International Conference on Recent Trends in Data Science and its Applications
DOI: rp-9788770040723.170

An Intelligent Authentication System to Enhance the Security of Network Banking

K Sathya
Dept.of.Computer Application, Saveetha College of Liberal Arts and Science, SIMATS,
Chennai, Tamilnadu, India Email: sathyak.sclas@saveetha.com

K Kalaiselvi
Dept.of.Computer Application, Saveetha College of Liberal Arts and Science, SIMATS,
Chennai, Tamilnadu, India
kalaiselvik.sclas@saveetha.com

A Hency Juliet
Dept.of.Computer Application, Saveetha College of Liberal Arts and Science, SIMATS, Chennai,Tamilnadu, India
hencyjulieta.sclas@saveetha.com

Sakthivel V
Konkuk Aerospace Design Airworthiness Institute, Konkuk University,
05029, Seoul, South Korea
Email: mvsakthi@gmail.com

Vishnu Kumar Kaliappan
Department of Computer Science and Engineering, KPR Institute of Engineering and Technology,
Tamil Nadu, 641407, India

***Abstract*—The security of single-level authentication as a graphical password entirely depends on confidentiality and strength. Even if graphical passwords are the fine stproxy approach to subdue the weak point soft he text-based password, single-level authentication is not enough to secure our dataain the devices. Hence, Facet Pass a novelmulti-level graphical authentication technique is proposed with an arrangement of 44 of 16 facets with four different colours. This approach in corporates by the process of facet touch, swap and fading an imation (manual) with deep convolutional neural network architecture for facial recognition mechanisms (automatic) which protect from exhaustive attack, technology-based recording, dictionary, and smudge attack. Visual complexity score of Facet Pass measured using Euclidean physical length. The success probability of the brute force attack is calculated based on permutation and combination. An investigation is conducted systematically on the challenges of FacetPass password in both security and usability perspectives with 113 participants of various age groups, and the people are from different educational status. The outcome of this work outperforms well with the usability and security of existing VAP code, CD-GPs, and EvoPass.**

***Index Terms*—facet, swap, fade, facial, graphical password**

I. INTRODUCTION

Many kinds of research are emerging with much authentication technique, but there is no replacement for text passwords with other alternatives to authenticate the user for the past ten years.However,password-basedauthenticationhasitsinherent security vulnerabilities, amongst which password disclosure is a significant security problem that was raised by Long et al. [1]. Text-based passwords leak through numerous attacks, including Ransomware, key loggers, secret cameras, and web accesstiminganalysis.Aspassword-basedauthorizationhasbeen generally used for service industries, online communities and some other useful services, the implications of password leakage might be catastrophic [2]. The Modified ASCII Value (MAV) is created to reinforce the wedges' encryption algorithm to protect a text-based password depending on the ASCII values [3]. Instead of typing text with a keyboard, Luis A. Leiva and Francisco Alvaro developed a captcha; the user retypes a computational statement and resolves it on a touchscreen [4]. Hence, protecting text password is another major complication in thesedays.

The graphical password entry method is sensitive to shoulder surfing threats in which a neighbouring antagonist capturesthe password while entering it on a user interface without anyadvanced recording equipment, such as a secret camera. In thiswork consists, two mechanisms (i) Touch and Swap image-based graphical password and (ii) Facial Recognition authentication. This practice enhances the resistance to shoulder surfing and attacks by brute-force attacks without modifying thepassword frequently like text-based password practices. Usersof FacetPass are required to touch and swap on the fadinganimated facets within the time when it goes invisible. If theuser fails to complete it within the single fading animationtime (standard evolving time and user configured evolvingtime) another two chances are given. The user should waitfor another 30 seconds if they miss all the three opportunities.Facial Recognition is the detection of the legitimate user by thecaptured facial images using the front camera automaticallywith the assistance of an algorithm for a deep neural network.The remaining part of the paper is organized as mentionedbelow, in section 2 the related study is explained briefly withsubtitle of recall and recognition based GPs. Then in section 3 the flow of the proposed FacetPass – a graphical password work is depicted in detail with FacetPass Registration, Facet Touch and Swap and Time-Evolving attribute. Further we analyzed about experimental result of security and usability insection4.Finallyweconcludethepaperinsection5.

II. RELATEDWORKS

A. Recall and Recognition based GPs

Nowadays, graphical passwords are other alternatives for text passwords to authenticate the user. Authentication or identity management is the tool used to allow users to validate their identity with web services. In recent decades, graphical password techniques have gained more publicity as an excel- lent alternative to the text-based password system suggested by Angeli A. D et al. [5]. For those who have a poor vision, this strategy is uncomfortable because their excessive images appear on a small screen.Azad S et al. in 2017 introduced vibration and pattern code in a 2X2 grid [6], Kim Dand Dunphy P [7] proposed Multi-touch 3X3 grid nine circular targets arranged in a system, Tiny-Lock model is proposed by Kwon T and Na s in 2014 [8]. Because of the long-term memory (LTM) issues, Wixted [9] specified

DOI: rp-9788770040723.170

text-based passwords are difficult for users to remember dynamic and unordered passwords over time to handle certain alphanumeric characters. With the enhancement of conventional graphical passwords by merging current input styles such as clicking, choosing the right and drawing, Meng [10] created a Click- Draw oriented graphical password authentication structure (CD-GPs).

A graphical password was developed by Blonder [11] to enable users to click on multiple prescribed regions over an image for identity verification. With the help of attributes and passwords, Jianghong Wei et al. [12] established a two-factor user authentication. Wiedenbeck et al. [13] introduced the authentication scheme of a pass point that allows people to click anywhere on an image to construct the passwords. Chiasson et al. [14] created a cued click points (CCP) structure that allows users to click on a series of images at one position per image.

All graphical based authentication systems may be narrowly divided into four major categories (i) recognition-based model(ii) purely recall-based model (iii) cued-recall-based model and (iv) hybrid model. This proposed FacetPass is designed based on the combination of biometric-based authentication and cued-recall of knowledge-based authentication. Majority of graphical passwords are focused on recognition of given images such as Pass faces and classification and recognition of user-uploaded images which are described by Hayashi E et al.[15].

III. PROPOSEDMETHODOLOGY

A. *FacetPass: A Graphical Password -Overview*

Facet means one of the tiny flat surfaces cut on a whole object, and these facets of an entire image utilized for touch and swap. In this paper, Facet touch-swap with facial recognition evolves as a new conglomerate graphical passwordfor increased usability and robustness. FacetPass incorporates recall and biometric techniques to provide all mobile devices, apps and websites with a distinct type of password. It offers several resilience measures against different attacks. Here legitimate users are required to touch and swap of the facet in the grid along with facial identification of the user for the authentication purpose.

The facial recognition task is done by the device with the set of user's face images with multiple angles to train the min the registration.Fig.1 reveals the details of this proposed scheme. This paper connects the technical contribution of facet touch, swap and fading animation with facial recognition to solve an existing problem in a graphical password. To avoid spoofing attack and to strengthen the security of a graphical password, users facial feature recognition is added in thi swork.

FacetPass Registration The subsequent actions are necessary for the password registration process. The user should touch on the facets that he wishes to swap in the first step. Even though the user swaps two facets, the initial facet alone gets the touches. In the second step, the user is swapping facets during the fading out animation. In the next step user's face is captured automatically by the device in the facet's background at the same time. The same steps follow at the authentication process as well.

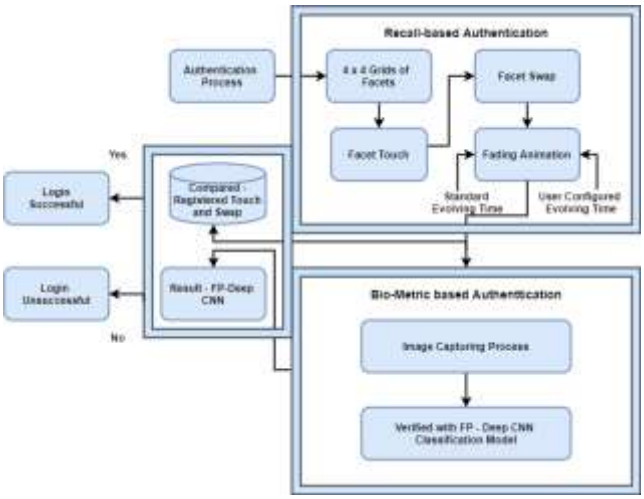

Fig. 1. Authentication process of FacetPass

B. *Facet Touch andSwap*

Within this proposed report, we developed an innovative method of user authentication via a grid of 16 facets in four different colors. For creating the password, the user needs to do several consecutive touching and swapping of facets on the grid. Fig.2 shows a graphical password scheme, a grid with arrangements of 16 facets and various instances of image capturing process by the legitimate user and other users. In the first level of authentication, the user needs to do a single touch or multiple touches with facet swapping, and in the second level, the system automatically capturing the image of the person who swaps the facets to validate the person is permissible or not. While login, if users sequence of touches, swaps and facial features match with the registered data, the access is acquired by the user, otherwise the access is denied. Hence, the user should provide the registered touch and swap sequence with facial features to get authentication.

Fig. 2. Avarious instances of FacetPass: i) Initial FacetPass without user image. ii)Swap instance with fading animation. iii) Visible swapped Facets with capturedimage.iv)Aninstanceofvisiblenon-swappedFacetswithcapturedimage.

C. *Time-Evolvingattribute*

FacetPass is using fading animation to have a more shoulder surfing resilient model by reducing the possibilities of identifying the target facets. This facet animation starts losing its original colour, at one particular point of time it becomes invisible (hidden). The user can change the progress time of facets fading and hidden duration on their

DOI: rp-9788770040723.170

own for strengthening shoulder surfing resilient. In pure standard evolving time, fading and hidden time are fixed that cannot be altered by the user. In pure user config evolving time, user set both fading and hidden time. In a combination of standard and user config evolving time, either user can change the fading time or invisible time as given in Eqn 1, 2, 3 and 4. We conducted an experiment with a different age group between 21 and 70, and Table 1 shows the observedresult.

$$\phi_s(1) = £_{sf} + £_{si} \quad (1)$$

$$\phi_u(2) = £_{uf} + £_{ui} \quad (2)$$

$$\phi_{su}(3) = £_{sf} + £_{ui} \quad (3)$$

$$\phi_{us}(4) = £_{uf} + £_{si} \quad (4)$$

1) Φs(1purestandardevolvingtime
2) Φu(2pureuserconfigevolvingtime
3) Φsu (3 , φus (4 combination of standard and user config evolvingtime.
4) $£_{sf}$- standard fadingtime.
5) $£_{si}$- standard hiddentime.
6) $£_{uf}$- user config fadingtime.
7) $£_{ui}$- user config hidden time.

TABLE I: THE PERCENTAGE OF USERS FOR EVOLVING TIME SETTING

Age	$\phi_s(1)$	$\phi_u(2)$	$\phi_{su}(3)$	$\phi_{us}(4)$	Total user
21 - 30	1%	91%	5%	3%	99%
31 - 40	11%	78%	6%	5%	89%
41 - 50	23%	57%	12%	8%	77%
51 - 60	34%	33%	22%	11%	66%
61 - 70	55%	21%	15%	9%	45%

IV. EXPERIMENT ANALYSIS - USABILITY AND SECURITY

Hackersusevarioustechniquestocrackpasswords.Inthisse ction, the most common prevailing cracking schemes are tested with FacetPass and described below. Table 2 indicates the evaluation of the space for password of proposed and related schemes while it is applied in mobile devices. It shows that intruders must dissipate more duration to find the correct count of touch and swaps. In Evopass, Selection of pass images from their private image increases the difficulty of mounting dictionary attacks [16]. In Facetpass, user's face capturedbyacameraofthedeviceautomaticallythathelpsto improve the ability to withstand against a dictionary attack. As a result of this experiment, we came to know most of the users selected 3-6 facets for their registration which increases the difficulty to crack the passwords with limited possibilities.

A. Touch and swap operations

The participants are classified according to their age and designation. Table 3 and 4 shows information about the number of touch and swap based on their age and category. The younger participants used a large number of tapsand swappingcomparewiththeagedpeople.Theparticipant'sages from 21 to 30 and 31 to 40 used 4-9, 3-9 touches and 5-9, 3-7 swapsrespectively.Ontheotherhand,elderparticipantsuse3-4 taps and 3-5 swapping. In the designation category, students use 4-9 touches 6-9 swapping, and the senior people use 3-6 and 3-5 touches and swaps respectively. When compare with students, elder participants are not comfortable with touchand swapping in smart devices. The result of this experiment concludes that the number of taps and swaps usage varies for different age group anddesignation.

TABLEII EVALUATION OF PASSWORD SPACE

TABLE III: TOUCH AND SWAP OPERATIONS BASED ON AGE.

Age	No. of Touches	No. of Swaps
21 - 30	4 - 9	5 – 9
31 - 40	3 - 9	3 – 7
41 - 50	3 - 6	3 – 6
51 - 60	3 - 4	3 – 5
61 - 70	3 - 4	2 – 3

TABLE IV: TOUCH AND SWAP OPERATIONS BASED ON DESIGNATION

Designation	No. of Touches	No. of Swaps
Students	4 - 9	6 – 9
Teachers	4 - 8	5 – 8
Officers	5 - 7	5 – 9
Home Makers	3 - 8	5 – 7
Senior People	3 – 6	3 – 5

V. CONCLUSION

FacetPass, a novel graphical password to increase authentication for a user to gain access to a device, application or website in smart devices is proposed. To raise the password space and avoid attacks such as Brute-force assault, guessing, shoulder surfing, smudge and dictionary attacks, it incorporates recall and biometric-based GP. This proposed system is easy to use and recall than existing graphical password systems, and the user can handle facets for touch and swap manipulation effortlessly. A lab experiment was conducted with 113 participants to calculate time consumption and usability of FacetPass in diverse angle. Thus the result shows that this FacetPass is secured and user - friendly. In future, we are interested to construct this FacetPass working against spoofing attack with the standard algorithm.

REFERENCES

[1] J. Long, S. Pinzon, J. Wiles, and K. D. Mitnick, "Dumpster diving," 2008, pp. 1–12.

[2] Q. Yan, Y. Li, J. Han, J. Zhou, and R. H. Deng, pp. 196–211, 2015.

[3] P. L. Chithra and K. Sathya, "A Novel Password Encryption Using Wedges Algorithm with QR Code," Intern J of Pure and App Math, vol. 119, no. 7, pp. 857–861, 2018.

[4] Gomathy, V., Janarthanan, K., Al-Turjman, F., Sitharthan, R., Rajesh, M., Vengatesan, K., &Reshma, T. P. (2021). Investigating the spread

of coronavirus disease via edge-AI and air pollution correlation. ACM Transactions on Internet Technology, 21(4), 1-10.

[5] A. D. Angeli, L. Coventry, G. Johnson, and R. K, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," Int. J.Hum.-Comput. Stud, vol. 63, pp. 128–152, 2005.

[6] S. Azad, M. Rahman, M. S. A. N. Ranak, B. M. F. K. Ruhee, N. N. Nisa, N. Kabir, and A. Rahman, "Vap code:A secure graphical password for smart devices," Mohamad Zain J, vol. 59, pp. 99–109, 2017.

[7] D. Kim, P. Dunphy, P. Briggs, J. Hook, F. Kianoush, J. W. Nicholson, and J. Nicholson, "Multitouch authentication on table tops," in Proceed of the SIGCHI confer on human factor in comput systs (CHI). ACM, 2010, pp. 1093–102.

[8] Rajesh, M., &Sitharthan, R. (2022). Introduction to the special section on cyber-physical system for autonomous process control in industry 5.0.Computers and Electrical Engineering, 104, 108481.

[9] T. J. Wixted, "The psychology and neuroscience of forgetting," Annu Reviw of Psychol, vol. 55, pp. 235–269, 2004.

[10] Y. Meng, "Designing click-draw based graphical password scheme for better authentication, Proceed of IEEE intern confer on network, architec, and stora," NAS, pp. 39–48, 2012.

[11] G. Blonder, "Graphical passwords," U.S.Patent, vol. 5, pp. 961–961, 1996.

[12] J. Wei, X. Hu, and W. Liu, "Two-factor authentication scheme using at- tribute and password," International Journal of Communication Systems, vol. 30, no. 1, 2014.

[13] J. Wiedenbeck, Waters, Jean-Camille, A. Birget, Brodskiy, and

N. Memon, "Passpoints: Design and longitudinal evaluation of a graph- ical password system," Int. J. Hum-Compu Studi, vol. 63, pp. 102–127, 2005.

[14] S. Chiasson, P. C. V. Oorschot, and R. Biddle, "Graphical password authentication using cued clickpoints," in Proceedings of the 12th European sympos on research in comput securi (ESORICS). Springer, 2007, pp. 359–174.

[15] E. Hayashi, R. Dhamija, N. Christin, and A. Perrig, "Use your illusion: secure authentication usable anywhere," Sympo on Usabl Privac and Securi, pp. 35–45, 2008.

[16] X. Yu, Z. Wang, Y. Li, L. Li, L. W. T. Zhu, and Song, pp. 179–198, 2017.