# A Graphical Password based on Captcha (AGPC)

Kanupriya R R
Computer and Information Science department
Sarabhai Institute of Science and Technology ( SIST)
Vellanad, Thiruvananthapuram, Kerala

Reshmy V R
Computer and Information Science department
Sarabhai Institute of Science and Technology ( SIST)
Vellanad, Thiruvananthapuram, Kerala

***Abstract*-- A Graphical Password based on Captcha (AGPC) introduces a new password system that incorporates artificial intelligence and graphical password system. Text-based password schemes have inherent security and usability problems, leading to the development of graphical password schemes. A great many graphical password schemes have been proposed as alternatives to text-based password authentication. However, most of these alternate schemes are vulnerable to spyware attacks. Using CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) we can retain the advantages of graphical password schemes while reducing usability and security problems. Captcha distinguishes human users from computer by presenting a challenge i.e. a puzzle beyond the capability of computer but easy for humans. CAPTCHA is now a standard internet security technique to protect online email and other services from being abused by malicious programs. Here we introduce a new graphical password scheme based on captcha technology with the help of an algorithm called Visual Cryptographic Scheme Algorithm (VCS algorithm).**

***Keywords—Captcha, Graphical password, VCS Algorithm***

## I. INTRODUCTION

Computer security depends largely on passwords to authenticate human users. Today, authentication is the principal method to guarantee information security and the most common and convenient method is password authentication. Nowadays username and text-based password are the most common and widely used technique in knowledge based authentication methods. However, the vulnerabilities of this traditional technique are well known. One of the main problems is in remembering the passwords. Studies have shown that users tend to pick short passwords or passwords that are easily remembered. Unfortunately these passwords can be easily guessed or broken. On the other hand, passwords that are hard to guess or break are often hard to remember. Thus large portion of customer service calls are related to one's forgetting his or her password. Previous studies have showed that human's memory can only remember limited number of text-based passwords, because of that limitation they are likely to write down their password in the form of plaintext. In addition, they also tend to use a single password for different kinds of applications.

The main objective of improving the existing user authentication technology is to make the method usable and secure for the user. To fulfill the need for improved password usability and security, the concept of graphical passwords was proposed in 1996. The main goal of graphical passwords is to use images or shapes to replace text, since people perform far better when remembering pictures than words. For over a century, psychology studies have recognized the human brain is apparently superior memory for recognizing and recalling visual information as opposed to verbal or textual information. It has also been suggested that graphical Passwords are hard to guess or broken by brute force methods. 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. In addition, graphical passwords have also been implemented and applied to workstations, websites, login applications, ATM and mobile devices such as personal digital assistance (PDAs). However existing graphical passwords are far from perfect.

A new authentication scheme combining graphical password with text-based CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) is proposed here. Captcha distinguishes human users from computer by presenting a challenge.

Shoulder surfing attack is addressed here. i.e. the secret cannot be stolen even when an attacker watches or camera records when the victim enter the password, online guessing attack, relay attacks, dictionary attacks etc. It has many applications for practical security including online polls, free email services, search engine bots etc.

## II. CAPTCHA

Using hard AI problems for security is an exciting new paradigm. Under this paradigm, the most notable primitive invented is Captcha which distinguishes human users from computers by presenting a challenge i.e. a puzzle, beyond the capability of computers but easy for humans. Captcha is now a standard Internet security technique to protect online email and other services from being abused by bots.

### *A. Captcha classification*

There are two types of visual Captcha:

- text Captcha
- Image-Recognition Captcha (IRC).

The former relies on character recognition while the latter relies on recognition of non-character objects. Text Captcha relies on the difficulty of character segmentation, which is computationally expensive and combinatorialy hard. Machine recognition of non-character objects is far less capable than character recognition. IRCs rely on the difficulty

of object identification or classification, possibly combined with the difficulty of object segmentation.

*1) Text Captcha*

EZ-Gimpy and Gimpy-r are two examples of the visual text CAPTCHA. They are objects with background clutter and distortions. In both EZ-Gimpy and Gimpy-r, the user is presented with a 290 pixel × 80 pixel JPEG image and prompted to enter a "guess" as to what word or sequence of letters is shown. The letters in EZ-Gimpy are from one font, and the background clutter can consist of white noise, a grid, or other patterns such as swirls. The letters in Gimpy-r are from two fonts, and the background clutter is mostly different colored distortion patterns such as boxes, waves, and ripples. The EZ-Gimpy test uses a dictionary of 561 words while the Gimpy-r test uses a set of four random letters from a dictionary of 19 letters.

*2) Image Recognition Captcha*

There are three tasks to construct image recognition CAPTCHAs.

a) The naming images CAPTCHA.

The naming CAPTCHA presents six images to the user. If the user correctly types the common term associated with the images, the user passes the round. Figure 3 shows an example of one round of the naming CAPTCHA. The common term illustrated in the figure is astronaut.

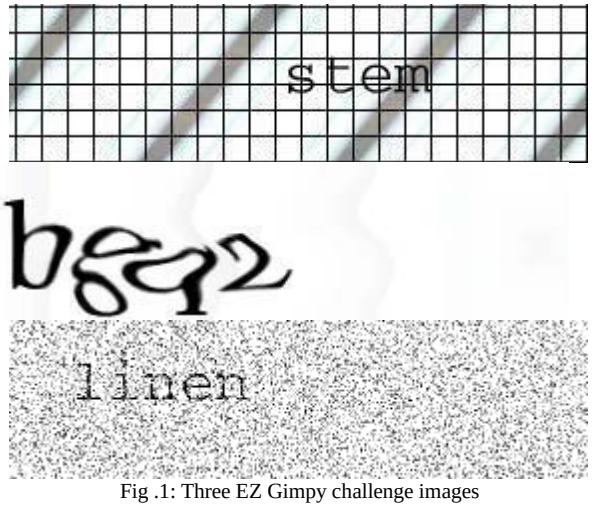


Fig .1: Three EZ Gimpy challenge images


Fig. 2: Three Gimpy-r challenge images

*b) The distinguishing images CAPTCHA.*

The distinguishing CAPTCHA presents two sets of images to the user. Each set contains three images of the same subject. With equal probability, both sets either have the same subject or not. The user must determine whether or not the sets have the same subject in order to pass the round. For example, of six images, the subject of the top three images could be briefcase, and the subject of the bottom three images could be plate.

c) The identifying anomalies CAPTCHA.

The anomaly CAPTCHA presents six images to the user: five images are of the same subject, and one image (the anomalous image) shows a different subject. The user must identify the anomalous image to pass the test. Figure 3 shows five images of moose and one image of weave.

## III. GRAPHICAL PASSWORDS

According to the authentication methods, the current graphical passwords can be broadly categorized into four general classes:-

- Drawmetric schemes
- Locimetric schemes
- Cognometric schemes
- Hybrid schemes

Hybrid schemes combine two or more of Drawmetric schemes, Locimetric schemes, and Cognometric schemes.

*A. Drawmetric schemes*

Drawmetric schemes are also known as recall-based schemes. In Drawmetric schemes a user reproduces a drawing on a grid that he/she created or selected during the registration process. DAS (Draw A Secret) was the first scheme in this category. DAS was proposed by Jermyn in1999. In this scheme, a user is asked to draw a simple picture using a mouse or stylus. The drawing consists of one continuous stroke or several strokes separated by "pen-ups", on an NxN grid. The picture is mapped to a sequence of coordinate pair of grid cells. For a successful login, the user needs to reproduce the picture. According to a survey, users tend to set predictable passwords which are vulnerable to dictionary attack. Thorpe proposed Grid Selection, which is composed of two parts: the drawing grid and the DAS password. Users first select a rectangular region from a large and fine grained grid, and then draw the picture on the region, similar to DAS. Users have to remember the location of chosen region, increasing memorability difficulty. BDAS

proposed by Dunphy is an extension of DAS where a background image is added to DAS. But possible hotspots or image-specific patterns are vulnerable to dictionary attack.

Inspired by old Chinese game of "Go", Tao designed a new graphical password scheme, Pass-Go, in which a user drew the password using grid intersection point instead of cells. Consequently the coordinate system refers to a matrix of intersections rather than cells as in DAS

Due to finer grid structure, the theoretical password space of Pass-Go, which allows diagonal movements and pen color as optional parameters, is larger than DAS's. Background Pass-Go (BPG), proposed by Por, added background images to Pass-Go to assist users in remembering their password and reducing the success rate of guess attacks, similar to idea of BDAS. Multi-Grid Background Pass-Go (MGBPG) proposed by Por based on the inspiration of Multi-Grid DAS, Pass-Go and BPG. In MGBPG, users can select a personalized background image and grid line scaling to decrease memorability. The issue in MGBPG is to find a balance between a memorable password and higher security.

Varenhorst presented the Passdoodle, allowing users to create a freehand drawing as a password without a visible grid. A doodle should consist of at least two pen-strokes placed anywhere on the screen and can be drawn in a number of colors. The matching process in

Passdoodle is more complex than in DAS. After reading the mouse input, the system begins to scale and stretch the doodle into a grid, and then compares the stretched doodle with stored user data. Weiss proposed PassShapes, a similar system to Passdoodle. PassShapes is simple geometric shapes constructed from an arbitrary combination of eight different strokes. During login, there is no grid and the password can be drawn in variable sizes or positions on the screen since only strokes and their order are evaluated.

To date there are only two commercial products of Drawmetric graphical password schemes. An unlock Scheme to unlock screens on Google Android cell phones. A user can decide his own unlocking pattern by drawing his finger or stylus over several points in 3x3 grid. However the Android screen-unlock scheme has been proved to be susceptible to "smudge attack" where attackers get the password via the smudges on the screen. In the windows 8 system Microsoft introduced a new graphical password scheme. First a user is provided an image and then draws a set of gestures in the image. The three types of gestures provided include: circle straight lines, and taps. Any combination of those gestures can be used for a password. But attack types like hotspots (i.e. dictionary attack) and shoulder surfing remains a concern.

*B. Locimetric scheme*

Locimetric schemes are also called click-based graphical password schemes. In Locimetric schemes, a user is provided with an image so that he or she can choose any point in the specified zone or any place in the image as a password click point. Successful authentication includes the right click points and their correct order. In Blonder's first graphical password scheme, the user is required to click on predetermined areas (or tag regions) of the predetermined graphical image in a predetermined sequence, as a means of entering a password. Blonder's authentication system had some disadvantages. For example predefined regions should be readily identifiable and the number of predefined regions is small. V-GO is a commercial graphical password scheme developed by Passlogix based on Blonder's idea. In order to be authenticated users must click on various items in a graphical image in the correct sequence. Every candidate item in the image has an invisible borderline for detecting whether or not an item has been clicked by a mouse. Users can easily remember the password by using components.

In wiedenbeck's Passpoints users can click on any place in the image (as opposed to some pre-defined areas ) to create a password. To login users must re-enter the chosen click points within a system specified tolerance and also in the correct order. The theoretical password space of Passpoints is quiet large. But Passpoint is vulnerable. To shoulder surfing attack since attackers can observe the clickpoints directly during authentication. Sfr proposed Viskey is a commercial version of Passpoints for the PPC (pocket personal computer). This scheme is used for screen-unlock by taping on a correct sequence of click-points with a stylus or finger.

Chiasson proposed Cued-click points (CCP) to reduce hotspots and improve usability of click based graphical password schemes, a variation of passpoints in which users click on one point for a sequence of images. The next image is displayed based on the location of the previous click point that is, each image after the first is a deterministic function of the current image and the coordinates of the user-entered click-point. If users click an incorrect point, a wrong image will be displayed. It is meaningless to attackers without knowledge of the correct password. But users tend to select click-points falling within known hotspots. Chiasson later designed Persuasive Cued Click Points (PCCP) by adding a persuasive feature to encourage users to select more random passwords. Specifically during password creation the images are slightly shaded except for a small square view port area randomly positioned on the image. Users are required to select a click point within this viewport and not click outside of this viewport. They can press the shuffle button to randomly reposition the viewport as often as they want until a suitable location is found. During password login the images are displayed normally without shading or the viewport and users are allowed to click anywhere. PCCP is effective at removing major concerns related to common hotspots and patterns thus increasing the effective password space while still maintaining usability. PCCP further reduces the hotspot effects. However as it failed to address the issue of shoulder surfing attack, user's passwords of CCP and PCCP can still be broken as long as the attacker captures the login process or input sequence.

*C. Cognometric schemes*

Cognometric schemes also known as recognition based schemes or search metric schemes, involve identifying whether one has seen an image before. In cognometric schemes the user creates a password by choosing several images from a large portfolio of images, with the selected images becoming the user's password. During authentication the user must successfully identify his/her password image from decoy images. Dhamija proposed déjà vu in 2000 where users selected a certain number of random art pictures from a

set of pictures generated by a program in the registration phase. During authentication the system displays a challenge set that contains both password pictures and decoy pictures. User must identify the password pictures. It is convenient to store and transmit the art images generated by small initial seeds. Moreover the art images make it difficult to record or share with others. Déjà vu has many drawbacks. For example an obscure picture is hard to remember and the password space is much smaller than that of alphanumeric passwords.

PassFaces are proposed by Brostoff motivated by the fact that human is familiar with faces. Users need to click on face images pre-selected in registration for several such rounds. Relative literature reported serious security problems in PassFaces. It is vulnerable to Shoulder Surfing and spyware because face images are shown clearly. The probability of guessing attack is high with few authentication rounds. In addition there are some predictable images users are more inclined to select based on gender, race and complexion.

Similar to PassFaces, Story needs only one round of authentication. In Story password images are a sequence of several unique images that creates a story to enhance memorability. When users authenticate "tell a story" can string password pictures up. The story requires users to remember the order of images. So it is difficult for users who did not take the advice of using a story to guide their image selection to remember the password. Cognitive authentication is designed to resist spyware and shoulder surfing. If a user stands on a picture belonging to the portfolio then he will move right or down until the right or bottom edge of the panel is reached. The label of row or column is recorded and a multi choice question which includes the label for the path's correct point is displayed for each round. The system computes the cumulative probability that the correct answer was not entered by chance after each round. When probability passes a certain threshold authentication is successful. The threshold enables the system to tolerate some user errors. An observer who records any feasible number of successful authentication sessions cannot recover the user's secret by the brute force or the enumeration method.

Convex Hull Click also resists Shoulder Surfing in a public environment where video recording and electronic capture are ineffective in this situation. Hundreds of icons displayed randomly in one panel and users choose and memorize several icons to create a password. Each panel includes at least 3 or more password icons. These 3 or more password icons together form a convex Hull during login. Because users don't click the pass icons directly, it resists shoulder surfing attack. Additionally this scheme enjoys a large password space with the negative consequence of increasing login time significantly. Colorlogin is also designed for protection from Shoulder Surfing attack. When a user clicks on a row containing pass icon it means that he has chosen the correct pass icon. All icons in that row are then replaced with lock icons. A round authentication will not be considered successful unless all pass-icons in one panel are correctly chosen. The background color decreases user's login time. Although the password space is large once the pass icon's color is revealed the password space shrinks sharply.

GPI (Graphical password with icons) / GPIS (Graphical password with icons suggested by the system) is designed aimed at solving the hotspot problem. In GPI users select 6 icons from 150 icons as a password in one panel. With GPIS the system generates a random password and displays it to users. If the user is not satisfied with the password he/she can request the system to generate new password until accepted. The main drawback of GPIS is its unacceptable login time and small size of icons.

*D. Hybrid schemes*

Hybrid schemes are typically the combination of two or more schemes or other authentications. These schemes are used to overcome the limitations of a single scheme such as shoulder surfing, hidden camera, or spyware and so on. Jiminy used image as a cue for helping users choose easy to remember passwords. In this scheme users are provided with templates based on color that contain several holes. The user first selects an image chooses a color template picks a specific location inside the image then clicks on the position to place the template and records the password. During login user must select the right template place it on the correct location on the image then enters the characters visible through the holes from top to bottom. Compared to remembering alphanumeric passwords this scheme only requires users to remember the precise location of template on the image. However experiments show that users have difficulty remembering precise locations and their selections tend to be predictable suggesting doubt about the efficiency of hotspot resistance.

Fig .3 CAPTCHA

Using CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) proposed by Gao retains the advantages of graphical password schemes. In the register phase users select and remember images as their password images (pass-images). To be authenticated, the user needs to distinguish his pass-images as well as complete a test by recognizing and typing the adjunctive string below each pass image.

Zhao and Li proposed a Scalable Shoulder Surfing Resistant Textual Graphical Password Authentication Scheme (S3PAS). This scheme seamlessly integrates both textual and graphical passwords and is resistant to Shoulder Surfing, hidden camera and spyware attacks. During the registration phase users select a string k as the original password. The length of k depends on different environments and different security requirements. In the login phase they find their original password in the login image then click

inside the invisible triangle called “pass-triangles” created by the original password. “Click a secret” proposed by M.Eluard is a combination of Locimetric and Cognometric schemes that allows entering a secret through interaction with an image. Users create a personal image by replacing some particular regions of the original image with an alternate version. The particular region named GECU (Graphical Element Chosen by User) has a specific graphical element present in the original image (e.g. people, animals, vehicles, signs, architectural elements and so on). In registration phase the user clicks on GECU in the original image which is then replaced by an alternate version. When he /she think the current image is suitable the user validates their personal image. This process continuous for several rounds creating the user’s password. In the login stage the user clicks on GECU in the initial image until he/she finds all of his personal images. Although this scheme enhances the interaction with images, its usability is not high due to the limitation of its small theoretical password space.

## IV. VISUAL CRYPTOGRAPHY SCHEME(VCS)

One of the best known techniques to protect data is cryptography. It is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. We can achieve this by one of the following access structure schemes.

The (2, 2) Threshold VCS Scheme: This is a simplest threshold scheme that takes a secret Message and encrypts it in two different shares that reveal the secret image when they are overlaid. In (2, 2) VCS the first 2 represents the minimum number of share images needed to recover a secret image. The second 2 represents the total number of share images produced. The VCS model is dependent on the basis matrix which forms the entire model. In linear algebra basis is a set of linearly independent vectors, can represent every vector in the vector space. The entire model of (2, 2) VCS can be described by tow basis matrices one for a black pixel and one for a white pixel. The basis matrices of (2, 2) VCS are:

B1=10 01 and

B0=01 01

In a basis matrix element 1 means the presence of a black pixel in the share image generated from this matrix and element 0 means the presence of a white pixel. The rows of a basis matrix correspond to the share images and describe how the pixel in secret image is divided in share image. For example consider the pixel to be shared is black pixel, and then the dealer takes the B1 basis matrix and examines the rows. For the share1 image he copies the black pixel as a combination of black pixel and white pixel as in 1st row of B1 matrix. For the share2 image he copies black pixel as a white and black pixel combination as in 2nd row of the B1 matrix. In the same way for the white pixel, share1 image gets the pixel as in 1st row of B0 matrix and share2 image gets the pixel as in 2nd row of B0 matrix. Note that the choice of shares for a white and black pixel is randomly determined (there are two choices available for each pixel). Neither share provides any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices. When the two shares are superimposed the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixel and one white sub pixel as shown in fig 4.

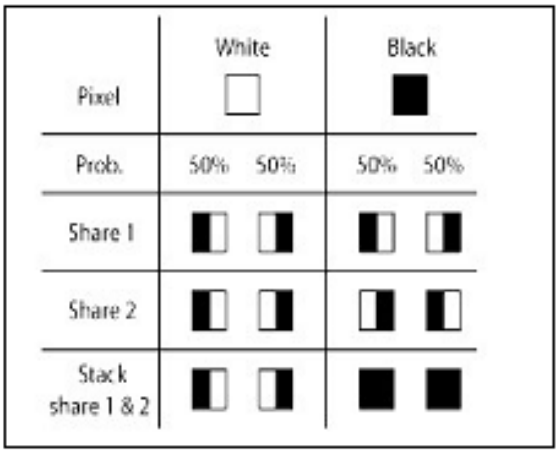


Fig.4. (2, 2) visual cryptography scheme.

## V. DESIGN PROCESS

There are 2 phases in this project

- Registration phase
- Login phase

### *A. Registration phase*

In the registration phase, user is presented with some images. User should select any one of the images. A key is generated from the image and it is split into 2 shares, Share1 and Share 2. These shares are encrypted to provide confidentiality. Then share 1 is send to user via email and share 2 is kept with the server.

The process of registration is shown in the activity diagram below in fig. 5.

### *B. Login phase*

In the login phase, user browses his/her share and from this and with share from server captcha image is generated. Then user gets logged in.

The process of login is shown in the activity diagram below in fig. 6.

## VI. RESULTS

The shares generated are combination of black & white pixels whose stacking results in original image which is also a black & white image. In the registration phase the most important part is the creation of shares from the image captcha where one share is kept with the user and other share can be kept with the server. For login, the user needs to enter a valid mail id in the given field. Then he has to browse his share and process. At the server side the user's share is combined with the share in the server and an image captcha is

generated. The user has to enter the text from the image captcha in the required field in order to login into the website.

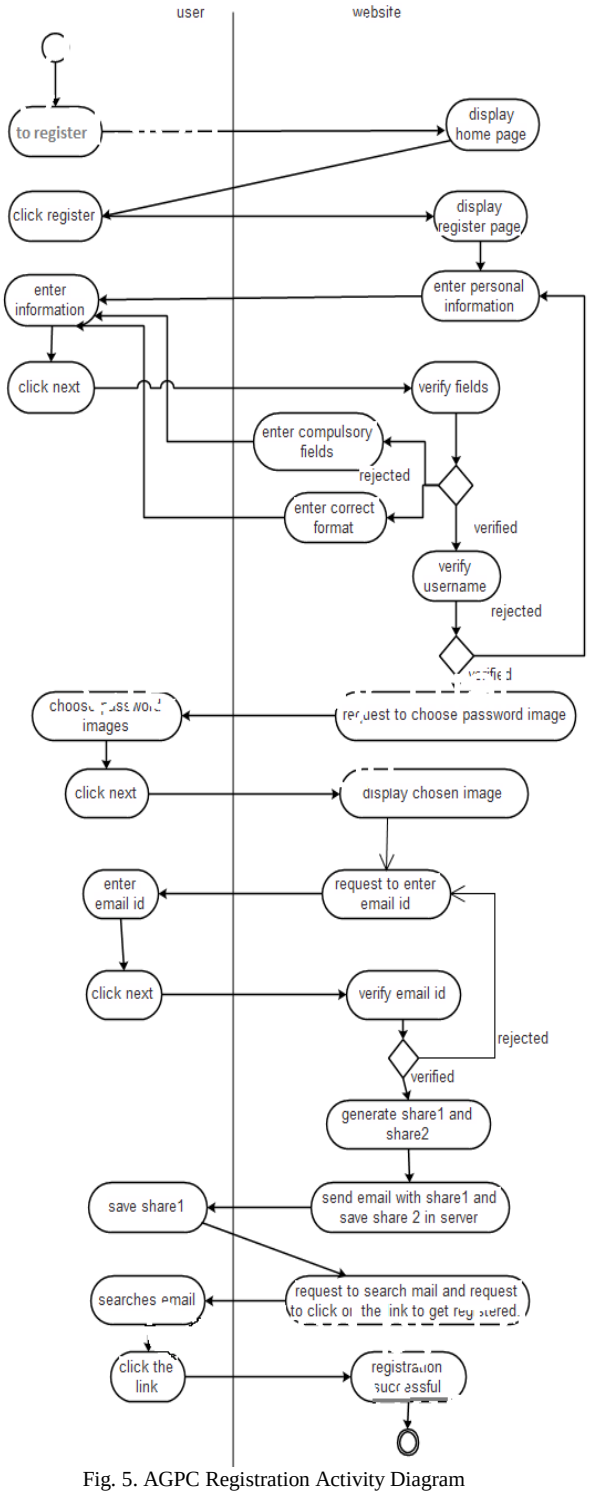


Fig. 5. AGPC Registration Activity Diagram

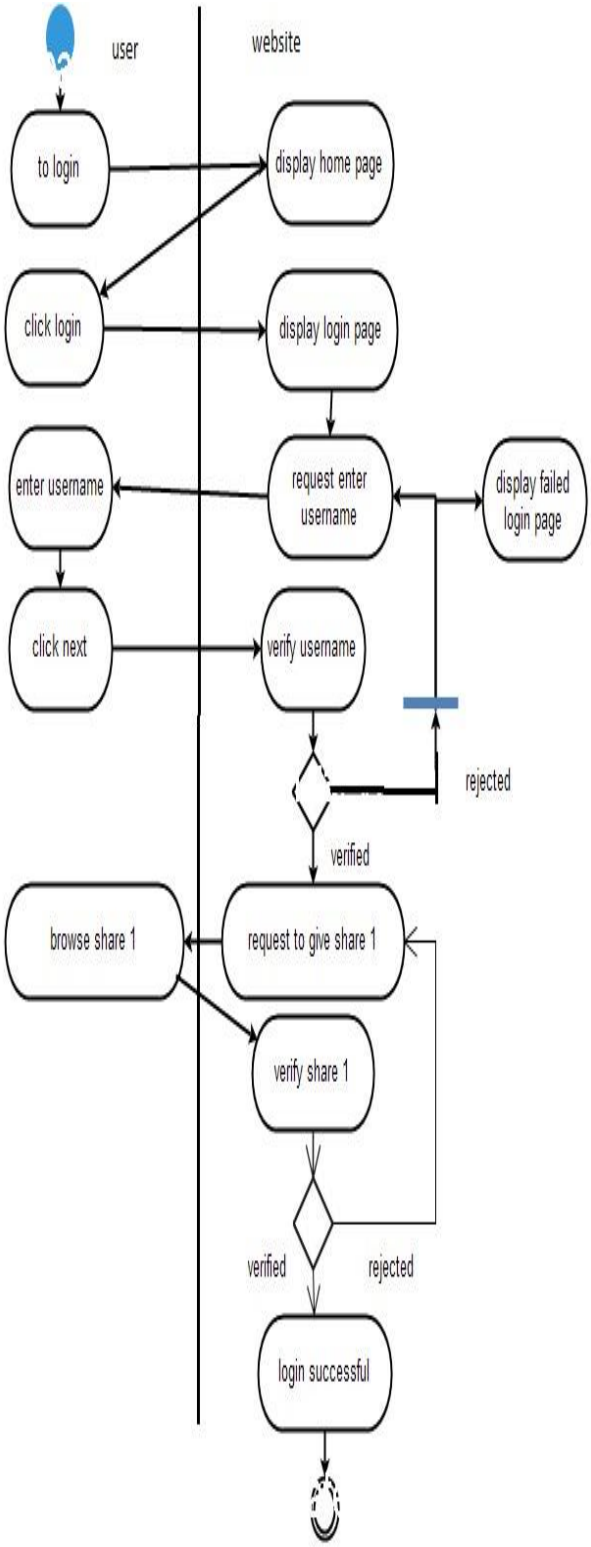


Fig. 6. AGPC Login Activity Diagram

## VII. ACKNOWLEDGMENT

Immeasurable appreciation and deepest gratitude for the help and support to all the people who in one way or the other have contributed in making this work possible. The authors are grateful to all friends and classmates who provided their valuable suggestions and support. The authors like to express their gratitude to their beloved parents for the love, support and encouragement.

## VIII. CONCLUSION

Using graphical password based on image Captcha technique, no machine based user can crack the password or other confidential information of the users. It also prevents intruder's attacks on the user's account. It is useful to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping markets etc.

## IX. REFERENCES

[1] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, "Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems" ,IEEE transactions on information forensics and security ,vol.9,no. 6,june 2014.

[2] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Computer. Surveys*, vol. 44,no. 4, 2012.

[3] M. Alsaleh, M. Mannan, and P. C. van Oorschot, "Revisiting defenses against large-scale online password guessing attacks," *IEEE Trans. Dependable Secure Computer.*, vol. 9, no. 1, pp. 128–141, Jan./Feb. 2012.

[4] D. Weinshall, "Cognitive authentication schemes safe against spyware," in *Proc. IEEE Symp. Security Privacy*, May 2006, pp. 300–306.

[5] G. Mori and J. Malik, "Recognizing objects in adversarial clutter," in *Proc. IEEE Computer. Society Conf. Computer. Vis. Pattern Recognition.*, Jun. 2003, pp. 134–141.

[6] G. Moy, N. Jones, C. Harkless, and R. Potter, "Distortion estimation techniques in solving visual CAPTCHAs," in *Proc. IEEE Computer. Soc. Conf. Computer. Vis. Pattern Recognition.*, Jul. 2004, pp. 23–28.

[7] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, "Against spyware using CAPTCHA in graphical password scheme," in *Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl.*, Jun. 2010, pp. 1–9.

[8] J. Bonneau, "The science of guessing: Analyzing an anonymized corpus of 70 million passwords," in *Proc. IEEE Symp. Security Privacy*, Jun. 2012, pp. 20–25.

[9] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The designnand analysis of graphical passwords," in *Proc. 8th USENIX Security Symp.*, 1999, pp. 1–15.

[10] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," *Int. J. Netw. Security*, vol. 7, no. 2, pp. 273–292, 2008