HCTL Open International Journal of Technology Innovations and Research (IJTIR)
http://ijtir.hctl.org
Volume 14, April 2015
e-ISSN: 2321-1814, ISBN (Print): 978-1-62951-946-3

A Survey of Captcha based Web and Application Security Methods and Techniques

Sandeep Mahato[1], Varun Prakash Saxena[2], Devendra Bhavsar[3]

sandeep.mahato94@gmail.com

Abstract

CAPTCHA program is used to differentiate human from computers and has many applications like online polls, free e-mail services, worm and spam protection, preventing dictionary attack, search engine bots. CAPTCHA ensures bots won't enter a website. CAPTCHA is a reverse turing test based on text, image or audio based challenge response system. In this reverse turing test interrogator is computer rather than a human. It is widely accepted that a good CAPTCHA must address two main requirements: robustness and usability. In this paper design principles and some CAPTCHA based techniques are described with their advantages and disadvantages. It may help to study and develop more robust CAPTCHA with good usability.

Keywords

CAPTCHA, Design Principles, reserve turing test

Introduction

CAPTCHA *(Completely Automated Public Turing Tests to tell computers and* Humans Apart) is used for HIP (Human Interaction Proof). Different types and methods of CAPTCHAs are being studied to maximize robustness and usability of CAPTCHA. Image Verification security method ensures the HIP where human user can easily recognize the same from distorted text. Sometimes heavily distorted text image becomes difficult to recognize for human also so that at the time of designing CAPTCHA only significant distortion and noise is to be added.

CAPTCHA design principles

This article has proposed design principles to create secure CAPTCHA which include Core feature principle, Anti-recognition, Anti-segmentation.

Core features principles are

Randomize of character length: CAPTCHA should not be of fixed size. It gives enough information to attackers.
Randomize the character size: Use of several fonts reduces the classifier accuracy.

Wave the CAPTCHA**:** Waving the characters in CAPTCHA raise the difficulties for attackers to find cut points.

The anti-recognition techniques considered are

1.Using multiple fonts or font-faces.
2. Which charset the scheme uses.
3. Using variable font size.
4. Distorting the CAPTCHA globally using attractor fields.
5.Blurring letters.
6. Tilting Rotating characters with various angles.
7. Rotating the characters in a wave fashion.

The anti-segmentation techniques considered are:-

1. Complex Background: Try to hide the text in a complex background to "confuse" the solver.
2. Lines: Add extra lines to prevent the solver from knowing what the real character segments are.
3. Collapsing: Remove the space between characters to prevent segmentation.

The breaking of CAPTCHA

This paper also discuss about the CAPTCHA breakers which are able to break many popular text based CAPTCHAs.

Decaptcha (CAPTCHA solver program) uses five stage pipeline

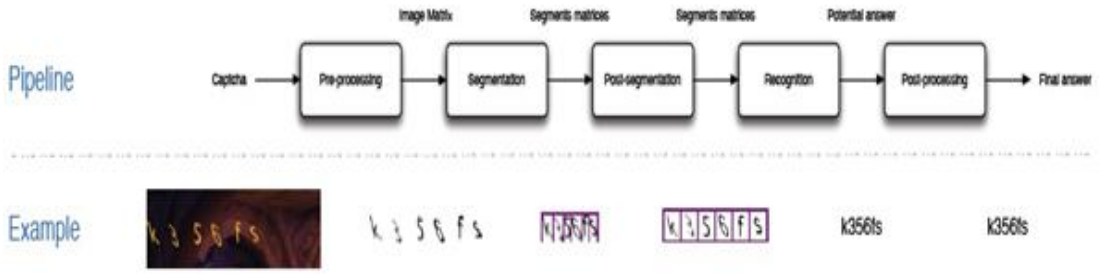

Figure 1 Decaptcha five stage pipe line

1. Pre-processing: In this stage background is removed and captcha is binarized and values are stored in matrix.
2. Segmentation: In this stage Decaptcha tries to segment captchas using various methods like color filling segmentation which uses paint bucket color flood algorithm.
3. Post-segmentation: In this stage segment's sizes are normalized for easier recognition.
4. Recognition: In this stage classifiers are taught about looks of letters after the segmentation of CAPTCHA.
5. Post-processing: In this stage output of classifier is improved [1].

Distortion Estimation Techniques in Solving Visual CAPTCHAs

This article explores Distortion Estimation Techniques to solve Visual CAPTCHA. Visual CAPTCHAs are used to prevent spammers from performing automated techniques in acquiring free email accounts from sites such as Yahoo and to stop automated ticket purchases from Ticketmaster.

This distortion Estimation technique with correlation approach uses core and minipatch.
In this approach "core" and "minipatch" framework correctly identifies the word in an EZ-Gimpy challenge image and Gimpy-r image challenge used by yahoo. Core was defined as most distinct or least correlated with the rest of the image. These cores represent the most distinct features of the word and acts as an anchor points between the template and challenge image. Three such sections or cores were found that do not overlap. "Minipatches":- template word was split into small overlapping sections called "minipatches". Now keeping track of core positions with respect to minipatch positions. Any variation in minipatches represents the type of distortion occurred. If large range of minipatches of distortion needs to be estimated, large set of minipatches with more variation may be used with the cost of increased execution time.
On the basis of these cores and minipatches matching is done.
Matching: It involves three steps
• Background removal: Background noise is removed using thersholding technique which takes into account the number of neighbour pixels that are above the threshold. After this processing, the image includes the challenge word and small bits of background noise.
• Template core anchoring onto the challenge image:- (Core anchoring) With the clean challenge image, each template image is tested against the cores and minipatches. Starting with the three cores, the best correlated locations are found.
• Optimal minipatch placement and correlation calculation:- Starting with the most beneficial correlated core, we first choose the minipatch closest to the core location. These details as well as the relative location on the next minipatch are used to formulate the minipatches, beginning the minipatches closest to the core and dealing outwards.

The core and minipatch approach compares each template image with the challenge image. In the case where you will find there's substantial dictionary and enormous local distortions, the computation time becomes unmanageable. You will find too many templates and minipatch variations to take into account before attaining a guess. Therefore this information works on the new multi-stage approach that estimates the neighbourhood distortions so finds web site image using the lowest average distortion through the challenge image. Through the initial guess, It builds confusion matrices when a maximum likelihood test was placed on maximize success. Geometric constraints are exploited to attenuate the search space in addition to to differentiate between virtually identical images.

The correlation approach works well when there are small distortions with a small dictionary. For more accuracy, there is a tradeoff between using more core and minipatch variations versus runtime. The direct distortion estimation approach works well on images with large continuous distortions. [2]

Pixel count attack

In this case study for yahoo 100 random samples were collected for sample set and observed that CAPTCHA had following characteristics:
1. It was the distorted image of letters from English word randomly chosen coming from a fixed number of 6000 words.
2. The distortion method used became a random shearing technique through which picture of text is distorted by randomly shearing it both vertically and horizontally. The

pixel in each column with the image are translated up or down by an amount that varies randomly from one column to a higher.
3. There was clearly only two colours in each challenge image, one for background and other for foreground, the choice of colours was either user specified or randomly developed by the CAPTCHA.
4. Each Challenge only used capital letters.
5. Each letter might overlap when projected vertically but rarely associated with the other.

Pixel count attack might be achieved easily since several pixels of every challenge image were of background color and any pixel in addition to background color value inside the image foreground could easily and automatically extracted by way of program. Although a letter may be distorted in a different shape whenever, it comprised a consistent quantity of foreground pixels from the challenge image—that is certainly, each letter stood a constant pixel count. The pixel count per letter at a to Z was done and found that most letters were built with a distinct pixel count. Vertical segmentation lines were utilised to split up image by cutting through columns without foreground pixel by any means. Amount of fore ground pixels of segment were counted and compared with pixel count lookup table to discover the letter within the segment. Search for table contains distinct pixel count for every letters.

Basic Attack

For basic attack first used the vertical segmentation method, an ordinary technique that maps a graphic to a histogram representing the volume of foreground pixels per column inside image. Using vertical segmentation lines image is separated by cutting through columns with no foreground pixels at all. If we segmented task, our attack simply counted the amount of foreground pixels in each segment.

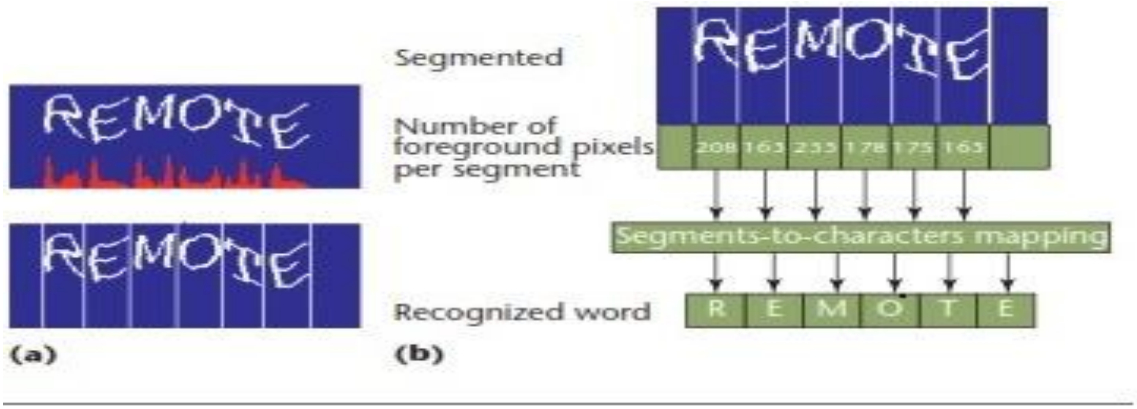

Figure 2 basic attack

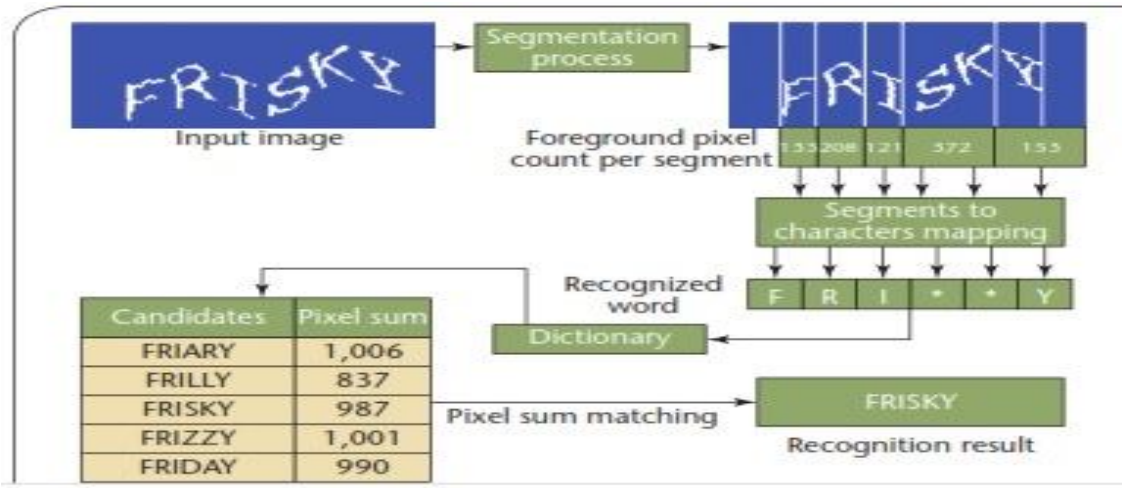

Figure 3 Dictionary Attack

Dictionary Attack

Sometimes basic attack failed to completely recognize some challenges. The target CAPTCHA used English words; basic attack can be enhanced by using a dictionary attack as follows. We first compiled a dictionary of roughly 6,000 six-letter English words. We used any partial result that the basic algorithm returned as a string pattern to identify candidate words in the dictionary that matched the pattern [3].

Recently proposed CAPTCHAs

Multi color captcha scheme with Empirical Algorithm for Protecting Text-based CAPTCHAs against Segmentation Attacks

This article aims to provide an effective and efficient method to generate text-based CAPTCHAs which may avoid against segmentation attack. Multi colors and concept of brush without using drifting parts was used with color selection process by users or developers for the CAPTCHA in this proposed scheme. They have used simple accumulating functions to accomplish diffusion on painted colors and DES encryption to realize an excellent a higher level confusion within the brush pattern. To facilitate normal users and developers, it proposes an empirical algorithm with support of Taguchi approach to guarantee the products the chosen color schemes. This proposed methodology has at the least three advantages — 1) the settings of color schemes is usually fully customized by the user or developer; 2) the standard of selected colors have desirable statistical features which can be ensured by Taguchi method; 3) the algorithm may be fully automated into computer programs. A CAPTCHA that entirely relies upon color arrangement to supply reasonable security and usability simultaneously. This post addresses this problem by making a methodology to create usable CAPTCHAs by employing multiple colors. The main issues for this were- How many colors shall a text-based CAPTCHA have? Which colors shall be chosen base colors for a text- based CAPTCHA? How shall the colors be mixed and arranged to protect a text-based CAPTCHA against segmentation attack?

To resolve these issues fundamental principle of confusion and diffusion was adopted in security to frustrate most color clustering algorithms and applied Taguchi method to

select colors so that they have good statistical properties and difficult to be separated by using most statistical analysis. After that it randomizes the pattern whilst coloring the CAPTCHA in order to frustrate the attacker who can make a few success attacks. In this article an algorithm was included to select desirable colors, a methodology to paint the selected colors onto the CAPTCHA and a pilot study of usability of our generated CAPTCHAs.

The Taguchi method was “intended as being a cost-effective approach for reducing variation in products and processes.” it aims to cut back the variation of certain product in an uncertain environment for example finally user’s premises and also to make economical decisions found to be optimum during laboratory experiments for being so in end-user’s environments. Therefore, Taguchi method is also known as a robust experiment design. Taguchi’s preferred method of minimizing the number of experiments is to use the orthogonal array concept. Using Taguchi’s terminology, an experiment ‘factor’ that affects color mixture, such as different brushes; and a ‘treatment’ of a factor is a chosen, fixed value of that factor, such as a color of a brush were chosen. An orthogonal array was taken which is an array or matrix consisting of a set of symbols, (like, {0, 1}), which represent attributes of the objects; and any two columns in an orthogonal array should have same numbers of pairs of symbols (such as “00”, “01”, “10” and “11”) which balances the comparisons. Different treatments were arranged in different columns of an orthogonal array in a balanced manner so that all columns can be evaluated independently. Then a user of Taguchi method can choose freely to map the colors with binary symbols.

Defined orthogonal arrays (OAs) are matrices with the following two properties-
Those elements appearing in a column occur the same variety of times and people elements appearing in the column occur exactly the same variety of times. These properties make certain that the fairness condition holds. The first property suggests the same prospects for appearance of each and every parameter value; the next one suggests that all possible values of 1 parameter appear against their counterparts of any parameters. After choosing OA and mapping experimental settings observable data is collected in an array whose row size is same as OA but column size may vary. The minimal number of samples can be determined on the basis of the number of outliers and a properly chosen OA.

Based on Taguchi method, empirical algorithm was proposed as-
Step 1. Determine the number of brushes and the number of colors for each brush.
Step.2. Based on the numbers of Step 1, choose an appropriate OA that can accommodate the required settings.
Step.3. Choose a handful set of colors for each brush.
Step.4. Map the color settings to the selected OA.
Step.5.Obtain the experimental result array by evaluating the R-G-B values based on the mixture of the colors in each row of the OA.
Step.6. Calculate the logarithmic value by using Equation 1 for each row of the array obtained in Step 5
Step.7. Perform an ANOVA test to identify the color sets which is not significantly different to any other color set. If there exists any, replace those color sets and repeat Step 4 until all of the color sets pass the ANOVA test.[4]

Question based CAPTCHA

In this posting Question based CAPTCHA was proposed in which judging by some pre-designed patterns of questions were prepared. During these patterns a few of the portions of the condition were variable and changeable and they are generally chosen from some items randomly. For instance question can be like "You will discover 5 cats, 3 apples, and 4 dogs on the table. How many pets do you have available in total?" The answer then is 7

e-ISSN: 2321-1814, ISBN (Print): 978-1-62951-946-3

(3 cats+4 dogs=7 pets). Here user only needs to enter lots. To boost the diversity and selection of the questions by designing different and various patterns and even cause them to tougher and even more sophisticated, too. In place of some words you can put a perception of those words like in place of cat, apple, dogs and table it's possible to take their images. Computer may recognize images however it has to separate text from images that could be a hard task. Possibility of computers to successful answers on this kind of real question is very less considering that the computer necessitates the following abilities:-

1- Computer must recognize phrase shown in the image through OCR-based software.
2- Computer must recognize shapes shown from the image. Needless to say before who's must separate texts from the images which might be a difficult process inside of it.
3- After recognition of texts and pictures your computer must be able to understand the question.
4- Eventually and in some cases if the computer does each of the above-mentioned stages successfully it has to be necessarily capable to answer the shown question.

Example of Question based CAPTCHA

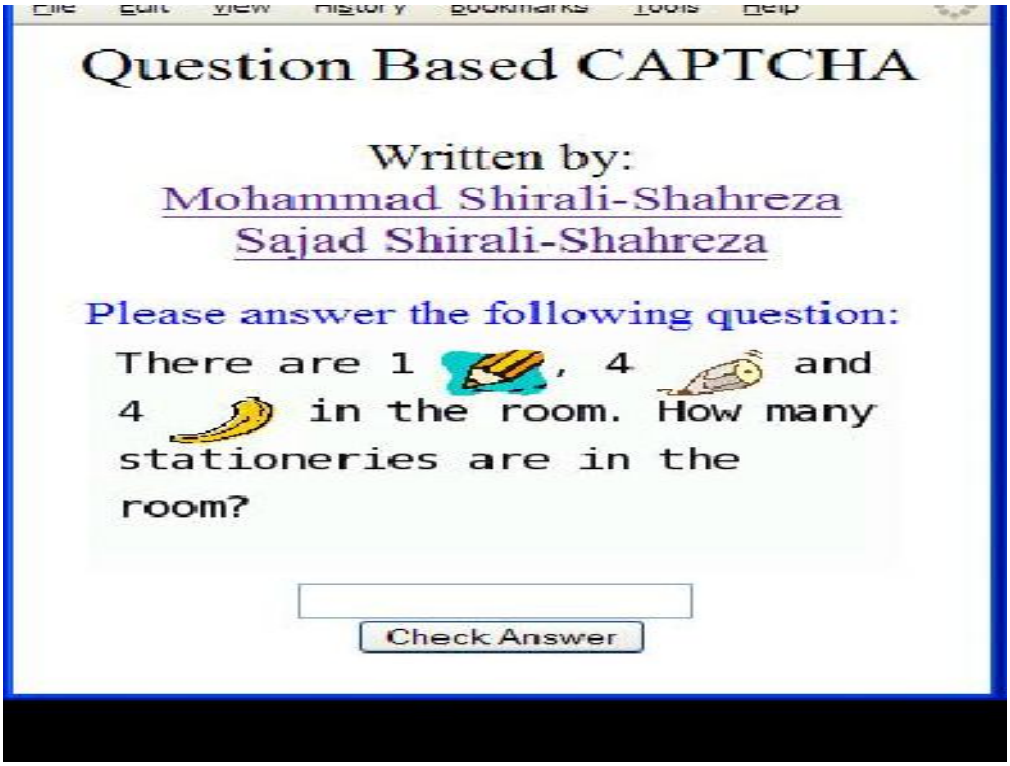

Figure 4 Question based CAPTCHA

Advantages of Question based CAPTCHA

1. Unlike OCR-based CAPTCHA methods, this technique requires only typing lots because answer. So it will be simple to operate, saves users some time and much more comfortable for him or her.
2. In this particular method it's not necessary to employ a keyboard and then we simply have to go into lots. Therefore we can utilize this method on devices which don't have a keyboard or on devices through which it is hard to employ a keyboard, such as mobiles and Pocket PCs.
3. Using this method doesn't need any processing to be filmed by client which enables it to be executed on small devices and also on devices with limited resources.[5]

Advanced Color based Image CAPTCHAs

The CAPTCHA types are generally text based or image based. Current Image-based CAPTCHAs facing problems of Computer-based recognition algorithms for extracting shape, special point features etc. In like manner overcome with this problem, images usually are distorted. But more distortions make images even for humans to recognize.

In this post, a new color based CAPTCHA is described, which provides color based images to human and human will answer withc color name or other sorts of question asked during turing test. In the following paragraphs the target were to make a database of different color images, then during turing test this software picks an colored image at random order, presents for the user with assorted questions like “What's color of the style”, “Enter final number of color”, “Enter middle color image”, “Enter colour of object in image”, “Enter background color”, “Enter color”, etc, now if user responds with correct answer. A few examples of developed color CAPTCHA is offered the following: Single color CAPTCHA, Multi color CAPTCHA. Colored image based CAPTCHA.

Single color CAPTCHA: In single color CAPTCHA the interrogator will ask the color of image, in reply user need to enter the correct color of CAPTCHA, for correct answer user will pass turing test.

Multi color CAPTCHA: In case of multicolour CAPTCHA the interrogator can ask different type of questions like how many colours are given in image? Enter name of color in middle. Enter name of maximum %age in image. Enter name of left side color. Enter name of right side color.

Figure 5 Multi-color CAPTCHA

Colored image based CAPTCHA: In image based CAPTCHA an image will be given and interrogator will ask the question on the basis of image like an image of car is given and the question is : Enter the color of car. Enter background color. Etc.

Figure 6 Colored image based CAPTCHA

It gives a combination of image and question based CAPTCHA and improves usability but issue with this are if user don't know the color of the image or type wrong spelling of color. This proposed and tested CAPTCHA technique offers some advantages which are easy to understand for all type of users, simple to use, security improved, user friendly, least complexity and user can solve this CAPTCHA within least amount of time because of its simplicity of problem or question. Coming from a security viewpoint, this new scientific studies are supposed to advance the creation of previous CAPTCHA techniques, because computer machine cannot solve the name of color but an individual may easily understand in regards to the name on the color and need for question asking during turing test. Security can be improved in future work using the concept of colors or multi colored layered CAPTCHA can be developed by increasing the number of colored layers which layers are changing their color after some fixed amount of time but before entering the answer of the question.[9]

Word Grouping CAPTCHA

The problem with current text based CAPTCHA (hottest CAPTCHA) schems is always that many of them are actually either not robust enough (an easy task to break them) or they are too complicated annoying to learn even for humans. Word grouping is a kind of CAPTCHA in which user has got to divide the given words by 50 % subgroups.

In word grouping CAPTCHA the user is presented with six words, and is asked to divide the group into two subsets, using any categorizing the user wishes. The words will be easier so that any user can do that.

Figure 7 Word group CAPTCHA

Advantage of Word Grouping CAPTCHA

No readability issue with word grouping CAPTCHA. Words are easily understandable, no confusion in recognising them. We can add large number of word group sets in our database. No problem with people having colour vision problem. User just needs to divide the words in two subgroups. It only requires text based interface. As it is new in comparison with existing CAPTCHA system so attacks are less vulnerable

A word grouping CAPTCHA was proposed which may face usability issue if user submit the CAPTCHA without selecting group for all six words or only selects few from the group.

Evolution parameters of different CAPTCHA

Consistency- It answers the following. When presented with the same CAPTCHA, how reproducible is a user's answer? The level of consistency will clearly vary across different Captcha, and the acceptable level will vary by application (some may be more lenient than others).

Entropy -By entropy, we mean do different people answer the same CAPTCHA in the same way?

Ease of generation-How difficult is it to generate a given CAPTCHA? Can it be generated given only randomness, or does it require a pre-computed or pre-generated corpus.

Implementation-Finally, how easy is it to implement? Does it require complex and elaborate graphics, or can it be implemented for a text-only system? How accessible is it?

Evaluation of different CAPTCHA

Text based CAPTCHA

Consistency- For Text based CAPTCHA Consistency is high. Entropy**-** Nearly everyone provide the same solutions for all of the Text based CAPTCHAs; there is essentially no variation. In some cases user may confused a z with an x and an 'o' with an 'a', but all of the other answers chances are same. Ease of generation– Text based CAPTCHAs are, by design, fairly easy to generate they simply require the text to be rendered and some randomness. Implementation- Implementation is easy in comparison with other image based or word grouping CAPTCHA.

Picture CAPTCHA

Consistency –Consistency is a useful one, if user can recognize the image correctly. Entropy- Entropy is a lot less than text based CAPTCHA, given it is dependent upon the products picture, difficulty higher level of picture and user's ability to recognize pictures. Image recognition is really a hard problem Easier generation-It utilizes a larger database of photographs and animated images of everyday object. Implementation -some implementations use only a little fixed pool of CAPTCHA images. Eventually, when enough image solutions have been collected by an assailant in a period of time, the test may be broken by researching solutions within a table based on a hash on the challenge image.

Word Grouping

Consistency-Word Grouping seems somewhat memorable without much practice. We suspect that this rate can be boosted with a tiny bit of practice.

Entropy- In principle, each word grouping has 2^6 possible outputs and we expect to see a large amount of variation. Ease of generation-Word Grouping has some of the limitations on its corpus, it cannot become too large or users will not recognize some of the words. Implementation**-** The implementation is straightforward, and has several desirable properties. The task is easy and the user interface is simple and accessible which means that it can work on screen readers or in a text-only environment like a login window. [6]

A more robust CAPTCHA

This article proposes a text-based CAPTCHA algorithm during which each challenge will be related to main features in order to enhance the CAPTCHA security. Different and extra features each and every challenge might be generated randomly. The randomness is utilized to scale back the danger of predicting the next challenge. A far more robust CAPTCHA was proposed in the following paragraphs with multiple secure features and very effective for breaking attack but simple to solve by user. It refers to replay attack as after each page refresh principle popular features of captcha can be changed as:

CAPTCHA's code can be a group of characters (uppercase and lowercase) and numbers. Multiple randomizing functions are used to generate a random code (stream of characters and numbers) in each challenge in order to make it not prone to a dictionary attack.

The duration of the code is varied (minimum length is 6 characters-numbers). Multiple font types are utilized to prevent intrusion using image processing techniques. String/codes are rotated at different angels. Lines are utilized to prevent segmentation. The numbers plus the amount of lines and their positions could be varied each and every time so that you can distort the text image randomly before being presented on the user. The written text image could possibly be blurred using some specific technique in order to make CAPTCHA a hardship on malicious software. Image dimensions could possibly be varied inconsistent considering the features above. Whenever CAPTCHA's code and line colour are saved in gray scale colours at different levels.

CAPTCHA is done by generating a picture from text in php using GD library. GD library is definitely an free code library containing been used in this work to the dynamic creation of images which can be customized a whole lot in different formats. The CAPTCHA image code is first created after which it the Html page is generated using the input fields for displaying CAPTCHA image lastly the proper code/string is submitted. The two files, first file sports ths form which provides the CAPTCHA image, and the other employed to generate the captcha image. If a user tries gain access to an internet site that's been protected using a Captcha to prevent abuse by automated programs, the user requests a secure form online server.

In order to avoid the dictionary attack, the proposed scheme generates a random string (code) created from of characters (uppercase/lowercase) and numbers through using steps: A string which include things like numbers from (0-9) and letters (uppercase and lowercase) from (a-z), could be shuffled randomly by using str_shuffle() php function. Part on the shuffled string might be returned using substr() php function. this portion is specified with the start and length parameters (the space parameter could possibly be equal to the code length value which generated previously randomly when using the rand function rand (6,12)). Thus the size of the code/string is done variable at each time. [7]

Two-Tier CAPTCHA

This short article introduces a fresh CAPTCHA scheme called Two-Tier CAPTCHA. First a alphanumeric CAPTCHA code with image is generated. Second Query associated with that CAPTCHA code. E.g. enter only Digits .Rate of the difficulty may be increase d as a way to improve its proof against the attacks with the help of a lot more query and combination in database. The algorithm of this scheme causes it to be hard for bot programs which signify it is more secure.

The advantage of using Two-Tier CAPTCHA will it be can solved by human users easily and challenging to solve by bots. This Two-Tier CAPTCHA methods use a same input method as used by lots of popular web sites and services where users type some keywords or characters into a port box.

A bot program required some capability to provide correct input for a few-Tier CAPTCHA.
1. Computer program must recognize alphanumeric code shown in image through OCR-based software.
2. After recognition of alphanumeric code from CAPTCHA image computer must be able to understand the query related that CAPTCHA.
3. At last and in some cases if computer does the many previously referred to steps successfully it's quite challenging to evaluate the precise input, that is required because the query generated randomly, there isn't a specific pattern between queries as well as in

some query we use another field of the web form, i.e. Please provide the value since you provide in User Name.

Good thing about Advance Two-Tier CAPTCHA
• Enhanced Security
• Convenient to use because user must provide input like OCR-based CAPTCHA.
• Prevent automated attacks
• Random combination are going to be generated, so difficult to spot the pattern.[8]

Hybrid Collage CAPTCHA

This paper introduces a fresh form of CAPTCHA called hybrid collage CAPTCHA. One of the CAPTCHA methods is Collage CAPTCHA. It's a way of distinction between human and computer programs through recognition and locating a picture of object among some objects. This article improves the resistance of Collage CAPTCHA method by an improved method called Hybrid Collage CAPTCHA. This scheme displays images on left and right side from the screen.. On right side screen we have now the related images in conjunction with different texts in distorted form. Now the pc program asks user to choose the picture with correct texts. If the user select correctly, then user is allowed to enter the text of the image inside given text box. If entered name is correct, then we guess that user is human.
The proposed scheme is based on following algorithm-
Step 1. Start
Step 2. Computer chooses goal image
Step 3. Computer generates six corresponding images
Step 4. Computer automatically generates names for images in CAPTCHA format
Step 5. Computer program ask the user to choose the correct image
Step 6. User selects the image
Step 7. Is selected image correct?
I. If yes, text box gets enabled and User enters the name i. Is entered name correct? a. If yes, user successfully
gets registered. b. If no, goto step 2.
II. If no, goto step 2.
Step 8. Stop.

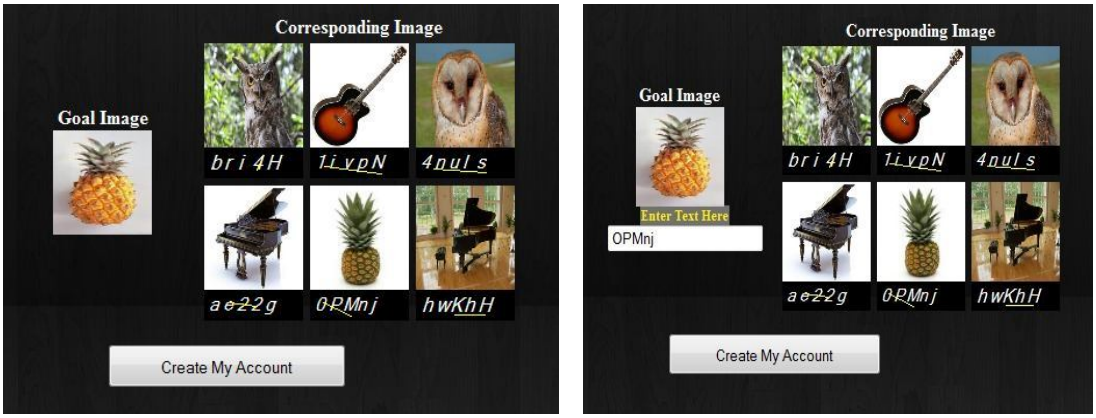

Figure 8 Hybrid Collage CAPTCHA

The improved method is designed to increase the resistance of Collage CAPTCHA Method. In this particular method computer requires four abilities to give quality:
I. To find out is very important in the concerned object.
II. To find the concerned object on screen.
III. To uncover the item containing the “selected object” on the screen.

IV. To go into the name of the image within the text box.

It is sometimes complicated for that computer to realize these tasks in correct order, merely a human user can recognize and opt for the concerned object.
Using this method can also be implemented on other devices like cellphone, PDA (Personal organiser), as well as the devices who have touch screens, because no keyboard is required in this method and as well you don't have to heavy processing. [10]

Methods to design robust CAPTCHA

CAPTCHA designers may use methods to design a robust CAPTCHA:
1. Allow it to become tough to separate the writing from the background by employing multiple colors for both foreground and background, leave no pattern that might help distinguish the foreground automatically, you need to include some foreground colors in to the background And or vice-versa.
2. Allow it to become difficult to segment each image by connecting characters together or add more cracks in each character.
3. Pass impossible to distinguish a character by counting its pixels by causing all characters have the same pixel count all the time. Or create a character have unique pixel counts in a variety of challenges (if your difference isn't sufficient, an approximation method could probably determine each character).
4.Random warping provides another good defence from the pixel count attack .by way of example, local warp can introduce "small ripples, waves, and elastic deformations across the pixels with the character" and global warp generates character-level, elastic deformations; both can make a character's pixel count less predictable [3].

Conclusion

This paper studies and analyses different CAPTCHA techniques and design principles. It also describes advantages and disadvantages of different CAPTCHA techniques. Based on these methods for more robust CAPTCHA were proposed for designers.

References

[1]. E. Bursztein, M. Martin, and J. Mitchell, "Text-based captcha strengths and weaknesses," in *Proceedings of the 18th ACM conference on Computer*

[2] G. Moy et al., "Distortion Estimation Techniques in Solving Visual CAPTCHAs," *Proc. IEEE Conf. Computer Vision and Pattern Recognition*, IEEE CS Press, 2004, pp. 23–28

[3]. Jeff Yen, Ahmad Salah, " CAPTCHA security-Case Study", IEEE CS, 2009

[4]. Pan Lei, and Zhou Yan, "Developing an Empirical Algorithm for Protecting Text-based CAPTCHAs against Segmentation Attacks", 12th IEEE International Conference on Trust Security and Privacy in Computing and Communications (TrustCom), pp. 636-643, July 2013.

[5]. Mohammad Shirali-Shahreza, Sajad Shirali-Shahreza, " Question Based CAPTCHA", IEEE International Conference on Computational Intelligence, 2007.

[6]. Dayanand , **"**WORD GROUPING CAPTCHA-A NOVEL APPROACH FOR SECURING WEB SERVICES" International Journal of Electrical, Electronics and Data Communication Volume-1, Issue-, July-2013.

[7]. Mumtaz M. Ali AL-Mukhtar and Rana Riad K. AL-Tai "A More Robust Text Based CAPTCHA For Security in Web Applications" IJETTCS vol.3 issue 2 march-april 2014

[8]. Poonam Yadav and Sujata "Security Issues in Cloud Computing Solution of DDOS and Introducing Two-Tier CAPTCHA", *IJCCSA Volume 3 no 3 june 2013*

[9]. Mandeep kumar ,Renu Dhir "Design and Comparison of Advanced Color based Image CAPTCHAs" IJCA(0975-8887) vol.61no.15 jan 2013

[10]. Divya Shanker, Prashant Gupta, Aditya Jaiswal "Hybrid Collage CAPTCHA" International Journal of Communication and Computer Technologies Volume 01 – No.31, Issue: 05 May 2013.

[11]. Sandeep Mahato; Varun Prakash Saxena; Raj Gaurav Mishra, Securing Web Services and Application using Captcha Security, HCTL Open International Journal of Technology Innovations and Research (IJTIR), Volume 14, April 2015, eISSN: 2321-1814, ISBN (Print): 978-1-62951-946-3.