Volume 4, Issue 3, March 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Secure Recognition Based Graphical Password by Watermarking

Rahul Ingle[1], Mayuri Bawane[2], Karishma Dudhbade[3], Reena Tijare[4], Prof. Sneha Ramteke[5]

[1,2,3,4]Department of Computer Technology, Rajiv Gandhi College Of Engineering & Research, Nagpur, India

[5]Lecturer, Department of Computer Technology of Engineering & Research, Nagpur, India

Abstract— One of the most important topics in data protection or information security today is user authentication i.e. genuineness. The most common computer authentication or securing data is to use alphanumerical as the measure, using the text-based strong password schemes that often makes memorizing the password so difficult that makes the users writing them down on a piece of paper or saving inside the computer. The GUA (Graphical User Authentication) or simply graphical password has proposed an alternate scheme as an alternative to the text based schemes by the fact that humans tend to remember images better, as pictures are comparatively easier to be remembered or recognised. This type of interface provides an easy way to create and remember the passwords for the users. However, one big issue that is bothering GUA is shoulder suffering attack that can capture the users mouse clicks and image gallery attack that can change the images of the gallery with physical attack.

Keywords— Graphical Password; Recognition Based Algorithm; Authentication Security; Shoulder surfing; image gallery attack; Watermarking

I. INTRODUCTION

The most common computer authentication method is the user to submit its user name or a text password. The "Picture Superiority Effect" has coined to describe and show the Graphical-Based Passwords (GBP) reflects the as a solution to conventional or traditional password techniques. The problem arises because the passwords are expected to comply with two fundamentally conflicting requirements:

1) Passwords should be easy to remember, and the user authentication method so being used or the protocol should be accessible and executable quickly and easily.

2) Passwords should be secure, i.e., they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user.

Furthermore, such a term underscores the impact of GBP's in that the "effect" is on account of the fact that graphics and texts are easier to commit to memory than conventional password techniques. The graphical user authentication (GUA) system requires a user to select a memorable image from the available resources present in the computer. Such a selection of memorable images would depend on the nature of the image itself and the specific sequence of click locations. Images with meaningful content will support the user's memorability.

II. BACKGROUND

A number of articles mentioning file viewers in software and computer engineering journals, primarily with respect to the role of file viewers in software design. Following are some disadvantages of the current system:

- Brute force attacks uses algorithm to generate every possible combination of words to break the text based passwords GUA proves to be more robust and resistant to brute force attacks because the attack software needs to produce all possible mouse motions to imitate passwords especially when trying to recall the graphical passwords.
- Spyware attacks uses small utilities and applications present in users computer to record sensitive data during mouse and key press operations, but with the GUA even if the movements are recorded the accuracy is not achieved in identifying the graphical passwords.
- Dictionary attacks are the attacks which uses the concept of using words that are present or found in dictionary to check the possibilities of any were used as the password by the user
- "Memory Management and User Authentication" is a need of the hour.
- A hectic and a cumbersome task is recognising the text based passwords. As it is easier to remember the combinations of geometrical shapes patterns, colours more than the alphanumeric characters.

III. RELATED WORK

Our main aim is to develop an user friendly environment i.e. To design and build a system that can switch between as many formats as possible, as robustly as possible and visualizing the file's contents. To build such an application named "A Secure Recognition Based Graphical Password By Watermarking" that would be consolidation of all the different applications. "Secure Recognition Based Graphical Password by Watermarking" will be the combination of securing the password. This will reduce the efforts expected from the user and thus will provide more luxury. In our project we have

decided to provide a platform to the users wherein they will have a choice to select from the resources available on their respective computers. A particular user will be able to browse his/her computer to search for the image and the text which he/she decides as the password. Once the image is selected, our application will validate it pixel by pixel, then encrypt it, crosscheck with the information in database, and send it to further use. In this case, we are applying visible watermarking to encode the data so that it's rendered safe from the attacks.

In our project we are trying to use the concept of Dynamic Link Library (DLL) in order to omit the need of different types of converters required at each step. DLL, which is non executable code, will provide the required support (internal library) to the main interface which we are trying to create.

Format, or to copy information from the viewed file to the system-wide clipboard.

The DLL is available majorly with asp.net framework. Thus we are planning to incorporate DLL and similar features of asp.net framework in our project in order to make it as much user friendly as possible.

In our project there are corresponding two modules:

- Registration module
- Login phase

The concept of Watermarking is limited-functionality as Watermarked multimedia objects are not still resilient to attacks rather they are vulnerable to attacks because the digital contents can be digitally edited.

They can be edited like intentional or unintentional ways as cropping, gamma correction, compression or low pass filtering. To withstand such attacks watermarks must be robust as well as have the resistance to handle such kinds of attacks and should be well designed and encapsulated to avoid these kinds of attacks.

"Authentication and Data Security" is a need of the hour. A hectic and a cumbersome task is to remember the text based or the alphanumeric password as it bit tedious to remembering them, the users generally makes a note of it, or saves in the computer's memory. Memorability has its two respective perspectives:

• The process of selecting or choosing and the method or the encoding techniques of the password chosen by the user.

• Defining the methodology that has implied to retrieve the original password.

This is a general proposed approach; it just gives us the tentative and a brief idea about our project.

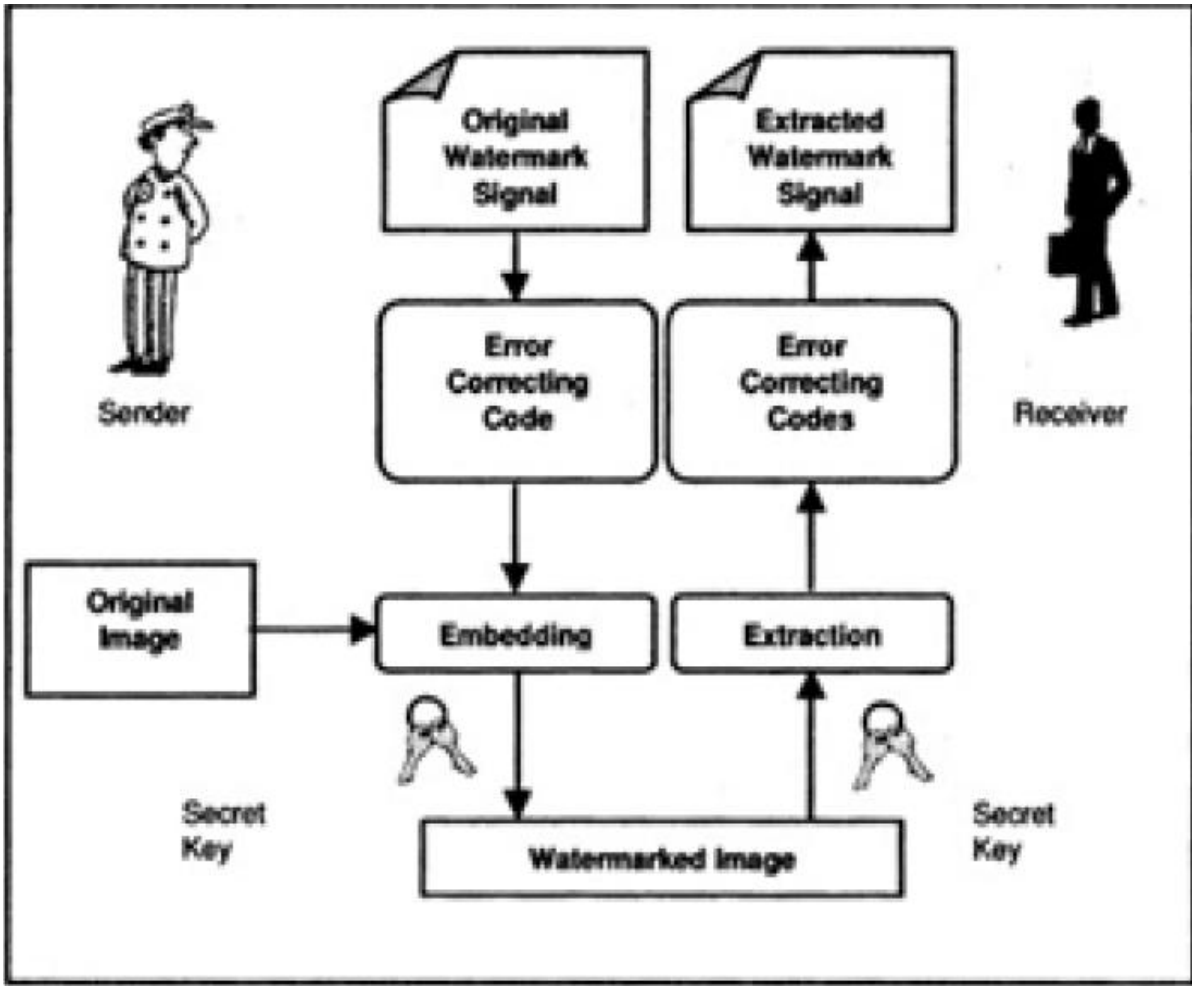

Figure 1: Proposed Approach

The figure above shows how exactly our project is exactly going to work. This is our proposed approach.

IV. BASIC MODEL

In the following diagram, the basic approach is given

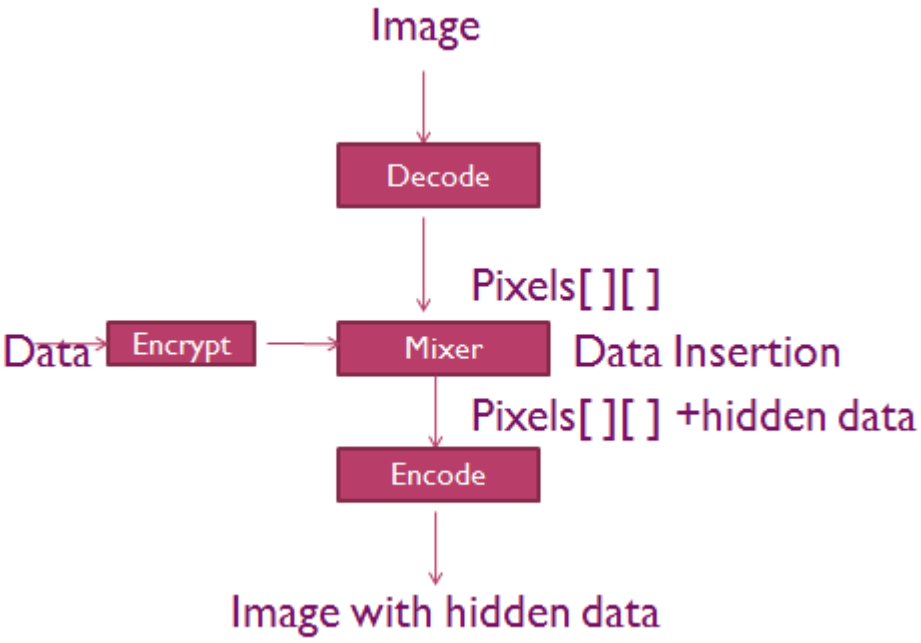

Figure 2: Flow chart of Image Hiding

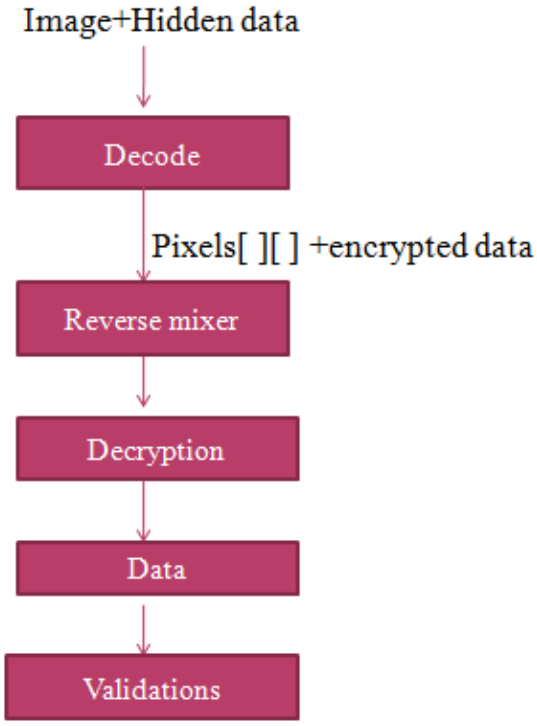

Figure 3: Flowchart of image retrieval

Our main aim is to develop an user friendly environment i.e. To design and build a system that can switch between as many formats as possible, as robustly as possible and visualizing the file's contents. To build such an application named "A Secure Recognition Based Graphical Password by Watermarking" that would be consolidation of all the different applications.

"Secure Recognition Based Graphical Password by Watermarking" will be the combination of securing the password. This will reduce the efforts expected from the user and thus will provide more luxury.In our project we have decided to provide a platform to the users wherein they will have a choice to select from the resources available on their respective computers. A particular user will be able to browse his/her computer to search for the image and the text which he/she decides as the password. Once the image is selected, our application will validate it pixel by pixel, then

encrypt it, crosscheck with the information in database, and send it to further use. In this case, we are applying visible watermarking to encode the data so that its rendered safe from the attacks.

V. SYSTEM DESIGN

A Secure Recognition Based Graphical Password by Watermarking will work as follows:

1) **TEXT**: A user needs to enter a password which is combination of alphabets and digits i.e. alphanumeric password. This password will be highly secure as it will not be entirely visible to the user. Only asterisk i.e. '*' will be seen on the screen. Here the user is allowed to have any possible combination of uppercase and lower case as the password will be different for both the cases. The password will then be sent backhand to the database and the necessary encoding techniques will be employed.

2) **IMAGE**: After choosing the text password, the user needs to select an image from the drives present on the computer. The image can be present anywhere on the computer. The image can be of the most commonly used formats like .gif, .png, .bmp, .jpg, etc. This image will be concatenated with the text password that has been provided by the user in the previous step. This combination will then be watermarked and the combination of bytes thus generated will then be sent to the database for further processing.

VI. SCREEN SHOTS

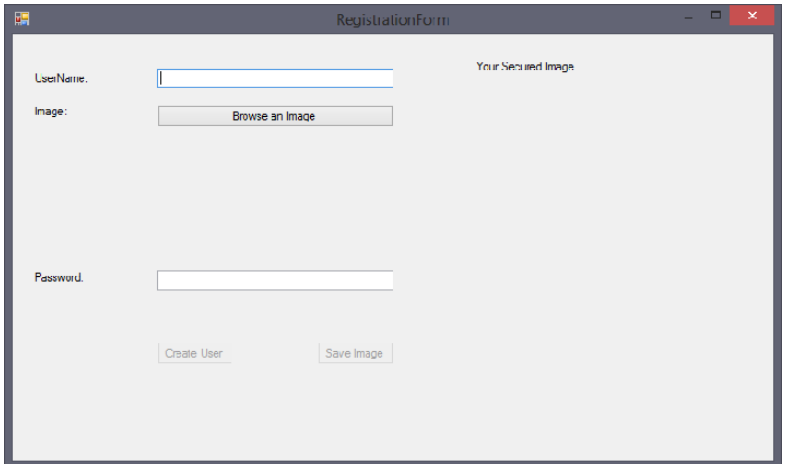

Figure 4: Structure of Registration Form

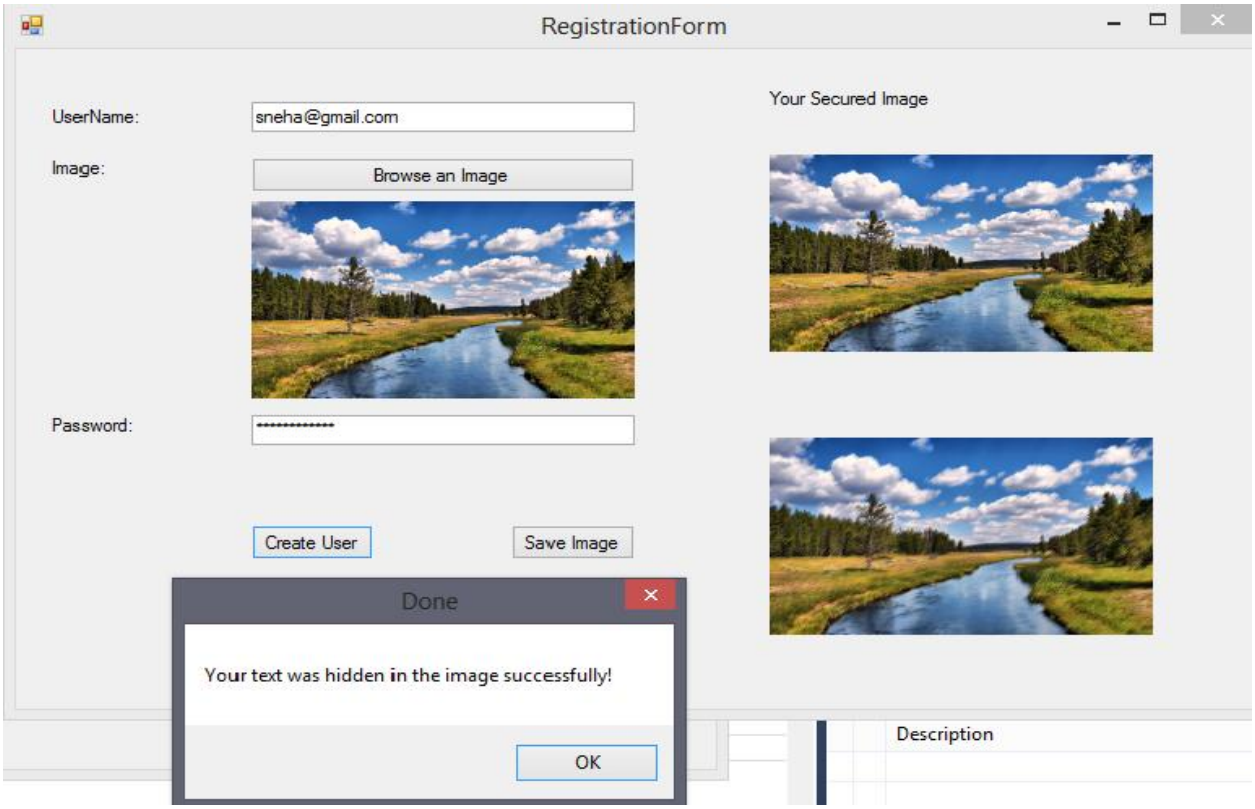

Figure 5: Registration Form

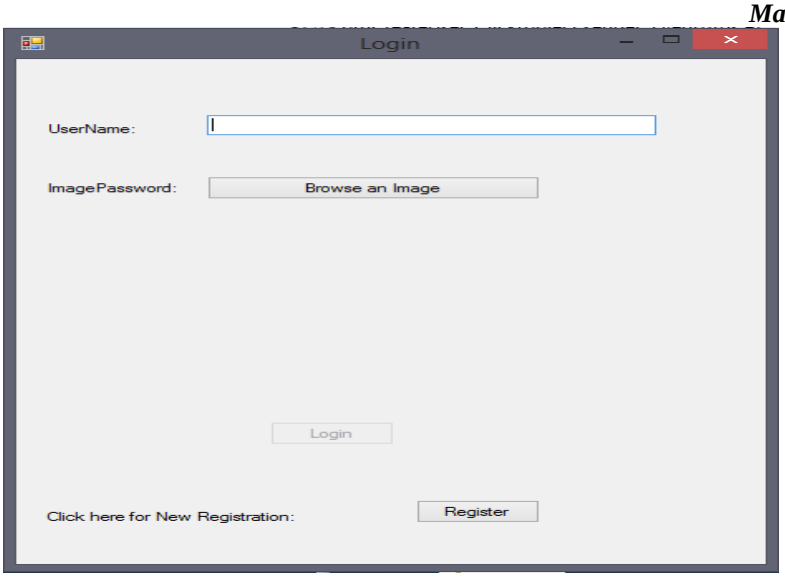

Figure 4: Structure of Login Form

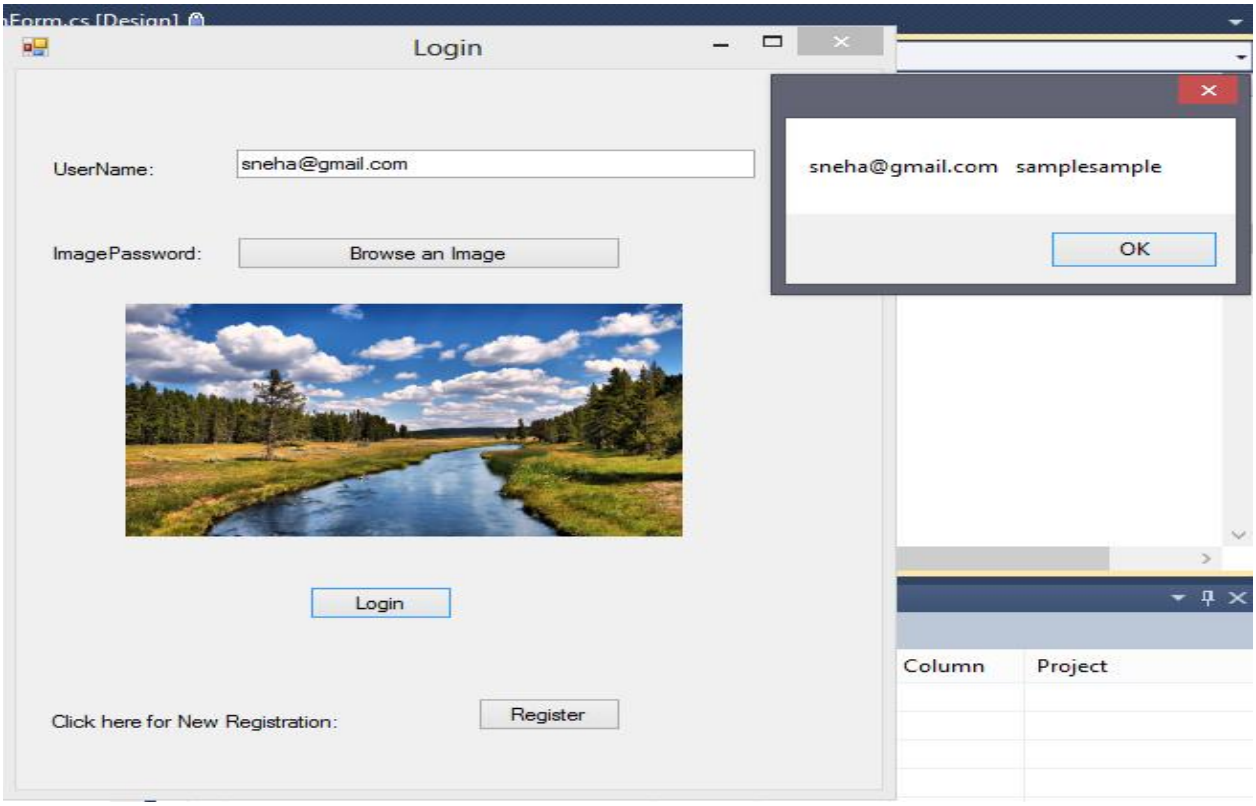

Figure 4: Login Form

VII. CONCLUSION

The empirical testing of graphical passwords indicates strengths and weaknesses, but it is effective and encouraging. In information security, user authentication is the most important and critical of all the elements. Researches gave the data that some users and empirical studies have proven that human are better at memorizing graphical passwords i.e. combinations of geometric figures, shapes, colours, patterns, textures compared to textual password... This proves that graphical password is a more desirable alternative to alphanumerical passwords. Presented the recognition based algorithm type of graphical password. In this paper we have presented description and analysis of the recent advances in the Watermarking techniques. These techniques are branched and classified into several categories depending upon the domain in which the hidden data is inserted, the size of the hidden data and the requirement of which the hidden data is to be extracted. This paper proposes a new graphical password algorithm that uses watermarking techniques and random character set to provide stronger security against image gallery attacks and shoulder surfing attack. Finally the technique so evaluated provides a level of resistance to the common attacks of graphical passwords.

ACKNOWLEDGMENT

There are many persons in RGCER College have supported us. Without them, the project would obviously not have looked the way it does now. The first person we would like to thank is our Project Guide **Professor Sneha Ramteke**, Professor of **Computer Technology Department**, RGCER, Nagpur. She has helped us in many ways. Her enthusiastic engagements in our project work and her never-ending stream of ideas have been absolutely essential for the results, presented here. We are very grateful that she has spent so much time with us discussing different problems ranging from philosophical issues down to minute technical details. We would also like to express my sincere thanks to**. PROF. Sandip Kamble,Head of Department of CT, Rajiv Gandhi College of Engineering and Research Nagpur** for his Guidance and kind support. We express our deepest sense of gratitude to **Dr. M. M.Raghuvanshi, Principal, RGCER, Nagpur.**

REFERENCES

[1] A.H. Lashkari, F.T., "Graphical User Authentication (GUA)," 2010: Lambert Academic Publisher.
[2] Komanduri, S. and D.R. Hutchings," Order and Entropy in Picture Passwords," in Canadian Information Processing Society. 2008.
[3] Hu, W., X. Wu, and G. Wei, "The Security Analysis of Graphical Passwords," in International Conference on Communications and Intelligence Information Security. 2010.
[4] Lashkari A.H., A.G., Leila Ghasemi Sabet, Samaneh Farmand, "A New Algorithm on Graphical User Authentication (GUA) Based on Multi-line Grid. Scientific Research and Essays (SRE)," 2010. 5 (24).
[5] Hayashi, E. and N. Christin, Use Your Illusion: "Secure Authentication Usable Anywhere," in Proceedings of the 4th symposium on Usable privacy and security (SOUPS). 2008, ACM.
[6] Chiasson, S., et al., "Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords," in ACM, 2009.
[7] Wiedenbeck, S., J.-C. Birget, and A. Brodskiy," Authentication Using Graphical Passwords:Effects of Tolerance and Image Choice, " in Symposium On Usable Privacy and Security (SOUPS). 2005.
[8] Dhamija, R. and A. Perrig, D´ej`a Vu: "A User Study. Using Images for Authentication," in The proceeding of the 9th USENIX security Symposium. 2000, USENIX
[9] Man, S., et al., "A password scheme strongly resistant to spyware," in Int. Conf. on Security and Management. 2004: Las Vegas.
[10] Forget, A., S. Chiasson, and R. Biddle, "Shoulder-Surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords," ACM, 2010.
[11] Lashkari A.H., S.F., Omar Bin Zakaria and Rosli Saleh, "Shoulder Surfing attack in graphical password authentication," 2009, International Journal of Computer Science and Information Security (IJCSIS).
[12] Man, S., D. Hong, and M. Matthews, "A Shoulder-Surfing Resistant Graphical Password Scheme – WIW, " in International conference on security and management. 2003: Las Vegas.
[13] CAPEC, Standard Abstraction Attack Pattern List (Release 1.6). 2011, "Common Attack Patterns Enumeration and Classification (CAPEC),": USA.
[14] Todorov, D., "Mechanics of User Identification and Authentication," 2007: Auerbach Publications.
[15] Gordon, P., Data Leakage – "Threats and Mitigation," in InfoSec Reading Room. 2007, SANS Institute.

