International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

A STUDYING ABOUT THE DIFFERENTS VARIETIES OF CAPTCHA

NAME - PABITRA MOHAN PANIGRAHY
DESIGNATION – RESEARCH SCHOLAR SUNRISE UNIVERSITY ALWAR
GUIDE NAME - DR. SURAJ VISWANATH POTE
DESIGNATION- Associate professor SUNRISE UNIVERSITY ALWAR

ABSTRACT
CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a widely utilized security mechanism designed to differentiate between human users and automated bots on digital platforms. As the internet continues to evolve and interactivity becomes more crucial in online interactions, the need to safeguard websites and applications against malicious activities such as spam, data scraping, and unauthorized access has grown substantially. This abstract delves into the concept, evolution, and various implementations of CAPTCHA systems.

Keywords: - Captcha, Person, Security, Machines, Software.

I. INTRODUCTION

Information security is a crucial area of study in today's technological landscape. Here, I'll go through how CAPTCHA is utilized as a current-day security check to determine whether or not a computer is being managed by a bot or a person. To tell machines and humans apart, CAPTCHAs are implemented. An internet bot, often known as a web robot, is a piece of software that performs mechanized operations in cyberspace. Conventional methods of security, such as requiring each user to log in with a unique username and password, are often compromised, and a wide variety of automated assaults may be carried out with the use of specialized software. The word "CAPTCHA" was created in the year 2000 by CMU (Carnegie Mellon University) researchers Luis Von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford [1]. The "Completely Automated Public Turing Test" (CAPTCHA) is a time-efficient method for determining whether or not a user is human. The term "Turing test" refers to the commonly accepted interpretation of a machine's actions when given with a set of predetermined choices from which it must make a decision [2]. The benefit of CAPTCHAs is that it is difficult for computers to decipher the text behind the distortions in the photos, but people have no trouble doing so. CAPTCHA uses a Reverse Turing test [3] in which the CAPTCHA software is the judge and the user is the participant. If the test is successful, the user is recognized as human; otherwise, automated assaults are suspected.

To stop automated programs from misusing websites like free email services, wikis, blogs, etc., CAPTCHA is used as a defense mechanism [4]. It is often used to protect web-based applications since it is a human-interactive proof method [5]. CAPTCHA's primary use is security, however it is also utilized as a standard. A benchmark is a baseline against which performance may be measured in an objective, scientific way [11]. Protecting

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

E-mail and other services against automated assaults is a common CAPTCHA function.

CAPTCHAs must adhere to three fundamental requirements: CAPTCHA (i) is straightforward for humans to decipher, (ii) should be simple for a machine tester to develop and grade, and (iii) should be challenging for a software robot to circumvent. Education, commerce, online banking, and even social interactions are now mostly conducted through the internet. In order to access these sites, visitors are required to fill out a variety of surveys and registration forms, providing personal information about themselves in the process. The proliferation of digital technology has led to the development of several hacking programs capable of automatically stealing sensitive information. Therefore, attacker assaults by fake entry on such sites raise traffic, use computer resources, slow down the server, and occasionally alter the whole web examination. So, a CAPTCHA is needed whenever this kind of thing happens.

II. CAPTCHA VARIETIES:

Text Based CAPTCHA

These days, one popular kind of CAPTCHA is text-based. They make use of people's superior ability to read text from images compared to those of Optical Character Recognition and other machine vision systems. CAPTCHAs that use text are generated at random. Clients see these text CAPTCHAs when they first log in to the system [6]. CAPTCHAs that are based on text are quite simple to solve. It's very practical, however it calls for a massive database of inquiries. Because there are so few character and number classes in text-based CAPTCHA, it is challenging for clients to distinguish the correct letters and numbers. The optical person acknowledgment approach may be used to decipher the text-based CAPTCHA.

Image Based CAPTCHA

Every image tells a story. We may utilize pictures instead of words in this manner. A user of an image-based CAPTCHA is presented with a set of images from which to choose one for verification purposes. If the chosen photo matches, the person is verified as authorized to access the system. Pennsylvania State University suggested an image-based CAPTCHA [8]. Even though text-based CAPTCHA has been attacked by bots, image-based CAPTCHA is more secure since bots can't read it. Pi CAPTCHA's CAPTCHA presents the user with a simple, straight-forward option to choose the right picture from a set of alternatives [9]. Clients with similar tastes are put to the test using image-based CAPTCHAs. Since pattern recognition is a challenging AI problem, it's not easy to bypass this test by relying on pattern recognition alone in a picture-based CAPTCHA.

Audio based CAPTCHA

Both text-based and image-based CAPTCHA designs have the same issue: they are inaccessible to those who have limited or no vision. When text or pictures are distorted on a screen, they become unreadable for users with visual impairments. An audio CAPTCHA variant [22] has been created as a solution to this issue. This technology allows users with visual impairments to access the internet by listening to the text and typing what they hear.

Biometric based CAPTCHA

Human physiology is included into biometric CAPTCHA systems. Users are

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

all unique in their own ways. The user's eyes, mouth size, nose size, hair color, etc. are all examples of biological attributes that may be used to identify the user. The computer then compares the current user's biometric information with that previously saved. Real-Time CAPTCHA, a novel login verification method, has been developed to increase the security of current biometric methods that depend on video or photos of a user's face. employing a unique "challenge" that is simple for humans but challenging for attackers employing machine learning and image generating technologies to impersonate legitimate users is the basis of this method.

III. ARTIFICIAL NEURAL NETWORKS

Is it possible for a computer to make a call and then adjust variables in an experiment or setting to accommodate that call? whether you want to know whether a lump of silicon and metal can make judgments and act on those decisions as we humans can, the answer is yes.

To solve many problems that can be easily solved by the perceptual and intellectual ability of people, we have created an intellectual gadget that performs a variety of well-defined domestic duties with simplicity and consistency unsurpassed by humans. Using their senses of sight, hearing, touch, smell, and taste, humans are able to build mental instances in their Biological Nervous System from data presented in these and other formats. Even when the facts are changed or twisted by transformations like translation, rotation, and scale, the brain still forms these patterns. When the input data is noisy, missing, or mixed up with data from a different model, humans may nevertheless recall the previously-learned patterns. To yet, no computer vision framework has come close to matching the human eye's ability to discriminate between pictures formed by objects of wildly varying sizes, positions, and orientations. Even when covered with muck or obscured by other objects, people can clearly discern them under a variety of lighting situations. To add insult to injury, the demonstration of accurate language recognition technology pales in comparison to the demonstration of human adults who can readily recognize words uttered by various persons at varying speeds, pitches, and volumes, despite distortion and background noise. A biological neural network structure, composed of billions of neurons organized in a massively complex way, with each neuron connecting to thousands of others and working together to solve tough problems, is responsible for all of the human's duties. The mind has a structure that we may duplicate in a sequential fashion; this structure is parallelism. We can program Artificial Neural Networks, which are made up of different programmable computational elements (P.E), to do calculations anywhere in the globe.

In order to measure the tested capacities when we have no idea what kind of capacity they are, we can program or prepare the neural network to store, perceive, and cooperatively recover examples or data set passages to address combinatorial reorganization issues, to channel commotion from estimation information, to control badly characterized issues,, predications, and assurance as missed examples.

For a long time, the world's attention has been focused on the development of a conceptual framework capable of shaping

the actions of individuals. Several interesting and doable smart paradigms, such as the Artificial ANT system, the Cultural Revolution, DNA computing, and Immunity NET, may be integrated with the existing ANN technology. Because of its adaptability, ANN may readily incorporate a wide variety of existing paradigms. McCulloch and Walter Pitts, in the early years of 1943, devised a kind of a computing component called the McCulloch Pitts neuron, which executes a weighted sum of the inputs to the elements followed by a threshold logic operation [13]. This was a major step forward in the development of ANN.

IV. CONCLUSION

This study demonstrates that storing CAPTCHA as weight matrices is a significant improvement over the previous methods. In Chapter 1, we cover the foundations of CAPTCHA technology, the several types of CAPTCHA (such as Text based CAPTCHA, Audio based CAPTCHA, Image based CAPTCHA, Biometric CAPTCHA, and Puzzle based CAPTCHA), the ideas behind Artificial Neural Networks, and the goals of our study. Thesis or research-oriented research plan The remit and importance of the current study have been outlined.

Our investigation into previously established systems is covered in Chapter 2. The CAPTCHA system has evolved into a reliable defense mechanism against malicious code. Different CAPTCHA implementations are discussed in this chapter. We also detail CAPTCHA's potential uses and the security risks associated with it, including dictionary attacks, brute force assaults, spoofing, Man in the Middle attacks, DoS attacks, and phishing scams. We have also shown the operation of the Back propagation method. We have detailed the training and performance of many neural networks, including trainlm, trainbfg, traingd, traingdm, traingdx, trainnrp, trainoss, trainscg, traincgb, traincgp, trainbfg, trainr, and trainnrp.

The simulation work on the first goal of our study effort, i.e. machine learning of text form of CAPTCHA, is presented in Chapter 3 of this thesis. We have used MATLAB as a tool to train text-based CAPTCHA code samples. To train the network, we turned to MATLAB's neural network toolkit. The results are quite good, just as we expected, as seen by the performance curve. The machine was able to learn from the examples given to it.

Next, I expanded my research to determine which of the neural network toolbox's fourteen training functions is most suited for text CAPTCHA. We ran simulations for the same set of samples with the following fourteen functions: trainlm, trainbfg, trainbr, traincgb, traincfg, trainoss, trainnrp, trainscg, trainr, traincgp, traingdm, traingda, traingdx, and trainoss, and we compared their training performance in terms of time, epochs, and mean squared error (MSE). After training, we discovered that the trainlm function of the neural network toolbox provided the greatest results for teaching the system to correctly recognize text CAPTCHA patterns. Our experiment, our training settings, our performance curve, our weights and matrices, and our tests all point to a good or excellent result, thus we can confidently declare that our study has been successful.Because hackers can never decrypt the Text CAPTCHA for the weight matrix created in Neural Networks, it is incredibly helpful for users.

REFERENCES

1) Zhang, Lili, et al. "Captcha automatic segmentation and recognition based on improved vertical projection." 2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN). IEEE, 2017.
2) R. Hussain, H. Gao, and R. A. Shaikh, “Segmentation of connected characters in text-based CAPTCHAs for intelligent character recognition,” Multimedia Tools and Applications, pp. 1–15, 2016.
3) Chow, Yang-Wai, Willy Susilo, and Pairat Thorncharoensri. "CAPTCHA Design and Security Issues." Advances in Cyber Security: Principles, Techniques, and Applications. Springer, Singapore, 2019, 69 -92.
4) Siripitakchai, Apichai, Suphakant Phimoltares, and Atchara Mahaweerawat. "EYECAPTCHA: An enhanced CAPTCHA using eye movement." 2017 3rd IEEE International Conference on Computer and Communications (ICCC). IEEE, 2017.
5) Menna M.Elbalky, Medhat A. Tawfeek , Hamdy M. Mousa, “A comprehensive Study for Different Types of CAPTCHA Methods and Various Attacks”, Journal of Emerging Technologies and Innovative Research, June 2021, Volume 8, Issue 6.
6) Yu Hu1, 2, Li Chen1,2*, Jun Cheng3 , “ A CAPTCHA recognition technology based on deep learning” IEEE 2018, 978-1-5386.