REVIEW PAPER ON DEEP LEARNING TECHNIQUES FOR SECURING WEB SERVICES BY USING TEXT,IMAGE & PATTERN BASED CAPTCHAS

SHUBHANGI SUDAM GIRI[1], ASST. PROF. V. S. KARWANDE[2]

ME Student, CSE Dept. Everest Educational Society's Group of Institutions, Aurangabad, Maharashtra

Asst.Prof. CSE Dept. Everest Educational Society's Group of Institutions, Aurangabad, Maharashtra

Abstract- Recent research on recommendation has shifted from explicit ratings to implicit feedback, such as A CAPTCHA is a program or CAPTCHA stands for Completely Automated Public Turing Test To Tell Computers and Humans Apart, Created by Carnegie Mellon University .There are different type of CAPTCHA .User type the letters of a distorted image in Mostly useful CAPTCHA, somewhere sum of sequence of letters or letters digits which looks on the screen. The reason is that the test is delivered by a computer, in difference to the streamer Turing test that is handled by a person ,a CAPTCHA is occasionally express as a set aside Turing test. Today most of the websites utilize captcha generated towards secure their site from scrappers, online polls, dictionary attacks and search engine bots, for enhanced pledge usability and security both are to be egalitarianism. Here the text CAPTCHA is scrutinized in minuscule and the need for image CAPTCHA is put abroad .Increase characteristic of the image CAPTCHA are integrated and a new CAPTHA with enhanced capability is advanced. We Use Deep Learning Technique for securing Web Services by Using Text, Image & Pattern Based Captcha.

Keywords: Completely Automated Public Turing Test To Tell Computers and Humans Apart (CAPTHA), Optical Character Recognition (OCR), Global Unique Identifier (GUID), State Information Database (SID).

I INTRODUCTION

In recent years, the focus of recommender system research has shifted from explicit feedback problems such as Captcha prediction to implicit feedback problems. In Carnegie Mellon University by a group of researchers found CAPTCHA in 2000.For prevent exploitation of the website security against spammers, scrappers, online and dictionary attack CAPTHA installation is required. First introduced CAPTCHA was Text based, it Re-Captcha with recollection of letters and words in English. These were explosion with help of OCR system, for increasing its complexity to protect against attack via utilizing fonts, adding noise and having overlapping letters. Text type CAPTCHA fragmented by using letter bifurcation and character conceding .Usability and security is the goal of CAPTHA 3D present a plan of action depends on numbers of factors like rotation, overlapping, obstacle, noise, background color, scaling, font, special character, background texture. The investigation of 3D type of CAPTCHA conveys that it is secure as it provides resistance to preprocessing, OCR pixel count and dictionary attack [1].

This paper alleviate the shortcomings of survive perspective and proposes a new CAPTCHA It is easy to solve for human because CAPTCHA is simple test but it's hard for computer machine. Commercial websites like web-based email providers, Ticket Master, Go Daddy, and Face book used this for preserve their expedient from attacks initiated by insignificant scripts. [2]. By using a CAPTCHA thousands of accounts, posting hundreds of comments in weblogs are signing up so security mechanism is very important for prevent them. The most common system programs include:

- In online polls thousands of votes as masquerading humans for voting system.

- For sign up for a lot of email accounts with free email service providers in Email account registration system.

- Email Spam system which conventionally sends thousand spam message Search engine system, which conventionally register web pages to raise their rankings in a search engine.[4]

A CAPTCHA test is made up of two easy parts:

- A randomly given rise to sequence of letters or numbers that look as a prevent image, and a text box.

- To pass the test and demonstrate your human identity, simply type the characters you see in the image into the text box. [5]

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), this is a type of security

measure known as provocation-reaction substantiate. This helps preserve you from mailshot and password decryption by asking you to absolute an easy test that demonstrate you are human and not a computer System trying to break into a Password preserved account.

II LITERATURE SURVEY

2.1. M. Tariq Banday, N. A. Shah, "A Study of CAPTCHAs for Securing Web Services", IJSDIA International Journal of Secure Digital Information Age, Vol. 1. No. 2, December 2009.

In this paper, explain various aspects of CAPTCHA methods that include its types, generation methods, robustness against attacks and various usability aspects. It presents relative merits and demerits of text and image based CAPTCHA methods. Atomizing various Web activities by replacing human to human interactions on the Internet has been made indispensable due to its enormous growth. However, bots also known as Web-bots which have a malicious intent and pretending to be humans pose a severe threat to various services on the Internet that implicitly assume a human interaction. Accordingly, Web service providers before allowing access to such services use various Human Interaction Proof's (HIPs) to authenticate that the user is a human and not a bot. Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) is a class of HIPs tests and are based on Artificial Intelligence. These tests are easier for humans to qualify and tough for bots to simulate. Several Web services use CAPTCHAs as a defensive mechanism against automated Web-bots[1].

2.2 Narges Roshanbin,James Miller, "A Survey And Analysis Of Current Captcha Approaches", Journal of Web Engineering, Vol. 12, No.1&2 ,2013.

In this paper, propose a Computer programs are misusing Internet services designed for humans. A CAPTCHA, Completely Automated Public Turing test to tell Computers and Humans Apart, is a standard security mechanism to defend against such attacks. Two fundamental issues with CAPTCHAs are usability and robustness. It is important for a CAPTCHA to be both legible for humans and strong against malicious computer programs. Recently, computer vision and pattern recognition algorithms have broken many well-known CAPTCHAs. Lack of security and usability in CAPTCHAs designed to protect popular websites such as Gmail and Yahoo mail, with almost 500 million users in July 2011, would cause huge problems. Therefore, security researchers have become motivated to discover techniques to improve CAPTCHAs. Exploiting the gap in the recognition abilities between humans and computers is a key point to design a

CAPTCHA that is hard-to-break for machines but easy-to-solve for humans [2].

2.3. S. Mankhair, A. Raut, M. Mohimkar, K. Sukal, A. Khedekar, "Secured CAPTCHA Password Verification Using Visual Cryptography", International Journal of Engineering Science and Computing, May 2016.

In this paper,work on With the advent of internet, various online attacks has been increased and among them the most popular attack is phishing. Phishing is an attempt by an individual or a group to get personal confidential information such as passwords, credit card information from unsuspecting victims for identity theft, financial gain and other fraudulent activities. We are using visual cryptography algorithm for separating privileges. The use of visual cryptography is explored to preserve the privacy of an image CAPTCHA by decomposing the original image CAPTCHA into two shares (known as sheets) that are stored in separate database servers (one with user and one with server such that the original image CAPTCHA can be revealed only when both are simultaneously available; the individual sheet images do not reveal the identity of the original image CAPTCHA. Once the original image CAPTCHA is revealed to the user it can be used as the password [3].

2.4. P. J. Charde, M. S. Khandare, "Review Paper on Improved Security Using Captcha as Graphical Password", IJSRSET, 2016.

In this Paper, focused on many security primitives are based on hard mathematical problems. Using hard AI problems for security is emerging as an exciting new paradigm, but has been underexplored. In this paper, we present a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme. CaRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. Notably, a CaRP password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set. CaRP also offers a novel approach to address the well-known image hotspot problem in popular graphical password systems, such as Pass Points, that often leads to weak password choices. CaRP is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security [4].

2.5. A. Sinha, Dr. S. Tarar, "Review Paper on Different CAPTCHA Techniques", International Journal of Computer

Science And Technology, March 2016.

In this paper, Discuss about CAPTCHA is a program or a system that protects against automated scripts (or bots). It generates tests that humans can pass but computer programs cannot. CAPTCHA systems are widely used nowadays for protecting and providing security to internet based services for humans from abuse by bots. Different types of CAPTCHA technologies are discussed in this paper and a detailed analysis on their reliability is performed. Subsequently,a new CAPTCHA technique is proposed which is based on facial expression detection[5].

2.6. M. Tang , H. Gao , Yang Zhang , Yi Liu ,Ping Zhang ,Ping Wang, "Research on Deep Learning Techniques in Breaking Text-Based Captchas and Designing Image-Based Captcha", IEEE Transactions on Information Forensics and Security ,Volume: 13 , Issue: 10 , Oct. 2018.

In this paper, Discuss about The ability of hackers to infiltrate computer systems using computer attack programs and bots led to the development of Captchas or Completely Automated Public Turing Tests to Tell Computers and Humans Apart. The text Captcha is the most popular Captcha scheme given its ease of construction and user friendliness. However, the next generation of hackers and programmers has decreased the expected security of these mechanisms, leaving websites open to attack. Text Captchas are still widely used, because it is believed that the attack speeds are slow, typically two to five seconds per image, and this is not seen as a critical threat. In this paper, we introduce a simple, generic, and fast attack on text Captchas that effectively challenges that supposition. With deep learning techniques, our attack demonstrates a high success rate in breaking the Roman-character-based text Captchas deployed by the top 50 most popular international websites and three Chinese Captchas that use a larger character set. These targeted schemes cover almost all existing resistance mechanisms, demonstrating that our attack techniques are also applicable to other existing Captchas. Does this work then spell the beginning of the end for text-based Captcha? We believe so. A novel image-based Captcha named Style Area Captcha (SACaptcha) is proposed in this paper, which is based on semantic information understanding, pixel-level segmentation, and deep learning techniques. Having demonstrated that text Captchas are no longer secure, we hope that our proposal shows promise in the development of image-based Captchas using deep learning techniques[6].

III PROPOSED METHOD

The most common system programs include: In online polls thousands of votes as masquerading humans for voting system .For sign up for a lot of email accounts with free email service providers in Email account registration system. Email Spam system which conventionally sends thousand spam messages Search engine system, which conventionally register web pages to raise their rankings in a search engine. [3]

Interaction from a person in order to be granted as a person or a member of a group have been able to successfully avert malicious programs from getting approach to Web services that is called Human Interaction Proof (HIP).CAPTCHA is a class of HIP tests and are peaceful for attacker to trained and tough for system to replicate.

When good CAPTCHA is generated following characteristics must be satisfied:

1. Teat must be given rise to fundamentally

2. Test result must be easy and quick

3. It must hold out against attacks although the algorithm is known.

In the form of web pages, data stored in a database or files or some other service intended to be used by human users on the client which is Public and protected resources hold by web server. Following are types of CAPTCHAs:

1 Text CAPTCHAs:

Text CAPTCHA is easy to implement. The simplest yet novel approach is to present the user with some questions which only a human user can solve.

Examples of such questions are:

1. What is nine minus two?

2. What is the fourth letter in COLLEGE?

3. If tomorrow will a Sunday, what was yesterday?

This type of question is very easy for person to solve, but it is difficult for a computer system. User request solicitation for deep pockets is sending by the client system to the server, which is appreciated to it if the deep pockets are not saved. To generate a CAPTCHA image server uses some CAPTCHA image generation algorithm. For image generation which may employ use of images stored in an image database use different algorithms for different CAPTCHA techniques.
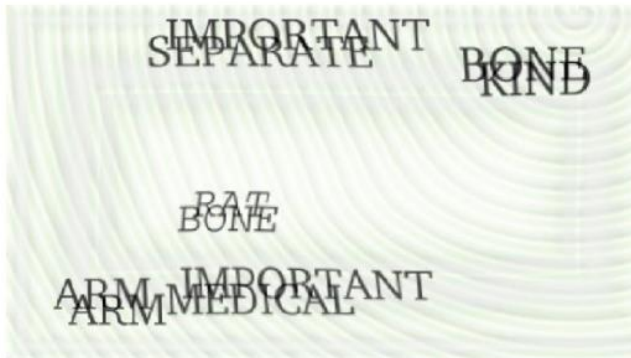
1.1. Gimpy:

In Gimpy distorted text and the inability of computer programs to do the same, it is based on human ability. From a dictionary Gimpy works choosing ten words randomly, and displaying it in a distorted and overlapped type.

To enter a subset of the words in the image Gimpy then asks the users. A computer program cannot capable of identifying the words correctly. The human user is capable of identifying the words correctly

Gimpy is a very dependable text CAPTCHA fabricate by CMU in participation with Yahoo for its Messenger

service. Gimpy is depended on the human potential to read extraordinarily warped text and the incapacity of computer programs to do the same. Gimpy works by collecting some words randomly from a dictionary, and exhibiting them in a deformed and overrun manner. Gimpy then demand to the users for enter a portion of the words in the image. The human user is proficient of recognizing the words precisely, where as a computer program cannot.


Figure 1: Gimpy CAPTCHAs.

2 Image CAPTCHAs:

To generate a CAPTCHA image server uses some CAPTCHA image generation algorithm. Different algorithms uses for image generation for Different CAPTCHA techniques which may exploit use of images recorded in an image database. Global Unique Identifier (GUID) of the client along with state information also at the server CAPTCHA solution is stored in the State Information Database (SID).Make sure that only client that received CAPTCHA can produce a well-grounded result by using GUID of the client. Alternatively of keeping the CAPTCHA result and other state statistics on server in SID, it be may kept in hemp or cipher form in a cookie on the client.

A web page accommodating the created CAPTCHA image, the cookie is attached to the client who contributes it in a web browser to the user. A user responds to CAPTCHA test and the result is passed by the client to the server. The server checks the legitimacy of CAPTCHA result by distinguished between the stored GUID and the GUID of the client sending the result.

The result on condition that the client is next differentiates with the result stored in SID and cookie and appropriately either access is permit or repudiated. In case approach is repudiates, a message is attached to the client and the process starts over again. A CAPTCHA execution may provisional block access for a client if it continually fails to respond to a number of CAPTCHAtests.
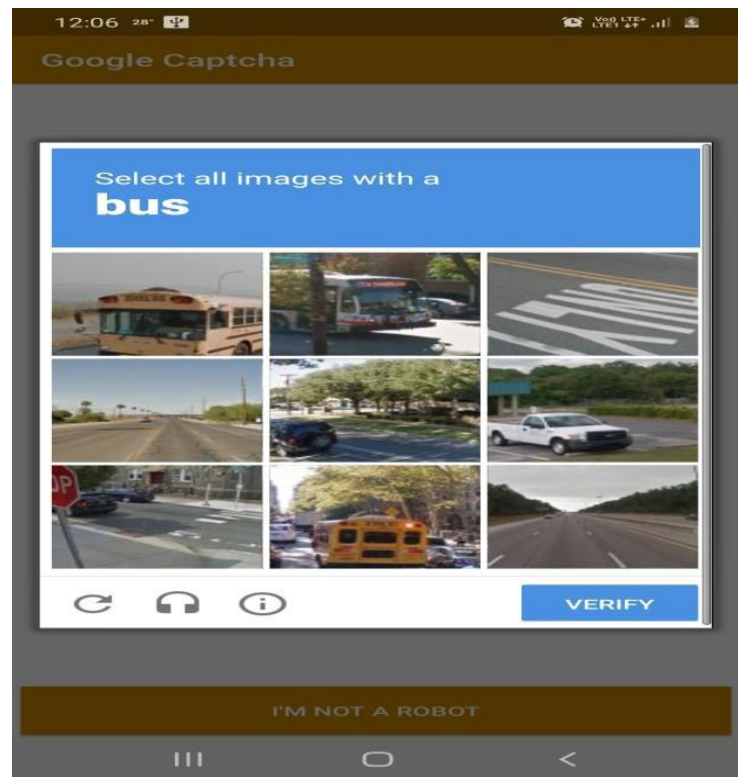
Figure 2: Verification Image with selecting bus as object.

### 2.1 Security of popular image CAPTCHA:

To break a variety of real-world CAPTCHA schemes contrivance three simple yet powerful generic attack frameworks that can be used to break a variety of real-world CAPTCHA schemes. This is powerful because they

- Manage an extensive offline investigation for each CAPTCHA scheme,

- Accumulate plenty data based on this offline investigation, and

- Instruct precise and specific image conceding and discernment mock-ups.[4]

2.2 CAPTCHA Image Generation Process:

It is not possible to generalize the algorithm for generation of CAPTCHA image; however, the steps listed below provide a guideline for creation of a basic text-based CAPTCHA image:

1. Create a CAPTCHA of desired dimension sufficient to hold the different images.

2. 2. Set the background color for empty space in every image. Some CAPTCHA uses a simple white background.
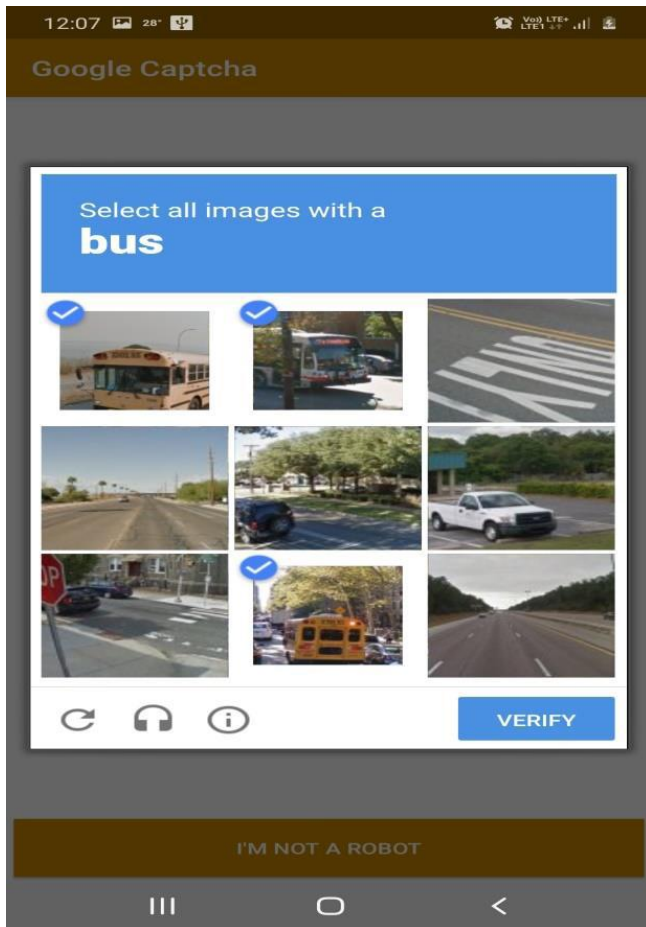
Figure 3: Selecting bus as object from CAPTCHA.

3. Generate n random images from the designated image set and digit set.

4. Chose the font, pixel size, image style, background color and other related attributes.

5. Select a unique object from selected different images. That image is then placed on the CAPTCHA image.

6. Place that image on CAPTCHA image to make the image read by the OCR programs.

7. Finally, apply a distortion to the generated CAPCTHA image by combining all images

Forming a complex background CAPCTHA image of needed dimension and optionally add desired type of noise and other From the image database present at the server or by downloading the images from the Internet select images or objects then apply transformations like ascending, gyration, lucidity, etc. to every and place it on the CAPTCHA image at crave positions. Result of this is CAPTCHA image which is shown to user.

When user get this image then user need to recognize object or concept presented in this image and act accordingly.
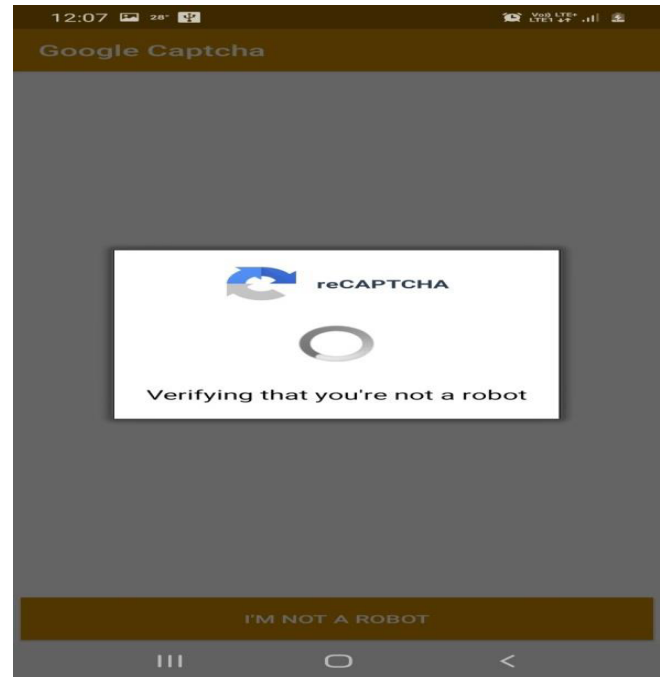

Figure 4: reCAPTCHA

2.3 APPLICATIONS

- It is used to prevent system from using various types of computing services.

- In online polls, registering for free email accounts (which may then be used to send spam), and, more recently, preventing system-created spam by requiring that sender pass a CAPTCHA test before the email message is delivered by this applications averting system from taken part.

- This is useful to prevent people from using system to assist with massive downloading of content from websites.

- In online message boards and blog comments to prevent system from attaching mailshot links as a message or comment

3. Pattern Based Captcha:

A pattern Captcha is a grid of 3X3 cell, where drawing a specific pattern (connecting specific sequence of cells in order) will unlock the Web Services. In this problem, the task is to calculate number of ways of making the lock pattern with number of connections in given range. In general terms, we are given a range as min and max, we need to tell how many patterns can be made which use at least min connection cell and at most max connection cell.
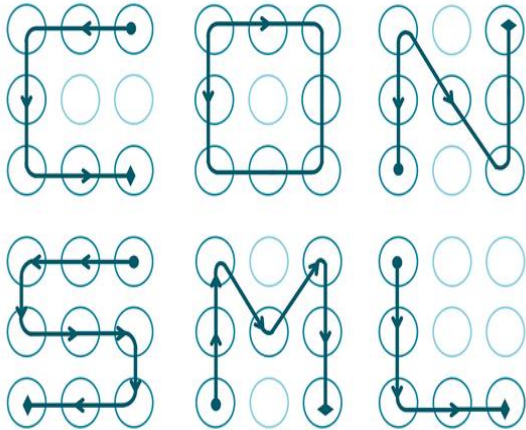
Figure 5: Pattern Based Captcha

V CONCLUSION

In this paper we introduced different types of CAPTCHA. This CAPTCHA technique are provided and scrutinized against misrepresentation, content and demonstration feature. Further, different exposure of the advanced technique have been designated on the basis of image size, feedback time ,perfection, time for image creation, deformation and robustness against attacks on data obtained through user studies and experiments. The results prevailed have corroboration the efficiency of the technique under discussion.

REFERENCES

[1] M. Tariq Banday, N. A. Shah, "A Study of CAPTCHAs for Securing Web Services", IJSDIA International Journal of Secure Digital Information Age, Vol. 1. No. 2, December 2009.

[2] Narges Roshanbin,James Miller, "A Survey And Analysis Of Current Captcha Approaches", Journal of Web Engineering, Vol. 12, No.1&2 ,2013.

[3] S. Mankhair, A. Raut, M. Mohimkar, K. Sukal, A. Khedekar, "Secured CAPTCHA Password Verification Using Visual Cryptography", International Journal of Engineering Science and Computing, May 2016.

[4] P. J. Charde, M. S. Khandare, "Review Paper on Improved Security Using Captcha as Graphical Password", IJSRSET, 2016.

[5] A. Sinha, Dr. S. Tarar, "Review Paper on Different CAPTCHA Techniques", International Journal of Computer Science And Technology,March 2016.

[6] M. Tang , H. Gao , Yang Zhang , Yi Liu ,Ping Zhang ,Ping Wang, "Research on Deep Learning Techniques in Breaking Text-Based Captchas and Designing Image-Based Captcha", IEEE Transactions on Information Forensics and Security ,Volume: 13 , Issue: 10 , Oct. 2018.