An Algorithm for Automatically Choosing Distractors for Recognition Based Authentication using Minimal Image Types

Ron Poet* and Karen Renaud*

Department of Computing Science University of Glasgow, UK

Abstract: When a user logs on to a recognition based authentication system, he or she is presented with a number of images, one of which is their pass image and the others are distractors. The user must recognise and select their own image to enter the system. If any of the distractors is too similar to the target, the user is likely to become confused and may well choose a distractor by mistake.

It is simple for humans to rule on image similarity but such a labour intensive approach hinders the wider uptake of these mechanisms. Automating image similarity detection is a challenging problem but somewhat easier when the images being used are minimal image types such as hand drawn doodles and Mikons constructed using a computer tool.

We have developed an algorithm, which has been reported earlier, to automatically detect if two doodle images are similar. This paper reports a new experiment to discover the amount of similarity in collections of doodles and Mikons, from a human perspective. This information is used to improve the algorithm and confirm that it also works well with Mikons.

Keywords: Authentication, visual, image, recognition, distractor, similarity, algorithm.

1. INTRODUCTION

The password is the authenticator of choice for most modern software applications. Unfortunately it is deeply flawed in an environment where computer users access many systems and have far too many “secret” passwords to remember. The obvious consequence is reuse of passwords [1], insecure recording of passwords [2] and use of weak passwords [3] which are easily broken by determined intruders.

These facts have been well known for almost 30 years [4]. The use of the password persists for the very simple reason that it is by far the easiest option for system developers and support staff. The mechanisms and mechanics of passwords are well understood and relatively easy to police. Furthermore, much of the burden resulting from the unsuitability of the password falls on the end-users [5]. Some financial burden falls onto companies who have to man call centres, many of whose calls are related to forgotten passwords [6].

Unfortunately, many alternatives to passwords have not yet demonstrated that they are in a position to improve the situation to any significant extent. Biometrics seem to have limited validity for a web-based system when the additional requirements of a biometric reader and privacy concerns [7] are considered. Some organisations, in an attempt to harden the password, require two-factor authentication, a token such as a card accompanied by a password [8]. Other organisations, mostly banks, issue their users with one-time password mechanisms [9]. These are all very well, but are far from being universally usable due to the cost and the possibility of the token or device being mislaid, stolen or damaged.

It is also worth considering password users. They are far more heterogeneous than the original password user of 40 years ago: the young technophile with excellent cognitive and memory skills. The computer user of today ranges from the young to the very old, from the highly educated to the barely literate, from the disabled to the dyslexic. The password requirement, of exact and precise unaided recall, is simply unrealistic for many of these users.

An alternative approach to authentication is to use *recognition* rather than *recall* to provide the “password”. In a recognition based system, the user’s “password”, the *target* is displayed on the screen, together with a number of *distractor* “passwords”. The collection of target and distractors is called a *challenge* set. The user just needs to recognise his or her “password”, rather than recall it from scratch. In almost all cases, the “password” is actually a pass image, since it is easier for the user to find and recognise an image rather than the sort of text that would make a good password. The latter task is akin to searching for text in a table, which is obviously more difficult than searching for an object in a grid. An early example of such a system that has been used in industry is the PassFace system[1], although long term evaluation has suggested some flaws [10].

The following section will introduce recognition based authentication. Section 3 outlines our research in using image based authentication mechanisms and explains our focus on image similarity. Section 4 outlines our algorithm

*Address correspondence to these authors at the Department of Computing Science, University of Glasgow, UK;
Tel: +141 330 5321; Fax: +141 330 4913
E-mails: ron@dcs.gla.ac.uk, karen@dcs.gla.ac.uk

[1] http://www.passfaces.com

for automating similarity detection. Section 5 describes a new experiment to determine the amount of similarity in collections of simple images and applies this information to our algorithm. Section 6 concludes.

2. RECOGNITION BASED AUTHENTICATION USING IMAGES

When a user registers with an image recognition based systems they are either provided with a pass image or several pass images by the system or supply these images themselves. The latter option maximises memorability but can also makes it easier for a potential intruder to guess the identity of the image password. Then when they log in they must recognise their image or images as described earlier. Initially the protagonists of this kind of mechanism relied solely on the picture superiority effect [11] to enhance the memorability. Unfortunately this effect is easily negated if the system is not designed with due care [12].

In order to design these systems for maximum efficacy, we need first to understand how humans engage in visual search. The literature on visual search makes it clear that it is not a predictable process [13]. The eye flits and fixates on the images in the challenge set in a completely random and unpredictable fashion, often revisiting distractor images before finding the target [14]. The process tends to be serial if the challenge set is composed of heterogeneous images [15] but will not necessarily start at the top left corner and proceed to bottom right. It is impossible, therefore, to predict how long it will take for someone to locate their own image. Various aspects will impact on the efficiency of the process, including the visual complexity of the image [16], the number of, and overall, colours the images share [17, 18], the image size (which enhances discriminability [19]), the number of images in the challenge set [20], the similarity of the images to each other (both in terms of semantics and syntax) [21, 22], the age of the viewer [23], the genre and task being carried out [24].

3. USING SIMPLE IMAGE TYPES IN AUTHENTICATION

The choice of image type for image-based authentication is crucial. Different image types have been trialled, with some demonstrating more efficacy than others: faces [10], abstract art [25], system provided or user-taken photographs [26, 27], icons [28], doodles [29] and Mikons [30]. A comparison between photographs, user photographs and doodles showed that doodles performed best in terms of memorability [31].

Our research has focused primarily on the use of what we call *simple image types*, of which doodles and Mikons are instances. These images have superior memorability because they have been provided by the users. As explained in [30], the actions engaged in during production of these images enhance memorability.

3.1. Experiences & Issues

One simple image type is a doodle, or simple sketch. A system using doodles as part of the authentication mechanism which controls access to a small community website has been running for 5 years now [29].

Users enroll by filling out a form which requires them to draw a doodle and provide other details. The doodle is manually scanned and the resulting image file uploaded. Doodles are very memorable but the success of such a scheme depends on the availability of a scanner during enrolment. Fig. (**1**) shows a collection of typical doodles, some of which are similar.

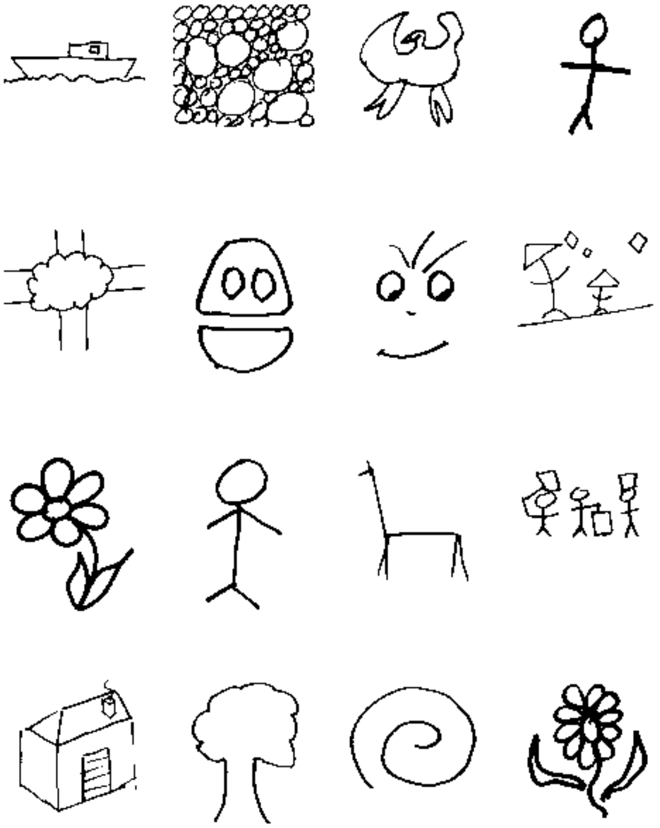

Fig. (1). A Collection of Doodles.

The logical next step was to allow the user to create a simple image using a browser based drawing tool. A mouse is not really precise enough to allow the user to produce a good freehand sketch, an electronic doodle, and so most browser based drawing tools let the user construct simple images from a collection of templates. Fig. (**2**) shows the Mikon engine, with an example of the templates shown on the right. We have used the Mikon tool[2] in an experiment reported in [30]. Mikon is short for My Icon, and these simple images have proved to be just as memorable as doodles. Fig. (**3**) shows a collection of typical Mikons.

3.2. Ways to Attack Recognition Based Systems

The aspect that makes recognition based systems easier to use: the fact that the “password” is displayed on the screen for easy identification also makes it easier to attack. There are a number of ways in which recognition based systems are vulnerable to attack:

- *Brute Force* — Recognition based systems help the user to remember their pass image by showing it to them, along with distractors. This will also help the attacker, since they know that one of the images shown will be the correct pass image. This is vulnerable to a brute force attack if the attacker is

[2] http://www.mikons.com

allowed to try a number of variations of image choices without hindrance. This can be thwarted by requiring the user to provide several pass images with a series of challenge sets, increasing the difficulty for the attacker. In one of our systems, for example, each user must provide four pass images, each part of a 4 x 4 challenge set. In addition, if authentication fails several times in a row then re-enrolment may be required.

- *Denial of Service* — The re-enrolment requirement used to guard against a brute force attack can also make a denial of service attack possible. An attacker can deliberately try to log in as someone else, failing enough times to force the victim to re-enroll. Thus, requiring re-enrolment to avoid a brute force attack should be used with care.

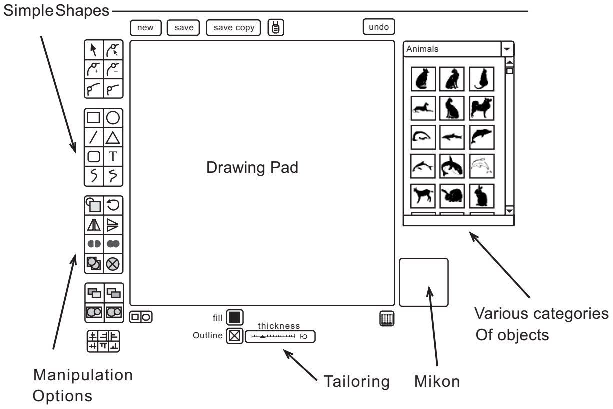

Fig. (2). Drawing Mikons

Fig. (3). A Collection of Mikons.

- *Intersection Attack* — If the system uses varying distractors ie. a different set each time the challenge set is displayed, the intruder can simply keep refreshing the display to see which image does not change. This is thwarted by fixing the distractors at registration.
- *Shoulder-Surfing* — Since the images are displayed and the user needs to identify the image, most often by clicking on it, it is possible for someone to observe which choices have been made. Some recognition-based systems allow users to enter their choice by means of the keyboard rather than the mouse, and this makes it much harder for an observer to identify the target image.
- *Social Engineering* — If the user is permitted to supply their own "secret" images, it might be possible for an intruder to guess which images belong to a particular person. This is a problem for images such as photographs but less so for minimal image types such as sketches (doodles) or Mikons. These are provided by the user but are much less likely to be easily attributed to the artist.

3.3. Choosing Distractors

There are a number of aspects to consider when choosing distractor images for a challenge set. The first question is the source of the distractor images. If they are selected from a system provided pool of "good" distractors then user supplied target images may well stand out as noticeably different. Thus we choose our distractors from the collection of target images provided by existing users.

Another aspect of choosing distractors is that of objectionable images. It would be a big drawback if one of the distractor images, seen every time the user logs on, was objectionable to him or her, for whatever reason. This is a difficult problem to confront, since what is objectionable to one person, as a distractor, may be perfectly acceptable to the person who supplied it as a target. This will be an issue for all systems that allow users to provide their own pass images. Asking an administrator to reject objectionable images when they are registered would place a large administrative burden on the system without solving the problem. There will always be images that an administrator finds acceptable but to which a user objects, based on individual perspectives. In our systems we resolve this problem by letting users ask for distractors to be replaced.

3.4. Avoiding Similar Distractors

The distractors to be used can thus be chosen at random from the larger set of potential distractors, but this has the disadvantage that distractors similar to the target image will be chosen from time to time. This could obviously cause problems for the user when they log in, since they might choose the similar looking distractor by mistake. On the other hand, if the challenge set contained two similar distractors, it would not confuse the user, since neither would be similar to the target. It could however help the attacker since the two similar distractors would not be the target.

In addition, simple image types exacerbate the similarity problem. In terms of doodles, we found that many users would draw a simple stick man. If one of the distractors were also a stick man, undeniably not *their* stick man but definitely a contender, users took longer to identify their doodle, and often chose the wrong one. Mikon images are also relatively simple, and the Mikon drawing tool offers a number of templates which users can incorporate into the Mikons.

Some users just chose one of the templates, without elaboration, as their pass image. This leads to a raised incidence of similarity. However, the simplicity of these images facilitates both the prevalence of the problem and the possibility of affecting a solution. Image similarity is judged based on visual similarity and subjective aspects such as semantic context, assigned labels and visual ability. According to the picture superiority effect [11], the viewer will have attached a label to the target image, which may be brought to mind during the search process. The search will therefore be guided by both semantic and perceptual similarity matchings.

We could try to eliminate similarity related to semantic category and assigned labels by classifying and labelling each image and then choosing each distractor from a different category and ensuring that labels differ. This is extremely time consuming and, unfortunately, shown to be unreliable [32].

On the other hand, we could automatically eliminate visual similarity by using an algorithm which detects it. In this case, a potential distractor image is chosen at random and checked automatically to see if it is similar to the target and any distractors already chosen. If it is, then it is discarded and another candidate chosen. This process continues until the challenge set is complete.

3.5. False Negatives and False Positives

The effectiveness of the similarity algorithm is measured by comparing its decisions with those of a human experimenter. The human determination of similarity is subjective and there is also the question of how similar two images have to be before they are classified as similar. In our experiments we used the following subjective definition of similarity. *Two images are similar if the experimenter thinks they would cause confusion to a user when he or she logs in.* No algorithm will give perfect results, and a failure by the algorithm, judged against the experimental decision, will be either a false negative or a false positive.

A *false negative* will occur when the algorithm decides that two images are not similar when in fact they are judged to be similar. This means that an image will be accepted as part of the challenge set when in fact it is similar to one of the existing images. This is undesirable.

A *false positive* occurs when two images are said to be similar when they are not. This would result in a distractor being rejected as similar, when in fact it could have been included in the challenge set. In general this will not cause a problem, since any dissimilar image can be used in the challenge set. There is nothing special about the falsely rejected image compared with the other images that are included in the challenge set.

There will be a problem if the false positive rate is too high and unduly restricts the choice of distractors. In an extreme example, if the algorithm classified all pairs of images as similar without actually examining them then it would be impossible to choose any distractors, since all possible distractors would be classified as similar to the target doodle. In a more realistic example, if the false positive rate were too high, it might be difficult to choose enough distractors. Also in this case, a small number of images will be clearly different from almost all other images and appear in a large number of challenge sets, potentially helping an attacker.

In summary, the algorithm should be tailored to produce as few false negatives as possible, while at the same time not making the false positive rate so high that it becomes difficult to choose a varied set of distractors.

4. SIMILARITY ALGORITHM

Details of the algorithm, together with experiments to test its validity have been reported in [32]. The algorithm measures three aspects of each simple image: the number of separate black regions (NB), white regions (NW) and number of joins (NJ) between lines. Two images are compared by calculating the weighted sum of the absolute differences of these three measures. If this weighted sum is below a given threshold (T) then they are classified as similar. In summary, $image_1$ and $image_2$ are classified as similar if

$$w_B|NB_1 - NB_2| + w_W|NW_1 - NW_2| + w_J|NJ_1 - NJ_2| < T$$

The experiment reported in [32] used doodle images. 100 challenge sets were constructed using the algorithm and another 100 by choosing the distractors at random. Several experimenters were asked to examine all the challenge sets and report any pairs of similar doodles.

That experiment clearly showed the effectiveness of the algorithm for selecting doodle distractors.

5. AN EXPERIMENT TO DETECT TOTAL SIMILARITY IN A COLLECTION OF SIMPLE IMAGES

In this paper we report an additional experiment with the following three goals:

- To determine from a human perspective how many pairs of doodles in a collection are similar.
- To use this information to investigate the effects of varying the weights and threshold in the algorithm on the false positive rate, false negative rate and available choice of distractors.
- To test the effectiveness of the algorithm with a collections of Mikons.

5.1. Subjective Similarity

The first part of the experiment was to determine, from a human perspective, which simple images appeared similar. Asking an experimenter to pass judgment on all possible pairs in a large enough set of images is not feasible. Preliminary experiments showed that an all pairs investigation of a set containing more that 50 simple images, and hence 1225 pairs, could not be carried out because of investigator fatigue. A set of 50 images also did not contain enough similar images to make this investigation worthwhile.

The approach adopted was to build a program that let an experimenter move the images in a collection around, grouping similar ones near to each other. Similar pairs were then labeled as such and recorded by the program.

We have a collection of 549 doodles and from these 300 were selected at random to be the subject of this investigation. 81 similar pairs were identified and out of the 300 doodles, 60 were similar to another doodles and 240 were unique. The experiment took around 2 hours, with most of the time spent rearranging the doodles.

The same approach was used with our collection of 2808 Mikons. 658 were chosen at random and 87 similar pairs identified. 70 Mikons were similar to another Mikon, while 588 were unique.

5.2. Experiments with the Algorithm

The second part of the experiment involved writing a program that checked all the possible pairs of images and compared the subjective experimental determination of similarity with that produced by the algorithm. It was relatively easy to change the weightings and threshold so that a large number of different combinations could be investigated.

The variables are the weights $w_B : w_W : w_J$, which must sum to 1, and the threshold T. The derived quantities are N, the number of false negatives, P the percentage of false positives and C, the minimum choice. N is a relatively small number compared with the 44,850 possible doodle pairs and the 216,153 possible Mikon pairs. P as a percentage corresponds to a much larger number of pairs. The choice for each image is the number of other images classified as not similar to it by the algorithm. C is the minimum of all these numbers.

Changing the weights corresponds to investigating the relative importance of NB, NW and NJ in the algorithm. Increasing T will increase P while decreasing N. C is inversely related to P, since increasing the false positive rate will decrease the choice. C is also dependent on the size of the set of images. The results as reported in Tables **1** and **2** specify $w_B : w_W : w_J$ and T and report N, P and C. This information is reported in a different way in Tables **3** and **4**. Here a target value of P is chosen and the value of T that produces the closest result reported. In some cases a linearly interpolated value of T is recorded when no actual value is close enough.

5.3. Single Measure Results

Firstly, the effects of NB, NW and NJ was examined in isolation using weights of 1:0:0, 0:1:0 and 0:0:1. The results are summarised in Tables **1** and **2**. A threshold of -1 classifies all doodles as different, corresponding to a random choice of distractors.

These results also appear in Tables **3** and **4**, which record the effects of targeting a false positive rate of 33% and 20% respectively. Two interesting conclusions can be drawn:

- The results for doodles and Mikons are very similar.
- The black region count is less effective than the others. This is best seen in Tables **3** and **4**, where the black region count produces a much higher level of false negatives than the others.

Table 1. Single Measure Results for Doodles

T	Black			White			Joins		
	N	P	C	N	P	C	N	P	C
-1	81	0	299	81	0	299	81	0	299
0	47	22	175	55	7	255	68	5	267
1	26	43	91	35	22	187	44	14	225
2	11	61	42	26	34	139	31	24	184
3	8	74	17	15	44	99	21	33	145
4	6	81	13	7	52	68	17	41	111
5	5	87	7	6	60	45	13	48	87

Table 2. Single Measure Results for Mikons

T	Black			White			Joins		
	N	P	C	N	P	C	N	P	C
-1	87	0	657	87	0	657	87	0	657
0	31	31	316	59	8	557	65	4	603
1	17	54	142	32	22	406	51	13	517
2	4	69	59	24	33	294	34	22	433
3	3	78	30	20	43	203	24	30	352
4	2	86	16	9	52	145	18	38	284
5	1	90	7	7	60	108	12	44	203

Table 3. Results with a False Positive Rate of 33%

Weights	Doodles			Mikons		
	N	T	C	N	T	C
1 : 0 : 0	37	0.5	133	31	0.0	316
0 : 1 : 0	24	2.0	139	24	2.0	294
0 : 0 : 1	21	3.0	146	24	3.0	352
0 : .25 : .75	18	3.4	135	20	3.6	302
0 : .50 : .50	18	3.0	132	19	3.2	303
0 : .75 : .25	21	2.8	130	23	2.8	294

Table 4. Results with a False Positive Rate of 20%

Weights	Doodles			Mikons		
	N	T	C	N	T	C
1 : 0 : 0	48	0.0	173	50	0.0	400
0 : 1 : 0	35	1.0	191	32	1.0	406
0 : 0 : 1	30	2.0	189	34	2.0	433
0 : .25 : .75	32	2.2	194	33	2.4	424
0 : .50 : .50	25	2.2	175	28	2.2	393
0 : .75 : .25	21	1.8	180	29	2.0	393
.17 : .66 : .17	33	1.67	188			

5.4. The Right Mix of NW and NJ

Following on from this, we investigated the effects of just including NW and NJ in different amounts, using weights of 0:.25:.75, 0:.5:.5, 0:.75:.25. These results are also reported in

Tables **3** and **4**. The last line in Table **4** uses the weights and threshold from [32], which also produced a false positive rate of 20%.

The simple conclusion to be drawn from these results is that the algorithm is not very sensitive to the values of w_W and w_J. Setting them both to 0.5 would be an appropriate choice.

5.5. Varying the Threshold

The choice of threshold T depends on the desired value for the minimum choice C. Empirical results for our systems, where we must provide 60 distractors for each user, suggests that C should be no less than 200. Other systems with a different number of distractors per user will have different criteria for C. Increasing C beyond this value will not produce a noticeably more varied set of distractors but will increase the number of false negatives, which is undesirable. The value of C also depends on the size of the set of images.

Looking at the results for our set of 300 doodles, we notice that a threshold of 3.0 (giving P=33%) reduced N to about 25% of the random choice value. Unfortunately C is around 130, which is too low. Using a threshold of 2.2 (P=20%) increases the choice to around 180 but also increases N to around 30% of the random choice value. A threshold of 2.0 is about right for a set of 300 images.

Our set of 658 Mikons generates plenty of choice even when T=3.2 (P=33%), which is not surprising given the increased number of images to choose from. In this case N equals 22% of the random choice value. Raising the threshold to 4.0 gives a choice just over 200, with N=16, corresponding to 18% of the random choice value.

6. CONCLUSION

This paper has discussed recognition based user authentication systems using pass images. The focus of our research is developing an algorithm for constructing a challenge set by choosing distractors that are not similar to the target image or each other. Details of the algorithm were presented in [32] where it was used with a collection of doodles.

This paper reports a new experiment to determine the amount of similarity in collections of doodles and Mikons, as determined by human experimenters. This information has been used to improve the algorithm and give a more comprehensive estimate of how much better the algorithm is than random choice.

Our new experiment showed that 80% of a collection of 300 doodles were unique, while 89% of a larger collection of 658 Mikons were unique. This indicates that a typical user is more likely to create a unique Mikon than a unique doodle. We cannot say more than this because of the different demographics of the doodle and Mikon users.

Our work with the algorithm shows that the black region count can be discarded and the white region count and number of joins combined with equal weights. In systems which produce 60 distractors per user, the best value for the threshold ranges from 2.0 for a small set of 300 images to 4.0 for a larger set of around 700 images. The threshold must be adjusted to provide an acceptable amount of choice when constructing challenge sets. When used with the larger set of images, the algorithm only generates around 20% of the undesirable false negatives compared with a random choice. Even with a small set of images, the algorithm still only produces around 30% false negatives when compared with a random choice.

REFERENCES

[1] Gaw S, Felten EW. Password management strategies for online accounts. In: SOUPS '06: Proceedings of the second symposium on Usable privacy and security. New York, NY, USA: ACM Press 2006; pp. 44-55.

[2] Ives B, Walsh KR, Schneider H. The domino effect of password reuse. Commun ACM 2004; 47(4): 75-8.

[3] Adams A, Sasse MA. Users are not the enemy: why users compromise security mechanisms and how to take remedial measures. Commun ACM 1999; 42(12): 40-6.

[4] Morris R, Thomson K. Password security: a case history. Commun ACM 1979; 22(11): 594-7.

[5] Sinclair S, Smith SW. The TIPPI point: towards trustworthy interfaces. IEEE Secur Priv 2005; 3(4): 68-71.

[6] Brown AS, Bracken E, Zoccoli S, Douglas K. Generating and remembering passwords. Appl Cogn Psychol 2004; 18(6): 641-51.

[7] Johnson ML. Biometrics and the threat to civil liberties. Computer 2004; 37(4): 90-2.

[8] Schneier B. Two factor Authentication: too little, too late. CACM 2005; 48(4): 136.

[9] Viega J. Security - Problem solved? Queue 2005; 3(5): 40-50.

[10] Brostoff S, Sasse A. Are Passfaces more usable than passwords? A field trial investigation. In: McDonald S, Ed. People and Computers XIV - Usability or Else! Proceedings of HCI 2000. Springer 2000; pp. 405-24.

[11] Paivio A. Why are pictures easier to recall than words? Psychon Sci 1968; 11(4): 137-8.

[12] Renaud K. Guidelines for designing graphical authentication interfaces. Int J Comput Secur 2009; 3(1): 60-85.

[13] Woodman GF, Luck SJ. Electrophysical measurement of rapid shifts of attention during visual search. Nature 1999; 400(6747): 867-9.

[14] Horowitz T, Wolfe J. Memory for rejected distractors in visual search? Vis Cogn 2003; 10(3): 25798.

[15] Humphreys GW, Quinlan PT, Riddoch MJ. Grouping processes in visual search: effects with single and combined feature targets. J Exp Psychol 1989; 118(3): 258-79.

[16] Wolfe JM, Oliva A, Horowitz TS, Butcher SJ, Bompas A. Segmentation of objects from backgrounds in visual search tasks. Vision Res 2002; 42(28): 2985-3004.

[17] Yokoi K, Uchikawa K. Color category influences heterogeneous visual search. J Opt Soc Am 2005; 22(11): 2309-17.

[18] Rogowitz BE, Frese T, Smith JR, Bouman CA, Kalin E. Perceptual image similarity experiments. In: Human Vision and Electronic Imaging III. Proceedings of the SPIE, 3299. San Jose, CA 1998; pp. 576-90.

[19] Ben-Av MB, Sagi D. Visual attention and perceptual grouping. Percept Psychophys 1992; 52(3): 277-94.

[20] Bricolo A, Gianesini T, Fanini A, Bundesen C, Chelazzi L. Serial attention mechanisms in visual search: a direct behavioural demonstration. J Cogn Neurosci 2002; 14(7): 980-93.

[21] Duncan J, Humphreys GW. Visual search and stimulus similarity. Psychol Rev 1989; 96(3): 433-58.

[22] Sato TR, Watanabe K, Thompson KG, Schall JD. Effect of target-distractor similarity on FEF visual selection in the absence of the target. Exp Brain Res 2003; 151: 356-63.

[23] Ball KK, Beard BL, Roenker DL, Miller RL, Griggs DS. Age and visual search: expanding the useful field of view. J Opt Soc Am 1988; 5(12): 2210-9.

[24] Squire DM, Pun T. A Comparison of human and machine assessments of image similarity for the organization of image databases. In: Scandinavian Conference on Image Analysis. Lappeenranta, Finland 1997.

[25] Dhamija R, Perrig A. De´ja` vu: A user study using images for authentication. In: Proceedings of USENIX Security Symposium. Denver, Colorado 2000; pp. 45-58.

[26] Pering T, Sundar M, Light J, Want R. Photographic authentication through untrusted terminals. Secur Priv 2003; 2(1): 30-6.

[27] Tullis TS, Tedesco DP. Using personal photos as pictorial passwords. In: CHI2005. Portland, OR, USA 2005; pp. 1841-4.

[28] Komanduri S, Hutchings DR. Order and entropy in picture passwords. In: Proc Graphics Interface 2008. Windsor, Canada 2008; pp. 115-22.

[29] Renaud K. A visuo-biometric authenticaton mechanism for older users. In: Proc British HCI 2005. Sept 5-9, Edinburgh 2005; pp. 167-82.

[30] Renaud K. Web Authentication using Mikon Images. In: World Congress on Privacy, Security, Trust and Management of e-Business. Saint John, New Brunswick, Canada 2009.

[31] Renaud K. On user involvement in production of images used in visual authentication. J Vis Lang Comput 2009; (1): 1-15.

[32] Poet R, Renaud K. A mechanism for filtering distractors for doodle passwords. Intern J Pattern Recognit Artif Intell 2009; 23(5): 1005-29.

Received: May 27, 2009 Revised: September 9, 2009 Accepted: September 10, 2009