ISSN: 2836-8495

Research Article

Journal of Current Trends in Computer Science Research

SEC-SKETCH: A Secret-Sketch Graphical Authentication System

Elugbadebo Oladapo Joseph[1], Johnson Femi Temitope[2*] and Akande Adenike Folasade[1]

[1]*Computer Science Department, Federal College of Education, Abeokuta, Nigeria*

[2]*Computer Science Department, Federal University of Agriculture, Abeokuta, Nigeria*

[*]Corresponding Author
Johnson Femi Temitope, Computer Science Department, Federal College of Education, Abeokuta, Nigeria.

Submitted: 2024, Aug 13; **Accepted**: 2024, Sep 16; **Published**: 2024, Oct 01

Citation: Joseph, E. O., Temitope, J. F., Folasade, A. A. (2024). SEC-SKETCH: A Secret-Sketch Graphical Authentication System. *J Curr Trends Comp Sci Res, 3*(5), 01-09.

Abstract

Graphical authentication is being widely accepted as a collaborative and an alternative to textual password authentication systems because it has reasonably solved the problem of memorability. However, the present graphical authentication system does not provide efficient security for the systems. In this paper, a Secret-Sketch graphical authentication system (SEC-SKETCH) is proposed to enhance the security of computer and network-based systems. It encompasses three states for its completion commencing from registration to login and authentication phases. Criteria such as Threshold and Percentage Accuracy which provide strong resistance to hidden-camera and shoulder attacks are complemented in the mode of analysis. To assess how effective and user-friendly the suggested system is, a demo system that utilizes traditional recall techniques like Passdoddle, Quantitative Draw-A-Secret (QDAS), Syukri, and Draw-A-Secret (DAS) is developed and then compared with the SEC-SKETCH scheme. The experiment showed that SEC-SKETCH performed the best with 0.10% FNMR, 0.15% FMR, and 0.02% EER compared to all other recall-based technique.

Keywords: Security, Graphical Authentication, Pattern Matching, Features Extraction, Threshold, Security

1. Introduction

The use of secret keys provided by users upon request with specific usernames has been one of the oldest and most common authentication methods in both online and offline systems. Often, they are stored in an encrypted form on servers so that a penetration of the file system does not reveal password lists [1]. Systems with weak passwords are vulnerable to dictionary attacks and brute force attacks whereas strong passwords are harder to remember. In password-authenticated systems, a correct pair (username and password) grants access to the system's services or resources [2]. Unfortunately, passwords are susceptible to several vulnerabilities and drawbacks [3]. Its shortcoming ranges from user-selected weak or easily guessable passwords to more sophisticated threats such as malware and keyboard sniffers [4]. Despite these shortcomings, usernames and passwords still present a major form of authentication [5].

Over the years, the computer industry has continuously been in a quest for better alternatives techniques have been proposed for enhancing the security of the information and system, such as employing multifactor authentications which allow two or more independent factors to be used as part of user credentials. However, most of our current systems still use primitive text-based authentication [6-9]. To amend some of the shortcomings of the textual passwords, researchers turned their attention to passwords that utilize graphical objects [10,11]. Graphical authentication has been proposed as a user-friendly alternative to password generation and authentication. Having two or more factors strengthens security but complicates the authenticating process [12]. More specifically, two-factor authentication has been with us for quite some time. Popular examples of two-factor authentication systems are the ATMs used for financial transactions which allow the user to have a bank-issued card (credit or debit card) and a personal identification number (PIN).

This paper focuses on the development of a Secret-Sketch graphical authentication system" (SEC-SKETCH) which combines recognition (username and textual passcode) and recall-based techniques (Sketching of an image). The SEC-SKETCH scheme allows the user to use a canvas of an orthogonal matrix (using

Principal Component Analysis) to draw an image as a password. A sketch-based graphical authentication system is introduced for the user to provide a higher level of security without compromising user convenience. It also aims to provide a large, full graphical password space, and more importantly, increase the memorability of the users. To support the ability for memorization, the image drawn should be of meaningful content because meaning for arbitrary things is lacking in most humans.

The rest of this paper is organized as follows: Section 2 reviews and discusses the related work on graphical passwords. In Section 3, the proposed architecture of the Methodology which includes the recognition phase, the Login phase, and the authentication phase is displayed. The algorithm and authentication requirement is also introduced in this section. Section 4 presents the experimental results of this paper and compares them with those of other related studies. At the same time, the performance of the proposed system is also presented. Finally, the Conclusion and Future works are given in Section 5.

2. Related Work

Several works have been performed by researchers on securing and authenticating users' access to the system's resource utilization. According to Curran and Doyle human brains function better in recalling or recognizing images than text or words. Moreover, the recall process of human memory could be enhanced by using images or pictures as a means of authentication rather than strings or texts [13,14]. Based on this notion the idea of graphical passwords for authentication was proposed to overcome limitations with text-based password systems. The first graphical password substitute was introduced by Greg, based on the notion that people can remember images better than words or text. Although a recognition-based graphical password is easy, which increases the usability it requires several rounds of image recognition for authentication to provide a reasonably large password space, which was tedious [3,15,16]. Guodong et al., proposed a logistic-tent map reduction algorithm to produce a confusion sequence on plain images which enabled the compression and encrypting of cipher images with a randomly generated set of numbers based on a calculated compression ratio. The confusion sequence helps to generate secured encrypted secret images that can be used for authentication.

Vishal et al. implemented a modified intuitive approach to graphical password authentication systems, where users can select a sequence of click-points on an image as their password for an easier authentication process. This was in response to the growing interest in graphical authentication techniques. Convolution sliding scrambling based on chaotic sequences (PCSS-CSDP) was used by Zhihua et al [18]. to break down encrypted images into shadow images and remove pixel correlations [19]. This made their suggested model even more capable of identifying and encrypting sensitive from non-sensitive data in plain pictures. Information security was improved through a level cyclic shift and dynamic combination (AS-BCSDC) authentication system and the IWT-M-embedding technique, which embeds shadow pictures into carrier images.

Jonathan proposed a graphical password scheme that could classify the randomly generated password into three groups, the first group used text-based passwords the second group was given a static visual palette to enter the randomly assigned password the third group used the entry method that incorporates random synonym images to enter the randomly assigned password [20]. Researchers in adopted the cued recall-based techniques for authentication. Bhat et al [21]. investigated the use of a polynomial-based encryption/decryption system in conjunction with visual LAMSIS (lossless authenticated multiple secret image sharing) cryptography as a means of implementing one-time authentication to deter user fraud [22]. The results of an experimental analysis demonstrated that the quantity of images shared through this strategy is either the same as or less than the total amount of shares produced by any broad method of sharing one hidden image at a time. Bin et al, created a way to secure data from steganalysis. They worked on developing an authentication method and secure transmission by compressing picture data [23]. To create an N-multi-segmented cipher picture, which can only be recovered when the recipient receives an equal amount of segmented cipher images, secret images were inserted with the least significant bit. Image corruption will, nevertheless, always result from even a slight interruption or delay in the transmission frequency. Sivrajani et al. developed a graphical password authentication system that effectively blocks common attacks including dictionary and brute force attacks, safeguarding financial and personal data against breaches and cyber-attacks [24]. Attackers are likely to intensify their efforts to compromise desktop and mobile systems in response to the steadily rising usage of mobile phones and other devices.

Another technique known as the Grid selection technique was proposed by Thorpe and Van to enhance the password space of DAS [1]. Their study showed the impact of stroke count on DAS password space which decreases significantly with fewer strokes for a fixed password length. To improve the DAS security level, they suggested the "Grid Selection" technique, where the selection grid is large at the beginning, a fine-grained grid from which the person selects a drawing grid, a rectangular area to zoom in, in which they may enter their password. There have been notable developments in graphical authentication systems since 2022. The integration of graphical passwords with blockchain technology was proposed by Shinde et al., and Deshmukh [25,26]. Adopting blockchain and IPFS technologies, they presented a Visual-D-Auth, an authentication platform that provided safe access via the Decentralized Single Sign-On (DSSO) method. Their study used a novel graphical password-generating technique that produced extremely secure passwords and Deshmukh focused on tamper-proof records for decentralized authentication [25].

To give Smartphone users safe authentication, Loganathan et al., suggested developing an Android app using grid-based, picture-based, graphical password authentication [27]. Using Java programming in Android Studio and flowcharts, the app was developed in five sections. It performed better than other graphical password types in terms of predictability, usability, and attack resistance. Together, these studies demonstrate how graphical

authentication systems can improve the user experience and security. Priti developed a secured image-based three-factor user authentication system, moving away from a single technique for user authentication [28]. Jebakumar et al. also included a three-layered security mechanism that makes it extremely difficult for attackers to figure out or limit the password, even with repeated camera-based hacking attempts for their system [29].

3. Methodology

In this section, a Secret-Sketch (SEC-SKETCH) graphical authentication system is proposed and discussed. The SEC-SKETCH approach uses a combination of both recognition and pure recall-based scheme. The implementation of SEC-SKETCH allows the image to be sketched with the user's finger on a free-hand mouse with a template template-matching method of analysis used which shows an improvement on the approaches adopted by the existing schemes. This template matching approach used by SEC-SKETCH places emphasis on the order of pixels' stroke length and their coordinate's location as its priority to be considered before any access can be granted to any user. Another SEC-SKETCH area of improvement over the existing pure similar techniques was the introduction of criteria such as "Threshold and Percentage Accuracy" which invariably makes the SEC-SKETCH scheme more secure and usable compared to the existing systems. The algorithm, architecture, and requirements for implementation are also described below.

The Model Architecture

The architecture of SEC-SKETCH showing the basic blocks involved in authenticating a user is depicted in Figure 1. The proposed system comprises three phases (the registration the Login and Authentication). The first step in the REGISTRATION process requires the user to choose a text password and username. Next, using a finger or a free-hand mouse as a graphical password, the user can construct an image on a canvas of GXG coordinate pairs of grid cells. A series of inconsistent input or sketches supplied by the user during the registration phase is aggregated through the different data points around the coordinates to generate a series of points that can be used for authentication.

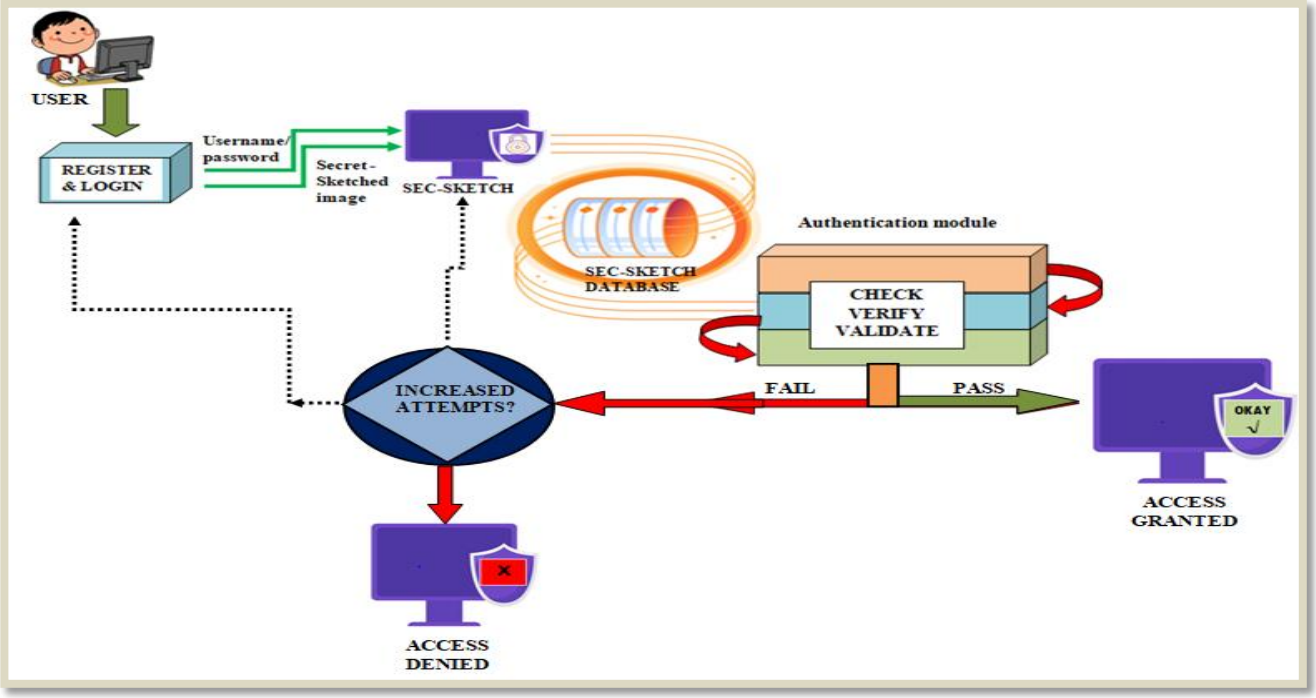

Figure 1: The Proposed Secret-Sketch (SEC-SKETCH) Architecture

The SEC-SKETCH administrator receives the username, text password, and secret drawing from the user ensuring their safety. In the second stage, known as the "LOGIN phase," the user provides their username, text password, and graphical password, which was created by drawing a symbol in the same manner as in the previous phase. The SEC-SKETCH access module will receive the credentials during the third phase, known as the authentication phase, and use them to perform calculations depending on the designated system threshold including the number of matched pixels, the location of the drawing on the canvas, the dimension of sign drawn on G x G coordinates pairs and the degree of tolerance before access could be granted or denied.

Algorithm for Secret-Sketch Architecture Registration Phase:

i. User (ui) submits registration request (username and password) to server (S).

ii. Server (s)checks the availability of received IDS and displays canvas for the user

iii. User(ui) creates and submits a secret sketch sign with a free-hand mouse on a grid canvas comprises of GXG coordinate pairs

iv. Upon receipt of h(Pwi), S accept SEC-SKETCH(n) based on the specified Threshold (k)and percent accuracy (j).

v. S creates and compares user profiles with user ID portfolio image, and stores them in the knowledge database before he can be recognized as registered user.
vi. Ui request login
vii. Upon receipt of the login request, the server sends the login page along with server's Digital certificate containing its public key.
viii. User suppliesID, the client computersPwi=kn,jn,f(n); checks whether Pwi* equals Pwi (k,j,f) that are already stored in the knowledge database; if valid it generates random secret "Pi".*
ix. It then computes Ri=h (IDi)+h(Pi); Encrypts Ri,Pi and Pwi using server's public key as Si=EkUs (Ri,Pi,Pwi) and sends Si to server.
x. Upon receipt of Si; server decrypts it using its private key as DkPs (Ri,Pi,Pwi).

Authentication Phase:

xi. The server(S) verifies user(ui) as mathematically represented Kn< K
(is user's threshold less than or equal server threshold)
xii. Jn < j(is user's percentage accuracy less than or equal server P. A)
xiii. f(n)<3
(is users drawing attempt less than or equal 3)
vii. If the validated sign is correct, it will be accepted and takes the user directly to the application.
viii. If the validated sign is incorrect, it rejects the login request, then both user and server proceeds to compute f(n) by increasing the number of failures for three times after which the system exit and the authentication process is terminated.

Additional Requirements and Algorithms for SEC-SKETCH System.

Deciding the genuine authentication attempt in the SEC Sketch, a template is developed for each user of the proposed system and validated based on the selected threshold and accuracy.

1. Threshold

The distance between one pixel to another, and the location of the pixel in the sign drawn during the registration phase are compared with those from an authentication phase. This is to be able to decide whether the distance is lower than the stipulated threshold in the database which is invariably considered as a genuine attempt. Contrarily, if the distance is farther, the stipulated threshold in the database is considered an impostor attempt.

Running the simulations of authentication attempts, an algorithm that chooses a random template that compares genuine and impostor attempts is used. This algorithm calculates the distance of genuine and impostor attempts against each randomly chosen template and sorts them in two arrays. One contains the genuine attempts and their distances to the template and the other contains impostor attempts and their distances to the template.

The two thresholds selected were high and low, meaning that all legitimate users are permitted and rejected. The percentage of legitimate attempts denied access known as the False Non-Match Rate (FNMR) is computed for each level as mathematically represented in Equation 1. Equation 2 calculates the value of the impostor fraction that managed to get access to the system known as the False Match Rate (FMR).

$$FNMR = \frac{number\ of\ denied\ genuine\ attempts}{total\ number\ of\ genuine\ attempts} \ldots\ldots\ldots\ldots\ldots (1)$$

$$FMR = \frac{number\ of\ allowed\ impostor\ attempts}{total\ number\ of\ impostor\ attempts} \ldots\ldots\ldots\ldots\ldots (2)$$

A. Threshold computation algorithm

```
for i\=i to n to n
create mi for ui
 for ui^' s∉mi do
if u^' s∉mi then
 for m∉mi do
Calculate 1dp
calculate 1dp∉atempt vs m
if smi∉ui & // then
 store du^' p∉mi as gen attempt
Else
store du^' p as imp attempt
end if end
 for end if end
for
end for
```

B. Percentage Accuracy Check Algorithm

```
If (img1.width == img2.width
AND img1.height == img2.height)
   for I = 0 to img1.width
     for j = 0 to img1.height
       begin
          if (px1==px2)
                match = match + 1;
          else
               unmatch = unmatch + 1;
          next j,
                Next i
                end;
```

2. Percentage Accuracy

From the total number of pixels in the sign drawn by the user during registration, a certain number of pixels must be matched or correlated with the one made during the authentication stage. This is done based on the user's specifications to determine whether the user is genuine or not. The P.A. algorithm considered whether the number of pixels of the sign drawn on the two templates (i.e. registration and authentication) by the user are similar and determines if the number of matched pixels meets up with the number specified by the user during registration in the database. If the number of matched pixels still falls within the range of users' specifications, it is considered a genuine attempt; otherwise, it is taken as an impostor attempt. The percentage of matching criteria

is calculated using equations 3 and 4.

NOTATION	MEANING
$Ui\ (useri)$	$An\ individual\ user\ interacting\ through\ the\ system\ with\ the\ server\ for\ access\ granting\ or\ denying\ (Individual\ User)$
ID	$User\ Identity$
$h(IDi)$	$Unique\ User\ Identity$
S	$Server$
$Client$	$Users'\ Computer\ System$
Pwi	$Password\ stored\ in\ the\ Server\ database$
$Pwi*$	$Password\ supply\ through\ client\ computer\ during\ login$
K	$Threshold\ stored\ in\ the\ server\ database$
$K*l$	$Threshold\ used\ for\ client\ computer\ during\ login$
j	$Percentage\ accuracy\ stored\ in\ the\ server\ database$
$j*$	$Percentage\ accuracy\ used\ for\ the\ client\ computer\ during\ login$
F	$Users'\ signed\ drawn\ stored\ in\ the\ server\ database$
$f*$	$Users'\ signed\ drawn\ supply\ through\ client\ computer\ during\ login$
Pi	$A\ server\ randomized\ user's\ password\ secret$
$h(pi)$	$Unique\ user\ random\ secret$
Ri	$User's\ request$
Si	$Server's\ public\ Key$
$EKUs$	$Encrypted\ User's\ key$
$\mathrm{Kn}Kn \leq K$	$Is\ users'\ threshold\ less\ than\ or\ equal\ server\ threshold$
$Jn \leq J$	$Is\ users'\ threshold\ less\ than\ or\ equal\ server\ threshold$
$f(n) \leq 3$	$Is\ users'\ sign\ drawing\ attempt\ less\ than\ or\ equal\ 3$
$DKPs$	$Decrypted\ server's\ private\ key$

Table 1: Algorithm Notations and their Meanings

The second algorithm checks the two images to see if they are dimensionally equal i.e. height-wise and width-wise. If the two images are dimensionally equal, it goes by iterating over each pixel on both images. At each pixel (px) i=0, j=0, i=n, j=m, it checks if pxi1 equals pxj2. If pxi1 equals pxj2, it implies no difference in both images at that particular pixel. However, if pxi1 is not equal to pxj2, it implies that both images are different at that particular pixel. The calculation of percentage accuracy is described in Equations 3 and 4 with their corresponding matching criteria.

$$Percentage\ Accuracy\ (PA) = \frac{T-UM}{T} x\ 100\% \quad .....(3)$$

Where
UM = Number of Unmatched Pixels and
T = Total number of pixels of an image or written as Percentage Accuracy
(PA)= M/T x 100% ..... (4)

Where
M = T – UM and M is the number of Matched Pixels

The matching criteria are;
i. If PA =100, this implies case 1 i.e. both images are the same
ii. If PA <= 0, this implies case 2, i.e. both images are totally different.
iii. If 0< PA < 100, this implies case 3, i.e. both images are slightly the same or different.

4. Result and Discussion

To evaluate the efficiency of SEC-SKETCH, an experiment involving 200 participants from the Federal College of Education, Abeokuta, Ogun State, Nigeria was carried out for each technique. Computer literates were specially selected, they were given a demonstration for better understanding purposes and users were requested to log in after which the usability test was conducted with the participants in three sessions. The sessions were conducted in a time frame of one week taking into consideration, the FNMR, FMR, and EER. Figure 2 presents the interface of the SEC-SKETCH system.

Performance and Evaluation Analysis of SEC-SKETCH System

The performance analysis of this SEC-SKETCH system was measured based on the recognition error rates, which are defined as follows

i. False Non-Match Rate (FNMR): the rate at which the system rejects a legitimate user. FNMR is also called Type I error.
ii. False Match Rate (FMR): the rate of the system accepting an impostor. FMR is also called Type II error.
iii. Equal Error Rate (EER): the value at which FMR equals FNMR. This is the most balanced performance index.

Furthermore, a demo version of popular pure recall-based techniques, including passdoddle, Quantitative Draw-A-Secret (QDAS), Syukri, and Draw-A-Secret (DAS), were developed and compared with the SEC-SKETCH system to assess the

effectiveness and usability of the SEC-SKETCH among two hundred randomly selected computer users. Special attention was paid to the false non-match rate (FNMR), false match rate (FMR), and equal error rate (EER). The results obtained are depicted in Figures 3 to 6.

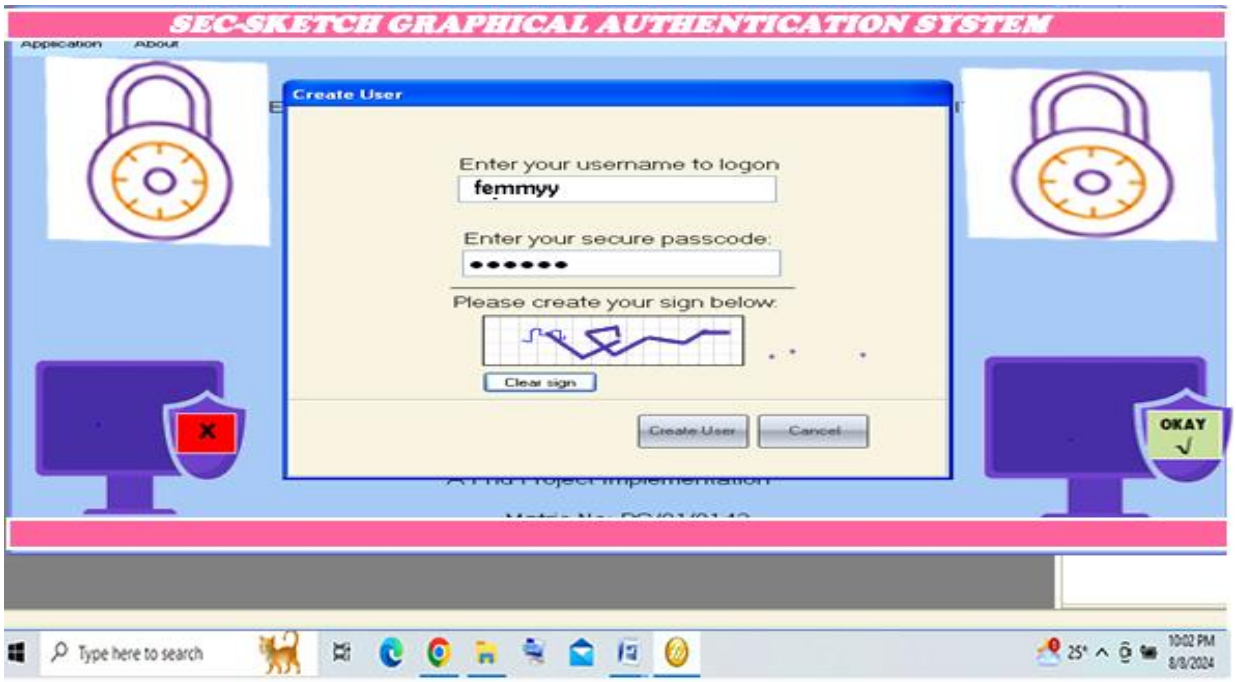

Figure 2: User Interface of SEC-SKETCH System

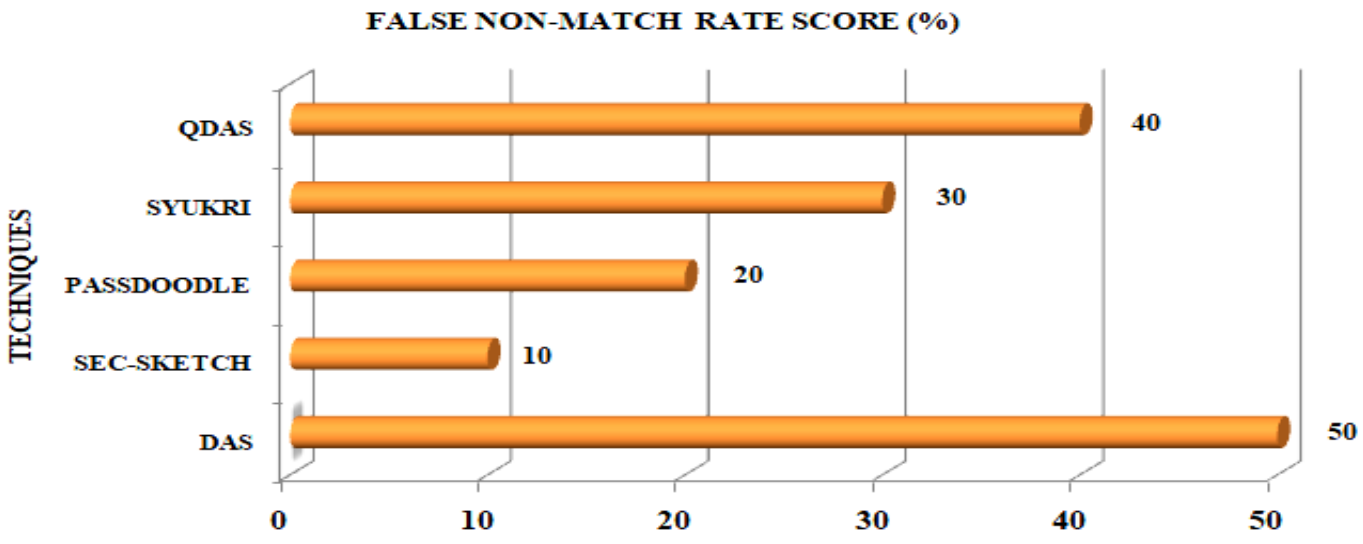

Figure 3: User interface of SEC-SKETCH system

The FNMR performance analysis session for every pure recall-based method is shown in Figure 3. It illustrates the performance level of each approach. Among all the pure recall-based techniques in use, DAS has the lowest performance measurement at 50%, followed by 20% for Passdoodle, 30% for Syukri, 40% for QDAS, and 10% for SEC-SKETCH which indicates the highest performance measurement level.

Figure 4 shows the results of each pure recall-based technique's FMR performance analysis session. The chart illustrates the effectiveness of each tested technique. It reveals that Passdoodle has the lowest performance measurement at 50%, Syukri at 40%, DAS at 30%, QDAS at 25%, and SEC-SKETCH at 15% for all the pure recall-based approaches.

Figure 5 shows the outcome of calculating the Equal Error Rate, which is a function of both FNMR and FMR, using data gathered from people who participated in experiments. It shows the error

rate performance level of each technique and reveals that Syukri has the lowest performance measurement at 6.5%, followed by passdoodle at4.5%, DAS at 4%, QDAS at 3%, and SEC-SKETCH at 2%. This indicates that SEC-SKETCH has the best error rate performance measurement level when compared to all other techniques, and has the most optimally balanced threshold for the system. To have a detailed and holistic view of the evaluation results for the SEC-SKETCH, the information in Figure 6 is also presented.

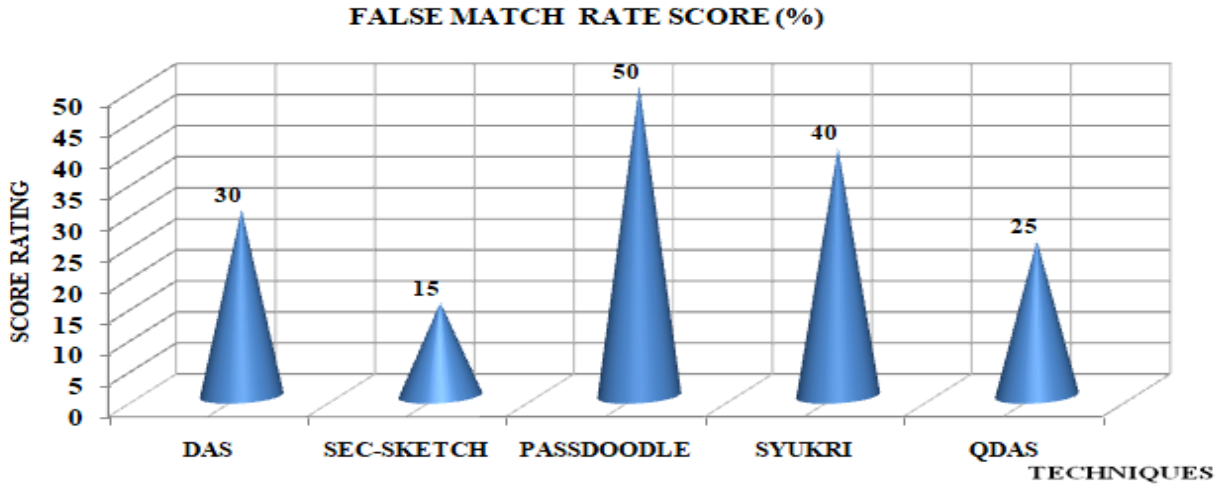

Figure 4: False Match Rate

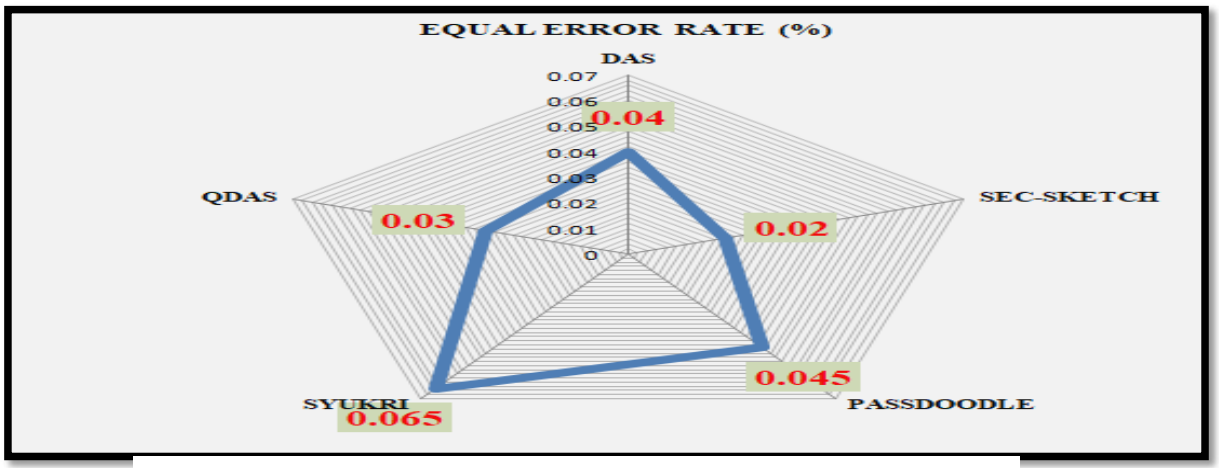

Figure 5: Equal Error Rate

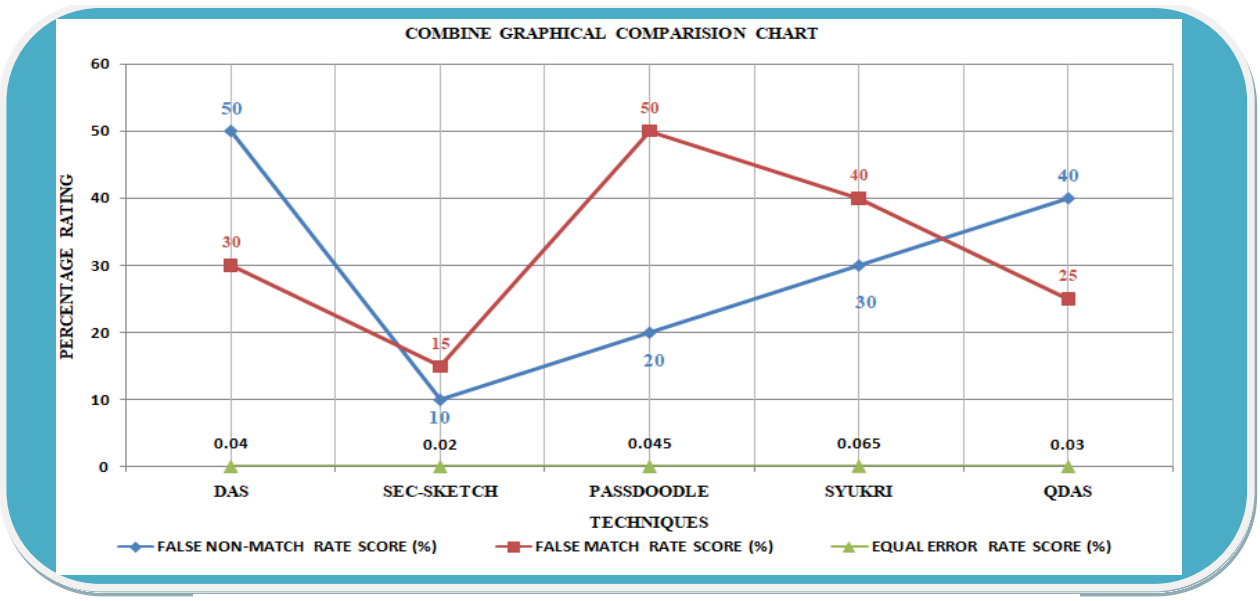

Figure 6: Performance Metrics of SEC-SKETCH

5. Conclusion and Future Work

A developing trend in the last ten years has been graphical passwords as an alternative to conventional text-based passwords. This study proposes a SEC-SKETCH system, which offers higher security than comparable graphical authentication methods and text-based systems. Despite the justification that graphical passwords are easier to remember than text-based passwords there is currently a paucity of user research and strong evidence to bolster this claim.

According to our preliminary investigation, employing conventional attack techniques like dictionary attacks, brute force searches, or malware to crack graphical passwords is more challenging. By utilizing the user's ability to recall images and the memory trigger associated with patterns of newly drawn images, the developed SEC-SKETCH technique shows great promise as a valuable, usable, and memorable authentication mechanism for securing systems resources. In terms of usability and memorability, SEC-SKETCH has an advantage over other similar schemes.

In addition, the results of the performance analysis conducted in this paper utilizing the template matching approach, which includes the FNMR, FMR, and EER features, users overwhelmingly preferred SEC-SKETCH than other similar authentication techniques.

Future research should encompass a comprehensive evaluation of SEC-SKETCH's deployment as an authentication mechanism in mobile and low-memory- devices encompassing an extended examination of the practical implementation and the potential use of lengthier SEC-SKETCH generated passwords. A more thorough analysis of SEC-SKETCH's security is warranted since it should tackle potential avenues for attackers to leverage the creation of hotspots. Conclusively, more research should be done to identify the multiple time-based attacks that target graphical authentication systems.

References

1. Hua, Z., Zhang, K., Li, Y., & Zhou, Y. (2021). Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing. *Signal Processing, 183,* 107998.
2. Almuairfi, S., Veeraraghavan, P., & Chilamkurti, N. (2013). A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices. *Mathematical and Computer Modelling, 58*(1-2), 108-116.
3. Greg E. B (1996). "Graphical Password", U.S. Patent No. 5559961.
4. Johnson, F. T., Joseph, E. O., & Akande, A. F. (2024). Security Concerns in Electronic Files Authenticated Systems. *COJ Rob Artificial Intel, 3*(3), 1-8.
5. Bhavana, A., Alekhya, V., Deepak, K., & Sreenivas, V. (2013). Password authentication system (PAS) for cloud environment. *International Journal of Advanced Computer Science and Information Technology, 2*(1), 29.
6. Devika, S., & Backiyalakshmi, R. (2014). Design and analysis of user identification for graphical password system. *IJCSIT, 16*(4), 369381.
7. Yan, X., Lu, Y., Yang, C. N., Zhang, X., & Wang, S. (2020). A common method of share authentication in image secret sharing. *IEEE Transactions on Circuits and Systems for Video Technology, 31*(7), 2896-2908.
8. Luo, Y., Lin, J., Liu, J., Wei, D., Cao, L., Zhou, R., ... & Ding, X. (2019). A robust image encryption algorithm based on Chua's circuit and compressive sensing. *Signal Processing, 161,* 227-247.
9. Sabzevar, A. P., & Stavrou, A. (2008, November). Universal multi-factor authentication using graphical passwords. In *2008 IEEE international conference on signal image technology and internet based systems* (pp. 625-632). IEEE.
10. Shaikh, J., Pawar, C. C., Jadhav, V. S., & Sindhu, M. R. (2015). User authentication using graphical system. *Progress*

in Science and Engineering Research Journal, 17(3), 56-61.
11. Wen, W., Hong, Y., Fang, Y., Li, M., & Li, M. (2020). A visually secure image encryption scheme based on semi-tensor product compressed sensing. *Signal Processing, 173*, 107580.
12. Wang, J., Zhang, L. Y., Chen, J., Hua, G., Zhang, Y., & Xiang, Y. (2019). Compressed sensing based selective encryption with data hiding capability. *IEEE Transactions on Industrial Informatics, 15*(12), 6560-6571.
13. Curran, T., & Doyle, J. (2011). Picture superiority doubly dissociates the ERP correlates of recollection and familiarity. *Journal of Cognitive Neuroscience, 23*(5), 1247-1262.
14. Lashkari, A. H., Saleh, R., Towhidi, F., & Farmand, S. (2009, December). A complete comparison on pure and cued recall-based graphical user authentication algorithms. In *2009 Second International Conference on Computer and Electrical Engineering* (Vol. 1, pp. 527-532). IEEE.
15. van Oorschot, P. C., & Thorpe, J. (2011). Exploiting predictability in click-based graphical passwords. *Journal of Computer Security, 19*(4), 669-702.
16. Vishal, S.R. and Amol, D.G. (2014). *Analysis of Graphical Based password.International Journal of Engineering Research and Application (IJERA).* ISSN; 2248-9622, pp.1-5
17. Ye, G., Pan, C., Dong, Y., Shi, Y., & Huang, X. (2020). Image encryption and hiding algorithm based on compressive sensing and random numbers insertion. *Signal processing, 172,* 107563.
18. Vishal, S.M., Pravin, S.M., Yashraj,M.P., Siddhesh,K. (2023). Graphical Password Authentication Using Blockchain Technology. International Research Journal of Modernization in Engineering Technology and Science. Pp.991-999.
19. Gan, Z., Song, S., Zhou, L., Han, D., Fu, J., & Chai, X. (2022). Exploiting compressed sensing and polynomial-based progressive secret image sharing for visually secure image selection encryption with authentication. *Journal of King Saud University-Computer and Information Sciences, 34*(10), 9252-9272.
20. Sparks, J. W. (2015). *The Impact of Image Synonyms in Graphical-Based Authentication Systems* (Doctoral dissertation, Nova Southeastern University).
21. Masrom, M., Towhidi, F., & Lashkari, A. H. (2009, October). Pure and cued recall-based graphical user authentication. In *2009 International Conference on Application of Information and Communication Technologies* (pp. 1-6). IEEE.
22. Bhat, K., Reddy KR, U. K., Kumar HS, R., & Mahto, D. (2021). A novel scheme for lossless authenticated multiple secret images sharing using polynomials and extended visual cryptography. *IET Information Security, 15*(1), 13-22.
23. Wu, B., Xie, D., Chen, F., Wang, X., & Zeng, Y. (2022). A multi-party secure encryption-sharing hybrid scheme for image data base on compressed sensing. *Digital Signal Processing, 123,* 103391.
24. Sivaranjani, N., Sanjana, P., Sindhubairavi, S., & Saishrre, L. (2024, February). Graphical Password Authentication using Image Processing (GPAIP). In *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 185-191). IEEE.
25. Shinde, R. D., Jathar, K. R., Pardeshi, A. D., & Thorat, S. A. (2023, July). Graphical Password Authentication Using Decentralized Single-Sign-On. In *2023 World Conference on Communication & Computing (WCONF)* (pp. 1-9). IEEE.
26. Deshmukh, P.S , Manish D. , Atharv G. , Dipesh G., Sarthak W.,(2024), Graphical Password Authentication using Blockchain. International Journal for Research in Applied Science and Engineering Technology. Volume 12 Issue IV,pp. 1-8
27. Loganathan D., Umme K., Shakthi S. , Sania M. , and Arbaz A., (2023). Graphical Password Authentication: Image Grid Based Digital Lock for Mobile Apps. International Journal for Research in Applied Science and Engineering Technology. Volume 11, Issue V, pp.1-18.
28. Golar, P., & Sharma, R. A secured image based three factor user authentication system.
29. Ramalingam, V., Iyer, A., & Narayanan, M. S. (2023, June). Resisting Visual Hacking: A Novel Graphical Password Authentication System. In *2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN)* (pp. 910-915). IEEE.

Copyright: *©2024 Johnson Femi Temitope, et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.*