decoy images. If all of the user target images featured subjects wearing light clothing on a dark background shown from the waist up, the coding facilitated the selection of decoy images with similar image composition. During the usability study we observed that volunteers strongly preferred some occupational categories over others. For future work, a production version of the graphical password system could automate the decoy

selection process by having users identify specific occupations with no personal associations, thereby enabling the software tool to automatically draw decoy images from those unfamiliar occupational categories.

4 Usability study design

Our usability study software displayed varying screen configurations of increasing image density during a series of exercises. Each exercise accepted user inputs in the form of touchscreen or mouse image selections, recorded user action elapsed times, and authentication success/failure. The usability configurations ranged from a 3 × 5 display of 15 images to a 7 × 10 display of 70 images. Success was defined as user selection of their target image sequence in the correct order. If the user is unsuccessful at selecting their correct sequence, then the authentication request is considered a failure, the failure is recorded, and the display is refreshed with a re-randomised display of images. The image arrangement re-randomises with each display presentation to include screen refreshes. A casual onlooker will not observe a static placement pattern in the location of any images. Re-randomising the arrangement of images also defends against smudge attacks (Aviv et al., 2010) by ensuring that all portions of the screen will be touched by the user's finger. A security policy invoking a lock-out interval upon three successive failures or screen refreshes provides further defence against brute force attacks.

The cognitive challenge presented is that while longer password sequences result in greater entropy, they add to the user memorisation, recall, and visual search burden. A goal of our work is to measure the time needed to find and select target password images within surrounding decoy images as screen image density increases. The probability of choosing correct images in incorrect order also increases with personal sequence length. Increasing the number of images on the display to achieve higher entropy forces each image to be smaller, and therefore harder to see and discern image details. Several questions arise that our usability study seeks to answer. How do users search the displayed images? Do users consciously adopt specific search patterns looking for their target images? Does peripheral vision aid in speeding up the search for the target images? Do users remember the current locations of subsequent target images encountered 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?

4.1 Procedures

We recruited 19 volunteers, all over the age of 60, from the local community. After signing the consent form, volunteers were provided information about study goals, definition and benefits of strong passwords, and a description of the tasks they would be expected to perform. In contrast to previous work, we met individually with volunteers at convenient off campus locations. This strategy ensured that all volunteers completed the exercise sessions. The most popular locations were in volunteer homes or at local coffee shops. While meeting outside the lab environment was not as time efficient, it had the advantage of putting volunteers at their ease in familiar settings.

Table 2 Usability study comments

User comment	*Comment topic*
It was interesting. Very advantageous for seniors, young people would not recognise images from earlier times.	Overall opinion
I memorised those people before I got home, and I live close by.	Memorisation
It was interesting.	Overall opinion
It was fun.	Overall opinion
I have to think, but it is easy thinking.	Recall
It was easy to quickly recognise my chosen images because I have followed the careers of those individuals all my life.	Recall
It has been a week and I cannot forget my password image sequence.	Recall
I was mentally saying the names in my head.	Memorisation
I can remember my image sequence easily after a week and I cannot normally remember my passwords or the cell phone numbers of friends.	Recall
My finger got ahead of my brain and I touched my third image instead of my second image.	Recall
I can visualise these photographs, I like the people, they are like friends.	Recall
The 70-image display took too long to hunt through and would not be practical in real world application.	Searching for images
I was struck by the sports guys shown on the display, so I chose them.	Thematic analysis during guessing attack

During the initial session, each volunteer utilised the graphical password software tool to browse the database of images and select their target image sequences. Volunteers often shared that they developed a mental story or acronym to aid recall of their image sequences in the correct order. The mental story was formed from the user's previous personal association with the subjects in the images.

Volunteers were contacted at least a week after choosing their images, to perform a series of authentication exercises. In total, 74 sessions, each consisting of 44 individual exercises was held that lasted from an hour to an hour and a half each. Each exercise consisted of two screens. An introductory screen provided brief instructions and allowed the user to indicate when they were ready to proceed to the exercise displayed on the second screen. The purpose of the introductory screen was fourfold: allow the user to control the pace of the exercises, provide a small break to allow the user's short term memory to clear from the previous exercise, provide an opportunity for the user to ask

questions without adversely affecting exercise timing, and clearly delineate the start time of each exercise. Many of the volunteers described themselves as not comfortable or confident using computers. The introductory screen was deliberately intended to foster user confidence by providing the user with control over the pace of exercise activity.

The second screen consisted of the images displayed in a grid pattern similar to Figure 1. An adjacent space was dedicated to hold selected images. Each user chose their image sequence and then selected the 'OK' button to signify exercise completion. Immediate feedback was presented via a success or failure message in a text box. The user then acknowledged the feedback before proceeding to the next screen. If the password sequence was incorrect, the display screen reloaded with a re-randomised image pattern and the user tried again. If the password sequence was correct, the introductory screen for the subsequent exercise appeared. After the last exercise, elapsed times were displayed for the user. This prompted much discussion with volunteers who were curious about the processes running behind the scenes, and the techniques used to interpret timing information. User comments were recorded and specific questions were asked regarding conscious visual search techniques and ease of finding target images. Volunteer comments are listed in Table 2.

It should be noted that throughout this study, participants were permitted to keep personal notes about their chosen password sequences. Personal notes were not permitted to be consulted during volunteer sessions. This is consistent with their current widespread practice of keeping written records of personal text passwords.

The suite of 44 exercises consisted of 35 exercises requiring selection of a personal password image sequence and nine exercises requiring the typing of given text passwords for comparative performance analysis. Personal password sequences varied among lengths of four, seven, and ten images. Display screen image densities ranged from 5×3, 4×4, 5×5, 6×6 to 7×10. Sequences of length four were chosen from all display densities. Sequences of length seven, and ten were chosen only from the 7×10 display densities, as lesser densities did not provide sufficient display space to conceal target images among the decoy images. Volunteers went through the exercises initially using the mouse, and repeated the exercises using the touchscreen to allow analysis of performance differences between the two input modalities.

To investigate volunteer search patterns, we designed eight of the exercises with images deliberately either clustered together or arranged in a linear pattern. User images close together in specific patterns enables analysis of peripheral vision effects on image recognition. Our intuition is that clustering may speed up image recognition and reduce search time.

Five exercises employed 'pseudo-random' image placement patterns to enable analysis of visual seeking patterns constant across all volunteer sessions. All remaining exercises were true random arrangements generated at each exercise invocation. Volunteers were not provided any information about specific pattern arrangements before their exercise sessions.

Varying image sizes and densities permit analysis of the effects of image size on visual search and perception of image details. Our intuition is that smaller images may be more challenging to view by an aging user population, resulting in increased elapsed authentication times and increased recall error rates.

Varying image attributes such as differing or similar foreground and background colours may affect speed of recognition. Our intuition is that some images will prove harder to find, increasing sequence selection times. For future work, a formal definition of an optimal facial image may facilitate image usability, and be a valuable reference in a decoy image selection model.

5 Usability study results

5.1 Recall performance

Nineteen volunteers completed a total of 995 discrete exercises selecting personal password sequences from varying display image densities. Thirty errors were recorded in the 995 exercises for a successful recall rate of 97%, superior to all but two previous works (see Table 3). The recall rates were 98.1% for four-image passwords, 92.5% for seven-image passwords, and 86.6% for ten-image passwords, reflecting the increasing difficulty associated with recalling and selecting longer sequences accurately. Seven of the 30 errors occurred with the touchscreen. The remaining 23 errors occurred using the mouse. The reduced error rate with the touchscreen may be a result of either the ease and immediacy of directly touching the screen with the finger, or a result of the ordering of exercises. Touchscreen exercises always followed mouse exercises. The mouse exercises could have served as memory reinforcement, and equipment and procedural training for the subsequent touchscreen exercises. The sources of errors are shown in Table 4 presented in order of frequency of occurrence.

Errors associated with memory, such as recall, transposition and omission were few. Some volunteers offered comments that they used mental stories or mnemonic sequences to aid recall. One individual chose a chronologically ordered sequence of the US Presidents. Another chose eastern major league baseball team coaches. A third created a mnemonic of the last names of their image subjects.

Errors recorded due to inadvertent equipment issues included pressing too hard and registering a 'double click' on an image without intending to select that image twice in a row. The test software did not allow the volunteer to 'backspace' to correct such errors which were frequently recognised immediately. After disregarding the ten errors originating in equipment issues, the recall rate becomes 97.4%. Our demonstrated recall rate is comparable to the best previous work yet our work also makes the challenging task of password entry easier and fun for older users.

Table 3 Password recall comparison

Password system	*Technique*	*Recall*
Passhint	Art	97.5%
Passhint	Object	97.5%
Graphical password system	Facial images	97%
Passhint–original	Mikon	71%
Passhint–original	Doodle	66%
Passhint–original	Art	55%
Passhint–original	Object	78%
Passhint	Mikon	95%
Passhint	Doodle	95%
BDAS study #1	Drawing	50%
BDAS study #2	Drawing	95%
DAS study #1	Drawing	57%
DAS study #2	Drawing	95%
GridMap one week	Map points	61%
GridMap two weeks	Map points	83%
Pictures	One week	67%
Characters	One week	50%

Table 4 Error categories

Description of error	*Count*
Selected incorrect image due to incorrect recall	8
Selected incorrect image due to equipment issue, e.g., inadvertent double-click or double-touch	10
Transposed valid images	6
Omitted valid images	6
Total errors	30

5.2 Authentication timing

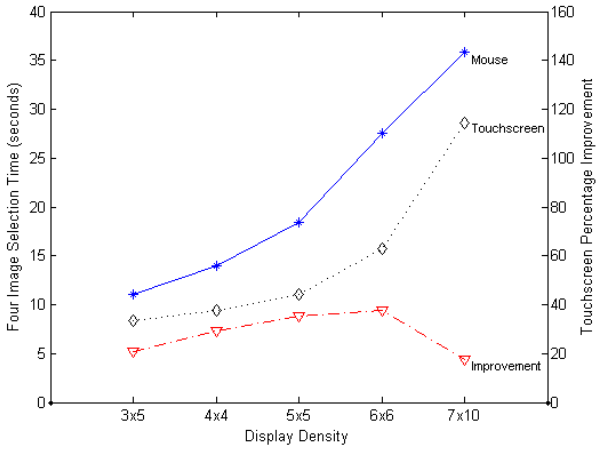
Median authentication times with four-image password sequences at varying screen densities are shown in Figure 7. Blue asterisks indicate results from 324 exercises with the mouse, black diamonds indicate results from 285 touchscreen exercises, and red triangles denote percentage performance improvement of the touchscreen over the mouse. Overall results show median time improvement of 32% using the touchscreen versus the mouse. Median time to select a four-image password image sequence at a low density was about ten seconds. This is less time than many volunteers would take to look up a text password in their personal notes. As screen density increased, time needed to select a four-image sequence increased. Many volunteers commented that searching the 7 × 10 screen displays took too long, ranging from 30 to 35 seconds.

Table 5 compares the time ranges taken to perform a successful authentication versus previous work. The minimum recorded time of our system was 7.4 seconds, better than half of the other systems. The maximum time was 33 seconds, substantially longer than other systems. It must be mentioned that the other systems all conducted usability studies with predominantly young, college age participants. Our study was conducted entirely with participants over the age of 60, some significantly over 60 with minor physical disabilities, some with no ability to touch type.

Table 5 Authentication timing comparison

Password system	*Time range*
Graphical password system – mouse select four from 16	7.4 to 33 seconds
Passhint	13 to 17 seconds
Pictures	13.7 seconds
Characters	10.5 seconds
DAS	4.5 to 7.5 seconds
DAS disappearing stroke	5.3 to 9.6 seconds
DAS line snaking	5.9 to 12.4 seconds

Figure 7 Median authentication timing with constant sequence size and varying input device modality (see online version for colours)



5.3 Individual image selection timing

Figure 8 shows the separate individual image selection timing for the same volunteer exercises whose median time results are shown in Figure 7. At each screen density (with one exception) median time needed to find a subsequent image always decreased. Some volunteers commented that they noted the locations of later images in each sequence during the process of searching for earlier images in their sequences, a form of 'drive by' recognition. Variance in finding and selecting images increased significantly as screen density increased, reflecting the increased effort needed to search among more images.

5.4 User input device modality

Figure 9 shows median authentication timing data for varying user input devices. Volunteers selected varying length personal image sequences from a constant image display density of 70. Volunteers performed 82 mouse (blue bars) and 75 touchscreen exercises (red bars). For all three

personal sequence lengths, touchscreen use improved sequence selection timing.

Figure 8 Individual image selection timing (see online version for colours)

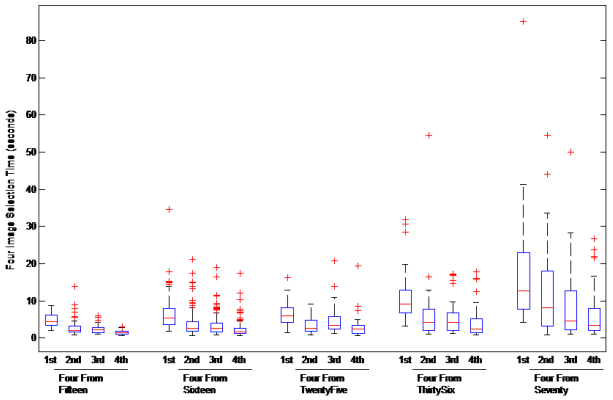
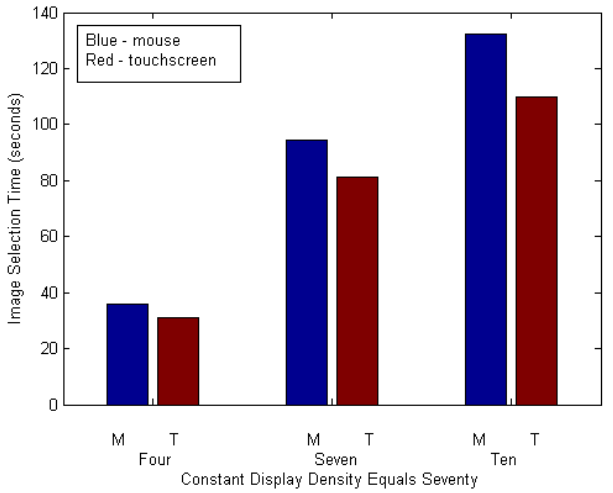


Figure 9 Median authentication timing with varying sequence sizes and varying input device modality (see online version for colours)

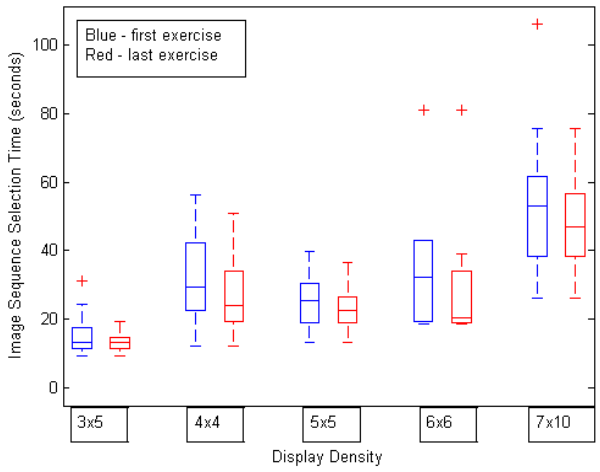


We were interested in understanding the impact of using a touchscreen versus using a mouse. Many older persons have no touchscreen experience, or may have disabilities that limit arm and finger movements needed to reach out and accurately select images. Figures 7 and 9 show that our concerns were unfounded as use of the touchscreen significantly improved median timing by 32%. As shown by the bottom curve in Figure 7, use of the touchscreen increasingly improved performance times as screen image density increased until reaching the densest display, 7 × 10. This suggests that some other factor overcame the advantage provided by the touchscreen. Our volunteers repeatedly commented that the 7 × 10 screen had too many images which took too long to search.

5.5 *Training benefits*

We were interested in understanding any training benefits resulting from repeating exercises at similar sequence lengths and display image densities. Previous work noted the challenge of getting volunteers to return for subsequent exercise sessions in the lab environment (Van Balen and Wang, 2015). The increased effort we made by going to each volunteer made it possible to observe and measure repeated exercise sessions. Through observation we noted that initial exercises were often encumbered by volunteer unfamiliarity with handling the equipment and operating the software. Figure 10 provides a comparison of the median timing differences of first attempts versus last attempts at repeated identical exercises using the mouse. Blue data identifies the first exercise. Red data identifies the last exercise. Results show that the median performance improved, and variance decreased, reflecting user improvement with practice.

Figure 10 Authentication training effects (see online version for colours)



5.6 *Personal image sequence selection timing*

At the start of our study, each volunteer was asked to carefully select personal images important to them. Appropriate selection was key to a successful and efficient password image sequence. Volunteers were instructed to take their time and find meaningful password images. Table 6 provides a comparison of the time taken to decide upon and select each user's personal four image password sequence from the database of 550 images. Many volunteers found the image selection experience enjoyable, relating stories about their personal associations with the subjects in the images. Those users enjoying the selection process took markedly longer to complete their image sequence selection than other users. The faster users selected their image sequences in a comparable timeframe to the Passhint system. Through observation we noted that volunteers often consciously decided on a strategy of selecting images based on occupational category, or era of professional fame before beginning their image selections. The minimum time for a volunteer to select four images was 52.2 seconds, less than the 55 second mean of the Passhint system, showing that our system can be a practical alternative to Passhint for password creation.

Table 6 Password selection timing comparison

Password system	*Selection time range*
Passhint	55 to 58 seconds
Graphical password system – four images	52.2 to 401 seconds

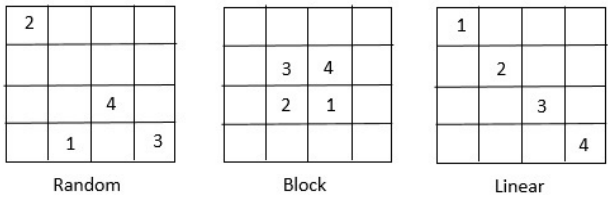
5.7 Guessing study

We conducted a guessability study with a subset of our usability study participants. Our intuition was that attackers of comparable age to our volunteers would have a greater chance of recognising the display images and discerning any themes that might provide hints to actual password images. Five participants were asked to view the 6 × 6 display screens of five other participants and then guess which four images formed the 'victim's' personal password image sequence. Guessers were told only the sex of the password owner and reminded that the password owner was over 60 years old. None of the guessers were successful at guessing a correct sequence. Guessers did choose at least one of the four images making up each sequence, ineffective for a successful attack. The best guesser chose three of the four correct images, in incorrect order, by performing a thematic analysis on the displayed images. A security policy requiring user selection of target images from multiple categories would thwart this type of adversary analysis.

5.8 Image pattern effects

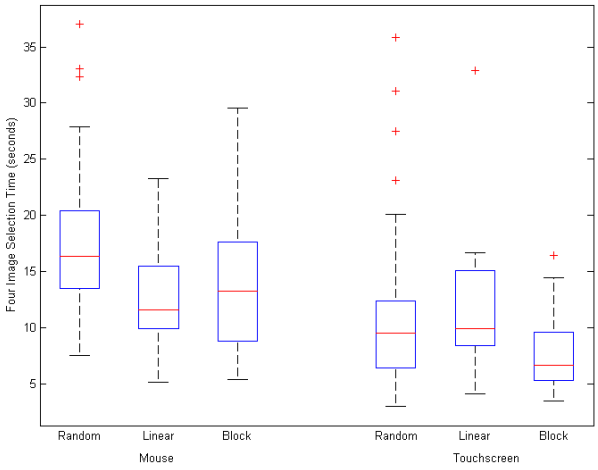
We were interested in learning if peripheral vision could play a role in target image recognition. Some exercises placed target images in deliberate patterns. As shown in Figure 11, a random arrangement could result in the placement of images anywhere, whereas a block pattern puts the four target images immediately adjacent to each other. A linear pattern places the four images in a line on the display. The results for 19 volunteers selecting four images from a display of 25 images with the mouse and the touchscreen are shown in Figure 12. With both mouse and touchscreen, the block pattern resulted in improved median timing performance. The linear arrangement achieved comparable median timing performance to the random pattern with the touchscreen and improved median performance with the mouse. This provides evidence that users recognise nearby target images more quickly.

Figure 11 Image arrangement examples



We were interested in learning how our volunteers approached performing our exercises given that this was a completely new technique. After each exercise session, volunteers were asked about any consciously adopted image search strategies. Some volunteers stated they just allowed their eye to generally roam about the screen display with no conscious direction. Other volunteers adopted 'search left to right by row' or 'search up and down by column' strategies.

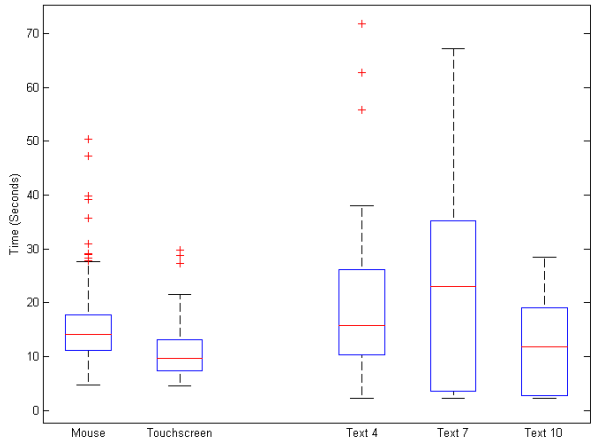
Figure 12 Timing effects of varying image arrangement patterns (see online version for colours)



5.9 Text password comparison

We were interested in measuring the elapsed time differences between entering a graphical password sequence and typing a text password. Figure 13, from left to right, illustrates the median timing to enter a four-image password sequence with the mouse, then the touchscreen, typing a four character strong text password, then a seven character strong text password and finally a ten character strong text password. Volunteers were asked to mentally create each strong text password for themselves. They were timed solely on typing of the text. We observed our volunteers putting significant effort into typing even the short four-character text password. Often they were challenged by finding unfamiliar keyboard symbols or they were very slow typists. The median time to enter a four-image sequence with the mouse was 14.2 seconds, less than the 15.7 second median time needed to type a four character strong text password. Entering the four-image sequence with the touchscreen was faster yet with a median time of 9.9 seconds, a 37% improvement over text entry. The wider variance shown with the text entry may be attributable to the wide range of typing skills demonstrated by our volunteers. We further observed that our over-60 volunteers enjoyed selecting the image sequences and felt that typing a strong text password was not enjoyable because of the effort needed to find correct keys and unusual symbol characters.

Figure 13 Timing comparison between image and text-based password sequences (see online version for colours)



6 Graphical passwords on smartphones

Older persons have significantly lagged younger generations in adopting modern technology (Pew Research Center, 2014) but are now quickly embracing smartphones. 64% of those 65 and older owned smartphones in 2015, reflecting an 8% increase in a single year (Pew Research Center, 2015). Since smartphones are designed as inherently touch-based devices, and users spend up to 9% of their smartphone-engaged time unlocking their devices (Harbach et al., 2014), our graphical password technique would seem appropriate for the smartphone platform. As a group, older persons have visual, mobility, and orthopaedic disabilities which limit hand or finger use, lengthen visual search processes, adversely affect the ability to perceive small icons, and compromise their ability to move arms, hands and 'fingers smoothly and continuously' (Czaja and Lee, 2012). These physical characteristics can render some current smartphone unlock mechanisms difficult and frustrating to use. Our graphical password technique can turn unlocking into an engaging and fun experience, key to maintaining a positive user experience (Calvo and Peters, 2014) that discourages users from disabling security unlock mechanisms.

With a view toward widespread smartphone adoption by older persons we compared our graphical password technique with many common 'phone lock' mechanisms in use today. Our survey methodology was to examine the online descriptions of the first 25 'phone lock' apps found in the Amazon Android (Amazon App Store, 2016), Apple iPhone (Apple iTunes iPhone App Store, 2016) and Google Play Android (Google Play Android App Store, 2016) app stores. The most common 'phone lock' apps included:

- Slider – slide finger along indicated path to unlock smartphone.
- Zipper – slide finger along image of a zipper to unlock smartphone.
- Numeric PIN – select four-digit (or higher) PIN from numeric keyboard display.
- Alphanumeric password – select text password from ten-digit keyboard display.
- Pattern swipe – swipe finger across display pattern connecting pre-entered symbols.
- Voice phrase match – utter a passphrase into the smartphone microphone.
- Drawing match – swipe finger across display creating a drawing that must match pre-entered drawing.
- Smartphone shaking – hold an unlocked phone against a locked phone and shake them together to pass the unlocked state (Findling et al., 2014).
- Fingerprint scanner (fake) – hold finger to target to unlock phone.
- Fingerprint scanner (real) – hold finger to target for scanning and match to pre-entered fingerprint scan.

Table 7 Smartphone 'phone lock' technique comparison

Technique	*S*	*C*	*DR*	*A*	*SR*	*P*	*Note*
Graphical password system	H	H	H	H	H	H	Assuming choose four images from 16 images, randomised display.
Slider	H	N	N	H	N	N	Anyone with physical access may unlock the smartphone.
Zipper	H	N	N	H	N	N	Anyone with physical access may unlock the smartphone.
Numeric PIN	L	H	H	L	M	N	Assuming four (or greater) digit PIN.
Alphanumeric password	L	H	H	L	M	M	Assuming four (or greater) alphanumeric character password.

Notes: S – Physical size.
C – Complexity.
DR – Data replacement.
A – Accessibility.
SR – Smudge resistance.
P – Personalisation.

Table 7 Smartphone 'phone lock' technique comparison (continued)

Technique	*S*	*C*	*DR*	*A*	*SR*	*P*	*Note*
Pattern swipe	M	H	H	L	L	L	Assuming four (or greater) dot swipe pattern on a nine (or greater) dot grid.
Voice phrase match	L	H	H	M	H	H	Physical size is not relevant to the voice recording quality. Button touches needed to start voice recording.
Drawing match	H	H	H	L	H	H	Challenging for shaky hands to recreate line drawings consistently.
Smartphone shaking	L	H	N	L	H	N	Physical size is not relevant to the quality of the shake pattern reproduction. Button touches needed to start shake measurement.
Fingerprint scanner – fake	H	N	N	H	N	N	Also known as 'prank scanner.' Simple touch and hold of finger on large target image Anyone with physical access may unlock the smartphone.
Fingerprint scanner – real	L	H	L	H	H	H	Limited current availability for Samsung, Apple iTouch and Android 6+ smartphones.

Notes: S – Physical size.
C – Complexity.
DR – Data replacement.
A – Accessibility.
SR – Smudge resistance.
P – Personalisation.

Our survey analysis considered smartphone physical icon size, unlock technique entropy, ability to replace compromised unlock code, accessibility, touchscreen smudge-resistance, and capacity for personalisation. Our results are shown in Table 7. Each technique was rated using a scale of none, (N), low (L), medium (M) or high (H).

Physical size of finger target icons displayed on the smartphone touchscreen is very important. As described by Fitt's Law, the time taken to touch a target is a function of icon size and distance (Dix et al., 2004; Rogers et al., 2011). Larger finger targets are easier to see and touch. We reviewed the complexity of each technique in order to gauge resistance to brute force attacks. Many of the apps devolved to simple slider switches which anyone with physical access to the smartphone could unlock the device. More complex techniques such as PIN, pattern, and password entry required users to locate and touch very small target characters or icons. Users with vision impairments would benefit from enlarging portions of the screen to make viewing and touching easier. Attempts to enlarge the on-screen keyboard displays were unsuccessful. Any unlock apps providing screen enlargement capability also add significant task functional complexity as measured through goals, operators, methods, and selection (GOMS) analysis of enlargement and scroll motions necessary for successful unlocking (Card et al., 1983). As an example, a user able to directly view and select an icon would be able to successfully select the desired icon in one step. A user needing to enlarge a section of the screen would need to select the screen area to be enlarged, make a zoom gesture and then select the desired icon, a minimum of three steps.

Unlock codes may become compromised and require replacement. In such cases PINs, passwords, and the graphical password technique enable easy replacement of the unlock coding. Other techniques such as real fingerprint scans or facial photo matching are limited to the user's ten fingerprints or single facial image. Once available biometric data is exhausted, the user must seek an alternative unlock technique. Accessibility in design enables those with disabilities to successfully utilise the unlock technique. Unlocks requiring matching of line drawings are challenging for those with shaky hands drawing on the touchscreen. Both the hand holding the smartphone and the hand with the drawing finger add variation to the executed drawing. Smudge patterns are created on touchscreens executing repeated swipe patterns on static symbol grids. Lastly, unlock techniques providing some user personalisation features assist with unlock pattern recall.

As shown in Table 7, our graphical password technique, in a proposed 3 × 3 or 4 × 4 configuration, provides large target size, good complexity, smudge-resistance, and a high degree of personalisation. We measured a ten digit keypad displayed on a Droid Maxx running Android 4.4.4. Each character measured 0.25 by 0.25 inches. The same screen with a 4 × 4 graphical password presentation provides 0.6 by 0.6 inches for each image, more than twice the target space of the ten-digit keypad. The large target size

facilitates users with vision, finger and arm mobility impairments. As older users more widely adopt smartphones, our graphical password technique will continue to be beneficial.

7 Conclusions

The entry of traditional text passwords is a common everyday user activity, but some portions of the user population find them difficult to use. Our interview-style study of older computer users revealed challenges with the creation, recall, and management of their strong text passwords. By basing our graphical password system design on the selection of familiar facial images from the past personal history of the individual older user, we have created a naturally easy-to-recall authentication mechanism. Through use of mouse or touchscreen image selection, we have created a faster password entry mechanism that facilitates the manually impaired user. The entropy of our technique is superior to equal length text passwords. Our usability study with 19 volunteers demonstrated a 97% recall success rate, faster password selection than many previous graphical password systems, and faster performance than traditional text password entry with a keyboard.

References

Amazon App Store (2016) *Amazon Appstore for Android* [online] https://www.amazon.com/mobile-apps/b/ref=topnav_storetab_mas?ie=UTF8&node=2350149011 (accessed 15 August 2016).

Apple iTunes iPhone App Store (2016) *Apple iTunes iPhone App Store* [online] https://itunes.apple.com/us/genre/ios/id36?mt=8 (accessed 14 September 2016).

Aviv, A., Gibson, K., Mossop, E., Blaze, M. and Smith, J. (2010) 'Smudge attacks on smartphone touch screens', in *USENIX 2010: Proceedings of the 4th USENIX Conference on Offensive Technologies*, USA, USENIX Assn, Article Nos. 1–7.

Biddle, R., Chiasson, S. and Van Oorschot, P.C. (2012) 'Graphical passwords: learning from the first twelve years', *ACM Computing Surveys*, August, Vol. 44, No. 4, pp.1–41.

Bonneau, J. and Preibusch, S. (2010) 'The password thicket: technical and market failures in human authentication on the web', in *WEIS 2010: Proceedings of the 9th Workshop on the Economics of Information Security*, USA.

Brostoff, S. and Sasse, M. (2000) 'Are passfaces more usable than passwords? A field trial investigation', *People and Computers XIV-Usability or Else!*, pp.405–424, Springer, London.

Calvo, R. and Peters, D. (2014) *Positive Computing: Technology for Well-Being and Human Potential*, The MIT Press, USA.

Card, S., Moran, T. and Newell A. (1983) *The Psychology of Human-Computer Interaction*, Lawrence Erlbaum Associates, Hillsdale, New Jersey, USA.

Carter, N., Novak, E., Li, C., Qin, Z. and Li, Q. (2015) 'Graphical passwords for older computer users', in *UIST 2015: Doctoral Symposium at 28th ACM User Interface Software and Technology Symposium*, USA.

Chowdhury, S., Poet, R. and Mackenzie, L. (2014) 'Passhint: memorable and secure authentication', in *CHI 2014: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Canada, pp.2917–2926.

Czaja, S. and Lee, C. (2012) 'Older adults and information technology opportunities and challenges', in *The Human-Computer Interaction Handbook*, pp.825–840, Taylor & Francis Group, LLC.

Dix, A., Finlay, J., Abowd, G. and Beale, R. (2004) *Human-Computer Interaction*, 3rd ed., Pearson Education Limited, Harlow, England.

Dunphy, P. and Yan, J. (2007) 'Do background images improve 'draw a secret' graphical passwords?', in *CCS 2007: Proceedings of the 14th ACM conference on Computer and Communications Security*, USA, pp.36–47.

Farzin, F., Hou, C. and Norcia, A.M. (2012) 'Piecing it together: infants' neural responses to face and object structure', in *Journal of Vision*, Vol. 12, No. 13, pp.1–14.

Findlater, L., Froehlich, J., Fattal, K., Wobbrock, J. and Dastyar, T. (2013) 'Age-related differences in performance with touchscreens compared to traditional mouse input', in *CHI 2013: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, France, pp.343–346.

Findling, R., Hintze, D., Muaaz, M. and Mayrhofer, R. (2014) 'ShakeUnlock: securely unlock mobile devices by shaking them together', in *MOMM 2014: Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia*, Taiwan, pp.165–174.

Florencio, D. and Herley, C. (2007) 'A large-scale study of web password habits', in *WWW 2007: Proceedings of the 16th International Conference on World Wide Web 2007*, Canada, pp.657–666.

Gauthier, I., Skudlarski, P., Gore, J. and Anderson, A. (2000) 'Expertise for cars and birds recruits brain areas involved in face recognition', *Nature Neuroscience*, Vol. 3, No. 2., pp.191–197.

Google Play Android App Store (2016) *Google Play Android App Store* [online] https://play.google.com/store/apps?hl=en (accessed 13 September 2016).

Hao, Z. and Li, Q. (2016) 'Towards user re-authentication on mobile devices via on-screen keyboard', in *HOTWEB 2016: Fourth IEEE Workshop on Hot Topics in Web Systems and Technologies*, USA, pp.78–83.

Harbach, M., Von Zezschwitz, E., Fichter, A., De Luca, A. and Smith, M. (2014) 'It's a hard lock life: a field study of smartphone (un)locking', in *SOUPS 2014: Tenth Symposium on Usable Privacy and Security*, USA, pp.213–230.

Haris, N., Majid, R., Abdullah, N. and Osman, R. (2014) 'The role of social media in supporting elderly quality daily life', in *i-USEr 2014: 3rd International Conference on User Science and Engineering*, Malaysia, pp.253–257.

Harmon, K. (2009) *Can You Lose Your Fingerprints?* [online] https://www.scientificamerican.com/article/lose-your-fingerprints/ (accessed 21 December 2017).

Kanwisher, N. (2010) 'Functional specificity in the human brain: a window into the functional architecture of the mind', in *PNAS 2010: Proceedings of the National Academy of Sciences of the United States of America*, Vol. 107, No. 25, pp.11163–11170.

Komanduri, S. and Hutchings, D. (2008) 'Order and entropy in picture passwords', in *GI 2008: Proceedings of Graphics Interface*, pp.115–122.

Lindley, S., Harper, R. and Sellen, A. (2008) 'Designing for elders: exploring the complexity of relationships in later life', in *BCS-HCI: Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction*, UK, Vol. 1, pp.77–86.

Liu, J., Harris, A. and Kanwisher, N. (2010) 'Perception of face parts and face configurations: an fMRI study', *Journal of Cognitive Neuroscience*, Vol. 22, No. 1, pp.203–211.

Nicholson, J., Coventry, L. and Briggs, P. (2013) 'Age-related performance issues for PIN and face-based authentication systems', in *CHI 2013: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, France, pp.323–332.

Passfaces Corporation (2015) *The Science Behind Passfaces* http://www.passfaces.com/published/The%20Science%20Behind%20Passfaces.pdf. (accessed April 2015).

Password Strength (2016) *Password Strength* [online] https://en.wikipedia.org/wiki/Password_strength (accessed 26 April 2016).

Pew Research Center (2013) *Who's Not Online and Why* http://pewinternet.org/Reports/2013/Non-internet-users.aspx (accessed 16 May 2017).

Pew Research Center (2014) *Older Adults and Technology Use* http://www.pewinternet.org/2014/04/03/older-adults-and-technology-use/ (accessed 16 May 2017).

Pew Research Center (2015) *U.S. Smartphone Use in 2015* http://www.pewinternet.org/files/2015/03/PI_Smartphones_0401151.pdf (accessed 16 May 2017).

Rogers, Y., Sharp, H. and Preece, J. (2011) *Interaction Design*, 4th ed., John Wiley & Sons, Ltd, West Sussex, UK.

United States Census Bureau (2014) *An Aging Nation: The Older Population in the United States*, P25-1140, USA.

Van Balen, N. and Wang, H. (2015) 'GridMap: enhanced security in cued-recall graphical passwords', in *SECURECOMM 2015: International Conference on Security and Privacy in Communications Networks*, Vol. 152, pp.75–94, Springer, USA.

Waycott, J., Vetere, F., Pedall, S., Kulik, L., Ozanne, E., Gruner, A. and Downs, J. (2013) 'Older adults as digital content producers', in CHI *2013: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, France, pp.39–48.

Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A. and Memon, N. (2005) 'PassPoints: design and longitudinal evaluation of a graphical password system', *International Journal of Human-Computer Studies*, Vol. 63, Nos. 1–2, pp.102–127.

Yin, Y., Li, Q., Xie, L., Yi, S., Novak, E. and Lu, S. (2016) 'CamK: a camera-based keyboard for small mobile devices', in *INFOCOM 2016: 35th Annual IEEE International Conference on Computer Communications*, USA.