Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.744 – 754

RESEARCH ARTICLE

A GRAPHICAL PASSWORD BASED AUTHENTICATION BASED SYSTEM FOR MOBILE DEVICES

Er.Aman Kumar[1], Er.Naveen Bilandi[2]

[1]Department of Computer Science and Engineering, DAV University, Jalandhar, Punjab, India
[2]Department of Computer Science and Engineering, DAV University, Jalandhar, Punjab, India
Email: amank764@gmail.com, Naveen.bilandi@davuniversity.org

Abstract: Authentication is one the most important security primitive. Password authentication is most widely used authentication mechanism. Password provides security mechanism for authentication and protection services against unwanted access to resource. To address these authentication problems, a new alternative authentication method have been proposed using picture as passwords. Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and there, more secure. Using a graphical password, user click on images rather than type alphanumeric characters. In this paper, we have purposed a new hybrid graphical password based system, which is a combination of recognition and recall based techniques that offers many advantages over the existing systems and may be more convenient for the user. Our scheme is resistant to shoulder surfing attacks on graphical passwords. This scheme is proposed for mobile devices which are more handy and convenient to use than traditional desktop computer systems.

Keywords: Graphical Password, Smart Phones, Authentication, Network Security

I. Introduction

One of the major functions of any security system is the control of people in or out of protected areas. Authentication is the process of determining that the person requesting a resource is the one who he claims to be. Most of the authentication system these days uses a combination of username and password for authentication. Computer security systems must also consider the human factors such as ease of a use and accessibility. Current secure systems suffer because they mostly ignore the importance of human factors in security [1]. A password is a secret that is shared by the verifier and the customer. ”Passwords are simply secrets that are provided by the user upon request by a recipient.” They are often stored on a server in an encrypted form so that a penetration of the file system does not reveal password lists [2]. Graphical passwords (GP) use pictures instead of textual passwords and are partially motivated by the fact that humans can remember pictures more easily than a string of characters [3].A graphical password is an authentication system that works by having the user select fromimages, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA).

Graphical passwords may offer better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words. The idea of graphical passwords was originally described by Greg Blonder in 1992 [4].A dictionary search can often hit on a password and allow a hacker to gain entry into a system in seconds. But if a series of selectable images is used on successive screen pages, and 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 10 quadrillion, 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. A graphical password is easier than a text-based password for most people to remember. Suppose an 8-character password is necessary to gain entry into a particular computer network. Strong passwords can be produced that are resistant to guessing, dictionary attack. Key-loggers, shoulder-surfing and social engineering. Graphical passwords have been used in authentication for mobile phones, ATM machines, E-transactions.

II. Current Authentication Methods

Authentication is a process which allows a user to confirm his identity to an application. It provides access control and user accountability. Users often create memorable passwords which are easy for attackers to guess, but strong system assigned passwords are difficult for the users to remember. An authentication system should encourage strong passwords while maintaining usability and memorability. Authentication methods are broadly classified into three main areas. Token based authentication (two factors), Biometric based authentication (three factor), Knowledge based authentication (single factor) [5]

A. Token Based Authentication

Token based authentication is based on “Something You Posses”. For example smart cards, a driver’s license, credit card, a university ID card etc. In this method a token is used to access a specific resource by user. Many token based authentication systems also use knowledge based authentication techniques to enhance security.

B. Biometric Based Authentication

Biometric authentication system uses physiological or behavioral characteristics of a person for authentication. It is based on "Something You Are". Some of the biometric authentication systems use fingerprint recognition, face recognition, iris recognition or voice recognition to authenticate the users. Biometric identification depends on computer algorithms to make a yes or no decision .This method enhance user service by providing quick and easy identification.

C. Knowledge Based Authentication

The knowledge based authentication is the most commonly used authentication systems. They are two types: Text based password and picture based passwords. Although there are different type of authentication techniques available alphanumeric passwords are the widely used because they are versatile and it is easy to implemented use. The text based passwords need to satisfy two contradictory requirements. That is it should be easily remembered by user and it should be hard to guess by an attacker. So these text passwords are vulnerable to dictionary attacks bruteforce attacks. Knowledge based authentication can be used along with other authentication techniques to ensure security.

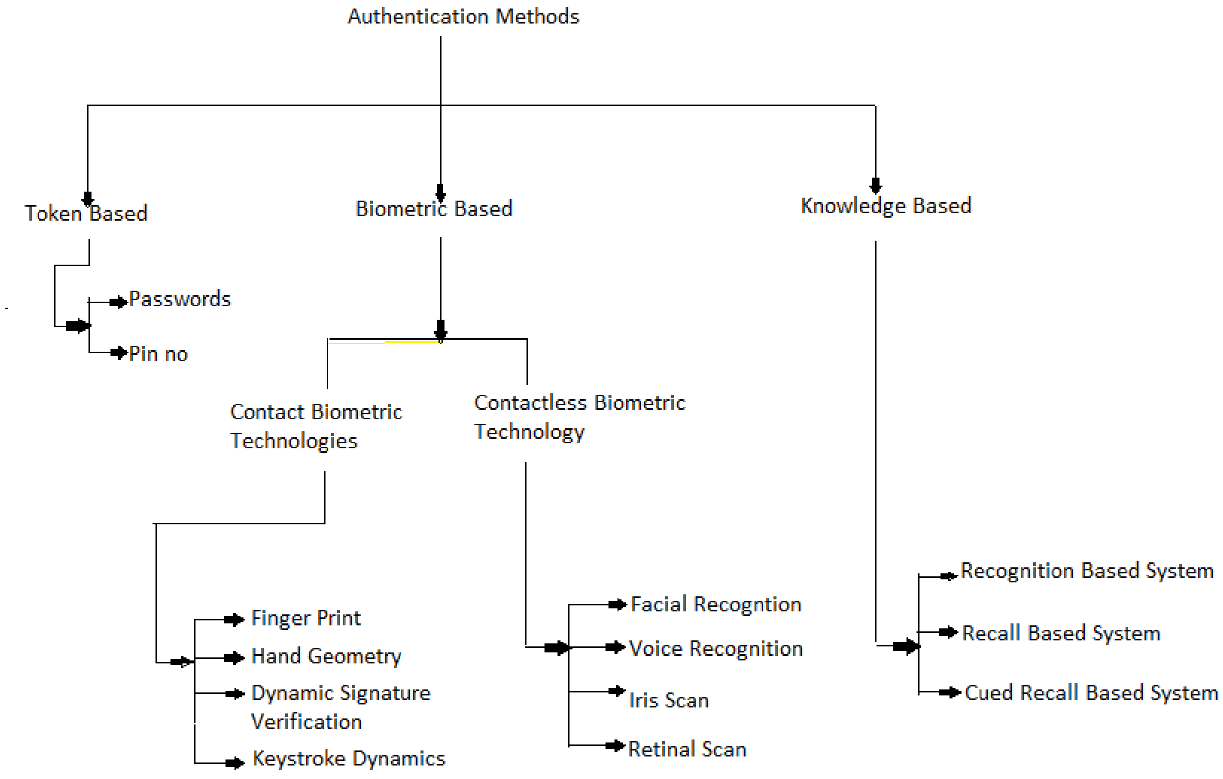

Figure1: Classification of Authentication Methods

III. Classification of Graphical Password Based Systems

Graphical based passwords schemes can be broadly classified into four main categories:

A. Recognition Based Systems

In recognition based systems which are also known as cognometric systems. Recognition based techniques involve identifying whether one has seen an image before. The user must only be able to recognize previously seen images, not generates then unaided from memory.

B. Pure Recall-Based Systems

In pure recall-based system users need to reproduce their passwords without being given any reminder, hints or gesture. Although this category is easy and convenient, but it seems that users hardly can remember their passwords similar to DAS and Qualitative DAS

C. Cued Recall-Based Systems

Cued recall based systems which are also called Icon metric Systems. In cued recall-based system, a user is provided with a hint so that he or she can recall his/her password.

D. Hybrid Systems

Hybrid systems which are typically the combination of two or more schemes. Like recognition and recall based or textual with graphical password schemes. Detailed classification of systems involved in these four categories is shown in Figure 2.

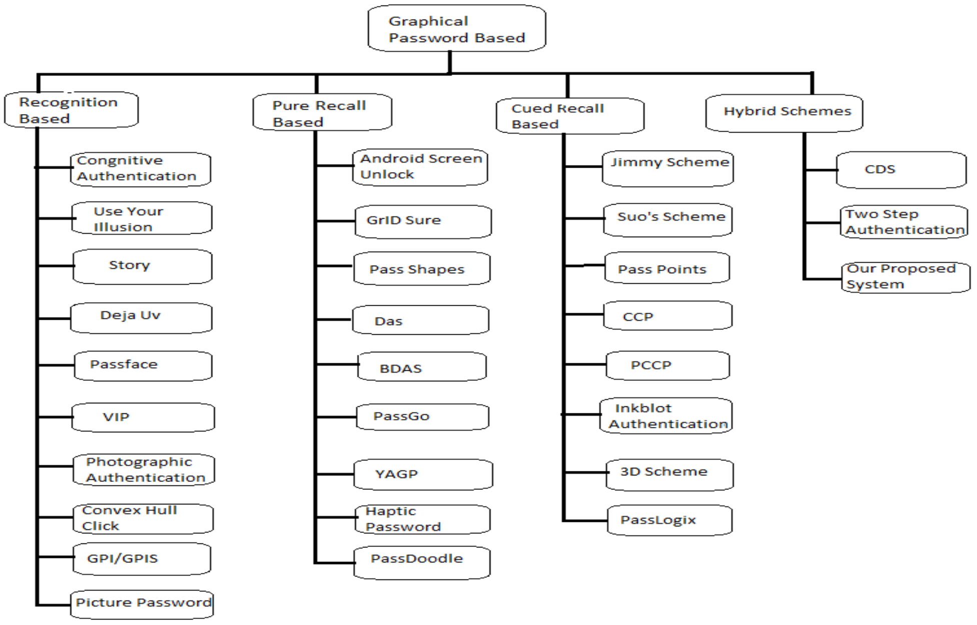

Figure 2: Classification of Graphical Password Based Systems

IV. Literature Review

Farnaz Towhidi and Maslin Masrom[6] described eight recognition-based authentication algorithms in terms of their drawbacks and attacks. In the next section, the usability standards from ISO and the related attributes for graphical user authentication usability are discussed. In this study, eight algorithms from recognition-based graphical password authentication are reviewed and surveyed.

Harsh Kumar Sarohi, Farhat Ullah Khan in their paper [7] we conduct a comprehensive survey of the existing graphical authentication systems. We have classified these methods in to three main areas: Recognition based schemes, pure recall based schemes and Cued recall based schemes. Graphical passwords are more secure than text based passwords. During our analysis we found that it is very difficult to perform attacks on graphical passwords like brute force, Dictionary attack, and spyware.

Gloriya Mathew, Shiney Thomas proposed [8] a new technique that uses cues click point graphical password method along with the use of one-time session key is proposed. Graphical passwords are strong alternative to test based and biometric authentication. The system combine graphical password and one-time session key trying to achieve the best of both methods which will increases the security. The system has adopted the crud click point technique which offers attractive usability properties, such as curing and good memorability.

Susan Wiedenbeck Jim Waters, Jean-Camille Birget and Alex Brodskiy Nasir Memon in their paper [9] we describe the Pass Point system, its security characteristics, and the empirical study we carried out comparing Pass Point to alphanumeric passwords. The empirical testing of Pass Points indicates strengths and weaknesses, but is overall encouraging.

Wazir Zada Khan, Mohammed Y Aalsalem and Yang Xiang [10] presented a new hybrid graphical password based system, which is a combination of recognition and recall based techniques that offers many advantages over the existing systems and may be more convenient for the user. 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.

A. Problems of Recognition Based Methods:

Dhamijia and Perrig proposed a graphical password based scheme Déjà Vu, based on Hash Visualization technique [11]. The drawback of this scheme is that the server needs to store a large amount of pictures which may have to be transferred over the network, delaying the authentication process. Another weakness of this system is that the server needs to store the seeds of portfolio images of each user in plaintext. Also, the process of selecting a set of pictures from picture database can be tedious and time consuming for the user. This scheme was not really secure because the passwords need to store in database and that is easy to see.

Another recognition based technique is proposed by Man et al [12]. He proposed a shoulder-surfing resistant algorithm which is similar to that developed by Sobrado and Birget. The difference is that Man et al has introduced several variants for each pass-object and each variant is assigned a unique code. Thus during authentication the user recognize pre-selected objects with an alphanumeric code and a string for each pass-object. Although it is very hard to break this kind of password but this method still requires the user to memorize alphanumeric codes for each pass-object variants.

B. Problems of Recall Based Methods:

The problem with the Grid based methods is that during authentication the user must draw his/her password in the same grids and in the same sequence. It is really hard to remember the exact coordinates of the grid. The problem with Passlogix is that the full password space is small. In addition a user chosen password might be easily guessable [9]. DAS scheme has some limitations like it is vulnerable to shoulder surfing attack if a user accesses the system in public environments, there is still a risk for the attackers to gain access to the device if the attackers obtained a copy of the stored secret, and, brute force attacks can be launched by trying all possible combinations of grid coordinates, Drawing a diagonal line and identifying a starting point from any oval shape figure using the DAS scheme itself can be a challenge for the users, and finally Difficulties might arise when the user chooses a drawing which contains strokes that pass too close to a grid-line, thus, the scheme may not be able to distinguish which cell the user is choosing.

“Pass Points” is the extended version of Blonde’s idea by eliminating the predefined boundaries and allowing arbitrary images to be used. Using this scheme it takes time to think to locate the correct click region and determine precisely where to click. Another problem with these schemes is that it is difficult to input a password through a keyboard, the most common input device; if the mouse doesn’t function well or a light pen is not available, the system cannot work properly [13]. Overall, with both “Pass Points” and “Passlogix”, looking for small spots in a rich picture might be tiresome and unpleasant for users with weak vision.

V. Proposed System

Taking into account all the problems and limitations of graphical based schemes, we have proposed a hybrid system for authentication. This hybrid system is a mixture of both recognition and recall based.Proposed system is an approach towards more reliable, secure, user-friendly, and robust authentication. We have also reduced the shoulder surfing problem to some extent.

A. Working of Proposed System

Proposed system comprises of 9 steps out of which steps 1-3 are registration steps and steps 4-9 are the authentication steps.

Step 1: The first step is to type the user name and a textual password which is stored in the database. During authentication the user has to give that specific user name and textual password in order to log in.

Step 2: In this second step objects are displayed to the user and he/she selects minimum of three objects from the set and there is no limit for maximum number of objects. This is done by using one of the recognition based schemes. The selected objects are then drawn by the user, which are stored in the database with the specific username. Objects may be symbols, characters, auto shapes, simple daily seen objects etc.

Step 3: In this third step during authentication, the user draws pre-selected objects as his password on a touch sensitive screen with a mouse or a stylus. This will be done using the pure recall based methods.

Step 4: In this step, the system performs pre-processing.

Step 5: In the fifth step, the system gets the input from the user and merges the strokes in the user drawn sketch.

Step 6: After stroke merging, the system constructs the hierarchy.

Step 7: Seventh step is the sketch simplification.

Step 8: In the eighth step three types of features are extracted from the sketch drawn by the user.

Step 9: The last step is called hierarchical matching.

During registration, the user selects the user name and a textual password in a conventional manner and then chooses the objects as password. Textual password can be a mixture of digits, lowercase and uppercase letter. After this the system shows objects on the screen of a PDA to select as a graphical password. After choosing the objects, the user draws those objects on a screen with a stylus or a mouse. Objects drawn by the user are stored in the database with his/her username. In object selection, each object can be selected any number of times. Flow chart of registration phase is shown in Figure 3.

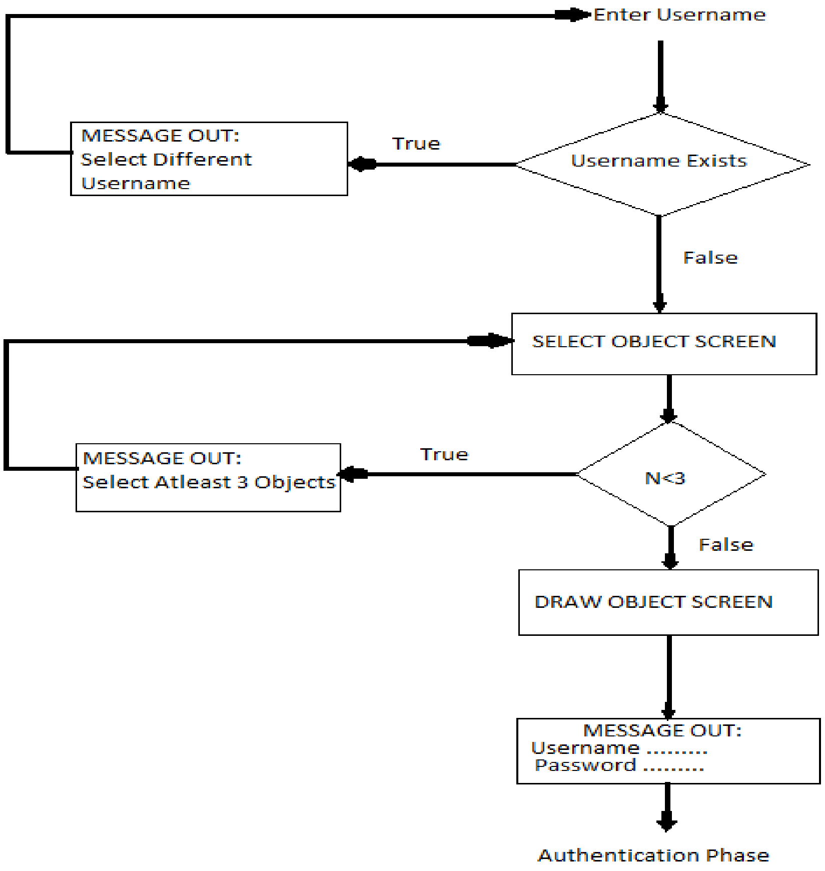

Figure 3: Flow chart for Registration Phase

During authentication, the user has to first give his username and textual password and then draw pre-selected objects. These objects are then matched with the templates of all the objects stored in the database. Flow chart of authentication phase is shown in Figure 4. The phases during the authentication like the pre-processing, stroke merging, hierarchy construction, sketch simplification, feature extraction, and hierarchical matching are the steps. They propose a novel method for the retrieval of hand drawn sketches from the database, finally ranking the best matches. In the proposed system, the user will be authenticated only if the drawn sketch is fully matched with the selected object's template stored in the database. Pre-processing of hand drawn sketches is done prior to recognition and normally involves noise reduction and normalization. The noise occur in the image by user is generally due to the limited accuracy of human drawn images. [14]

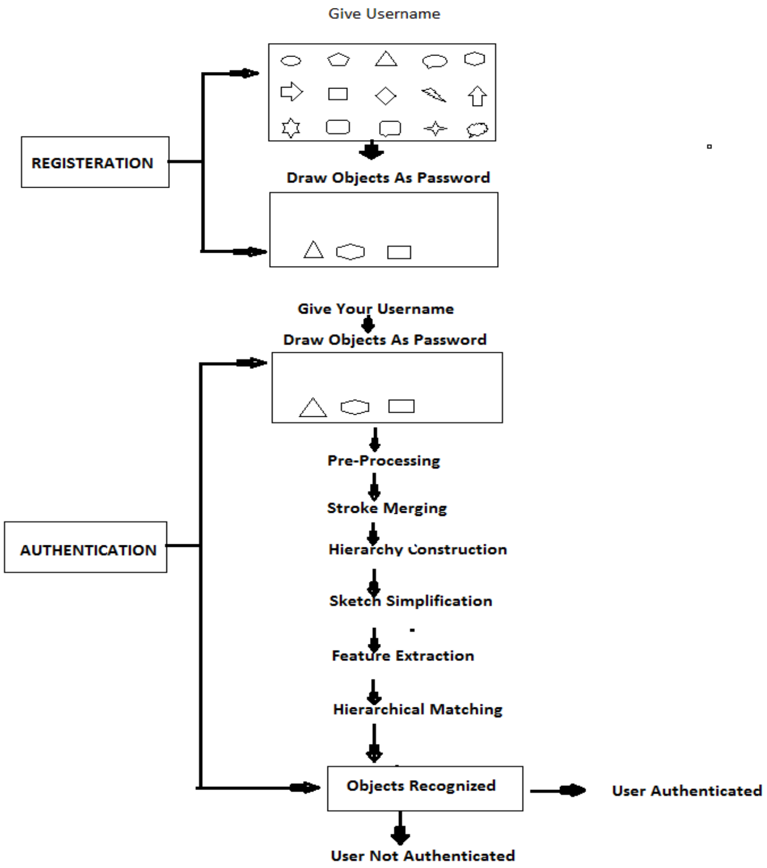

Figure 4: Graphical Representation of Proposed System

In case, if user draws very large or a very small sketch then the system performs size normalization which adjusts the symbols or sketches to a standard size. The Stroke merging phase is use to merge the strokes which are broken at end points. If the end points are not close, then that stroke is considered as open stroke and it may be merged with another open stroke if the end point of one stroke is close to the end point of the other. The strokes are then represented in a hierarchy to simplify the image and to make it meaningful for further phases [15]. In the next step of sketch simplification, a shaded region is represented by a single hyper-stroke. After sketch simplification three types of features are extracted from the user re-drawn sketch. These features are hyper stroke features, Stroke features, and bi-stroke features.

In the last step of hierarchical matching, the similarity is evaluation the top to bottom hierarchical manner. The user is allowed to draw in an unrestricted manner. The overall process is difficult because free hand sketching is a difficult job. The order in which the user has selected the objects does matter in our proposed system i.e. during the authentication phase, the user can draw his pre-selected objects in the same order as he had selected during the registration phase. So, in this way the total combinations of each password will be 2^n –1, 'n' being the number of objects selected by the user as password during the registration phase.

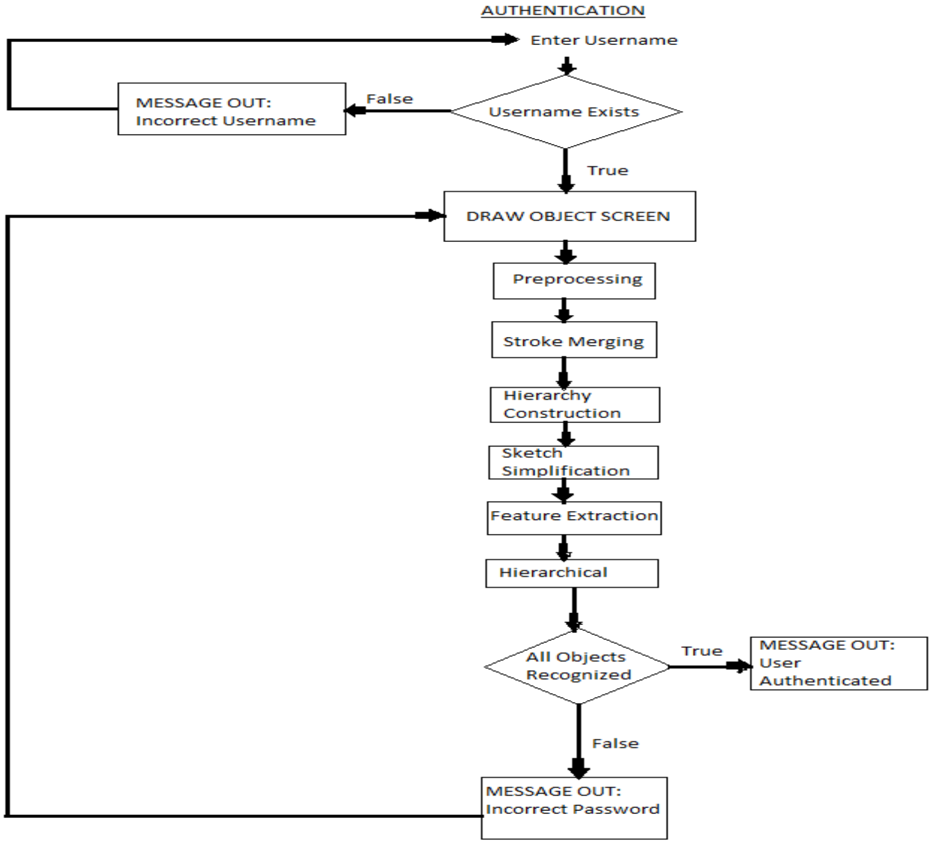

Figure 5: Flow Chart for Authentication Phase

VI. Conclusion & Future work

In many authentication methods and techniques are available but each with its own advantages and shortcomings. In view of above, we have proposed authentication system which is based on graphical password schemes. Although our system to reduce the problems with existing graphical based password schemes but it has also some limitations any issues like all the other graphical based password techniques. We need our authentication systems to be more secure, reliable and robust as there is always a place for improvement. 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.

References

[1] Rachna Dhamija and Adrian Perrig, “Deja Vu: A User Study. Using Images for Authentication” In Proceedings of the 9th USENIX Security Symposium, August 2000.

[2]Authentication:http://www.objs.com/survey/authent.htm

[3] Patric Elftmann, Diploma Thesis, “Secure Alternatives to Password-Based Authentication Mechanisms” Aachen, Germany October 2006.

[4] G. E. Blonder Graphical password, U.S. Patent 5559961, Lucent Technologies, Inc. (Murray Hill, NJ), August 1995.

[5] Approaches to Authentication:
http://www.e.govt.nz/plone/archive/services/see/see-pki-paper-/chapter6.html?q=archive/services/see/see-pki-paper-3/chapter6.html

[6] Ali Mohamed Eljetlawi, Norafida Ithnin. "Graphical password: comprehensive study of the usability features of the recognition base graphical password methods," Third 2008 International Conference on Convergence and Hybrid Information Technology. 1137-1143. 2008

[7] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication Using Graphical Passwords: Basic Results", In Human-Computer Interaction International (HCII 2005), Las Vegas, NV, 2005.

[8]"PersuasiveCued ClickPoint:Design,Implementation and Evaluation of a Knowledge-Based Authentication Mechanism", Sonia Chiasson, Member, IEEE, Elizabeth Stobert ,Student Member, IEEE Alain Forget, Robert Biddle, Member, IEEE, and Paul C, van Oorschot, Member, IEEE.

[9] Wiedenbeck, S., Waters, J., Birget, J.C., Broditskiy, A., & Memon, N. (2005). Pass Points: Design and evaluation of a graphical password system. Submitted

[10] X. Suo, **"**A design and analysis of graphical password**"**, Master's thesis, College of Arts and Science, Georgia State University, August 2006

[11] A.Perrig and D.Song, "Hash Visualization: A New Technique to improve Real-World Security". In International Workshop on Cryptographic Techniques and E-Commerce, pages 131--138, 1999.

[12] S. Man, D. Hong, and M. Mathews,"A shoulder surfing resistant graphical password scheme", In Proceedings of International conference on security and management. Las Vegas, NV, 2003.

[13] Xiayuan Suo, YingZhu, G. Scott. Owen, "Graphical Passwords: A Survey", In Proceedings of Annual Computer Security Applications Conference, 2005.

[14] Hafiz Zahid Ullah Khan, "Comparative Study of Authentication Techniques", International Journal of Video & Image Processing and Network Security IJVIPNS Vol: 10 No: 04.

[15]Wing Ho Leung and Tsuhan Chen, "Hierarchical Matching For Retrieval of Hand Drawn Sketches", In Proceeding of International Conference on Multimedia and Expo –Volume 2(Icme'03), 2003