ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 10, Issue 3, March 2025

Improved Security for Hybrid Textual-Graphy Password Authentication Systems

[1] Kamaleswari P, [2] Ezhilvathani A, [3] Sabarinathan J
[1] [2] [3] DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, Er. Perumal Manimekalai College of Engineering, Hosur, India.
kamale.csc@gmail.com, ezhilvathani.nz@gmail.com, sabarinathan0015@gmail.com

Abstract: ***The advancement of technology has resulted in numerous positive results. The majority of human activities can now be substantially simplified thanks to technological improvements. The same is true for cybercriminals who, among other things, want to get access to user accounts in order to steal sensitive information for their own purposes. Even if technology improvements are clearly good, it is our job as customers to take all reasonable efforts to protect our data. There are several precautions at our disposal. However, the security of any given system is never guaranteed. All of our efforts are aimed at lowering the likelihood of a security breach. Authentication is carried out via a textual and graphical password paradigm[1]. We chose this approach because humans are naturally visual beings, and we believe that adopting a cued-recall and recognition-based method can increase a system's defences. A password with an entropy [5] of 60 or above is considered strong. This password technique, once rigorously tested, can prove to be a very good alternative to multi-factor authentication, which would force the user to wait for an OTP or some other annoyance. Our method seeks to alleviate all of the difficulties faced during the process by proposing a simple gateway for user identification. This approach aids in the creation of passwords with entropy near to 89, which is considered a strong password.***

Keywords— security breach, authentication, entropy, password

I. INTRODUCTION

To begin the authentication process, a user enters their username and password, which are then checked against the system's databases.

A layman assumes this to be secured when in reality this is only one speck of security and all that happens behind the scenes is what adds to the security we usually see and apply. A textual password can very well be cracked using certain spyware attack modules. Similarly, MITM or man-in-the-middle attacks steal information by posing as a legitimate entity over the internet when in reality they are merely a third-party entity. Dictionary attacks and brute-force attacks are other common examples of security-compromising attacks.

Textual passwords have their limitations in terms of length, combinations, and visual features that could cajole the memory of the user. Hence, they could be more vulnerable to password breaches. There have been instances of breaches where a person was able to breach into passwords[8] of WINDOWS XP within a few minutes by just using a few (25) graphical processing units. Passwords using just alphanumeric elements are also subjected to a few human limitations such as the ease of memorizing the passwords. People tend to choose passwords that are easier to remember when needed for authentication rather than a strong and secure password which will take the attacker a lot of time to breach into. This makes people stick to more conventional passwords such as birthdate, name, or something historical yet easily identifiable. Dictionary attacks will easily succeed against all these passwords and put data at a lot of risk.

To enhance security, many systems have employed a hybrid model of both textual and graphical password authentication systems [1] [3]. Even they are not secure as graphical passwords are susceptible to shoulder-surfing [6]. There is always going to be a conflict between the strength and simplicity of a password. The more simple the password, the more simple to remember it but at the same time it is more prone to be cracked as well. A simple short password will require lesser time to be processed but again will be prone to be compromised easily[9]. Therefore, what we want to achieve is to find ways to keep a password simple and yet make it strong enough to withstand any and every attack there is possible.

There have been several prior uses of hybrid models. They apply the concept via a wide variety of media, including text, grids, drawings, photographs, etc. All of them are prone to assaults like[3]:

i. Shoulder-Surfing
ii. Brute-force

Authentication systems are always on the brink of evolution. Today we see a lot of multi-factor authentication systems[10] [11] employed to make authentication systems stronger and withstanding cyber-attacks. One very popular scheme of the same kind is that of the one-time password.

The stakeholder must provide a one-time password[12] to prove their legitimacy. Time complexity would grow, and the authentication process might be slowed down as a result. Therefore, alternatives must be considered since they may be vulnerable to assaults such as man-in-the-middle attacks. In this research, we propose a combination of textual-graphical authentication paradigms to improve system security.

II. LITERATURE REVIEW

Passwords used nowadays are mostly schemes that use the knowledge of the user to secure the entities that need to be secured using the password. Users are required to provide information that is precisely known to them as something that can be used at the time of authentication of the user credentials.

Some types of passwords that we came across while reading up different passwords are:
1. Search Metric
2. Draw Metric
3. Loci Metric
4. Multifactor Schemed Passwords
5. Hybrid Scheme Passwords

Search Metric: These are purely recognition-based schemes.
Dhamija et al suggested a Déjà vu scheme employs abstract visuals for authentication purposes. The user must choose many pictures from the available options to complete the authentication process. Déjà vu is particularly susceptible to shoulder surfing attacks.
The user's capacity to recall information is another weakness of the Déjà vu method. When passwords are represented as abstract visuals, they are very difficult to recall.

Issues with Déjà vu schemes are looked to be mitigated by the Pass faces scheme. Passfaces scheme uses human pictures as password elements which require the user to choose amongst nine pictures the right image on one page. Passfaces fails the spyware attack test and is prone to shoulder surfing.

To overcome this vulnerability, a Story scheme was suggested by Davis et al[15]. In which the user chooses his password element images relating to a story in his mind. This improves the memorability of the password. This in turn is prone to spyware attacks and shoulder surfing.
Widen back[13] suggested the Convex Hull Click which requires the user to choose from a triangle on the screen his password elements.

Draw Metric: Draw metric schemes consist of drawing a line, grid, etc. for authentication.
Jeremy et al[17], proposed a technique called Draw a Secret (DAS), which asked users to retrace a line or grid as a form of authentication. Spyware assaults and shoulder surfing might easily exploit this. A further problem was that the user's inability to remember the password may prevent them from successfully authenticating.

Yan et al[18]. proposed a betterment of the DAS by proposing adding a background to the password authentication page where the user must redraw the lines and grids for authentication and hence improving the memorability of the password chosen by the user. This scheme is also prone to spyware attacks and shoulder-surfing. This is called the BDAS scheme.
Passdodles[19] is an attempt to address the limitations of previous draw metric solutions by allowing users to freely draw and use whatever figures they like as passwords. Shoulder surfers and mouse recorders will undoubtedly find ways to break this system.
Loci Metric or Cued Recall-Based Schemes: Loci metric schemes are a kind of password that require the user to choose it from a list of x, and y coordinates. These techniques rely on cued recall, in which the user is presented with a hint—typically

an image—that may or may not correspond to a part of their password. The user will need to utilize their memory skills to determine whether the presented piece of information is, in fact, part of their password.

Blonder[13] proposed the first scheme that uses a graphical password containing multiple predefined points of an image. This scheme lacked in umpteen password space. To mitigate the above drawback, Widenback et al[14] proposed a scheme similar to that of Blonder's but with a larger password space. This is known as the PassPoints scheme. "Hotspots" which are easy-to-remember points chosen by the user for their passwords can be taken advantage of by attackers. Aside from that, this approach is susceptible to hacking attempts like shoulder surfing and malware.

Chaisson[4] improved the Pass Points framework by further improving password space and by introducing the Cued Click Points Schemes. This has a bigger password space and makes brute force attacks difficult to be implemented.

Hybrid Schemes: This plan is a compilation of several authentication methods used to bolster the safety of a given system. Our proposed system here in this study is no exception. Zhao and Li devised S3PAS[21] , a hybrid model. In this approach, the textual password must use only standard alphanumeric characters. On the login screen, these characters are shown as an image for further security. Users are prompted to choose the correct password character from a logical triangle. While S3PAS can prevent shoulder-surfing, it may be vulnerable to other assaults that monitor the user's every move.

Zheng et al[16] introduced a scheme which makes use of password shapes and numbers. It uses a mix of DAS and textual(numeric) characters. At the time of initiation, the user is required to choose his characters and also draw a secret key as his password. At the authentication, the user is required to input the numbers that would form his password given on the login screen. Despite their apparent immunity to keylogger assaults, they are easy prey for shoulder surfers.
An anti-spyware system was proposed by Alsaiari et al. Their scheme is called GOTPass[6]. They actively use DAS in their password scheme. While logging in the user must redraw the DAS key.

In certain setups, the user is given a passkey that is created randomly and sent to them through headphones. Intrusion attacks and brute force assaults may be possible with this. To facilitate password choosing, Chakraborty et al[20]. developed a colour pass model in which 10 colours are shown to the user. When authenticating, the user will input a number from a set of tables that have been sent to them through headphones; the corresponding colour will then be shown on the screen. In this case, the attacker might "surf" on the shoulders of the defenders.

S. Z. Nizamani et al[1] proposed a model that is brute force attack resistant which requires the user shall choose both a text-based password and a graphical password from the images provided. At the time of logging in the user is shown a table consisting of the elements of their password and is asked to choose the latest two elements of the password. All the elements are assigned some random numeric value and the user must input the sum of the values of the latest two elements along with the number of password elements found in the table. This is then authenticated with the information available in the database. This provides some layers of security but is prone to shoulder surfing.

Multi-Factor Authentication: Multi-factor authentication refers to any system that uses more than one authentication method. Factors include: User knowledge, possessions, biometrics, location, and time of authentication. Most authentication systems nowadays use a variety of multi-factor authentication systems to enhance the security of a given system.
Combining OTP with a textual password and a biometric may exponentially increase the strength and security of a user's password.

Another system proposed by Kansuwan and Chomsiri[22] is by asking the user to provide a password, CAPTCHA, and an OTP at the time of logging in.

III. PROPOSED AUTHENTICATION SCHEME

Authentication in this scheme is handled through a dual-module approach. To utilize the service, a user must first register by selecting a unique collection of 5 photos and entering his personal information (such as a username and password). At authentication time, once the user has provided his login and password, they will be shown a series of photos and asked to choose one from each cycle. They would see 9 pictures on the screen and have to choose the one that was included in the graphical password. If they guess correctly, they will go on to the next round of passwords, where they will be presented with another set of nine photographs. If they make a mistake in one stage, they may still pick the pictures in the following cycle to

throw off their opponent. If the final picture is the same and the text password is entered correctly, then the user has been verified. If not, the password is invalid.

When a user creates an account, they may choose a password that will be hashed and stored using SHA256. While logging in the user would again be required to enter the password which will still be put under the SHA256 hashing algorithm. The selected hash will be matched with the stored hash, if the hashes match only then the images would be checked for a match. Once the hash values are matched, the images will be checked if they are correctly chosen and in the proper order. If both the criteria are satisfied pertaining to images, only then the user is authenticated. If at any stage either the textual password is wrong or any of the images is wrong, the user will be notified only at the end of the last cycle that the hybrid password entered is wrong and they must choose again.

What this does is it makes it very difficult for the attacker to go back and try to guess and employ a brute force attack. Given that we would be utilizing a series of 5 photos as a graphical password, users would have to log in by selecting an image from a collection of 9 given in cycles of 5 times.

An attacker would require at least 4.5X10^35 attempts to brute force the password in such a scenario. This helps in enhancing the hybrid textual-graphical password scheme.

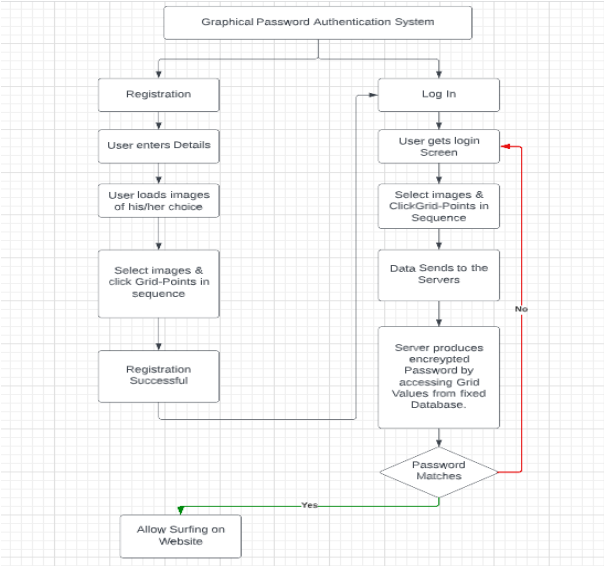
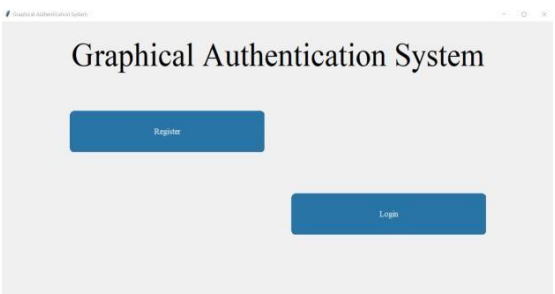


FIG 1: WORKFLOW DIAGRAM

IV. IMPLEMENTATION

1. The User Will Be Directed To A Page Titled Graphical Authentication System.



ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 10, Issue 3, March 2025

2. IF THE USER HAS NOT REGISTERED, THE USER MUST CLICK ON THE REGISTER

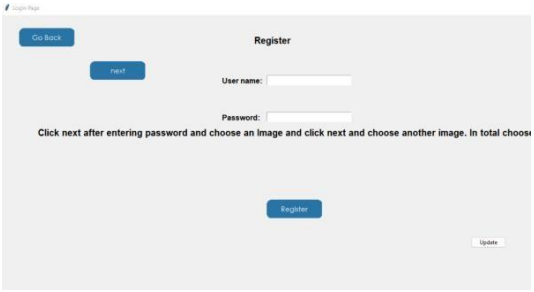


FIG 3: REGISTRATION PAGE

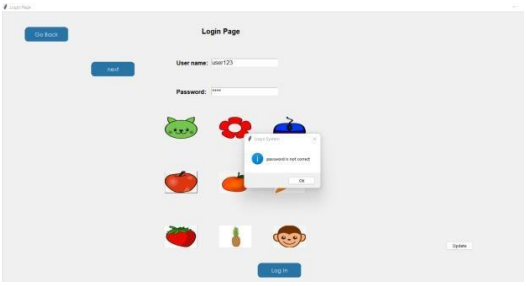


FIG 4: LOGIN PAGE

After inputting all the information and selecting the images in the cycle, the user must click on register.

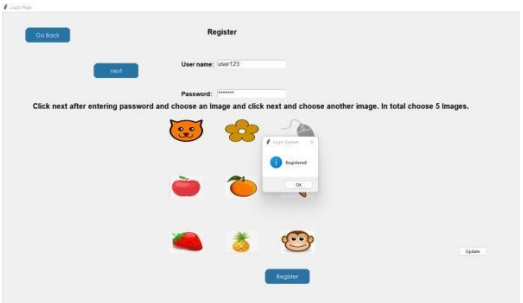


FIG 5: REGISTRATION COMPLETE

1. If the user is already registered, they may choose to directly press the login tab on the main menu.

2. Once the user is on the user page, he must first input username and password and then press next upon which he will be shown the set of images to choose from.
   If the user does not enter the right password, the tool won't check for the images and simply terminate the authentication.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 10, Issue 3, March 2025

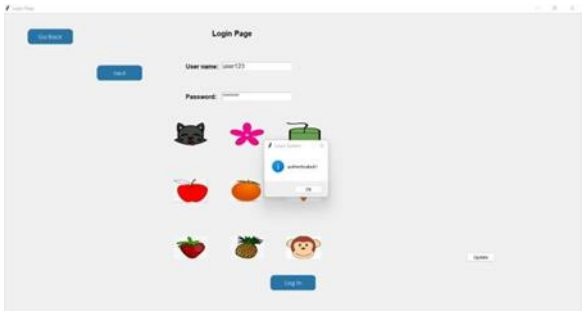


FIG 6: INCORRECT PASSWORD

If The User At Any Stage Chooses The Wrong Image, They Will Not Be Authenticated. Only After The Entire Cycle Of Choosing Images From All Cycles Will The Final Verdict Of Authentication Be Shown To The User. If The User Chooses All The Right Images, Then They Will Be Authenticated, Else No.

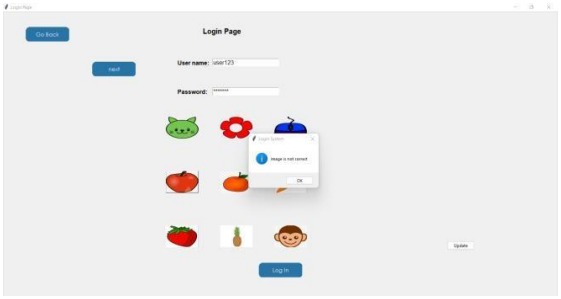


FIG 7: WRONG IMAGE

6. Once the user enters the right credentials and chooses the right images, they will be authenticated.

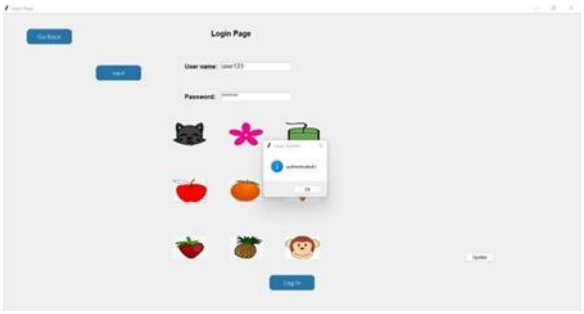


FIG 8: AUTHENTICATED

•

Result

The Purpose Of Our Project Was To Come Up With A Method That Could Help Us Enhance The Present Security Schemes. A Hybrid Model Of The Textual And Graphical Password Was Implemented. One Of The Points To Be Noted Has To Be The Password Entropy Strength That Our Scheme Would Offer Going Forward. A Password Entropy Is An Indicator Of The Strength Of A Password. It Helps

You Predict How Difficult It Would Be For An Attacker To Compromise A Password. The Calculation Of Password Entropy For Any Password Is Given Below.

Number Of Possible Combinations = Sl

Entropy = log2(Number of Possible Combinations)

Where L is the length of the password, indicative of the characters in a password, and S denotes the number of characters available to be used in the password.

The minimum number of characters that would be required to generate an alphanumeric password shall be set at 8 and the number of graphical elements has to be 5.

With that in mind, the password entropy will be:

S=115(a-z, A-Z,0-9, @, #, $,50 images)

L=13 elements minimum (8 alphanumeric + 5 graphical)

Number of Possible Combinations = SL

= 6.1527876e+26

Entropy = log2(Number of Possible Combinations)

= log2(6.1527876e+26)

= 89

A password having an entropy of 60 and above is said to be a strong password. This scheme of passwords once put through rigorous testing can prove to be a very good alternative to the multi-factor authentication that would require the user to wait for an OTP or some other hassle. Our approach looks to mitigate all the hassles encountered throughout the process and looks to propose a hassle-free gateway for the authentication of users.

Upon implementation and trials of our model, we have found that with the amount of password space set the minimum at thirteen, and maximum as a choice, the password entropy will be on a steady growth. Taking at least thirteen password characters (textual + graphical) we can achieve a password entropy of the order of 89, with an available character space of a hundred and fifteen characters.

IV. CONCLUSION

Implementation Of Any Model Is Meaningful Only After It Is Vigorously Tested. After Vigorous Testing Of Our Model, We Intend To Add More Features To The Cause Of Security To Enhance And Make It Easier For People To Use. After Adding Necessities Such As Password Reset And Other Features, Blocking An Account Upon Several Invalid Attempts And Sending Of Email As An Update To Intrusion. Future Works Are To Detect Vulnerabilities And Minimize The Ability To Be Attacked By Attackers.

One Of Our Greatest Ambitions Is To Provide The General Public With A Single Sign Feature Which Will Enable People To Log In To Multiple Places Using Our Authentication System. This Of Course Requires A Lot Of Manpower And Hence Resides In Our Future Works And Ambitions Section.

A Huge Task Force Behind Us Would Enable Us To Work Our Way Towards Our Ambition And Implement It Successfully For The Greater Good Of The General Public.

A Single Sign-On Feature Is Something That Will Make Lives Easier For People. People Would Not Require Remembering A Variety Of Authentication Credentials But Just One Set Of Usernames And Passwords (Textual + Graphical) Which Will Enable Them To Sign In/Log In Anywhere, Anytime.

Further Enhancements Of The Schemes Will Not Only Make Our Model More Secure But Also More Accessible To The General Public Who Not Only Desire But Also Deserve Security.

Our Intentions Are Just To Serve The People With The Best Security Possible, And We Shall Strive To Provide The Same With All Our Best Efforts To Serve The Greater Good Of The People.

REFERENCES

[1] “A Novel Hybrid Textual-Graphical Authentication Scheme with Better Security, Memorability, and Usability” SYED RAHEEL HASSAN, SHAH ZAMAN NIZAMANI, EHAB ATIF ABOZINADAH, RASHID MEHMOOD, AND RIAZ AHMED SHAIKH

[2]” A Simple and Secure Reformation-Based Password Scheme” FAISAL ALANAZI, HASSAM, ABDUL WAHEED, RIMSHA MANZOOR, MAHDI ZAREEI, SAJID AMANULLAH BALOCH, AND MUSHTAQ ALI

[3] ‘’EYEDi: Graphical Authentication Scheme of Estimating Your Encodable Distorted Images to Prevent Screenshot Attacks’’ TAKAYUKI KAWAMURA, TADASHI EBIHARA, NAOTO WAKATSUKI, AND KEIICHI ZEMPO

[4] “Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism” Paul C. van Oorschot, Robert Biddle, Alain Forget and Sonia Chiasson Elizabeth Stobert

[5] Password Entropy Calculator https://generatepasswords.org

[6] “Graphical onetime password (GOTPass): A usability evaluation” S. Furnell I, P. Dowland, M. Papadaki, and H. Alsaiar

[7] “Deja Vu_A user study: Using images for authentication” A. Perrig and R. Dhamija

[8] J. Gosney, ‘‘Password cracking HPC,’’ in Proc. Passwords Conf., 2012, pp. 6–34.

[9] P. Dunphy, Usable, Secure and Deployable Graphical Passwords. School of Computing Science, Newcastle University, 2013

[10] M.-K. Lee, H. Nam, and D. K. Kim, ‘‘Secure bimodal PIN-entry method using audio signals,’’ Comput. Secur., vol. 56, Feb. 2016.

[11] H.-T. Pan, H.-W. Yang, and M.-S. Hwang, ‘‘An enhanced secure smart card-based password authentication scheme,’’ IJ Netw. Secur., vol. 22, no. 2, 2020.

[12] J. Hendryli and D. E. Herwindiati, ‘‘Voice authentication model for a one-time password using deep learning models,’’ in Proc. 2nd Int. Conf. Big Data Eng. Technol., 2020.

[13] 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, nos. 1–2, pp. 102–127, Jul. 2005.

[14] G. E. Blonder, ‘‘Graphical password,’’ U.S. Patent 5 559 961, Sep. 24, 1996.

[15] D. Davis, F. Monrose, and M. K. Reiter, ‘‘On user choice in graphical password schemes,’’ in Proc. 13th Conf. USENIX Security. Symp., vol. 13, 2004, p. 11.

[16] Z. Zheng, X. Liu, L. Yin, and Z. Liu, ‘‘A hybrid password authentication scheme based on shape and text,’’ J. Comput., vol. 5, no. 5, pp. 765–772, May 2010.