Graphical User Password Using Cued Clicks

M.AishwaryaM.A.BlesslynRajeeta Ms .K.RajaSundari AP/CSE
Francis Xavier Engineering college Francis Xavier Engineering college Francis Xavier Engineering college
Department Of CSE, Department Of CSE, Department Of CSE,
Aishwarya230498@gmail.comblesslynrajeeta@gmail.comSundari.november@gmail.com

Abstract

Graphical Password Security consists of the provisions and policies adopted by a network administrator to prevent and monitor uni-authorized access, misuse, modification, or denial of a computer network and network-accessible resources. The most pre dominant computer authentication method is to use alphanumeric user names and password. This method has been shown many major disadvantages this is due to the problem that users tend to choose passwords that can be easily guessed and hacked by the hackers. In our research we conduct a comprehensive study on the existing graphical password technique and provide a possible solution using graphical password scheme which have been possessed as a possible alternate to text based scheme.This schemes are subjected to dictionary attacks. As a solution, user graphical password schemes are a promising alternative to text-based recognition schemes where instead of text, images are chosen for a password. Results show that the proposed scheme of user graphical password system with multiple alphabet images is more recognisable.

Introduction:

Network Security consists of the provisions and policies adopted by a network administrator to prevent , monitor unauthorised access, misuse, modification, or denial of a computer network and network accessible resources. Network involves the authorisation of access to data in a network, which is controlled by the network administrator. Users choose are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private such as within a company, others which might be open to public access. Network security is involved in organisations, enterprises, and types of institutions. It does as its title explains: It secures the network, as tell as protecting and overseeing operations being done. The simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

SVMs are inherited by SVR as tell, such as implementing the structural risk minimization principle, having good generalization for future test data, using the kernel trick, and having a sparse solution. Due to these benefits, SVR has been successfully used in many fields Recently, SVR has been extended to solve ordinal regression and multiregression. Hothever, the issues in SVMs also exist in SVR and its extension.

These issues include:

1. How to choose a proper kernel to tune the parameters; 2. How to incorporate prior knowledge function; 3.How into the learning process; and 4. How to speed up the optimal programming when the training set is very large. These issues are fundamental to further research for SVR. The first three issues can refer to Research about speeding up SVMs can be classified into three categories:

1)Using fast algorithms to solve quadratic programming2)Establishing new models to avoid quadratic program-mingand 3) selecting a subset of the training set to reduce the scale of the optimal programming In this paper, the only focus on how to select an appropriate subset for SVR. Only minor patterns named support vectors can influence the learning result in SVM-related algorithms.

The previous pattern selection work for SVM-related algorithms mainly focuses on support vector classification (SVC) or one-class SVM (OC-SVM). Most of this research can be classified into two groups: cluster-related methods and k-nearest neighbours (kNNs) related methods. The pattern selection work for SVR includes. Wang

and Xu divided the training set into several groups and then calculated the similarity bet then each pat-tern and the centre of the corresponding group. If the similarity is greater than a threshold, the pattern is discarded. Guo and Zhang pointed out that this method would lose too much accuracy. Sun and Cho proposed to measure sparseness, variability, and uniqueness of each pattern, and they needed three thresholds to determine whether a pattern should be retained. Guo and Zhang usedexternal patterns to represent the training set instead, where the external pattern is the global or local maximum/minimum in the training set. They pointed out that the support vector is always the global or local extremum. They needed to find kNNs of each pattern. If a training set contains l patterns, finding kNNs

Existing System:

Security plays a major role in the authentication process in high severity applications. Passwords are the type of secret code used in the process of authentication.

In the existing system, a captcha and a picture based authentication is designed to access the system.

The concept of visual cryptography has been integrated with the captcha for individual user and gets splitted equally in order to restore in the server.

The Server provide authentication to the requestor thereby verifying the captcha by merging the splitted shares to ensures the authorized human interpretations.

The attestate by means of picture also has been the part of the methodology that has a feature of clicking a spot on password.

Draw-based [1] type, choice based [2] type, click-based [3] type. In draw-based type, users have to draw some secrete. In Choice-based type, users have flexibility to select sequence of images to set password. In the case of click-based method, a user has to select click points on the image.

S.Wiedenbeck et al. (2005) [4] introduces a pass-points technique which helps to achieve usability by reducing the problem of memorable passwords over text based passwords method. Here user needs to select five click points on the image for registration. For authentication user needs to select five click points in the tolerance area in the same order. But it fails in the hotspot problem.

Sonia Chiasson et al. [5] proposed one method called cued click points which provides more usability and security than pass-points method. Here user can select one click point for one image up to n levels. In login phase user should follow the order and select the click point within the tolerance area. Cued click points provide usability but suffered with hotspot problem.

Suo et al. [8] proposes a shoulder-surfing resistant version of PassPoints. During login, the image is blurred except a small focused area. Rather than using a mouse to select their click points, use Y (for yes) or N (for no) on the keyboard, or use the right and left mouse buttons, to indicate if their graphical-point is within the focused area.

PERSUASIVE CUED CLICK POINT:

Hotspots and shoulder surfing problem reduces the security in the graphical based authentication. Attackers can retrieve the passwords using skewed password distribution.

An earlier result shows that most of the people are attracted on the same area of the image. So it is easy to attack. Observation reveals that if users select the click point without any other involvement still there is a chance to appear for hotspot problem. Researchers suggest that the user choice in all types of graphical passwords is inadvisable. To eliminate this, system involvement is needed to select more random graphical click points.

The attackers acquire knowledge of a particular user's credentials through direct observation or through external recording devices such as video cameras while the authorized user enters the information. An attacker who accurately observes one login has enough information to log in independently.

The PCCP uses persuasive technology to motivate users to select less guessable password and make it more complex to select every click point as hotspot. Mainly at the time of password creation using images are shaded except viewport and it is positioned randomly to avoid hotspots. This hotspot information allows attackers to improve guesses and could have a chance to produce new hotspot Point. Viewport size is

intended to offer a various distinct points but still cover only an acceptably small fraction of all possible points. Selection of Graphical click point of user must be inside the viewport only. Outside of the viewport will not respond for user clicks. The user has the flexibility to change the view-port area which is provided by the system whenever a user doesn't satisfy with the generated view-port area. phase, images are displayed without shading and user needs to select correct click points for authentication.

- The statistic from spatial analysis was used to measure clustering of click-points within data sets (the formation of hotspots).
- The J-statics combines nearest neighbour calculations and empty-space measures for a given radius r to measure the clustering of points.
- A result of J closer to 0 indicates that all of the data points cluster at the exact same coordinates, J ¼ 1 indicates that the data set is randomly dispersed, and J > 1 shows that the points are increasingly regularly distributed.

Proposed System

Replacing the textual password with a graphical password is the core idea of the project. In the older ages, the passwords were materialized in the form of graphical passwords with X,Y as co-ordinates on the images. Randomization clicks on the images enable the user to access the system is one of the major drawback. To overcome the issue, Persuasive cued click points (ccp) comes into an image/picture. A picture will be framed with multiple click points in turn, which will have successive cued clicks on the images.(ccp) The core point is, the user should select a secure hotspot in the image. The viewports are positioned randomly rather than allocating points particularly to avoid known hotspots. Such information might allow hackers to improve guesses and could lead to the formation of new hotspots. even if there is a possibility of selecting the correct points in the first image. ,The possibility of selecting the second hot spot becomes complex end where the user will be deviated to various other points And also the possibility of access to the application gets complex and not possible.

Proposed Algorithm

Fast Image Segmentation Algorithm

Input: training set$\boldsymbol{S}$consists of$\{\boldsymbol{xi},yi\}^{l}$=$i$1
Output: a subset$\boldsymbol{S}$of$\boldsymbol{S}$

Step 1: sort$\{\boldsymbol{xi},yi\}^{l}$=in ascending order according to target i1 values;
Step 2: find the local region around$y_i$according to algorithm 1;

Step 3: find the k-nearest neighbours of$\boldsymbol{x}_i$in its correspond-ing local region and calculate $D(\boldsymbol{x}_i)$;
Step 4: sort$\{\boldsymbol{xi},yi,\}^{l}$= in descending order according to $ID(\boldsymbol{x}_i)$;
Step 5: retain the topτ*$l$patterns (0< τ <1)to construct $\boldsymbol{S}$.

- The image is partitioned into connected regions by grouping neighbouring pixels of similar intensity levels.
- Adjacent regions are then merged under some criterion involving perhaps homogeneity or sharpness of region boundaries.
- A simple example of segmentation of threshold a Gray scale image with a fixed threshold t.
- Each pixel p is assigned to one of two classes, P-0 or P-1, depending on whether I(p) < t or I(p) >= t.

IMPROVISED CUED CLICK POINTS:

The PCCP heavily concentrated on hotspots issue. To eliminate this, it uses persuasive technology. This technology is good enough but usage is not much beneficial because here users have the facility to change the location. So still there will be a chance for hotspot. The PCCP doesn't provide any technique for minimizing shoulder surfing problem.

Improved persuasive cued click point method is enhancement of PCCP by adding some techniques. This paper mainly concentrates on reducing hotspot and shoulder surfing problem.
In this method we have four phases

1. pre-processing phase

2. Registration phase.
3. Login phase
4. Processing phase

Experimental Research

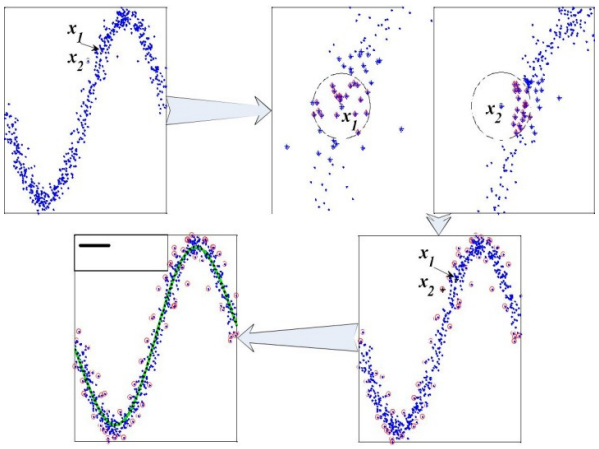

Fig.1-Pattern Selection

The usability functionality can be measured based on two factors, they are: success rate and password generation time.

Success rate: it can be calculated based on successfullogin of a user. User faces some minor difficulty during the registration phase due to blurring on the image because they face some difficulty to identify the image. It is user-friendly after completion of login phase.

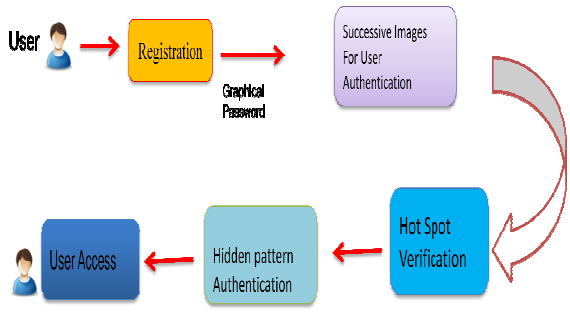

Fig.2-Data Flow Diagram

The user has to proceed Registration in a graphical Password in Successive Images for the user Authentication using a Hotspot Verification over a hidden Pattern Authentication which gets the User Access.

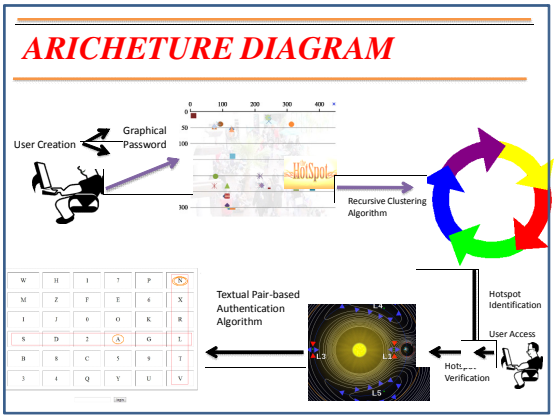

Fig.2- Architectural Diagram

The Architectural Diagram of Graphical User Password created by user by recursive Clustering Algorithm by hotspots which has to be verified by the user and gets into a Textual Pair Based Authentication Algorithm.

Conclusion:

We have generated security by visual cryptography within the server for authentication functions and merged to verify the credibility. Within the planned methodology, a Graphical Image secret has been designed that gives the users with associate degree choice to choose the hotspots within the hierarchy of the photographs. The sequential choice of the precise hot spots within the splitted image can modify the user to manoeuvre to subsequent thriving pictures. These hotspots are the approach differently in a different way in our own way otherwise outstanding way of authentication. In this project we are going to secured way authentication in web security vulnerabilities and identifying the attacks from hackers. It could be a valuable process to securing our website. In future it can be able to handle in a secured authentication while hot spot generates the fake clued click point to make moresecured it can send alert messages to mobile phones and in email which has been blocked ip address and mac address as a text. So the user can identify the intruders.

Reference:

1. (2012, Feb.). *The Science BehindPassfaces*[Online].
2. Available:http://www.realuser.com/published/ScienceBehindPassfaces.pdf
3. I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in *Proc. 8th USENIX SecuritySymp.*, 1999, pp. 1–15.
4. 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
5. 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.
6. P. C. van Oorschot and J. Thorpe, "On
7. predictive models and userdrawn
8. graphical passwords," *ACM Trans. Inf. Syst. Security*, vol. 10, no. 4, pp. 1–33, 2008.
9. K. Golofit, "Click passwords under investigation," in *Proc. ESORICS*, 2007, pp. 343–358.
10. A. E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the passpoints graphical password scheme," in *Proc. Symp. Usable PrivacySecurity*, 2007, pp. 20–28.
11. 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.
12. 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.
13. Y. Ren, P. N. Suganthan, and N. Srikanth, "A novel empirical mode decomposition with support vector regression for wind speed fore-casting," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8,
    a. 1793–1798, Aug. 2016.
14. J. Wu and H. Yang, "Linear regression-based efficient SVM learning for large-scale classification," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 26, no. 10, pp. 2357–2369, Oct. 2015.
15. R. Herbrich, T. Graepel, and K. Obermayer, "Large margin rank boundaries for ordinal regression," in *Proc. Adv. Neural Inf. Process. Syst.*, 1999, pp. 115–132.
16. W. Chu and S. S. Keerthi, "New approaches to support vector ordinal regression," in *Proc. 22nd Int. Conf. Mach. Learn.*, 2005,
    a. 145–152.
17. B. Gu, V. S. Sheng, K. Y. Tay, W. Romano, and S. Li, "Incremental support vector learning for ordinal regression," *IEEE Trans. NeuralNetw. Learn. Syst.*, vol. 26, no. 7, pp. 1403–1416, Jul. 2015.
18. Y. Xiao, B. Liu, and Z. Hao, "A maximum margin approach for semisupervised ordinal regression clustering," *IEEE Trans. Neural Netw.Learn. Syst.*, vol. 27, no. 5, pp. 1003–1019, May 2016.
19. M. Sánchez-Fernández, M. de Prado-Cumplido, J. Arenas-García, and F. Pérez-Cruz, "SVM multiregression for nonlinear channel estimation in multiple-input multiple-output systems," *IEEE Trans. Signal Process.*, vol. 52, no. 8, pp. 2298–2307, Aug. 2004.
20. [13] P.Bouboulis, S. Theodoridis, C. Mavroforakis, and L. Evaggelatou-Dalla, "Complex support vector machines for regression and quaternary classification," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 26, no. 6, pp. 1260–1274, Jun. 2014.
21. D. You, C. F. Benitez-Quiroz, and A. M. Martinez, "Multiobjective optimization for model selection in kernel methods in regression," *IEEETrans. Neural Netw. Learn. Syst.*, vol. 25, no. 10, pp. 1879–1893,Oct. 2014.
22. B. Chen, H. Liu, and Z. Bao, "Optimizing the data-dependent kernel under a unified kernel optimization framework," *Pattern Recognit.*, vol. 41, no. 6, pp. 2107–2119, 2008.
23. B. Pan, W.-S. Chen, C. Xu, and B. Chen, "A novel framework for learning geometry-aware kernels," *IEEE Trans. Neural Netw. Learn.Syst.*, vol. 27, no. 5, pp. 939–951, May 2016.
24. F. Bellocchio, S. Ferrari, V. Piuri, and N. A. Borghese, "Hierarchical approach for multiscale support vector regression," *IEEE Trans. NeuralNetw. Learn. Syst.*, vol. 23, no. 9, pp. 1448–1460, Sep. 2012.
25. L. Jian, Z. Xia, X. Liang, and C. Gao, "Design of a multiple kernel learning algorithm for LS-SVM by convex programming," *Neural Netw.*, vol. 24, no. 5, pp. 476–483, 2011.

25. C. G. Sentelle, G. C. Anagnostopoulos, and M. Georgiopoulos, "A simple method for solving the SVM regularization path for semi-definite kernels," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 4,
    a. 709–722, Apr. 2016.
26. Y. Ding, L. Cheng, W. Pedrycz, and K. Hao, "Global nonlinear kernel prediction for large data set with a particle swarm-optimized interval support vector regression," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 26, no. 10, pp. 2521–2534, Oct. 2015.
27. E. Osuna, R. Freund, and F. Girosi, "An improved training algorithm for support vector machines," in *Proc. IEEE Workshop Neural Netw. SignalProcess.*, Sep. 1997, pp. 276–285.
28. J. C. Platt, "Fast training of support vector machines using sequential minimal optimization," in *Advances in Kernel Methods-Support VectorLearning*. Cambridge, MA, USA: MIT Press, 1999, pp. 185–208.
29. C. J. Hsieh, K. W. Chang, C. J. Lin, S. S. Keerthi, and S. Sundararajan, "A dual coordinate descent method for large-scale linear SVM," in *Proc.25th Int. Conf. Mach. Learn.*, 2008, pp. 408–415.
30. S. Shalev-Shwartz, Y. Singer, N. Srebro, and N. Cotter, "Pegasos: Primal estimated sub-gradient solver for SVM," *Math. Program.*, vol. 127, no. 1,
    a. 3–30, 2011.
31. O. L. Mangasarian and E. W. Wild, "Proximal support vector machine classifiers," in *Proc. Knowl. Discovery Data Mining (KDD)*, 2001,
    a. 77–86.
32. O. L. Mangasarian and E. W. Wild, "Multisurface proximal support vector machine classification via generalized eigenvalues," *IEEE Trans.Pattern Anal. Mach. Intell.*, vol. 28, no. 1, pp. 69–74, Jan. 2006.
33. Jayadeva, R. Khemchandani, and S. Chandra, "Twin support vec-tor machines for pattern classification," *IEEE Trans. Pattern Anal.Mach. Intell.*, vol. 29, no. 5, pp. 905–910, May 2007.
34. Y.-J. Lee and O. L. Mangasarian, "RSVM: Reduced support vector machines," in *Proc. SIAM Int. Conf. Data Mining*, vol. 1. 2001,
    a. 325–361.
35. M. B. de Almeida, A. de Padua Braga, and J. P. Braga, "SVM-KM: Speeding SVMs learning with *a priori* cluster selection and *K* -means," in *Proc. 6th Brazilian Symp. Neural Netw.*, Nov. 2000, pp. 162–167.
36. F. Zhu, J. Yang, N. Ye, C. Gao, and G. Li, "Neighbors' distribution property and sample reduction for support vector machines," *Appl. SoftComput.*, vol. 16, pp. 201–209, Mar. 2014.
37. F. Zhu, J. Yang, J. Gao, C. Xu, S. Xu, and C. Gao, "Finding the samples near the decision plane for support vector learning," *Inf. Sci.*, vols. 382–383, pp. 292–307, Mar. 2017.
38. M. Nandan, P. P. Khargonekar, and S. S. Talathi, "Fast SVM training using approximate extreme points," *J. Mach. Learn. Res.*, vol. 15, no. 1,
    a. 59–98, 2014.
39. H. Shin and S. Cho, "Neighborhood property–based pattern selection for support vector machines," *Neural Comput.*, vol. 19, no. 3, pp. 816–855, 2007.