A Review on CAPTCHA as a Graphical Password to Secure Input Credentials

Sandeep Piplotia[1], Bhavana Gupta[2]

[1]*Associate Research Fellow,* [2]*Associate Professor*

Oriental College of Technology, Bhopal

Abstract - CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a technique to identify whether user is a human or a robot. Generally CAPTCHA is used for denying robot entries in database in the form of distorted alphanumeric characters. But now in the proposed work, CAPTCHA is going to be used as input credentials such as username and password to secure the authentication systems from different kind of attacks. If a robot is not able to input username and password then it will be impossible to hack any account. The use of secure credentials like username and password for authenticating any specific application is one of the most important steps to access it securely. There are so many different techniques are already exists to secure an authentication system. But somewhere somehow these systems got failed in securing the username and password from the hackers or not able to identify whether the attempt is made by human or robot. But in proposed system, the method of Gaming CAPTCHA is being used in which different letters including alphabetic and numeric are in the form of different orientations where every character have their own color which need to be recognized and hit with the same color ball which is kept in the lower section of the dialogue box as per the desired letter to choose. So, all inputs will have been made by a game not by input devices. Text fields will be totally disabled that can only be accessed by gaming CAPTCHA. The motive of this paper is to review previous system and its techniques where they are lacking.

Keywords - CAPTCHA, Authentication, Graphical Password, Image processing, Game, Robot.

1. INTRODUCTION

Fig. 1.1CAPTCHA as a Graphical Password

CAPTCHA is a way to identify whether the user is bots or human. The techniques of securing input credentials are already been discovered where user will have to enter password just by clicking distorted letters which belong to coordinates values. Each coordinate represents a letter and return it for user corroboration.

2. LITERATURE SURVEY

2.1 Review on existing systems:

Bin B. Zhu et al.[1]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 [1]

Vikas K. Kolekaret al [2]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.
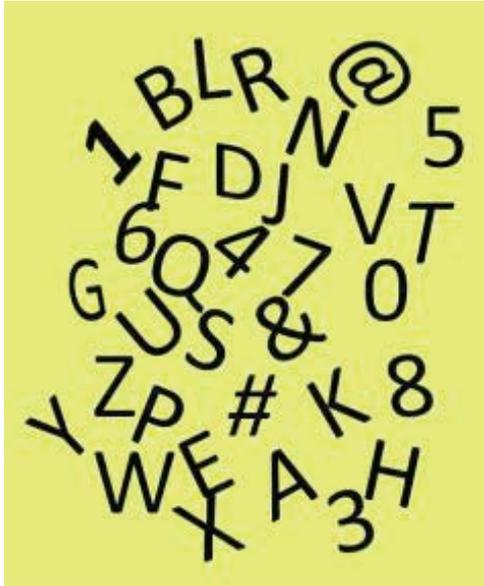
Fig. 2.1.2Graphical CAPTCHA based on characters [2]

Fig. 2.1.3Graphical CAPTCHA based on animal sequences [2]

Anjitha Ket al [3]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 [4]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 data

set of values is being stored in the form of coordinate values which represent a password.
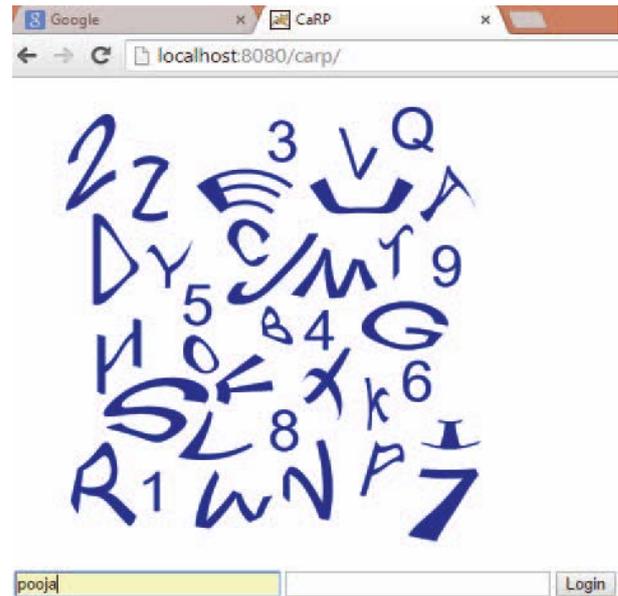

Fig. 2.1.4Click Text based CAPTCHA[4]

Devina Vinod et al [5]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.
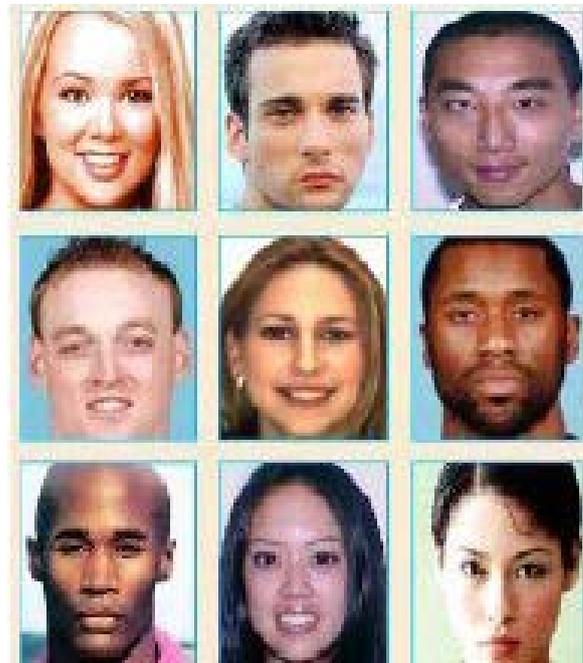
Fig. 2.1.5 Similar Faces Based CAPTCHA [5]

Priyanka J. Chardeet al [6]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.
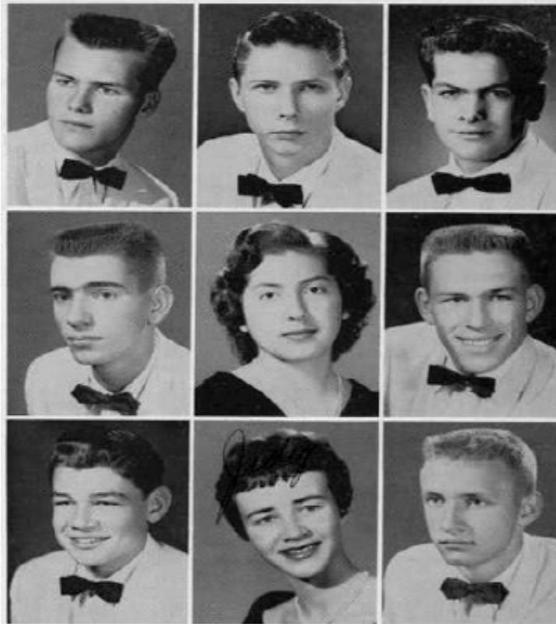

Fig. 2.1.6Image Selection based

CAPTCHA [6]

Priyanka Pipersaniya et al [7] 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.
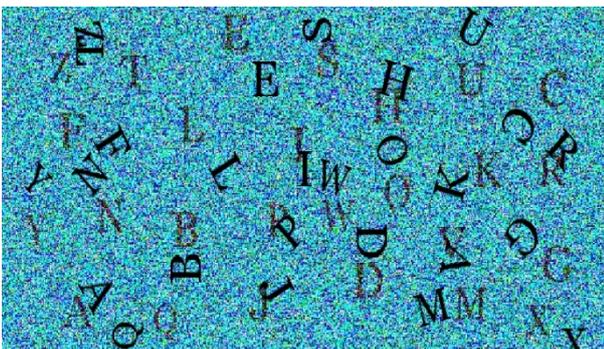

Fig. 2.1.7Dynamic Position based

CAPTCHA [7]

3. PROBLEM STATEMENTS

Existing systems arebased on clicks over distorted letters which only can be recognized by human. But brute force attack can affect the system by recognizing its representation of letters on behalf of coordinate values. Some hard AI problems confuse users to recognize similar faces and sequence of faces and hard to remember at the time of login. A sequence of animal is often hard to remember for login authentication. We require a system

which can secure the input credentials and password should be on user's choice. This credential should be secured while registering it or authenticating [it] at all.
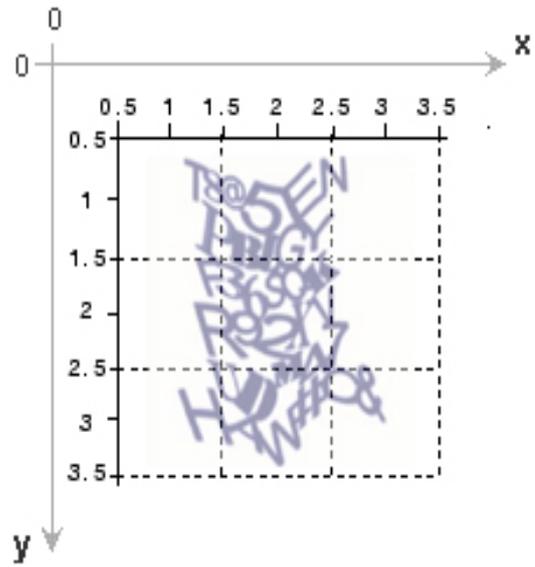

Fig. 3.1Coordinates based CAPTCHA

Fig. 3.2 Replica Alphabets [7]

Fig. 3.3Soley Edge Detection [7]

4. CONCLUSION

Thus the survey of the systems concluded at a point of that system is either based on coordinate's values or finding similar faces which may comprises the location on the basis of coordinates stored in the database. The base system proposed a CAPTCHA which offers dynamically located CATPCHA where user will have to click on moving letters which do not possess any static positions. But system is lacking for AI problems which represent simple logics.

5. FUTURE SCOPE

The present systems get enhanced in future by turning it in hard AI problems which can only solved by human. A hard logic is required to secure the input credentials instead of moving it. The proposed system can fulfill the drawback of present systems.

REFERENCES

[1] 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.

[2] 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.

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

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

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

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

[7] 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).