Improving Security by Enhancing FsCAPTCHA with Morphing Faces

Sherry Mathew [1*], Leena Shaji[2]
[1*]PG Scholar, Dept. of computer science and engineering
[2]Asst.Professor, Dept. of computer science and engineering
TKM Institute of Technology, Kollam, India

***Abstract*—The Internet is a world-wide broadcasting medium for interaction between individuals and their computers without regarding its geographic location. But it represents an insecure channel for exchanging information leading to data theft or intrusions like phishing. So, Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA)is used as an additional layer of Security in most of the websites which distinguish humans from automated attacks. This paper proposes an enhanced face image-based CAPTCHA with a feature-line morphing technique to distort human faces and optimizing the face detection tests using simulated annealing.The result shows an improving security from most of the facial feature extraction methods and reduces the time complexity comparing to existing approaches.**

***IndexTerms*—Internet security, CAPTCHA, face detection, morphing**

I INTRODUCTION

The Internet is a widespread information infrastructure with various services such as online shopping, E banking, and Online Voting etc. It poses a significant challenge in providing effective online security from automated attacks.

CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) provides secondary authentication to reduce attacks by classifying human users and automated attacks. Text-based CAPTCHAs are used in many applications but they pose a challenge due to language dependency. CAPTCHAs provide an additional layer of security and are frequently paired with account login systems to prevent brute force password attacks. Several kinds of challenges can be posed by scripts or bots,which can put a heavy load on the servers and enforce a DoS (Disk Operating System) attack, generate multiple fake accounts in case of registration forms, which are not profitable to both the service provider and the client.Existing CAPTCHA implementations generally belong to one of three categories: (1) text-based, (2) image-based, or (3) video and audio-based.

In text-based CAPTCHAs, users must recognize the distorted characters and correctly enter them in the space allocated. Text-based CAPTCHAs are easy to generate but are vulnerable to optical character recognition (OCR) attacks [1]. Many text-based CAPTCHAs have been developed including CMU's EZ-Gimpy [2], Baffle Text [3], reCAPTCHA [4],Handwritten Word-based CAPTCHA [5] etc. Image-based CAPTCHAs generally rely on image classification where users are presented with a series of images and asked to identify the relationship between them. Examples of Image-based CAPTCHAs are ESP-PIX [6] and Asirra image-based CAPTCHA [7], IMAGINATION: A Robust Image-Based CAPTCHA Generation System [8]. Since the image categories are selected from a fixed list, there is a high likelihood of random guessing. Audio-based CAPTCHA are mainly introduced for visually-impaired users. These generally work by playing the recording of a set of words or characters with users being asked to type-in what they hear. But these CAPTCHAs are subject to attacks using speech recognition software.Video-based CAPTCHAs, users are shown You Tube videos and asked to tag them with descriptive keywords [9].

II RELATED WORKS

Several tests are proposed based of face image CAPTCHA for distinguishing human and computer users. Face Recognition CAPTCHAs (DeapeshMisra and KrisGaj,2006) in which, human face photographs from a public database is distorted using two different image processing transformations. Distorted photographs of several different human subjects to match by human users[10],Image-based face detection CAPTCHA for improved security(Brian M. Powell et al.,2010) in which,coordinates of human face bounding box are calculated and stored for each CAPTCHA. The web server will randomly select a CAPTCHA to display,when a user access the website containing the CAPTCHA. After reading the instructions on how to complete the CAPTCHA, users use their mouse to click on all human faces[11],Image CAPTCHA based on Distorted Faces(Cristina Romero Macias et al.,2011) the method uses a feature-line morphing technique to distort the faces which morphs the well-known person's face into a cartoon or an animal .The user has to recognize the well-known person that appears in the image choosing the name from a list.[12],FaceDCAPTCHA: Face detection based color image CAPTCHA(GauravGoswamia et al.,2012)algorithm generates a CAPTCHA that offers better human accuracy and lower machine attack rates compared to existing approaches. To solve the CAPTCHA, users must correctly identify visually-distorted human faces embedded in a complex background without selecting any non-human faces and marks the approximate center of all genuine face images present in the CAPTCHA.[13], fgCAPTCHA : Genetically Optimized Face Image CAPTCHA(Brian m. Powell et al.,2014)a novel image-based CAPTCHA that

combines the touch-based input methods favored by mobile devices with genetically optimized face detection tests to provide a solution that is simple for humans to solve.[14].

III PROPOSED APPROACH

There are many feature extraction methods to recognize the human faces even though the distortions are applied. So a new approach is proposed called FsCAPTCHA in which feature-line morphing technique is used to distort the human faces (morphs human face with the animal face), embedded on complex background and optimized the distortion settings using simulated algorithm, which reduces the time complexity comparing to previous approach. The proposed approach combines four distinct elements:

1) A set of images, some of which are photographs of real human faces, animal faces and others face-like images such as cartoons or sketches.
2) A feature line morphing technique is used to morph the human faces with the animal faces.
3) A complex background pattern designed to confuse the face detection software and embedded with morphed faces and cartoon faces.
4) A set of distortions are selected and these distortions are optimized using simulated annealing.

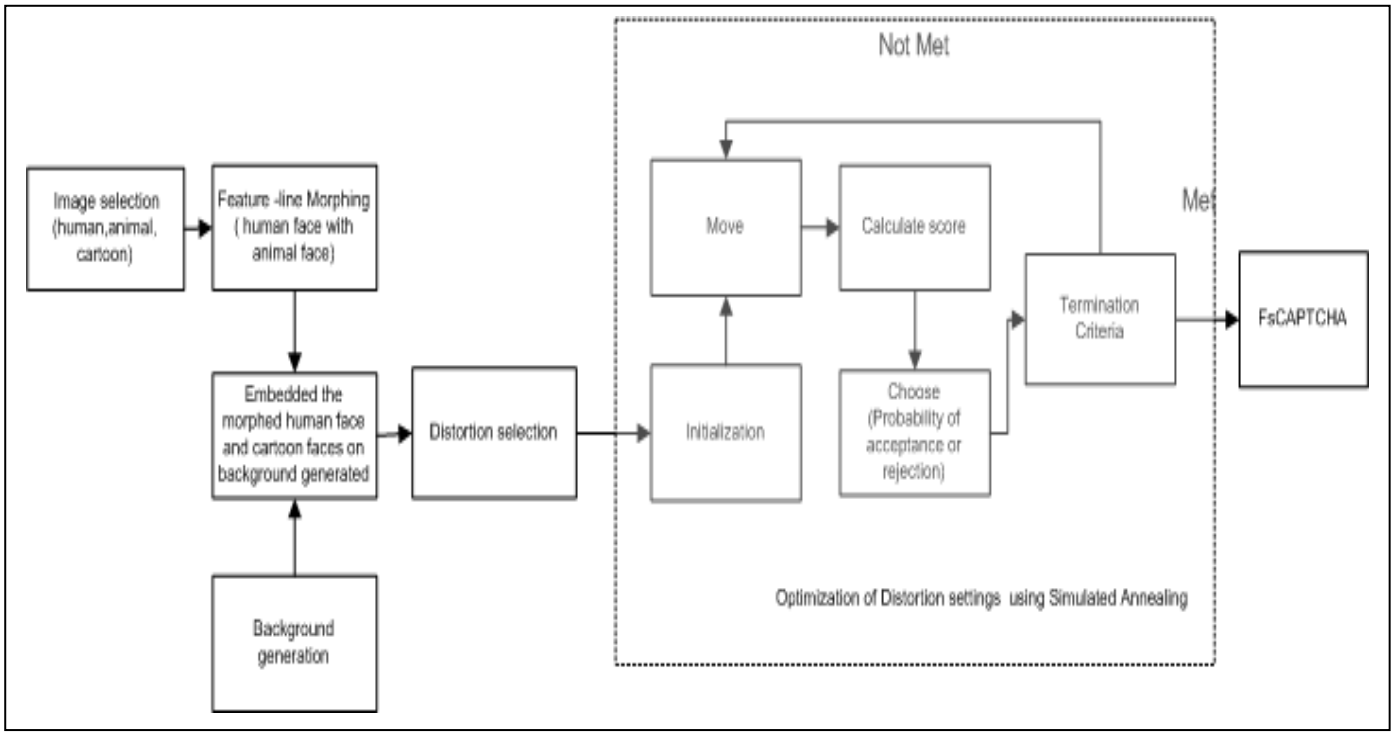


Fig 1 Steps involved for generating FsCAPTCHA

The Fig 1 describes the steps involved for generating the Face Image CAPTCHA: Image selection, Feature line morphing technique, Background generation,Embedded the selected images on background generated, Distortion selection, and Distortion optimization.

- Image selection: Image selection: Images of real human faces, animals and cartoon faces are collected from the available face databases.
- Feature line morphing technique: It is an animated transformation of oneimage into another [12] and it is divided into three stages: feature specification, warp generation and transition control.
  - Feature specification: The correspondencebetween images is done with pairs of feature primitives.
  - Warp generation: The mapping functions betweenimages which are to be morphed are computed.
  - Transition control: The transition rates in between the images are controlled.

The fig 2 given shows an example for morphing human faces with animal faces results a morphed human face. It distorts the primitive features of human face,which help to protect from face detection algorithm.

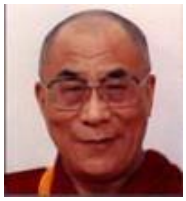
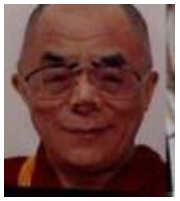
Human Faces	Animal Faces	Morphed Human Faces
		
		

Fig 2 an example for Morphing Human faces with the animal faces

- Background generation: The background is composed of many overlapping rectangles in various RGB colors and sizes. Height and width are based on a fraction of the overall image size that is randomly scaled.
- Embedded selected images (morphed faces and cartoon faces) on Background generated: The images selected are placed on random locations of Background generated in such a way that,
  $N_{total} = \{N_m + N_c | N_m \geq 2, N_c \geq 1\}$ (1)
  Where $N_{total}$is the total number of faces and N_m is the number of morphed human faces and $N_c$is the number of cartoon faces.
- Distortion selection: These distortions are classified into three categories: geometric, noise-based, and degradation distortions.
  Geometric distortions alter the shape, size, or position of embedded images. Noise based distortions add interference that is not present in the original image. Degradation distortions are designed to reduce detail or contrast, making it difficult to distinguish embedded images; Distortion types can be applied to reduce the automated attack rate.
- Distortion optimization: Distortions can be optimized by using the Simulated Annealing to provide good solutions with less time complexity. The Algorithm includes several steps such as:
  - Initialization: Set a score with random initial placement of morphed human faces, non-faces and the distortions applied on it. This can be considered as the current CAPTCHA.
  - Move:Perturb the placement of faces and non -faces and distortion levels applied on it through a random change. It can be taken as new CAPTCHA.
  - Calculate score:Calculate the changes in the score made in first two steps such that,
    $\Delta S = I_s - M_s$(2)
    where, $I_s$and M_s represents the initial score and the altered score made by random move,Δ S is the change in I_s and M_s
  - Choose: The probability of acceptance or rejection of the CAPTCHAdepends on change in score in first two steps.
  - Update: The CAPTHA with minimum score based on the placement of morphed human faces and Non-faces (without overlapping) and the distortion levels applied on background ground is preserved for next step.
  - Termination Criteria: After the update stage, if the requested rounds is reached, then preserved CAPTCHA is taken as best solution and store in the CAPTCHA bank. Otherwise, resulting CAPTCHA in update step is provided as input to the move step and operation of simulated annealing continues until the requested rounds reaches end with a best result.

III PERFORMANCE EVALUATION

This section presents the description of images and the complex background used to generate the CAPTCHA and evaluates the performance by comparing it with other image CAPTCHAs.

For experimental evaluation, photographs of 500 human faces, 500 animal faces and 500 cartoon faces are stored in image database. The human face and the animal faces from the database are randomly choose and morphed to distort the feature of human faces using image metamorphosis. A complex background with 500 x300 pixels consisting of a series of colored rectangles randomly superimposed over each other as shown in Fig 3.The morphed human faces and cartoon faces are randomly selected and embedded on the complex background generated. The distortion are applied on it and optimized by using simulated annealing.

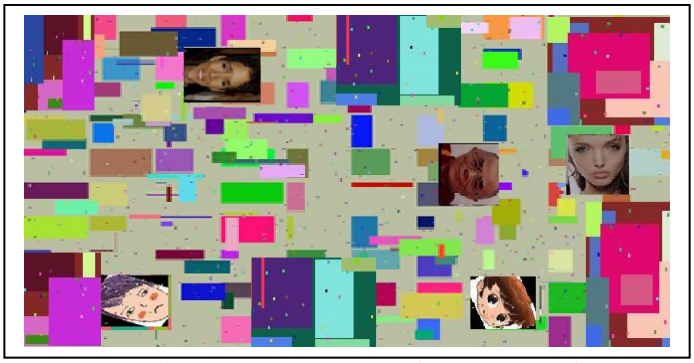


Fig 3 Example for FsCAPTCHA with a set of morphed human faces and cartoon faces

The results of proposed CAPTCHA are analyzed and compared it with other image CAPTCHAs. The graph given in Fig 4 shows the performance evaluation of FsCAPTCHA, FgCAPTCHAand IMAGINATION in Human success rate, Face detection rate, Time complexity. The evaluation in FsCAPTCHAshows a high performance in human successrate and less performance in face detection rate and time complexity comparing to other two image CAPTCHAs.

The FsCAPTCHA provides high performance in preventing spam and malicious software to break through web applications and increase security when logging in.

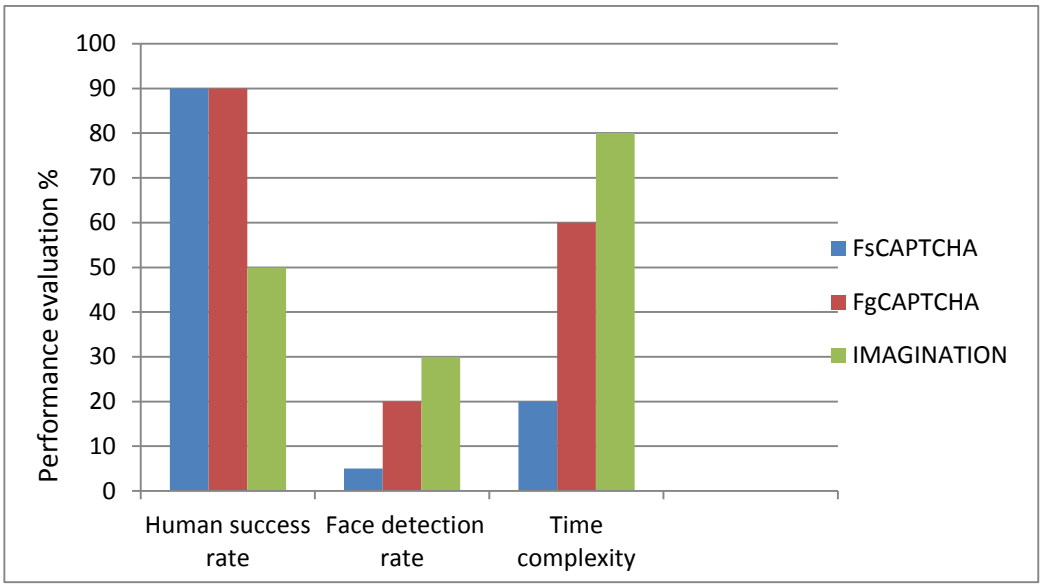


Fig 4 Comparisons in performance evaluation of various image based CAPTCHA$_S$

IV CONCLUSION

Enhancement in face image CAPTCHA can improve the security from most of face detection algorithm by using feature based morphing method and simulated annealing is used to optimize a face detection test by decreasing time complexity. The FsCAPTCHA provides high accuracy rate in distinguishing human users and automatic face detection algorithm. It can be readily used on all devices such as computers or in touch-based handled devices, since it has no language requirements. Users can easily recognise human faces from that of cartoons or sketches, even if it is distorted. But machine cannot recognise faces easily because it does the matching by pattern or feature extraction which is different from original image. The proposed approach shows more effectiveness and makes it easier to distinguish human users and other attacks.

REFERENCES

[1] Chellapilla, K., Larson, K., Simard, P.Y., and Czerwinski, Building Segmentation Based Human-Friendly Human Interaction Proofs (HIPs), In: Human Interactive Proofs, 2005, pp.1-26.

[2] M. Blum, L. A. von Ahn, and J. Langford, The CAPTCHA Project, Completely Automatic Public Turing Test to tell Computers and Humans Apart," www.captcha.net, Dept. ofComputer Science, Carnegie-Mellon Univ., and personal communications, November, 2000.

[3] M. Chew and H.S. Baird, BaffleText: a Human Interactive Proof, Proc., 10th SPIE/IS&TDocument Recognition and Retrieval Conf. (DRR2003), Santa Clara, CA, 2003, January 23-24.

[4] L.V.Ahn, B. Maurer, C. McMillen, D. Abraham, and M. Blum. reCAPTCHA: Human Based Character Recognition via Web Security Measures. Science Express, 2008, 321(5895):1465-1468.

[5] A.Rusu and V. Govindaraju. Handwritten CAPTCHA: Using the Difference in the Abilities of Humans and Machines in Reading Handwritten Words, In Proceedings of the 9thInternational Workshop on Frontiers in Handwriting Recognition, 2004, pages 226{231.

[6] C. Pope and K. Kaur. Is It Human or Computer? Defending ECommerce with CAPTCHAs, IEEE IT Professional, 2005, 7(2): 43-49.

[7] J. Elson, J.R. Douceur, 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, 2007, 366-374.

[8] 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 (MULTIMEDIA05), 2005,pages 331-334.

[9] Kurt Alfred Kluever and Richard Zanibbi, Balancing usability and Security in a Video CAPTCHA, Symposium on Usable Privacy and Security (SOUPS) 2009, July 15–17.

[10] DeepeshMisra and Kris Gaj"Face Recognition CAPTCHAs",inProceedings of the Advanced InternationalConference on Telecommunications and International Conference on Internet and Web Applications and Services,2006.

[11] Brian M. Powell and Adam C. Day, Richa Singh and MayankVatsa, AfzelNoore "Image-based face detection CAPTCHA
for improved security", in Int. J. Multimedia Intelligence and Security,Vol. 1, No. 3, 2010.

[12] Cristina Romero Macias, EbroulIzquierdo"Image CAPTCHA based on Distorted Faces" , in IET conference publications, pp. 1- 6,2011.

[13] Gaurav Goswamia,Brian M. Powell b, MayankVatsa, RichaSingh a, AfzelNoore "FaceDCAPTCHA: Facedetection Based color image CAPTCHA", in Future Generation Computer Systems, Vol.31, pp. 59_68, Feb.2012.

[14] Brianm. Powell, Gaurav goswami, Mayankvatsa,Richa and Afzelnoore "fgCAPTCHA: Genetically optimized face image CAPTCHA", in IEEE journals & magazine, vol.2,pp.473-484,2014.