Iraqi Journal of Information and Communications Technology(IJICT)
Vol. 6, Issue 1, April 2023

www.ijict.edu.iq

ISSN:2222-758X
e-ISSN: 2789-7362

PASS POINT SELECTION OF AUTOMATIC GRAPHICAL PASSWORD AUTHENTICATION TECHNIQUE BASED ON HISTOGRAM METHOD

Safa F. Abbas[1], **Lahieb M. Jawad**[2]
[1,2] College of Information Engineering, Al-Nahrain University, Baghdad, Iraq
Safaaf.abbas@gmail.com[1], lahieb.moh@coie-nahrain.edu.iq[2]
Corresponding Author: Lahieb M. Jawad
Received:13/5/2022; Revised: 04/08/2022; Accepted:16/10/2022
DOI:10.31987/ijict.6.1.212

***Abstract*- Graphical passwords, as opposed to textual passwords, require the user to pick pictures or draw symbols rather than input written letters. They are an option that may be explored in order to get over the issues that are caused by the system of passwords that are based on text. It has been hypothesized that graphical passwords are more difficult to crack using a brute force technique or to figure out through guessing. This paper proposes an authentication system based on a graphical password method. The proposed system computes the password points using histogram arithmetic and encrypts the chosen password points using SHA512. The envisioned system has been realized as an android application and evaluated with existing research considering multiple measurements such as required login time, password space, and entropy. The findings reveal that the new suggested system outperforms the reference work by more than 85% in terms of login latency and more than 72% in terms of entropy results..**

keywords: **Grid blocks, Authentication, Hash function, Histogram, Dynamic points**

I. INTRODUCTION

Graphical password is an alternative way of authentication using these interfaces that have been more widely available with the appearance of touch screens, notably with the increasing use of this technology in smartphones and tablets. A graphical password is a method of authentication using images rather than text, numbers, or special characters because human beings can remember pictures better than text. A graphical password consists of three primary techniques (recognition-based, recall-based, and hybrid techniques). In the recognition-based technique, a user is introduced to a set of pictures. By correctly identifying the images the user chose during registration, authentication is successfully completed. It includes many algorithms, such as the Sobrado and Birget Method, the Dhamija and Perrig Scheme, and the Passfaces Method. A user is asked to re-create an item from memory as part of the recall-based technique. They created or decided upon during the sign-up process, such as pattern and click-point, Recall-based authentication techniques generally fall into one of three categories: pure, cued, or hybrid. Systems that depend exclusively on users' memories for authentication require users to reproduce or draw something as their password without providing any hints during the login phase, while cued recall-based authentication systems provide users with some clues or hints implicitly to produce their passwords during this stage [1].

A hybrid is a combination of two or more graphical password schemes, as CAPTCHA. These schemes are introduced to overcome the drawbacks of a single scheme, such as hidden cameras, shoulder surfing, and spyware. In addition to the security challenges, they are developing authentication methods that are safe and simple to use. The user usability of a system is closely connected to how securely it is utilized; in instances where the system is not user-satisfying, users may discover unsecured email methods to keep passwords or just overcome or misuse the security measures. Passwords

ISSN:2222-758X
e-ISSN: 2789-7362

have become so common in our daily lives that many people prefer to use them creatively, such as with words from their vocabulary or numbers from their date of birth. Hackers can take advantage of these simple patterns, such as using a starting capital. Many password approaches can be breached using commonly used passwords, letter frequencies, or frequency-based attacks.

Classical textual passwords are still extensively used in many fields, and one well-known security and usability flaw [2] is required because a poor password can be readily guessed by attackers, reducing authentication security significantly [3]. Therefore, using a graphical password reduces the issues of text passwords and has many problems that need to be solved. The graphical password requires much more storage space; password registration and login take a long time to process. Thus, in this work, a new pass point select automatic technique based on the graphical password histogram method is proposed to improve performance evaluation for this password. This work aims to introduce a new automatic pass point selection password instead of a large number of manual systems that exist and overcome problems that face it, such as long processing time, inaccurate selection of points and forgetting their places, large storage space for images, etc. The proposed system meets these requirements by determining points automatically based on the histogram.

II. Related Work

Greg E. Blonder conceptualized and designed the Blonder in 1996. During the registration process, the user must construct a password by clicking on various locations on a picture. During the authentication session, the image is displayed to the user. To be authorized, the user must click on the tough spots in a predetermined order. The downside of this approach is that it only allows for a limited number of unique passwords. Because the number of pre-defined clickable locations is restricted, the password must be lengthy to be safe [5].

Wiedenbeck et al. (2005) [4], designed and implemented the PassPoints method, which consists of presenting a picture to the user and asking him to choose a set of points on the image. Each point entered during the authentication procedure is matched to the matching point in the original registration set and must be within a specific acceptable limit of that point.

Hemavathy et al., (2017) [6], The histogram is created in this module based on the query picture from the image collection. The graph's horizontal axis indicates tonal dissimilarities, while the number of pixels making up that color is shown along the vertical axis. Black and dark areas are represented by the leftmost horizontal axis, while the middle range of gray is in the middle, and the rightmost axis is white. The vertical axis indicates the size of the seized territory in each of these zones. As a result, the histogram for an extremely dark image will have most of its data on the graph's left side and center. The user can register by uploading the image, and once the photo is uploaded, it will be compared to the LDN code that is used to store features of the original image.

ISSN:2222-758X
e-ISSN: 2789-7362

Figure 1: Using histogram with a graphical password

Yang et al., (2018) [7], The 'PassPositions' graphical password system, as well as its upgraded variant, the 'PassPositionsII,' are described in detail. The PassPositions system has been adapted to function in the Android environment with the Galaxy Tab, and it is now available. Because it is currently compatible with a wide range of Android mobile devices, it is simple to deploy, and it is a light system. It can be used to replace text-based password schemes in a wide range of mobile applications, including mobile games.

Wiangsripanawan (2018) [8], HapticPoints suggested graphic password authentication using PassPoints, where the user clicks on a series of fake click points in the password image by randomly adding haptic input to the image. It has also been improved in its capacity to avoid dictionary attacks, in particular hotspot attacks, by including picture saliency during the registration process, which informs the user about the suitability of the password image selection made by the user. As a result of PassPoint and HapticPoints being studied for their usability, Compared to PassPoints, HapticPoints provide a more secure password and better protection against the vulnerabilities described by the threat model. Ali et al., (2019) [9],

Fractal-Based Authentication Technique (FBAT) uses a Sierpinski triangle to overcome shoulder surfing, brute force, and smudging attacks. Password guessing is weak in this scheme, making it resistant to attacks. As a result, this technique may be deployed on any device that requires authentication, such as ATM machines, smartphones, and computers. Kumar et al., (2019) [10], The concept of CaRP presents a new family of graphical passwords that use a novel technique to defend against online guessing attempts, such as dictionary attacks. The use of the captcha and pass position methods can help in the protection of sensitive data stored in a public cloud.

Azad et al., (2019). [11], presented a new hybrid graphical authentication technique that easily integrates PassPoints and Press Touch Code (PTC) schemes into one. The inclusion of the PTC increases the amount of password space available while also helping in the defense against shoulder surfing attacks; the suggested scheme's performance is evaluated in terms of security, functionality, and user-friendliness. A comparison to other similar procedures shows that the proposed

ISSN:2222-758X
e-ISSN: 2789-7362

method is better than those methods.

Plasencia et al., (2022). [12], This paper introduces a new technique for identifying DIAG or LINE-shaped graphic passwords in PassPoints. Experiments demonstrated that, for a set of five points, the number of Delaunay triangles ranges from three to five depending on the position of the points, and that this number is independent of the image size chosen by the user or the system. In this study, we estimated the probability distribution of the average of the maximum angles in the Delaunay triangulation, where the number of triangles per password is irrelevant. Matta, P.,

Pant, B. (2020) [13], introduced a graphical password system. The proposed scheme for authenticating IoT system resources applies to all IoT-related domains. For secure access to IoT resources, this paper suggests a visual password scheme called Two Clicks per Character (TCpC) . Important aspects of authentication systems like password resets and replacements are also discussed.

Abdalkareem et al., (2021) [14], To protect confidential information, this paper suggests a novel method of password generation based on mouse movement and a special case location recognized by the number of clicks. It has been suggested that users click in two or three distinct places to require more complex passwords. This approach was developed to reduce the likelihood of a user's password being guessed by increasing the number of possible mouse motion combinations used in graphical password generation.

III. BACKGROUND

A. *Histogram equalization*

In order to produce the highest possible picture quality, the varying It is preferable for light intensities captured by pixels in a digital image to fill the full range of tonalities. It follows that the lowest possible light intensities in a picture should be assigned the value zero, while the highest possible light intensities should be assigned the highest possible value of the discrete mapping range. A wide range of image intensity values that are evenly distributed ensures strong image contrast [15][16]. This is the histogram equalization for an individual pixel that occupies the position (x,y) and which has an initial associated intensity I(x,y), as shown in the following [histogram] equation[15]:

$$I(x,y) = \frac{L-1}{N} C_f(x,y) \tag{1}$$

Where L.is the number of potential intensity values, Cf (I) denotes the cumulative frequency distribution of the pixel intensity I, and N represents the total number of pixels contained within the image. The cumulative frequency distribution is the total of all image histogram values in the range [0, L 1] across time[17].

B. *Hash function*

A hash function is a technique that accepts an arbitrary amount of data as input and returns an output of a specified size in return [18]. Hash functions are extremely significant in network security and cryptography because they may be used to verify data. A check is performed in order to ensure the integrity and authenticity of information or data transmitted between the source and the destination. In both symmetric and asymmetric key cryptosystems, the hash function is utilized

ISSN:2222-758X
e-ISSN: 2789-7362

for key generation. According to how difficult it is to break different algorithms, different levels of security are provided by each of them. The integrity of the data in a highly protected system is extremely important. Users of the system can construct a message digest with the help of a cryptographic hash function, which can be used to detect unauthorized changes in the files. It is especially vital when dealing with mission-critical systems and sensitive databases. Several traditional hashing algorithms include SHA-1, SHA-2, SHA-3, MD4, MD5, Whirlpool, etc. [19]. The Hash in our proposed system is SHA-512.

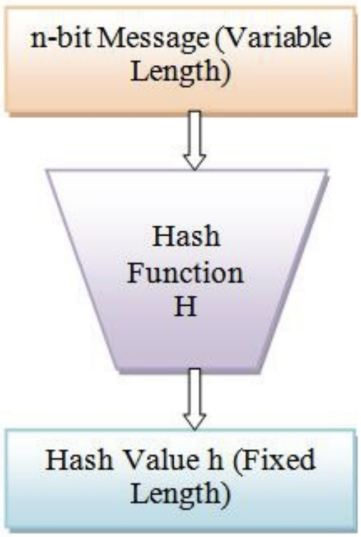


Figure 2: Hash Function

IV. PROPOSED SYSTEM

The primary purpose of this work is to develop and construct an authentication system using the graphical password mechanism. The proposed system has two major phases. The first is referred to as the registration step, and the second as the login stage. The last stage is used by all the mentioned stages and is called "Compute Hash Value of Password Points". Each of these phases is comprised of several steps. This section will depict every saga.

A. Registration Stage

The first phase is known as the "registration phase. When a user creates a new account, they must first provide the required registration information, including their username, email address, and text password. After confirming the provided information, the system prompts the user to choose an image and security level. The chosen image is then split into NxN blocks, and the system computes the histogram of each block following applying the threshold to select all points over the predefined threshold. and displays them on the image. The user must pick a password consisting of an arbitrary number of non-ordered points from the available points. The system next computes the hash value of all chosen points and stores it, together with all other user data, with the selected image, threshold value, and security level, in the database for use

ISSN:2222-758X
e-ISSN: 2789-7362

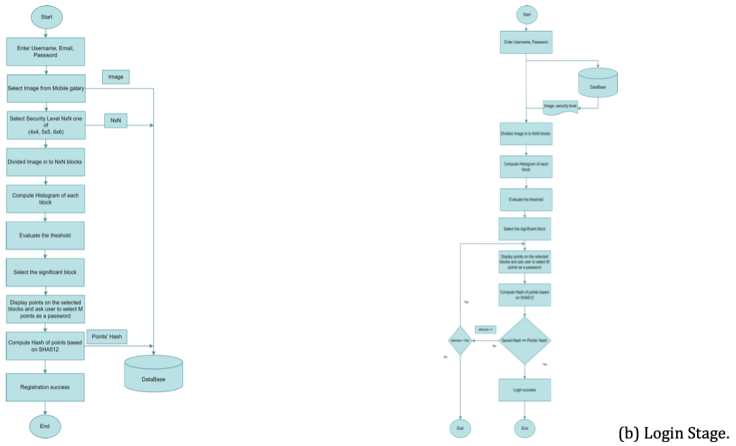
during the login process. The diagrams depict the main phases of the registration process. The authentication system's content-adding processes involve answering hint questions to guarantee that a lost password can be retrieved. As seen in Fig. 3.

B. Login Stage

The login phase of the proposed system is the second phase. At this stage, the user will be requested to provide basic login information, such as a username or email address, along with a text password. The system will next submit the information to the database to check whether the user already exists, and it will reply with all of the user information that was provided during the registration process. Once the picture has been received from the database, it will be split into NxN blocks and the histogram of each block will be generated, revealing the points to be selected. The system will then generate the hash of the chosen points and transmit it to the database so that the values may be compared. If they are identical , the user will be able to login successfully. Otherwise, they need to reselect the point. The number of password selections is limited. If the number of attempts is exceeded, the system advances to the hint question stage. Fig. 3 demonstrates the login stage of the system.

C. Hash Computed

Multiple hash algorithms are used to produce the text hash. In the approach we propose, SHA512 is used to compute the hash of the selected points. The number of points awarded varies based on the degree of security. Our system has three security levels: 4x4, 5x5, and 6x6. After selecting the points, the system stores them in an array and computes SHA512 for each one. Next, the hash value is concatenated. The combined hash value is then stored in the database. Fig. 4 illustration depicts the hash creation process.



(b) Login Stage.

Figure 3: Registration and Login Stage

ISSN:2222-758X
e-ISSN: 2789-7362

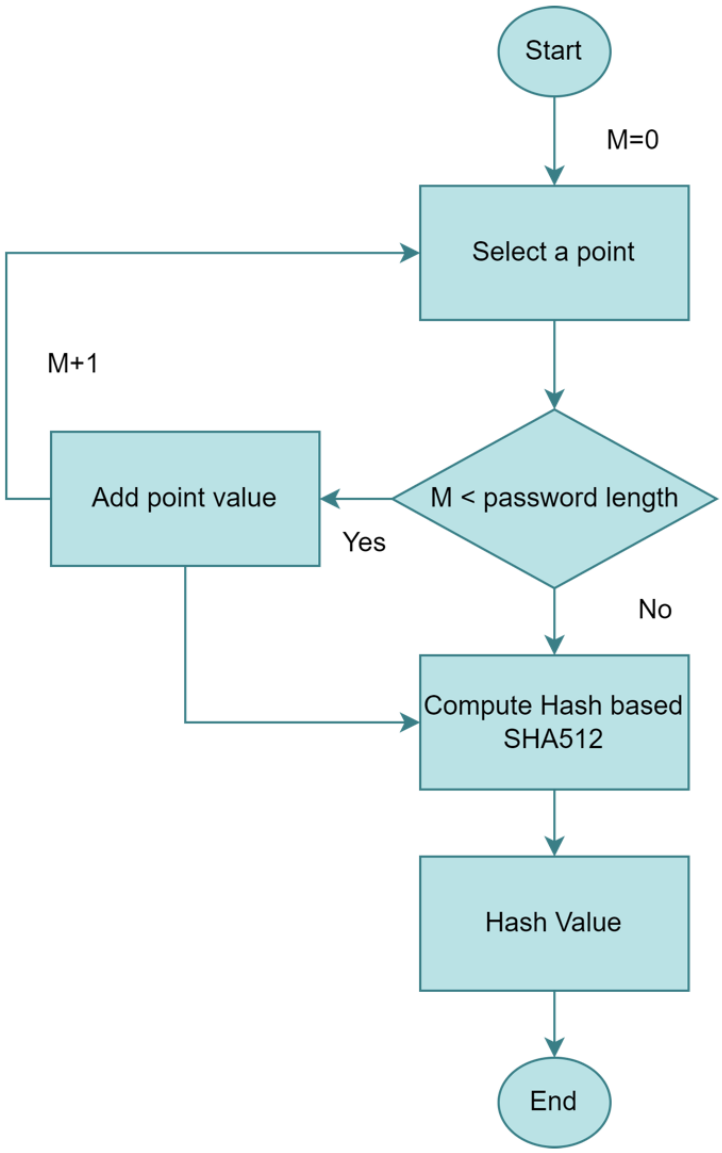


Figure 4: Hash Computed

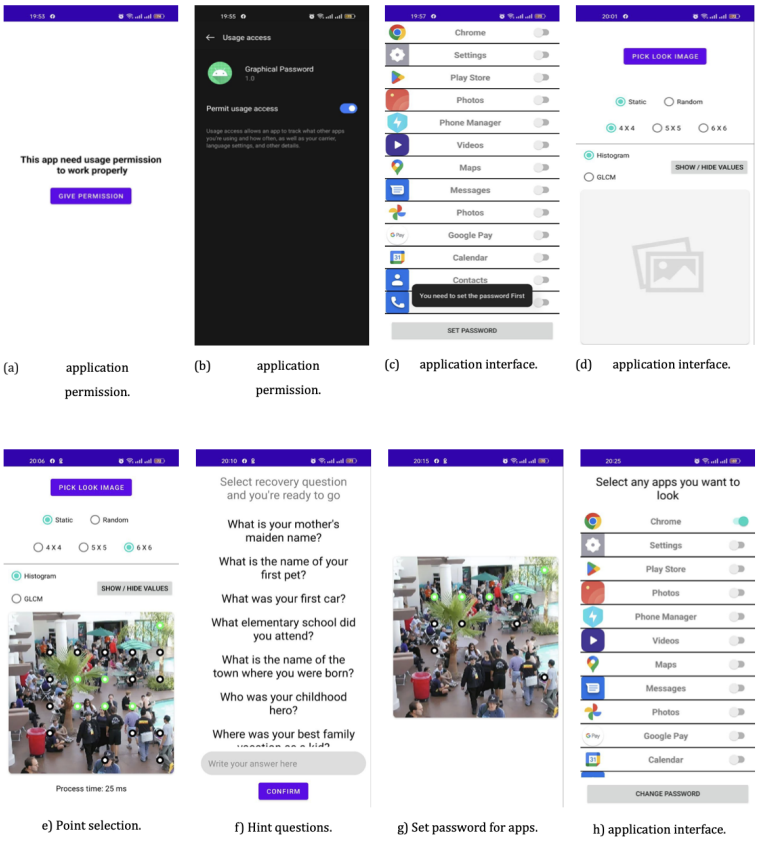
V. RESULTS

A. *Application Used*

The application is created using the programming language Kotlin and the integrated development environment Android Studio. The graphic demonstrates the process of the proposed application. As seen in Fig. (5, a), after being downloaded, the application asks the user for permission to use it. Then, all the installed programs will be shown. To protect them, a graphical password must first be set. Fig. (5, d) depicts the proposed application inviting the user to choose an image and security level, as illustrated in Fig. (5, c). The chosen image will then be divided into NxN blocks, and the user will be

ISSN:2222-758X
e-ISSN: 2789-7362

presented with the resulting points. In addition, the estimated time required to create the displayed points will be shown in Fig. (5, e). Choosing a hint question is the last step in choosing a graphic password. As seen in Fig. (5, f), the user is provided with a list from which to choose a particular hint question. As shown in Fig. (5, g), when a user returns and signs in, he or she must use the same points that were used during registration. The user is then able to choose programs and lock them so that they cannot be accessed without first entering a graphical password.



(a) application permission. (b) application permission. (c) application interface. (d) application interface.

e) Point selection. f) Hint questions. g) Set password for apps. h) application interface.

Figure 5: Application use steps

The calculation of the password space and the entropy in the proposed system depends on the dp (pixel density), which varies from one screen to another, as in Fig. 6, which shows the error when using a certain number of pixels and not depending on the pixel density to calculate the px for correctness area of the finger press on each screen within the specified area for each point using the following equation [20] to make the application suitable for use with all mobile devices:

$$px = dp \times \left(\frac{dpi}{160}\right) \tag{2}$$

Where $(dp = 16), px =$ pixel number, $dpi =$ dots per inch.

ISSN:2222-758X
e-ISSN: 2789-7362

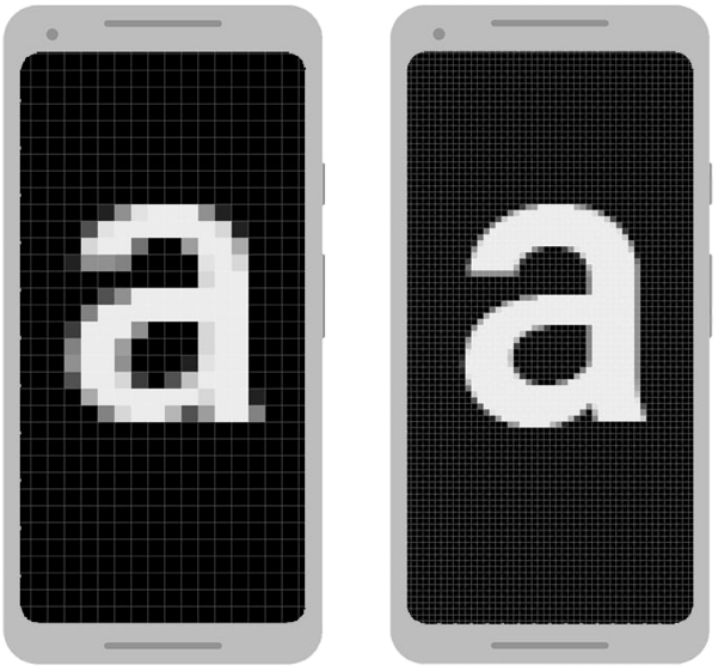


Figure 6: Two screens of the same size may have a different number of pixels

In the proposed system, as we tested the password space with image size NxM and $16\mathrm{dp}$, there is about $\mathrm{NxM/px}$, which (n=number of clicks) as can be seen in equation [21]:

$$\text{Password Space } = \left(\frac{N \times M}{px}\right)^{n} \tag{3}$$

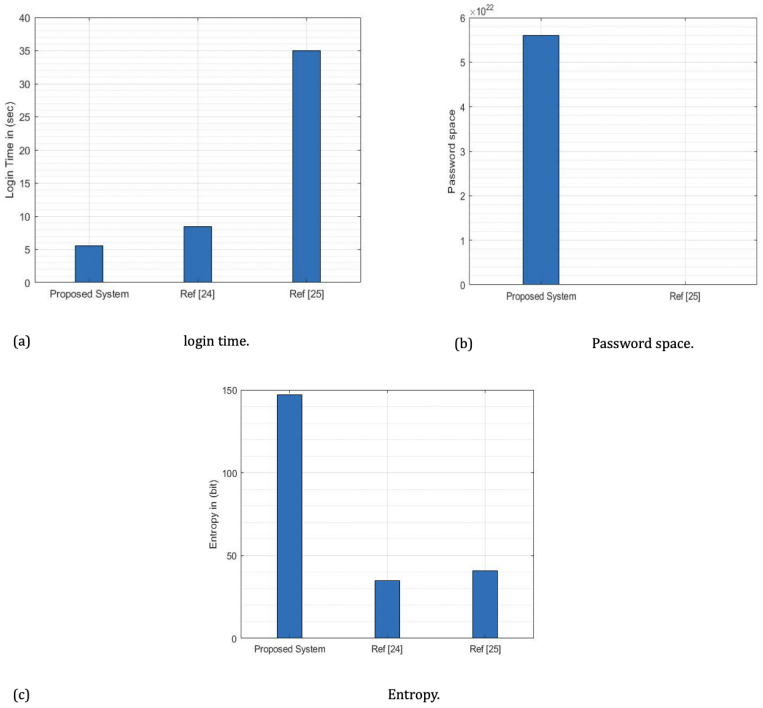
which (n=number of clicks). Password entropy is commonly used to evaluate the safety of a password and its resistance to brute-force or guessing assaults. The graphical password entropy attempts to estimate the likelihood of the attacker acquiring the correct password through random guessing. A graphical password's password entropy is calculated by multiplying the number of pixels by the log (number of clicks point) as the equation [21] [22]:

$$\text{Entropy } = px \log_2(n) \tag{4}$$

Where px= pixel number , n=number of clicks.

ISSN:2222-758X
e-ISSN: 2789-7362

B. Mathematical results



(a) login time. (b) Password space.

(c) Entropy.

Figure 7: Mathematical results of proposed system and other references.

The login time is included in the proposed system's performance calculation. The results demonstrate that the suggested system outperforms all cited techniques. As seen in Fig. (7, a), the application login time achieved a 43% improvement over Ref [24] and an 85% improvement over Ref [25]. The suggested system exhibited better performance as compared to the Ref [25] when the password space was taken into consideration. As a result, the system is more secure as it takes longer to decipher the produced password, as illustrated in Fig. (7, b). The entropy of a system is a measurement of how random and disordered it is; a high entropy indicates a high level of disorder. As illustrated in Fig. (7, c), the proposed system outperforms Refs [24, 25] by 76% and 72%, respectively. In terms of the number of click points, the application that was developed offers up to ten available click points that can be chosen during the process of selecting a password. On the other hand, both of the references only permit six points, which is significantly less efficient than our system.

VI. Conclusion

In this paper, an efficient authentication algorithm is proposed. The implementation is done in an effective Android application. The authentication methods have been proposed based on histogram image processing and click-point graphical passwords. A histogram has been applied based on the texture of the image. In addition, a series of equations and operations were used, starting with dividing images and applying histogram equations to find points and encrypting them. Testing of several images has been done to provide the string values of password space, entropy, and time. Three cases have been

implemented and compared with different scenarios, each with a different block size. Based on the results of the three cases, Case 1 with 4×4 blocks, Case2 with 5×5 blocks, and Case3 with 6×6 blocks. Case2 provides the best result compared with the other cases. the most accurate point location is due to the method of distributing points and the number of blocks in this case. The results show an improved performance of the cued click points technique in the Android application. A proposed system improves flexibility and efficiency. The user's password is quickly remembered. It is more resistant to hacking than other passwords and works better for memorization points than manual click-point passwords. In addition, we can see through the given results the significant difference in the values of password space, time, and entropy, and that's considering an improvement in the graphical password system to be safer to use by the user. According to our observation, the two significant challenges for researchers are the security and usability of graphical passwords. In Future work, texture features will be used in a new model to get a large key space size.

Funding

None

ACKNOLEDGEMENT

The author would like to thank the reviewers for their valuable contribution in the publication of this paper.

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] J. G. Kaka and O. J. O, "Recognition Based Graphical Password Algorithms: A Survey."
[2] T. Khodadadi, Y. Javadianasl, F. Rabiei, M. Alizadeh, M. Zamani, and S. S. Chaeikar, "A Novel Graphical Password Authentication Scheme with Improved Usability," 2021 4th Int. Symp. Adv. Electr. Commun. Technol. ISAECT 2021, no. March 2022, 2021, doi: 10.1109/ISAECT53699.2021.9668599.
[3] T. I. Shammee, T. Akter, M. Mou, F. Chowdhury, and M. S. Ferdous, "A Systematic Literature Review of Graphical Password Schemes," J. Comput. Sci. Eng., vol. 16, no. 4, pp. 163-185, 2020, doi: 10.5626/JCSE.2020.14.4.163.
[4] A. H. Lashkari, F. Towhidi, R. Saleh, and S. Farmand, "A complete comparison on pure and cued recall-based graphical user authentication algorithms," 2009 Int. Conf. Comput. Electr. Eng. ICCEE 2009, vol. 1, no. January, pp. 527-532, 2009, doi: 10.1109/ICCEE.2009.81.
[5] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," Int. J. Hum. Comput. Stud., vol. 63, no. 1-2, pp. 102-127, 2005, doi: 10.1016/j.ihhcs.2005.04.010.
[6] M. Hemavathy and S. Nireniena, "Multilevel Graphical Authentication for Secure Banking," vol. 2, no. 2, pp. $423 - 428, 2017$.
[7] G.-C. Yang and H. Oh, "Implementation of a Graphical Password Authentication System 'PassPositions,"' J. Image Graph., vol. 6, no. 2, pp. 117-121, 2018, doi: $10.18178/j0ig.6.2.117 - 121$
[8] T. Ratchasan and R. Wiangsripanawan, HapticPoints: The extended PassPoints graphical password, vol. 11402 LNCS. Springer International Publishing, 2019.
[9] A. Ali, H. Rafique, T. Arshad, M. A. Alqarni, S. H. Chauhdary, and A. K. Bashir, "A fractal-based authentication technique using sierpinski triangles in smart devices," Sensors (Switzerland), vol. 19, no. 3, 2019, doi: 10.3390/s19030678.
[10] D. Sathish Kumar, R. Rajkumar, R. Kalpana, and C. Associate, "Graphical Image Based Password Authentication System," Int. J. Res. Anal. Rev., vol. 6, no. 2, pp. 147150, 2019, [Online]. Available: www.ijrar.org.
[11] S. Azad, N. E. A. C. Nordin, N. N. A. Rasul, M. Mahmud, and K. Z. Zamli, "A Secure Hybrid Authentication Scheme Using Passpoints and Press Touch Code," IEEE Access, vol. 7, pp. 166043-166053, 2019, doi: 10.1109/ACCESS.2019.2948977.
[12] L. Suarez-Plasencia, J. Herrera-Macias, C. Legon-Perez, G. Sosa-Gomez, and O. Rojas, "Detection of DIAG and LINE Patterns in PassPoints Graphical Passwords Based on the Maximum Angles of Their Delaunay Triangles," Sensors, vol. 22, no. 5, pp. 1-16, 2022, doi: 10.3390/s22051987.
[13] P. Matta and B. Pant, "TCpC: a graphical password scheme ensuring authentication for loT resources," Int. J. Inf. Technol., vol. 12, no. 3, pp. 699-709, 2020, doi: $10.1007/s41870 - 018 - 0142 - z$
[14] Z. A. Abdalkareem, O. Z. Akif, F. A. Abdulatif, A. Amiza, and P. Ehkan, "Graphical password based mouse behavior technique," J. Phys. Conf. Ser., vol. 1755, no. 1, 2021, doi: $10.1088/1742 - 6596/1755/1/012021$.
[15] P. R. G. Kurka and A. A. DÃaz Salazar, "Applications of image processing in robotics and instrumentation," Mech. Syst. Signal Process., vol. 124, pp. 142-169, 2019, doi: $10.1016/j.ymssp.2019.01.015$
[16] J. H. Han, S. Yang, and B. U. Lee, "A novel 3-D color histogram equalization method with uniform 1-D gray scale histogram," IEEE Trans. Image Process., vol. 20, no. 2, pp. 506-512, 2011, doi: 10.1109/TIP.2010.2068555.

ISSN:2222-758X
e-ISSN: 2789-7362

[17] A. K. Bhandari, "A logarithmic law based histogram modification scheme for naturalness image contrast enhancement," J. Ambient Intell. Humaniz. Comput., vol. 11, no. 4, pp. 1605-1627, 2020, doi: 10.1007/s12652-019-01258-6.
[18] N. Kheshaifaty, A. G.-I. J. C. S. N. Secur.(IJCSNS), and undefined 2020, "Preventing multiple accessing attacks via efficient integration of captcha crypto hash functions," researchgate.net, vol. 20, no. 9, p. 16, 2020, doi: 10.22937/JCSNS.2020.20.09.3.
[19] P. P.-I. J. of C. S. and Mobile and undefined 2019, "A comparative study of hash algorithms in cryptography," academia.edu, Accessed: Nov. 08, 2022. [Online]. Available: https://www.academia.edu/download/59869343/V816201928.pdf.
[20] A. J. de Oliveira JÃºnior, S. R. L. de Souza, E. Dal Pai, B. T. Rodrigues, and V. C. de Souza, "Aurora: Mobile application for analysis of spatial variability of thermal comfort indexes of animals and people, using IDW interpolation," Comput. Electron. Agric., vol. 157, no. December 2018, pp. 98-101, 2019, doi: 10.1016/j.compag.2018.12.029.
[21] Ghiyamipour, âSecure graphical password based on cued click points using fuzzy logic,â Secur. Priv., vol. 4, no. 2, Mar. 2021, doi: 10.1002/SPY2.140.
[22] K. H. A. Al-Shqeerat and K. I. Abuzanouneh, âA Hybrid Graphical User Authentication Scheme in Mobile Cloud Computing Environments,â Int. J. Commun. Networks Inf. Secur., vol. 13, no. 1, pp. 68â75, 2021, doi: 10.17762/ijcnis.v13i1.4890.
[23] A. Chopra, V. Kumar Sharma, and M. Gupta, âAnalysis of Entropy Password Space in various Graphical PasswordsTechniques,â Jagannath Univ. Res. J., vol. III, no. I, pp. 2582â6263, 2022, [Online]. Available: http://jagannathuniversity.org/jurj.

