# A Review of Captcha and Graphical Passwords to Enhance Security and Usability to Next Level

**Vikas K. Kolekar**[1], **Milindkumar. B. Vaidya**[2]

[1,2]Savitribai Phule Pune University, Amrutvahini College of Engineering, Sangamner, Maharashtra, India 422608.

**Abstract:** ***Sometimes user will have to go through extra exhaustive steps for registration as well as login as far as security issues are concerns. These registration steps are influenced with some Artificial Intelligence logics and some tedious mathematical calculations which make login process more secure. Though security of particular user is extended to some level it requires some extra jugglery for registration and login which may be a long process for users. Hence there must be system with an easy and effective approach to solve the problem of long process of registration and login which extends security level to next extend. To extend this security to next level new area is in limelight named Captcha as graphical password. Captcha is basically challenge and response technique designed to differentiate humans from automated programs. It contains some tasks which are easy to humans and difficult to bots. Hence new schemes should be explored for registration and login process and simplified with captcha as graphical password schemes. These new schemes must be explored in such a way so that online guessing attacks, shoulder-surfing attacks, relay attacks etc. should get solutions. Hence by using captcha as graphical password schemes, system should be strong enough as far as security is concern.***

**Keywords:** Captcha, graphical password, hotspot, online guessing attack, shoulder-surfing attacks, security primitive.

## 1. Introduction

Cracking password is regular practice. These practices are like online guessing attack, online dictionary attack, shoulder surfing etc. Such attacks raise a big question to the security of system. In the current era, Captcha is used as standard Internet security technique to protect online email and other services from being abused by bots.

Hence it's a challenging and open problem to design such system that are efficient and having smart approach towards hard AI problems as far as security primitives are concern. Its prime need to focus on underexplored capabilities of Captcha. To explore the solutions for security and enhance its features Captcha as password technique found great advantages which is efficient to avoid such bot's attack. More ways should be searched on Captcha schemes which avoids online guessing, relay, shoulder-surfing, spammer attacks etc. Since in a guessing attack, wrong password guess is excluded from further trials. Such exclusion of wrong passwords leads to a better chance of finding the password. If we promote Captcha as a Graphical password then human guessing attacks can be minimize and to avoid certain trials if a new image with different pass-points in it is used for each trial, and, then certain guesses may be invalid and probability to guess perfect password is decreases. Separate images among different login attempts must contain independent information so that the authentication server can verify claimants only. Hence based on some existing system and by avoiding their drawbacks new techniques should be explored having Captcha as graphical password. These schemes must focus to develop probability mass function that minimizes the probability of guessing passwords through online guessing attacks, relay attacks, shoulder surfing attack etc.

## 2. Related Work

We have paper [1] for the reference and as a base which promotes and discusses various schemes having Captcha as graphical password.

There are some existing systems that worked on the graphical passwords but they have their own drawbacks hence we have to develop password schemes above all of these existing schemes. There are existing systems like Passface [2] in which user selects a portfolio of faces from a database in creating a password. During authentication, a panel of candidate faces is presented for the user to select the face belonging to his portfolio. This process is repeated several rounds, each round with a different panel. A successful login requires correct selection in each round. The set of images in a panel remains the same between logins, but their locations are permuted. But when particular person get an idea regarding portfolio faces then he can easily pass the login process.

Story [3] is also same as Passface but in this user have to provide proper order of portfolio faces at time of login. It is also not good scheme as far as shoulder attack is concern.

Déjà vu [4] is also similar but uses a large set of random art images. Cognitive Authentication requires a user to generate a path through a panel of images as follows: starting from the top-left image, moving down if the image is in his portfolio, or right otherwise. The user identifies among decoys the row or column label that the path ends. This process is repeated, each time with a different panel. A successful login requires that the cumulative probability that correct answers were not entered by chance exceeds a threshold within a given number of rounds. This process is also not good against shoulder attack.

Draw–A–Secret [5] is a recall based scheme requires a user to regenerate the same interaction result without cueing. It is the first recall-based scheme proposed. A user draws his password on a 2D grid. The system encodes the sequence of grid cells along the drawing path as a user drawn password. It can be also break as far as shoulder surfing is concern.

For proper security purpose Captcha as graphical password is considered. Text captcha and Image-Recognition captcha are two types of captcha.  For text captcha design [6] paper named ‘A low-cost attack on a Microsoft CAPTCHA,’ By J. Yan and A. S. El Ahmad is considered. In this paper, they analyze the security of a text-based Captcha designed by Microsoft and deployed for years at many of their online services including Hotmail, MSN, and Windows Live etc. It covers Microsoft specific services only. For designing customized Captcha human interactions proofs should be captured which is discussed in [7] paper named ‘Building segmentation based human-friendly human interaction proofs,’ By K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski. This paper discusses about human interaction proofs (HIPs) and various human interactions, image processing and machine learning techniques. Clutter alphabet management in Captcha is introduced here. It proves that character segmentation difficulty relies on text Captcha. It is difficult from computation point of view and combinatorial hard. Here object segmentation is directly and exponentially depends on number of objects and polynomially dependent of the size of the Captcha alphabet.

S. Li et al. [8] discussed some image processing and pattern recognition techniques is proposed to break all e-banking Captcha schemes. The success rates of proposed attacks are either equal to or close to 100%. They also discuss possible enhancements to these e-banking Captcha schemes. In [9] a new graphical password scheme against spyware is discussed. It provides an option to text based passwords. Use of Captcha to protect sensitive user inputs on an un-trusted client is discussed in [10]. Some common aspects of client-side attacks (e.g., Trojan horses) against Web applications and present two simple techniques that can be used by Web applications to enable secure user input are discussed in it. It also conducted two usability studies to examine whether the techniques that propose are feasible.

S. Chiasson et al. in [11] said that cued click points (CCP) are the inputs to form password. First click on image decides the further sequence of images. For wrong click wrong sequence of image is generated. S. Chiasson et al. [12] discussed Persuasive Cued Click Points (PCCP) technique. Here instead of queued display of images, randomly placed images are used. User has to click on that randomly placed images. It offers more secure way of login.

R. Biddle et al. in [13] enlisted and discussed all these schemes briefly along with advantages and disadvantages. S. Wiedenbeck et al. in [14] discussed PassPoints, which 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 same sequence during authentication.

S. Pinkas et al. in [15] discussed technique to avoid online dictionary attack. It also used Captcha and password for login and specific Captcha based password authentication protocol is discussed. Along with username and password user has to solve Captcha challenge also. This challenge is possible for specific number of times in case of failure.

## 3. Analysis

In this paper, we reviewed Captcha schemes and click-based graphical password schemes. Captcha can be attacked with help of relay attack and image processing algorithms. In click-based graphical passwords there are some schemes like Passface in which when shoulder-surfer gets an idea of portfolio faces then he can easily predict the password in it and can login into system. Also there are techniques like story, Déjà- vu, Draw-A-Secret which is also not good from shoulder surfing point of view. There are some techniques like PassPoints and cued click point in which images are used for registration and login but hotspot remains as the problem. Also there are some schemes based on cued-recall techniques which are also not good from online guessing and shoulder surfing point of view.

Hence there are no perfect techniques that provide smart solution to these online attacks with minimal AI operations.

## 4. Construction of Proposed System

We propose that our system is easy to understand and will overcome attacks like online dictionary attack, shoulder surfing attack, relay attack etc. It is found that click-based Captcha as Graphical Password schemes are useful in terms of security and usability. Hence proposed system must implement Captcha as graphical password schemes for registration as well as login. In one of the Captcha as graphical password scheme password can be entered with click in a reverse, skipped sequence, shuffled way instead of entering password in sequential order click i.e., clicking on scheme identifying number followed by clicking the password string characters on the canvas.

Our proposed system’s focus will be on recognition and recognition–recall based schemes. These schemes should provide smart and good solutions for various attacks as mentioned earlier. Also these schemes should not pose much hard AI problems that increase the execution time.

## 5. Conclusion

Provision for online dictionary attacks, shoulder-surfing attacks, and relay attacks can be done using Captcha as graphical password with simple AI techniques having recognition or recognition-recall schemes in it. These schemes are required at time of registration of user as well as login of user. This proposed system can be developed in low cost and it will boost the security and the usability primitives.

## 6. Acknowledgment

We would like to thank family members and friends who knowingly or unknowingly helped us in this work.

## References

[1] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu , "Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems," in *IEEE Transactions on Information Forensics and Security*, June 2014, pp.891-904.

[2] (2012, Feb.). *The Science Behind Passfaces* [Online]. Available: http://www.realuser.com/published/ScienceBehindPassfaces.pdf

[3] D. Davis, F. Monrose, and M. Reiter, "On user choice in graphical password schemes," in *Proc. USENIX Security*, 2004, pp. 1–11.

[4] R. Dhamija and A. Perrig, "Déjà Vu: A user study using images for authentication," in *Proc. 9th USENIX Security*, 2000, pp.1–4.

[5] 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.

[6] J. Yan and A. S. El Ahmad, "A low-cost attack on a Microsoft CAPTCHA," in *Proc. ACM CCS*, 2008, pp. 543–554.

[7] K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski, "Building segmentation based human-friendly human interaction proofs," in *Proc. 2nd Int. Workshop Human Interaction Proofs*, 2005, pp. 1–10

[8] S. Li, S. A. H. Shah, M. A. U. Khan, S. A. Khayam, A.-R. Sadeghi, and R. Schmitz, "Breaking e-banking CAPTCHAs," in *Proc. ACSAC*, 2010, pp. 1–10.

[9] 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.

[10] M. Szydlowski, C. Kruegel, and E. Kirda, "Secure input for web applications," in *Proc. ACSAC*, 2007, pp. 375–384.

[11] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in *Proc. ESORICS*, 2007, pp. 359–374.

[12] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing users towards better passwords: Persuasive cued click-points," in *Proc. Brit. HCI Group Annu. Conf. People Comput., Culture, Creativity, Interaction*, vol. 1. 2008, pp. 121–130.

[13] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Comput. Surveys*, vol. 44, no. 4, 2012.

[14] 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, July.2005, pp. 102–127.

[15] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in *Proc. ACM CCS*, 2002, pp. 161–170.

[16] G. E. Blonder, "Graphical passwords," *Lucent Technologies, Inc., Murray Hill, NJ, U. S.Patent,Ed.* United States, 1996.

[17] S. Chiasson, R. Biddle.and P. van. Oorschot, "A Second Look at the Usability of Click-Based Graphical Passwords," *Proceedings ACM Symp.Usable Privacy and Security(SOUPS)*,July 2007.

[18] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle, "Multiple Password Interference in Text and Click-Based Graphical Passwords," *Proceedings ACM ConferenceComputer and Comm. Security (CCS)*, Nov. 2009.

[19] L.Sobrado and J.C.Birget, "Graphical passwords," *The Rutgers Scholar, An ElectronicBulletin for Undergraduate Research*, vol. 4, 2002.

[20] E.Stobert, A.Forget, S.Chiasson, P.van Oorschot, and R.Biddle, "Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords," *Proceedings AnnualComputer Security Applications Conference(ACSAC)*, 2010.

[21] S.Chiasson, A.Forget, R.Biddle, and P.C.van Oorschot, "User Interface Design AffeectsSecurity: Patterns in Click-Based Graphical Passwords," *International Journal of Information Security*, vol. 8, no. 6, 2009, pp. 387-398.

[22] W. Jansen, "Authenticating Mobile Device Users Through Image Selection," *Data Security*,2004.

[23] D.Weinshall and S.Kirkpatrick, "Passwords Youll Never Forget,but Cant Recall," *Proceedings of Conference on Human Factors in Computing Systems(CHI)*. Vienna, Austria:ACM, 2004, pp. 1399-1402.

[24] W.Jansen, S.Gavrila, V.Korolev, R.Ayers, and R.Swanstrom, "Picture Password: A VisualLogin Technique for Mobile Devices," *National Institute of Standards and TechnologyInteragency Report NISTIR 7030*, 2003.

[25] K. Gilhooly, "Biometrics: Getting Back to Business," *Computerworld*. May 09, 2005.

[26] 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, pp. 435-452.

[27] J. Elson, J. R. Douceur, J. Howell, and J. Saul, "Asirra: A CAPCTHA that exploits interest-aligned manual image categorization," in *proc. ACM CSS*, 2007, pp. 366-374.

## Author Profile

**Mr. Vikas K. Kolekar** received the B.E. in Information Technology from Vishwakarma Institute of Information Technology, Pune in 2012. Currently he is pursuing Master's degree in Computer Engineering from Amrutvahini College of Engineering, Sangamner under Savitribai Phule Pune University. He is currently working in the field of security and privacy.

**Prof. Milindkumar B. Vaidya** received the B.E. in Computer Engineering and M.E. in Computer Science and Engineering. He is Assistant Professor at Amrutvahini College of engineering, Sangamner. He has 18 years of experience in teaching during which he published number of research papers at National and International Conferences. His area of interest includes distributed system and security.