RESEARCH ARTICLE OPEN ACCESS

Graphical Password by Watermarking for security

Vanita Lonkar, Sonali Raut, Suchita Mesakar
Assistant Professor, GWCET, Nagpur, India

Abstract—
The most common authentication method is to use alphanumerical usernames and passwords. This method has been shown to have considerable disadvantage. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is very difficult to guess, then it is often difficult to remember. To address this problem, some researchers have developed authentication methods that use pictures as passwords. Graphical Password based on the fact that humans tend to remember images better. In this paper, we will propose a new algorithm that using watermarking technique as the solution to solving image gallery attacks and using the random character set generation for each image for resistance to shoulder surfing attack to provide better system security. All the information images in registration phase will be process by copy right protection of watermarking where the login page will check this information for security purposes.
Keyword: Graphical Password, Watermarking, Secure reorganization, Virus attack, Puzzle solving.

I. INTRODUCTION

Now a day there are number of viruses which spread through internet via e-mail. To control this spreading we introduces the algorithm which uses watermarking concept. In this, when user want to send the e-mail or message he can send without any interruption, but when the virus are try to integrate in the message it fails because of the puzzle in front of it. If the user wants to attach the virus it can be possible by solving puzzle, but the viruses are not capable of solve the visual puzzle by itself so it get denial of service. The puzzle consist of image which is break in several parts, these image has watermarked sequence; if user arrange this sequence properly then he gets the privilege to attach the virus code otherwise he gets the denial of service. Human factors are often considered the weakest link in a computer security system. point out that there are major areas where human computer interaction is important: authentication, security operation, and developing secure systems. Here we emphasis on the authentication problem. The most frequent computer authentication method is for a user to submit a user name and a text password. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember .Unfortunately, these passwords can also be easily guessed or broken. According to a recent Computerworld news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords. On the other hand, passwords that are difficullt to guess or break are often difficult to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts. To address the problems with traditional user_name password authentication, substitute authentication methods, such as biometrics ,have been used. In this paper, however, we emphasis on another alternative: using pictures/images as passwords. Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures/images better than text; psychological studies supports such assumption . Pictures are generally easier to be remembered or recognized than text. In addition, if the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text based schemes and thus presumably offer better resistance to dictionary attacks. Because of these advantages, there is a growing interest in graphical password by watermarking . In addition to workstation and web log-in applications, graphical passwords have also been applied to ATM machines and mobile devices.

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should,[1] but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication. Like traditional watermarks, digital watermarks are only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible anytime else.[2] If a digital watermark distorts the carrier signal in a way that it becomes

perceivable, it is of no use.[2] Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal.

The needed properties of a digital watermark depend on the use case in which it is applied. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied.Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. But whereas steganography aims for imperceptibility to human senses, digital watermarking tries to control the robustness as top priority.Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool. It just marks data, but does not degrade it nor controls access to the data.One application of digital watermarking is *source tracking*. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies.

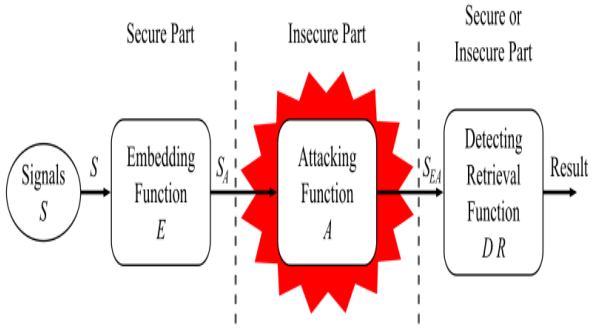

Fig.1.1 Digital watermarking

II. LITERATURE REVIEW

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[1] Information and computer security is supported largely by passwords which are the principle part of the authentication process. The most common computer authentication method is to use alphanumerical username and password which has significant drawbacks. To overcome the vulnerabilities of traditional methods, visual or graphical password schemes have been developed as possible alternative solutions to text-based scheme. A potential drawback of graphical password schemes is that they are more vulnerable to shoulder surfing than conventional alphanumeric text passwords. When users input their passwords in a public place, they may be at risk of attackers stealing their password. An attacker can capture a password by direct observation or by recording the individual's authentication session. This is referred to as shouldersurfing and is a known risk, of special concern when authenticating in public places. In this paper we will present a survey on graphical password schemes from 2005 till 2009 which are proposed to be resistant against shoulder surfing attacks.

III. PROBLEM DEFINITION

Now a day's development in technology causes new type of virus programs which are not easily recognizable by the user or the system. These viruses are train to spread over the network, which causes sudden failure of the entire machines in the network. To avoid this type of failure we have to minimize the chances of spreading of viruses on the network. This not only the problem of the single network but the whole world is in the influence of the viruses via internet.

To reduce this type of happening we are proposing the algorithm which provide the security against the viruses which are integrated with the message and spread all over the network where the message reach.

IV. PROPOSED WORK

A software system is always divided in to several subsystem that makes it easier for the development. A software system that is structured in to several subsystem makes it easy for the development and testing. The different sub system are known as the modules and the process of dividing an entire system in to sub system is known as modularization or decomposition

A system can't be decomposed in to several sub system in any way .There must some logical barrier

,which facility the separation of each module. The separation must be simple but yet must be effective so that the development is not affected.The system under consideration has been divided in to several modules taking in consideration the above mentioned criteria. The different modules are

- Main Module
- Sender Module
- Server Module
- Receiver Module

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.

We start with the development of server which connects the sender and receiver. The server takes the packets from the sender and forwards it to the destination. At this time it shows the status of the packet arrival.

The Sender side is consisting of four sub modules that are File selection, Virus attack, Puzzle solving and File sending. File selection module contain the "Brows button" which brows the computer files from which we select the particular file. Virus attack module consists of "Attack button" which fire the virus attack on the message. Puzzle solving module works when virus attack is happen, it consist of "Enter Image" button which takes user to the window. Here, starts the third sub module i.e. puzzle solving where he/she have to select an image and break into some pieces each piece consist of different watermark, this pieces have to arrange to form the desired image. The puzzle can be solved by the human being not by the virus as a result we get the security against the virus. The last sub module is File sending in which the user enter the ip address of the machine and press the send button.

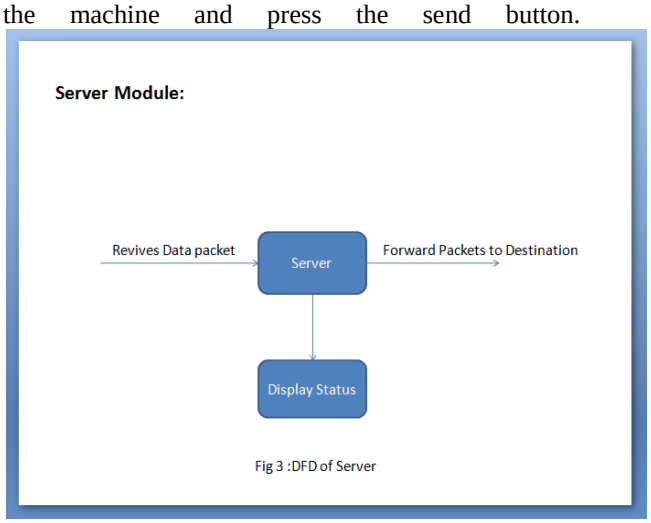

Fig 4.1. Server Module

The last development is of Receiver which receive the file and write it on the output file and create the result which consist of arrival time of the file, size of the file, transfer rate and size of the lost packet.

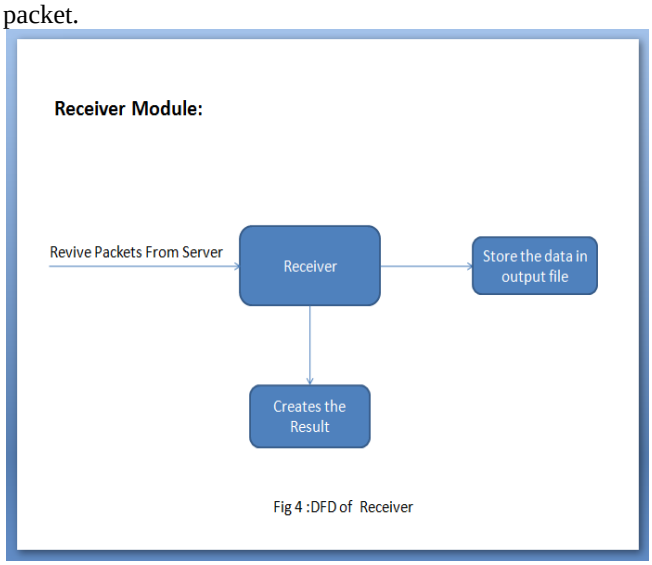

Fig4.2 Receiver Module

EXPERIMENTAL RESULTS

5.1 Usual Sender Side

This is the first slide, from which any user or sender sends the data files to the receiver in normal form.

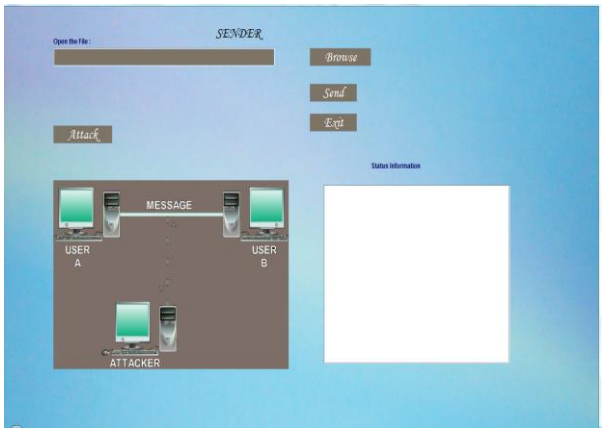

Fig 5.1 Usual Sender Side

5.2 Browse File

When the sender, firstly sends the data or files of data, at that time he will must firstly browse the file and than select that file and that file willoaded on to the sender side.

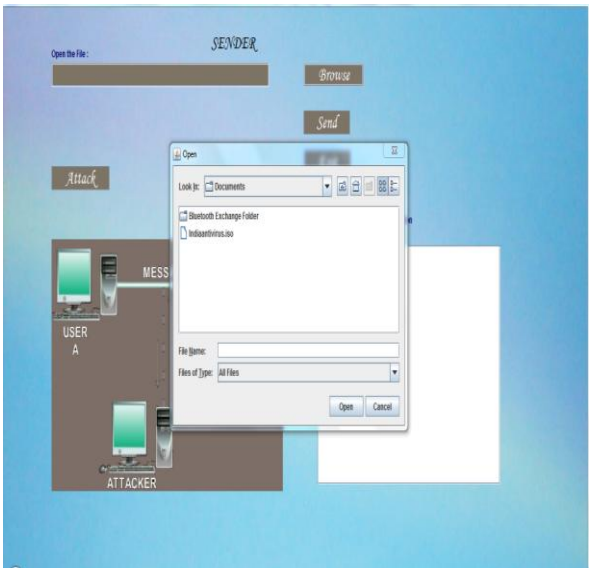

Fig 5.2 : Browse File

5.3 Virus Attack

When user enter his username and password at that time that will be easily guessed and cracked by virus, because 80% of alphanumerical password and username are cracked by the hackers and that virus are inserted by them on the sender side or server. In this way the message will be crashed or it will take more transmission time for travelling from sender to receiver.

Fig 5.3 Virus Attack

5.4 ReceiverWindow

If virus attack is caused then the data file is arrived at the destination, but the virus sends the same data file for more time, and due to this there is congestion will be takes place and at last bottlenecking will be takes place and due to this the time taken for transmission of data is more and that is shown in following result window.

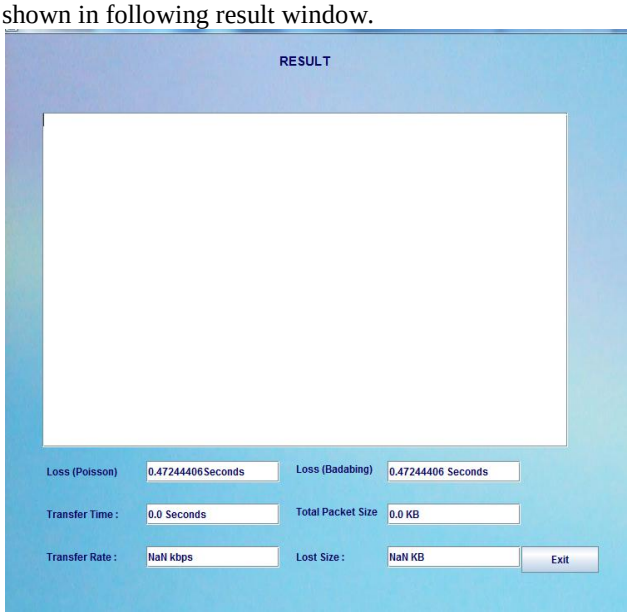

Fig 5.4 Receiver Side Result Display for virus attack

5.5 Original window

For avoiding the problem of attack of the viruses on to the message or the data of sender, we implement the new project and that include the following steps.

The first slide which must be visited by each and every sender while sending of data or file to the receiver and that is shown in the following window.

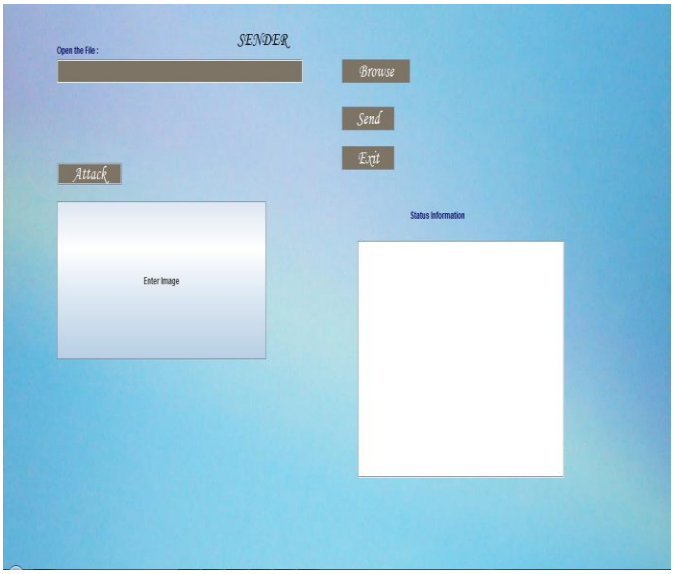

Fig 5.5 Original window

5.6 Browse Window

It is the second step in which when the sender wants to send the file or receiver. At that time he must have to browse the file and select that file, then that file will be loaded to the sender side as shown in following window.

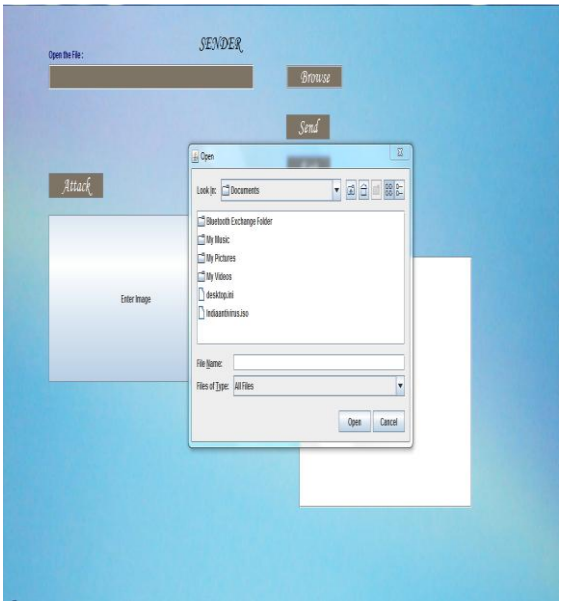

Fig 5.6 Browse Window

5.7 Attack

Once the file is loaded on to the senders side then, viruses try to attack on to the data at that time the server will provide the message on to the window that is enter proper image puzzle as shown in the following window.

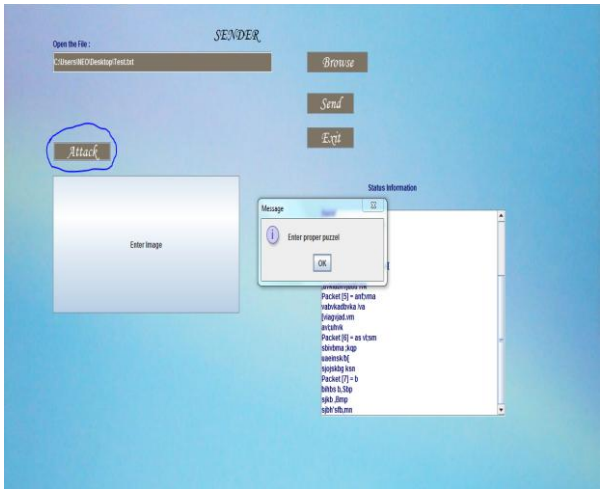

Fig 5.7 Attack

5.8 Selection of the image from the List

Then the server will provide the list of the images and from that list the sender wants to choose one image.

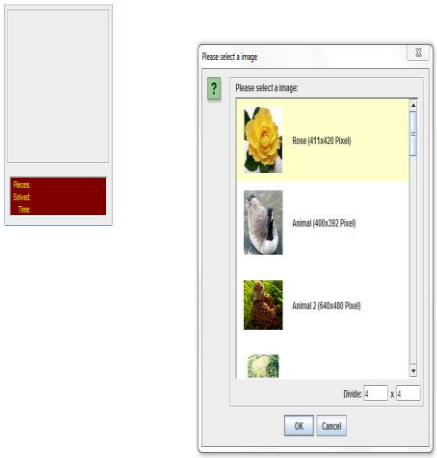

Fig 5.8 Selection of the image from the List

5.9 Arranging the Girds of the Image

After completion or selection of number of grids the sender must have to arrange the image sequence for completing the puzzle which is shown in the following window.

Fig 5.9 Arranging the Girds of the Image

5.10 Data Sent to the Receiver from Sender

After this process the complete data file loaded on the server and as soon as the sender clicks on send button that data will be sended to the server

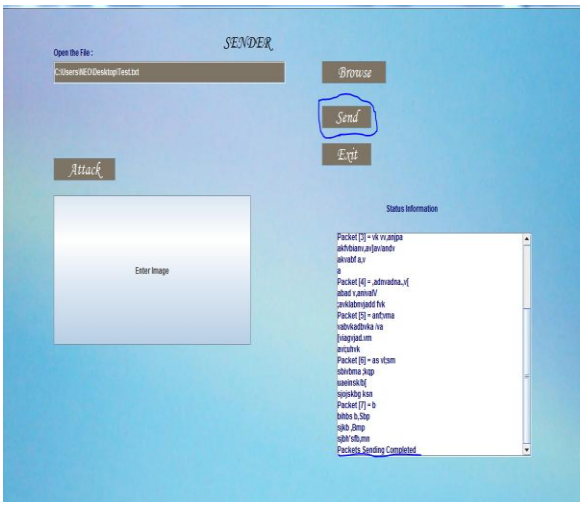

Fig 5.10 Data Sent to the Receiver from Sender

5.11 Data Arrival time Result at the receiver

When data is arrived at the receiver at that time it requires the less time, for transferring that data from the sender to receiver. The time required for transmission of the data can be verified and that is shown in the following window.

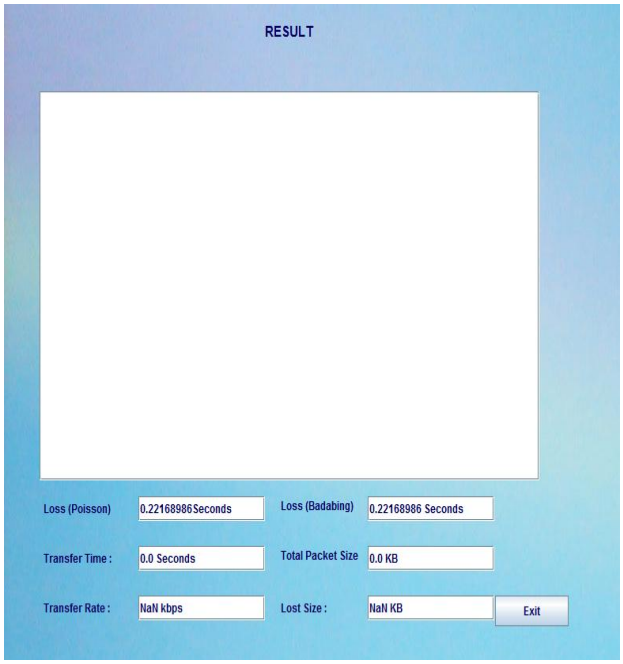

Fig 5.11 Data Arrival time Result at the receiver

V. Future Scope

The core element of computational trust is identity. Currently many authentication methods and techniques are available but each with its own advantages and shortcomings. There is a growing interest in using pictures as passwords rather than text passwords but very little research has been done on graphical based passwords so far. In view of the above, we have proposed authentication system which is based on graphical password schemes. Although our system aims to reduce the problems with existing graphical based password schemes but it has also some limitations and issues like all the other graphical based password techniques. To conclude, we need our authentication systems to be more secure, reliable and robust as there is always a place for improvement. Currently we are working on the System Implementation and Evaluation. In future some other important things regarding the performance of our system will be investigated like User Adoptability and Usability and Security of our system.

VI. Conclusion

As this paper focus on the message/data senders from the particular place to the receiver through the server, at that time on the server many viruses are previously implemented by the unauthenticated person and that are able to crack the user name and password and it is directly added into the data and it causes more time for transferring the data up to the receiver and that is reduced by using the technique

of watermarking because the virus can not think, it can only crack the username and password but not the image password hence that technique can provide more security to the whole system .

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.