Rise and Fall of Image Based CAPTCHA Schemes

Sanjeev Kumar[1]
Mohinder Kumar[2][0000-0003-2131-8387]
[1]Department of Computer Science, D.A.V. College, Abohar, PB INDIA
[2]Department of Computer Science & Applications, Panjab University Regional Centre, Muktsar, PB INDIA
[1]gumber_sanjeev@yahoo.com, [2]kumarmohinderr@yahoo.co.in

Abstract

CAPTCHA stands for Completely Automated Public Turing Test to Tell Computers and Human Apart. CAPTCHA is used for Internet Security specifically for accessing web sites. It is a Reverse Turing Test that identifies that the given problem is solved by a computer program or not. A number of CAPTCHA schemes are available today like, text-based, audio-based, video/animation-based, puzzle based etc. In this paper Image Based CAPTCHAs are collaborated at single place to analyze. The paper presents an extensive survey of Image Based CAPTCHA schemes from their generation to broken stage. Our target to review the literature is to identify and classify the existing literature on Image Based CAPTCHA, its types, the creation and breaking techniques. The paper puts light on the techniques that are used to generate these schemes and their limitations. The paper also discusses the effective methods for break these schemes.Modern classifiers such as Convolution Neural Networks and Dense Neural Networks are able to recognize image based data very effectively.

Keywords Words · Image Based CAPTCHA,Bot Program, Reverse Turing Test.
DOI Number: 10.48047/NQ.2022.20.12.NQ77737 NeuroQuantology2022;20(12): 4112-4120

1 Introduction

CAPTCHA stands for Completely Automated Public Turing Test to Tell Computers and Human Apart. The term is very popular in Internet Security. The word *Public* in the acronym tells that the code and data used by a CAPTCHA should be publicly available [1]. So if the code or data are private then it will not be a CAPTHCA. There are some valid reasons for making code or data public. First if a CAPTCHA uses private data then it is vulnerable to hacker attacks. If the hacker is successful in breaking the test the CAPTHCA ceases to be secure forever. Actually CAPTHCA must generate tests that are hard to pass for all computers but not hard to pass for computers that don't know a particular secret [1]. It is desired that a CAPTCHA should be broken because if a CAPTCHA is broken then a previously unsolved AI problem is solved. For the research community it is better as the more CAPTCHA that get broken, the more AI problem that get solved [1].

CAPTCHA was introduced by John Lanford of Carnegies Mellon University [1] but the basic work was done by Mori Naor who first time described the concept of Turing test to identify the difference between a human and BOT in 1996 [2]. The idea of Turing was introduced in 1950. It is about proving that you are a human to another human. A person asks you a number of questions and then he decides whether he/she is talking to a person or a program [3]. On the other hand it is a very different aspect to prove to a computer program that you are a

human or computer code. This process requires a test or set of tests that computers can evaluate. These tests are designed to be very easy for human to pass but computers cannot pass. In computer dictionary such tests are called CAPTCHA. So CAPTCHA are Human Interactive Proofs (HIPs), a challenge meant to be easily solved by computers but too difficult to be solved by current computer system. This must desired property is known as sweet spot as shown in Fig. 1

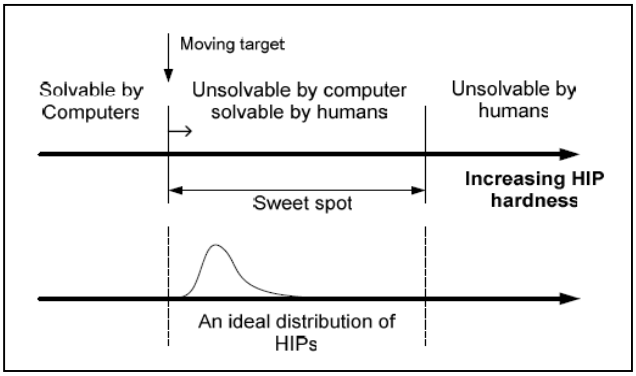


Fig. 1 Desired Properties of a CAPTCHA

2 Applications of CAPTCHA

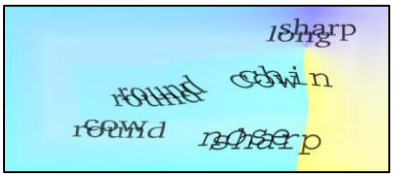
- Using CAPTCHA it is very easy to restrict robots or computer from playing online games. This is a fair play for fraud players [5][6][7].
- In the modern digital life most of the companies provide free email services. These are the target of bot attacks. A lot of companies use this technique to get free email accounts from which they can send junk mail. The best and easy method to avoid these bot attacks is the use of CAPTCHA. Most of the email providers have adopted this solution [1] [4].
- In modern days bank details like usernames, passwords and credit/debit card details are collected by phishing attacks. Actually some websites are exact copy of some original financial web sites and user is grabbed by giving secret and confidential details to these fake sites [10]. Here also CAPTCHA can be very affectively [11][12].
- Dictionary attack is a technique for defeating an authentication mechanism by trying to guess its secret password or passphrase by retrieving likely possibilities [8]. In such situations CAPTCHA can be very effective for defending against such dictionary attacks [9][10].
- Web scrapers (Program that extracts data from web sites) can be restricted from getting user's email addresses by presenting a checkpoint to solve a CAPTCHA before displaying email address information [1].
- After a fixed number of wrong attempts of password an account is locked but it is not a better solution. If the attempts are made by a computer program then it can replaced by entering a CAPTCHA to prove that there is a human on the other side and not a computer program [1] [4].
- CAPTCHA is used provides a solution against worms and spam to receive mail only if it is clear that there is not a computer program but human behind it.

3 Types of CAPTCHA

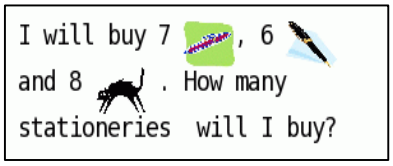
During the course of time many types of CAPTCHA schemes are developed for overcoming the limitations of previous ones. Some of the popular CAPTCHA schemes are listed below:-

- Text Based CAPTCHA
- Image Based CAPTCHA

- Audio Based CAPTCHA
- Video Based CAPTCHA



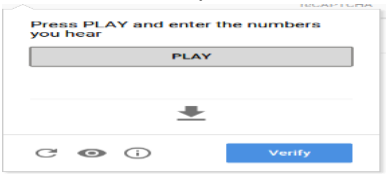
(a)



(c)

- Puzzle Based CAPTCHA

Some of the examples are shown in Fig. 2



(b)

(d)

Fig. 2 (a)Text Based CAPTCHA (b) Audio Based CAPTCHA (c) Puzzle Based CAPTCHA (d) Video Based CAPTCHA.

4 Image Based CAPTCHA

In this paper our concentration is on the Image Based CAPTCHA schemes. It may seems to be surprising that all the CAPTCHA schemes uses images most of the time then how image CAPTCHA is different. Actually in this scheme user is presented with images or images with text and asked to pick a correct picture or word that belongs to picture/s. This scheme is developed on the hypothesis hat computer programs are not as good as human in identifying graphics. In the next sub sections the development of such schemes is discussed:-

4.1 Reported Work on Development of Various Image Based CAPTCHA Schemes

As Text Based CAPTCHA schemes became vulnerable to attack so many researchers introduced a new method to defy computers. The proposed new schemes were based on the concept of image identification. This new scheme proved very popular even in modern days. The emergence of internet and wide image based applications like Facebook, Orkut and Google Image Search Engines boosted this new idea. The various Image Based CAPTCHAs that were developed are discussed below:-

- BONGO Method

The concept of Image based CAPTCAH like BONGO method was first proposed by M.M.Bongard in 1970 [24] . It is a visual pattern recognition problem. The user is given two blocks of some random shapes and finally a random shape is to be identified from the user by telling to which block it belongs. No language requirements are needed to pass the test but a program can be easily trained to solve this kind of visual puzzle. Chew and Tygar[29] described using labeled photographs to generate a CAPTCHA. They generated a database of labeled images by feeding a list of easily-illustrated words to Google Image Search [27]. For making it simpler so that bad images are not shown, they make its database small that resulted in a weak CAPTCHA. Also labels are also vulnerable to attack on image based CAPTCHAs.

- PIX CAPTCHA

In 2004 PIX CAPTCHA was proposed [13] as a solution to this problem. In this CAPTCHA some label images are picked from the database and a choice of 70 options are given to the user from which he has to pick one. The CAPTCHA is presented with four picture related to a common class. But the PIX CAPTCHA had a lot of problems like small database only 70 classes are used. If the database is large than more than 70 classes can be handled that make it time consuming. Finally some images are related to abstract class so the user is frustrated. HotCAPTCHA is also introduced in that was based on images. 9 images of humans

are presented to the user and the user is asked to select a "hot" one. The "Beauty" is a subjective concept so the choice is very confusing for number of cases. So the CAPTCHA is not very popular for most of the websites[13].

- Collage CAPTCHAs

In 2011 M. Shirali developed a number of new image-based CAPTCHAs like CAPTCHA for children in which the user is given some images of object like vehicles, animals etc. The user is given audio based (in English language) question to select particular type of object to pass the test. The images are downloaded online from Yahoo etc. this is very effective for such systems that does not support keyboard. In Collage CAPTCHA the images are presented to the user but this time the question is rendered on the screen rather than in audio. In Advanced Collage CAPTCHA the images are given in two set. Left side displays the goal image and the user are asked to pick all the images on the right side that belong to the left side image. So the numbers of clicks are more as compare to the previous CAPTCHA schemes. In Online Collage CAPTCHA the picture are retrieved online and otherwise it is same as Collage CAPTCHA [15][16][17][19][25].Other image-based CAPTCHAs that is known as Implicit CAPTCHA and Drawing CAPTCHA was proposed in 2008 by Shirali-Shahreza[14]. Implicit CAPTCHA is questions based CAPTCHA. The user is given a question in the image e.g. to click on the top of the hill etc. the scheme requires the use of English language. On the other hand Drawing CAPTCHA does not require any language proficiency. In this scheme the user is given a screen with noisy background with a number of dots. The user is asked to connect certain dots on the screen. So it is a mixture of image based and puzzle based CAPTCHA.Fig.3 shows some Image Based CAPTCHA examples:

(a) **(b)** **(c)** **(d)**

Fig. 3 (a) PIX CAPTCHA(b)Drag n Drop CAPTCHA(c)Implicit CAPTCHA Method (d) Assira CAPTCHA

- ASIRRA CAPTCHA

Microsoft developed ASIRRA CAPTCHA [27].It is an image based CAPTCHA. The user is given 12 images and is asked to find only cat among 12 images. Image size is 250 X 250. The images are collected from a large image database (3000000 images and 10000 added everyday) of petfindder.com. The author reported a quick response time 15 seconds to solve it. ASIRRA is secure CAPTCHA from a number of aspects. The design of ASIRRA is secured from Brute Force attack by using the use of token bucket algorithm. Further ASIRRA also maintains a two token bucket, one for per IP and one for per session. This technique saves it in the sharing IP address environment. The designers of ASIRRA also made it more useful and more accessible by the use of their novel Partial Credit Algorithm. In that they use the concept of intermediate verified users. Actually this algorithm made a scope of minor errors for the humans so that even after a wrong selection they are not treated as bots. Also with PCA and Tokens the success rate of bots is also controlled almost zero.

- Lineup CAPTCHA

A photo based authentication was proposed [30] by SaritaYardiet. all. It is known as Lineup CAPTCHA. The user is given a photo and asked to identify the person in the photo. The images of persons are taken from the Facebook account of the user. The persons that are being asked belong to the group of the user. The security of the scheme is enhanced by setting the level of the questions being asked. Like what is happening in the photograph etc. the authors assumes that to solve such kind of authentication requires a lot of effort.

- Multi Model CAPTCHA

Almazyad and Kouchay utilized Multi Model CAPTCHA in 2011[20] in this scheme the user is given an image with four text labels on it .The labels are associated with the image but only one is a perfect matches to the image .This perfect label has to input by the user to pass the challenge. For security the labels are embedded in the background of the image but these are very easily extracted from the image as the color of the text is same for all the labels. Font of the labels is same but not the straight as Times New Roman. Segmentation of the font is straight forward.

- Nintendo CAPTCHA

M. Shirali –Shahreza& S. ShiraliShahreza proposed this CAPTCHA also[18].It uses Nintendo DS that is lightweight game console used for playing audio/video, education, chat and internet surfing etc. the CAPTCHA is same as Online CAPTCHA but with a lesser number of objects (four) because Nintendo has a very small memory. Images are also small without rotation so that images can occupy lesser space. The drawback of this CAPTCHA is that it requires proficiency in English language as well as a device that is Nintendo enabled.

- IdentiPic CAPTCHA and DOG CAPTCHA

It is also an image based CAPTCHA. The user is given three pictures and three combo boxes having 10 options. The user is required to pick the correct option for each image to pass the test [22]. The DOG CAPTCHA is similar to Assira CAPTCHA. The user is asked to click on all the images until all the images are look like the given left side image [21].

The following Table 1 lists down the various Image Based CAPTCHAs with the usability and security measures.

Table 1. Image Based CAPTCHA Schemes

Ref	Scheme	Usability	Security	Language	Year
[24]	BONGO	100%	100%	English	1970
[29]	Anomalies Image CAPTCHA	95%	100%	Independent	2004
[13]	PIX CAPTCHA	90%	100%	English	2004
[13]	HOT CAPTCHA	95%	100%	English	2004
[27]	ASIRRA CAPTCHA	99.96%	100%	English	2007

[15]	Collage CAPTCHA	100%	100%	English	2007
[17]	Online Collage CAPTCHA	100%	100%	English	2007
[14]	Implicit CAPTCHA	100%	100%	English	2008
[14]	Drawing CAPTCHA	100%	100%	Independent	2008
[16]	Advanced Collage CAPTCHA	100%	100%	English	2008
[30]	Lineup CAPTCHA	100%	100%	English	2008
[19]	APTCHA for Children	100%	100%	English	2011
[18]	Multiple SEIMCHA	90%	17.5%	English	2011
[20]	Multi Modal CAPTCHA	100%	100%	English	2011

4.2 Reported Work on Breaking Image Based CAPTCHA Schemes

With the advancement of Machine Learning tools and advent of Deep Learning algorithms it became very easy to classify images. Very large number of images can be processed at very fast speed with latest GPUs. Many of the researchers tries to test these new algorithms to crack these security schemes that were based on purily images and they succeeded. The successful tacks on some of the above discussed schemes are as follows:-

- Breaking ASIRRA CAPTCHA

The ASIRRA CAPTCHA is broken with the success are of 82.7% [26]. The author used a SVM classifier that extracts the color features (F1, F2, F3) and texture features (G1). For the color features the author uses HSV model and images are divided into cells. The author said that as the number of images in the classifier is increasing the accuracy is also increasing. The author also pointed that the PCA is also helpful in breaking the CAPTCHA. But the Token Bucket Algorithm is decreasing the success rate of the classifier. Even the use of PCA and Token Bucket does not stop the classifier to break the ASIRRA CAPTCHA.

- Breaking Facebook Authentication

Iasonas Ploakiset. all designed a attack on the photo based CAPTCHA. They reported that a determined attacker can achieve 100% success rate of breaking suh Social Authentication like Facebook. Even a casual attacker can break these challenges with success rate of 22% [31]. They also highlighted a lot of weaknesses of Facebook's Social Authentication like it requires at least 50 friends to present the challenge, the user's friend must be tagged (this tagging is not very accurate most of the time so the usability is also very low for a legitimate user). The time of solve this challenge is 5 minutes that is very long as compare to other CAPTCHA's. 80% of the challenges contain such photos in which the person is not clearly visible. Also some of the challenges do not contain even a single face to be identified. The challenge is presented if the user is logging from a different geographical location or a new device is used to access the account. Finally the challenge presents the user with an option to bypass the test by providing their date of birth. The data is obtained very easily by the attacker because the profile contain date of birth etc. the author tried to break Social Authentication in two ways: casual attack and determined attack. In casual attack the attacker can gain victim's friend list that is publicly available (47% of the users) and a determined attacker can gain 84% by issuing friend request to the victim's friends. The user ID and names of the friends are retrieved by the Facebook database. Next the photos are stored with user ID and names by accessing the albums of the target's friends. Then by using face detection software the faces are detected. The faces are labeled with the tag information. Finally the names are classified with kNN classifier with k=3.

- Google reCAPTCHA

The latest indivisible CAPTCHA is announced by Google that is free from every text, image, video and puzzle. It just requires a click of the mouse by the user. It is very famous across the web sites. In 2016 [28] the first successful attack on Google Invisible CAPTCHA is reported.

Google reCAPTCHA is based on Google's advanced risk analysis system. Based on the level of confidence assigned to a specific request this system will select which type of challenge to present the user [28]. The collage is presented from simple to hard as follows:First the new user friendly CAPTCHA is presented to the user. After clicking the checkbox in the widget if the advanced risk analysis system has high confidence then the checkbox is changed to a tick. If the confidence is not high then according to the level of confidence one of the following versions of reCAPTCHA is represented as shown below:

- Image reCAPTCHA
- Distorted one word
- Scanned word
- Distorted two word
- Fallback CAPTCHA

The author tried to do a fake click on the Google reCAPTCHA and they succeeded in that. They highlighted a number of weaknesses in the Google's advanced risk analyses in term of browsing history (repeated on 9th day), genuine account and fake accounts (by bots), Geo locations (fraud countries), no detection of Automation of browser actives, mouse behavior (java script based click events), no reputation of cookies files, no site restriction of (number of requested per IP address), etc.The author also proposed a semantic based attack on the Google Image CAPTCHA. They used Google Reverse Image Search for image guess. They also strengthen their algorithm by the use of a lot of Image annotation generator like Clarifai, NeuralTalk etc. They developed their tag classifier and then attacked image CAPTCHA with the success rate of 70.78 %.Another kind of image CAPTCHA is also proposed by Facebook that is similar to Google reCAPTCHA. The same technique is also used to break Facebook Image CAPTCHA with a success rate of 83.5% .

5 Guidelines to Make Strong Image Based Authentication Schemes

It is proven that many of the popular images authentication schemes are already broken with a great success rate so there is a need to reconsider the designs of thee schemes. These schemes needs to be improved from the security point of view. On the other hand it is also very crucial to make these designs not so complex that they loose the usability factor. To achieve the sweet spot as described in Fig.1 the new designs must possess the balance between security and usability. Many of the security barriers have been applied in Microsoft and Google schemes but these are not very much effective to make these designs attack proof.Some methods, that can be applied to make these image authentication schemes stronger are as follows:

- Data base of image should be very dynamic that must be updated with very large number of new images. Most of the classification techniques are trained with some existing database. So to make these techniques unsuccessful the database must be updated at very fast speed.
- Simple images can be altered with noise and distortions. This method can be applied with great care because too much distortions and noise can make the images almost un identifiable both for the program as well as for humans.
- Partial images can also be used to make these designs stronger although such images should be enough easy to guess by the humans other-wise it can be a useless method.
- In spite of using real world images, cartoon images can be used with some combinations of colors. Some of the schemes like Four Panel CAPTCHA already used cartoon images but these images are binary images. Such images can generated with the help of filters tools that are mostly available in all image processing libraries.
- Matching of related images can also be very effective method while designing such schemes. Although the number of matches must not be greater than 3 otherwise it makes the challenge too much time consuming.

Conclusion

Security on the Internet is always very important issues from the beginning. In the recent times online registration, online games, online polls are becoming more popular that also attracts bot programs to create chaos on the web site. So it becomes very critical to provide a way to defy such bot programs. CAPTCHA is the best and cheapest method to provide the first level barrier. It is observed that Image Based CAPTCHAs have provided this security for a long time but now with the help of new classification algorithms these schemes have been compromised..

Image Based CAPTCHAs are still very much in use even after a number of attacks. The future of Image Based CAPTCHA is not over. With the help of image processing tool, creativity and mathematical approach the Image Based CAPTCHA can be given new life. The paper also suggests some of the guidelines in this path. The Image Based CAPTCHA schemes are never used with combination of another CAPTCHA schemes for providing more security. Such efforts can be very useful in the future if used by considering with right measures of usability.

References

1 Ahn L, Blum M and Langford J (2004) Telling Humans and Computers Apart Automatically. Communications of the ACM, 47(2):56-60..

2. Turing AM (1950) Computing Machinery and Intelligence. Mind, 59(236):433-460.

3. A. M. Turing, Computing Machinery and Intelligence. In: Mind ,vol 59, No. 236, pp. 433-460, 1950.

4. Pope C and Kaur K (2005) Is It Human or Computer? Defending e-commerce with CAPTCHAs. IT Professional, 7(2):43-49.

5. Yampolskiy R and Govindaraju V (2008) Embedded Non-interactive Continuous Bot Detection. Computers in Entertainment (CIE), 5(4):7:1-7:5.

6. Golle P and Ducheneaut N (2005) Preventing Bots from Playing Online Games. ACM Computers in Entertainment, 3(3):1-10.

7. Hilaire S, Kim H and Kim C (2010) How to Deal with Bot Scum in MMORPGs. Proceedings of IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR), 1-6.

8. Dictionary Attack, available at http://en.wikipedia.org/wiki/Dictionary_attack.

9. Chakrabarti S and Singhal M (2007) Password-based Authentication: Preventing Dictionary Attacks. Computer 40(6):68–74.

10. Pinkas B and Sander T (2002) Securing Passwords Against Dictionary Attacks. Proceedings of 9th Conference on Computer and Communications Security, 161–170.

11. Phishing Attack, http://en.wikipedia.org/wiki/Phishing.

12. Dynamic, Mutual Authentication Technology for Anti Phishing (2012),www.confidenttechnologies.com

13. Li C, Sudani W, Wang J, Liu F and Gill A (2010) Protection Through Multimedia CAPTCHA. Proceedings of 8th International Conference on Advances in Mobile Computing and Multimedia, 63-68.

14. Shirali-Shahreza M and Shirali-Shahreza S (2008b) Dynamic CAPTCHA. International Symposium on Communications and Information Technologies, 436-440.

15. Shirali-Shahreza M and Shirali-Shahreza S (2007a) Collage CAPTCHA. Proceedings of 9th International Symposium on Signal Processing and Its Applications, 1-4.

16. Shirali-Shahreza M and Shirali-Shahreza S (2008a) Advanced Collage CAPTCHA. Proceedings of 5th International Conference on Information Technology: New Generations, 1234-1235.

17. Shirali-Shahreza M and Shirali-Shahreza S (2007b) Online Collage CAPTCHA. Proceedings of 8th International

Workshop on Image Analysis for Multimedia Interactive Services, 58-58.

18. Mehrnejad M, Bafghi A, Harati A, and Toreini E (2011) Multiple SEIMCHA: Multiple Semantic Image CAPTCHA. International Conference on Internet Technology and Secured Transactions (ICITST), 196-201.
19. Shirali-Shahreza M and Shirali-Shahreza S (2008e) CAPTCHA for Children. Proceedings of International Conference on System of Systems Engineering, 1-6.
20. Almazyad A, Ahmad Y and Kouchay S (2011) Multi-Modal CAPTCHA: A User Verification Scheme. Proceedings of International Conference on Information Science and Applications (ICISA), 1-7.
21. CAPTCHA the dog, available at, http://www.CAPTCHAthedog.com.
22. identiPic CAPTCHA, available at , http://www.identipic.com.
24. Bongard M (1970) Pattern Recognition. Hyden Book Co. Spartan books.
25. Shirali-Shahreza M and S. Shirali-Shahreza S (2008c) A CAPTCHA System for Nintendo DS. Proceedings of the 7th ACM SIGCOMM Workshop on Network and System Support for Games, 104-105.
26. Golle P (2008) Machine Learning Attacks Against the Asirra CAPTCHA. Proceedings of the 15th ACM conference on Computer and communications security, 535-542.
27. Elson J, Douceur J and Howell J (2007) Asirra: A CAPTCHA That Exploits Interest-Aligned Manual Image Categorization. Proceedings of CCS, 366-374.
28. Sivakorn S, Polakis I and Angelos D (2016) I am Robot Deep Learning to Break Semantic Image CAPTCHAs. Proceedings of IEEE Euorpean Symposium on Security and Privacy.388-403.
29. Chew M and Tygar J (2004) Image Recognition CAPTCHAs. Proceedings of the 7thInternational Information Security Conference (ISC 2004), 268–279.
30. Yardi S, Feamster N and Bruckman (2008) A Photo-based authentication using social networks, Proceedings of WOSN ’08.ACM
31. Polakis L, Lanciniand M and Kontaxis G (2012) All Your Face Are Belong to Us: Breaking Facebook’s Social Authentication. Proceedings of the 28th Annual Computer Security Applications Conference, 399-408.