International Research Journal of Computer Science (IRJCS)
Issue 5, Volume 2 (May 2015)
ISSN: 2393-9842
www.irjcs.com

Images Pixel as Graphical Password Using Artificial Intelligence

THILAKARAJ.M-*PG Student II year MCA*
S.K. SARAVANAN, *Assistant Professor (Sel.Gr)*
G. DHARANI DEVI. *Assistant Professor (Sen.Gr)*
Department of Computer Applications, Valliammai Engineering College,
SRM Nagar,Kattankulathur-603203

Abstract: - ***We present a new security primitive based on hard Artificial Intelligence problems, namely, a novel family of graphical password systems built on top of Captcha technology. Graphical Password addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. Actually images as graphical password are used to secure the data with pixel representation of x and y coordinates. These security depends upon the pixel representation of the Images Graphical Password also offers a novel approach to address the well-known image hotspot problem in popular graphical password systems, such as PassPoints, that often leads to weak password choices.***

Keywords: Images Graphical password, password, hotspots, password guessing attack, security primitive.

INTRODUCTION

Artificial Intelligence Fundamental task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable. For example, the problem of integer factorization is fundamental to the RSA public-key cryptosystem and the Rabin encryption. The discrete logarithm problem is fundamental to the ElGamal encryption, the Diffie-Hellman key exchange, the Digital Signature Algorithm, the elliptic curve cryptography and so on. Using hard AI (Artificial Intelligence) problems for security, It is an exciting new paradigm. Under this paradigm, the most notable primitive invented is Captcha, which distinguishes human users from computers by presenting a challenge, i.e., a puzzle the capability of computers but easy for humans. Captcha is now a standard Internet security technique to protect online email and other services from being abused by bots. Image Graphical Password is click-based graphical passwords, where a sequence of clicks on an image is used to derive a password. Unlike other click-based graphical passwords, images used in graphical password are Captcha challenges, and a new image is generated for every login attempt. Image as graphical password can have multiple instantiations. In theory, any Captcha scheme relying on multiple-object classification can be converted to a Images as Graphical Password scheme as discussed in [1]. We present exemplary Image Password built on both text Captcha and image-recognition Captcha. One of them is a text Images as graphical password wherein a password is a sequence of characters like a text password, but entered by clicking the right character sequence on Password images.

BACKGROUND AND RELATED WORK

A recall-based scheme requires a user to regenerate the same interaction result without cueing. Draw-A-Secret was the first recall-based scheme proposed. A user draws her password on a 2D grid. The system encodes the sequence of grid cells along the drawing path as a userdrawn password. Pass-improves DAS's usability by encoding the grid intersection points rather than the grid cells[3]. BDAS adds background images to DAS to encourage users to create more complex passwords. In a cued-recall scheme, an external cue is provided to help memorize and enter a password. PassPoints is a widely studied click-based cued-recall scheme wherein a user clicks a sequence of points anywhere on an image in creating a password, and re-clicks the same sequence during authentication. Cued Click Points is similar to PassPoints but uses one image per click, with the next image selected by a deterministic function. Persuasive Cued Click Points extends CCP by requiring a user to select a point inside a randomly positioned viewport when creating a password, resulting in more randomly distributed click-points in a password.

Graphical Password

In this module, User are having authentication and security to access the detail which is presented in the Image system. Before accessing or searching the details user should have the account in the otherwise they should register first.

Images as Graphical Password in Authentication

It was introduced into use both Images and Password in a user authentication protocol, which we call Images-based password authentication protocol, to counter online dictionary attacks.

The Images as graphical password protocol in requires solving a Images pixel challenge after inputting a valid pair of user ID and password unless a valid browser cookie is received. For an invalid pair of user ID and password, the user has certain probability to solve a Images Pixel challenge before being denied access.

Thwart Guessing Attacks

In a guessing attack, a password guess tested in an unsuccessful trial is determined wrong and excluded from subsequent trials. The number of undetermined password guess decreases with more trials, leading to a better chance of finding the password. To counter guessing attacks [5], traditional approaches in designing graphical password aim at increasing the effective password space to make passwords harder to guess and thus require more trials.

Security of Underlying Images Pixel

Computational intractability in recognizing objects of images pixel in fundamental to Graphical Password. Existing analyses on Images Pixel security were mostly case by case or used an approximate process. No theoretic security model has been established yet.

RECOGNITION-BASED Image Graphical Password

For this type of Image as Graphical password is a sequence of visual objects in the alphabet. Per view of traditional recognitionbased graphical passwords, recognition-based CaRP seems to have access to an infinite number of different visual objects.

ClickText

ClickText is a recognition-based Images Pixel scheme built on top of Pixel password. Each digital images files stored inside a computer has a pixel value which describes how bright that pixel is, and what color is should be. During extraction, the image files are dividing into grids; it can be 16 by 16 grids or 8 by 8 grids[7]. Each grid is being calculated its pixel value with compression algorithm. Then , all grids pixel value with compression algorithm. Then all grids pixel value will be transform into a single value with compression algorithm once again. This is how pixel value is being produce and acquire from an image. In this graphical authentication method, pixel value will be used as authentication key for a password.

ClickAnimal

RECOGNITION-RECALL Graphical Password

In recognition-recall Grphical Password, a password is a sequence of some invariant points of objects. An *invariant point* of an object is a point that has a fixed relative position in different incarnations of the object, and thus can be uniquely identified by humans no matter how the object appears in Graphical password images. To enter a password, a user must identify the objects in a Images pixel, and then use the identified objects as cues to locate and click the invariant points matching her password. Each password point has a tolerance range that a click within the tolerance range is acceptable as the password point. Most people have a click variation of 3 pixels as discussed in [4][6]. TextPoint, a recognition recall graphical password scheme with an alphabet of characters, is presented next, followed by a variation for challenge response authentication.

Image Generation

TextPoints images look identical to ClickText images and are generated in the same way except that the locations of all the clickable points are checked to ensure that none of them is occluded or its tolerance region overlaps another clickable point's. We simply generate another image if the check fails. As such failures occur rarely due to the fact that clickable points are all internal points; the restriction due to the check has a negligible impact on the security of generated images.

Authentication

When creating a password, all clickable points are marked on corresponding characters in a image Pixel representation for a user to select. During authentication, the user first identifies her chosen characters, and clicks the password points on the right characters. The authentication server maps each user-clicked point on the image to find the closest clickable point. If their distance exceeds a tolerable range, login fails. Otherwise a sequence of clickable points is recovered, and its hash value is computed to compare with the stored value. In PassPoints, salient points should be avoided since they are readily picked up by adversaries to mount dictionary attacks, but avoiding salient points would increase the burden to remember a password. This conflict does not exist in TextPoints. Clickable points in TextPoints are salient points of their characters and thus help remember a password, but cannot be exploited by bots since they are both *dynamic* (as compared to static points in traditional graphical password schemes).

• **Dynamic:** locations of clickable points and their contexts (i.e., characters) vary from one image to another. The clickable points in one image are computationally independent of the clickable points in another image.

• **Contextual:** Whether a similarly structured point is a clickable point or not depends on its context. It is only if within the right context, i.e., at the right location of a right character.

SECURITY ANALYSIS

Automatic Online Guessing Attacks

In automatic online guessing attacks, the trial and error process is executed automatically whereas dictionaries can be constructed manually. If we ignore negligible probabilities.

1. Internal object-points on one Images pixel are *computationally-independent* of internal object-points on another Graphical password image. Particularly, clickable points on one image are computationally-independent of clickable points on another image.

2. Images pixel as graphical password trials in guessing attacks are mutually independent. The first property can be proved by contradiction. Assume that the property does not hold, i.e., there exists an internal object-point α on one image A that is non-negligibly dependent of an internal object-point β on another image B *[8][9]*.

An adversary can exploit this dependency to launch the following chosen-pixel attack. In the learning phase, image A is used to learn the object that contains point α. In the testing phase, point β on image B is used to query the oracle. Since point α is non-negligibly dependent of point β, this CPA-experiment would result in a success probability nonnegligibly higher than a random guess, which contradicts the CPA-secure assumption. We conclude that the first propertyn holds. The second property is a consequence of the first property since user-clicked internal object-points in one trial are computationally-independent of user-clicked internal object-points in another trial due to the first property. We have ignored background and boundary object-points since clicking any of them would lead to authentication failure.

Shoulder-Surfing Attacks

Shoulder-surfing attacks are a threat when graphical passwords are entered in a public place such as bank ATM machines. Images as graphical password is not robust to shoulder-surfing attacks by itself. However, combined with the following dual-view technology, Graphical password can thwart shoulder-surfing attacks. By exploiting the technical limitation that commonly-used LCDs show varying brightness and color depending on the viewing angle, the dual-view technology can use software alone to display two images on a LCD screen concurrently, one public image viewable at most view-angles, and the other private image viewable only at a specific view-angle. When a Images Pixel as graphical password is displayed as the “private” image by the dual-view system, a shoulder-surfing attacker can capture userclicked points on the screen, but cannot capture the “private” image that only the user can see. However, the obtained user-clicked points are useless for another login attempt, where a new, computationally-independent image will be used and thus the captured points will not represent the correct password on the new image anymore.

Implementaion:

Here I am using database of xamp to store the database that name details and x & y ordinates of Images as Grahical Password and then using jquery concept of accessing images as graphical password.The Images is used to store the x & y coordinates of doGet and doPost method that stored in server.

Testing is the process of executing the program with the intension of finding as yet discovered error. The primary purpose of testing is to detect software failures so that defects may be discovered and corrected. Software testing, depending on the testing method employed, can be implemented at any time in the software development process. Traditionally most of the test effort occurs after the requirements have been defined and the coding process has been completed, but in the agile approaches most of the test effort is on-going. As such, the methodology of the test is governed by the chosen software development methodology.

Testing cannot establish that a product functions properly under all conditions but can only establish that it does not function properly under specific conditions. A strategy for software testing may also be viewed in the context of the spiral and concentrates on each unit of the software as implemented in source code. Finally we arrive at system testing, where the software and the other system elements are tested as a whole

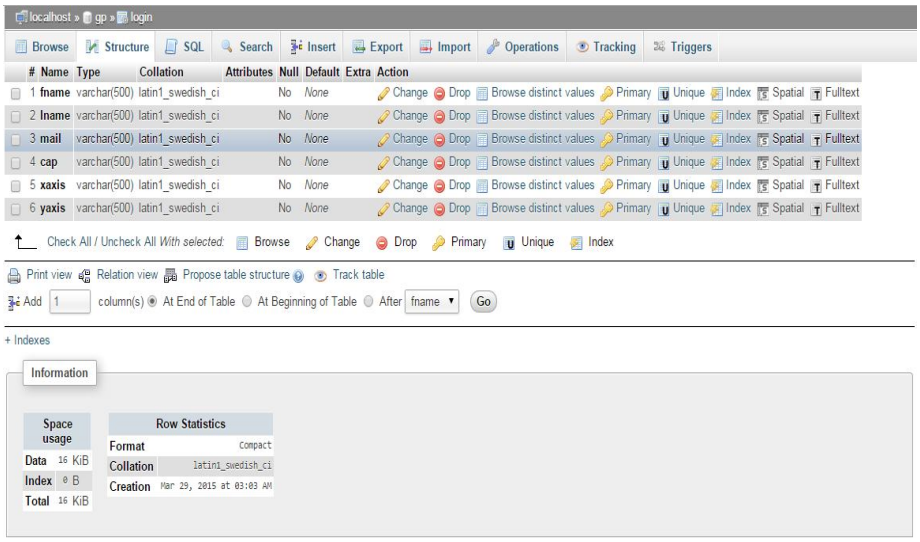

Fig-1: Database of the Image Pixel as Graphical Password

.

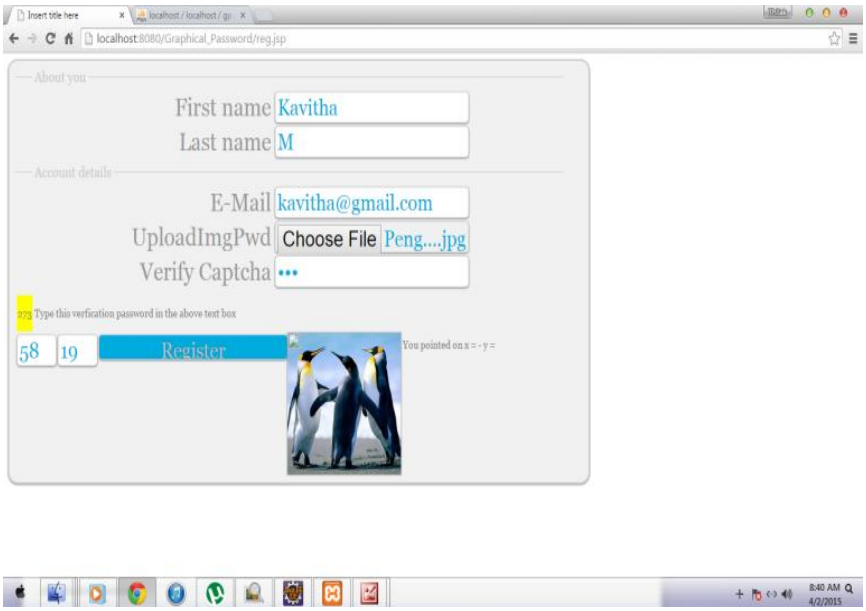

Fig-2: Image Pixel as Graphical Password Using AI of x & y Coordinates.

CONCLUSION

Our graphical password system provides more security to data and protection against different attack. Our graphical password system is based on text password and graphical password. For successful login user has to select correct image which is chosen by user during a registration and this system provide text password which provide more security to data Future work is based on Pattern.

We have proposed Images of graphical password, a new security primitive relying on unsolved hard AI problems. Graphical password is both a Images Pixel and a graphical password scheme. The notion of Images as graphical password introduces a new family of graphical passwords, which adopts a new approach to counter online guessing attacks: a new image is used for every login attempt to make trials of an online guessing attack computationally independent of each other. A password of graphical password can be found only probabilistically by automatic online guessing attacks including brute-force attacks, a desired security property that other graphical password schemes lack.

REFERENCES

1. R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Comput. Surveys*, no. 4, 2012.
2. (2012, Feb.). *The Science Behind Passfaces* [Online]. Available: http://www.realuser.com/published/ScienceBehindPassfaces.pdf
3. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in *Proc. 8th USENIX Security Symp.*, 1999
4. H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," *Int. J. Netw. Security*, vol. 7, no. 2, pp. 273–292, 2008.
5. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," Jul. 2005
6. N. Joshi. (2009, Nov. 29). *Koobface Worm Asks for CAPTCHA* [Online]. Available: http://blogs.mcafee.com/mcafee-labs/koobface- worm-asksfor- CAPTCHA M. Motoyama, K. Levchenko, C. Kanich, D. McCoy, G. M. Voelker, and S. Savage, "Re: CAPTCHAs—Understanding CAPTCHA-Solving Services in an Economic Context," in *Proc. USENIX Security*, 2010
7. P. C. van Oorschot and J. Thorpe, "On predictive models and userdrawn graphical passwords," *ACM Trans. Inf. Syst. Security* 2008.
8. K. Golofit, "Click passwords under investigation," in *Proc. ESORICS*, 2007,
9. E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the passpoints graphical password scheme," in *Proc. Symp. Usable Privacy Security*, 2007,

BIOGRAPHIES

Mr. M.Thilakaraj *is a Student Pursuing MCA course in Valliammai Engineering College. He is a talented, dedicated and hard working student.*

Mr. S.K.Saravanan *is an Assistant Professor, in Department of Computer Application, Valliammai Engineering College. He has 16 years of teaching experience in Engineering College.*

Ms. G.Dharani Devi *is an Assistant Professor, in Department of Computer Applications, Valliammai Engineering College. She has 14 years of teaching experience in Engineering College.*