

A Preliminary Experiment on Grid Densities for Visual Password Formats

Yesaya Tommy Paulus
Department of Information Systems, STMIK Dipanegara

Herlina
Department of Electrical Engineering and Information Technology, Gadjah Mada University

Khairu Zeta Leni
Faculty of Visual Art and Design, Bandung Institute of Technology

Hiramatsu, Chihiro
Faculty of Design, Department of Human Science, Kyushu University

他

<https://hdl.handle.net/2324/7449719>

出版情報 : pp.122-127, 2018-11-01. IEEE

バージョン :

権利関係 : © 2018 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.



A Preliminary Experiment on Grid Densities for Visual Password Formats

Yesaya Tommy Paulus¹, Herlina², Khairu Zeta Leni³, Chihiro Hiramatsu⁴, Gerard B. Remijn⁵

^{1,4,5} Kyushu University
Faculty of Design, Department of Human Science
Fukuoka, Japan

¹STMIK Dipanegara
Department of Information Systems
Makassar, Indonesia

²Gadjah Mada University
Department of Electrical Engineering and Information Technology
Yogyakarta, Indonesia

³Bandung Institute of Technology
Faculty of Visual Art and Design
Bandung, Indonesia

Abstract—Visual passwords are passwords made by selecting a sequence of objects on a screen, such as symbols, pictures, or patterns, either by manual input or eye-gaze-based input. Visual passwords can be useful alternatives to alphanumeric passwords, particularly for authentication on devices in semi-private or public spaces (e.g., on ATMs, laptops, smartphones, or car dashboards). The grid is an essential factor in the use of a visual password, because it can act as a guide for the position of an object and its identification. In this study, we obtained user judgments of 16 different grid densities for three visual password formats. The grid densities were in between 2×2 to 7×7 cells (columns $\times$ rows). The participants were asked to judge how easy to use and how safe they thought the grid densities would be, if they would use it for password authentication with eye tracking in a public setting. The results showed that for each visual password format some grid densities were thought to be relatively difficult to use (e.g., a 7×7 grid) or potentially unsafe (e.g., a 2×2 grid). Following this, the password registration time was measured for 16 grid densities (from 3×3 to 6×6 cells). The participants were asked to memorize and register a visual password (short or long) using actual eye tracking. The preliminary results show that password registration time increased when the number of grid cells increased and that the password format might influence registration as well.

Keywords—visual password; visual memory; eye tracking; eye gaze; grid density; grid size

I. INTRODUCTION

A visual password is a sequence of objects consisting of symbols, pictures, or patterns that allow a user to authenticate him/herself on a system (e.g., an Automated Teller Machine (ATM), a smartphone, or a laptop). In general, visual password systems can be clustered into three distinct categories: locimetric, drawmetric, and cognometric systems [1-2]. The visual objects in these three systems can be selected by means of various input techniques, e.g., by mouse, keyboard, finger touch, stylus, or by eye tracking.

Locimetric systems, based on the so-called loci method [3], require the user to select some focus points on an image

as a password. In “PassPoints,” the user has to select five different points on an image by using a mouse to perform authentication [4]. Cued Click-Point (CCP) is another example of a locimetric system in which the user has to select one point on a sequence of images using a mouse [5]. One variant of CCP is Cued Gaze-Points (CGP), which requires the user to select points on a sequence of images using eye tracking, while holding the spacebar on a keyboard for a few seconds to record his/her gaze [6]. In locimetric systems, a grid for displaying images is not strictly used, but grid squares (e.g., 14×14 pixels, or 20×20 pixels) are used as tolerance areas for performing a click (or a gaze) on an image.

Drawmetric systems enable visual authentication based on drawing or writing on a grid. A first example is SUIS (Signature-Based User Identification System), in which the user has to draw his/her signature on a grid as a visual password, and then digitize and store it for user identification [7]. The second example is “EyePassShapes,” which combines two authentication systems, the “PassShapes” [8] and the “EyePIN” [9]. Here, the user has to draw strokes on two different grid sizes of 100 and 150 pixels, using eye tracking and a keyboard sequentially. Another example of a drawmetric system is “Draw a Secret (DAS),” in which the user has to draw a password on a grid of 5×5 cells on a PDA (personal digital assistant) using a stylus or mouse [10]. Research on visual passwords drawn with a stylus on a PDA showed that users had no problem drawing visual passwords in five different grids, i.e., grids of 15×20 , 30×40 , 48×64 , 60×80 , and 120×160 pixels [11]. However, since this research was performed with grids expressed in pixel numbers and without eye tracking, it is difficult to estimate what grid densities are potentially suitable for the eye-gaze-based drawmetric system.

Lastly, cognometric systems are visual password systems that take human cognitive abilities into account, such as the ability to remember and recognize faces, scenes or visual objects. These systems require the user to search and select symbols, pictures, or patterns as his/her password during an authentication process, in which all visual objects are placed

within a grid. “Visual Identification Protocol (VIP)” is a visual password system in which objects are selected by using a mouse in two different grid densities, i.e., 3×4 and 4×4 cells [1]. In “Déjà Vu,” the user uses a mouse to select and memorize a set of abstract images displayed in a 5×5 grid [12]. Another example is “PassFaces” which is based on recognition of a target face presented in a 3×3 grid surrounded by eight distractors [13]. One study tested “PassFaces,” with eye-gaze-based authentication. The authors reported that eye tracking could potentially be applied as a suitable option for authentication in a system, e.g., an ATM [14]. Eye tracking was also used in a series of studies on “ImagePass.” This system uses single-object images as a visual password, in which the user has to click on a series of images presented in a 4×4 grid [15]. However, in this system, eye tracking was used just as an analysis method – not as input method – in order to analyze gender differences and to consider the cognitive processes in visual password selection.

Many of the visual password systems described above thus employ a kind of grid. However, the grid density (i.e., the number of cells) varies widely and research on the usability of grid densities has not been performed systematically. Just one study suggested that increasing the grid density produces a stronger password, because many pieces of information (i.e., visual objects) can be selected by the users. Increasing the grid density, however, could affect password memorization too [16]. In order to identify which grid densities potentially are suitable with eye tracking, it is important to obtain judgments related to how easy to use and how safe the user thinks each grid density would be, when authenticating a password on the grid using eye tracking. Here we report an evaluation of a variety of grid densities for visual passwords, ranging from 2×2 to 7×7 cells (see Fig. 1).

In Experiment I, the participants were asked to sit in front of a computer and to create an ideal visual password by selecting objects on the display using manual input with a mouse, thus without eye tracking. The ideal visual password was an imaginary password that consisted of four to eight objects (alphanumeric characters, dots, or visual icons). Following this, the participants had to give assessments for three visual password formats on grid densities in between 2×2 to 7×7 cells, in relation to how easily and safely they thought each grid density could be used for making a visual password in a real situation with eye tracking. We obtained the participant judgments by using a 7-point rating scale. The present study was meant to reduce the range of possible grid densities for a follow-up experiment with actual eye tracking.

II. EXPERIMENT I

A. Method

1. Participants

Twenty-seven participants (11 males, 16 females) with normal or corrected-to-normal vision participated in this experiment on a voluntary basis. They were 21-47 years of age (mean = 27.01 years, SD = ± 6.53 years). Twenty-four participants were Asian (Japanese, Chinese, Malaysian, and Indonesian), 2 participants were Caucasian, and 1 participant was Latino/Hispanic. All participants gave informed consent as to their participation after the purpose and procedure of the experiment was explained to them.

2. Apparatus

The interface for the grids was presented on a monitor (Lenovo ThinkVision, 20-in, refresh rate of 60 Hz) with a resolution of 1600×1200 pixels. Each grid was set against a gray background (3.64 ± 0.09 cd/m²). The monitor was placed on the desk with a height of 70 cm from the floor and at a viewing distance of approximately 62 cm where the participant was sat. It is a suitable viewing distance for registration on eye tracking devices [17].

The interface for the questions about the grid was presented on a Laptop (Lenovo Z40, 15-in) with a resolution of 1366×768 pixels and a refresh rate of 60 Hz. This laptop was placed below the monitor. The interface was programmed in Visual Studio C# (2015), and the data gathered from the participants were saved in a MySQL database. The experiment was performed under a room lighting condition at an illuminance of 106.42 ± 11.36 lux, as measured using a TOPCON Illuminance Spectro Meter IM-1000 at the location where the participant was seated. Stimulus luminance on the monitor was measured using a TOPCON Luminance Meter BM-9. The luminance and illuminance values used here were similar to those used with the same experimental set-up [17-18]. The measurements were performed ten minutes before the start of the experiment.

3. Stimuli

For three visual password formats, sixteen different grid densities were made with 2×2 to 7×7 cells (columns $\times$ rows, see Fig. 1). The first format was an alphanumeric visual password format. For the alphanumeric format, numbers, letters, and special characters were presented on each grid. One cell of a grid was always reserved for a ‘Clr’ (Clear) key. This key could be used by the participant to clear his/her input. In the case of a grid density of four cells, i.e., a 2×2 grid, the digits 1, 2, 3, and ‘Clr’ were presented starting from the top left to the bottom right cell. If the grid density exceeded ten cells, letters (in alphabetical order) and special characters were added to the numbers. For example, on a 7×7 grid with 49 cells, the numbers 0 to 9, the letters A to Z, and the special characters -, +, *, /, =, :, ;, ?, !, (, \,), along with ‘Clr’ were presented starting from the top left to the bottom right cell. The alphanumeric characters in the grid cells were black with a luminance of 0.73 ± 0.21 cd/m², on a white background (8.45 ± 0.65 cd/m²).

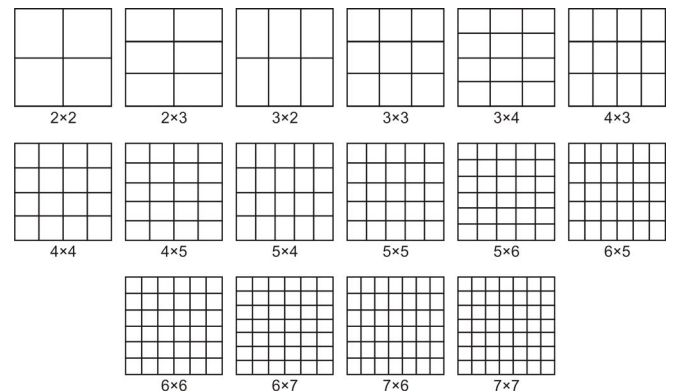


Fig. 1. Sixteen different grid densities for three visual password formats were used in Experiment I.

The second format was a pattern format. The pattern format consisted of dots, which could be selected by the

participant to create a visual pattern as a password. The dots were black ($0.80 \pm 0.26 \text{ cd/m}^2$) and white ($8.12 \pm 0.92 \text{ cd/m}^2$). That is, a white dot with a radius of 47 pixels was placed in the middle of a black dot with a radius of 128 pixels, and both dots were presented together as a key.

The third format was a picture format, which consisted of visual icons in a fixed order on a grid, with the number of icons depending on the grid density. Similar to the alphanumeric format, a 'Clr' key with the same function occupied one cell of a grid in this format. The visual objects were a single picture in gray with a luminance of $3.10 \pm 1.04 \text{ cd/m}^2$, against a white background ($8.29 \pm 0.94 \text{ cd/m}^2$).

Each key of a password (i.e., alphanumeric character, dot, or visual icon) was put in a grid cell with a size of 128×128 pixels, which was 3.44° in visual angle and every pixel within a key was 0.027° in visual angle. A stimulus pane was made with a size of 1600×1200 pixels for each grid density for each of the three visual password formats. A text box was displayed on the upper part of the pane (1600×125 pixels), while a grid was displayed for a given password format on the main part of the pane, with a size of 1600×1075 pixels (see Fig. 2).

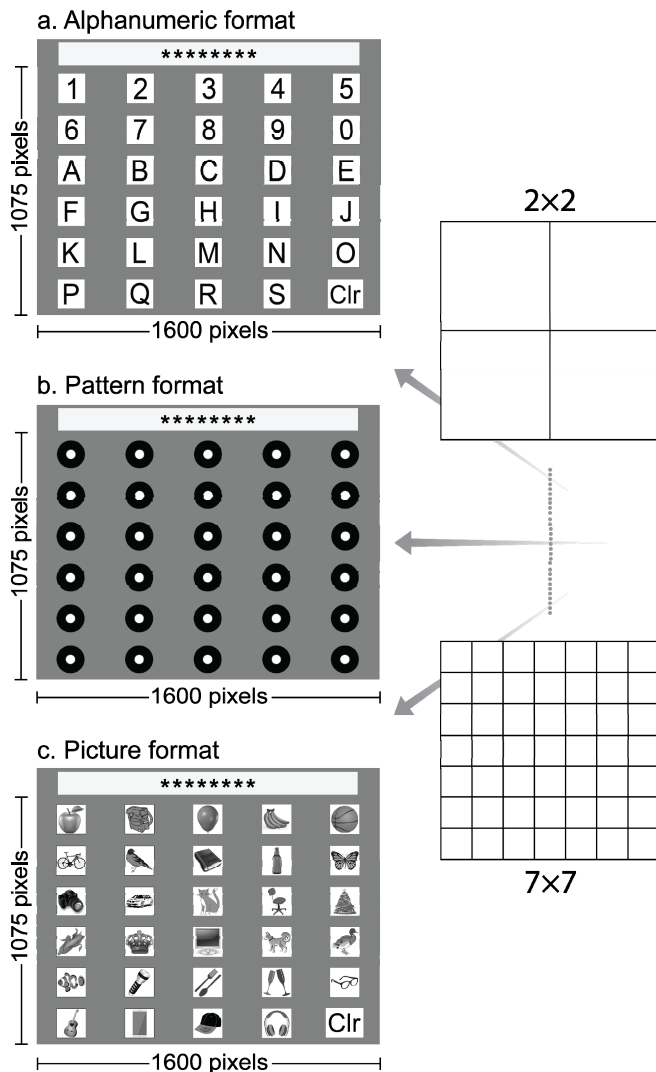


Fig. 2. Example of stimuli. The three visual password formats [a. The alphanumeric format with a grid of 5×6 cells (columns $\times$ rows), b. The pattern format with a grid of 5×6 cells (columns $\times$ rows), and c. The picture format with a grid of 5×6 cells (columns $\times$ rows)] were presented in each of the 16 different grids depicted in Fig. 1.

When the participant selected a key (an alphanumeric character, a dot, or a visual icon), an asterisk would be displayed on the text box above the grid, and a chime sound would be played (1538 ms, 64.61 Hz – 3733 Hz), to indicate that the participant had made a selection.

4. Procedure

The participant was asked to sit in front of a desk on which the laptop and monitor were placed. The participant was asked to make an “ideal” password for each grid density on three visual password formats. Each grid was displayed on the monitor in a random order when the participant made a password. He/she was instructed never to create a real password used in his/her daily life. Furthermore, although each participant was using a mouse to make passwords, he/she was asked to imagine using the eye-tracking system during the experiment. The participant was instructed that the password should be an imagined password, with a minimum length of four and a maximum length of eight objects. For each format, the imagined password was created by clicking objects on the monitor using a mouse. For the alphanumeric format, the participant had to select a sequence of characters such as numbers, letters or special characters, as his/her password. For the pattern format, he/she had to draw an assembly of dots as a password, while for the picture format, the participant had to select icons/images as his/her password.

After making a password, the participant was asked whether he/she thought that a particular grid density would be easy to use for making a visual password, on a scale between 1 (not easy) and 7 (very easy). Next, the participant was instructed to evaluate the potential safety of the grid for visual password input with eye tracking, between 1 (not safe) and 7 (very safe). The participant was not given any instructions as regards the meaning of “easy to use” or “potential safety” of the visual password format and grid. These evaluations were performed with a program on the laptop. Each evaluation for each grid was saved in a database.

In order to get used to the program interface, the participant was asked to run a practice program before starting the actual experiment. In the practice program, the participant had to practice making a password twice for each format, on a grid randomly chosen from the 16 grids. After that, the participant made the evaluations. After practice, the participant performed the experiment with counterbalance in the order of the three visual passwords. That is, nine participants first made passwords in the alphanumeric format, then in the pattern format, and finally in the picture format, for each of the grids. Another nine participants started with the pattern format, followed by the picture format, and ending with the alphanumeric format. The remaining nine participants started with the picture format and ended with the pattern format. The experiment for all formats took about 60 minutes for each participant. The procedures of the experiment were approved by the Ethical Committee of the Faculty of Design, Kyushu University.

B. Results

Fig. 3 shows the participant judgments ($n=27$) on whether a grid was potentially easy and safe to use for the alphanumeric visual password format. As the number of grid cells increased, the participants judged the grid as increasingly less easy to use [black circles, ranging from the

2×2 grid (6.30 ± 0.53), to the 7×7 grid (3.52 ± 0.84]. Contrary, as the number of grid cells increased, the participants thought that in an imagined situation using eye tracking, making a visual password would become safer [white circles, ranging from the 2×2 grid (1.26 ± 0.27), to the 7×7 grid (6.44 ± 0.37)].

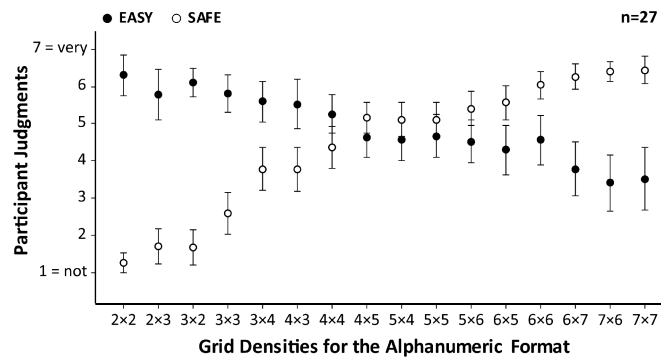


Fig. 3. The participant judgments (n=27) on whether a grid was potentially easy (black circles) and safe (white circles) to use for the alphanumeric visual password format. Error bars indicate $\pm$ 95% confidence intervals around the means.

Table I shows the 95% confidence intervals (CIs) around the means (n=27) of the “easy” and “safe” judgments for the alphanumeric visual password format. In order to get an indication of which grid density would be useful for this format, we compared the interval ranges with the midpoint of the rating scale, i.e., “4”. Regarding the “easy to use” judgments, the means and the 95% CIs for the 2×2, 2×3, 3×2, 3×3, 3×4, 4×3, 4×4, 4×5, and 5×5 grids exceeded the scale midpoint, suggesting that these grid densities tended to be easy to use with the alphanumeric format. For the “potentially safe” judgments, the means and the 95% CIs for the 4×5, 5×4, 5×5, 5×6, 6×5, 6×6, 6×7, 7×6, and 7×7, grids were greater than the scale midpoint, showing that these grid densities were judged as potentially safe for the alphanumeric format.

TABLE I. THE MEANS AND THE 95% CONFIDENCE INTERVALS OF THE EASY AND SAFE JUDGMENTS FOR EACH GRID DENSITY FOR THE ALPHANUMERIC VISUAL PASSWORD FORMAT

Grid Density (columns × rows)	Easy (95% CIs)	Safe (95% CIs)
2×2	6.30 [5.77,6.83]	1.26 [0.99,1.53]
2×3	5.78 [5.10,6.46]	1.70 [1.23,2.17]
3×2	6.11 [5.72,6.50]	1.67 [1.20,2.14]
3×3	5.81 [5.32,6.30]	2.59 [2.03,3.15]
3×4	5.59 [5.03,6.15]	3.78 [3.20,4.36]
4×3	5.52 [4.86,6.18]	3.78 [3.18,4.38]
4×4	5.26 [4.75,5.77]	4.37 [3.81,4.93]
4×5	4.63 [4.10,5.16]	5.15 [4.74,5.56]
5×4	4.56 [4.00,5.12]	5.11 [4.66,5.56]
5×5	4.67 [4.09,5.25]	5.11 [4.64,5.58]
5×6	4.52 [3.94,5.10]	5.41 [4.96,5.86]
6×5	4.30 [3.64,4.96]	5.56 [5.11,6.01]
6×6	4.56 [3.90,5.22]	6.04 [5.67,6.41]
6×7	3.78 [3.06,4.50]	6.26 [5.93,6.59]
7×6	3.41 [2.65,4.17]	6.41 [6.14,6.68]

Grid Density (columns × rows)	Easy (95% CIs)	Safe (95% CIs)
7×7	3.52 [2.68,4.36]	6.44 [6.07,6.81]

Fig. 4 shows the participant judgments (n=27) on whether a grid was potentially easy and safe to use for the pattern format. Similar to the judgments for the alphanumeric format, participants assessed the grid progressively not easy to use when the number of cells in the grids increased (black circles). However, when the grid became denser, they thought it increasingly safer to use in an imagined situation in which eye tracking would be used to make the password (white circles).

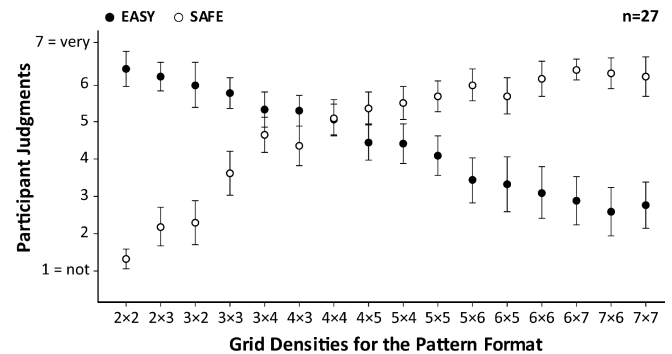


Fig. 4. The participant judgments (n=27) on whether a grid was potentially easy (black circles) and safe (white circles) to use for the pattern visual password format. Error bars indicate $\pm$ 95% confidence interval around the means.

Table II shows the 95% CIs around the means (n=27) of the “easy” and “safe” judgments for the pattern visual password format. A comparison was performed between interval ranges with the midpoint of the rating scale, i.e., “4”, to get an indication of which grid density would be useful for this format. For the “easy to use” judgments, the means and the 95% CIs for the 2×2, 2×3, 3×2, 3×3, 3×4, 4×3, and 4×4 grids were greater than the scale midpoint. As regards the “potentially safe” judgments, the means and the 95% CIs for the 3×4, 4×4, 4×5, 5×4, 5×5, 5×6, 6×5, 6×6, 6×7, 7×6, and 7×7 grids exceeded the scale midpoint, suggesting that these grid densities were considered potentially safe for the pattern format.

TABLE II. THE MEANS AND THE 95% CONFIDENCE INTERVALS OF THE EASY AND SAFE JUDGMENTS FOR EACH GRID DENSITY FOR THE PATTERN VISUAL PASSWORD FORMAT

Grid Density (columns × rows)	Easy (95% CIs)	Safe (95% CIs)
2×2	6.44 [5.97,6.91]	1.33 [1.06,1.60]
2×3	6.22 [5.85,6.59]	2.19 [1.68,2.70]
3×2	6.00 [5.40,6.60]	2.30 [1.70,2.90]
3×3	5.78 [5.37,6.19]	3.63 [3.05,4.21]
3×4	5.33 [4.86,5.80]	4.67 [4.20,5.14]
4×3	5.30 [4.89,5.71]	4.37 [3.84,4.90]
4×4	5.07 [4.66,5.48]	5.11 [4.62,5.60]
4×5	4.44 [3.97,4.91]	5.37 [4.94,5.80]
5×4	4.41 [3.88,4.94]	5.52 [5.07,5.97]
5×5	4.11 [3.58,4.64]	5.70 [5.29,6.11]
5×6	3.44 [2.84,4.04]	6.00 [5.57,6.43]
6×5	3.33 [2.59,4.07]	5.70 [5.21,6.19]

Grid Density (columns × rows)	Easy (95% CIs)	Safe (95% CIs)
6×6	3.11 [2.43,3.79]	6.15 [5.68,6.62]
6×7	2.89 [2.25,3.53]	6.41 [6.12,6.70]
7×6	2.59 [1.95,3.23]	6.30 [5.89,6.71]
7×7	2.78 [2.16,3.40]	6.22 [5.69,6.75]

Fig. 5 shows the participant judgments (n=27) on whether the grid densities for the picture format were potentially easy to use and safe. Also for this format, as the number of grid cells increased, the participants judged the grid as increasingly less easy to use (black circles), but safer (white circles).

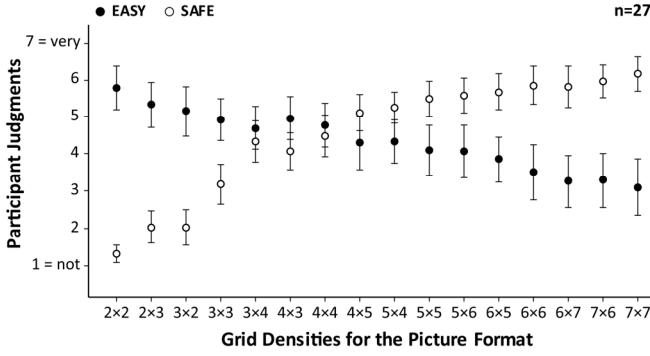


Fig. 5. The participant judgments (n=27) on whether a grid was easy (black circles) and safe (white circles) to use for the picture visual password format. Error bars indicate $\pm$ 95% confidence interval around the means.

Table III shows the 95% CIs around the means (n=27) of the “easy” and “safe” judgments for the picture format. Regarding the “easy to use” judgments, the means and the 95% CIs for the 2×2, 2×3, 3×2, 3×3, 3×4, 4×3, and 4×4 grids exceeded the scale midpoint (“4”), suggesting that these grid densities were thought to be easy to use with the picture format. For the “potentially safe” judgments, the means and the 95% CIs for the 4×5, 5×4, 5×5, 5×6, 6×5, 6×6, 6×7, 7×6, and 7×7 grids exceeded the scale midpoint, suggesting that these grid densities tended to be potentially safe for the picture format.

TABLE III. THE MEANS AND THE 95% CONFIDENCE INTERVALS OF THE EASY AND SAFE JUDGMENTS FOR EACH GRID DENSITY FOR THE PICTURE VISUAL PASSWORD FORMAT

Grid Density (columns × rows)	Easy (95% CIs)	Safe (95% CIs)
2×2	5.78 [5.20,6.36]	1.33 [1.10,1.56]
2×3	5.33 [4.73,5.93]	2.04 [1.61,2.47]
3×2	5.15 [4.49,5.81]	2.04 [1.57,2.51]
3×3	4.93 [4.37,5.49]	3.19 [2.66,3.72]
3×4	4.70 [4.12,5.28]	4.33 [3.77,4.89]
4×3	4.96 [4.38,5.54]	4.07 [3.58,4.56]
4×4	4.78 [4.18,5.38]	4.48 [3.92,5.04]
4×5	4.30 [3.58,5.02]	5.11 [4.62,5.60]
5×4	4.33 [3.75,4.91]	5.26 [4.85,5.67]
5×5	4.11 [3.43,4.79]	5.48 [5.01,5.95]
5×6	4.07 [3.37,4.77]	5.56 [5.09,6.03]
6×5	3.85 [3.25,4.45]	5.67 [5.18,6.16]
6×6	3.52 [2.78,4.26]	5.85 [5.34,6.36]

Grid Density (columns × rows)	Easy (95% CIs)	Safe (95% CIs)
6×7	3.26 [2.56,3.96]	5.81 [5.25,6.37]
7×6	3.30 [2.58,4.02]	5.96 [5.51,6.41]
7×7	3.11 [2.37,3.85]	6.15 [5.68,6.62]

Taken together, Experiment I shows that some grid densities are not particularly suitable for visual password formation using eye tracking. Regarding the safety judgments, the 95% CIs around judgment means of grid densities with either two columns or rows (2×2, 2×3, and 3×2) did not exceed the scale midpoint (“4”) in any of the three visual password formats. The results for “easy to use” judgments were less clear-cut, but since the 95% CIs around judgment means of grid densities with either seven columns or rows (6×7, 7×6, and 7×7) did not firmly exceed the scale midpoint in two of the three visual password formats (the pattern format and the picture format), these grids can be considered as relatively difficult to use. From this, it results that grid densities ranging from 3×3 to 6×6 are considered suitable for visual password formation using eye tracking.

This preliminary experiment has several limitations. First, the meaning of “easy to use” or “potential safety” of the grid densities was not given to the participants when evaluating the grids. Second, it is not known how much time was required to create a password on each grid. In the following Experiment II, the participant used eye tracking to perform visual password registration with a short password (4 visual objects) and a long password (6 visual objects). The amount of time for password registration was measured, as an indicator of grid density usability for eye tracking.

III. EXPERIMENT II (PRELIMINARY RESULTS)

A. Method (summarized)

Standing in front of the monitor, the participant was shown a visual password, randomly generated in the alphanumeric format, the pattern format, or the picture format. The password consisted either of 4 or 6 objects. The participant was then asked to memorize the password within two minutes. Following this, he/she was instructed to register the memorized password on the screen interface with his/her eye gaze by selecting visual objects on 16 grids (from 3×3 to 6×6 cells, columns × rows). There were six participants (three males, three females).

TABLE IV. THE AVERAGE TIME (SECONDS) FOR PASSWORD REGISTRATION BY MEANS OF EYE TRACKING FOR EACH GRID DENSITY FOR THREE VISUAL PASSWORD FORMATS

Grid Density (columns × rows)	4 Objects			6 Objects		
	AN	PA	PI	AN	PA	PI
3×3	5.98	6.01	6.42	8.90	8.94	9.18
3×4	7.48	6.39	6.67	9.41	9.16	14.60
3×5	8.94	5.91	9.20	9.64	12.39	10.99
3×6	10.62	11.18	8.86	14.26	12.34	16.36
4×3	8.26	6.55	7.93	9.99	12.11	11.37
4×4	10.22	8.74	7.03	11.55	8.88	11.42
4×5	7.24	9.78	8.40	10.36	9.61	13.97
4×6	9.51	8.71	13.48	15.96	11.69	13.72
5×3	6.33	6.51	8.54	10.07	12.61	14.29

5×4	7.78	6.73	6.97	11.27	12.53	16.01
5×5	7.45	9.41	8.75	12.79	10.85	17.34
5×6	9.63	6.99	13.43	17.49	17.34	14.96
6×3	7.96	6.33	7.55	9.96	13.25	15.45
6×4	8.34	8.45	11.25	11.54	12.17	16.53
6×5	6.56	7.50	8.19	9.32	14.42	11.52
6×6	8.37	8.73	11.79	11.26	11.53	16.30

B. Results

Table IV shows the average password registration time (n=6) for each grid density of the three visual password formats [Alphanumeric (AN), Pattern (PA), Picture (PI)]. Overall, the registration time with eye tracking for short and long passwords required more time when the number of grid cells increased. Although statistics on these preliminary results have yet to be performed, for some grid densities registration of passwords in the picture format seemed to take relatively more time than password registration in the alphanumeric and the pattern format.

IV. DISCUSSION & CONCLUSION

Experiment I describes an evaluation of different grid densities in between 2×2 to 7×7 cells for use with three visual password formats. The participants (n=27) were asked to make an imaginary password on the screen using a mouse, and imagine they were using eye tracking to make the password. The objective of the experiment was to minimize and identify the range of the possible grid densities for an experiment with actual eye tracking (Experiment II). Hence, besides making the password, this experiment also required the participants to assess the 16 grid densities about whether they are easy to use and potentially safe for making a visual password in an imagined situation using eye tracking. The results suggest that grid densities from 3×3 to 6×6 cells seem adequate.

In Experiment II, participants (n=6) memorized and registered a short and long password (4 or 6 visual objects) using actual eye tracking. They registered passwords on grid densities, from 3×3 to 6×6 cells, for three visual password formats. The preliminary results show that registration time increased when the grid became denser. A reason could be that when the number of grid cells increased, either in columns or rows, the distance between the visual objects decreased, making it difficult to correctly select each individual object by eye tracking. Furthermore, it seems that password registration in the picture format took more time for some grid densities, but more data are being collected and statistics have to be performed. Further investigations are required to obtain an objective measure of whether a particular grid is easy to use by measuring the time and accuracy of visual password formation and authentication using eye tracking. An indication of the subjective feeling of safety may be the password length.

ACKNOWLEDGMENTS

The procedures described here have been approved by the Ethical Committee of the Faculty of Design, Kyushu University, Japan. We would also like to thank the participants for their time and efforts. YTP received support from the Indonesia Endowment Fund for Education (LPDP), Ministry of Finance of Indonesia, and Ministry of Research,

Technology and Higher Education of the Republic of Indonesia (RISTEKDIKTI). GBR and CH are supported by the Q-DAI Jump Program.

REFERENCES

- [1] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," *Int. J. Hum. Comput. Stud.*, vol. 63, no. 1–2, pp. 128–152, 2005.
- [2] K. Renaud and A. De Angeli, "Visual Passwords: Cure-All or Snake-Oil?," *Commun. ACM*, vol. 52, no. 12, p. 135, Dec. 2009.
- [3] K. L. Higbee, *Your memory: How it works and how to improve it*, Second Edi. New York: Marlowe & Company, 1977.
- [4] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *Int. J. Hum. Comput. Stud.*, vol. 63, no. 1–2, pp. 102–127, 2005.
- [5] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," in *Proceedings of the 12th European conference on Research in Computer Security - ESORICS'07*, pp. 359–374, 2007.
- [6] A. Forget, S. Chiasson, and R. Biddle, "Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '10*, pp. 1107–1110, 2010.
- [7] S. Alam, "SUIS: An online graphical Signature-Based User Identification System," in *Proceedings of the 2016 Sixth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, pp. 85–89, 2016.
- [8] R. Weiss and A. De Luca, "PassShapes - Utilizing Stroke Based Authentication to Increase Password Memorability," in *Proceedings of the 5th Nordic conference on Human-computer interaction building bridges - NordiCHI '08*, pp. 383–392, 2008.
- [9] A. De Luca, M. Denzel, and H. Hussmann, "Look into my Eyes! Can you guess my Password?," in *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*, 2009.
- [10] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in *Proceedings of the 8th conference on USENIX Security Symposium - SSYM'99*, 1999.
- [11] H. Gao, X. Guo, X. Chen, L. Wang, and X. Liu, "YAGP: Yet Another Graphical Password Strategy," in *Proceedings of the 2008 Annual Computer Security Applications Conference - ACSAC '08*, pp. 121–129, 2008.
- [12] R. Dhamija and A. Perrig, "Deja vu: A User Study Using Images for Authentication," in *Proceedings of the 9th conference on USENIX Security Symposium - SSYM'00*, 2000.
- [13] M. G. Tusciano, A. Tulasyan, A. Shetty, M. Rumao, and A. Shetty, "Graphical password authentication using Pass faces," *Int. J. Eng. Res. Appl.*, vol. 5, no. 3, pp. 60–64, 2015.
- [14] P. Dunphy, A. Fitch, and P. Olivier, "Gaze-contingent passwords at the ATM," in *Proceedings of the 4th Conference on Communication by Gaze Interaction - COGAIN*, pp. 59–62, 2008.
- [15] M. Mihajlov and B. Jerman-Blazic, "Eye Tracking Graphical Passwords," in *Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity*, pp. 37–44, 2018.
- [16] J. Thorpe and P. C. van Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords," in *Proceedings of the 20th Annual Computer Security Applications Conference - ACSAC '04*, pp. 50–60, 2004.
- [17] Y. T. Paulus, C. Hiramatsu, Y. K. H. Syn, and G. B. Remijn, "Measurement of viewing distances and angles for eye tracking under different lighting conditions," in *Proceedings of the 2017 2nd International Conference on Automation, Cognitive Science, Optics, Micro Electro-Mechanical System, and Information Technology - ICACOMIT*, pp. 54–58, 2017.
- [18] Y. T. Paulus, G. B. Remijn, Y. K. H. Syn, and C. Hiramatsu, "The use of glasses during registration into a low- cost eye tracking device under different lighting conditions," in *Proceedings of the 2017 2nd International Conference on Automation, Cognitive Science, Optics, Micro Electro-Mechanical System, and Information Technology - ICACOMIT*, pp. 59–64, 2017.