A Cued-Recall and Emotion Classification Graphical Password Authentication Scheme

Danilo E. Vieira[1], Tonny L. Mesquita Abreu[1], Max E. Vizcarra Melgar[1], Luz A. M. Santander[2]
[1]Department of Computer Engineering, Centro Universitário IESB, Brasília, DF - Brazil
[2]Department of Statistics, Universidade Federal Fluminense, Rio de Janeiro - Brazil
E-mails: [1]danilo_espidola@hotmail.com, [1]tonnyluiz00@gmail.com, [1]maxvizcarra@ieee.org, [2]luzamandams@est.uff.br

***Abstract*—This paper presents an alternative visual authentication scheme with two secure layers for desktops or laptops. The first layer is a recognition-based scheme that addresses human factors for protection against bots by recognizing a Captcha and images with specific patterns. The second layer uses a clicked based Cued-Recall graphical password scheme for authentication, it also exploits emotions perceived by humans and use them as decision factor. The proposed authentication system is effective against brute-force, online guessing and relay attacks. We believe that the perception of security is enhaced using human emotions as main decision factor. The proposed scheme usability was tested using the Computer System Usability Questionnaires, results showed that it is highly usable and could improve the security level on ATM machines.**

***Index Terms*—Authentication; Graphical password; Usable security; Pattern.**

I. Introduction

A fundamental task on information security is the authentication of an authorized user on an operating system. Alphanumeric password is the most used authentication method on desktop/laptop operating systems. This scheme has several limitations and weakness [1], such as the use of easy guessing memorable strings (which do not reach the maximum entropy [2]), online guessing and dictionary attacks [3], [4]. Several objective experiments in cognitive psychology show that users tends to forget or miss a password composed by pseudorandom sequences of text symbols [3]. The human limitation performance reduces the usability level of the text password scheme.

Graphical authentication techniques have been deeply studied in the last decade [4]. Graphical password schemes are highly usable because of the ubiquity of graphic interfaces and available input devices such mouse or touch-screen. Given the graphical authentication usability level, people prefer to memorize graphical patterns than text passwords.

A Recognition-Based scheme is a Graphical Password method, it aims to identify one or a group of images in a portfolio [5]. The selected images have a common visual pattern detected by the user. The user is authenticated and the system is unlocked, if and only if, the observer selects the correct set of images. Three tipical examples of Recognition-Based methods are: 1) The PassFaces algorithm [5], where the user selects known faces from a set of generic faces and their locations are permuted on each round. 2) Déja Vù is another example, it uses a large set of random-art images. A set of memorized images have to be selected as authentication prove [6]. Figure 1 shows an example of Random Art images used on the Déja Vù algorithm. 3) Cognitive Authentication, where the user selects images forming a path [7]. The path is computed beginning on the top left image and finishing on the right-most end or bottom end image, the moving transition goes down if the user stand on a picture that is part of a set of known images or goes right if is not.

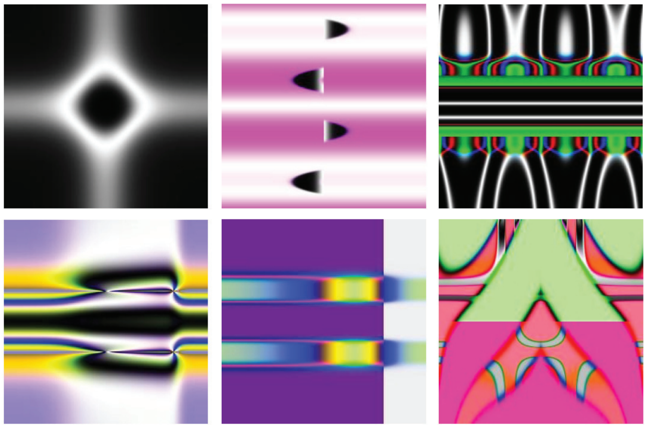


Fig. 1. Examples of a recognition-based algorithm [6].

Another Graphical Password method is the Cued-Recall scheme. An example of this scheme is the PassPoints algorithm [8], in this scheme, a user selects memorized regions of an image as password and re-clicks the same sequence on authentication. The Recognition-Based and Cued-Recall schemes were broken with dictionary attack of 2^{13} to 2^{16} and 2^{26} to 2^{35} entries, respectively [9], [5].

A text Captcha (Completely Automated Public Turing test to tell Computers and Humans Apart) is an image recognition method that relies on the difficulty of solving hard Artificial Intelligence problems [10], [11]. The security level of Captchas has been widely studied, their recognition probability relies on the expensive computationally cost and the hard combinatorial output sequences [5].

Image emotion analysis is very challenging, mainly due to the lack of temporal information and the inaccurate interpretation of a meaningful picture. The emotion diagnostic is decided based on empirical concepts from psychology and art theory [12]. Images with several objects, concepts and emotional regions have less probability to be correctly decided [13].

In the ideal scenario, users should perceive that Graphical Password schemes are secure systems. The perception of security is strongly associated with the notion of trust [14], [15] and less the notion of security itself. The lack of trust is the principal reason why many consumers and companies choose not to use some security programs [14]. Users do not trust on authentication programs because they are usually based on complex mathematical problems, which are executed with no (or very little) user interference [16].

In this paper we propose an alternative two-layer Graphical Password scheme. The first layer uses the Captcha and Recognition-Based scheme for bot prevention. The other layer uses a Cued-Recall scheme with emotion image decision as final authentication step. The proposed scheme was developed on the OpenCV programming environment [17]. This paper is divided as follows. In Section II, we describe the Graphical Password scheme and its usability evaluation. In Section III, we show the results of the proposed system. Finally, in Section IV we present our conclusions.

II. Graphical Password Authentication Scheme

In this section, we present the 2 sequential graphic authentication layers. In particular, we aim to satisfy the following requirements:

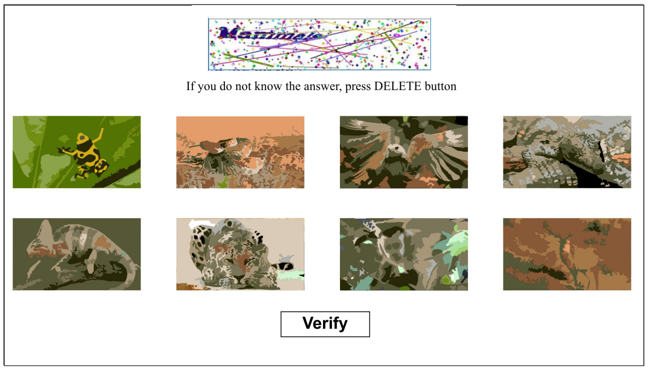
- Captcha security method.
- Recognition-Based method.
- Recognition of emotional images.
- Cued-Recall security layer.

The proposed system is designed to be triggered as authentication requirement of an application. The only input interface is the mouse. Each graphical security layer only tolerates a single error authentication. If a second error occurs or a keyboard is pressed, the system shuts down (i.e. not restarted). The shutdown procedure is performed using the keyboard and mouse control on OpenCV. Password settings are registered on the installation process.

A. Captcha and Recognition-Based Image Layer

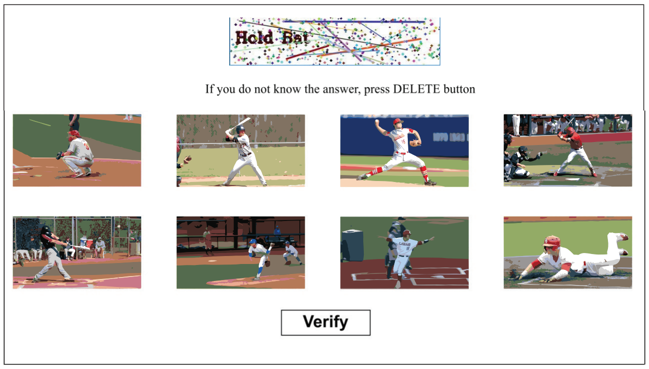
The Recognition-Based layer shows a single image for authentication, the image height and width is projected to be equal than the screen size. A Captcha and a set of vector images, which are more difficult to interpret for bots, are shown in the main image.

The user has to interpret the Captcha message, which is used as main characteristic on the set of images. Once the user reads Captcha message, a subset of n of m ($n \leq m$) vectored images is chosen according the interpretation of the Captcha message. If the user selects the correct images (on the first or second attempt), the system pass to the second security layer. The Captcha content and its respective images are pseudorandomly changed on every attempt. Figures 2 and 3 show examples of the first security layer with different subjects to choice.



If you do not know the answer, press DELETE button

Fig. 2. Example of first authentication layer with images of animals as subject.



If you do not know the answer, press DELETE button

Fig. 3. Example of first authentication layer with images of sports as subject.

Given than Captcha attacks are computationally expensive and combinatorial hard [5], the attacker bot will not be able to understand the Captcha message, thus, the probability of a successful authentication (A) on layer 1 is shown in Equation 1.

$$P(A) = P(G_1 \cap G_2) = \frac{n!(m-n)!}{(m+1)!} \quad (1)$$

where G_1 is the event of correctly select the amount of shown images and G_2 is the event of match the correct images.

Figures 2 and 3 show examples of the first authentication layer with $m = 8$ images and $n = 3$ correct images. In Figure 2, the correct mammals images are monkey, jaguar and deer. In Figure 3 the correct sport images are pictures with a player holding the bat.

B. Emotional and Cued-Recall Image Layer

The second layer is shown after the successful authentication on layer 1. In this layer, the user selects regions of a single image for authentication. The image height and width is projected to be equal than the screen size. The authentication process uses an emotional and cued-recall graphic password. The main image has $i \times j$ rectangles divided by grids, each rectangle is partitioned in 4 subrectangles. Each subrectangle contains an (pseudorandom ordered) emotional picture with the following subjects: Amusement, Anger, Excitement, and

Sadness. These emotions categories are used on several emotion classification methods [18].

For a successful authentication, the user selects as a previous defined password, $q \geq 3$ click-based rectangles within an emotion category, the rectangle selection (i, j) can be repeated. Only two authentication attempts are allowed, if the user failures twice, the computer is shuttled down. Figures 4 shows an example of the authentication process on an image with $i = 3$ and $j = 4$ rectangles. In this example, the user selects as password the following sequence: (1) first selected rectangle with sadness category; (2) second selected rectangle with excitement category; (3) third selected rectangle with anger category; and (4) fourth selected rectangle with sadness category.

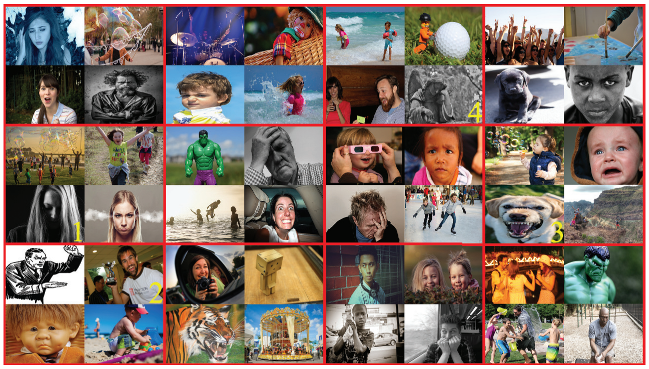


Fig. 4. Example of second authentication layer process with $(i = 3) \times (j = 4)$ rectangles.

Figures 5 shows another example of the second authentication layer with 20 rectangles $(i = 4) \times (j = 5)$ and a total of 80 emotion images.

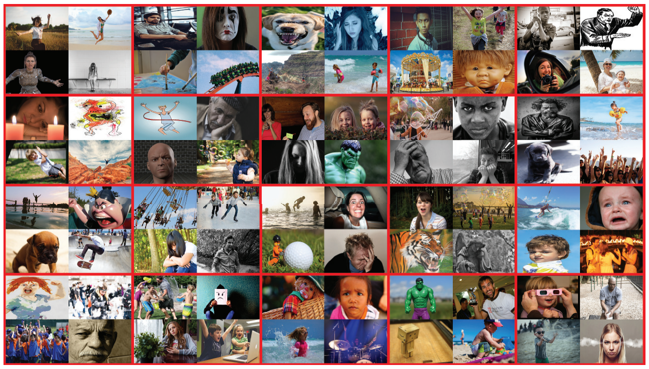


Fig. 5. Example of second authentication layer image with $(i = 4) \times (j = 5)$ rectangles.

Equation 2 shows the probability of a correct selection p of a rectangle $R_{i,j}$ within an emotion E_k, for $1 \leq k \leq 4$.

$$p = P(R_{i,j} \cap E_k) = P(R_{i,j})P(E_k|R_{i,j}) = \frac{1}{4ij} \quad (2)$$

For a successful authentication on layer 2, the attacker has to match q click-based selections on the correct sequence. Equation 3 shows the probability of a correct authentication (B) on layer 2.

$$P(B) = p^q = (\frac{1}{4ij})^q \quad (3)$$

Figure 6 shows how the two-layer authentication system works.

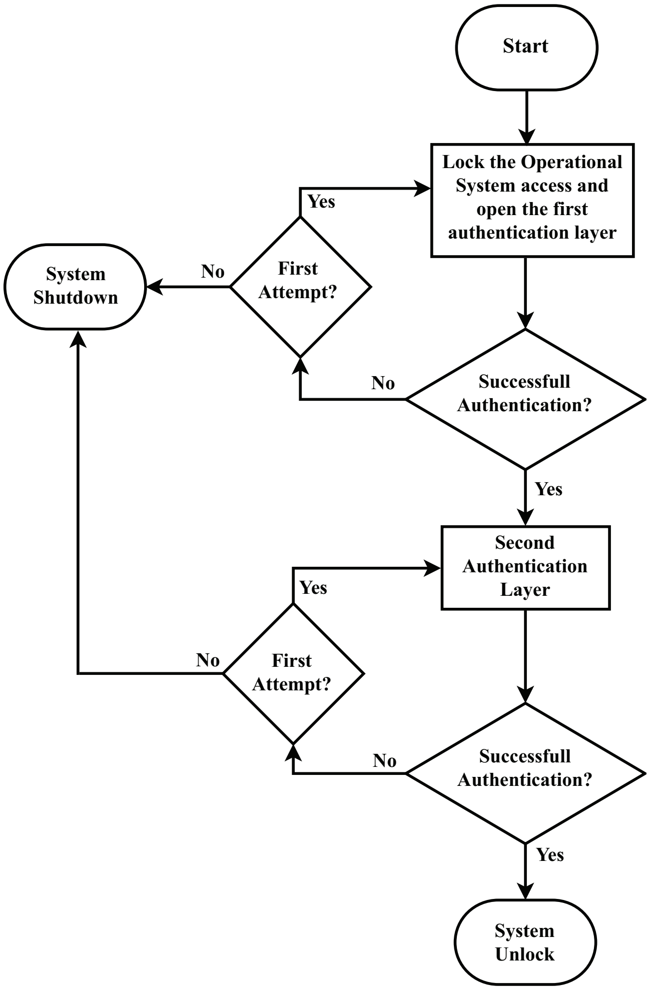

Start
Lock the Operational System access and open the first authentication layer
Yes
System Shutdown
No
First Attempt?
No
Successfull Authentication?
Yes
Second Authentication Layer
Yes
No
First Attempt?
No
Successfull Authentication?
Yes
System Unlock

Fig. 6. Flowchart of the proposed authentication scheme.

C. System Usability

Rating scales can be discrete or continuous, labeled or unlabeled, or with numbered rating points or categories. The experiment consisted on a subjective assessment of the usability level. The scores were performed using the Computer System Usability Questionnaire [19] with a set of 20 users.

This usability metric consists on 19 subjective evaluations: (1) Overall, I am satisfied with how easy it is to use this system; (2) It was simple to use this system; (3) I can effectively complete my work using this system; (4) I am able to complete my work quickly using this system; (5) I am able to efficiently complete my work using this system; (6) I feel comfortable using this system; (7) It was easy to learn to use this system; (8) I believe I became productive quickly using this system; (9) The system gives error messages that clearly tell me how to fix problems; (10) Whenever I make a mistake using the system, I recover easily and quickly; (11) The information (such as online help, on-screen messages, and other documentation) provided with this system is clear; (12) It is easy to find the information I needed; (13) The information provided for the system is easy to understand; (14) The information is effective in helping me complete the tasks and scenarios; (15) The organization of information on the system screens is clear; (16) The interface of this system is pleasant; (17) I like using the interface of this system; (18) This system has all the functions and capabilities I expect it to have; and (19) Overall, I am satisfied with this system.

Each question can be answered with a 1 to 7 score, where 1 corresponds to strongly disagree and 7 corresponds to strongly agree.

III. Experimental Results

As layer 1 and 2 verifications are independents, the complete authentication probability is $P(S) = P(A) \times P(B)$. Table I shows some authentication probabilities for the proposed scheme considering that bots attacks are not effective against authentication layers 1 and 2. Naturally, the probability access is lower (close to zero) for higher values of m, i, j and q.

TABLE I
Successful system authentication probability on a bot attack.

m	n	i	j	q	$P(S)$
8	3	3	4	3	1.79×10^{-8}
8	3	3	4	5	7.78×10^{-12}
8	3	3	4	7	3.37×10^{-15}
8	3	3	4	9	1.46×10^{-18}
8	3	4	5	3	3.87×10^{-9}
8	3	4	5	5	6.05×10^{-13}
8	3	4	5	7	9.46×10^{-17}
8	3	4	5	9	1.47×10^{-20}
8	4	3	4	3	1.43×10^{-8}
8	4	3	4	5	6.22×10^{-12}
8	4	3	4	7	2.70×10^{-15}
8	4	3	4	9	1.17×10^{-18}
8	4	4	5	3	3.10×10^{-9}
8	4	4	5	5	4.84×10^{-13}
8	4	4	5	7	7.56×10^{-17}
8	4	4	5	9	1.18×10^{-20}

Figure 7 shows the normalized [0 - 1] average results of the Computer System Usability Questionnaire, where 1 corresponds to strongly agree and 0 corresponds to strongly disagree.

Users revealed that the weakest usable aspects of the system are topics related to information displayed on layers 1 and 2 (questions number 9, 12 and 14). The stronger points of the system are related to effectiveness and satisfaction perception (questions number 2, 5, 17 and 19), which are associated to the notion of trust. As the proposed authentication scheme avoids to display clues that can be used by a bot, it is natural the perception of low information guide on questions 9, 12 and 14.

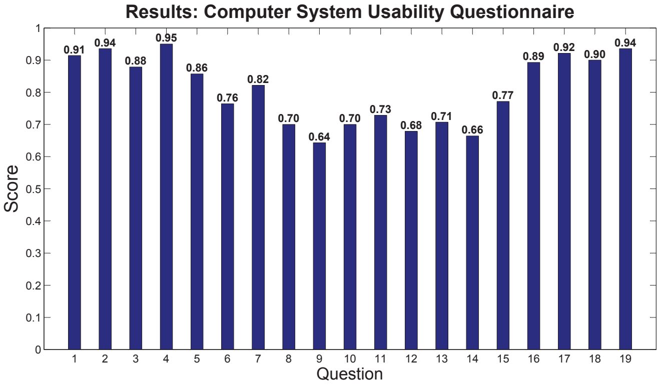


Fig. 7. Average results of the Computer System Usability Questionnaire.

IV. Conclusion

In this paper, we proposed a two-layer graphical password scheme. Unlike the existing methods, our method employs a Captcha and Recognition-Based Image Layer, and an Emotional and Cued-Recall Image Layer. These layers rely on the user's natural cognitive abilities.

As user gets different independent challenge images for the first and second authentication layers, this scheme is robust to dictionary, rely and brute-force attacks. The cracking probability is lower for a larger number of possible showed images on layer 1, and for images with larger amount of subrectangles and required clicks on layer 2. The system also counts with bot prevention using the shutdown event for more than one authentication failure attempt on layer 1 and 2.

Experimental results showed that users consider the security system as effective and satisfactory, even if it does not show generic information for fixing problems. This scheme is also useful for sensitive data processing applications.

Acknowledgment

This work was supported by the Centro Universitário IESB.

References

[1] Paul Dunphy and Jeff Yan, "Do Background Images Improve 'Draw a Secret' Graphical Passwords?" in *Proceedings of ACM CCS*, 2007, pp. 1–12.

[2] T. Wu, "A real-world analysis of Kerberos password security," in *Proceedings of the ISOC Symposium on Network and Distributed System Security*, February 1999.

[3] J. Yan, A. Blackwell, R. Anderson and A. Grant, "Password Memorability and Security: Empirical Results," in *Proceedings of IEEE Security & Privacy*, vol. 2, 2004, pp. 25–31.

[4] Vikas K. Kolekar and Milindkumar B. Vaidya, "Click and Session BasedCaptcha as Graphical Password Authentication Schemes for Smart Phone and Web," in *Proceedings of the International Conference on Information Processing (ICIP)*, December 2015, pp. 669–674.

[5] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, "Captcha as Graphical PasswordsA New Security Primitive Based on Hard AI Problems," in *Proceedings of the IEEE Transactions on Information Forensics and Security*, vol. 9, June 2014, pp. 891–904.

[6] R. Dhamija and A. Perrig, "Déja Vù: A user study using images for authentication," in *Proceedings of the 9th USENIX Security*, 2000, pp. 1–4.

[7] D. Weinshall, "Cognitive authentication schemes safe against spyware," in *Proceedings of the IEEE Symp. Security Privacy*, May 2006, pp. 300–306.

[8] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, “PassPoints: Design and longitudinal evaluation of a graphical password system,” in *Proceedings of the Int. J. HCI*, vol. 63, July 2005, pp. 102–127.

[9] R. Biddle, S. Chiasson, and P. C. van Oorschot, “Graphical passwords: Learning from the first twelve years,” in *Proceedings of the ACM Comput. Surveys*, vol. 44, 2012.

[10] J. Yan and A. S. El Ahmad, “A low-cost attack on a microsoft CAPTCHA,” in *Proceedings of the ACM CCS*, 2008, pp. 543–554.

[11] J. Elson, J. R. Douceur, J. Howell, and J. Saul, “Asirra: A CAPTCHA that exploits interest-aligned manual image categorization,” in *Proceedings of the ACM CCS*, 2007, pp. 366–374.

[12] Tianrong Rao, Min Xu, Huiying Liu, Jinqiao Wang, and Ian Burnett, “Multi-Scale Blocks Based Image Emotion Classification Using Multiple Instance Learning,” in *Proceedings of the ACM International Conference on Multimedia*, September 2016, pp. 634–638.

[13] Sicheng Zhao, Yue Gao, Xiaolei Jiang, Hongxun Yao, Tat-Seng Chua, and Xiaoshuai Sun, “Exploring principles-of-art features for image emotion recognition,” in *Proceedings of the ACM International Conference on Multimedia*, 2014, pp. 47–56.

[14] C. Castelfranchi, “The role of trust and deception in virtual societies,” in *Proceedings of the 34th Annual Hawaii International Conference on System Sciences*, 2001, p. 8.

[15] P G W Keen, “Electronic commerce relationships: Trust by design,” in *Prentice Hall PTR*, 2000.

[16] D. K. Smetters and R. E. Grinter, “Moving from the design of usable security technologies to the design of useful secure applications,” in *Proceedings of the Workshop on New Security Paradigms - NSPW*, September 2002, p. 82.

[17] Souhail Guennouni, Anass Mansouri, and Ali Ahaitouf, “Multiple Object Detection using OpenCV on an Embedded Platform,” in *Proceedings of the Third IEEE International Colloquium in Information Science and Technology (CIST)*, October 2014, pp. 374–377.

[18] Ming Chen, Lu Zhang, Jan P. Allebach, “Learning Deep Features for Image Emotion Classification,” in *Proceedings of the IEEE International Conference on Image Processing (ICIP)*, September 2015, pp. 27–30.

[19] Debbie Stone, Caroline Jarrett, Mark Woodroffe, Shailey Minocha, “User Interface Design and Evaluation,” in *Morgan Kaufmann*, March 2005.