International Journal of Advancement in Electronics and Computer Engineering (IJAECE)
Volume 11, Issue6, June. 2022, pp.101-105, ISSN 2278 -1412

Review Analysis on Versatile CAPTCHA Generation Using Machine Learning and Image Processing

Aman Deep Chanpuriya[1], Ankur Taneja[2]
[1]Mtech Scholar, amandeepchanpuriya267@gmail.com,SAMCET(RGPV) Bhopal, India
[2]Assistant Prof., SAMCET(RGPV) Bhopal, India

Abstract *– CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) is a method for determining whether or not a user is human or a robot. Generally, CAPTCHA is used to prevent robots from entering databases using distorted alphanumeric characters. However, CAPTCHA will now be utilised as input credentials, such as login and password, to protect authentication systems from various types of assaults in the proposed work. It will be difficult to hack any account if a robot is unable to enter the username and password. One of the most crucial steps in gaining secure access to any programme is to utilise secure credentials such as login and password for authentication. There are currently a plethora of approaches for securing an authentication system. However, these solutions have failed to protect the login and password from hackers or to determine whether the attempt is made by a human or a robot. However, in the proposed system, the Gaming CAPTCHA method is used, in which different letters, both alphabetic and numeric, are in the form of different orientations, with each character having their own colour that must be recognised and hit with the same colour ball that is kept in the lower section of the dialogue box according to the desired letter to choose. As a result, all inputs will have been generated by the game rather than by input devices.*

Keywords*:* **CAPTCHA, Authentication, Graphical Password, Image processing, Game, Robot**

I. Introduction

Authentication is required and is a vital step in gaining access to any system. We commonly use text passwords as a security measure, however these are vulnerable to attacks and are insecure. These can be hacked and are vulnerable to phishing, brute force attacks, dictionary attacks, and other forms of cyber-attack. There is a severe hazard to text-based passwords among this phishing.

By using a masquerading assault, one can obtain information such as user details such as login, password, and contact information, as well as other details.

There are many problems in User authentication. And for authentication purpose computer security depends on password. Password has some important characteristics which are as follows:

1. It should be changeable.
2. It should be quickly and easily executable.
3. It should be easy to remember.

The challenge with text password method is difficulty in remembering them. To solve the problems with old username and password authentication system, an alternative authentication scheme such as Graphical password is a solution. Humans are more likely to recall pictures and line drawing object or real objects than texts so we can set graphical password as the password scheme. So this will remove the big challenges.

In Graphical password images can be set as password thus resulting in easy recalling of password and this scheme of password implementation is more user friendly then conventional password scheme to text password.

In addition to web login application and work-stations, graphical passwords have also been used to ATM machines and mobile devices so this password scheme can be implemented to all these places.

The biggest problem with old password scheme was that computer programs were generated to crack the password and password was breakable through many computer attacks. CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) is programs that generate tests that are human solvable, which can't be guessed through current computer programs. Hence in solving captcha human involvement is must. Defending the sites against various attacks such as bots, resisting automatic adversarial attacks is possible through the program of implementing Captcha.

Captcha also prevents system from dictionary attacks, spam and worms. CaRP is Captcha as a graphical password, which is a combination of both captcha and graphical password as a single entity for authentication. IN CaRP click-based graphical password strategy is implied. It differs from other password scheme as in graphical password scheme only one image is used and user has to click on that image for authentication but in CaRP images used are Captcha challenge for the user, and for every login attempt a new CaRP image is

generated. CaRP solves a number of security problem altogether that are online guessing attacks, relay attacks etc. and, if combination with dual-view technologies like graphical password or text password it can minimize shoulder-surfing attacks. In this review a difference has been studied between existing password scheme and CaRP technology.

II. LITERATURE SURVEY

2.1 Review on existing systems:

Vaibhavi Deshmukh et. al.[1] Due to the significant increase in the size of the internet and the number of users on this platform there has been a tremendous increase in load on various websites and web-based applications. This load is from the user end which causes unforeseen conditions which leads to unacceptable consequences such as crash or a data loss scenario at the webserver end.

Therefore, there is a need to reduce the load on the server as well as the chances of network attacks that increase with the increased user base. The undue consequences such as data loss and server crash are caused due to two main reasons: the first one being an overload of users and the second due to an increased number of automatic programs or robots. A technique can be utilized to overcome this scenario by introducing a delay in the operation speed on the user end through the use of a CAPTCHA mechanism. Most of the classical approaches use a single method for the generation of the CAPTCHA, to overcome this proposed model uses the versatile image CAPTCHA generation mechanism. We have introduced a system that utilizes manualbased, face detection-based, colour based and random object insertion technique to generate 4 different random types of CAPTCHA. The proposed methodology implements a region of interest and convolutional neural networks to achieve the generation of the CAPTCHA effectively.

Bin B. Zhu et al.[2] proposed a system that prevents users from brute force attack by providing CAPTCHA as graphical password. In this paper, an image representssome alphanumeric letters in distorted form where user will have to identify it correctly and clickto enter desired password. Each letter has its own representation which has been assigned by coordinate values.Coordinate values can easily identified by image processing and attack can be applied on the basis of these coordinate value. So, the security has been broken if any of the letters is identified by their coordinates.

Fig. 2.1.1Coordinate Based Graphical Password [2]

Vikas K. Kolekaret al [3]proposed a system that is based on graphical CAPTCHA for login authentication. The system which has been proposed in this paper is also based on distorted letters as graphical password along with animal sequence password.It means that user will have to select the sequences of animals for creating graphical password which is based on sequence of clicks made by users. It is often easier to identify the positions of animals by Soley edge detection method and a sequence does not possess secured password. There are x and y coordinates for each letter which represent a letter or a area of that particular symbol which it covers. By clicking there letters, they return its coordinate values in the back end of the system.

Fig. 2.1.2Graphical CAPTCHA based on characters [3]

Fig. 2.1.3Graphical CAPTCHA based on animal sequences [3]

Anjitha Ket al [4]proposed a system which is also based on click based graphical CAPTCHA where user will have to select password by clicking on it and weakness is described earlier in the previous section of the review.

Pooja Jaiprakash Kulkarniet al [5]proposed a system which is also based on previously described techniques. As shown in the figure 2.1.4, some letters are distorted and some are in the standard form. Each letter has covered a region and active region relies from some coordinate values. All these values stored in the database and a dataset of values is being stored in the form of coordinate values which represent a password.

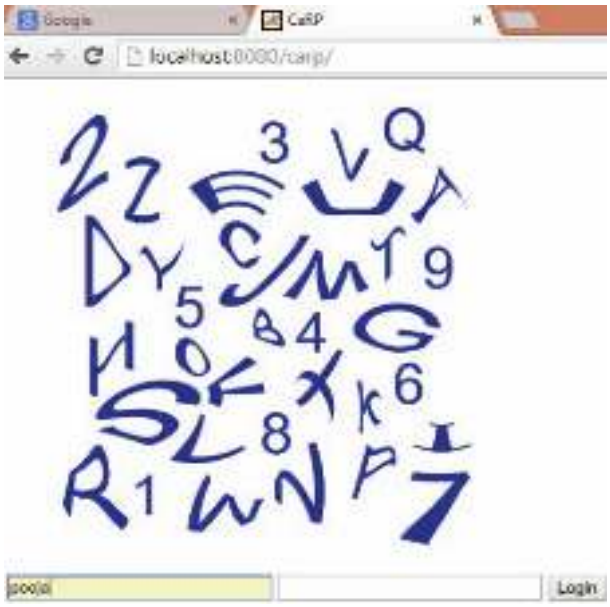

Fig. 2.1.4Click Text based CAPTCHA[5]

Devina Vinod et al [6]proposed a system which is differ from entire click text based CAPTCHAs. It is based on hard AI problems that cannot be easily solved. In this system user require to identify the similar faces and click on them to pass. This kind of CAPTCHA requires severe observation to recognize the similar faces.

Fig. 2.1.5 Similar Faces Based CAPTCHA [6]

Priyanka J. Chardeet al [7]reviewed some CaRP based CAPTCHAs and also proposed a system in which user has to select one image from set of various images of famous places, person or companies and identify it during login time. This kind of CAPTCHA is differing from click based CAPTCHA because there is not a particular click point on the image instead of that whole image are clickable and return results. Authentication is based on selection of image during registration time.

Fig. 2.1.6Image Selection based

CAPTCHA
[7]

Priyanka Pipersaniya et al [8] proposed a system neither based on coordinates nor sequences of faces or animals, instead of that it is based on moving alphabets which do not possess a static position. Background reflects replica of letters which may confuses the robot to recognize the correct one, but still a dark one represent the correct alphabet.

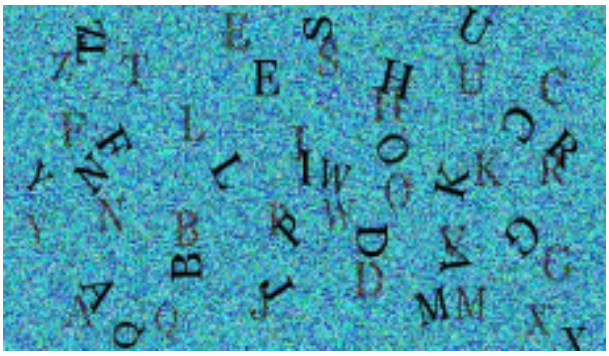

Fig. 2.1.7Dynamic Position based

CAPTCHA
[8]

III. METHOD

Graphical Passwords

There are several graphical password methods. Recognition, recall and cued recall these are the three methods
of graphical password system and these ivolve the of memorizing and recognizing the password involved. In recent review more methods can be found. A recognition based technique requires identifying the objects from a set of given objects that belongs to the password which had been already defined by the user. The scheme is Pass faces in which a user creates password by choosing a set of faces from a Database. In authentication, user selects a face belonging to her portfolio from a panel of faces represented to her. This method is repeated many times, each time containing a different set of faces.
In each round the image set remains the same but the images are permuted randomly. Correct Selection in each round leads to successful login. An extra hint is provided to user in cued-recall technique, so that user can easily memorize and enter the password. In this scheme users are required to memorize the specific points present in image. PassPoints is click-based cued-recall scheme in which a user picks particular points at anyplace on an image by clicking on them thus creating a password and user must click on those points while authenticating. Deterministic function to select next images and one click per images as in Pass Point are used by Cued Click Points (CCP). Among the three types recall is the hardest for users (human) memory while recognition is easiest to remember. Recognition is also the weakest in resisting guessing attacks.

Captch

Captcha are the challenges that can be solved by humans only as captcha asks general question or give problems which are very easy for humans to answer but almost impossible for computers to solve as they need to identify the objects and then apply algorithm, but each time a new random captcha gets generated resulting in failure of predefined program to solve captcah.
Captcha are of two types: Text Captcha and Image-Recognition Captcha.
The Image Recognition Captcha is based on recognition of non-character objects and text Captcha depends on character recognition. The characters in text captcha are generated randomly and are human readable but difficult for computer to answer as these are represented in different fashion than usual.Non-character object recognition by machine is more difficult and complicated as compared to character recognition thus making IRCs more secure than text Captcha. In Asirra the binary object classification is done in which user is presented with a set of images with some images possessing some similarities and user is asked to click all the images having some common property. Thus this kind of challenges can be solved by humans only because of the fact that computers are not capable of finding similar objects because each time a different set is introduced as a challenge.

IV. Conclusion

As a result, the survey of the systems that concludes at a point in that system is either based on coordinate values or discovering similar faces that may contain the location based on coordinates stored in the database. The base system proposed a CAPTCHA that gives dynamically positioned CATPCHA, in which the user must click on moving characters that have no fixed places. However, the system falls short when it comes to AI challenges that involve simple logic.

REFERENCES

[1] Versatile CAPTCHA Generation Using Machine Learning and Image Processing by Vaibhavi Deshmukh, Swarnima Deshmukh, Shivani Deosatwar and Reva Sarda IEEE 5th International Conference on Computing ommunication and Automation (ICCCA)
Galgotias University, Greater Noida, UP, India. Oct 30-31, 2020.

[2] Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems proposed by Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu in IEEE 2014.

[3] Click and Session Based—Captcha as Graphical Password Authentication Schemes for Smart Phone and Web proposed by Vikas K. Kolekar and Milindkumar B. Vaidya in 2015 on IEEE.

[4] Captcha As Graphical Passwords-Enhanced With Video-Based Captcha For Secure Services proposed by Anjitha K and Rijin I K in 2015 on IEEE.

[5] The Graphical Security System by using CaRP proposed by Pooja Jaiprakash Kulkarni and Dr. G. M. Malwatkar in 2015 IEEE.

[6] Captcha As Graphical Password For High Security proposed by Devina Vinod1, Anjana S.2 in 2015 of Global Journal of Advanced Engineering Technologies.

[7] Review Paper on Improved Security Using Captcha as Graphical Password proposed by Priyanka J. Charde, Prof. M. S. Khandare in 2016 IJSRSET.

[8] Advanced CAPTCHA as a graphical password for better secure authentication, proposed by Priyanka Pipersaniya and Jijo S.Nair, in 2017 of International Journal of Innovations in Engineering and Technology (IJIET).