International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2494-9150 Vol-01, Issue 12, MAR 2016.

The Graphical Lock : Color Image Technique

[1]Archana Pawar, [2]Jayasurya Pillai, [3]Pooja More, [4]Sarita Kedilkar

[1,2,3,4]Computer Engineering, Smt. Indira Gandhi College of Engineering, Navi-Mumbai, Maharashtra, India.

[1]archanapawar987@gmail.com, [2]amjaya246@gmail.com, [3]poojamore993@gmail.com, [4]sarita.kedilkar@gmail.com

Abstract—Passwords seem to be a simple technology, but authentication isn't the simplest Internet security problem. In the vast majority of computer systems, passwords are the method of choice for authenticating users. The most common computer authentication method is to use alphanumerical passwords. This method has been shown to have major drawbacks. As, users tend to pick passwords that can be easily guessed or on the other hand, if a password is hard to guess, then it is often hard to remember. Hence numerous authentication alternatives are being considered like "Token based authentication", "Knowledge based authentication", "Biometric based authentication". Graphical Authentication is considered a great alternative due to following factors: First, Human can remember pictures better than text; Second, The possible password space is bigger hence reduce the chance of dictionary attack. This paper explores a graphical authentication technique that maintains correct balance between the two important factors of Authentication: Security and Usability.

Keywords **—Password, Security, Textual Password, Recognition Based, Recall Based, Graphical Authentication.**

I. INTRODUCTION

Graphical passwords were firstly introduced in 1999. The memorability of graphical password schemes is confirmed by psychological tests and studies over recent years. These tests conclude with the fact that word and image-based passwords are processed in a different way in the mind. Text-based passwords are represented by symbols, which are given a meaning that associates them with the text seen, and image-based passwords are given a perceived meaning based on what is being directly observed.[1] The dual-coding theory[2] is the most widely used theory explaining this difference.

The proposed methods of graphical user authentication used nowadays are broadly classified in the following two main categories, according to the memory task involved in the way of remembering and entering the password:

- Recognition-based methods, in which the user is authenticated after successfully choosing those images that he initially selected during the registration phase of the method, from a specific set of images. These methods can also be found under the names "cognometric" or "searchmetric".
- Recall-based methods, in which the user is authenticated after successfully reproducing something that he originally created during the registration phase without being given any reminders. Those methods are also referred to as draw metric systems. There is also an intermediate category called Cued-Recall that is placed between the aforementioned two methods as a combination of them.

II. RELATED WORK

A. Graphical Authentication Schemes

In Recognition-based schemes, during the registration phase users are required to choose their pictures, symbols or icons from a collection presented to them by the system. During the authentication phase, users are required to recognize their choice in order to be successfully identified. Research shows hat 90% of the users using this method could remember their password after a two month period[3]. Techniques belonging to recognition based schemes are the following:

- Passface scheme[4]
  - Guessing and Shoulder Surfing attacks are possible
  - total authentication time needed is greater than that of using textual passwords
- Deja-Vu scheme:[5]
  - Time delay compared to textual password method: more time is needed to create the portfolio than creating a text password and more time to login since the user has to compare the images he sees
- Triangle and Movable schemes: The login process may be slow, having in mind that the user locate his pass-points over hundreds of objects
- WIW & WIW extended schemes: The user has to memorize the unique codes of each Pass-Object

- Picture password scheme mainly designed for mobile devices: The existence of only thirty thumbnail photos makes a small password space. Taking into consideration that each thumbnail image has a unique numerical value this results to the fact that the password length is considerably less than the actual text-password length
- Awase-E scheme, a variation of the previous scheme;
- Story scheme: Using the story scheme requires a sequence of images in order for a user to make up a story
- Jetafida scheme

In the trial version 30 persons participated with 51.76% total evaluation scores. Figure 1 shows a usability comparison of recognition-based methods.

In Recall-based schemes, during the registration phase users are required to perform an action, such as creating a simple sketch; at the authentication stage they are required to reproduce what they created earlier. The latter recall stage is divided into two categories, Pure recall and Cued recall . Notable techniques belonging to Pure recall-based schemes are the following:

- Draw A Secret (DAS) scheme:
  - A survey in 2002 showed that most of the participated users forgot their stroke order and that they could remember their textual password easier than the DAS used passwords
  - The users often use weak graphical passwords, making them vulnerable to graphical password attacks
- PassDoodle scheme: People were in the position to remember the doodle itself but not the order in which it was drawn
- Grid Selection scheme: same asthe DAS scheme drawbacks
- Pass-G0 scheme, an extension ofthe DAS scheme using a 9x9 grid
- Syukri scheme : Using as a writing device makes signatures drawing hard to be done correctly since the majority of users are not familiar with this kind of writing.

Notable techniques belonging to Cued recall-based schemes are the following:

- Blonder scheme: The image being used is pre-defined and cannot be changed
- PassPoint scheme: users using the Passpoint method need more time to learn their passwords compared to users using alphanumeric text and it takes longer for them to be authenticated
- PassLogix v-Go scheme: This technique has a poor password space due to item limitations that can be moved within the images
- VisKey SFR Password: a four spot Viskey can offer theoretically almost one billion possibilities to define a password.

However, these are not enough to avoid the off-line attacks by a high speed computer.

	Recognition Based techniques	Usability Features										
		Satisfaction									Efficiency	Effectiveness
		Mouse Usage	Create Simply	Meaningfull	Assignable Image	Memorability	Simple Steps	Nice Interface	Training Simple	Pleasant Picture	Applicable	R&A
1	PassFace	√	√	X	√	√	√	√	√	√	X	√
2	Déjà vu	√	√	X	√	X	√	X	√	X	X	√
3	Triangle	√	√	X	X	√	√	X	X	X	X	√
4	Movable Frame	√	√	X	X	√	√	X	X	X	X	√
5	WIW	X	√	X	√	√	√	X	√	X	√	X
6	Picture Password	√	√	X	√	√	√	√	√	√	√	X
7	Story	√	√	√	√	√	√	√	X	√	√	X
8	Jetafida	√	√	X	√	√	√	√	√	√	√	X

Figure 1. Usability Comparison of Recognition Based methods (√: Yes, X: No)

	Recall Based techniques	Usability Features								
		Satisfaction							Efficiency	Effectiveness
		Mouse Usage	Create Simply	Meaningfull	Memorability	Simple Steps	Nice Interface	Training Simple	Applicable	R&A
1	DAS	√	X	X	X	√	NA	√	√	√
2	PassDoodle	√	X	√	X	√	NA	√	√	X
3	Grid Selection	√	X	X	X	√	NA	√	X	√
4	Pass-Go	√	√	X	√	√	X	√	X	√
5	Blonder	√	√	X	√	√	X	√	√	X
6	PassPoint	√	√	X	√	√	√	√	√	√
7	Syukri	√	X	√	√	√	√	√	√	√
8	PassLogix v-Go	√	X	√	√	X	√	X	√	√
9	VisKey SFR	√	√	X	√	√	√	√	√	√

Figure 2. Usability Comparison of Recall Based methods (√: Yes, X: No)

III. PROPOSED SYSTEM

A. *Colors Image Technique:*

Color Image Technique is an graphical authentication process. . The main idea behind the project was to create an easy and fast process of user authentication. The Color Image Technique Authentication has no special needs concerning the hardware and software requirements. It's a versatile technique which can be used in mobile devices or web based application or for Desktop authentication.

Recall Based Technique as discussed above shows the common feature of high password space hence providing higher security but at the same time it is not able to provide able to provide a user friendly technique.

Recognition based on the other hand is very much user friendly technique but password space in recognition based is not as high as in recall based technique hence questioning its security provision

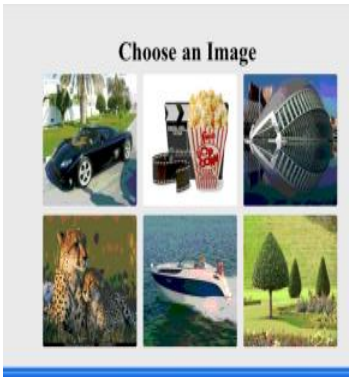
Hence a hybrid technique deriving the best feature from both the techniques can help to provide usability with security, which is the main focus of Color Image Technique.

B. *Description of Color Image Technique:*

Color Image Technique is divided into two phases the registration phase and the login phase.

In registration phase, the user is provided with images to select from; the selected image is then divided into *n* smaller chunks and scrambled. User has to choose at least one chunk and assign an RGB value to it, which will be assigned as his password and stored in database the chunks and their RGB level values

During authentication the selected image is provided, scrambled randomly every time the user tries to login, the user is must recognize his chunk from the scrambled image and assign the RGB level value by clicking on it. Each click is considered +1 RGB level value for that chunk. The value during authentication is cross checked with one in database. If the two images match, having the same intensity values of the three primary colors (Red, Green, Blue) for the correct chunks, the user is successfully authenticated. So Color Image Technique is considered hybrid of Recognition based and Recall Based Techniques.

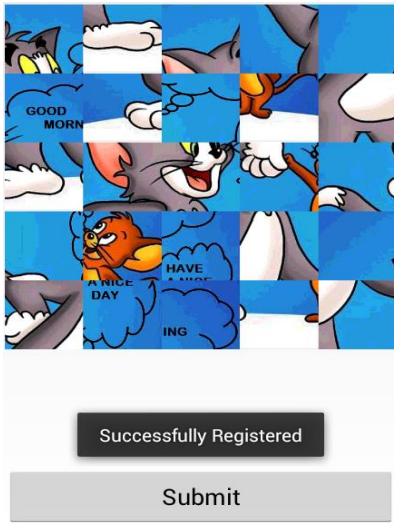


. User selects an image

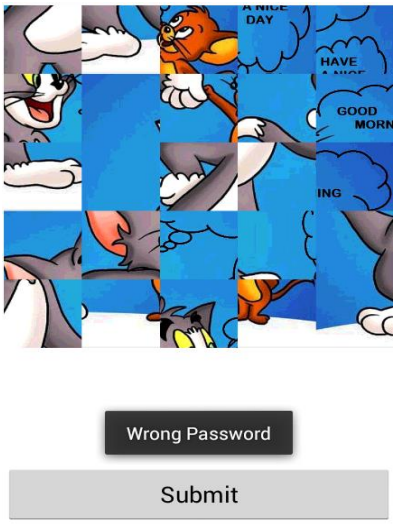
The selected Image

Scrambled Image

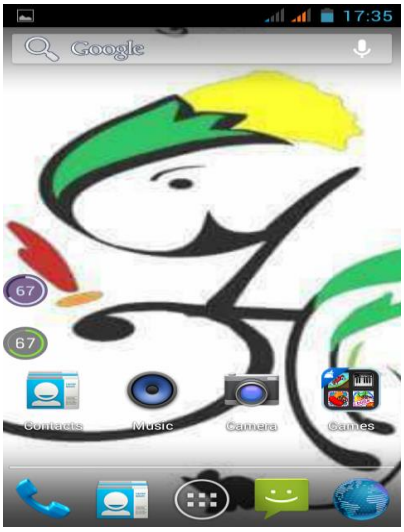
Single chunk selected and RGB set



Registration Successful



Authentication Failure



Authentication Successful

Figure 3: Authentication Screenshot

C. Future Scope

For future work, to increase the security, concept of gesture and neighborhood chunk concept can be added to increase the password space of the technique

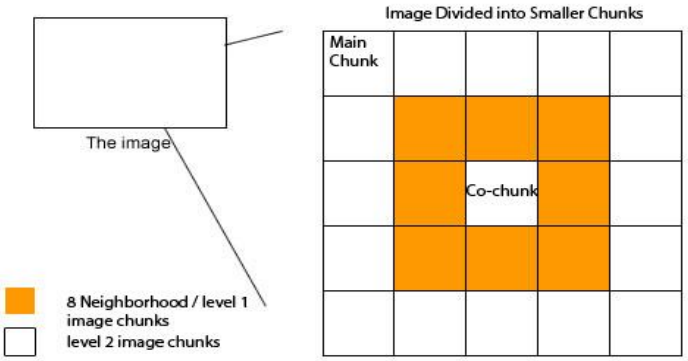


Figure 4: Authentication Screenshot

In this there can be a main chunk and a co chunk which will be selected by the user during registration. During authentication, the image must be scrambled in such a way that the main chunk is at most only two levels away from co-chunk. And the user must bring the main chunk at 8 neighborhood of the co-chunk.

This can increase the password space and also protect against guessing attack and shoulder surfing attack to an extent.

The RGB Concept and can be integrated with neighborhood concept in following three different ways:

- The Main Chunk can also be the RGB Chunk
- Main Chunk and RGB Chunks can be completely Different
- Main Chunk can also be one of the many RGB Chunks

The integration type chosen solely depends on user's capability to remember and recognize the chunks and its value.

Hence all the three option must be provided to the user to so it doesn't affect the Security and Usability factor of color image technique and user can select the option best suitable according his level of comfort and cognitive ability.

D. Conclusion

Two important factors: security and usability was the main focus for this technique. It provides better password space than text based password hence provide better security than text based password from traditional security attacks.

In Graphical Authentication, The main two techniques, Recall based and Recognition based have its own strength and weakness. A hybrid technique is able to reap benefits of the both the techniques and provide the important factor of security and usability at its optimum level.

Color Image Technique is versatile as it doesn't have any hardware or software requirements and can be integrated in all environments with ease.

REFERENCES

[1] C. Herley, P. C. van Oorschot and A. S. Patrick, 2009"Passwords: If We're So Smart, Why Are We Still Using Them?", Financial Cryptography and Data Security, Lecture Notes in Computer Science, Springer Berlin Heidelberg, Vol. 5628, 230-237, 2009, doi:10.1007/978-3-642-03549-4_14.

[2] A. Paivio, 2006. "Mind and Its Evolution, A Dual Coding Theoretical Approach", Psychology Press, Nov. 2006, ISBN-10: 0805852603.

[3] X. Suo, Y. Zhu and G. S. Owen, 2005. "*Graphical Passwords: A Survey*", 21st Annual Computer Security Applications, doi:10.1109/CSAC.2005.27. K. Elissa, "Title of paper if known," unpublished.

[4] S. Wiedenbeck, J. Waters, J-C. Birget, A. Brodskiy, N. Memon, 2005. "*PassPoints, Design and longitudinal evaluation of a graphical password system*", International Journal of Human-Computer studies, Academic Press Inc,. 102-127, July 2005, doi: 10.1016/j.ijhcs.2005.04.010.

[5] R. Dhamija and A. Perrig, 2000. "*DeJa Vu: A User Study Using Images for Authentication*", Proceeding of the 9th USENIX Security Symposium, CiteSeer: 10.1.1.36.6339.

[6] G. Blonder, 1996. "*Graphical passwords*", United States Patent 5559961, 1996.

[7] A.F. Syukri, E. Okamoto and M. Mambo, 1998. "*A User Identification System Using Signature Written with Mouse*", 3rd Australasian Conference on Information Security and Privacy (ACISP), Springer-Verlag, Lecture Notes in Computer Science, Vol. 1438, 403-441, doi: 10.1007/BFb0053751.

