A shoulder-surfing-resistant image-based authentication system with temporal indirect image selection

Takumi Yamamoto[1,3], Yuko Kojima[2], Masakatsu Nishigaki[1,4]
[1]Graduate School of Science and Technology, Shizuoka University, 3-5-1, Johoku, Naka, Hamamatsu, Japan
[2]Graduate School of Informatics, Shizuoka University, 3-5-1, Johoku, Naka, Hamamatsu, Japan
[3]Research Fellow of the Japan Society for the Promotion of Science (DC1)
[4]Japan Science Technology and Agency, CREST
E-mail: f5745037@ipc.shizuoka.ac.jp, gs07027@s.inf.shizuoka.ac.jp, nisigaki@inf.shizuoka.ac.jp

Abstract – *Although image-based user authentication systems have gotten a lot of attention recently to reduce the burden of memorizing passwords, they can be vulnerable to shoulder-surfing attacks. To overcome this problem, shoulder-surfing-resistant image-based authentications with indirect image selection (indirect image-based authentication, or I-IBA) have been proposed. However, because they spatially arrange image-sets over a wide space, two problems with these schemes are that they require a large screen and that it is difficult for authorized users to find and select their pass-images in the wide area. Therefore, by temporally arranging the image-sets, we implemented another indirect image-based authentication scheme (temporal I-IBA, or TI-IBA) that is not constrained by the screen size and makes it easy for authorized users to recognize their pass-images. We conducted fundamental experiments to study the feasibility of TI-IBA.*

Keywords: image-based user authentication systems, shoulder-surfing, indirect image selection, I-IBA, TI-IBA

1 Introduction

Although password-based systems are now widely used in all kinds of authentication, they have some shortcomings in that they neglect human limitations. Most users of password-based systems fail to change their passwords frequently and prefer to use simple passwords since it is not easy to memorize the long random strings that make strong passwords. The shortcomings of password-based systems have been discussed [1].

To cope with these shortcomings, image-based user authentication systems using graphical passwords, or pass-images, instead of passwords have been studied. Authentication based on the recognition of pass-images [1-3] is especially effective since people are much more efficient at recognizing previously seen images than at accurately recalling passwords. However, such systems have a different problem: since pass-images must be displayed for each authentication trial, the systems are vulnerable to observing attackers (so-called "shoulder-surfers"). Shoulder-surfing attacks can be a serious problem for image-based authentication systems since the use of images makes it easier not only for authorized users but also for shoulder-surfers to see and memorize pass-images.

To overcome this problem, shoulder-surfing-resistant image-based authentications with indirect image selection (indirect image-based authentication, or I-IBA) has been proposed [4,5]. However, because these schemes spatially arrange image-sets for indirect image selection on a wide field, they have two main shortcomings: they require a large screen and it can be difficult for authorized users to find their pass-images among the wide space. Therefore, by temporally presenting the image-sets, we developed a shoulder-surfing-resistant scheme that is not as constrained by screen size and is easy for authorized users to recognize their pass-images. As described in greater detail in section 3, our temporal indirect image-based authentication (TI-IBA) scheme displays images in sequence, like a slide-show, and the user selects the slide-show that contains his or her own pass-image(s) from among several individual slide-shows. With this display method, indirect image selection is possible without using a large screen.

In conventional image-based authentication systems, there are N images in the authentication window, while in TI-IBA, there are N image-sets (slide-shows) in the authentication window. Each image-set contains M images, and the M images are sequentially and repeatedly presented like a slide-show. In this paper, the switching rate of slide-show is empirically set as around ten times per second.

One out of the N image-sets has the user's pass-image(s). The authorized user knows his or her pass-image(s), so it is easy for the authorized user to recognize his or her pass-image and select the slide-show that contains it. At the same time, although shoulder-surfers may be able to observe the slide-show (image-set) selected by the authorized user, it is difficult for them to identify the specific pass-image(s) within the set.

In the next section, we discuss the drawbacks of conventional I-IBA. We discuss our temporal I-IBA (TI-IBA) in section 3. Then we describe experiments to evaluate the

effect of our system in section 4. Finally, we discuss our future work and our conclusions in section 5.

2 Related Work

In this section, we introduce conventional indirect image-based authentication (I-IBA) scheme proposed by Sobrado et al. [4,5] and present its shortcomings.

The system displays many images (icons) which are randomly arranged on screen as a challenge. The user has to find his or her pass-images (pass-icons) chosen, and mentally create a convex hull formed by all of the user's pass-images presented on the screen. Then, the user sends back the response by clicking inside the convex hull. This task is repeated several times to authenticate the user. Fig. 1 is an example of an authentication screen in Sobrado's scheme.

Figure 1 Authentication screen in Sobrado's scheme

Because user doesn't click the pass-images directly, it is difficult for shoulder-surfers to identify the pass-images even if they observe and record the authentication process. However, if the number of images on the screen is small, the chance of clicking a correct area by guesswork increases.

Thus, this kind of scheme that arranges many images in space needs a wide authentication screen. Moreover, it can be difficult and burdensome for an authorized user to find the pass-images (pass-icons) in a large, crowded space.

3 Proposed system (TI-IBA)

To overcome these drawbacks of conventional I-IBA, we propose another shoulder-surfing-resistant image-based authentication scheme using temporal indirect image selection (temporal indirect image-based authentication, or TI-IBA).

3.1 Concept of TI-IBA

Conventional I-IBAs [4,5] arrange many images spatially; our TI-IBA presents these images sequentially (temporally), like a slide-show.

The slide-show is presented to the authorized user, and the user must answer whether or not the slide-show contains his or her pass-image(s). This is the basic idea of the proposed system. Fig. 2 is a basic overview of the system.

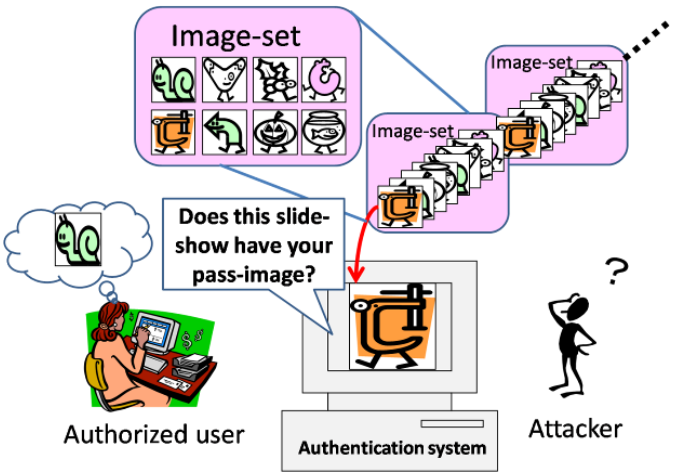

Figure 2 Basic overview of proposed system.

In this basic system, however, even an attacker has a fifty percent chance of giving a correct response by guessing randomly. Moreover, it is impractical to display a large number of images as one slide-show, since it takes a longer time for users to view all images.

So, to cope with these issues, we use decoys as conventional image-based authentication systems do [1-3] (Fig. 3). That is, the system prepares N image-sets. Each image-set has M images, and these M images are sequentially and repeatedly presented as a slide-show. In other words, the N image-sets are presented as N individual slide-shows, respectively, The N slide-shows are displayed together on the authentication screen. In this paper, the switching rate of slide-show is empirically set as around ten times per second.

One out of the N image-sets has the user's pass-image(s). The authorized user knows his or her pass-image(s), so it is easy for the authorized user to recognize his or her pass-image and select the slide-show that contains it. At the same time, although shoulder-surfers may be able to observe the slide-show (image-set) selected by the authorized user, it is difficult for them to identify the specific pass-image(s) within the set. Fig. 4 is a more detailed overview of the TI-IBA.

Figure 3 Example of the authentication screen of conventional image-based authentication [3].

To put it differently, we changed the conventional image-based authentication system in which the user selects a pass-image from among N images to a system in which the user selects a slide-show which contains the pass-image(s) among N slide-shows.

3.2 Authentication scheme

TI-IBA has 2 phases: registration and authentication.

Registration phase. This has four steps.

1. The system presents several images to the user.
2. The user selects P images to use as pass-images.
3. The user memorizes those selected pass-images.
4. The system registers the P images as that user's pass-images.

Authentication phase. This has three steps.

1. The system prepares N image-sets $\{S_i \mid i=0\sim N-1\}$ of M images $\{I_{ik} \mid i=0\sim N-1, k=0\sim M-1\}$. One out of the N image-sets contains one or more (at most P) pass-images.
2. The system displays N image-sets on an authentication screen, in which each image-set is displayed as individual slide-show. That is, users see N slide-shows on the screen, where every images $\{I_{ik} \mid k=0\sim M-1\}$ in the i-th image-set S_i are presented sequentially and repeatedly in the i-th slide-show.
3. The user identifies which slide-show contains his or her pass-image(s) from among the N slide-shows, and selects the slide-show to authenticate him or herself.

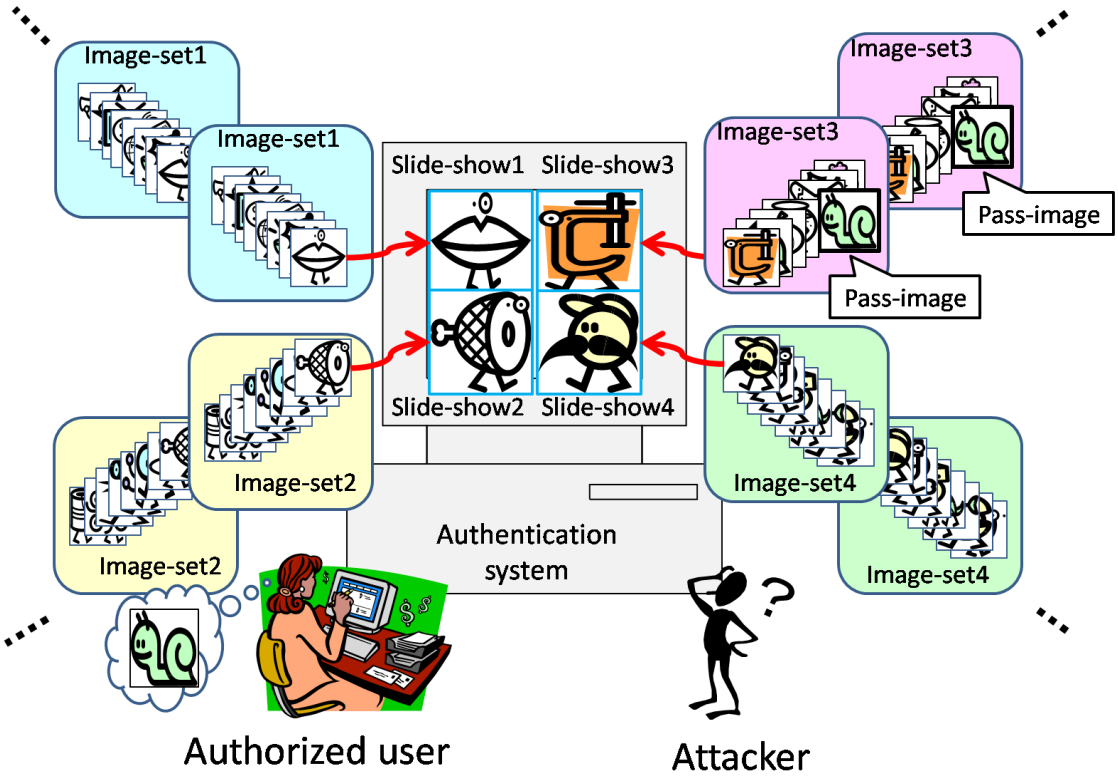

Figure 4 Overview of proposed system

The number of pass-images P, the number of slide-shows (image-sets) N, the number of images in each slide-show M, and the number of repetitions (rounds) of authentication phases Q are adjusted to meet the required security level for applications. Fig. 5 is an example of an authentication screen, where the number of slide-shows (N) is four, and the number of images in each slide-show (M) is six. Four images presented on the screen are continuously changed at fixed intervals V, respectively. In the example of Fig. 5, the authentication screen is changed in the following order: (a)→(b)→(c)→(d)→(e)→(f)→(a)→(b)→.


(a) $T(t)=T_0+6tV$


(b) $T(t)=T_0+(6t+1)V$


(c) $T(t)=T_0+(6t+2)V$


(d) $T(t)=T_0+(6t+3)V$


(e) $T(t)=T_0+(6t+4)V$


(f) $T(t)=T_0+(6t+5)V$

Figure 5 Example of an authentication screen

4 Evaluation Experiments

We did experiments to evaluate the effectiveness of our TI-IBA. The examinees in the experiments were six volunteers who were college students.

4.1 Authentication by legitimate users

In terms of memory tasks, TI-IBA utilizes the human ability to recognize previously seen images. The ability to recognize previously seen images has been well studied by many cognitive psychologists. In general, it is much easier to recognize images than to recall the same information from memory without help [6]. Moreover, recognition tasks are less affected by aging than recall tasks [7]. In studies of conventional image-based authentication system [1-3], mitigation of users' cognitive load of memorizing secret information has been reported by using pass-image instead of password.

Although our TI-IBA uses N slide-shows instead of N images, the difference in display method will have an affect not on its memory load to memorize pass-images but on its cognitive load to recognize pass-images. In other words, there is no significant difference in memory load between TI-IBA and conventional image-based authentication systems. Thus, we focus on the recognition task of TI-IBA, and then verify whether or not the cognitive load to recognize pass-image(s) from among several individual slide-shows is sufficiently small.

a) Experimental procedure

In this experiment, we varied three parameters N, P, and V to evaluate their effects, trying all possible combinations of them. In this experiment, the parameter M and Q were fixed at twenty and one, respectively.

N: The number of slide-shows displayed on the authentication screen. This paper hereafter refers to a system in which N individual slide-shows is displayed as "N-alternative authentication". In this experiment we use N={4, 9}.

P: The number of pass-images the authorized user has to memorize. One out of N slide-shows (image-sets) contains all the P pass-images. In this experiment we use P={1, 2, 3}.

V: The switching interval (in milliseconds) of the slide-show. In other words, the display speed of slide-show is 1/V images per millisecond. In this experiment we use V={100, 150}.

Taking the parameter settings N=4, P=3 and V=100 as an example, the experimental procedure was as follows.

(i) The system prepared 77 unique decoy images (N×M - P images).
(ii) The 77 images were divided into 4 groups: 20, 20, 20, and 17 images.
(iii) 3 pass-images were inserted randomly into the group that consisted of 17 images.
(iv) Then the system assembled 4 image-sets of 20 images (S_0, S_1, S_2, S_3). Each image contained in S_i (i=0~3) is indicated as I_{ik} (i=0~3, k=0~19).
(v) The system chose an integral number j randomly from 0 to 19.
(vi) The system extracts 4 images I_{ij} (i=0~3) from each image-set S_i (i=0~3), and display these 4 images on the authentication screen as in Fig. 5.
(vii) After a lapse of one hundred millisecond, the system assigned j+1 (mod 20) to j and displayed updated images I_{ij} (i=0~3).

Table 1 authentication result (N=4, V=100)

	# of pass-images displayed (P)					
	P = 1		P = 2		P = 3	
subject	success rate	time [sec]	success rate	time [sec]	success rate	time [sec]
a	100.0%	2.27	100.0%	2.27	100.0%	1.48
b	70.0%	5.40	100.0%	2.09	100.0%	2.27
c	90.0%	9.40	100.0%	2.58	100.0%	3.37
d	100.0%	2.96	80.0%	4.38	100.0%	2.03
e	100.0%	2.31	100.0%	1.78	100.0%	1.69
f	100.0%	1.86	100.0%	2.15	100.0%	1.72
average	93.3%	4.03	96.7%	2.54	100.0%	2.09

Table 2 authentication result (N=4, V=150)

	# of pass-images displayed (P)					
	P = 1		P = 2		P = 3	
subject	success rate	time [sec]	success rate	time [sec]	success rate	time [sec]
a	100.0%	2.67	100.0%	2.74	100.0%	1.97
b	100.0%	4.66	100.0%	3.08	100.0%	1.84
c	100.0%	7.46	100.0%	2.51	100.0%	2.45
d	90.0%	3.87	100.0%	4.96	100.0%	2.41
e	100.0%	3.01	100.0%	1.95	100.0%	1.86
f	100.0%	3.43	100.0%	2.02	100.0%	2.37
average	98.3%	4.18	100.0%	2.88	100.0%	2.15

Table 3 authentication result (N=9, V=100)

	# of pass-images displayed (P)					
	P = 1		P = 2		P = 3	
subject	success rate	time [sec]	success rate	time [sec]	success rate	time [sec]
a	100.0%	4.76	100.0%	5.78	100.0%	6.43
b	50.0%	4.27	100.0%	4.88	100.0%	4.41
c	100.0%	13.34	100.0%	4.11	100.0%	6.53
d	90.0%	13.11	100.0%	5.08	100.0%	8.13
e	100.0%	2.67	90.0%	10.12	100.0%	5.39
f	100.0%	3.71	100.0%	4.33	90.0%	5.12
average	90.0%	6.98	98.3%	5.72	98.3%	6.00

Table 4 authentication result (N=9, V=150)

	# of pass-images displayed (P)					
	P = 1		P = 2		P = 3	
subject	success rate	time [sec]	success rate	time [sec]	success rate	time [sec]
a	100.0%	2.11	100.0%	3.60	100.0%	2.42
b	70.0%	5.84	100.0%	5.54	100.0%	3.04
c	100.0%	14.05	90.0%	4.45	100.0%	4.35
d	90.0%	7.18	100.0%	11.02	100.0%	9.97
e	100.0%	4.13	100.0%	7.83	100.0%	6.28
f	90.0%	2.25	100.0%	4.13	100.0%	2.92
average	91.7%	5.93	98.3%	6.10	100.0%	4.83

(viii) The previous steps (vii) were repeated until the user clicked an image (slide-show) among the 4 images (slide-shows). Note that the user can click whenever the slide-shows are running.

All subjects (authorized users) were required to attempt authentication in all combinations of system parameters (N, P, V).

b) Experimental result

Table 2 lists the results of the experiments. Subjects had shown better performance in success rate and selection time with the four-alternative system (N=4) than the nine-alternative system (N=9).

Selection time for the nine-alternative system became longer as the slide-show speed increased (namely, as the switching interval V decreased), while that for the four-alternative system became shorter as the slide-show speed increased. Because the number of images that the user has to recognize in one glance was small in the four-alternative system, the user was able to find the correct pass-image(s) even when the slide-show speed became faster.

Moreover, as the number of pass-images was increased, both the success rate and the selection time improved. Therefore, it is hypothesized that the increase of the number of pass-image causes a reduction in cognitive load. The examinees told us, however, that they tended to look for one particular image that had distinguishing features. This means that all the pass-images will not always have an effect on reduction of the cognitive load of authorized users. Instead, it may be possible to further reduce the cognitive load of authorized users by selecting pass-images appropriately.

In this experiment, we used Q=1 which means a very simple authentication system where the user carried out four or nine-alternative selection only one time. For more practical use, the user has to repeat the four or nine-alternative selection several times with different combinations of decoy images. For instance, when we use the four-alternative system in place of a 10000 possible combination PIN, the user needs to repeat it at least seven times. For nine-alternative system, repeat it at least five times. A simple estimation of the selection time in such a practical environment is that it would take 14~29 seconds to repeat the four-alternative selection seven times, and 25~35 seconds to repeat the nine-alternative selection five times. Compared to this, in Sobrado's study [5] where a scaled-down setting was used to determine whether novices could learn, remember, and authenticate successfully using Sobrado's scheme, the average time needed to authenticate was more than 70 seconds.

Thus, cognitive load in temporal indirect image selection in our TI-IBA is expected to be smaller than that of conventional I-IBA (Sobrado's scheme).

4.2 Experiment for shoulder-surfer

TI-IBA aims not only at increasing the usability for the authorized users by temporal indirect image selection, but also at providing a comparable level of robustness against shoulder-surfing attacks with conventional indirect image-based authentication schemes. In this paper, we assume that an observing attacker, or shoulder-surfer, has relatively high memory (e.g., a video camera). We checked how difficult it is for shoulder-surfer to identify the pass-images obscured by means of TI-IBA under this extreme observation condition.

a)Experimental procedure

In this experiment we assume that an attacker can record all M images contained in image-set selected by an authorized user. That is, the attacker will obtain X image-sets of M images by repeating shoulder-surfing X times. Then the attacker can eliminate the candidate of the pass-image(s) by finding the images not common to all image-sets which were selected by the authorized user at each authentication process.

By increasing X one by one, we can evaluate how many times the subject (shoulder-surfer) needs to observe (record) the authentication process to identify the authorized user's pass-image(s).

In this experiment we used the simplest system in the experiment of section 4.1: (N, P, M, Q) = (4, 1, 20, 1). Since we assume that an attacker can record all images contained in an image-set selected by an authorized user, switching interval V of the slide-shows is a don't-care in this experiment.

Using the same notation as section 4.1(a), the experimental procedure was as follows;

Step 1: The examiner prepares one pass-image and 79 decoy images.
Step 2: 4 image-sets (S_0, S_1, S_2, S_3) of 20 images were randomly created from the 80 images (one pass-image and 79 decoy images). Only one image-set had one pass-image.
Step 3: An image-set with pass-image is color-printed on paper.
Step 4: The paper is presented to the subject (shoulder-surfer).
Step 5: The subject is required to identify the pass-image from the given paper(s).
Step 6: Steps 2~5 are repeated using the same 80 images until the attacker can identify the pass-image. The more papers the subject is given, the more candidates he or she can eliminate.

b) Experimental results

Table 5 lists the results of the experiments. Table 5 indicates the number of candidates the subject could narrow all the candidates of pass-images down to as the number of shoulder-surfing X increased.

Table 5 # of candidates the subject could narrow all candidates down to by multiple shoulder-surfings

subject	# of shoulder−surfings			
	1 [time]	2 [time]	3 [time]	4 [time]
a	20	6	2	1
b	20	4	1	1
c	20	2	1	1
d	20	4	1	1
e	20	7	3	1
f	20	6	2	1
average	20	4.83	1.67	1

From these results, four times viewing the complete record of the authentication task were enough for shoulder-surfing attackers to identify the pass-image in the case of (N, P, M, Q)=(4, 1, 20, 1). These results corresponded approximately to our theoretical evaluation (omitted for space). This means our proposed TI-IBA still is not robust enough against a (strong) shoulder-surfing attack such as a video camera recording.

However, an optimistic interpretation is that it is essential for a shoulder-surfer to use several video camera recordings to identify all of the pass-images obscured by means of TI-IBA. Therefore, our proposed temporal indirect image selection is expected to increase the robustness of image-based authentication system against shoulder-surfing attack to the same level as conventional indirect image selection (Sobrado's scheme [4,5]) does.

Of course there are various threats (e.g. intersection attack, exhaustive attack, etc.) as well as shoulder-surfing attack to image-based authentication. Robustness against those attacks of TI-IBA is highly dependent upon the system parameters N, P, M, V, and Q. In a more practical system, appropriate parameter settings are an essential factor. We have not explored this yet and leave this as an area for future work.

5 Conclusions and Future Work

In this paper, we proposed a shoulder-surfing-resistant image-based authentications scheme TI-IBA that presents image-sets not spatially but temporally. The TI-IBA is less constrained by screen size and easier for authorized users to recognize their pass-images.

Moreover, we implemented a prototype TI-IBA system and did experiments to evaluate its effectiveness. In the

experiments, we found that the cognitive load of our TI-IBA was expected to be smaller than that of conventional I-IBA (Sobrado's scheme [4,5]), and that it was required for shoulder-surfers to use several video camera recordings to identify all of the pass-images obscured by means of TI-IBA.

Although our proposed system was still insufficient, we believe our results represent a positive step toward making image-based authentication systems feasible. We will explore the most appropriate parameter settings (N, P, M, V, Q) for further reduction of the cognitive load for the user and increase of the robustness against various threats.

Acknowledgements

We are deeply grateful to Mr. Kenta Takahashi of Hitachi, Ltd., Systems Development Laboratory, whose comments and suggestions were innumerably valuable throughout our study. This work was partially supported by a grant-in-aid for JSPS Fellows (No.20-6290) and Secom Science and Technology Foundation, Japan.

References

[1] R. Dhamija, and A. Perrig, "Deja Vu: A User Study Using Images for Authentication", 9th USENIX Security Symposium, pp.45-58, 2002.

[2] T. Takada and H. Koike, "Awase-E: Image-Based Authentication for Mobile Phones Using User's Favorite Images", LNCS 2795, Human-Computer Interaction with Mobile Devices and Services, pp. 347--351, Springer, 2003.

[3] T. Pering, M. Sundar, J. Light, and R. Want, "Photographic Authentication through Untrusted Terminals", IEEE Pervasive Computing, Vol 2. No 1, pp.30-36, 2003.

[4] L. Sobrado, and J.-C. Birget, "Graphical passwords", The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, Vol.4, 2002.
http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm

[5] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme", In Proc. AVI'06, pp 177-184, 2006.

[6] J. Nielsen, "Usability Engineering", Academic Press, 1993.

[7] D. Schofield, and B.A. Robertson, "Memory storage and aging", Canadian Journal of Psychology, 20, 220-236, 1996.