

Graphical User Authentication in Mobile Device using the web RGB color palette

I. Krikelas

Technological Educational
Institution Athens, Ag. Spiridona
12210 Athens, Greece
(+30)2105385312
ikrikelas@gmail.com

I. Xydas

Technological Educational
Institution of Athens, Ag. Spiridona
12210 Athens, Greece
(+30)2105385736
xydas@teiath.gr

P.-F. Bonnefond

XLIM Laboratory, CNRS, UMR 6172
University of Limoges
83, rue d' Isle 87000 Limoges, France
(+33) 628180338
bonnefond@unilim.fr

ABSTRACT

Existing graphical authentication methods take into account the fact that users are more capable of remembering pictures instead of text. Graphical authentication schemes are expected to be less vulnerable to specific hacker attack techniques that have greatly improved in recent years. The usability aspect of a graphical authentication product refers to the extent that a product can be used by users to achieve goals with effectiveness, efficiency and satisfaction in a specified context of use. This paper describes a prototype system providing graphical authentication of mobile devices over the Internet, covering both usability and security aspects. Color images are assigned to the mobile users and authentication is achieved by modifying the Red-Green-Blue (RGB) color intensity values of the assigned image.

Author Keywords

Graphical mobile authentication, mobile device authentication, graphical passwords, web color graphical authentication

ACM Classification Keywords

H.5.2 [Information Interfaces and Presentation]: User Interfaces - *Graphical user interfaces (GUI)*.

General Terms

Security, Human Factors

1. 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: 1) 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 [3]. These methods can also be found under the names "cognometric" or "searchmetric". 2) 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 [3]. Those methods are also referred to as drawmetric systems. There is also an intermediate category called Cued-Recall that is placed between the aforementioned two methods as a combination of them.

2. RELATED WORK

2.1 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 that 90% of the users using this method could remember their password after a two month period [3] [4] [5]. Techniques belonging to recognition-based schemes are the following: i) Passface scheme [6]; Drawbacks: a) Guessing and Shoulder Surfing attacks are possible b) total authentication time needed is greater than that of using textual passwords ii) Deja-Vu scheme [7]; Drawbacks: a) 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 iii) Triangle and Movable schemes [8]; Drawback: The login process may be slow, having in mind that the user locate his pass-points over hundreds of objects iv) WIW & WIW extended schemes [9], [10]; Drawback: the user has to memorize the unique codes of each Pass-Object v) Picture password scheme mainly designed for mobile devices [11]; Drawback: 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 vi) Awase-E scheme, a variation of the previous scheme [12]; vii) Story scheme [13]; Drawback: Using the story scheme requires a sequence of images in order for a user to make up a story viii) Jetafida scheme [14]; Drawback: 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 [3] and Cued recall [15]. Notable techniques belonging to Pure recall-based schemes are the following: i) Draw A Secret (DAS) scheme [16]; Drawbacks: a) 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 b) The users often use weak graphical passwords, making them vulnerable to graphical password attacks ii) PassDoodle scheme [17]; Drawback: People were in the position to remember the doodle itself but not the order in which it was drawn iii) Grid Selection scheme [18]; Drawbacks: same as the DAS scheme drawbacks iv) Pass-G0 scheme, an extension of the DAS scheme using a 9x9 grid [19]; v) Syukri scheme [20]; Drawback: 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: i) Blonder scheme [21]; Drawback: The image being used is pre-defined and cannot be changed ii) PassPoint scheme [22] [23]; Drawback: 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 iii) PassLogix v-Go scheme [24]; Drawback: This technique has a poor password space due to item limitations that can be moved within the images iv) VisKey SFR Password [25]; Drawback: 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 [15]. Figure 2 shows a usability comparison of Recall Based methods.

Recognition Based techniques	Usability Features										
	Satisfaction								Efficiency	Effectiveness	
	Mouse Usage	Create Simply	Meaningfull	Assignable Image	Memorability	Simple Steps	Nice Interface	Training Simple			
1 PassFace	✓	✓	X	✓	✓	✓	✓	✓	X	✓	
2 Déjà vu	✓	✓	X	✓	X	✓	X	✓	X	✓	
3 Triangle	✓	✓	X	X	✓	✓	X	X	X	✓	
4 Movable Frame	✓	✓	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	Pleasant Picture			
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)

2.2 Graphical Authentication Security

An authentication mechanism must provide adequate security in order to meet its goal. Attacks of a graphical password system are classified in two categories: guessing attacks (brute-force and dictionary attacks) and capture attacks (shoulder surfing, spyware and social engineering attacks). A comparison table among all algorithms based on attack patterns is presented in [4] and [15].

3. MASTERLOGIN PROJECT

3.1 Colors in web page design

Colors used in webpage design are commonly specified using RGB. Initially, the limited color depth of most video hardware led to a limited color palette of 216 RGB colors, defined by the Netscape Color Cube [26]. However, with the predominance of 24-bit displays, the use of the full 16.7 million colors of the HTML RGB color code no longer poses problems for most viewers. In short, the web-safe color palette consists of the 216 (6^3) combinations of red, green, and blue where each color can take one of six values (in hexadecimal): #00, #33, #66, #99, #CC or #FF (based on the 0 to 255 range for each value discussed above). These hexadecimal values represent 0%, 20%, 40%, 60%, 80%, 100% in terms of intensity respectively. This is adequate for splitting up 216 colors into a cube of dimension 6. However, lacking gamma correction, the perceived intensity on a standard 2.5 gamma CRT / LCD is only: 0%, 2%, 10%, 28%, 57%, 100%. The RGB color model for HTML was formally adopted as an Internet standard in HTML 3.2, however it had been in use for some time before that. This Web color Palette was used in our project to change the color of images provided to users for authentication.

3.2 Description of the MasterLogin Project

The MasterLogin Project is an internet authentication process. The main idea behind the project was to create an easy and fast process of user authentication to gain access to web sites. This solution has been designed with mobile devices in mind. Nowadays a large variety of mobile devices are in circulation, with many capabilities and characteristics. The MasterLogin Authentication Project has no special needs concerning the mobile device. The only requirements for the mobile devices are an active internet connection, and a Web

Browser with HTML capabilities. Since mobile technology is a fast-paced industry a specific 3rd generation mobile is selected in order to customize the MasterLogin Authentication Area to suit its needs. iPhone4 (Apple Inc) was selected due to its large touch-screen and widespread use. Any other mobile device can be used (smartphone or small tablet) provided that this mobile device has a screen suitable for this kind of application. Mobile devices with smaller screens will be harder to use. The MasterLogin Authentication process is shown in Figure 3. On the Server side the MasterLogin Authentication Project uses a database where all the user credentials are stored, running on an SQL Server 2008. Both the administrative and the end user modules are programmed using Visual Studio 2008. The end user page is an ASP.Net page hosted on a local Internet Information Server. Images are assigned to users, during the registration process, with the chosen RGB values. During authentication, the user chooses the image that has been assigned to him from a list of available images and then changes the RGB level values of the picture to his chosen ones stored in the database. If the two images match, having the same intensity values of the three primary colors (Red, Green, Blue), the user is successfully authenticated. So, the MasterLogin project is a hybrid solution of aforementioned Recognition-based and Recall-based authentication methods.

The project is divided into two modules. The first module, called the “MasterLogin Supervisor”, is the administration module. It gives the system administrator the ability to manage the images that will be used and the users to be registered. The color modifications of a user selected image are done by using three track-bars representing the three basic colors (RGB), one for each color. The second module, called “MasterLogin Authentication Area”, is the internet-based interface of the Authentication subsystem. The MasterLogin authentication page is an asp.net web page created in order to authenticate a mobile user. First the user selects the image he is registered to and then by setting his own and unique RGB level values to match the values in the stored image he/she authenticates successfully. The authentication page is designed specifically for the iPhone screen resolution but can be adapted to any mobile device with an appropriate display screen for web surfing. Figures 5 and 6 present screenshots of the MasterLogin authentication page:

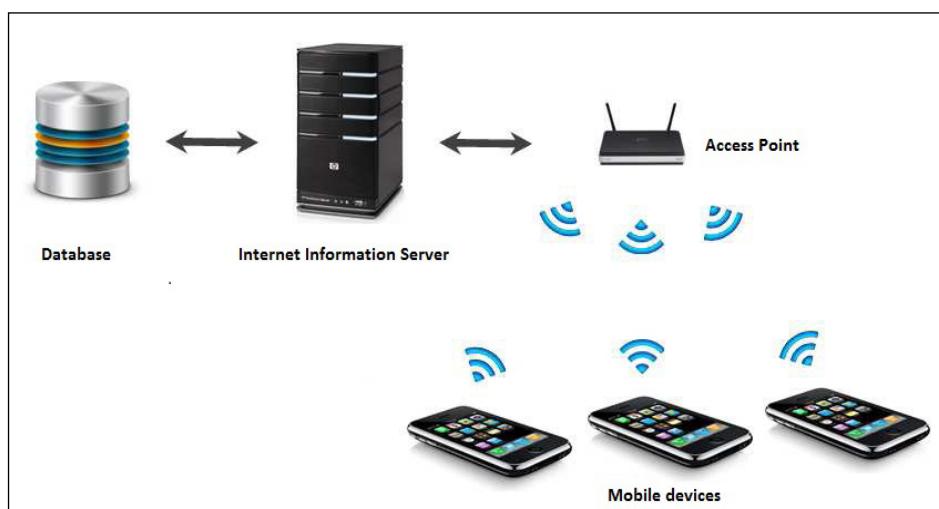


Figure 3. MasterLogin project components

In Figure 4 a histogram comparison is shown regarding two images. The left one is the original image imported to the Images Database after having changed color values of the pixels to meet

the web palette standards. The one on the right is the same image produced during the authentication phase by the same user in order for him to be authenticated.

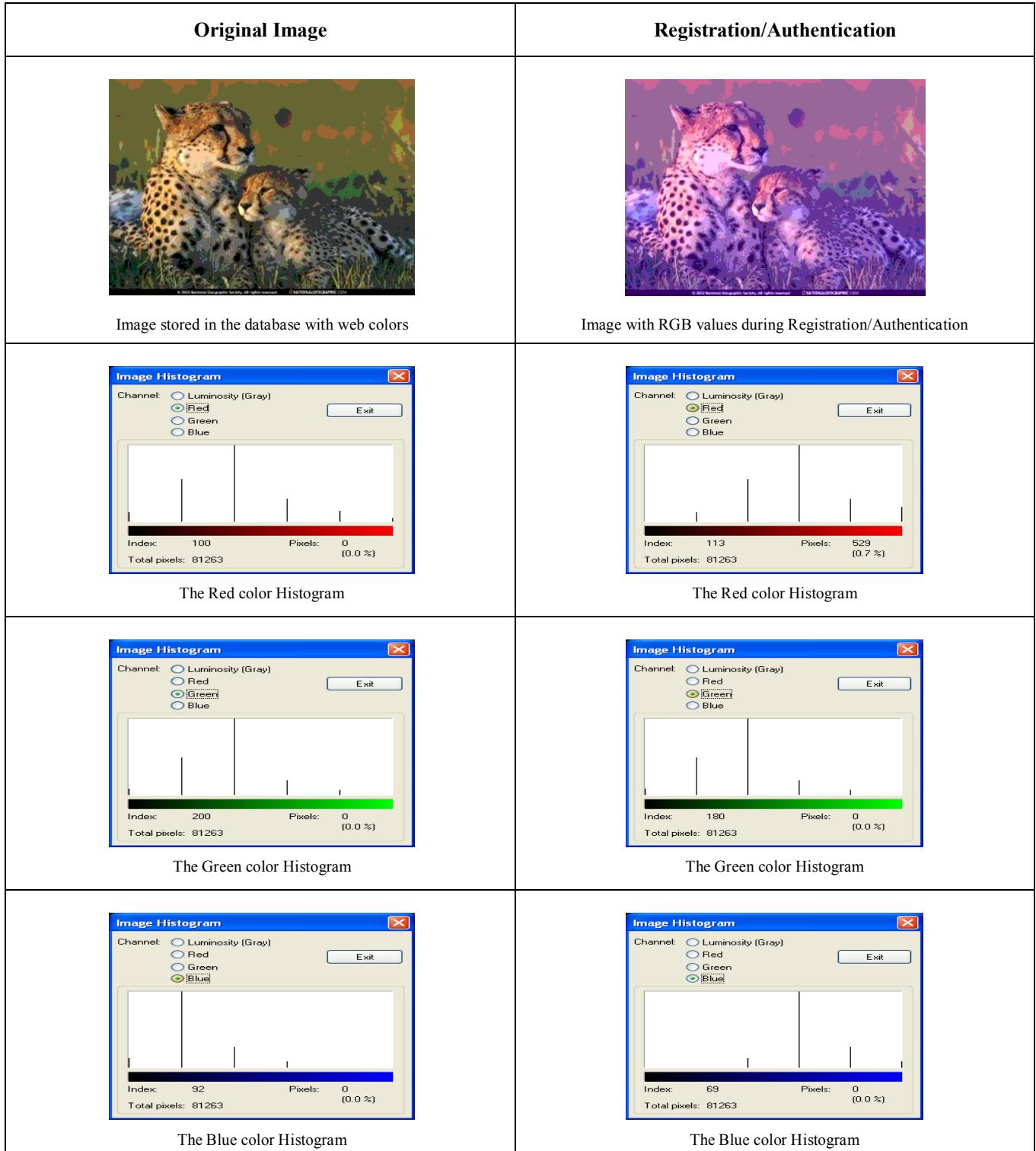


Figure 4. Images and color histograms

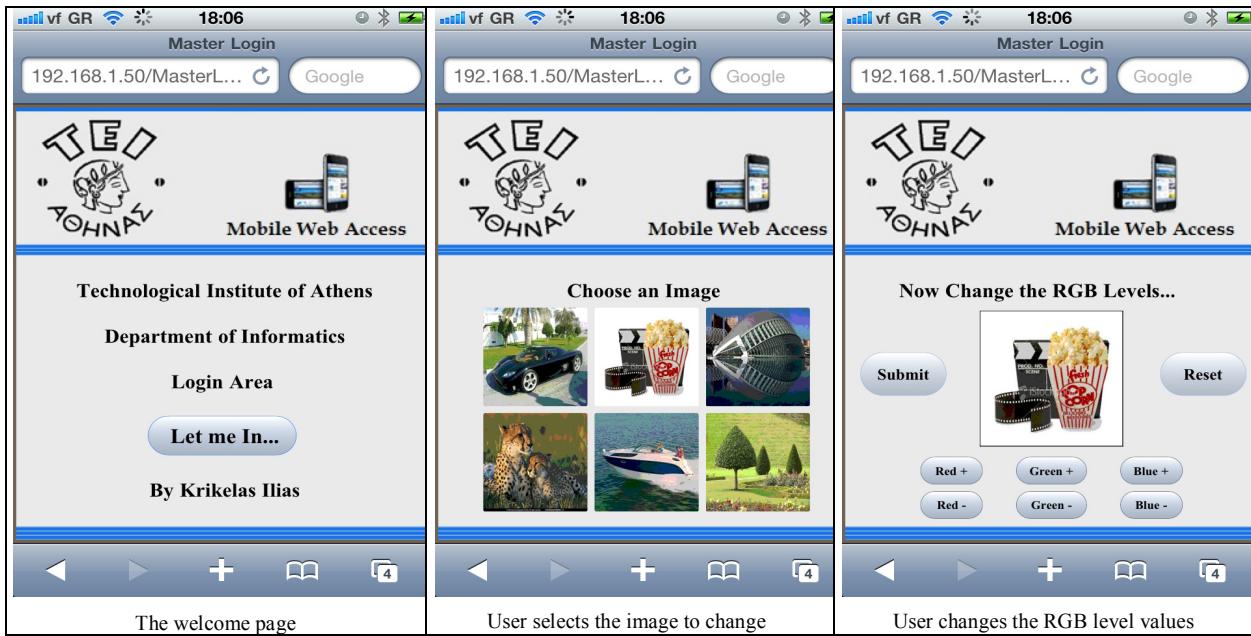


Figure 5. Authentication screenshots

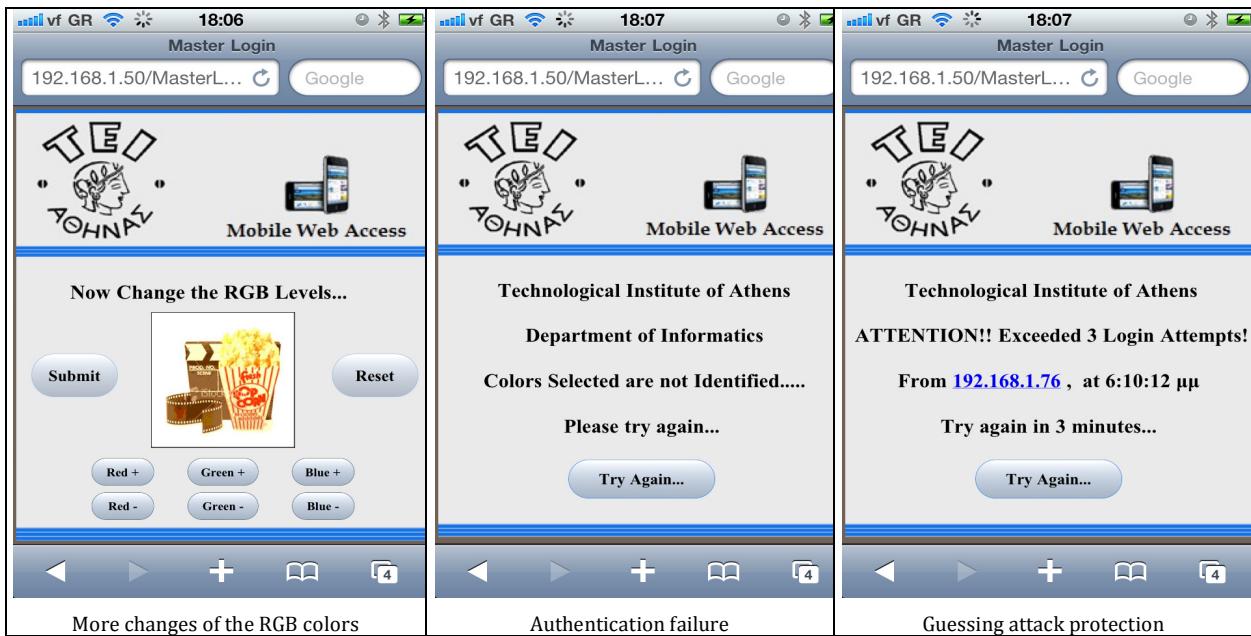


Figure 6. Authentication failure screenshot

3.3 Usability of the MasterLogin Project

As with all the other existing graphical authentication techniques, a usability measure was performed for our project (see Figure 7). The used attributes are shown below:

- i) Mouse Usage: the program does not use a mouse since it is mobile-oriented; instead, the touch-screen of a next-generation mobile device is very easy to use.
- ii) Create Simply: this is done by the administration panel by a simplified procedure.
- iii) Meaningful: not a story followed like the Story scheme, but an image changing colors.

iv) Assignable Image: this is done by the administration panel by a simplified procedure.

v) Memorability: it is applicable since the user needs to know the RGB levels he uses.

vi) Simple Steps: a very simple procedure changing the Red, Green and Blue colors of the Image.

vii) Intuitive Interface: the graphical interface is very simple and intuitive.

viii) Simple Training: this can be done in the administration panel during the user registration.

ix) Pleasant Picture: all the images are selected at the user's discretion.

- x) Efficiency: the MasterLogin Authentication can be very easily adopted for mobile user authentication over the web being reliable and accurate.
- xi) Effectiveness (R&A: Reliability & Accuracy): is easily applicable as a mobile user authentication procedure.

	Recognition Based techniques	Usability Features										Efficiency	Effectiveness
		Satisfaction								Applicable	R&A		
		Mouse Usage	Create Simply	Meaningfull	Assignable Image	Memorability	Simple Steps	Nice Interface	Training Simple	Pleasant Picture			
1	MasterLogin Project	✓	✓	X	✓	✓	✓	✓	✓	✓	✓	✓	✓

Figure 7. MasterLogin Usability features

3.4 Security of the MasterLogin Project

A security evaluation of the MasterLogin Authentication Project is given below (Figure 8):

- i) Brute Force: a brute force attack can take place, but this is handled by the program itself.
- ii) Dictionary: a dictionary attack is not possible since no text is used at all.
- iii) Guessing: a guessing attack can take place, but this is handled by the program itself.

- iv) Spyware: a spyware attack is not likely to take place.
- v) Shoulder Surfing: a shoulder surfing attack is very possible to occur, hence depends on the vigilance of the user in order to protect the authentication process.
- vi) Social Networking: a social networking attack like in most of the graphical authentication techniques is unlikely to succeed since the authentication deals with images and colors.

	Recall Based Techniques	Attacks					
		Brute Force	Dictionary	Guessing	Spyware	Shoulder Surfing	Social Networking
1	MasterLogin Project	X	✓	✓	X	✓	X

Figure 8. The MasterLogin attack possibilities

4. CONCLUSION – FUTURE WORK

Usability and security of a graphical authentication system are two aspects linked together. As security increases, usability of the scheme may decrease. So, designing a scheme for a bank should differ from designing the same scheme for an e-shop subscription. An ideal solution would give both usability and security at the desired levels. Our project satisfies all the usability features defined by the ISO standards: ISO 9241 (Ergonomics requirements for office work with visual display), ISO 9126 (External and Internet Quality) and ISO 13407 (the life cycle of computer based interactive systems). Security is also enhanced, since brute force and guessing attacks are handled by the program, dictionary and spyware attacks are not likely to take place and social networking attacks are unlike to take place as we deal with images and their colors. An Internet standard in HTML 3.2, the RGB color model for web sites has been used in our project. In the future this color model could be enhanced by supporting regular RGB palettes of 15-bit (32,768 colors) or 24-bit (16,777,216 colors) and/or non-regular RGB palettes of 16-bit (65,536 colors).

5. ACKNOWLEDGMENTS

The MasterLogin project was a Masters dissertation (Master ISICG: Sciences et technologies de l'information et de la communication, informatique, synthèse d'images et conception graphique). The Technological Educational Institution (TEI) of Athens runs this Masters in parallel with the University of Limoges, France.

6. 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.
- [4] F. Towhidi and M. Masrom, 2009. "A Survey on Recognition-Based Graphical User Authentication Algorithms", International Journal of Computer Science and Information Security, Vol. 6, No. 2,119-127, ISSN 1947 5500, arXiv:0912.0942.
- [5] PL. Lin, LT. Weng and PW. Huang, 2008. "Graphical Passwords Using Images with Random Tracks of Geometric Shapes". Congress on Images and Signal Processing, doi: 10.1109/CISP.2008.603.
- [6] Real User Corporation. "The Science Behind Passfaces". White paper: <http://www.passfaces.com/published/The%20Science%20Behind%20Passfaces.pdf>, 2010.
- [7] 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.
- [8] L. Sobrado and J.C. Birget, 2002. "Graphical passwords". The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, Vol. 4.
- [9] S. Man, D. Hong and M. Mathews, 2003. "A shoulder surfing resistant graphical password scheme". Proceedings of International conference on security and management, Las Vegas.
- [10] D. Hong, S. Man, B. Hawes and M. Mathews, 2004. "A password scheme strongly resistant to spyware", Proceedings of International conference on security and management, Las Vegas, 94-100.
- [11] J. Wayne, G. Serban, K. Vlad, A. Rick and S. Ryan, 2003. "Picture Password: A Visual Login Technique for Mobile Devices", National Institute of Standards and Technology (NIST), NISTIR 7030, USA.
- [12] T. Takada and H. Koike, 2003. "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images", 5th International Symp. On Human Computer Interaction with Mobile Devices and Services (MobileHCI2003), Springer, Vol. 2795, 347-351.
- [13] D. Davis, F. Monroe, M.K. Reiter, 2004. "On User Choice in Graphical Password Schemes", Proceedings of the 13th conference on USENIX Security Symposium.
- [14] A.M. Eljetlawi and N.B. Ithnin, 2009. "Graphical password: Usable Graphical Password Prototype", Journal of International Commercial Law and Technology, Vol. 4, issue 4, 298-309.
- [15] A.H. Lashkari, Dr R. Saleh, S. Farmand and Dr. O.B. Zakaria, 2009. "A wide-range survey on Recall-Based Graphical User Authentications algorithms based on ISO and Attack Patterns", International Journal of Computer Science and Information Security, Vol. 6, No. 3, 17-25, ISSN 1947 5500, arXiv: 1001.1962.
- [16] I. Jermyn, A. Mayer, F. Monroe, M.K. Reiter and A.D. Rubin, 1999. "The Design and Analysis of Graphical Passwords", Proceedings of the Eighth USENIX Security Symposium.
- [17] J. Goldberg, J. Hagman, and V. Sazawal, 2002. "Doodling Our Way to Better Authentication", Proceedings of Human Factors in Computing Systems, Minneapolis, Minnesota, USA, doi:10.1145/506443.506639.
- [18] J. Thorpe and P.C. van Oorschot, 2004. "Towards Secure Design Choices for Implementing Graphical Passwords", 20th Annual Computer Security Applications Conference (ACSAC), Tucson, Arizona, doi: 10.1109/CSAC.2004.44.
- [19] H. Tao, 2006. "Pass-Go, a New Graphical Password Scheme". School of Information Technology and Engineering, University of Ottawa, Canada, M.S. thesis.
- [20] 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.
- [21] G. Blonder, 1996. "Graphical passwords", United States Patent 5559961, 1996.
- [22] S. Wiedenbeck, J. Waters, J-C. Birget, A. Brodskiy, and N. Memon, 2005. "Authentication using graphical passwords: Basic results", Proceedings of Human-Computer Interaction International (HCII 2005), Las Vegas, NV.
- [23] 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.
- [24] <http://www.oracle.com/us/corporate/Acquisitions/passlogix>
- [25] <http://www.sfr-software.de>
- [26] <http://web.mit.edu/debi/www/colorcube.html>