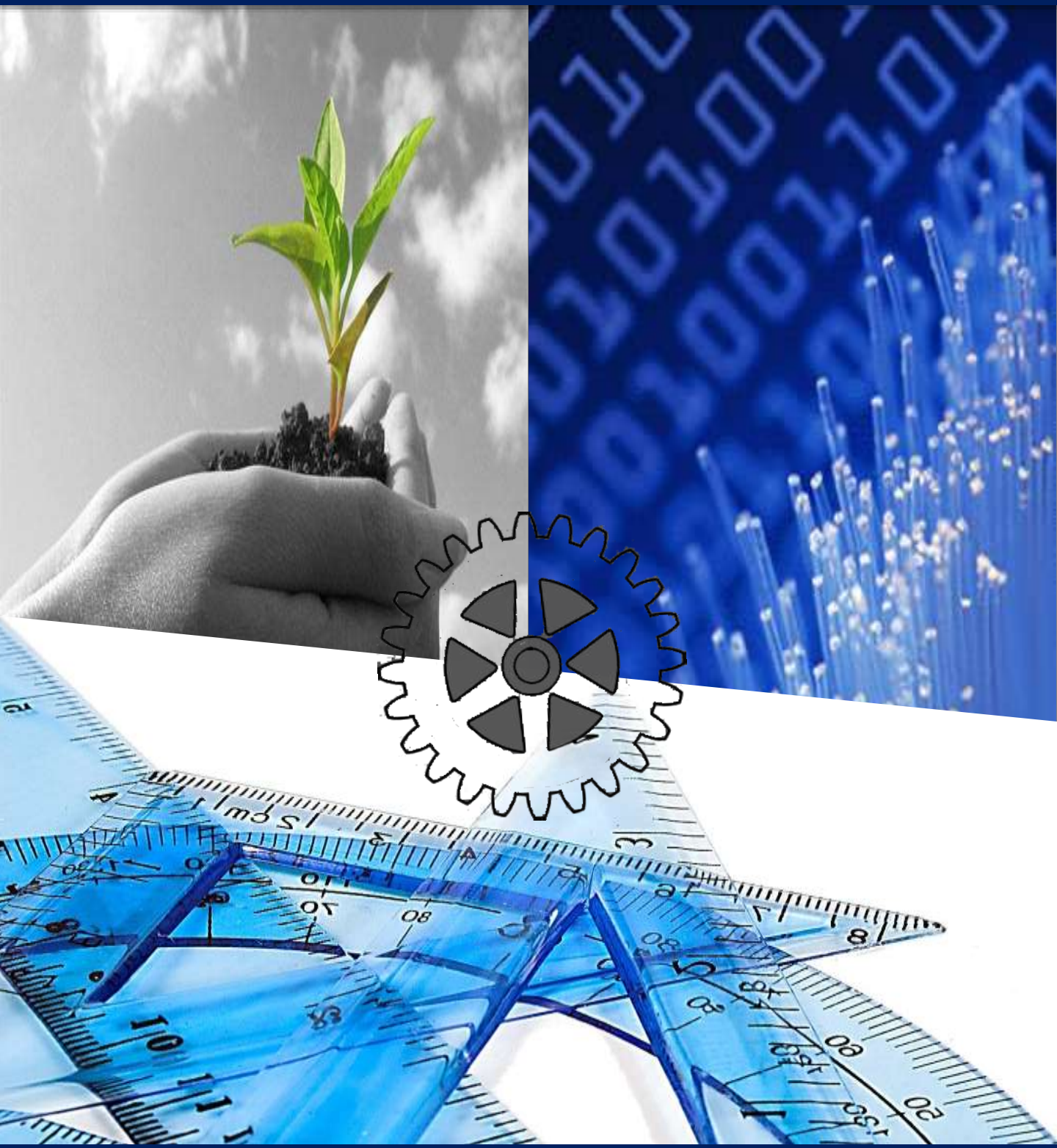
American Journal of Agricultural Science Engineering and Technology

ISSN: 2158-8104 (Online), 2164-0920 (Print)

Volume: 3, Issue: 1



Published by: e-Palli, Florida, USA

The *American Journal of Agricultural Science, Engineering and Technology (AJASET)* is blind peer reviewed international journal publishing articles that emphasize research, development and application within the fields of agricultural engineering, science and technology. The AJASET covers all areas of Agricultural Science, Engineering and Technology, publishing original research articles. The AJASET reviews article within approximately two weeks of submission and publishes accepted articles online immediately upon receiving the final versions.

Published Media: Online and Print

ISSN: 2158-8104 (Online), 2164-0920 (Print)

Frequency: 4 issues per year (*January, April, July, October*)

Area of publication: Agricultural Science, Engineering and Technology. The subjects covered by the journal includes but not limited to:

Agribusiness	Experimental Agriculture	
Agricultural Economics and Agri-business	Food science and technology	
Agricultural Engineering	Genetics Technology	
Agricultural Statistics	Geophysics	
Agriculture extension and rural development	GIS and Remote Sensing	
Agro-forestry and Ecotourism	Horticultural Science	
Agronomy	ICT for Agricultural Development	Agro-tourism Irrigation and Water Resource
Applied Agriculture	Land Use	
Applied Economics and Finance	Modeling and Crop and Animal System	
Aquaculture	Pathology and Plant Protection	Bioinformatics Plant Breeding and Crop Science
Biotechnology, Bio-composite Technology	Post harvesting Technique and Technology	
Climate Change and Green Technology	Precision Agriculture	
Collaborative Engineering	Production Engineering	Computational Biology
Renewable Energy		
Crop Science	Social Science and Agricultural Development	
Decision Support System	Soil Science	Entomology Tropical Agriculture
Environmental Science and Extension	Veterinary Science and Technology	

Members of Editorial Board

TABLE OF CONTENT

USER AUTHENTICATION THROUGH CUED CLICK POINTS BASED GRAPHICAL PASSWORD

Hasi Saha[1*], G C Saha[2], Roshidul.H[3], Zakirul Islam[4]

ABSTRACT

User authentication is a fundamental component in most computer security context. In recent years, computer and network security has been formulated as a technical problem. A key area in security research is authentication which is the determination of whether a user should be allowed access to a given system or resource. In this respect, Authentication is a process by which a system verifies the identity of a user. Authentication may also be generalized by saying that "to authenticate" means "to authorize". Users tend to pick passwords that can be easily guessed, on the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem some researchers have developed authentication methods that use pictures as passwords, known as graphical passwords. Graphical passwords are a proposed alternative to text passwords that have been shown to have good usability and security properties that use images for login, and leverage the picture superiority effect for good usability and memorability. Categories of graphical passwords have been distinguished on the basis of different kinds of memory retrieval (recall, cued-recall, and recognition). Though there are several kinds of graphical password, But We have choose to implement the cued click based due to efficient and more secured, Cued click points is a click-based graphical password scheme, Users click on one point per image for a sequence of images. The next image is based on the previous click-point. Performance was very good in terms of speed, accuracy, and number of errors.

Graphical passwords may offer better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words rather than the recommended jumble of characters.

Key Word: Cued click points, Graphical passwords and Authentication.

[1] Lecturer, Department of Computer Science & Information Technology, HSTU, Dinajpur, Bangladesh,hasi.cse3@gmail.com

[2] Assistant Professor, Department of Computer Science & Information Technology, BSMRAU, Gazipur, Bangladesh

[3] Associate Professor, Department of Computer Science & Information Technology, BSMRAU, Gazipur, Bangladesh

[4] Department of Computer Science & Information Technology, HSTU, Dinajpur, Bangladesh

Introduction

User authorization includes the problems of security and usability. It is not acceptable if both are essential and important. The issue is proved under the information-based authorized methods. Graphical passwords are very important and safe than common text passwords since they tackle the capability of the man to identify and recall the pictures. Under this theory, we studied under the field of information-based on usability and security. Text-Based Password is the series of features which has gain permission to the file, PC, or application. The passwords are simple and cheap to execute and it is known to many users. The brains can function and save great quantity of graphical data since human beings live and communicate within atmosphere and the sense of view is predominant for many actions. This graphical information shows numerous bytes of data and hence to give great password spaces. Hence, graphical password methods give the method to create passwords of human-friendly to enhance the stage of safety. The use of passwords is known to be ancient. Sentries would challenge those wishing to enter an area or approaching it to supply a password or watchword, and would only allow a person or group to pass if they knew the password. In modern times, user names and passwords are commonly used by people during a log in process that controls access to protected computer operating systems, mobile phones, cable TV decoders, automated teller machines (ATMs), etc.

Authentication is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person or software program, tracing the origins of an artifact, or ensuring that a product is what it's packaging and labeling claims to be. Authentication often involves verifying the validity of at least one form of identification (F.Alsulaiman and A.El Saddik, 2006).Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of login password (K. Renaud, 2005). Authentication has become mere important for an organization to provide an accurate and reliable means of authorization (Khan 2007). The authentication methods can be divided into three major parts, such as

- **Token based Techniques.**
- **Biometric based Techniques.**
- **Knowledge based Techniques**.

Humans have exceptional ability to recognize images previously seen, even if those images were viewed very briefly. Several recognition-based graphical password schemes have been

proposed in recent years (S. Akula *et alI,* 2004*)*. Sobrado and Birget developed a graphical password technique that deals with the shoulder- surfing problem (L.Sobrado and J.-C. Birget,2002). In the first scheme, the system will display a number of pass-objects (pre-selected by user) among many other objects

In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Graphical passwords requiring pure recall are most similar to text passwords because users must remember their password and reproduce it without any cues from the system (I. Jeremyn *et a*l, *1999)*. This is a difficult memory task and users sometimes devise ways of using the interface as a cue even though it is not intended as such.

In Draw-A-Secret DAS (G. H. Bower *et al*, 1975), users draw their password on a 2D grid using a stylus or mouse (see Figure: 2.3). The password is composed of the coordinates of the grid cells that the user passes through while drawing. A drawing can consist of one continuous pen stroke or several strokes.

To log in, users repeat the same path through the grid cells. The theoretical password space is determined by the coarseness of the underlying 2D grid and the complexity of the images. A coarser grid helps with usability, while a finer grid increases the size of the password space.

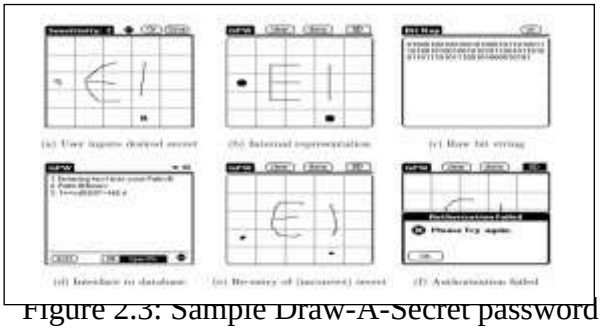


Figure 2.3: Sample Draw-A-Secret password

The study has been carried out to achieve the following objectives:

Now a day we are using many system, whether it is computer based or web based. The security of the system is the main fact. For the security of the system we are facing the password system. The main objectives of my proposed system is given below

- The objective of the proposed system is to implement of a Cued Click Points graphical password.
- Design and develop a password system that is easy to guess.
- To design a system that is acceptable to all type of users, although he/she is an illiterate.
- To design a system that is implemented as a password system in both desktop and web.
- To design a system that is easy to maintain.

Background Study

i. Background of the Text password

Despite the large number of options for authentication, text passwords remain the most common choice (*K.* Renaud, 2005) for several reasons. Text passwords are easy and inexpensive to implement, and are familiar to most users. And finally, passwords are portable since users simply have to recall them, as opposed to tokens which must be carried. However, text passwords also have a number of the inadequacies from both security and usability viewpoints, such as being difficult to remember and being predictable if user-choice is allowed (*D.* Klein, 1990*).*

ii. Background of the Graphical Password

Here we discuss some graphical password systems based on recognition or cued recall of images. Most existing systems are based on recognition. The best known of these systems are Pass faces. To create a password, the user chose four images of human faces from a portfolio of faces. To log in the user saw a grid of nine faces, which included one face previously chosen by the user and eight decoy faces. The user had to click anywhere on the known face. This procedure was repeated with different target and decoy faces, for a total of four rounds. If the user chose all four correct faces, he or she successfully logged in. Data from this study suggest that Pass faces are more memorable than alphanumeric passwords. On the other hand, passwords based on image recognition have a serious disadvantage. Only a small number of faces can be displayed on each screen, e.g., in Pass faces nine faces. An attacker has a 1-in-9 chance of guessing this Pass face. Consequently, the login process requires repetitive rounds of face recognition. If four rounds are used the chance of guessing the password is $(1/9)^4$ = 1.5 x 10-4. With a few thousand random guesses an attacker would be likely to find the password. To increase security similar to that of 8-character alphanumeric password, 15 or 16 rounds would be required. This could be slow and annoying to the user (D. Davis *et al*, august 2004).

In Pass Points, a password consists of a sequence of five click-points on a given image. Users may select any pixels in the image as click-points for their password. To log in, they repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points (*K.P. Yee*, 2004).

The usability and security of this scheme was evaluated by the original authors (*S.*Chiasson,July 2007) and subsequently by others. It was found that although relatively usable, security concerns remain. The primary security problem is hotspots: different users tend to select similar click-points as part of their passwords. Attackers who gain knowledge of these hotspots through harvesting sample passwords or through automated image processing techniques can build attack dictionaries and more successfully guess Pass Points passwords (Thorpe, J. and van Oorschot, 2007*)*.

Blonder-style passwords are based on cued recall. A user clicks on several previously chosen locations in a single image to log in. As implemented by Pass logix Corporation (Boroditsky, 2002), the user chooses several predefined regions in an image as his or her password. To log in the user has to click on the same regions. The problem with this scheme is that the number of predefined regions is small, perhaps a few dozens in a picture. The password may have to be up to 12 clicks for adequate security, again tedious for the user. Another problem of this system is the need for the predefined regions to be readily identifiable. In effect, this requires artificial, cartoon-like images rather than complex, real-world scenes.

Proposed System

We propose and examine the usability and security of Cued Click Points (CCP), a cued-recall graphical password technique. Users click on one point per image for a sequence of images. The next image is based on the previous click-point. We present the results of an initial user study which revealed positive results. Performance was very good in terms of speed, accuracy, and number of errors.

1) Users preferred CCP to Pass Points (Wiedenbecketal,2005), saying that selecting and remembering only one point per image was easier, and that seeing each image triggered their memory of where the corresponding point was located. We also suggest that CCP provides greater security than Pass Points because the number of images increases the workload for attackers or a sequence of images. The next image displayed is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in. CCP offers both improved usability and security.

Requirement Specification

Cued Click Based Password Scheme

In the Cued click based graphical password, the image is displayed on the screen by the system. The image is not secret and has no role other than helping the user remember the click points. Any pixel in the image is a candidate for a click point.To log in, the user has to click again closely to the chosen points, in the given sequence. Since it is almost impossible for human users to Click repeatedly on exactly the exact point, the system allows for an error tolerance r in the click locations (e.g., a disk with radius r = 7 or 10 pixels). This is done by quantizing (discretizing) the click locations, using three different square grids, as described in [12]. Each grid has width 6r between grid lines (horizontal or vertical).Each one of the three grids is staggered with respect to the previous grid by a distance 2r vertically and a distance 2r horizontally;(see Figure: 2. 1)

If there were only one quantization grid then a selected click point could be close to a grid line and small variations in the user's clicking could lead to a click in a different grid square, thus leading to the wrong password. On the other hand, one can prove that with the three staggered grids every point in a two-dimensional image is at distance at least r from the grid lines of at least one of the three grids; we say that the point is safe" in that grid.

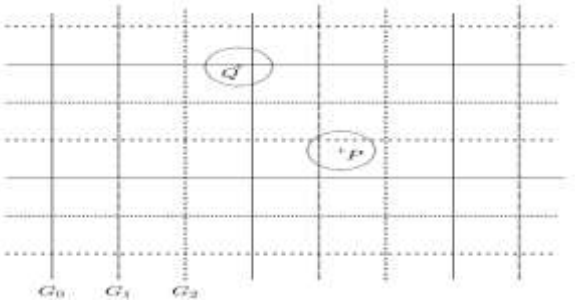


Figure 2.1: Three staggered grids.

The simultaneous use of multiple grids makes the click points robust" against the inevitable small uncertainties in the clicking; hence, this form of discretization is called robust discretization", or “robust quantization". Click positions are mapped into grid squares. A sequence of click points is represented by a sequence of grids together with a sequence of grid squares. For secure storage of passwords by the system, a function is applied to the sequence of grid squares. An important feature of the click points system is that the underlying images for a password are not restricted to simple comics-like drawings. Complex real-world images can be used; users can even install their own images. Natural images help users remember complex passwords better.

i. Functional Requirements

The various functional requirements of this system are the following:

- ✓ Selection of first image during registration, Database module for maintaining the framework
- ✓ Pre-Processing modules for different areas, Customizable

iii. User Interface Requirements

To achieve the objectives and benefits expected from the computer based system, it is essential for people who will be involved to be confident of their role in the new system. This involves them in understanding the overall system. As the system becomes more complex the need for education and training is more and more important. Education of the user should really have taken place much earlier in the project when they were being involved in the investigation and design work. Once the staff has been trained the system can be tested.

iv. Performance Requirements

Considering the interactive nature of the task the system must have the following characters.

- ✓ Minimum response time ,Efficient CPU utilization, Less Memory space ,High reliability ,High flexibility ,User friendly

v. Other Nonfunctional Requirements

Nonfunctional requirements define system properties and constraints it arises through user needs, because of budget constraints or organizational policies, or due to the external factors such as safety regulations, privacy registration and so on. Nonfunctional requirements are:

- ✓ Security ,Reliability, Maintainability ,Portability ,Extensibility ,Reusability, Application Affinity/Compatibility Resource Utilization

System Design and Method

A. General Overview of System Design

The purpose of system design is to create a technical solution that serves both the user and the admin. The system should be designed in such a way that is very flexible to use for both the administrator and the user. The preparation of the environment needed to build the system, the testing of the system and the migration and the preparation of the data that will ultimately be used by the system are equally important. In addition to designing the technical solution, system design is the time to initiate focused planning efforts for both the testing and data preparation activities. Both the admin section and the user section are designed in such a way that both parties enjoy the facilities of the application.

B. Modular Design of Cued Click Points Authentication

The whole system is divided into two parts i.e. the user and the admin section. That is why the modular design of the system is also divided into two modular diagrams, one for admin and another for naive user. Both modules are shown below

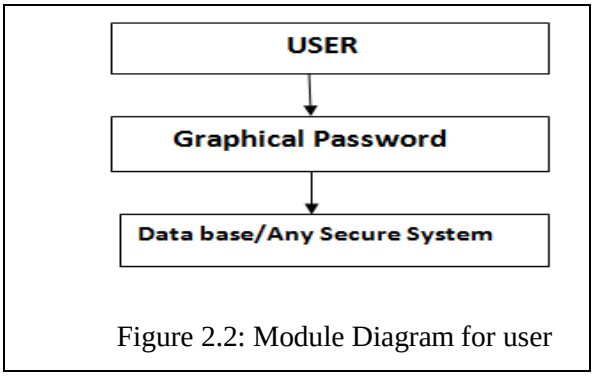


Figure 2.2: Module Diagram for user

Use Case Diagram

The use case diagram consists of the following criteria mentioned below.

It should be the scenario that describes the interaction between a user and the system and it displays the

relationship among actors and use cases.

There are two components in a use case diagram that helps understand the use case diagram. Those are,

Actor and Use-case

An actor in a use-case diagram represents a user using the system. On the other hand, a use-case represents

the set of acts that a user might perform while using the system.

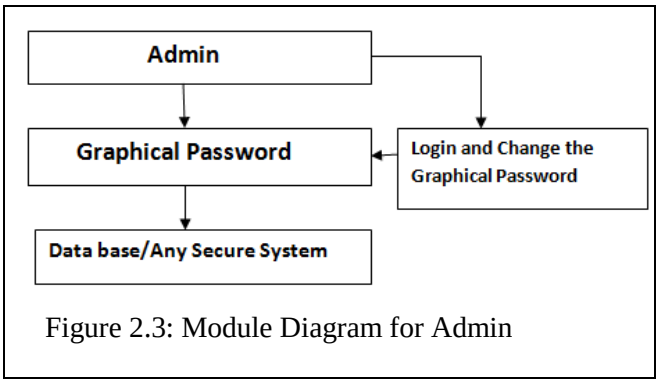


Figure 2.3: Module Diagram for Admin

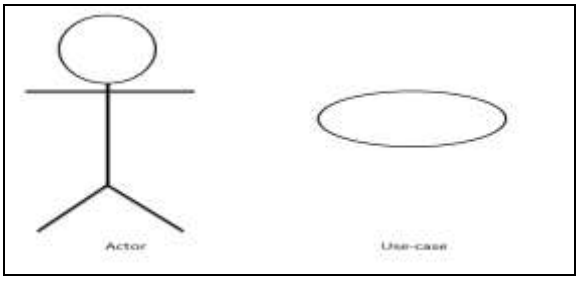


Figure 2.4: Symbol of Actor and use-case diagram.

The use-case diagram for the admin displays the interaction between the admin and the system. Figure: 2.5 show the use case diagram for admin.

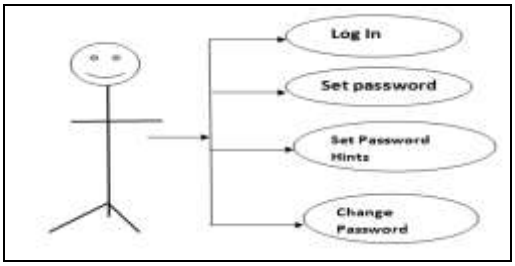


Figure 2.5: Use case Diagram for Admin

The use-case diagram for the naïve user displays the interaction between the user and the system. Figure: 2.6 show the use case diagram for the naive user.

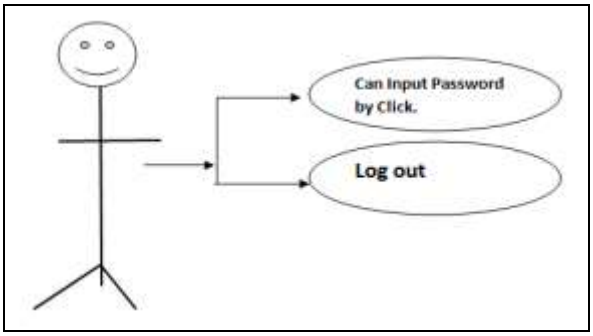


Figure 2.6: Use case Diagram for Naive user.

C. Module Design

The coding would allow any one particular module to be corrected or improved without making any significant change to any other module. The both software and hardware implementation of the system is given below:

Software Module Implementation

The designed system was implemented using Visual Studio 2010 in .net framework, Text file is used to store the information. The different modules of the system are:

User interface, Admin registration process, Picture selection process, Password selection process.

User Interface/Welcome Page

The screen shots of the Welcome page are below

The page contains Admin button, About, And Exit buttons. The Admin button shows the admin login form. About button shows information about the Author, Exit button, Exit the system.

Admin Registration Form

The admin registration form is given below:

The form takes two information, The Uses name and password. Also here is an option the Change password that is used to change the admin password, another button is CLOSE that is used to close the Login form. **Picture Browsing and Password Selection Form**

The screen shout of picture browsing and password selection form are given below.

Figure

The UPLOAD button Upload the image into image box, The SET button sets the password into click position of the image in the image box. The SEE PASSWORD shows the click position co-ordinates, and show the password hints into the password hints text box.

Results and Discussions

In this research i have practically implemented the Cued Click Point Graphical passwords which offer better security than text-based passwords and give the more accurate result. The dictionary search can often hit on a password and allow a hacker to gain entry into a system in seconds. So a series of selectable images is used on successive screen pages, and hence increase its security.

Graphical passwords are an alternative to textual alphanumeric password. It satisfies both conflicting requirements i.e. it is easy to remember & it is hard to guess. By the solution of the shoulder surfing problem, it becomes more secure & easier password scheme. By implementing other special geometric configurations like triangle & movable frame, one can achieve more security.Due to this vulnerability to shoulder surfing, it would appear that graphical passwords could never be used in environments where view of the screen is not exclusive to the person logging in. However, we have found that by applying the concept of challenge response it is possible to create schemes that counter the shoulder surfing problem.

It is more difficult to break graphical passwords using the traditional attack methods such as: We have used less number of series images, If there are many images on each page, a hacker must try every possible combination at random. If there are 100 images on each of the 8 pages in an 8-image password, there are 100^8, or 10 quadrillion (10,000,000,000,000,000), possible combinations that could form the graphical password! If the system has a built-in delay of only 0.1 second following the selection of each image until the presentation of the next page, it would take (on average) millions of years to break into the system by hitting it with random image sequences.

Conclusion

In this paper, it first introduced some typical graphical passwords authentication schemes. Then under its estimate criterions, the security analysis of graphical passwords was given. A comparison of current typical graphical password techniques is presented. The preliminary analysis suggests that it is more difficult to break cued click points graphical passwords using the traditional attack methods. Although our system aims to reduce the problems with existing graphical based password schemes but it has also some limitations and issues like the other entire graphical based password

References

F. Alsulaiman.A.S. (July 2006). A novel 3D graphical password schema. In IEEE International Conference on Virtual Environments, Human-Computer Interfaces and Measurement Systems,

K. Renaud.(2005). Evaluating authentication mechanisms, In L. Cranor and S. Garnkel, editors, Security and Usability: Designing Secure Systems That People Can Use.(pp103-128) .O'Reilly Media.

D. Klein. (1990.) Foiling the cracker: A survey of, and improvements to, password Security. In 2nd USENIX Security Workshop,

D. Davis, F. Monrose, and M. Reiter.(August 2004).On user choice in graphical password schemes. In 13th USENIX Security Symposium.

K.P. Yee. (2004). Aligning security and usability. IEEE Security & Privacy, 2(5), 48-55.

S.Chiasson, R. Biddle, and P. van Oorschot (July 2007), "A Second Look at the Usability of Click Based Graphical Passwords," Proc. ACM Symp. Usable Privacy and Security (SOUPS).

Thorpe, J. and van Oorschot (2007), P.C. Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords. USENIX Security Symp

S. Akula, V. Devisetty ((2004).),Image based registration and authentication system," Midwest Instruction and Computing Symposium.

R. Dhamija, A. Perrig,Dejµa Vu ((2000). User study using images for authentication", Ninth Usenix security Symposium 14-17.

I. Jeremyn, A. Mayer, F. Monrose, M.K. Reiter, A.D.Rubin (1999). The design and analysis of graphical passwords", Proc. 8th Usenix Security Symposium

W. Ku, M. Tsaur (2005). A remote user authentication scheme using strong graphical passwords", IEEE Conference on Local Computer Networks 351-357.

J.C. Birget, D. Hong, N. Memon (Sept. 2006). Graphical passwords based on robust discretization", IEEE Transactions on Information Forensics and Security, 1(3), 395-399. (Earlier version: Cryptology ePrint Archive, (http://eprint.iacr.org/2003/168, Aug. 2003.)

Furkan T., A. Ant Ozok, and Stephen H. Holden (July 2006)."A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords", Symposium on Usable Privacy and
Security (SOUPS). Pittsburgh, Pennsylvania, USA: ACM. 56-66.

Adams, A. and Sasse, M.A.(1999). Users are not the enemy. CACM 42, 12 41-46.

Dirik, A.E., N. Menon, and J.C Birget(2007). Modeling user choice in the PassPoints graphical password scheme. ACM SOUPS.

Pierce J.D., Jason G. Wells, Matthew J. Warren, and David R. Mackay (2003).1st Australian Information security Manage-ment Conference,

William Stallings and Lawrie Brown. (2008). Computer Security:Principle and Practices. Pearson Education.

Adams A. and Sasse M.A. (1999). Graphical Passwords. Communications of the ACM, ACM SOUPS (42), 41-46.

Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, P. C. van Oorschot. (2007), "Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism", IEEE Trans, 2(9). Ahmet Emir Dirik, Nasir Memon and

Jean-Camille Birget. (July 2007), "Modeling user choice in the PassPoints graphical password scheme", Symposium on Usable Privacy and Security 2007. USA :Pittsburgh, Pennsylvania,. ACM. 20-28.

L.Sobrado and J.-C. Birget(. 2002) "Graphical passwords", The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, 4(1).

S. Wiedenbeck, J. Waters, J. C. Birget (2005.), A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in Symposium on Usable Privacy and Security (SOUPS). Pittsburgh:Carnegie-Mellon University.

D. Nali and J. Thorpe (May 2004), "Analyzing User Choice in Graphical Passwords," Technical Report, School of Information Technology and Engineering, Canada: University of Ottawa.

INSTRUCTIONS FOR AUTHORS:

The article must type in Microsoft word and Times New Roman font. Full paper should not exceed 10 pages including figure, graph, and reference in A4 size document.

Text Format:

Language: Standard English

Font: Times New Roman

Text functions	Manuscript		
	Style	Font Size	Alignment
Title (All Capital)	Bold	12	Central
Author & Co-authors	Bold	11	Central
Address for correspondence	Normal	11	Left
Abstract heading	Bold	12	Central
Abstract & Main texts (1.5 Line Space)	Normal	11	Justify
Section heading	Bold	12	Left
Subsection heading	Bold	11	Left
Main Text	Normal	11	Justify

1) Text Flow

Title: Maximum 25 Words

Author & Co-author: Please write the Full Name of all authors and type the address of the author (s) in footnote

Abstract: Maximum 300 Words, 1.5 line spacing

> Author should mention the problem statement, methodology, major findings/contribution of the article.

Key Words: Maximum Five (5) key words

Main Text: Maximum 10 pages including abstract, graph, picture, and reference

Acknowledgement: Should not exceed 100 words

Reference: The AJASET strictly follows the *APA (American Psychological Association)* Citation Style**.**

Here are the details of APA Citation Style:

General Form of Journal:

Author, A. A., Author, B. B., & Author, C. C. (Year). Title of article, Title of Journal, xx(XX), xxx-xxx.

One Author

Turner, R. A. (2007). Coaching and consulting in multicultural contexts. Consulting Psychology Journal: Practice and Research, 59(4), 241-243.

Two to Six Authors [List all authors]

Brainerd, C. J., Reyna, V. F., Wright, R., & Mojardin, A. H. (2003). Recollection rejection: False-memory editing in children and adults. Psychological Review, 110(4), 762-784.

More than Six Authors [List the first six authors, then use et al.]

Wolchik, S. A., West, S. G., Sandler, I. N., Tein, J., Coatsworth, D., Lengua, L., et al. (2000). An experimental evaluation of theory- based mother and mother-child programs for children of divorce. Journal of Consulting and Clinical Psychology, 68(5), 843-856.

Online Journals, Magazines, Newspapers:

Article from E-journal website

Ray, O. (2004). How the mind hurts and heals the body. American Psychologist 59, 29-40. Retrieved from http://www.apa.org/journals/releases /amp59129.pdf

Lodewijkx, H. F. M. (2001, May 23). Individual-group continuity in cooperation and competition under varying communication conditions. Current Issues in Social Psychology, 6(12), 166-182. Retrieved from http://www.uiowa.edu/~grpproc/crisp/crisp.6.12.htm

NOTE: The full URL (or web address) is given with e- ournal websites (not from databases). There is no period at the end of a URL. Break a long URL before punctuation. Right Click on the URL and remove the hyperlink to eliminate the blue type and underline.

Online Report

NAACP (2005, April 29). NAACP supports Congressional fight to end predatory lending. Retrieved from http://www.naacp.org/inc//docs/washington/109/109_aa-2005-04-28.pdf

Online Report with No Author Identified and No Date

GVU's 10th WWW user survey. (n.d.). Retrieved August 19, 2005, from http://www.cc.gatech.edu/user_surveys/survey-1998-10/

Magazine Article

Henry, W. A., III. (1990, April 9). Beyond the melting pot. Time, 135, 28-31.

Newspaper Article with No Author and Discontinuous Pages

Generic Prozac debuts. (2001, August 3). The Washington Post, pp. E1, E4.

Books, reports, etc. in print format

General Form:

Author, A. A. (Year). Title of work. Location: Publisher.

One Author

Nagel, P. C. (1992). The Lees of Virginia: Seven generations of an American family. New York: Oxford University Press.

Corporate Author with an Edition and Published by the Corporate Author

American Psychiatric Association (1994). Diagnostic and statistical manual of mental disorders (4th ed.). Washington, DC: Author.

Anonymous Author

Guidelines and application form for directors, 1990 summer seminar for school teachers. (1988). Washington, DC: National Endowment for the Humanities.

Chapter in a Book

Burghardt, G. M. (1984). On the origins of play. In P. K. Smith (Ed.), Play in animals and humans (pp. 5-42). Oxford, England: Basil Blackwell.

Citing Secondary Sources:

When citing in the text a work discussed in a secondary source, give both the primary and the secondary sources. In the example below, the study by Seidenberg and McClelland was mentioned in an article by Coltheart, Curtis, Atkins, & Haller.

Seidenberg and McClelland's study (1989, as cited in Coltheart, Curtis, Atkins, & Haller, (1993) In the reference list, you would cite the secondary source that you have read, not the original study.