Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

Optimized Face Image CAPTCHA as Graphical Password

Shahana AR[1], Elizabeth Jacob[2]
[1,2] *Computer Science and Engineering, Indira Gandhi Institute of Engineering and Technology*

Abstract—Most of the existing security primitives are based on hard AI problems. But these have been underexplored. This paper introduce a novel family of graphical password build on top of CAPTCHA technology. It is a combination of both CAPTCHA and a graphical password scheme. Many online security problems like online dictionary attack, relay attacks, brute force attacks can be overcomed by this scheme. Password can be found only probablistically in guessing attacks. The system uses a novel face image CAPTCHA which are optimized using genetic learning algorithm. The CAPTCHA combines touch based input methods favoured by mobile devices. They provide a high level security toward automated computer attacks.

Keywords—Graphical password, CaRP, Captcha, dictionary attack, relay attack,brute force attack security primitive

I. INTRODUCTION

Creating graphic primitives based on hard AI problem is the fundamental task in security. Several new paradigms have been introduced. The most noted and used is the CAPTCHA. Completely Automated Public Turing Test to Tell Computers and Humans Apart or CAPTCHA have been widely used to prevent automated attacks. The require a user to perform a task that are easy for humans but difficult for computers. They are mostly added with the login system of websites. They thus provide an additional layer of security when paired with the login systems. There are mainly three types of CAPTCHA: image based, text based, video or audio based. Among these types text based CAPTCHA is commonly used. It provide the user with an image of visually distorted text. The user has to identify the alphabets and type the corresponding letters.

However the CAPTCHA technology have limited success as compared with cryptographic primitives based on hard AI problem. The proposed method introduces a The proposed system introduce a novel family of graphical password build on top of CAPTCHA technology which can be called CaRP (Captcha as gRaphical Password). It is a click based password in which a sequence of click on a face image CAPTCHA is used to derive a password.

CaRP have generic and simple notion with multiple instantiations. CaRP offer protection against online dictionary attacks, relay attacks, which have been considered as a major security threat in online services. Defense against online attack is given by several counter methods. But they do not work well due to two reasons

- It causes deniel of service attack and also incures expensive helpdesk cost on account reactivation.
- It is vulnerable to global password attacks

CaRP also offers protection against relay attacks which is an increasing threat to bypass CAPTCHA protection. It is robust to shoulder surfing attack when combined to dual view technology. CaRP requires solving a CAPTCHA challenge in every login attempts. The CAPTCHA used in the system is an optimized face image CAPTCHA called fgCAPTCHA. It leverages touch screen technology in mobile devices tha make CAPTCHAs more user friendly and intuitive. The

fgCAPTCHA is a CAPTCHA that consist of a composite background pattern and a set of images. Inorder to solve the CAPTCHA the user have to select the images that are given as password during registration of the user.

The typical application scenario of using captcha as graphical password include

- Carp can be applied to touch screen devices where typing password is cumbersome. The input devices available for touch screen technology is limited.
- The use of face image CAPTCHA instead of text captcha makes the system language independent.
- The can avoid online dictionary attacks, brute force attack, relay attacks and increase spammer's operating cost. This can reduce spam emails.

The remaining part of paper is organized as follows: Background and Related Work is presented in Section II. The Proposed method is presented in Section III. Section IV include the Conclusion.

II. BACKGROUND AND RELATED WORK

A. Graphical password

There are a large number of graphical passwords proposed. They can be classified as three according to the task involved in memorizing and entering passwords. They are recognition, recall, cued recall.

A scheme which requires identifying among decoys the visual objects belonging to a password portfolio was proposed in [1]. A user selects a portfolio of faces from a database in creating a password. A panel of candidate faces is presented during authentication. The user selects the faces belonging to her portfolio .By using different panel this process is repeated in several rounds. The correct selection of faces results in successful login.

In a recall based scheme the user is asked to regenerate the same interaction result without cueing. In Draw A Secret [2] system the user draws her password on a 2D grid. This sequence of grid cells are encoded along the drawing path as a user.

In case of cued recall scheme [3] an external cue is provided to help memorize and enter a password. In this scheme the user is asked to select a sequence of points anywhere on an image in creating a password and re clicking the same sequence during authentication.

From all these three types recognition is considered the most easiest for human memory and pure recall is the hardest.

B. Captcha

Captcha are used to determine between human and computers. There are mainly two types of visual Captcha: text Captcha and Image Recognition Captcha (IRC). Text captcha relies on recognition of characters and Image Captcha relies on recognition of non character objects. Machine recognition of non-character objects is far less capable than character recognition whereas IRCs rely on the difficulty of object identification or classification, possibly combined with the difficulty of object segmentation.

The idea of introducingboth captcha and password was first introduced in [4] which was called Captcha- based Password Authentication. The protocol used in [4] requires inputting a valid pair or user ID and password followed by solving a aptcha challenge.In recognition based graphical passwords used in [5] [6] Captcha was also used. A text Captcha is displayed below each image and the user is asked to locate her own pass image from decoy images followed by entering the characters at specific location of the captcha below each pass image as her password during authentication.

III. PROPOSED WORK

3.1 CaRP Overview

Traditional approaches to counter guessing attacks aim at increasing the effective password space to make password harder to guess. It thus require more number of trials. Even with a secure graphical password scheme, the passwords can be found out using brute force attack.

CaRP uses a completely different approach to solve automated guessing attacks. It makes each trial computationally independent of other trials.Thus a password can be found only probabilistically by automated guessing attacks.

Carp uses an alphabet of visual objects(images of faces) to generate a Carp image which is also a CAPTCHA. The main difference between CaRP and CAPTCHA image is that a CaRP image uses a CAPTCHA that can be used by the user to derive a password. Many CAPTCHA schemes can be converted to CaRP images .

Generally CaRP images are click-based graphical passwords. Based on the memory task in memorizing and entering password the CaRP image can be classified as recognition and recognition-recall. The proposed method uses recognition-recall method which requires recognizing the pre specified image and also those images int the same order as entered during registration. The recognition-recall method combines the task of both cued-recall and recognition. The recognition-basedmethod retains the advantage of being easy for humans and cued recall makes the advantage of large password space.

Any CAPTCHA schemes that rely on recognizing two or more predefined visual objects can be converted to a CaRP image. Here the system uses an IRC(Image Recognition Captcha) whick consist of several images of faces. The CAPTCHA used by the scheme is a genetically optimized face image CAPTCHA(fgCAPTCHA) which is described in the next section.

3.2 Generation of fgCAPTCHA

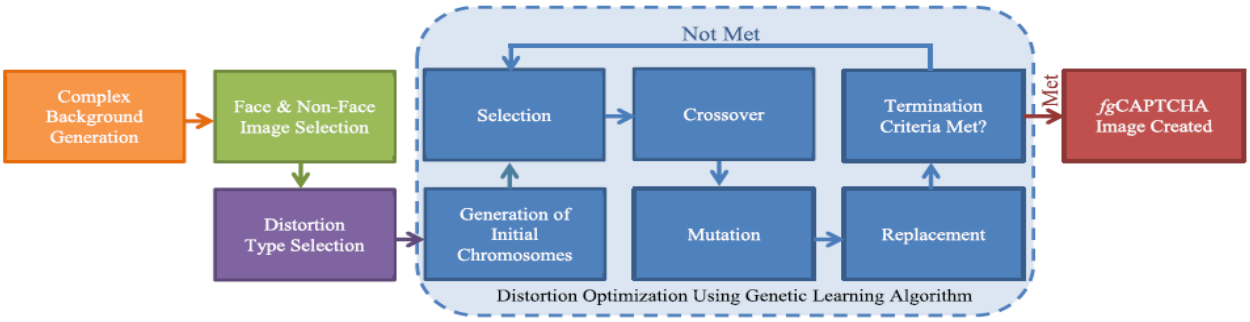

Fig 1. The steps involved in generation of fgCAPTCHA

The generation process can be represented as,

$$C=f\,(n_{min};\, n_{max};\, width;\, height;\, \Phi\, I_{face};\, I_{nonface}) \qquad (1)$$

where function *f* creates a new CAPTCHA of dimensions *width*-by-*height* pixels, containing a total of between n_{min} and n_{max} embedded images taken from sets I_{face} and $I_{nonface}$. The different stages involved in generation of fgCAPTCHA are as follows.

- **Generate initial chromosome**

The required number of sequence is generated.Sequence item consist of all the details regarding a specific image like width, hieght, rotation, position etc.Rank of each sequence is calculated based on overlap, color change, rotation and location.

- **Selection**

If the specified number of sequence is 4 then the step results in creation of 8 sequence. The first 4 will be the same as in initial step and the remaining is selected based on rank. The sequence with higher rank is taken when comparing two sequence

- **Cross over**

First 4 sequence remains unchanged. The remaining is taken 2 sequence at a time and the are combined.

- **Mutation**

First 4 sequence remains unchanged The remaining sequence is taken one at a time and random changes are made on each of them

- **Best solution**

The rank for all sequence is calculated Sequence are sorted based on rank' First 4 sequence with higher ranks are selected The process is repeated for specified number of rounds

3.3 Recognition-Recall CaRP

The user of the system is provided by a CAPTCHA during registering the account. The CAPTCHA will be an fgCAPTCHA described as in the previous section. The user selects three images from the CAPTCHA provided in a specific sequence. The backend database stores the location and ID of those images along with their order that has been entered by the user. The three selected image with that particular order now become the user's password.During login the user first enters the user id to retrieve the CAPTCHA. From the CAPTCHA the user selects the three images in the same order as it has been selected during registration. The clicked positions are recorded and compared with the values stored in the database to verify the user. If the user fails to select the correct images in correct sequence the access is denied.

The maximum number of trials with invalid password is limited to three i.e. if any attacker tries to guess the password will not be able to guess passwords more than three times. After three trials the user id will be blocked inorder to ensure that no guessing is done.

IV. CONCLUSION

We have proposed a new security primitive called CaRP relying on unsolved hard AI problems. It introduces a new family of graphical password to counter online guessing attacks. The CaRP image is also a CAPTCHA challenge and it make trials of an online guessing attack computationally independant of each other. A desired security property offered by CaRP is that a password can be found only probabilistically by online guessing attacks including brute force attack. The CAPTCHA used in by CaRP is a genetically optimized face image CAPTCHA which works efficiently in touch based technology used in tablets and smart phones and also in traditional computers. The CAPTCHA offer low attack rates,high human accuracy rates, and convenient mobile device usage which provides major improvements over existing desktop centric security CAPTCHAs in widespread use today.

REFERENCES

[1] (2012, Feb.). The Science Behind Passfaces [Online].vailable: http://www.realuser.com/published/Science Behind Passfaces.pdf
[2] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proc. 8th USENIX Security Symp., 1999, pp. 1–15.
[3] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," Int. J. HCI, vol. 63, pp. 102–127, Jul. 2005.
[4] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in Proc. ACM CCS, 2002, pp. 161–170.

[5] H. Gao, X. Liu, S.Wang, and R. Dai, "A new graphical password scheme against spyware by using CAPTCHA," in Proc. Symp. Usable Privacy Security, 2009, pp. 760–767.
[6] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, "Against spyware using CAPTCHA in graphical password scheme," in Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl., Jun. 2010, pp. 1–9.
[7] K. Golofit, "Click passwords under investigation," in Proc. ESORICS, 2007, pp. 343–358.
[8] A. E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the passpoints graphical password scheme," in Proc. Symp. Usable Privacy Security, 2007, pp. 20–28.
[9] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot spots in graphical passwords," in Proc. USENIX Security, 2007, pp. 103–118.
[10] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on passpoints-style graphical passwords," IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 393–405, Sep. 2010.
[11] P. C. van Oorschot and J. Thorpe, "Exploiting predictability in clickbased graphical passwords," J. Comput. Security, vol. 19, no. 4, pp. 669–702, 2011.
[12] T. Wolverton. (2002, Mar. 26). Hackers Attack eBay Accounts [Online]. Available: http://www.zdnet.co.uk/news/networking/2002/03/ 26/hackers-attack-ebay-accounts-2107350/
[13] HP TippingPoint DVLabs, Vienna, Austria. (2010). Top Cyber Security Risks Report, SANS Institute and Qualys Research Labs [Online]. Available: http://dvlabs.tippingpoint.com/toprisks2010 spyware using CAPTCHA in graphical password scheme," in Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl., Jun. 2010, pp. 1–9.
[14] H. S. Baird and T. Riopka, ``ScatterType: A reading CAPTCHA resistant to segmentation attack," in Proc. Document Recognit. Retr. XII, vol. 5676. San Jose, CA, USA, Jan. 2005, pp. 197_201.
[15] H. S. Baird, M. A. Moll, and S.-Y.Wang, ``ScatterType: A legible but hardto- segment CAPTCHA," in Proc. 8th Int. Conf. Document Anal. Recognit., vol. 2. Seoul, South Korea, 2005, pp. 935_939.
[16] H. S. Baird, M. A. Moll, and S.-Y.Wang, ``A highly legible CAPTCHA that resists segmentation attacks," in Proc. 2nd Int. Workshop Human Interact. Proofs, 2005, pp. 27_41.
[17] M. Chew and H. S. Baird, ``Baf_eText: A human interactive proof," in Proc. Document Recognit. Retr. X, Santa Clara, CA, USA, Jan. 2003, pp. 305_316.
[18] J. Yan and A. Salah El Ahmad, ``A low-cost attack on a microsoft captcha," in Proc. 15th ACM Conf. Comput. and Commun. Security, Oct. 2008, pp. 543_554.

