Use of Human Cognition in HIP Design via EmotIcons to Defend BOT Attacks

Mir Tafseer Nayeem
Department of Computer Science and Information Technology (CIT)
Islamic University of Technology (IUT)
Board Bazar, Gazipur-1704, Bangladesh
e-mail: mtnayeem@yahoo.com

Md. Saddam Hossain Mukta
Department of Computer Science and Information Technology (CIT)
Islamic University of Technology (IUT)
Board Bazar, Gazipur-1704, Bangladesh
e-mail: mukta944@gmail.com

Samsuddin Ahmed
CSE Discipline,
Chittagong University(CU),
Chittagong, Bangladesh.
e-mail: sambd86@gmail.com

Md. Mahbubur Rahman
Department of Computer Science and Engineering (CSE)
Bangladesh University of Engineering and Technology(BUET),Dhaka,Bangladesh.
e-mail: mahbub_cse89@yahoo.com

Abstract— **Many services in the internet including Email, search engine, social networking are provided with free of charge due to enormous growth of web users. With the expansion of web services, denial of service (DoS) attacks by malicious automated programs (e.g. web bots) is becoming a serious problem of web service accounts. In order to avoid tremendous attack from malicious computer programs, HIP, or Human Interactive Proofs has been introduced to distinguish humans from computers. HIPs are designed to be easy for humans but hard for machines. Unfortunately, the existing HIPs tried to maximize the difficulty for automated programs to pass tests by increasing distortion or noise. Consequently, it has also become difficult for potential users too. In our proposed technique we resolve this problem by making use of human cognitive processing abilities through emoticons focusing mainly on users. Features like language independence, using this for advertising purpose, ease of use interface for the touch-based smart-phone users, easy tuning of security and usability level make it very attractive to web service providers. In the result section, a microscopic large-scale user study was conducted involving 118 users to investigate the actual user views compare to existing state of the art CAPTCHA systems like ESP-PIX and Asirra in terms of usability and security and found our system can be solved with 88.04% average success rate in less than 7 seconds.**

Keywords- CAPTCHA; HIPs; Usability ;Security; OCR; Web Services; Cognitive Psychology; EmotIcons.

I. INTRODUCTION

A CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) or HIP (Human Interactive Proof) is an automatic security mechanism used to determine whether the user is a human or a malicious computer program .It is a program that generates and grades tests that are human solvable, but intends to be beyond the capabilities of current computer programs [1]. It has become the most widely used standard security technology to prevent automated computer program attacks. With the expansion of Web services, denial of service (DoS) attacks by malicious automated programs (e.g., bots) are becoming a serious problem as masses of Web service accounts are being illicitly obtained, bulk spam e-mails are being sent, and mass spam blogs (splogs) are being created. Thus, the Turing test is becoming a necessary technique to discriminate humans from malicious automated programs [1].

In the original Turing Test, a human judge was allowed to ask a series of questions to two players, one of which was a computer and the other a human. Both players pretended to be human, and the judge had to distinguish between them [2]. CAPTCHAs are similar to Turing Test in that they distinguish humans from computers, but they differ in that the judge is now a computer.

The CAPTCHA is usually a simple visual test or puzzle that a human can complete without much difficulty, but an automated program cannot understand. The test usually consists of letters, numbers or their combination with overlapping and intersection. A typical example of a text-based CAPTCHA challenge is shown in Figure 1. The CAPTCHA images may be distorted in some way or shown against an intricate background to keep them from being easily read by Optical Character Recognition (OCR) software) or other image recognition systems.

Currently, in order to defend malicious programs from issuing advertisements or other useless information recklessly, message boards of BBS, blog and wiki have widely used CAPTCHA challenges as a defense mechanism [1],requiring that users must input the correct letters to leave a message. CAPTCHs have a wide variety of applications on the web such as:

1. Offer a plausible solution against email worms and spams.
2. Protect Web pages from being crawled by search engines.
3. Pinkas and Sander [3] have suggested using CAPTCHAs to prevent dictionary attacks in password systems.
4. Collecting valid online polls where voters should show they are human before being allowed to vote.
5. CAPTCHA also plays a significant role in limiting usage rate. For example, the automatic use of a particular service is allowed unless such use goes beyond a certain extent and affects other users.
6. Several companies (Google, Yahoo!, Microsoft, etc.) offer free email services. Unfortunately "Web bots" which is a script capable of registering for thousands of email accounts every minute, wasting precious web space. This situation has been improved by requiring users to prove they are human before they can get a free email account.

Moreover, some spammers have found a creative way to provide their bots with CAPTCHA solving capabilities using pornographic sites, outsource the CAPTCHA-solving task to humans. For example, when a bot is faced

978-0-7695-4914-9/12 $26.00 © 2012 IEEE
DOI 10.1109/ICCSE.2012.33

with a CAPTCHA, it might place that CAPTCHA onto the entrance page of a pornographic site [12], and the next visitor to that site solves the CAPTCHA for the bot, in exchange for (free or price-reduced) entrance to the porn site[12]. In this paper we will try to defend this relay attack using the notion drag and place that require instant interactions of only human.

Researches on CAPTCHA mechanism have gained significant attention recently. Researchers encourage images, audio and video as a possible alternative to text-based CAPTCHA [22, 5, 6, 7]. Unfortunately, the existing CAPTCHA techniques tried to maximize the difficulty for automated programs to pass tests by increasing distortion or noise. Consequently, it has also become difficult for humans too. A recent study which investigated user's perceptions towards CAPTCHA challenges and also highlights the necessity for user friendly CAPTCHA challenges [8]. Results have shown that even experienced users face difficulties in solving a CAPTCHA challenge [8] need few tries or solving time is more than 18 seconds.

In this context, the work presented in this paper constitutes an effort towards focusing mainly on user's cognitive styles and performance related to CAPTCHA challenges within Web-based environments.Various research attempts have been reported [10, 11] that investigate the effect of cognitive styles of users on preference and performance issues in Web-based environments. We tried to balance the readability and security by making use of human cognitive processing abilities through emoticons. Other features like language independence, option for advertising , ease of use interface for the touch-based smart-phone users, easy tuning of security and usability level make it very attractive to web service providers and administrators.

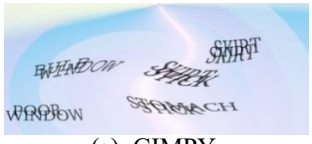
II. VARIOUS TYPES OF CAPTCHA METHODS

CAPTCHA methods, especially text-based, have been widely use as the main defense mechanism against bots on the web. Recently, with the advancements in computer vision technology, text-based systems have become vulnerable to bot attacks with a high success rate [13, 14, 15, 17, 18]. Hence a lot of work has proposed alternate CAPTCHA systems such as image-based [19, 20, 21, 24, 25, 26] , audio & video based systems [41, 28, 29, 30].

A. Text-Based CAPTCHAs:

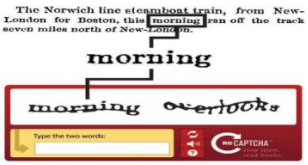
In this system computer generates a sequence of letters or digits after distorting them with a certain amount of noise render them on to the screen. The user is asked to identify the characters in order to pass the test. GIMPY [31] is a very reliable text CAPTCHA built by CMU in collaboration with Yahoo to protect chat rooms from spammers who were posting classified ads and writing scripts to generate free e-mail addresses (shown in Fig. 1(a)). Ez–Gimpy [14] is a simplified version of the Gimpy CAPTCHA, adopted by Yahoo in their signup page (shown in Fig. 1(b)). reCAPTHCA [35] is a free CAPTCHA service that helps to digitize books, newspapers and old time radio shows. More specifically, each word that cannot be read correctly by OCR is placed on an image and used as a CAPTCHA (in Fig. 1(c)). Microsoft's CAPTCHA [34] is used for services including Hotmail, MSN and Windows Live as shown in Fig. 1(d) .

Google CAPTCHA [36] is shown when URLs are added to Google and a new Gmail account is signed up (in Fig. 1(e)). Baffle Text [33] is Xerox PARC's version of the Gimpy test .This doesn't contain dictionary words, but it picks up random alphabets to create a nonsense but pronounceable distorted text to defeat dictionary attacks (in Fig. 1(f)). This technique overcomes the drawback of Gimpy CAPTCHA because, Gimpy uses dictionary words and hence, clever bots could be designed to check the dictionary for the matching word by brute-force.

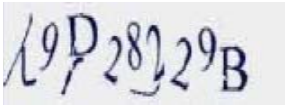


(a) GIMPY

(b) Ez–Gimpy



(c) reCAPTHCA



(d) Microsoft's CAPTCHA

(e) Google CAPTCHA

(f) Baffle Text

Fig. 1. Examples of text-based CAPTCHAs

Attacks on text-based systems mostly make use of OCR (optical character recognition) algorithms. These algorithms first segment the images into small blocks containing only one letter, and use pattern recognition algorithms to classify the letters in each block [13, 14, 15]. In counter-attack to these segmentation algorithms, text-based CAPTCHA systems employ the following techniques to increase robustness [37, 17]:

1. Adding more noises in the form of scattered lines and dots to the background.
2. Characters are connected, overlapped or twisted to increase difficulty in character recognition.

However, all the above techniques make the task harder for humans too. Connecting characters together creates ambiguous characters such as "vv" can be similar to "w", "cl" can be similar to "d", "nn" can be "m", "rn" can be "m" "rm" can be "nn" where users cannot be sure what they are. Moreover hard to tell distorted O from 0, 6 from G and b, 5 from S/s, 2 from Z/z, 1 from l. In case of dictionary words non-English users get into trouble with predicting.

Scheme	No of Choices	English Dependency	Probability of entering a Bot	Average Solving Time(in seconds)	Interaction
Move & Select	4	Yes	1/40	6.02	Mouse
ESP-PIX	72	Yes	1/72	13	Mouse
Asirra	12	no	1/12	17	Mouse
MMC	4	yes	1/4	8	Mouse & Keyboard

TABLE I: Summarization of the image based CAPTCHAs

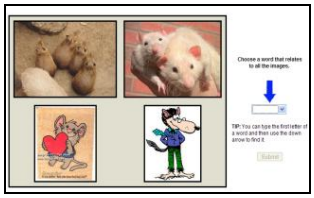
B. *Image-Based CAPTCHAs:*

In this, user is required to identify image. The advantage of image based CAPTCHA over text based is that pattern recognition is a hard AI Problem and therefore it is difficult to break this test using pattern recognition technique. The users of this CAPTCHA usually interact 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. ESP-PIX[20] is a Captcha script that instead of asking you to type letters requires that you look at a set of pictures and then select the word that best describes all the images(in Fig. 2(a)). It is available in English therefore end user must have a comprehensive English vocabulary. There are only 27% people in the world are English speaking [6].

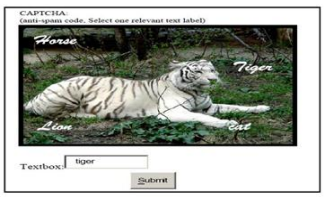
Asirra [19] a CAPTCHA that asks users to identify cats out of a set of 12 photographs of both cats and dogs provided by Petfinder.com are shown in Fig. 2(c). A typical Asirra challenge requires more screen space than a traditional text-based CAPTCHA. Moreover, Asirra is not accessible to those with visual impairments.

Multi Model CAPTCHA uses text and image based system together where end user is shown an image where four text labels associated with it. Text labels are attached in the image and the user is asked to select an appropriate text label [4]. A snapshot of Multi Model CAPTCHA is shown in Fig. 2(b).

Move & Select [16] it's a 2 layer CAPTCHA, desired to improve security and reduce the solving time of human. In the proposed solution, we try to make use of human cognitive processing abilities into our CAPTCHA design (in Fig. 2(d)). It is not suitable for visually impaired users. Also it may be challenging for users with learning disabilities. Table I summarizes all the image based CAPTCHAs discussed above.

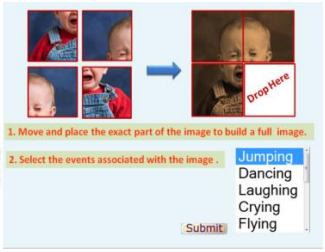


(a)ESP-PIX



(b) Multi Model CAPTCHA

(c) Asirra CAPTCHA



(d) Move & Select

Fig. 2. Examples of image-based CAPTCHAs

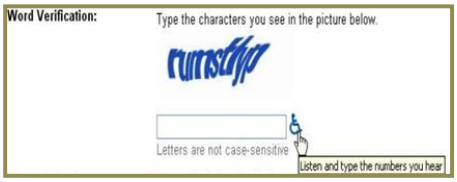
C. *Audio-Based CAPTCHAs:*

The program [41] picks a word or a sequence of numbers at random, renders the word or the numbers into a downloadable audio file and background noises are added to the sound clip using TTS software to make the test more robust against bots. These systems are highly dependent on the audio hardware and need to install essential software like Adobe Flash on their computers. These barriers lead to spend user's time more than standard response time which is typically about 5-15 seconds [40]. Because of high level of distortion characters produce similar sound like "d "and "b" [39]. These English words are unfamiliar to non-English humans. It helps visually disabled users but the worst case is for people who have problem in both hearing and vision. Fig. 3(b) below is the Google's audio enabled CAPTCHA.

D. *Video-Based CAPTCHAs:*

The final This is the newer CAPTCHA using animation or video in which a user must provide three words (tags) describing a video are shown in Fig. 3(a). According to some studies [38] [5], this approach may provide greater security (i.e., hard to be broken by computer programs) and better usability than text-based and image-based CAPTCHAs. YouTube which currently stores and indexes close to 150 million videos used as a video dataset in[27].However, video is also more complex and need more time and bandwidth to answer the challenge than other schemes.

(a) Video-based CAPTCHA



(b) Audio-based CAPTCHA

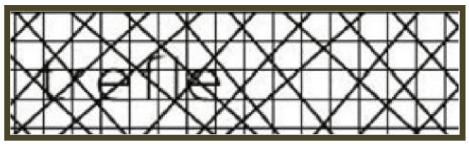
Fig. 3. Audio & Video based CAPTCHA

III. MOTIVATION

There are two major issues involved in designing a strong CAPTCHA test:

1. *Robustness* (difficult to break)
2. *Usability* (human friendly)

In the system *robustness*, the characters must be more distorted, so that the malicious computer software (e.g., a robot program) could not recognize them. *Usability* is concerned with making CAPTCHA tests easy to learn, use, understand and interpret for users. It has become difficult for automated programs to pass tests by increasing distortion or noise. Consequently, it has also become difficult for humans too example given in Fig. 4(a). That is not a good design obviously. On the contrary, if the design is quite easy to be identified by the user, then the computer may also be able to easily identify and solve it as illustrated in Fig. 4(b). We therefore need to adopt even more advanced human cognitive processing abilities to enhance CAPTCHA to overcome this problem.



(a) Better robustness but lack of usability

(b) Better usability but lack of robustness

Fig. 4. Usability vs. Robustness

Few more points about present state of the CAPTCHA's:

1. The findings of [8] indicate that users are already having a great difficulty in solving CAPTCHA challenges. There is a significant association between age and number of tries, since adults participants are more likely to solve CAPTCHA at first try considering themselves quite familiar with blogs and forums while teenager ones need two or more tries.
2. Non-native speakers of English were slower, though they were generally just as accurate unless the captcha required recognition of English words. So we will try to make our captcha language independent.
3. Users of CAPTCHA tests from touch based systems or smart-phones facing frequent problems where typing is more difficult.
4. Moreover, another limitation of traditional image-based approaches is it lacks customization of security levels depending on the nature and popularity of the website.

In our proposed solution we have considered all these factors in our design .This emoticon CAPTCHA solving ability comes naturally to humans as humans automatically employ their cognitive ability and commonsense .The same test for a bot would require both understanding the scenario image and selecting accurate emoticon, constituting a hard AI problem.

IV. THE PROPOSED CAPTCHA TEST

In this paper, the proposed method has been developed to distinguish human users and computer programs from each other by the fact that human user have special cognitive processing abilities on the other hand it is nearly impossible for OCR programs to have that and it falls into hard AI problem.

In designing a new CAPTCHA, the basic principles that we have taken care are:

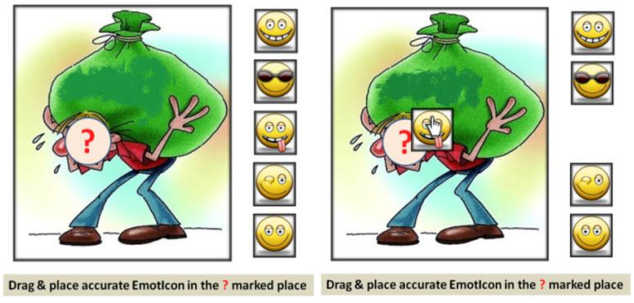
1. Easy for most people to solve.
2. Difficult for automated bots to solve.
3. Easy to generate and evaluate.
4. Users do not feel bored.

Cognitive Psychology is the study of human perception, attention, memory and knowledge, and the ways in which these have been applied in the design of computer interfaces. Cognitive psychology [32] relates the use computer systems:

1. How humans perceive the world around them (e.g. Web Pages).
2. How they store and process information and solve Problems (e.g. CAPTCHA tests).
3. How they physically manipulate objects (e.g. clicking a link, button, drag and place an object etc).

We know that there is a tradeoff between readability and security in solving CAPTCHA challenges. If we want to make the system more secure from the automated bots by adding more distortion and noise then the readability will be hampered for the users too. In our propose technique instead of increasing distortion or noise we will make use of human cognitive processing abilities into our CAPTCHA design through emoticons. This emoticon CAPTCHA solving ability comes naturally to humans as humans automatically employ their cognitive ability and commonsense.

The proposed CAPTCHA test based on human cognitive psychology through emoticons is shown in Fig. 5(a) where users need to drag the exact emoticon (from the set of emoticons given as a choice at the right side) associated with the scenario and place it onto the described position to pass the test . Though a lot of work has been done in the area of machine vision, recognition of emotion is still a tough task for machines and thus falls into a hard AI problem. On the other hand human user can do it very easily with special cognitive processing abilities. Moreover, computers cannot perform mouse actions such as drag and place as normal human does , this makes it an ideal choice for touch-based systems and smart-phones where typing is more difficult. A successful interaction is depicted in Fig. 5(b).



(a) CAPTCHA test (*main*) (b) CAPTCHA test (*in action*)

Fig. 5. Proposed emoticons CAPTCHA

V. USER STUDIES AND RESULTS

A large-scale user study was conducted to investigate the actual user views related to perceptions, cognition, and user preferences related to CAPTCHA systems with real usage scenario. An invitation was announced on the web site of the University and on social networking sites, by sending invitation to known email addresses in order to recruit participants for the survey. The aim of this selection process was to recruit a representative sample of participants of varying profiles, intended to increase internal validity of the survey by involving expert, average and novice users with respect to CAPTCHA challenges. For this purpose, we first built a website which would present the users with sample challenges.

In our experiment, we presented users first with as survey asking the following information:

1. Age
2. Native language (one from the Wikipedia list) (If native language is not English) Years studying English
3. Gender
4. Education (one of: no formal education, high school, bachelor's degree, master's degree, PhD)
5. Country of birth
6. Country of residence
7. Familiarity with computers (e.g. Internet, forum, blogs, and social networks)
8. Years using the internet
9. Frequency of internet use (e.g. daily, weekly, monthly or yearly)
10. Using internet from devices (e.g. Desktop , Laptop , Mobile phone , Smart phones etc)

A. *Demographics of Participants*

A total of 118 people participated so far of age between 14 and 66 in the study between April and June 2012. 26 of them completed half of the test, due to internet disconnection or had double answers and were omitted from the test sample. The final sample included 92 valid participants which mean that they does not have any kind of vision problem that hampered their effort to identify colors, shapes, or patterns. The distribution in age groups is depicted in Table II.

	Gender		Age Ranges			
	Male	Female	14-19	20-32	33-49	50-66
N	66	26	18	39	26	09
%	71.7	28.3	19.6	42.4	28.2	9.8

Table II: Demographics of the sample

B. *User Study Layout*

The participants were asked to visit a Web-page in order to take part in the study.

1. An initial questionnaire asking the users to enter the information explained above (e.g. Age, Gender, Years using the internet, Frequency of internet use etc.)
2. Then one challenge from each of the EmotIcon, ESP-PIX and Asirra CAPTCHA.
3. A final short questionnaire asking users to rate each CAPTCHA in terms of ease of use.

The study took an average of 5.3 minutes to complete for each participant.

C. *Usability Study*

Quoted from Jakob Nielsen [22], usability is defined by the following five quality components:

- *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?
- *Accuracy:* how successfully can a user pass a challenge? and how easily can they recover from the errors?
- *Satisfaction:* How pleasant is it to use the design?

Typically, the basic task that a CAPTCHA imposes to users is intuitive, easy to understand and easy to remember. Thus, CAPTCHA has a relatively good memorability. Therefore, in this paper, we will only consider the other four quality components.

a) *Average solving time*

As shown in Table III, users completed Emoticon CAPTCHA challenges faster than that of Asirra and ESP-PIX CAPTCHA. Each user takes an average of 4 seconds more to complete Asirra compare to Emoticon and ESP-PIX CAPTCHA.

Average solving time in Emoticon CAPTCHA is about 6.91 seconds from the distribution plots shown in Fig 6(c) .On the other hand solving time is comparatively higher for ESP-PIX CAPTCHA with most of the users taking around 6.93 seconds and for Asirra CAPTCHA is 10.78 seconds (in Fig 5(b), 5(a)) So proposed system has better efficiency compare to others.

	CAPTCHA test		
	EmotIcons	**ESP-PIX**	**Asirra**
Average solving time (in seconds)	6.9134	6.9375	10.7751

Table III: Average Time taken per challenge for each of the systems (*in seconds*)

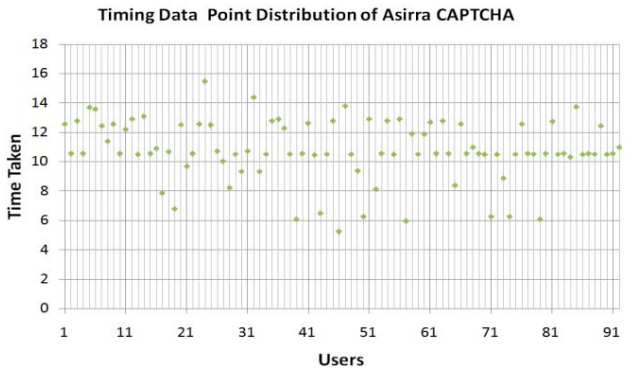
b) *Accuracy*

Accuracy or the success rate is defined how successfully a participant can pass a CAPTCHA challenge .The total number of correct attempts of Emoticon CAPTCHA (e.g. 88.04%) is higher than ESP-PIX CAPTCHA (e.g. 78.26%) as shown in Table IV, which clearly indicates that users are able to solve more challenges of Emoticon CAPTCHA correctly which signifies the proposed CAPTCHA has a higher accuracy or success rate.

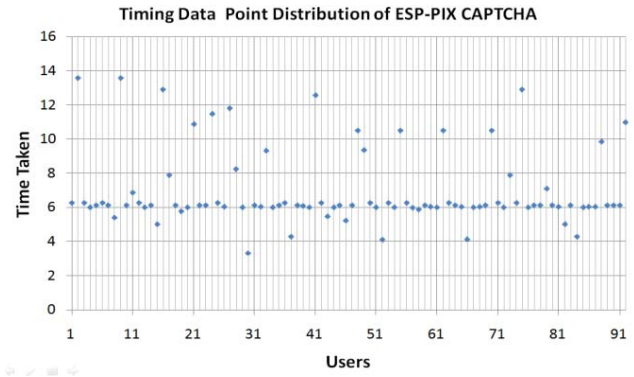
We notice that the success rate of Emoticon CAPTCHA (e.g. 88.04%) is very close to Asirra (e.g. 92.39%). This is actually surprising. We expected that solving a Emoticon CAPTCHA challenge will be much harder than solving a Asirra challenge because image-based CAPTCHAs have been widely deployed for a long time and users are quite familiar whereas users were experiencing our system for the very first time. This clearly suggests that our proposed design is pretty learnable.

CAPTCHA Tests	**Outcome**		**Average Success Time (*in seconds*)**
	Success	***Failure***	
EmotIcons	81/92 ≈88.04%	11/92 ≈11.96%	636/81 ≈ 7.85s
ESP-PIX	72/92 ≈78.26%	15/92 ≈21.74%	638/72 ≈ 8.86s
Asirra	85/92 ≈92.39%	7/92 ≈7.61%	991/85≈11.69 s

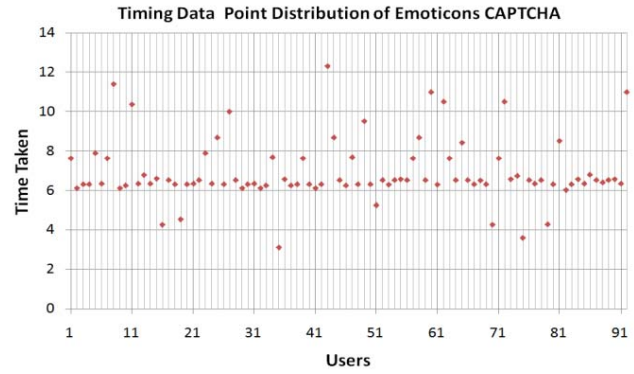
Table IV: Overview of the user result data



(a) Asirra CAPTCHA



(b) ESP-PIX CAPTCHA



(c) Emoticons CAPTCHA

Fig. 6.Timing Distribution of each system for all users (*in seconds*)

c) *Ease of use*

After the completion of the test users are asked to answer a question as presented below.

Which CAPTCHA is enjoyable to you?

A. ESP PIX
B. Asirra
C. EmotIcons
D. none of above

In the above poll we have collected 78 valid responses out of 92 users. After analyzing the valid responses we found that about 68% (≈53/78) of the responses are for C (EmotIcons CAPTCHA).So this scheme has better satisfaction because of its ease of use interface specially designed for mobile devices.

So we conclude that users subjectively satisfied and they will be willing to use such a scheme in future. So we have validated all the 5 usability goals defined by Jakob Nielsen with respect to our design. So our system successfully passed the usability test.

D. Security Study

EmotIcons CAPTCHA is more secure compare to other existing schemes because emotion detection is very difficult for computer bots. Moreover, drag and place require the instant interaction of human user to defend against relay attack. However, bots may try for a Brute force attack or random guess attack.

In our CAPTCHA scheme, the security mainly depends on 2 things and all these configurations are set in the server side and users are unaware of all this things.

Firstly, difficulty level depends on the no of emoticons given in the choice. This has been done to eliminate the requirement of keyboard in the CAPTCHA test.

Secondly, The dimension of the grids. Each time, the main scenario image is divided into N X M grid, so there are total $N * M$ blocks which size is nearly equal to each emoticons given in the choice. In Fig. 7. main image is divided into 5 X 4 grid that means 20 square blocks.

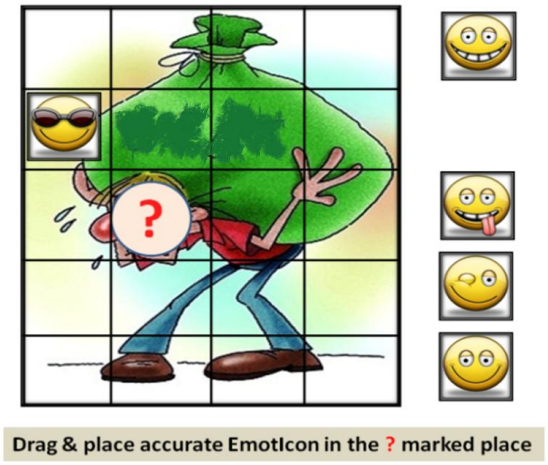


Fig. 7.A BOT trying to break Emoticon CAPTCHA using random guess attack

Brute force attack, trying to randomly guess the correct answer, is the most common attack. For our scheme, the probabilities of attacking varies with the value of N , M & l

Where, $N * M$=no of blocks we divide our scenario image (in the server side).

l=no of emoticons given in the choice.

Probability of an automated BOT entering into a site is $1/number\ of\ choices$ thus the probability of a single random guess is $C = \frac{1}{(N*M*l)}$. TABLE V, shows the result for three different conditions. The design of a emoticon CAPTCHA allows administrators to easy tuning of the security level depending on the nature and popularity of the website. However, increasing difficulty may also increase the response time and eventually decrease the success rate of novice potential users.

Dimensions N X M	No of pieces $(N * M)$	l =no of emoticons	Number of choices$(N * M * l)$	Probability C
5 X 4	20	5	100	0.01
6 X 5	30	6	180	0.005
8 X 8	64	7	448	0.002

TABLE V: Different difficulty levels of EmotIcons CAPTCHA.

I. CONCLUSION AND FUTURE WORKS

In this paper, we design a HIP named emoticon CAPTCHA to balance the readability and security of the CAPTCHA challenge design. By adding distortion and noise we restrict BOTs to break the test, but it eventually also difficult to humans to solve. We overcame this tradeoff by making use of human cognitive processing abilities into our CAPTCHA design through emoticons. We have validated our test through microscopic large-scale user study and find that our test is capable of being deployed in the internet in terms of security and usability. It also allows administrators to easy tuning of the security level and can use the scenario image for advertising purposes. Language independent and ease of use interface provides a great deal of satisfaction to the touch-based smart-phone users where typing is more difficult. These features make it very attractive to web service providers. Moreover, the proposed approach is not suitable for visually impaired users and it may be challenging for users with learning disabilities. Furthermore, generating a large database is always difficult for image based tests. So, our future work will undergo with creating a large database automatically, and then it will be more secure.

REFERENCES

[1] L. von Ahn, M. Blum, and J. Langford, "Telling humans and computers apart automatically," Communications of the ACM, vol. 47, no. 2, pp. 57-60, February 2004.

[2] M. Blum, L. A. von Ahn, and J. Langford, "The CAPTCHA Project, Completely Automatic Public Turing Test to Tell Computers and Humans Apart," Nov. 2000, http://www.captcha.net, Dept. of Computer Science, Carnegie-Mellon Univ.

[3] A. Turing. Computing machinery and intelligence. Mind, 49:433–460, 1950.

[4] Almazayd, A.S. Ahmed , Y Kouchay, "Multi Modal CAPTCHA: A User Verification Scheme". Presented at Int Conf n Information Science and Application, Korea, 2011

[5] Kluever, K.A., and Zanibbi, R. Balancing Usability and Security in a Video CAPTCHA. In Proc. SOUPS 2009, ACM Press (2009), Article 14, 11 pages.

[6] English Language taken from wikipedia and available at http://www.en.wikipedia.com/English_Language.

[7] Golle, P. Machine Learning Attacks Against the Asirra CAPTCHA. In Proc. CCS 2008, ACM Press (2008), 535-542.

[8] Fidas, C., Voyiatzis, A., and Avouris, N. On the Necessity of User-friendly CAPTCHA. In Proc. CHI 2011, ACM Press (2011), 2623-2626.

[9] Riding, R.J., and Cheema, I. Cognitive styles - An Overview and Integration. Educational Psychology 11, 3/4 (1991), 193-215.

[10] Brusilovsky, P., Kobsa, A., and Nejdl, W. The Adaptive Web: Methods and Strategies of Web Personalization. Springer, Berlin, Heidelberg, 2007.

[11] Brown, E., Brailsford, T., Fisher, T., Moore, A., and Ashman, H. Reappraising Cognitive Styles in Adaptive Web Applications. In Proc. WWW 2006, ACM Press (2006), 327-335.

[12] Van Oorschot, P. C. and Stubblebine, S. 2006. On Countering Online Dictionary Attacks with Login Histories and Humans-in-the –loop. ACM Transaction on Information and System Security. 9.3.August 2006:235-258.

[13] J. Yan and A. S. El Ahmad. A low-cost attack on a microsoft captcha. In Proceedings of the 15th ACM conference on Computer and communications security, CCS '08, pages 543–554, New York, NY, USA, 2008. ACM.

[14] G. Mori and J. Malik. Recognizing objects in adversarial clutter—breaking a visual captcha. In Proceedings of the Conference on Computer Vision and Pattern Recognition, 2003

[15] K. Chellapilla and P. Simard. Using machine learning to break visual human interaction proofs (hips). In In Advances in Neural Information Processing Systems, pages 265–272, 2005.

[16] Moin Mahmud Tanvee, Mir Tafseer Nayeem, Md. Mahmudul Hasan Rafee " Move & Select: 2-Layer CAPTCHA Based on Cognitive Psychology for Securing Web Services", International Journal of Video & Image Processing and Network Security IJVIPNS / IJENS vol. 11, issue 5 ,October,2011

[17] A. S. El Ahmad, J. Yan, and L. Marshall. The robustness of a new captcha. In Proceedings of the Third European Workshop on System Security, EUROSEC '10, pages 36–41, New York, NY, USA, 2010.ACM.

[18] E. Bursztein, S. Bethard, C. Fabry, D. Jurafsky, and J. C. Mitchell. How good are humans at solving captchas? a large scale evaluation. In Proceedings of 2010 IEEE Symposium on Security and Privacy(Oakland'10), 2010

[19] J. Elson, J. R. Doucerur, J. Howell, and J. Saul. Asirra: A Captcha that exploits interest aligned manual image categorization. In Proceedings of the 14th ACM conference on Computer and communications security, CCS '07, pages 366–374, New York, NY, USA, 2007. ACM.

[20] Esp-pix. http://server251.theory.cs.cmu.edu/cgi-bin/esp-pix/esp-pix.

[21] M. Chew and J. D. Tygar. Image recognition captchas. In Proceedings of the 7th International Information Security Conference (ISC), pages 268–279, 2004.

[22] Jakob Nielsen. Usability 101: Introduction to Usability, 2003. Available at http://www.useit.com/alertbox/20030825.html.

[23] R. Datta, J. Li, and J. Z.Wang. Imagination: a robust image-based captcha generation system. In Proceedings of the 13th annual ACM international conference on Multimedia, MULTIMEDIA '05, pages 331–334, New York, NY, USA, 2005. ACM

[24] Sq-pix. http://server251.theory.cs.cmu.edu/cgi-bin/sq-pix.

[25] 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, pages 345–350, NewYork, NY, USA, 2010. ACM

[26] B. B. Zhu, J. Yan, Q. Li, C. Yang, J. Liu, N. Xu, M. Yi, and K. Cai. Attacks and design of image recognition captchas. In Proceedings of the 17th ACM conference on Computer and communications security, CCS '10, pages 187–200, New York, NY, USA, 2010. ACM

[27] M. Cha, H. Kwak, P. Rodriguez, Y.-Y. Ahn, and S. Moon. ITube, You Tube, Everybody Tubes: Analyzing the World'sLargest User Generated Content Video System. In Proc. IMC2007, ACM Press (2007), 1–14.

[28] J. P. Bigham and A. C. Cavender. Evaluating existing audio captchas and an interface optimized for non-visual use. international conference on Human factors in computing systems, CHI '09, pages 1829–1838, New York, NY, USA, 2009.ACM.

[29] Audio and visual captcha. http://www.nswardh.com/shout/.

[30] H. Gao, H. Liu, D. Yao, X. Liu, and U. Aickelin. An audio captcha to distinguish humans from computers. In Proceedings of the 2010 Third International Symposium on Electronic Commerce and Security, ISECS '10, pages 265–269, Washington, DC, USA, 2010. IEEE Computer Society.

[31] School of Computer Science. (2009, Dec.). Gimpy. Carnegie Mellon. [Online]. Available: http://www.captcha.net/captchas/gimpy/.

[32] http://en.wikipedia.org/wiki/Cognitive_psychology

[33] M. Chew and H.S. Baird, "BaffleText, a Human Interaction Proof", In Proceedings of the 10th SPIE/IS&T Document Recognition and Retrieval Conference (DRR'03), Santa Clara, CA, USA, 2003, pp. 305-316.

[34] Hotmail, https://signup.live.com/signup.aspx.

[35] http://recaptcha.net/

[36] Google Accounts, https://www.google.com/accounts/NewAccount.

[37] K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski. Designing human friendly human interaction proofs (hips). In Proceedings of the SIGCHI conference on Human factors in computing systems, CHI'05, pages 711–720, New York, NY, USA, 2005. ACM.

[38] Cui, J.-S., Mei, J.-T., Wang, X., Zhang, D., Zhang, W.-Z.: A CAPTCHA Implementation Based on 3D Animation. In: International Conference on Multimedia Information Networking and Security, MINES, vol. 2, pp. 179–182 (2009)

[39] Jeff Yan, Ahmad Salah El Ahamd. " Usability OF CAPTCHAs Or usability issues in CAPTCHA design"

[40] http://captcha-bypass.com/

[41] T.Y Chan. "Using a Text-to-Speech Synthesizer to Generate a Reverse Turing Test", In Proceedings of the 15th IEEE International Conference on Tools with Artificial Intelligence, Sacramento, CA, USA, 2003, pp. 226-232.