A new CAPTCHA Authentication Mechanism based on Eight-panel Cartoon CAPTCHA and Clickspell

Chinnu. R
M. Tech. Research Scholar, Dept of CSE
KMEA Engineering College
Aluva, India
chinnuprasenan@gmail.com

Maria Joy
Assistant Professor, Dept of CSE
KMEA Engineering College
Aluva, India
mariajoy@kmeacollege.ac.in

A.Neela Madheswari
Associate Professor, Dept of CSE
KMEA Engineering College
Aluva, India
neela.madheswari@gmail.com

***Abstract*— CAPTCHA is a technique that is used to prevent automated programs from being able to acquire free e-mail or online service accounts. However, as many researchers have already reported, conventional CAPTCHA could be overcome by state-of-the-art malware since the capabilities of computers are approaching those of humans. Therefore, CAPTCHA should be based on even more advanced human-cognitive-processing abilities. In this paper, two level of CAPTCHA authentication is proposed. The first level is a Cartoon CAPTCHA , which ask the users to arrange an image into correct order by the process of Drag and Drop. The second level Clickspell, combined the features of text-based and image-based CAPTCHAs. Clickspell asks users to spell a randomly chosen word by clicking distorted letters for passing the test. Users can learn the definition(s) of the chosen word. Sound signature is added for right and wrong clicks. Also a background image is placed under the letters which add more security. In addition, Clickspell can add an advertisement image op-tionally. By this advertisement image, Clickspell improved the capability of resistance to the attack by malicious programs. The analysis shows that Clickspell is practical in the aspects of security and usability**

***Keywords*—Automated programs, Cartoon CAPTCHA, Clickspell, Human-cognitive, Malware, Sound Signature**

I. INTRODUCTION

Use of INTERNET has remarkably increased globally in the past 10-12 years and so the need of the security over it is important. With an increasing number of free services on the internet, we find a pronounced need to protect these services from abuse. Automated programs (often referred to as bots) have been designed to attack a variety of services. For example, attacks are common on free email providers to acquire accounts. Nefarious bots use these accounts to send spam emails, to post spam and advertisements on discussion boards, and to skew results of online polls.

If we are trying to sign up for a free email service offered by Gmail or Yahoo, first we have to pass a test, before the submission of our application because a single computer program can get thousands of free email accounts per second. It's not a hard test. For human, the test should be simple and straightforward. But for a computer, the test should be almost impossible to solve. This sort of test is a CAPTCHA. They are also known as a type of Human Interaction Proof (HIP). CAPTCHAs are basically software programs which act as a test to any user over internet that the person (user) is a human or another machine. This concept is used by all the big companies over internet Google, yahoo or facebook .We have probably seen CAPTCHA tests on lots of Web sites. The common kind of CAPTCHA used on most websites requires the users to enter the string of characters that appear in a distorted form on the screen. Users job is to type the correct series of letters into a form. If the letters match the ones in the distorted image, we pass the test and able to access the web resources.

CAPTCHAs are short for **C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part. The term "CAPTCHA" was coined in 2000 by Luis Von Ahnhttp://en.wikipedia.org/wiki/Luis_von_Ahn, Man uel Blum, Nicholas J. Hopper (all of Carnegie Mellon University), and John Langford .They are challenge-response tests to ensure that the users are indeed human. The purpose of a CAPTCHA is to block form submissions from spam bots – automated scripts that harvest email addresses from publicly available web forms.

CAPTCHAs are used because of the fact that it is difficult for the computers to extract the text from a distorted image, whereas it is relatively easy for a human to understand the text hidden behind the distortions. Therefore, the correct response to a CAPTCHA challenge is assumed to come from a human and the user is permitted into the website. The basic idea of CAPTCHAs is tell human and machine apart and also understand the vulnerabilities and its state of the art [5].

Everyone needs to create a test that can tell humans and computers apart, this is because of people trying to exploit weaknesses in the computers running the site. While these individuals probably make up a minority of all the people on the Internet, their actions can affect millions of users and Web sites. For example, a free e-mail service might find itself

bombarded by account requests from an automated program. That automated program could be part
of a larger attempt to send out spam mail to millions of people. The CAPTCHA test helps identify which users are real human beings and which ones are computer programs.

Spammers are constantly trying to build algorithms that read the distorted text correctly. So strong CAPTCHAs have to be designed and built so that the efforts of the
spammers are thwarted.

In this paper, we propose a "Two-level CAPTCHA authentication" for accessing web resources. First level is a Cartoon CAPTCHA, which ask users to arrange the image into correct order by the process of Drag and Drop. It mainly focuses on using the human ability to understand humor, which represents the ultimate in human cognitive processing abilities, and propose a new CAPTCHA that uses eight-panel cartoons.. Second level is Clickspell [7], which is based on spelling by requesting users to click on the mouse rather than press the keyboard. The main idea of Clickspell is randomly choosing a word from the dictionary and asking user to spell it by clicking the letter by letter in order. The letters of the chosen word are properly distorted and randomly located in the CAPTCHA image. A background image is placed under the letters. In addition, for educational purpose, a detailed definition of the chosen word will be given. Furthermore, Clickspell can easily add a commercial advertisement on it by adding a cover image (advertisement) on the CAPTCHA image. In this case, users have to click the letters via a moving mask as Due to the advertisement image and moving mask, it is harder to attack Clickspell by the malicious robots.

The rest of the paper is organized as follows: Section 2 deals with related works, section 3 deals with the motivation, section 4 gives the system model, section 5 gives a brief description about CAPTCHA. Section 6 presents our proposed system. Section 7 gives the mathematical model, followed by security and usability analysis in section 8., and section 9 introduces the results, and finally we conclude the paper in section 10.

II. RELATED WORKS

With the expansion of Internet, a great many daily activities are now done through Internet for convenience, including communication, education and e-commerce. As a matter of fact, web sites must ensure that the services are supplied to legitimate human users rather than bots to prevent service abuse. To thwart automated attacks, services often ask users to solve a puzzle before being given access to a service. These puzzles, first introduced by von Ahn et al. in 2003, Completely Automated Public Turing test to tell Computers and Humans Apart. CAPTCHAs are designed to be simple problems that can be quickly solved by humans, but are difficult for computers to solve. Using CAPTCHAs, services can distinguish legitimate users from computer bots while requiring minimal effort by the human user.

The image-based CAPTCHAs let users to use click operation to try to pass the test. And the most important character of text-based CAPTCHAs is easy to use, .i.e., enter the recognized vocabulary.

A CAPTCHA system must satisfied the following three characters:

(1) Human can recognize the contents and pass it easily.

(2) It is invoked to prevent robots to pass the system or to increase the processing cost through continuous attack.

(3) It should be generated easily and quickly.

Many researchers have recently pointed out security problems with conventional text recognition based-CAPTCHA [8] . Malicious automated programs that install a sophisticated Optical Character Reader (OCR) have been spreading and these have cracked conventional text recognition based-CAPTCHA . It has become difficult for automated programs to pass tests (read texts) by increasing distortion or noise. However, it has also become difficult for humans to read texts .Therefore we need to adopt even more advanced human cognitive processing abilities to enhance CAPTCHA to overcome this problem ie, a "Eight-panel cartoon CAPTCHA" [13] is proposed. The eight-panel cartoon CAPTCHA has an extremely high resistance to malware attacks, because it is considered nearly impossible for malware to reach a level where it can understand humor, regardless of how advanced the technology might be. Furthermore, because reading cartoons is fun and entertaining for humans, a eight-panel cartoon CAPTCHA will most likely be seen as an agreeable and enjoyable Turing Test that does not adversely affect convenience for users.

In 2009, Banday and Shah proposed an image-based CAPTCHA [9]. Their method composes several sub-images into a CAPTCHA image .Some of the sub-images are rotated by 180 degrees (flipped images) while some of them are non-flipped. Users were asked to click all of the non-flipped images for passing the test. Banday and Shah pointed out that their scheme offers the benefit of image-based CAPTCHAs, i.e., image flip CAPTCHA improve more security than text-based CAPTCHA. Also, it consume less Web page area (between 240×180 pixels and 480×360 pixels) than most image-based CAPTCHAs.

The MosaHIP (a Mosaic-based Human Interactive Proof) presented by Alessandro and Stefano [1] , aims to prevent massive automated access to web resources. MosaHIP produces a CAPTCHA image by composing real images and fake images. The real images present real objects, while the fake images are artificially produced from randomly cropped real images. There are two question-types in MosaHIP: concept-based and topmost. The concept-based question type asks users to drag a resource and drop on the designated real image, which is located in the CAPTCHA image. The topmost question type asks users to drop on the topmost one real image. In the image-based CAPTCHAs, MosaHIP is the first system to use the drag and drop operations for testing. Alessandro and Stefano's experimental results indicated that the pass rates of concept-based type and topmost type are 98% and 80% respectively. Furthermore, in order to prevent "Denial of Service" (DoS), MosaHIP uses a computationally

intense process on the clientside and resource metering technique.

III. MOTIVATION

The proliferation of the publicly available services on the Web is a boon for the community at large. But unfortunately it has invited new and novel abuses. Programs (bots and spiders) are being created to steal services and to conduct fraudulent transactions. Some examples:

- Free online accounts are being registered automatically many times and are being used to distribute stolen or copyrighted material.
- Recommendation systems are vulnerable to artificial inflation or deflation of rankings. For example, eBay, a famous auction website allows users to rate a product. Abusers can easily create bots that could increase or decrease the rating of a specific product, possibly changing people's perception towards the product.
- Spammers register themselves with free email accounts such as those provided by Gmail or Hotmail and use their bots to send unsolicited mails to other users of that email service.
- Online polls are attacked by bots and are susceptible to ballot stuffing. This gives unfair mileage to those that benefit from it.

In light of the above listed abuses and much more, a need was felt for a facility that checks users and allows access to services to only human users. It was in this direction that such a tool like CAPTCHA was created. Existing CAPTCHAs are easily vulnerable to automated attacks. So a better authentication mechanism is needed. For this, we proposed two level of CAPTCHA authentication.

IV. SYSTEM MODEL

For implementing the proposed work, JAVA with SDK version 1.7 is used. For simulation NetBeans IDE 7.1.2 is used. For analysis ImageJ tool is used.

V. CAPTCHA - A KEY TO WEB RESOURCES

A. Characteristics

A CAPTCHA is a means of automatically generating challenges which intends to:

- Provide a problem easy enough for all humans to solve.
- It is invoked to prevent robots to pass the system or to increase the processing cost (eg: time)

through continuous attacks.

- CAPTCHA should be automatically generated and graded.
- Test can be taken quickly and easily by human users
- Test will accept virtually all human users and reject software agents
- Test will resist automatic attack for many years despite the technology advances and prior knowledge of algorithms.

B. Need for CAPTCHA

We need CAPTCHA to prevent the following:

- Sabotage of online polls.
- Abusing free online accounts.
- Prevention to worms and Spams
- Protecting website registration
- Protecting Email addresses from scrapers.
- Preventing comment spam in Blogs.
- Preventing dictionary attack
- Free e-mail services
- Search engine bots etc

C. Types of CAPTCHA

1. Text-based CAPTCHA

Text-based CAPTCHA asks users to recognize the word that has been presented in a distortion form. This type of CAPTCHA is intuitive to users. In other words, it is easy to use without learning or training. Text-based CAPTCHA is most widely deployed in many famous websites, e,g: Yahoo, Hotmail, Gmail, YouTube, PayPal and so on. Text-based CAPTCHA is secure to defend automated program if properly designed, i.e., the distorted form of a word cannot be recognized by robots easily. However, if the word is misrepresentative, it is hard to recognize by humans.

Fig. 5.1 Text based CAPTCHA

2. Image-based CAPTCHA

In image-based CAPTCHAs, users have to identify the subject of an image. This type of CAPTCHA usually interacts with users by using a pointing device, e.g., mouse. In general, image-based CAPTCHAs require larger web page area, and need an image database maintained at the server [10] [2]. Asirra [6] in figure 5.2 asks users to identify photos of cats and dogs. Scene Tagging [11] is another type of image based CAPTCHA that composed of object images and background image .This composite image is scaled, distorted, warped, noise added, and so on. Users pass test when they choose or point to the right object image.

3. Audio-based CAPTCHA

Audio-based CAPTCHAs ask users to recognize the vocabulary that is heard from a speech. In general, an audio based CAPTCHA includes three parts: vocabulary, noise and audio production. To prevent robots from attacking easily, noises should be added into the speech. In addition, these noises should be created dynamically to increase the difficulty of recognition by robots. The audio-based CAPTCHA is an alternative for visually-impaired people.

Fig. 5.2 Asirra

.

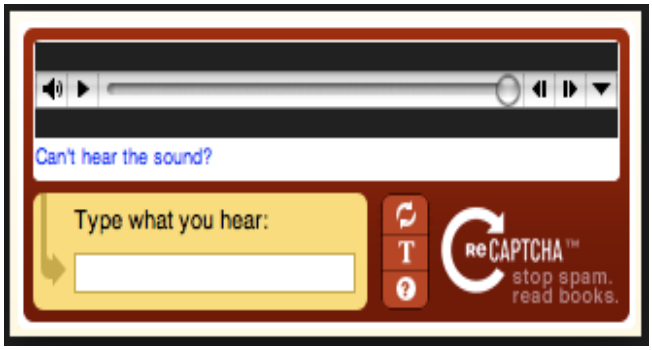

Fig. 5.3 Audio-based CAPTCHA

D. Issues of Existing CAPTCHAs

1. Text-based CAPTCHA

The main issues are the following:

- Distortion becomes a problem when it is done in a very haphazard way. Some characters like'd' can be confused for 'cl' or 'm' with 'r n'. It should also be easily understandable to those who are unfamiliar with the language.
- Content is an issue when the string length becomes too long or when the string is not a dictionary word.
- Presentation should be in such a way as to not confuse the users. The font and colour chosen should be user friendly.

The simplest CAPTCHA presents distorted or noise added text to users who visit various Web sites and want to use the services. If they can read the given text, they are certified as human. If they cannot read the text, they are certified to be malicious automated programs (bots). It has become difficult for automated programs to pass tests (read texts) by increasing distortion or noise. However, it has also become difficult for humans to read texts.

Fig. 5.4 CAPTCHA which is too noisy

2. Image based CAPTCHA

CAPTCHA uses many image processing procedures to defend itself against malicious robots' attacks. For examples, adding noise, scaling text, or rotating the image and so on. However, the processed results may not be recognized by human if the processed image is distorted too much. In otherwords, CAPTCHAs may not be recognized hardly by robots, but also difficult for people [4].

3. Audio-based CAPTCHA

Audio-based CAPTCHAs ask users to recognize the vocabulary that is heard from a speech. In general, an audio-based CAPTCHA includes three parts: vocabulary, noise and audio production. To prevent robots from attacking easily, noises should be added into the speech. In addition, these noises should be created dynamically to increase the difficulty of recognition by robots. If the amount of noise increases, it is difficult for human to identify the sound [3].

- Due to sound distortion, confusing characters can also occur in audio CAPTCHAs. For example 'p' and 'b'; 'g' and 'j', and 'a' and '8'.
- User should understand accent and pronunciation
- The use of color is not an issue for audio CAPTCHAs, but the integration with web pages is still a concern. For example, there is no standard graphical symbol for representing an audio CAPTCHA on a web page, although many schemes such as Microsoft use a speaker symbol.

E. CAPTCHA Circumvention

- Most text based CAPTCHAs have been broken by software like OCR, Segmentation, and by improving Character Recognition Software (OCR).
- Exploiting bugs in the implementation that allow the attacker to completely bypass the CAPTCHA.
- Using cheap human labor to process the tests (sweatshops).

Some text based CAPTCHAs have been broken by software which has 3 properties:

- Pre-Processing: Removal of background clutter and noise.
- Classification: Identifying the character in each region.
- Segmentation: Splitting the image into regions which each contain a single character.

VI. THE PROPOSED WORK

In our proposed system, two level of CAPTCHA authentication is performed.

A. Cartoon-based CAPTCHA

- It is a type of CAPTCHA based on arranging an image into correct order by the process of *Drag and Drop* [12]. An image is sliced into 4-pieces and shown to the user to rearrange it into a correct image, by dragging the piece-by-piece of image and drop it in correct place in the image.
- It mainly focuses on the user's ability to arrange an image, which represents the ultimate human cognitive processing abilities.

The authentication process used in this proposed method is as follows:

Step 1: A eight-panel cartoon with panels rearranged is displayed.

Step 2: The rearranged eight-panel cartoon is presented to the webpage visitor.

Step 3: The visitor rearranges the eight-panel cartoon into what appears to be the correct order. (The webpage could be equipped with a form allowing the visitor to input the correct order of panels.)

Step 4: If the order of the panels entered is correct, the visitor is identified as a human and entered into second level of authentication and if the order is incorrect, the visitor is identified as malware.

B. Clickspell

Clickspell combines the features of both text-based and image-based CAPTCHAs. The main idea of Clickspell is as follows:

- Randomly choosing a word from the dictionary and asking user to spell it by clicking the letter by letter in order.
- The letters of the chosen word are properly distorted and randomly located in the CAPTCHA image.
- A detailed definition of the chosen word will be given.
- A background image is placed under the letters.
- After each click, the letters will be displayed one by one.
- Separate sound will be produced for right and wrong click.
- Maximum 3 wrong clicks attempts are possible.

The CAPTCHA image of Clickspell can be divided into four parts: Banner area, explanation area, click area and advertisement area. Each part performs a particular function as follows.

• *Banner area*: Display a word randomly chosen from the dictionary. And this word is used for testing users. The users have to spell it by clicking the letter by letter for passing the test.

• *Explanation area*: Show the detailed definition of the chosen word in the designated language.

• *Click area*: All the letters of the testing word are properly distorted and randomly located in the click area. In the click area, a background image is placed under the letters. After each click, the letters will be displayed one by one. Two separate sounds are used for right and wrong clicks.

• Advertisement image: Click area can be covered an image and the covered image could be an advertisement ie, an advertisement image is placed on the top of click area and accompanying added a circle mask. Users can move the mask to finding the letters.

The detailed steps are explained as follows.

Step 1: Randomly chooses a word, W, from English dictionary (stored in a database). And place W on the banner area. Let $|W|$ denotes the number of letters of W.

Step 2: Set the click area of size $C_W \times C_H$ pixels. Produce the background image by drawing lines, dots, and polygons with random colors, transparencies and sizes. The number of the drawing objects depends on the size of $C_W \times C_H$. The larger size of $C_W \times C_H$, the number 4 of drawing objects must be increased.

Step 3: Set the letter of size $L_W \times L_H$ pixels. Each letter $L_i \in W$,for i =1,2,..., $|W|$, is properly distorted and randomly placed in the click area (above the background image). Note that in the click area, L_i cannot overlap with L_j, where $j \neq i, 1 \leq i, j \leq |W|$.

Step 4: Get the definitions and examples of W from the Google dictionary.

Step 5: If necessary, places the advertisement image of size $C_W \times C_H$ on the click area. When the advertisement image is placed, a circle mask is put on the advertisement image for looking for the letter Li ∈W. The center of circle mask is bound to the position of pointer device, e.g. Mouse. User can move the pointer device to look and click the letters for spelling the test word W. Each L_i can be assigned a different

size of $L_W \times L_H$. On Clickspell system, users will pass the test by spelling W correctly. While during the spelling process, the user may click a wrong letter. If the click errors greater than $E_{\max}$, the test is fail. For example, $E_{\max}$ =2 means that the test is failure when the third click error occurs.

The proposed system is composed of several modules. The following subsections explain each module.

1. Cartoon CAPTCHA implementation

- A type of CAPTCHA based on arranging an image into correct order by the process of Drag and Drop.

2. Image Query and Random word generation

- Image query module is for querying the image, which means giving the input to the system as an image.
- In random word generation, Click spell asks users to spell a randomly chosen word by clicking distorted letters for passing the test.

3. Definition and sound generation

- A detailed definition of the word is given.
- Users can learn the definition(s) of the chosen word.
- Also separate sound is produced for right and wrong click.
- After each click, the letters of the word will be displayed one by one.

4. Mask creation and Identification

- An advertisement image is placed on the top of click area and accompanying added a circle mask. Users can move the mask to finding the letters.
- Identification module is the checking module, whether the user correctly arranged the word or not.
- The user's work is to arrange the word using dictionary as an original word.
- After arranging, the system checks whether the arrangement is properly placed or not.
- If the words are correctly arranged, then the user is allowed for using the system or mail or folder. Otherwise, it is considered as the hackers or an automated.

VII. Security and Usability Analysis

A. Usability analysis

Usability is an important issue of CAPTCHA due to the variety in the backgrounds of users, such as disparity in age, culture, and language. Therefore, designing a CAPTCHA system has to consider two factors: visual perception and cognitive judgments. But how to examine the usability of CAPTCHA is an important issue. In 2003, Nielsen defined the usability by five quality components as follows :

• Learnability: How easy is it for users to accomplish basic tasks the first time they encounter the design?
• Efficiency: Once users have learned the design, how quickly can they perform tasks?
• Memorability: When users return to the design after a period of not using it, how easily can they re-establish proficiency?
• Errors: How many errors do users make, how severe are these errors, and how easily can they recover from the errors?
• Satisfaction: How pleasant is it to use the design?

In terms of the usability of CAPTCHA systems, Yan and Ahmad claimed the following three usability criteria: accuracy, response time, and perceived difficulty. Accuracy stands for "How accurately can a user pass a CAPTCHA challenge?".Response time stands for "How long does it take for a user to pass the test?". And perceived difficulty represents "How difficult to use do people perceive a CAPTCHA is?".

In our proposed work , usability analysis is performed by calculating average error rate and average pass rate using the following formula:

$$\text{Error rate} \quad : \quad \frac{N_e}{\sum |W|} \qquad (1)$$

Here N_e is the number of click error times and |W| is the total number of all letters. Probability of clicking wrong letters should be very low ie; distorted letters can be easily recognized by human.

Pass rates were measured by the number of failed tests divided by the total number of tests. The pass rates are higher than that of oppositions to click error rates. This is because only 3 wrong clicks are allowed during the spelling process; in other words, the test will fail when the more than 3wrong clicks occurs.

B. Security analysis

Here we use Canny edge detection algorithm and Adaptive thresholding, because Clickspell uses click operation to spell a word. If robots can separate the letters from the background, the locations of the letters will be appeared. To test whether or not the letters can be segmented from the background, the Canny edge detection
and adaptive thresholding methods are used.

Canny edge detection algorithm: An Edge is an area of significant change in the image intensity / contrast.Edge Detection is the process of locating areas with strong intensity contrasts. The main use of Edge Detection is extracting information about the image. E.g. location of objects present in the image, their shape, size, image sharpening and enhancement. The steps in Canny edge detector is given below:

1. Smooth the input image with a Gaussian filter.
2. Compute the gradient magnitude and angle.

- Edge strength is found out by taking the gradient of the image.
- A Roberts mask or a Sobel mask can be used.

$$|G| = \sqrt{G_x^2 + G_y^2} \approx |G_x| + |G_y| \qquad (2)$$

3. Apply non-maxima suppression to the gradient magnitude.
   - Trace along the edge direction and suppress any pixel value not considered to be an edge. Gives a thin line for edge.
4. Use double thresholding and connectivity analysis to detect and link edges.

Adaptive thresholding: Thresholding is used to segment an image by setting all pixels whose intensity values are above a threshold to a foreground value and all the remaining pixels to a background value. Adaptive thresholding typically takes a grayscale or color image as input and, in the simplest implementation, outputs a binary image representing the segmentation. For each pixel in the image, a threshold has to be calculated. If the pixel value is below the threshold it is set to the background value, otherwise it assumes the foreground value.

VIII. EXPERIMENTAL RESULTS

We analyse the proposed work to show that Clickspell is practical in the aspects of security and usability. Usability analysis is performed by calculating average error rate and average pass rate. Average error rate is calculated using the equation (1). Probability of clicking wrong letters should be very low ie; distorted letters can be easily recognized by human. Pass rates were measured by the number of failed tests divided by the total number of tests.

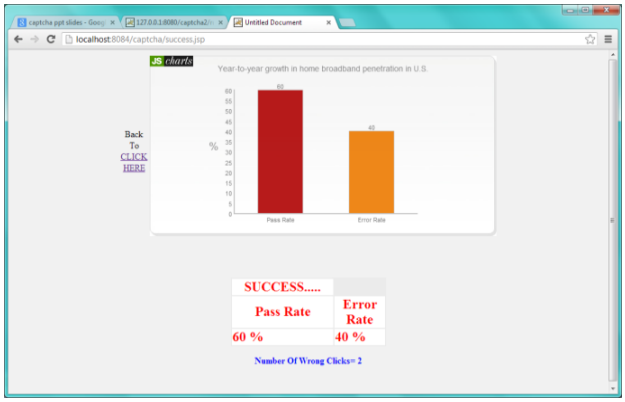

Fig. 9.1 Usability Analysis

The pass rates are higher than that of oppositions to click error rates. This is because:

- Only 3 wrong click are allowed during the spelling process; in other words, the test will fail when the more than 3 wrong clicks occurs.
- Separate sounds are given to wrong and right click.
- A detailed definition of the word is given in the explanation area. So error rate is low.

For Security analysis, we use Canny edge detection algorithm and Adaptive thresholding, because Clickspell uses click operation to spell a word. If robots can separate the letters from the background, the locations of the letters will be appeared. To test whether or not the letters can be segmented from the background, the Canny edge detection and adaptive thresholding methods are used. Here we compare Clickspell with a text-based CAPTCHA.

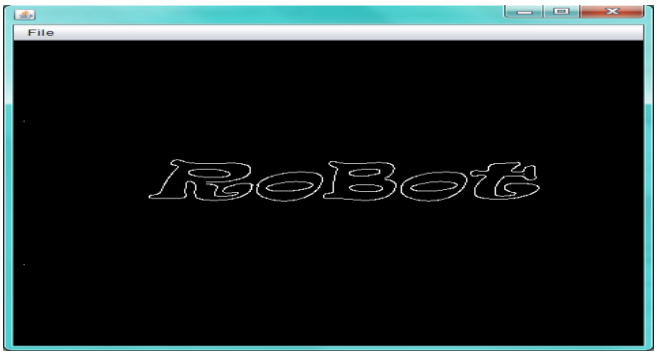

Fig. 9.2 Result of Canny edge detection- Text-based CAPTCHA

Automated programs can easily identify the letters in text based CAPTCHA.

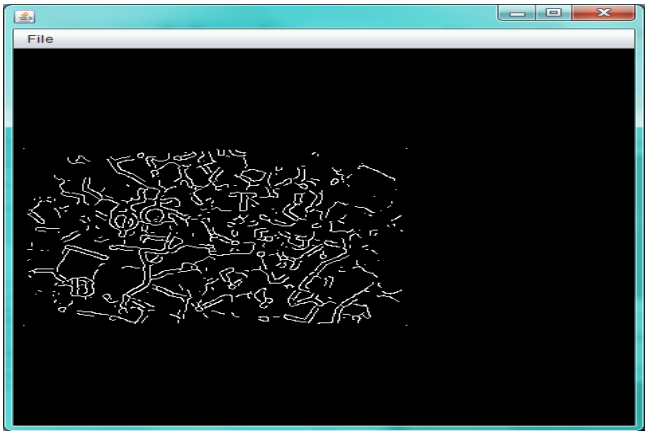

Fig. 9.3 Result of Canny edge detection - Clickspell

From the above figure it is clear that robots cannot easily separate the letters from the background image. Adding background image in Clickspell provide more security. So Clickspell offers more security compared to existing CAPTCHAs.

For adaptive thresholding, we use the tool *ImageJ*. From the result it is clear that it is impossible for the robots to identify the letters in Clickspell easily. The result is given below.

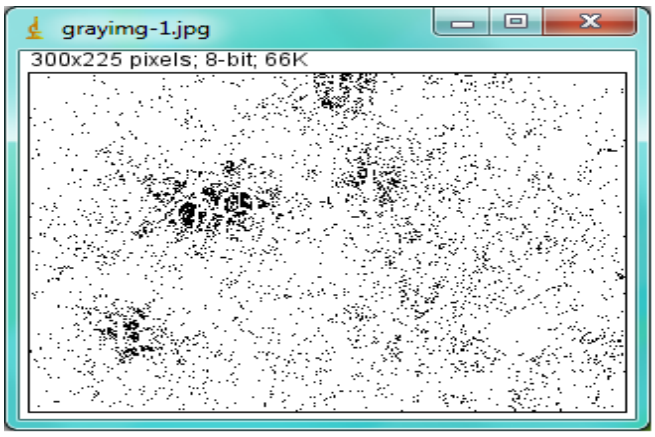

Fig. 9.4 Result of Adaptive thresholding

IX. CONCLUSION

To protect web resources from automated abuses, a two level authentication mechanism is proposed in this paper. First mechanism is a Cartoon CAPTCHA focus on the human cognitive processing abilities, and proposed a CAPTCHA that uses eight-panel cartoons. This method is expected to offer a new form of CAPTCHA that feature both security and usability, being difficult for advanced malware to decipher, and at the same time offering entertainment value for users,

who will enjoy reading the cartoons. Second authentication mechanism is Clickspell. To pass the Clickspell test, users have to spell a randomly chosen word by clicking on distorted letters. Clickspell derived the main feature of text-based CAPTCHA, i.e., easy to use. Furthermore, Clickspell retains the character of image-based CAPTCHA, i.e. recognize objects from an image. Clickspell provides the dictionary function for users to learn the definition(s) of the spelling words. Clickspell is practical when considering the aspects of security and usability. In particular, Clickspell is suitable for the devices which without a keyboard, e.g., smart phone, tablet PC and so on.

ACKNOWLEDGMENT

I am thankful to the management, the department of Computer Science and the department of Information Technology of KMEA Engineering College for their valuable support and guidance.

REFERENCES

[1] Alessandro Basso, Stefano Sicco," *Preventing massive automated access to web resources*", International journal on Computers and Security, Elsevier , vol. 28, pp.174-188,2008.

[2] Bin B. Zhu, Jeff Yan, Qiujie Li, Chao Yang, Jia Liu, Ning Xu, Meng Yi, Kaiwei Cai, "*Attacks and Design of Image Recognition CAPTCHAs*", CCS'10, October 4-8, Chicago, Illinois, USA,2010.

[3] Elie Bursztein,Romain Beauxis, Hristo Paskov, Daniele Perito Celine Fabry, John Mitchell," *The Failure of Noise-Based Non-Continuous Audio Captchas*", IEEE Symposium on Security and Privacy,2011.

[4] Gossweiler, M. Kamvar, and S. Baluja, "*What's up captcha?: a captcha based on image orientation*," In Proceedings of the 18th inter-national conference on World wide web, WWW '09, (New York, NY,USA), pp. 841–850, ACM, 2009.

[5] Guo, Feng," *The vulnerabilities and status of CAPTCHAs*", In Proceeding of the 3rd IEEE International Conference on Communication Software and Networks (ICCSN), 448-452 pages, 27-29 May 2011

[6] J. Elson, J. R. Douceur, J. Howell, and J. Saul, "*Asirra: a Captcha that exploits interest-aligned manual image categorization*," In Proceedings of 14th ACM Conference on Computer and Communications Security, pp. 366–374, 2007.

[7] Kuo-Feng Hwang, Cian-Cih Huang, Geeng-Neng You, "*A Spelling Based CAPTCHA System By Using Click*" , In Proceeding of the IEEE International conference on Biometrics and Security Technologies(ISBAST) , pages 1-8, 26-29 March 2012

[8] Ling-Zi, Xiao ." *A Case Study of Text-Based CAPTCHA Attack*", In Proceeding of the IEEE International Conference on CyberC ,121-124 pages 10-12 Oct. 2012

[9] M. T. Banday and N. A. Shah, "Image flip CAPTCHA," ISeCure, The ISC International Journal of Information Security, vol. 1, no. 2, pp. 105–123, 2009

[10] Monica Chew and J. D. Tygar, UC Berkeley ,"*Image Recognition CAPTCHAs*", In Proceedings of the 7th International Information Security Conference (ISC 2004), Springer, September 2004, pp. 268-279

[11] P. Matthews and C. C. Zou, "*Scene tagging: image-based captcha using image composition and object relationships*," in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ASIACCS '10, (New York, NY, USA), pp. 345–350, ACM,2010.

[12] Santhiya.J, Christobel Diana.S," *Drag and Drop Image CAPTCHA*", In proceeding of the International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012.

[13] Takumi Yamamoto,Tokuichiro Suzuki, Masakatsu Nishigaki*," A Proposal of Four-panel cartoon CAPTCHA: The Concept* In Proceeding of the 13th IEEE International Conference on Network-Based Information Systems, pages 575-578, 14-16 September 2010.

AUTHORS PROFILE

Chinnu .R received her B.Tech. during 2011 in Information Technology from SHM Engineering college Kadakkal, Kerala University. She is pursuing her M.Tech. in Computer Science and Engineering from KMEA Engineering College, MG University, India. Her research interests are network security and cryptography.

Maria Joy recieved her B.Tech. during 2008 in Computer Science and Engineering from Cochin University of Science and Technology and her M.Tech. during 2011 in Computer Science with specialization in Data Security from Cochin University of Science and Technology . She is currently

a Assistant Professor of Computer Science and Engineering at KMEA Engineering College, MG University, India. Her research interest is in security.

A. Neela Madheswari recieved her B.E. during 2000 and her M.E. during 2006 in Computer Science and Engineering. She is pursuing her Ph.D. in computer science and Engineering from Anna university, Chennai, India. Her research interests are in parallel computing and web technologies.