An Image-Based CAPTCHA Scheme Exploiting Human Appearance Characteristics

Sajida Kalsoom[1], Sheikh Ziauddin[1] and Abdul Rehman Abbasi[2]
[1] Department of Computer Science,
COMSATS Institute of Information Technology,
Park Road, Islamabad, Pakistan
[e-mail: {sajida.kalsoom, sheikh.ziauddin}@comsats.edu.pk]
[2] Design Engineering Laboratory
KARACHI Institute of Power Engineering (KINPOE)
Paradise Point, Karachi, Pakistan
[e-mail: qurman2000@gmail.com]
*Corresponding author: Sajida Kalsoom

Received October 26, 2011; revised January 9, 2012; accepted February 4, 2012; published February 28, 2012

Abstract

CAPTCHAs are automated tests that are there to avoid misuse of computing and information resources by bots. Typical text-based CAPTCHAs are proven to be vulnerable against malicious automated programs. In this paper, we present an image-based CAPTCHA scheme using easily identifiable human appearance characteristics that overcomes the weaknesses of current text-based schemes. We propose and evaluate two applications for our scheme involving 25 participants. Both applications use same characteristics but different classes against those characteristics. Application 1 is optimized for security while application 2 is optimized for usability. Experimental evaluation shows promising results having 83% human success rate with Application 2 as compared to 62% with Application 1.

Keywords: Human Interactive Proof, CAPTCHA, usability, security, human appearance characteristics

DOI: 10.3837/tiis.2012.02.017

1. Introduction

Human Interactive Proofs (HIPs) are used to differentiate between the human users and automated programs by requiring some kind of interaction from a user which is difficult for a program to imitate. CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a class of HIPs which involve challenge-response tests that are there to verify that response is from human and not machine. The process involves a computer program that generates and grades a test, and a user that submits the response (i.e. solves the test). If the response is correct, the user is classified as human. The main purpose of CAPTCHA is to prevent web services from automated scripting-based attacks. There are many practical applications of CAPTCHAs including preventing computer scripts from: voting in online polls, creation of email accounts, posting messages in discussion forums, and misuse of online shopping and online games to name a few.

A typical text-based CAPTCHA scheme consists of a query asking the user to read and type a randomly-generated character and/or numeric sequence. If the user correctly inputs the characters and/or numerals, he or she passes the test and authorized as human user, otherwise access is denied. However, such schemes are highly vulnerable to known attacks such as *optical character recognition* (OCR) based attacks, dictionary attacks and segmentation attacks. An alternative to the above-mentioned scheme is an image-based CAPTCHA scheme which is not vulnerable to such attacks. In this paper, we propose and evaluate an image-based CAPTCHA scheme using easily identifiable human appearance characteristics.

In our proposed method, the challenge consists of a randomly selected image from the database and the user is asked to associate characteristics to the displayed image from an available list of characteristics. To pass the test, the user has to associate all (five in our case) characteristics correctly. We test the proposed method with two applications to evaluate usability, compared to security feature and report our results in terms of their strengths and weaknesses.

The rest of the paper is organized as follows. In Section 2, we review the related work. In Section 3, we describe the proposed method. Next, we provide an experimental evaluation in Section 4. Security of the scheme is analyzed in Section 5. Some limitations and their potential solutions are discussed in Section 6 and finally we conclude the paper in Section 7.

2. Related Work

The first known practical CAPTCHA was the one designed by Broder (though they did not use the term CAPTCHA in their work) to prevent automatic URL submission in Alta Vista search queries [1]. Their CAPTCHA consisted of an image of text which is easy to read by average humans but is difficult to read by OCR software. The first use of the term CAPTCHA is due to Blum, Ahn, and Langford at Carnegie-Mellon University team [2] who developed the Gimpy CAPTCHA to prevent unauthorized advertising in Yahoo's online chat rooms. The challenge consists of multiple words containing different kind of distortions and clutters making it difficult for OCRs to read the text. A Gimpy challenge consists of 10 words and the user has to recognize 3 out of these 10 words to pass the test. Yahoo later on started using a simpler version of Gimpy named EZ-Gimpy. In EZ-Gimpy, the challenge is a single distorted word

and the user has to type that word correctly. **Fig. 1** and **Fig. 2** show sample Gimpy and EZ-Gimpy challenges, respectively.

Currently there exist a number of CAPTCHA schemes that can be categorized as text-based, speech/audio-based, image-based and video-based. Each one has its own merits and demerits. In the continued section, we review the literature for a number of such schemes with a focus on image-based CAPTCHAs. Pessimal print [3] is a text-based CAPTCHA scheme. The challenge consists of a low quality text-image that is readable by human but difficult for machine to read. They have selected medium length words (five to eight characters) to prevent template matching and feature-based attacks (as shorter words are good candidates for template matching attacks and longer words are more vulnerable to feature based attacks). A word is randomly selected from a list then typeface and image-degradation parameters are randomly selected from a list independently. They used Baird degradation model [4] to degrade the words. Results show that the words were human readable but OCR software was unable to read any of the words. Chew and Baird [5] proposed a text-based CAPTCHA named BaffleText based on human's Gestalt perception abilities. They used pronounceable non-dictionary words to prevent dictionary attacks and image-masking degradation to defend image restoration attack. Their experimental evaluation shows a human success rate of 79%.

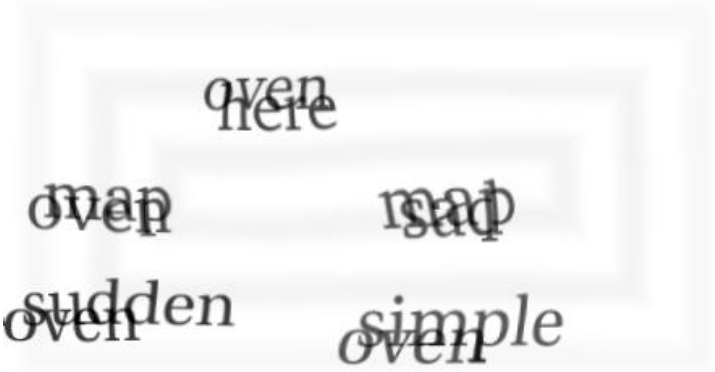

Fig. 1. A sample Gimpy challenge (Courtesy Greg Mori [6]). The challenge contains 10 distorted words. The user has to identify any 3 words correctly to pass the challenge.

Fig. 2. A sample EZ-Gimpy challenge presented to the user while creating a new Yahoo email account. The user has to type all characters correctly to pass the challenge.

A text-based CAPTCHA named ScatterType [7] was presented in 2005 to withstand segmentation attacks. In ScatterType, the text-images are pseudo-randomly generated which are fragmented using horizontal and vertical cuts and scattered using horizontal and vertical displacements. The text strings are English-like but non-dictionary words to resist lexical attacks. A user study is conducted with 57 users who submitted 4275 inputs. The experiment

was conducted at different levels of difficulty. Results show human pass rate of 7.7% for most difficult level and 81.3% for easiest level with an average success rate of 53%.

Most of the conventional text-based CAPTCHAs are vulnerable to known attacks, e.g., dictionary attacks, OCR attacks, segmentation attacks, etc. A number of text-based CAPTCHAs have been broken using AI attacks [8][9][10][11]. Additionally, text-based CAPTCHAs suffer from universality problem, i.e., they are language dependent. To overcome these problems researchers have presented image-based solutions. Rui and Liu [12] proposed a CAPTCHA scheme named ARTiFACIAL which is based on detecting human face and features. The user is presented with embedded faces in cluttered background. He or she has to identify a complete face and then click its six points: two for mouth corners and four for eye corners. They used 3 face detectors and one facial features detector to check resistance of their system against automated attacks. Both type of detectors showed a low success rate. The scheme was evaluated from 34 human users. Though human success rate was very high but some of the users were not comfortable with challenges as conscious effort was required to pass the tests.

Baird and Bentley [13] proposed a family of image-based implicit CAPTCHAs. In their work, the challenge is an image along with an instruction for the user to click on the mentioned position (e.g. click on the mountain top). The major problem with such tests is that they cannot be created automatically and need human effort to design them. Datta et al. [14] proposed a system named IMAGINATION for image-based CAPTCHAs generation. Their CAPTCHA is a double-round click and annotation process where the user has to click four times in all. The user is given a composite image formed by eight images and he or she has to click near the geometric center of the image which he or she wants to annotate. If the click is valid, i.e., it is near one of the centers, an image is presented to the user with a list of word choices after applying controlled annotation on that list. Now the user has to select the appropriate word from the list for the given image. The process is repeated one more time and completing both rounds correctly means challenge is passed.

Wen-Hung Liao [15] proposed another image-based CAPTCHA. An image is presented to the user with two non-overlapping blocks of the image exchanged with each other. In order to pass the challenge, the user has to click on the exchanged region. Asirra was presented by Elson et al. [16]. The challenge consists of images of cats and dogs, selected randomly from the database that is manually tagged and updated, and the user has to identify all images of cats in the displayed set. Gossweiler et al. [17] presented an image rotation based CAPTCHA. Different orientations of the same image are presented to the user and the user has to identify the image's upright orientation. The success rate is 84% when tested with three images. Kim et al. [18] proposed a CAPTCHA scheme which is an improvement of Gossweiler et al.'s idea. Instead of rotating whole image, different sub-images are selected and rotated. The user has to find the correct orientation for those sub-images in order to pass the test.

In addition to text-based and image-based CAPTCHAs, a few schemes have been designed for the visually impaired users. Holman et al. [19] proposed a CAPTCHA which includes both audio and visual data. The user is provided with the image of an object and its sound. To pass the challenge, user has to associate appropriate word with the given image/sound from the provided list of words. The CAPTCHA is suitable for users having either visual or hearing disability because a combination of audio and video data is given to the user. A prototype was evaluated from both blind and normal users and feedback from both groups was encouraging. A potential limitation is the limited number of easily identifiable image and sound combinations.

3. Proposed Scheme

As mentioned earlier, a CAPTCHA is a challenge-response game in which a challenge is given by the system and the response is provided by a human user. The challenge in our proposed CAPTCHA scheme is a human image along with a list of values (classes) for five relatively easily identifiable human appearance characteristics. The user response is to associate correct values with those characteristics for the given image.

3.1 Participants of the Study

We conducted a study for usability testing of the proposed image-based CAPTCHA scheme. Twenty five undergraduate university students participated in our study. We had two applications with same characteristics but different classes against those characteristics. Testing started with a 5-7 minutes demo to make users familiar with the system. Then users were called one by one to test the system. For each application, each user was asked to take the CAPTCHA test 5 times, i.e., submit 5 inputs for each application.

3.2 Our Scheme

We present an image-based CAPTCHA scheme using human appearance characteristics. Human face images are collected from widely used search engine Google and other publicly available databases. We label the images manually. The human characteristics we used are: *gender*, *hair type, hair color, ethnicity,* and *(facial) expression*. These characteristics are chosen since we feel that these are conveniently identifiable. Each characteristic is classified into two or more classes, e.g., gender has two classes: male and female while expression has 6 classes: anger, disgust, fear, joy, sad and surprise.

The working of the proposed scheme is as under. An image is given to the user along with a list of above-mentioned characteristics and corresponding classes. The user is asked to associate characteristics values to the image from the given list. If the user associates all characteristics correctly, he or she is considered a human; otherwise the user is considered a machine. Formally, our CAPTCHA challenge can be described as follows. Let I be the image shown to the user in a particular CAPTCHA challenge, let C_{mi} be the value of *i*th characteristic of I as assigned manually in the database (we call this *manually assigned class*), let C_{ui} be the value of *i*th characteristic of I as assigned by the user responding to CAPTCHA challenge (we call this *user assigned class*), then we say that a CAPTCHA challenge is passed iff $C_{mi} = C_{ui}$ for all i (in our scheme i={1,2,3,4,5})

We tested our scheme for two applications detailed below.

3.2.1 Application 1

This is first of the two applications which we designed for usability testing of our proposed image-based CAPTCHA. We use the following human appearance characteristics that are classified into the classes shown in the parentheses.

1. *Gender* (Male, Female)
2. *Hair type* (Long, Short)
3. *Hair color* (Black, Brown/Golden/Blonde, White/Grey)
4. *Ethnicity* (White/Caucasian, Black/African, Asian)
5. *Expression* (Anger, Disgust, Fear, Joy, Sad, Surprise)

This application works as follows: The user is presented with an image, randomly selected by the system from the database, and the user is asked to associate corresponding characteristics from a list for that image. **Fig. 3** displays our CAPTCHA as shown to the user.

If the user submits all correct values for the given challenge, the test is considered passed. If any of the user assigned classes do not match with the corresponding manually assigned classes, the test is considered failed and the user is asked to retry. For each new attempt, a fresh challenge is displayed to the user. The number of retries can either be unlimited or restricted depending on the type of application and the desired security level.

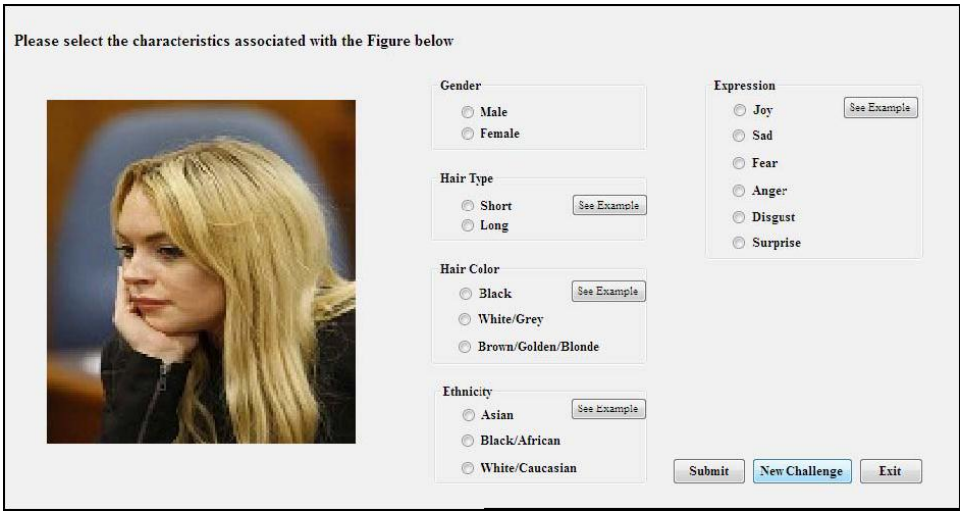

Fig. 3. An example of the proposed CAPTCHA challenge (Application 1)

The user is also provided with a "See Example" option as seen in **Fig. 4**. This option provides sample images for different classes against a given characteristic. These sample images may be helpful to the users in making their decisions, if they are in doubt about any particular characteristic. **Fig. 4** shows the sample images for short and long hair when help is requested for the characteristic "Hair Type".

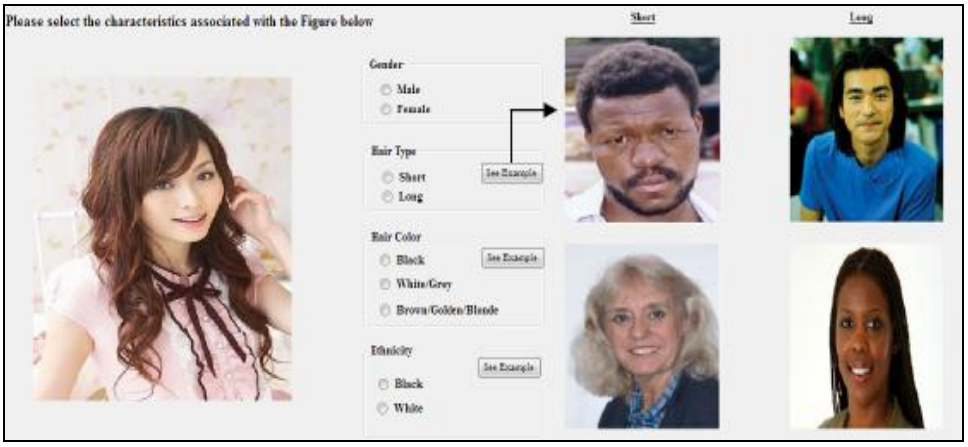

Fig. 4. Sample images for hair type using "See Example" help

A user can also request a fresh challenge if he or she feels that the current challenge is not

convenient to solve. After the user submits a challenge, he or she is informed about acceptance if all associated classes are correct and rejection otherwise.

3.2.2 Application 2

In many applications, usability is a major requirement and some of the security may be compromised to achieve desired levels of usability. For such type of scenarios, we implement our scheme for the selected human characteristics with reduced classes in ethnicity and expression. The new set of classes is as under.

1. *Gender* (Male, Female)
2. *Hair type* (Long, Short)
3. *Hair color* (Black, Brown/Golden/Blonde, White/Grey)
4. *Ethnicity* (Black/African, White/Caucasian)
5. *Expression* (Happy, Not Happy)

In application 2, ethnicity has been classified into 2 classes instead of 3 and expression has been classified into 2 classes instead of 6. The classification of other 3 characteristics remains unchanged. We intuitively felt that the most difficult task for user in application 1 would be correctly classifying expressions into 6 different categories. Results of application 1 (presented in Section 4) confirm our assumption. Other than the difference in number of classes, the working of application 2 is exactly the same as that of application 1. **Fig. 5** schematically shows the characteristics and classes used in application 2.

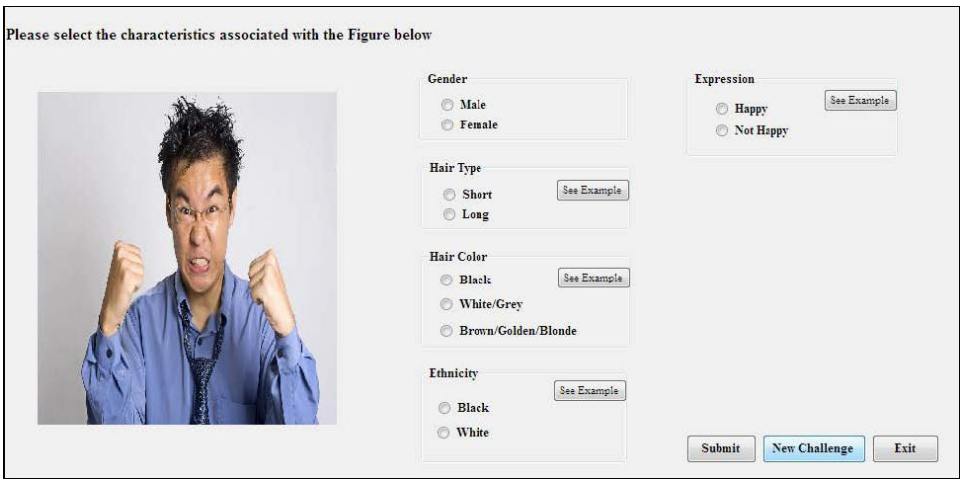

Fig. 5. CAPTCHA challenge of the proposed scheme (Application 2). Ethnicity and expression classes are reduced to 2 in each case.

4. Experimental Evaluation

4.1 Application 1

As mentioned earlier, we conducted a study with 25 participants to evaluate usability of the proposed scheme. Each user took CAPTCHA challenge 5 times resulting in a total of 125 attempts. For application 1, 77 attempts were successful while 48 were incorrect submissions resulting in a usability success rate of 62%.

In some cases, multiple misclassifications were made in a single incorrect response resulting in a total of 60 misclassifications against all characteristics. **Table 1** shows a distribution of user responses with respect to number of misclassifications in each attempt. As can be seen from the table, among incorrect submissions, most of the users have made just 1 misclassification while there are 3 misclassifications in the worst case. **Fig. 6** schematically represents number of misclassifications made against each characteristic (for both applications).

The results of application 1show that the expression characteristic was the most difficult to handle by the users resulting in 28 incorrect submissions. Ethnicity misclassification is also on the higher side while the other 3 characteristics have a relatively low misclassification rate.

Table 1. Number of misclassifications vs. number of attempts made by users

Number of misclassifications	Number of attempts	
	Application 1	Application 2
0	77	104
1	39	17
2	6	4
3	3	0

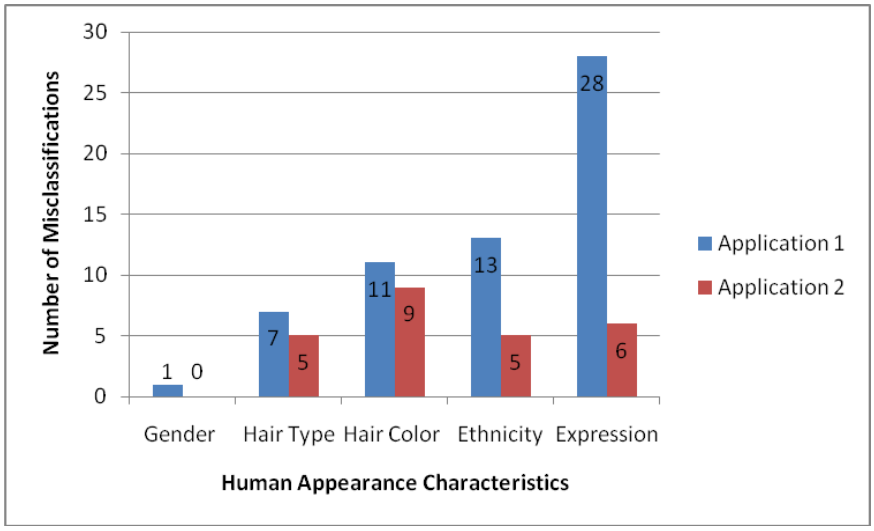

Fig. 6. Number of misclassifications made by the users against all characteristics

4.2 Application 2

As expected, the users find it quite difficult to classify multiple expressions accurately in application 1. In application 2, we reduced the number of expressions from 6 to 2 (*Happy* and *Not happy*). In addition, we also reduced the classes in ethnicity from 3 to 2 leaving the Asian class out.

Similar to application 1, 25 users submitted the responses 5 times each resulting in a total of 125 submissions. Number of successful attempts was recorded as 104 while 21 inputs were incorrect. Therefore, the human success rate was increased to 83% for application 2. There were a total of 25 misclassifications made against all characteristics. **Table 1** shows a

distribution of user responses with respect to number of misclassifications in each attempt. Similar to application1, most of the users have made just 1 misclassification while at most 2 misclassifications are there. **Fig. 6** shows misclassifications made against each characteristic (for both applications).

In application 2, the highest number of errors was recorded as 9 against hair color characteristic. Expressions were misclassified 6 times followed by 5 incorrect submissions each for both ethnicity and hair type characteristics.

4.3 Discussion on Results

Perception of individuals may vary quite significantly. For example, if a person has long hair according to one individual, it may not be the same for some other. In spite of these perception differences, the overall results are quite encouraging. In application 1, users classified all the characteristics correctly in 62% challenges which were further improved to 83% in application 2. Next, we discuss the results against each characteristic in some detail.

Gender: There was just one wrong submission under this category in application 1. After analyzing our database, we find out that it is more likely that the user has mistakenly selected the wrong option for that particular image.

Hair Type: There were 7 misclassifications for hair type in application 1 and 5 in application 2. Our analysis reveals that one reason of misclassifications is that some of the users did not consider the gender of the image to associate the corresponding hair type. Typically, females have longer hair and hence, the same length hair may be classified as long for males and short for females. But some of the users did not consider this fact. This type of failure rate can be minimized by training users to consider gender while associating hair type with the image.

Hair Color: For hair color, we have 11 and 9 misclassifications in application 1 and 2, respectively. Our analysis shows that images with lightening effects might have influenced the hair color selection. For example, in some of the images, shadow was present on one side of the head resulting in different hair color perception by different users. In addition, there were a few images where individuals had dyed their hair and as a result they had more than one shades in their hair again making the classification task difficult for the users. The error rate can be further reduced by carefully selecting the image dataset.

Ethnicity: Ethnicity class was mostly misclassified in application 1 with 13 misclassifications as compared to 5 in application 2. One reason of misclassifications could be the lack of geographic and social knowledge of the users. Some of the users could not classify correctly the ethnicity of Chinese and Japanese and categorized all of them on the basis of their facial color as “White/Caucasian". Many users also did not utilize the “See Example" option to get help on ethnicity using sample images.

Expression: As it can be seen in **Fig. 6**, expression characteristic is the one which caused single largest number of misclassifications among all characteristics in application 1. The errors were caused because it was difficult for the users to uniquely classify the given expression in a relatively long list of expression classes (6 classes: Anger, Disgust, Fear, Joy, Sad, and Surprise). **Fig. 7** shows the number of misclassifications against each expression class. For application 1, the figure shows 2 values against each class; 1) when a specific class is misclassified to any other class, and 2) when any other class is misclassified to that specific class. For example, “Joy to Any other” represents those misclassifications where manually assigned class was Joy but user assigned class was any of the other 5 classes. Similarly, “Any other to Joy” represents those cases where manually assigned class was not Joy but user assigned class was Joy. The results show that Surprise expression was most difficult for the

users to differentiate. There were 15 errors where either Surprise was misclassified to some other expression or some other expression was misclassified to Surprise. We expect that by more training and by selecting image dataset more carefully, overall success rate can be increased.

From the above discussion, it is evident that Application 2 has produced better usability results than Application 1. However, in Application 2, we have reduced number of classes which results in lower security against brute force attacks. In fact, usability and security are dependent on each other, i.e., more security mostly leads to less usability and vice versa. Same is true for our scheme. Application 1 is more secure than application 2 but has lower human success rate of 62% as compared to 83% for application 2.

Depending upon the required security level, human success rate of both applications can be further improved by modifying the challenge passing scenario. This can be done by requiring *m* out of *n* characteristics to match correctly instead of all *n* characteristics. For example, if we say that a CAPTCHA challenge is considered passed if any 4 out of 5 human characteristics are correctly tagged by the user, then the human success rates of application 1 and application 2 will be improved to 93% and 97%, respectively (Table 1: sum of number of attempts having 0 and 1 misclassification).

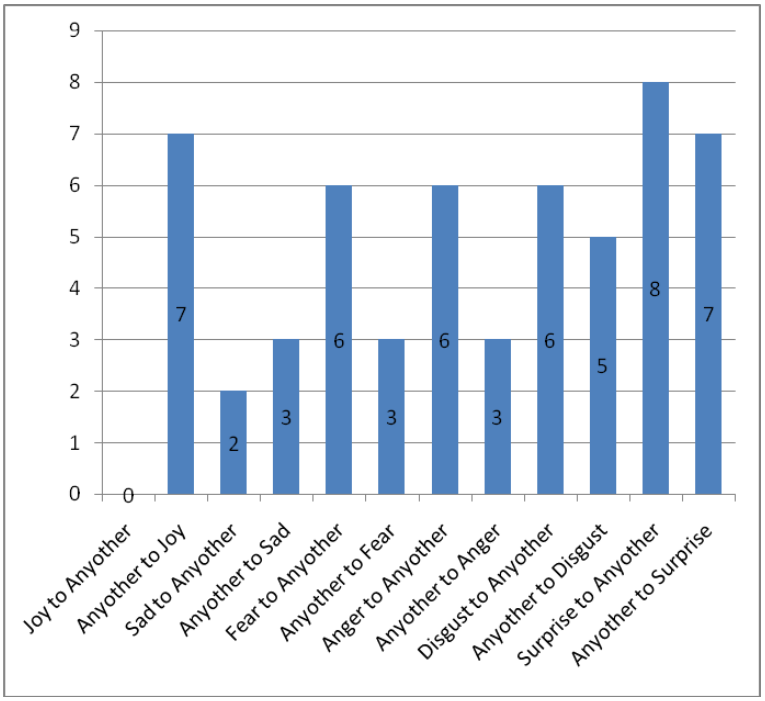

Fig. 7. Number of misclassifications involving different expression classes in application 1. Surprise expression proved to be most difficult for the users to classify.

5. Security Analysis of the Proposed Scheme

First, we discuss brute force attack against our scheme. A brute force effort requires 216 attempts to attack application 1 and 48 attempts for application 2. Although the above mentioned search space is not very large but as the purpose of CAPTCHAs is to prevent misuse of web services so if a bot is able to pass the challenge after 216 attempts, then most

probably it will not defeat the vary purpose of CAPTCHA. Additionally, challenge after every attempt is refreshed, so the attacker is not attacking the same image again and again. Besides this, we can block the user after a fixed number of attempts from the same IP address. In addition, to increase search space, 2 different images can be given to the user to associate characteristics. This will increase the brute force effort against application 1 from 216 to 46656 but it will also decrease the usability of the system.

Next we consider Artificial Intelligence attacks. The proposed scheme offers multiple machine challenges namely *gender classification*, *hair type classification*, *hair color classification*, *ethnicity classification* and *expression classification*. For some of these challenges, researchers have presented different algorithms giving reasonably accurate results on selected datasets. For example, gender classification is a two class problem and a lot of research has been done in automatically estimating human gender from facial images [20][21][22][23][24][25][26]. Similarly, research work has been done on ethnicity detection treating it as either a two class problem [23][25][27] (Asian/Non-Asian) or a three class problem [26][28] (Asian/Caucasian/African). Facial expression recognition is also an active area in AI research [29][30][31]. Though the above-mentioned systems show good classification results, they are typically limited to work with much lesser challenging images than those included in our dataset. Our database is extremely challenging for AI applications as we have images with lightening effects, cluttered background and side poses, etc. which makes the classification task much more difficult for machines as compared to that for humans.

To the best of our knowledge, there is no AI algorithm available to do the classification for the remaining two characteristics. In addition, it also looks intuitively difficult to train a system to classify hair color of images with lightening effects. Similarly, it is difficult for any software program or bot to identify the length of the hair in an image. For example, there is a person with long hair but have tied up his or her hair. Now a human can "see" its length but, most likely, a machine will not be able to classify the length correctly. In short, though there exist AI algorithms for detecting individual human appearance characteristics but passing CAPTCHA challenge as a whole in the proposed scheme is a difficult task for such algorithms due to involvement of multiple AI problems in a single challenge and presence of challenging images in our dataset.

6. A Modified Scheme to Overcome Manual Tagging Limitation

The major limitation of the proposed scheme is manual tagging of the images. By manual tagging, we mean that one has to manually associate values (classes) to the given characteristics for each image in the database. Unfortunately, this manual tagging approach is not feasible for real life applications with large datasets because it costs time and human resources. In this section, we propose a modification of the proposed scheme to overcome this limitation.

In the modified scheme, the user's response to a challenge is not only used to verify whether he or she has passed the test but also to tag those images in the database which have not been manually tagged. Initially a subset of the images is manually tagged while the tagging of remaining images (or new images which are subsequently added in the system) is automated through users' interaction with the system without a need to manually tag those images in the database. Instead of one image, now two images are shown to the user. The user is asked to associate characteristics with both images; one to pass the challenge (we call this *challenge image*) and the other to automatically tag the image in the database (we call this *database*

image). **Fig. 8** shows this modified CAPTCHA displayed to the user. The intuition is that if a user classifies all characteristics correctly for challenge image, it is quite likely that he or she will also classify all characteristics correctly for database image. In order to have more confidence in the classification of database image, we only mark the image as tagged in the database if all the values supplied by the users match for two consecutive appearances of that image. The following description explains the process in more detail.

For the proposed solution to work, we associate a *state* with each image in the database. An image can have one of the following three states: i) *Untagged*, ii) *Semi-tagged* and iii) *Tagged*. At the beginning, a subset is (manually) *tagged* and all the other images are *untagged*. In each CAPTCHA challenge, a challenge image and a database image (both randomly selected) are shown to the user. The challenge image is always *tagged* while the database image can be either *untagged* or *semi-tagged*. The user has to tag (classify) both images. If challenge image is not classified correctly by the user, the system displays a failure message and ignores the classification provided for database image. On the other hand, if challenge image is classified correctly by the user then database image is observed whether its status in the database is *semi-tagged* or *untagged*. If database image is *untagged* then its status is changed to *semi-tagged* and user assigned classes are stored in the database against that image. Alternatively, if database image is *semi-tagged* then its status is changed to either *tagged* or *untagged*. If all the classes assigned by the current user match with those in the database then the status is changed to *tagged* and classification is considered as final values for that image. On the other hand, if any of the classes do not match with the stored ones then the image is marked as *untagged* and its stored values are removed from the database. **Fig. 9** schematically illustrates this idea in the form of a flowchart.

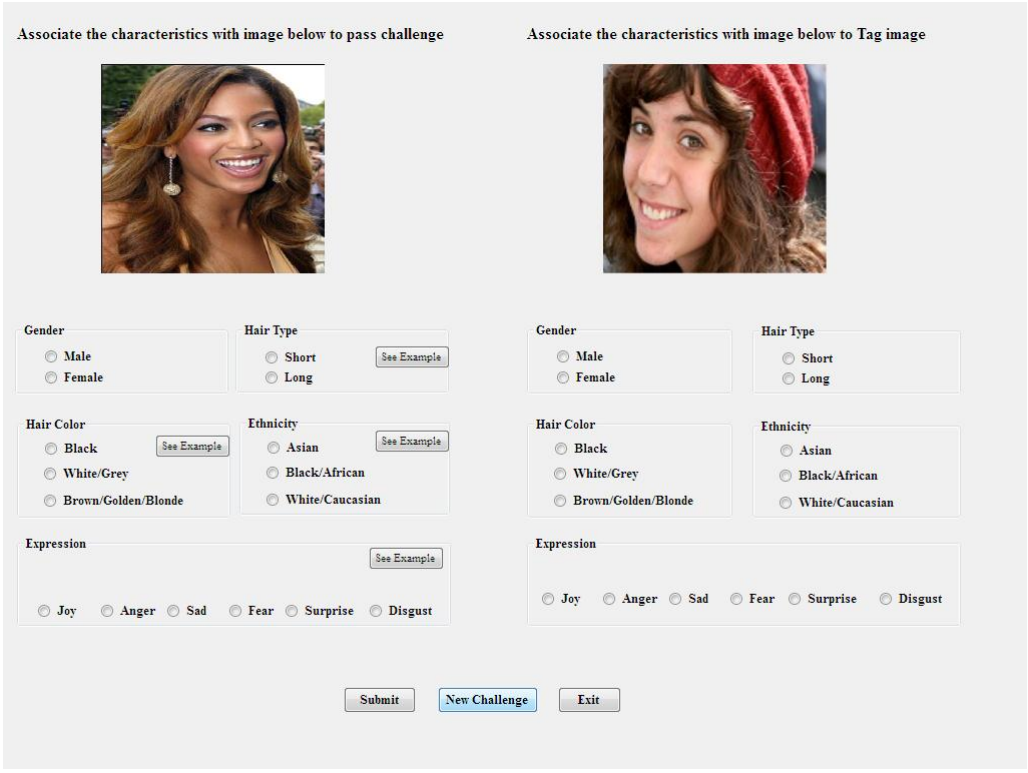

Fig. 8. CAPTCHA challenge of the proposed scheme for auto-tagging (Application 1). The challenge image is on the left while the database image is on right.

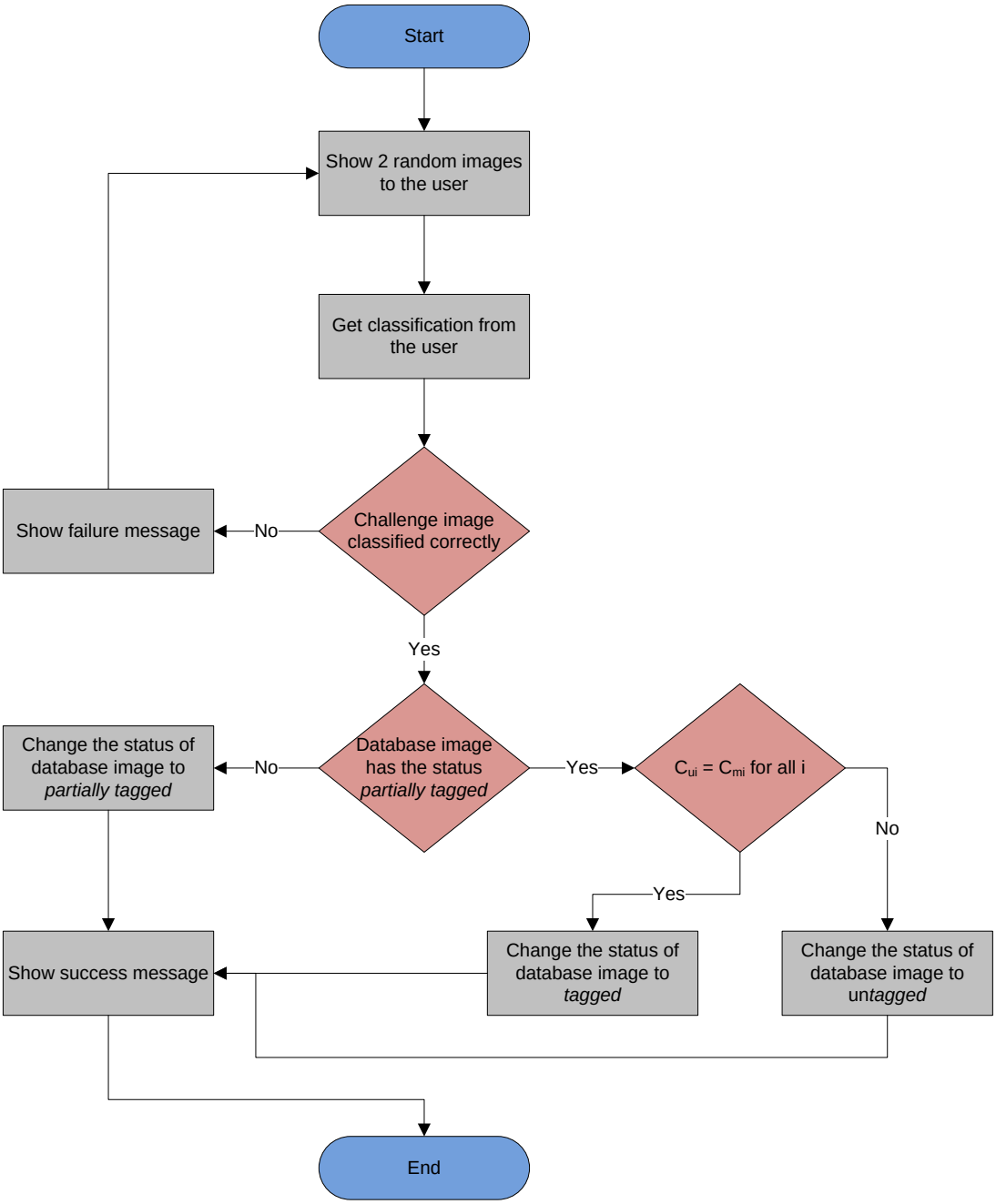

Fig. 9. A flowchart illustrating flow of control in our modified CAPTCHA to facilitate auto-tagging of images

Mathematically, we can explain our modified scheme as follows. The notations we use to describe the process are given in **Table 2**.

Table 2. Notations used for mathematical representation of modified scheme

Notation	Meaning
S_I	Set of all images in our database
S_T	Set of all tagged images in our database
S_S	Set of all semi-tagged images in our database
S_U	Set of all untagged images in our database
S_{SU}	$S_{SU}= S_S \cup S_U$ where U represents set union
I_C	Challenge image
I_D	Database image
C_{ui}	The value of *i*th characteristic of an image as assigned by the user responding to CAPTCHA challenge
C_{mi}	The value of *i*th characteristic of an image as assigned manually in the database

We use $x \overset{R}{\leftarrow} X$ to represent that an element x is selcted randomly from a set X. The algorithm of modified scheme is given below:

$I_c \overset{R}{\leftarrow} S_T$
$I_D \overset{R}{\leftarrow} S_{SU}$
If $(\mathbf{Tag}(I_C) == False)$
    Return $False$
Else
    If $(\mathbf{Status}(I_D == "semi\text{-}tagged"))$
        If $(\mathbf{Tag}(I_D) == True)$
            $\mathbf{Status}(I_D) = "tagged"$
        Else
            $\mathbf{Status}(I_D) = "untagged"$
        End If
    Else
        $\mathbf{Status}(I_D) = "semi\text{-}tagged"$
        $\mathbf{Update}(C_U, I_D)$ where $C_U = \{C_{ui}\}$ for all i
    End If
Return $True$
End If

The working of **Tag**, **Update** and **Status** sub-functions is given as under:

Tag(*I*) is a function that takes an image *I* as input and returns *True* if $C_{ui} == C_{mi}$ for all *i*; else it returns *False*.

Update(I,C_U) is a function that takes an image *I* and a set of characteristics C_U as input and updates all characteristics of *I* in database by corresponding values of C_U.

Status(*I*) is a function that takes an image *I* as input and returns status of *I* from the database ("*tagged*", "*semi-tagged*" or "*untagged*").

7. Conclusion

In this paper, we proposed a user friendly image-based CAPTCHA scheme based on the human appearance characteristics. We considered only those characteristics whose values are relatively unambiguous. We evaluated our proposed idea with two applications and presented the results comparing security and usability features. Our results indicate that some level of usability must be sacrificed to achieve higher level of security and vice versa. Our CAPTCHA challenge is not time consuming as users have to click using mouse instead of typing using keyboard which also results in avoidance of potential errors caused by misspellings and synonyms. Universality feature can be achieved by adding translator to dynamically convert the labels into user specified language. With two versions of the proposed scheme, we achieved a human success rate of 62% and 83%, respectively.

References

[1] M. D. Lillibridge, M. Abadi, K. Bharat and A. Broder, "Method for selectively restricting access to computer systems". *US Patent 6*,195,698., Feb.2001.
[2] Luis von Ahn, Manuel Blum, Nicholas J. Hopper and John Langford, "CAPTCHA: using hard AI problems for security," in *Proc. of EUROCRYPT 2003, international conference on the theory and applications of cryptographic techniques,* 2003. Article (CrossRef Link)
[3] A.L. Coates, H.S. Baird and R.J. Faternan, "Pessimal print: a reverse Turing test," in *Proc. of Document Analysis and Recognition,* 2001. Article (CrossRef Link)
[4] H.S. Baird, "Document image defect models," in *Proc. of Document Image Analysis*, 1995. Article (CrossRef Link)
[5] M. Chew and H.S. Baird, "BaffleText: a human interactive proof," in *Proc. of SPIE Document Recognition & Retrieval*, 2003. Article (CrossRef Link)
[6] Greg Mori, "Results on Gimpy", Oct. 2011. http://www.cs.sfu.ca/~mori/research/gimpy/hard/
[7] H.S. Baird and T.P. Riopka, "ScatterType: a reading CAPTCHA resistant to segmentation attack," in *Proc. of SPIE*, 2005. Article (CrossRef Link).
[8] Greg Mori and Jitendra Malik, "Recognizing objects in adversarial clutter: breaking a visual CAPTCHA," in *Proc. of Conference on Computer Vision and Pattern Recognition*, 2003. Article (CrossRef Link)
[9] J. Yan and El Ahmad, "A Low-cost Attack on a Microsoft CAPTCHA," in *Proc. of 15th ACM Conference on Computer and Communications Security*, 2008. Article (CrossRef Link)
[10] J. Yan and El Ahmad, "Is cheap labour behind the scene? Low-cost automated attacks on Yahoo CAPTCHAs", *School of Computing Science Technical Report,* 2008.
[11] El Ahmad, J. Yan, and L. Marshall, "The robustness of a new CAPTCHA," in *Proc.of the Third European Workshop on System Security*, 2010. Article (CrossRef Link)
[12] Y. Rui and Z. Liu, "ARTiFACIAL: Automated reverse Turing test using FACIAL features, *Multimedia Systems*, vol.9, pp.493-502, 2004. Article (CrossRef Link)
[13] H.S. Baird and J.L. Bentley, "Implicit CAPTCHAs," in *Proc. of SPIE*, 2005. Article (CrossRef

Link)
[14] R. Datta, J. Li and J. Wang, "IMAGINATION: a robust image-based CAPTCHA generation system," in *Proc. of the 13th annual ACM international conference on Multimedia*, 2005. Article (CrossRef Link)
[15] Wen-Hung Liao, "A CAPTCHA mechanism by exchanging image blocks," in *Proc. of the 18th IEEE International Conference on Pattern Recognition (ICPR'06), 2006.* Article (CrossRef Link)
[16] J. Elson, J. Douceur, J. Howell and J. Saul, "Asirra: a CAPTCHA that exploits interest-aligned manual image categorization," in *Proc. of the 14th ACM conference on Computer and Communications Security,* 2007. Article (CrossRef Link)
[17] Gossweiler Rich, Kamvar Maryam and Baluja Shumeet, "What's up CAPTCHA?: a CAPTCHA based on image orientation," in *Proc. of the 18th international conference on World Wide Web, 2009*. Article (CrossRef Link)
[18] Jong-Woo Kim, Woo-Keun Chung and Hwan-Gue Cho, "A new image-based CAPTCHA using the orientation of the polygonally cropped sub-images," *The Visual Computer,* , vol.26, pp.1135-1143, 2010.
Article (CrossRef Link)
[19] J. Holman, J. Lazar, J. Feng and J. D'Arcy, "Developing usable CAPTCHAs for blind users," in *Proc. of the 9th international ACM SIGACCESS conference on Computers and Accessibility*, 2007.
Article (CrossRef Link)
[20] B.A. Golomb, D.T. Lawrence and T.J. Sejnowski, "Sexnet: A neural network identifies sex from human faces," *Advances in neural information processing systems*, vol.3, pp.572-577, 1991.
[21] B. Moghaddam and M.H. Yang, "Gender classification with support vector machines," in *Proc. of Fourth IEEE International Conference on Automatic Face and Gesture Recognition,* 2000. Article (CrossRef Link)
[22] B. Moghaddam and M.H. Yang, "Learning gender with support faces," *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* vol.24, pp.707-711, 2002. Article (CrossRef Link)
[23] G. Shakhnarovich, P.A. Viola and B. Moghaddam, "A unified learning framework for real time face detection and classification," in *Proc. of Automatic Face and Gesture Recognito,2002*. Article (CrossRef Link)
[24] R. Iga, K. Izumi, H. Hayashi, G. Fukano and T. Ohtani, "A gender and age estimation system from face images," in *Proc. of IEEE SICE 2003 Annual Conference*, 2003.
[25] X. Lu, H. Chen, and A.K Jain, "Multimodal Facial Gender and Ethnicity Identification," in *Proc. of International Conference on Biometric,* 2006. Article (CrossRef Link)
[26] H. Lin, H. Lu and L. Zhang, "A new automatic recognition system of gender, age and ethnicity," in *Proc. of Sixth World Congress on Intelligent Control and Automation,* 2006. Article (CrossRef Link)
[27] X. Lu and A.K Jain. "Ethnicity identification from face images," in *Proc. of SPIE,* 2004. Article (CrossRef Link)
[28] S. Hosoi, E. Takikawa and M. Kawade, "Ethnicity estimation with facial images," in *Proc. of Sixth IEEE International Conferenc on Automatic Face and Gesture Recogniton,* 2004. Article (CrossRef Link)
[29] I.A. Essa and A.P. Pentland, "Facial expression recognition using a dynamic model and motion energy," in *Proc. of International Conference on Computer Vision,*1995. Article (CrossRef Link)
[30] Z. Zhang, M. Lyons, M. Schuster and S. Akamatsu, "Comparison between geometry-based and gabor-wavelets-based facial expression recognition using multi-layer perceptron," in *Proc. of Third IEEE International Conference on Automatic Face and Gesture Recognition,* 1998. Article (CrossRef Link)
[31] P.K. Manglik, U. Misra and H.B. Maringanti, "Facial expression recognition," in *Proc. of IEEE International Conference on Systems, Man and Cybernetics,* 2004. Article (CrossRef Link)

Sajida Kalsoom completed MS in Computer Science from COMSATS Institute of Technology (CIIT) in Islamabad, Pakistan. She is currently working as a lecturer in CIIT, Islamabad. Her research interests include information security and computer vision.

Sheikh Ziauddin is an assistant professor in department of computer science, COMSATS Institute of Information Technology in Islamabad, Pakistan. He did his PhD in Computer Science from Asian Institute of Technology in Bangkok, Thailand. His research interests include biometrics, image processing, cryptography, and computer security.

Abdul Rehman Abbasi is principal engineer at Design Engineering Lab, Karachi Institute of Power Engineering, Karachi, Pakistan. He completed his PhD in Mechatronics Engineering from Asian Institute of Technology in Bangkok, Thailand. His research interests include robotics, machine vision and machine learning.