Comparing the usability of doodle and Mikon images to be used as authenticators in graphical authentication systems

Soumyadeb Chowdhury
School of Computing Science
University of Glasgow
United Kingdom
soumc@dcs.gla.ac.uk

Ron Poet
School of Computing Science
University of Glasgow
United Kingdom
ron@dcs.gla.ac.uk

Abstract— **Recognition-based graphical authentication systems rely on the recognition of authenticator images by legitimate users for authentication. This paper presents the results of a study that compared doodle images and Mikon images as authenticators in recognition based graphical authentication systems taking various usability dimensions into account. The results of the usability evaluation, with 20 participants, demonstrated that users preferred Mikon to doodle images as authenticators in recognition based graphical authentication mechanisms. Furthermore, participants found it difficult to recognize doodle images during authentication as well as associate them with something meaningful. Our findings also show the need to consider the security offered by the images, especially their predictability.**

Keywords-component; Graphical authentication; Usability;User experiencep;Doodle; Mikon; Predictability

I. INTRODUCTION

An alternative approach proposed in existing studies [1, 2, 3] to help solve the problems of knowledge based authentication system is the use of graphical authentication systems that will rely on recognition of images, rather than recall of passwords. Graphical authentication mechanisms use different image types like faces [1], everyday objects [2], random art [3], doodles [8] and Mikon [10] as the authenticators. This relies on the picture superiority effect [4] and dual code theory [6]. It suggests that images can be recognized by people more readily than recalling alphanumeric characters because pictures are represented in memory with more details than alphanumeric characters [5].

In recognition-based graphical authentication systems the user's password is an image. The password image is displayed on a screen, together with a number of other images known as *distractor* images. A collection of password and distractor images is called a *challenge set*. The user needs to recognize the password image for authentication, rather than recall it from scratch. Given the need for usable authentication and existing interests in recognition-based graphical authentication systems as a potential solution, our focus in this paper is to compare the usability of Mikon and doodle images, when used as authenticators. The following section gives a brief overview of the existing work in this area.

II. RELATED WORK

A. *Doodle images*

Doodles are simple images hand-drawn on paper using a pen (Fig 1).The work reported in [8] made the users draw their doodles, scan them and submit them to the system to be used as passwords. The usability assessment revealed that the doodle images were memorable but the authentication system was time-consuming to use. A longitudinal experiment was reported in [9], to determine the efficiency of doodles, photographs and images belonging to different semantic categories like eatables, buildings, animals, and cars as authenticators. The results of the experiments suggested that doodle images performed better compared to other images in terms of memorability. In this context the authors pointed out that, the doodle images could capture the essence of an object and contain much less extraneous information compared to other types of images. So, doodles may require less visual and cognitive processing for identification. It was found that an authentication system with doodle images is time consuming in the enrolment stage because users not only have to draw the images, but scan them too. Thus the studies reported in the paper gives evidence that, doodle images possess the qualities that make them suitable authenticators in recognition based graphical authentication mechanisms, and the authenticators provided by the user themselves are more memorable compared to system generated authenticators.

B. *Mikon images*

Mikon images are icon like drawings drawn on screen (web browser) using a tool developed by the company Mikons.com (fig 2). The work reported in [10] made the users draw these images to be used as passwords. An experiment was conducted with 26 school students of 11-12 years of age to determine the performance of the Mikon authentication system. In terms of memorability, it was found that Mikons were also very successful. The success rate of authentication using Mikon images as authenticators was 87%. In terms of

scalability, Mikon systems performed better than doodle systems which required human involvement to scan and upload the authenticator. The results do not give any information about the efficiency of the authentication system using Mikon as authenticators. The findings of the study show the potential of the Mikon images when used as authenticators.

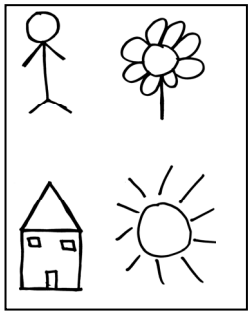

Figure 1. Doodle images

Figure 2. Mikon images

In all the existing work with doodle and Mikon images the users draw their images and submit them to the system which is time consuming. It is also difficult to control the tendency of the users to draw inappropriate or offensive image. So we focused on the method of selecting passwords from a given image archive which is less time consuming. Since both types of images have performed well, the focus of the present work is to compare the usability of the images and find their individual qualities and constraints when used as passwords.

The next section discusses the authentication systems developed for user evaluation.

III. SYSTEM CONFIGURATION

A. Authentication system

We developed two authentication systems. Doodle-select used doodle images as passwords and Mikon-select used Mikon images as passwords. The authentication systems had two stages.

Enrolment stage: In this stage, the users entered a unique username used to identify them during the authentication stage. There were four image selection screens. In each screen 20 images were displayed in a 5X4 matrix (fig 3). The users had to select one image from each screen as their password. The doodle collection comprised of images that were drawn by participants of the study reported in [9]. The Mikon collection comprised of images that were drawn by participants of the study reported in [10].

Authentication stage: In this stage the users were identified by the usernames they had entered. Once identified, users choose authenticator images in each step of the four step authentication process using a mouse. In each step, a screen appears with one challenge set containing 16 images: 15 distractor images and one authenticator image (fig 4). If the user selects all the authenticator images correctly then the authentication is successful, else the user has to go through the authentication stage again.

B. Implementation decisions

- *Lock Mechanism:* The authentication systems employed a lock mechanism. So after three unsuccessful authentication attempts the user would not be able to access the system.
- *Multistage authentication:* In the authentication systems, there were 4 challenge sets containing 60 distractor images and 4 authenticator images. So, the possibility of guessing the correct combination will be 1 in 65536, which is quite low [10].
- *Keeping the distractor images fixed for each authentication attempt:* The distractor images for each authentication stage was fixed during the enrolment phase to prevent intersection attack. The distractor images were chosen using the algorithm reported in [7].

The next section gives a detailed description of the experimental framework for user evaluation.

IV. EXPERIMENT

A. Participant information

The user study was conducted with 20 participants, 10 participants studying Management courses, 6 studying Computing Science and 4 studying different engineering courses in the university. They all were between ages 23- 28. Of all the participants we had 6 females and 14 males.

B. Experimental design

The experiment was designed such that each participant would use both the authentication systems. Since each of the participants used both the systems, in order to take into account the effects produced by the order of using the systems, the experimental design was counterbalanced by dividing the participants into two groups. Each group used the authentication system in different order. Both the groups had equal number (10 each) of participants.

Each participant first registered with one of the authentication systems and authenticated using the same password 20 times. They were then given a break of 30 minutes. After the break they registered with the second authentication system and authenticated themselves 20 times using the same password. After 5 days the participants were asked to complete the authentication procedure for both the authentication systems five times. Finally they were asked to fill a questionnaire on their experience of using the systems.

C. Independent and dependent variables

The independent variables of the experiment were: doodle images and Mikon images, being used as authenticators.

Table I gives an overview of the usability dimensions (dependent variables).

TABLE I. USABILITY DIMENSIONS-DEPENDENT VARIABLES

Dependant variable	Behavior to be measured	Method to measure
1. Effectiveness	Ease to remember	questionnaire
	Failure login rate	System log
2. Efficiency	Authentication time + enrolment time	System log
	Ease to enroll	questionnaire
	Ease to find the authenticator image during authentication	questionnaire
3. User satisfaction	Final preference of the user	questionnaire

D. Statistical tests

Some of the behavior of the dependant variables was measured using the quantitative data obtained from the system log. The quantitative data obtained from system log were nominal and hence could be ranked (for example shortest time to the longest time in case of efficiency). So we used a non parametric test called *Wilcoxon signed rank test* to find the statistical significance.

Some of the behavior of the dependant variables was measured using the data from questionnaires. In the questionnaire, each participant gave a score to the doodle and Mikon images on a scale of 1 to 5 (1 being the worst and 5 being the best). The scores represented the ratings of the images for the behavior of the dependent variables being measured. A participant rating 5 to Mikon and 4 to doodle images presumable prefers Mikon images. So the direction of each difference (score assigned to Mikon and doodle) is meaningful. So we used *Sign test* to assess the statistical significance of the results.

The following section discusses the results of the user evaluation.

V. RESULTS AND DISCUSSION

A. Effectiveness

Ease of remembering the authenticators: The results from the questionnaire revealed that, 65% of the participants (13/20) found it easier to remember the Mikon images, 25% (5/20) of the participants found it easier to remember the doodle images and for 10% (2/20) of the participants the memorability of doodle and Mikon images was the same. The sign test shows that the Mikon images produced significantly higher ratings than doodle images for this aspect ($p = 0.01 < 0.05$). The test provides evidence that participant preference differed significantly for the two images.

According to the literature on memorability of the images, the ease of remembering an image depends on the ease of assigning a name to the image [6,11]. So, images which are meaningful to some extent and easily understandable are easy to remember. This evaluation demonstrates the same. According to the participants, Mikon images were memorable because they were more meaningful and it was easy to understand them compared to the doodle images.

Failure login rate: There were no login failures while the participants used Doodle-select and Mikon-select

B. Efficiency

Enrolment time: It was found that the mean time taken to enroll in case of doodle-select was greater compared to Mikon-select (table II). The results of the wilcoxon signed rank test showed that the participants had significantly shorter enrolment time in Mikon-select compared to Doodle-select ($z=3.92$, $p<0.05$, $r=0.8$). These results can be attributed to the fact that, Mikon images are more meaningful and easy to understand.

TABLE II. MEAN TIME TO ENROLL

Authentication system	No of observations	Mean time in seconds
Doodle-select	20	39
Mikon-select	20	31

Ease to enroll: The qualitative data collected from the participants through interviews revealed that, 80% (16/20) of the participants found it easier to choose Mikon images as authenticators, 20% (4/20) of the participants found it easier to choose doodle images as the authenticator. The sign test shows that the Mikon images produced significantly higher ratings than doodle images for this aspect($p = 0.01 < 0.05$). The test provides evidence that participant preference differed significantly for the two images.

*Authentication time***:** It was found that the mean time taken to authenticate was more in the case of Doodle-select compared to Mikon-select (table III). The results of the wilcoxon signed rank test showed that the participants had significantly shorter authentication time in Mikon-select compared to Doodle-select ($z=3.24$, $p<0.05$, $r=0.7$).

TABLE III. MEAN TIME TO AUTHENTICATE

Authentication system	No of observations	Condition	Approximate mean time (in seconds)
Doodle-select	400	Training phase	49
	100	After 5 days	47
Mikon-select	400	Training phase	29.5
	100	After 5 days	29.9

This can be attributed to the fact that it was more difficult to recognize the doodle images than the Mikon images in the challenge set. It was reported that participants found it

difficult to find the doodle authenticator images in the challenge set. All the doodle images had the same texture (black and white line drawings), though their content were different, the participants had to look through all the images in the challenge set before they could find their authenticator image. Thus, they had to put effort in the authentication stages to find the authenticator image. This can be further explained from the literature on visual search. According to the guided search process discussed in [12], an image is initially divided into a number of representations- one for each of the features of the image like color, orientation etc. After this, a top down process matches representations in two images being compared, and at the same time another bottom up process categorizes the features in the two images. During this process, the internal memory storage of the human brain may omit some finer details of the image and store the bare bones of the image. According to the work reported in [5], instead of storing a replica of an image the long term memory stores a meaningful interpretation of the image eliminating the unimportant visual details.

The doodle images contain less information than Mikon images [10, 11]; hence they may require less visual and cognitive processing. But according to the theory of guided search discussed above, the image representation of a doodle image may not be descriptive enough in memory to be able to find and distinguish it from other such images, as it contains fewer features to provide information to the memory than to Mikon images. Human memory may also lose some of the image representation, leaving only bare bones of the doodle image, which may make it very difficult to identify the authenticator image in the challenge set when all the images differ by a very small extent excepting only the content of the image. All the participants found it easier to find the Mikon authenticators during authentication phase compared to doodle authenticators.

C. User satisfaction

The qualitative data collected from the participants revealed that, 85% (17/20) of the participants preferred Mikon images to be used as authenticators and 15% (3/20) preferred doodle images to be used as authenticators. In terms of all the usability dimensions, Mikon images scored better than to the doodle images, and most of the users were more satisfied with the Mikon images as they made the authentication system not only easy to use, but also less time consuming due to familiar and meaningful images of good visual quality. The sign test shows that the Mikon images produced significantly higher ratings than doodle images ($p= 0.01 <0.05$). The test provides evidence that participant preference differed significantly for the two images.

VI. SECURITY ANALYSIS

In case of images being used as passwords there is a lack of predefined dictionary of likely choices such as an English dictionary would provide for text passwords. But if the users choose images that are related to them for example their personal characteristics, interests, culture etc. then an intruder can merely predict the images based on their knowledge about the user and impersonate a legitimate user. So we analyzed the images chosen by the users taking into account the demographic information given by them.

The analysis in case of Mikon images revealed that out of 80 images chosen by the participants only 10 images were personally related to them. Thus 12.5% of the images may be predictable. In this context it is necessary to take into account that 10 images belonged to only 4 participants. Out of these, 2 participants chose all the images somehow related to them. Thus remaining 2 had only 1 image personally related to them. So 80% of the participants did not choose images related to them and their passwords were not predictable merely on knowledge about them.

In the Mikon-select system the theoretical password space would consist of all the images in the collection i.e. 80 images. The effective password space would consist of the number of distinct images chosen by the users as passwords from the collection. The effective password space for the Mikon authentication system was 69 indicating that some participants chose the same images as others. Only 3 images were chosen by more than 1 user which suggests that there were few popular images. On this basis, it would be difficult to launch a dictionary attack as 86.25% of the images fell under effective password space.

In case of the doodle images, the analysis revealed that 25 images were personally related to the participants. Thus almost 30% of the images were predictable if the demographic information of the participants were known. These 25 images belonged to 11 participants. Out of these, 3 participants chose all the images somehow related to them. Thus 55% of the participants chose images that were personally related to them. This is a large statistics compared to the Mikon images. So we can say that in case of doodle images participants chose password images that were related to them almost twice more often than Mikon passwords.

The effective password space in doodle-select was 45. So almost 44% of the images were not a part of the effective password space which may surely make the system more susceptible to a dictionary attack than Mikon-select. In this system each of the participants had more than one image in common with other participants. This can be attributed to the fact that in case of doodle images few images were meaningful. Hence all participants chose meaningful images to enhance memorability. Thus there is a conflict between memorability and predictability.

VII. CONCLUSIONS

This paper reported a small study carried out to compare the usability of doodle and Mikon password images in recognition based graphical authentication system. The results of the evaluation demonstrated most users preferred Mikon as passwords. From a security point of view, we conclude that the Mikon images are less predictable than the doodle images. But it is also necessary to investigate and compare the suitability of Mikon images with other image types in the

same setting. In this study we used a single password but in future this will be extended to multiple passwords because in real life users have to deal with many passwords.

The study conducted had a relatively small sample size and the time gap between two consecutive sessions was only 5 days. These limitations will be addressed in future studies, by making the evaluation with a large sample size from different work groups and also by increasing the time gap between two sessions.

We also propose an additional feature of time outs to increase the security of recognition based authentication systems. In this scheme each authentication step will be constrained by a timer that will make the authentication page expire after a specific time limit. A lock-out mechanism will be set after the authentication pages expires a specific number of times. This will ensure that an intruder cannot spend a lot of time in the authentication pages. But the usability of the feature has to be tested for legitimate users and the time limit has to be determined.

REFERENCES

[1] S. Brostoff, and A.M. Sasse, " Are Passfaces More Usable Than Passwords? A Field Trial Investigation", Proc. HCI 2000 People and Computers XIV - Usability or Else!, Springer-Verlag, Sept. 2000, pp. 405-424.

[2] D. Davis, F. Monrose, and M. Reiter, "On User Choice in Graphical Password Schemes", Proc. 13th Conference on USENIX Security Symposium, Aug. 2004, pp. 151-164.

[3] R. Dhamija, and A. Perrig, " Déjà Vu: A User Study Using Images for Authentication", Proc. 9th Conference on USENIX Security Symposium, Aug. 2000, pp. 45-58.

[4] S. Madigan, "Picture Memory", in Imagery, Memory, and Cognition: Essays in Honor of Allan Paivio, J. Yuille, Eds. Hillsdale: Lawrence Erlbaum Associates, 1983, pp. 65-86.

[5] J.M. Mandler, and G.H. Ritchey, "Long-term memory for pictures", Journal of Experimental Psychology: Human Learning and Memory, vol. 3, July 1977, pp. 386-396.

[6] A. Paivio, " Mental Representataions:A Dual Coding Approach", Oxford University Press, Oxford, 1986.

[7] R. Poet, and K. Renaud, "A Mechanism for Filtering Distractors for Doodle Passwords", International Journal of Pattern Recognition and Artificial Intelligence. vol. 23, Aug. 2009, pp. 1005-1029.

[8] K. Renaud, "A Visuo- Biometric Authentication Mechanism for Old Users", Proc. British HCI, Sept. 2005, pp. 167-182.

[9] K. Renaud, "On User Involvement in Production of Images Used in Visual Authentication", Journal of Visual Languages and Computing, vol. 20, Feb. 2009, pp.1-15.

[10] K. Renaud, "Web Authentication using Mikon Images", Proc. World Congress on Privacy, Security, Trust and the Management of e-Business, Aug. 2009, pp. 79-88.

[11] A. Szekely, and E. Bates, "Objective Visual Complexity as a Variable in Picture Naming", CRL Newsletter Center for Research in Language, University of California, May. 2000, pp. 3-33.

[12] M. Wolfe, "Guided Search 2.0 A Revised Model of Visual Search", Psychonomic Bulletin & Review. vol. 1, 1994, pp. 202-238.

APPENDIX

Usability assessment by users

Table A gives an overview of the ratings given by the participants to different usability aspects.

No: Participant number
Mem: Ease of remembering the image
Enr: Ease of enrolling to the system
Usat: User satisfaction using the system

No	Mikon			Doodle		
	Mem	Enr	Usat	Mem	Enr	Usat
1	4	5	4	3	3	3
2	3	2	3	4	3	4
3	5	4	4	3	2	3
4	3	3	3	4	4	4
5	4	5	5	3	3	3
6	4	5	5	3	3	3
7	5	4	5	4	3	2
8	3	4	4	3	2	3
9	3	5	2	4	3	4
10	3	3	5	5	4	3
11	4	5	4	2	3	3
12	3	4	4	3	3	2
13	4	4	4	5	2	3
14	3	4	5	4	2	2
15	5	4	5	3	3	3
16	5	5	5	4	3	3
17	4	4	4	2	3	2
18	3	5	4	4	3	3
19	4	5	5	2	2	3
20	4	4	4	3	3	2

Analysis of the images chosen by the users

Mikon images

Number of images selected by the user = 72/80.
Number of distinct images = 69.
Number of images common among users =3.
Let the common images be P, Q, and R.
Number of people chose P = 3.
Number if people chose Q = 4.
Number of people chose R = 4.
Most popular image is chosen by 4 people,

Doodle images

Number of images selected by user = 50/80.
Number of distinct images = 45.
Number of images common among users =5.
Let the common images be A1, A2, A3, A4, and A5.
Number of people chose A1 = 8.
Number if people chose A2 = 7.
Number of people chose A3 = 5.
Number if people chose A4 = 3.
Number of people chose A5 = 7.
Most popular image is chosen by 8 people.