IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

HANDKEY BIOLOCK – MANUALLY CRAFTED AUTHENTICATION FOR TOUCHSCREEN

Zinas Sharmila A[1], Dr. Sathya Srinivas D[2]

[1]M.Sc., Department of Computer Science and Engineering, Dr. MGR Educational and Research Institute, Chennai, India

[2]Faculty, Centre of Excellence in Digital Forensics, Dr. MGR Educational and Research Institute, Chennai, India

Abstract: This work enhances traditional authentication systems based on personal Identification Numbers (PINs) and One-Time passwords (OTP) through the incorporation of biometric information as a second level of user authentication. In my proposed approach, the user draws each digit of the password on the touchscreen of the device instead of typing them as usual. A complete analysis of the biometric system is carried out regarding the power of each handwritten digit and when increasing the length of the password and the number of enrolment samples. The new e-Bio Digit database, which comprises online handwritten digits from 0 to 9, has been acquired using the finger as input on a mobile device. OCR algorithms play a crucial role in this process, enabling computers to recognize and extract text from images.

***Keywords* - Handkey, BiolLcok, OCR, Touchscreen, Handwritten passcode.**

I. INTRODUCTION

Mobile devices today have become an indispensable tool for many people. The rapid and continuous deployment of mobile devices around the world is not only driven by strong developments in technology and newly integrated features but also by new internet infrastructure such as 5G enables real-time communication and use of social media, among other elements. In this way, the public and private sectors are aware of the importance of mobile devices for society and are trying to deploy their services through user-friendly mobile applications that ensure Data protection and high security. Traditionally, the two most common methods of user authentication are personal identification numbers (PINs) and one-time passwords(OTPs). While PIN-based authentication systems require users to remember their passwords, OP-based systems save users from having to remember them as the system is responsible for choosing and providing users with passwords. Separate passwords whenever needed, such as when sending a message to unauthorized people, public mobile devices, or special tokens.

Despite the popularity and widespread deployment of PIN and OTP-based authentication systems in real-world scenarios, many studies have highlighted the weaknesses of these methods. First, people often use passwords that support serial numbers, personal information such as date of birth, or simply words like “password” or “qwerty” that are easy to guess. Second, passwords entered on mobile devices such as tablets or smartphones are susceptible to “smudging attacks”, i.e. the deposit of grease on the touchscreen that can be used to allow imposters to guess passwords. Finally, password authentication is also vulnerable to “shoulder surfing”.This type of attack occurs when an impostor can directly observe or use external recording devices to collect user information. This attack has attracted the attention of many researchers in recent years due to the increasing deployment of mobile recording devices and public surveillance infrastructure. The biometric identification system is ready to meet these challenges by combining both levels of security and convenience. This study evaluates the benefits and potential of integrating biometrics into mobile password authentication systems, by requiring users to draw each digit of the password on a touch screen instead of typing the password as usual. In this way, standard authentication systems are improved by integrating dynamic handwritten biometric information. One use case is the internet using credit cards. Banks often send numeric passwords (usually 6 to 8 digits) to the user's mobile devices.

II. REVIEW OF LITERATURE

Ruben Tolosana; and Ruben Vera-Rodriguez et al.,2020 [3] proposed this work enhances two-word protection through two-factor authentication. This user draws each character of the word rather than codifying them as usual. They presented the Novel Mobile Touch DB public database. This database contains more than 64K online character samples tested by 217 stoners with 94 different smartphones up to 6 accession sessions. They performed a complete analysis of both traditional authentication systems analogous to Dynamic Time torturing (DTW) and intermittent Neural Networks(RNNs). This complete analysis of the proposed approach is carried out using both Mobile Touch DB and e-memoir Digit DB database. They had using 4 number of words and one training sample per character. These results encourage the deployment of the proposed approach in comparison with traditional compartmented predicated word systems where the attack would have a 100 success rate under the same fraud script.

Ruben Vera-Rodriguez, Ruben Tolosana, et al.,2021 [4]They had proposed the biometric tasks using the Sigma--Log-Normal model of the Kinematic proposition of rapid-fire-fire mortal movements and it's used for several operations, They reported experimental work for the operation of the Sigma- Log-Normal model to predict the biometric task for two case studies. online hand recognition to induce user predicated complexity groups and discovery of age groups(children from grown-ups) using touch screen patterns. These results show the benefits of using the Sigma-LogNormal model for modeling the complexity of biomechanical tasks in the two case studies considered.

Marcos Faudez-Zanuy, Jiri Mekyska, et al., 2021 [5] They had proposed behavioral signals(handwriting), in contrast to morphological bones (iris, point, hand figure) is the possibility of asking a user to perform multitudinous different tasks. This composition recently found the different handwriting delineation tasks in the field of security and health. They concentrated on online handwriting and hand-predicated commerce digitizing devices like smartphones and tablets during the consummation of the tasks. These biases permit the accession of on-face dynamics as well as in air movements in time, it's a ricer information when compared to the conventional pen and paper system. They had epitomized only those furnishing competitive results having a significant impact in the field.

Marcos Faundez-Zanuy, Julian Fierrez, et al.,2020 [6] They had proposed multiple operations in e-security, hand biometrics is the most popular but not the only one. Handwriting analysis also has an important set of operations in e-health. Both operations have some unsolved questions and relations. They had epitomized the state of the art and operations predicated on handwriting signals. They concentrated on the main achievements and challenges that should be addressed by the scientific community. They had commented on the significance of considering security and health. These are especially critical due to the risks essential when using these behavioral signals.

Sara Marullo, Maria Pozzi, et al., 2022[7] They had proposed a new hand posture called Finger Pen, Which involves a grip formed by the hand on the index croquette. Digital technologies have reduced the necessity for traditional pen-and-paper notation. The positive cognitive impact of Handwriting and digital notation is to use suitable tools to write over touchscreens or plate tablets. This system comparison with the most common posture that people tend to assume is carried out utilizing a biomechanical model. The results of a user study that the Finger Pen system is favored by stoners.

Se-RaMin, Young-Jin Jung, et al., 2020[8] compared upper extremity muscle exertion during handwriting tasks on paper and touchscreen among young grown-ups and the elderly. Muscle exertion is measured using electromyography in various arm muscles. These results showed lower muscle exertion in youthful grown-ups compared to the elderly, and lower exertion in the dominant hand compared to the non-dominant hand. also, muscle exertion was lower when writing on a touchscreen compared to paper. These results can be used to support touchscreens in the elderly. Also, they can be used as birth data for comparing the performance of- the paretic side and paretic side in cases relative to the central nervous system.

Thameur Dhieb, Sourour Njah, et al.,2020 [9] They had proposed a biometric predicated recognition system forensics document examination suitable for relating a document's author. Biometric systems have demonstrated an important enhancement in writing identification from online handwriting. pen identification is a challenging task in the description of a set of features suitable to characterize the different samples of handwriting documents. This system consists of the preprocessing and the segmentation of online handwriting into a sequence of strokes in the first step. also, from each stroke, They prize a set of static and dynamic features. ultimately, they used a Deep Neural Network as a classifier trial which is conducted on handwriting and ADAB databases, These results have been mileage for forensic examinations of handwriting.

III. RESEARCH METHODOLOGY

In the current system, a handwritten signature is one of the most socially accepted biometrics as it has been used in financial and legal agreements for many years and it also finds applications in mobile scenarios. These approaches are based on the combination of two authentication stages. Some of the challenges and problems in this type of authentication are the amount of data requested by the user during the enrolment and the security level provided by the biometric system. From the point of view of the security system, it seems clear that the ideal case would be to have as much information about the user as possible[10]. To overcome these problems this proposed system focuses on providing user-friendly mobile applications ensuring data protection and high security. Users should draw each digit of the password on the touch screen instead of typing them as usual. This way, the traditional authentication systems are enhanced by incorporating dynamic handwritten biometric information. This system involves two stages of authentication the drawn pin should be similar to the pin entered during the registration process.

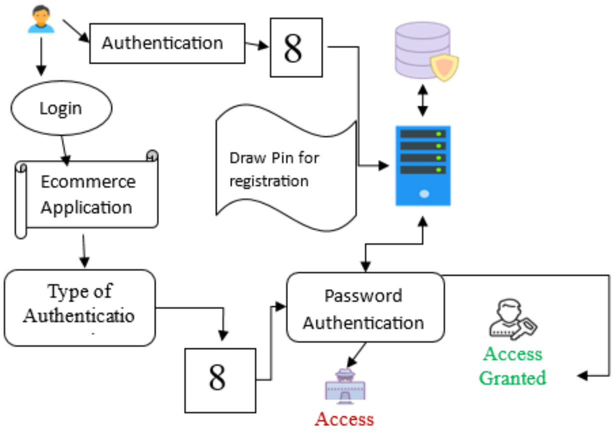
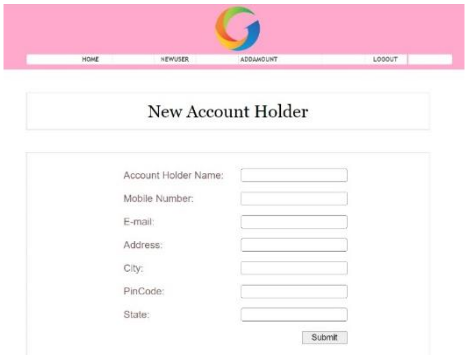


Fig. 1 Architecture Diagram

The second stage of authentication involves multiple options based on user preference where the user can set multiple sets of combinations. Users can set second-stage passwords as stroke, time, screen brightness, or sensor-based authentication system[11]. The incorporation of biometric information on traditional password-based systems can improve security through a second level of user authentication. These approaches enable active or continuous authentication schemes, in which the user is transparently authenticated. A handwritten signature is one of the most socially accepted biometrics. The incorporation of biometric information on traditional password-based systems can improve security through a second level of user authentication. Fig. 1 represents the architecture diagram of the project.

This research methodology starts by running a local Tomcat server in the same system, opening the bank webpage logging in as administrator then clicking the new account to create a new account holder. Fill in the details such as Name, E-mail, City, PIN code, and State then click submit. Fig. 2 shows the user registration steps for New Account Holder.

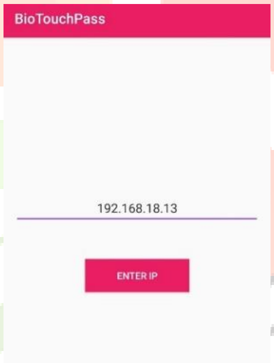


New Account Holder

Account Holder Name:
Mobile Number:
E-mail:
Address:
City:
PinCode:
State:

Fig. 2 User Registration Steps for New Account Holder

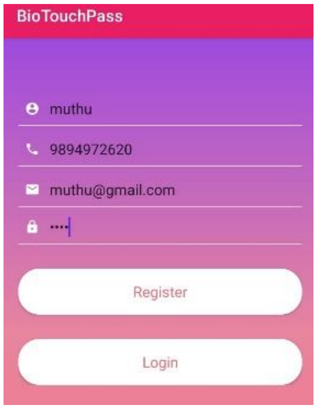
The submitted registered data is forwarded to the MySQL Database and then click the add amount tab to add the amount to the registered user account. Add the amount in rupees for the account holder. Check the data is saved in the MySQL server. Ensure that the network for the PC is hosted by the phone with the Mobile APK to perform every action on the local machines. Find the IP address of the computer to make a connection between the host phone and the computer[12]. Once the IP address is noted down, Install the APK in the smartphone, which is built in Android Studio for the Handkey-BioLock. Open the application on the smartphone. Fig. 3 represents the IP Address of the Local Machine in the Mobile App.



192.168.18.13

Fig. 3 Displaying IP Address of Local Machine in Mobile App

Enter the IP address of the computer in the IP address dialogue box. The user has an initial level Registration Process. The users provide their, own personal information for this process. The server in turn stores the information in its database and user can view a list of products on their page multiple list of products and their details. Fig. 4 shows the user registration steps for logging in to the E-Commerce App.



muthu
9894972620
muthu@gmail.com
••••

Fig. 4 User Registration in E-Commerce App

The E-Commerce web application can be viewed with the products. Users can select a list of products they wish to purchase. The selected product will be listed on a cart page and the user can initiate general purchase information that has to be filled in[13]. Completing general details, check bank details in the UPI tab within the application and then the user has to generate their four-digit PIN one by one screen using the password writing space. Fig. 5 shows the list of products in the Application.

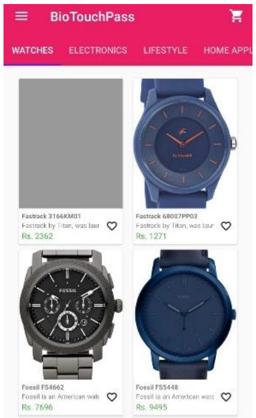


Fig. 5 Displaying the list of products

The drawn password is then converted into an image through Optical Character Recognition (OCR) numbers from each image fetched and verified with the user password. User has to register their four-digit password with multiple strokes during their registration process once the process is completed during the confirm password. The user has to confirm their password with the same password with stroke has to be verified. Strokes for each drawn digit should match with strokes given at the time of registration. Spyware attacks will be avoided by proposing the idea of using screen brightness as an authentication tool. The Android secure environment generates the 6-digit binary value. Based on the binary digit the brightness of the screen is changed to high or low. If the screen brightness is high, the user should input the correct PIN digit. Otherwise, the user should give the wrong and random PIN. The system will remove the digits inserted while the screen brightness is low apply the HMac algorithm for the PIN given by the user and generate the Signature for the user PIN which is a digestible Value to avoid a MAN-IN-MIDDLE attack. The server gets the signature of user generated PIN, generates the signature value for the Original PIN, and compares two signatures. If the two Signatures are equal, the user can access the Profile of the user. If not user cannot access the profile. After successful creation, shop any products, click buy now, then go to the payment page. Fig. 6 represents the authentication of 4-digit handwritten passcode.

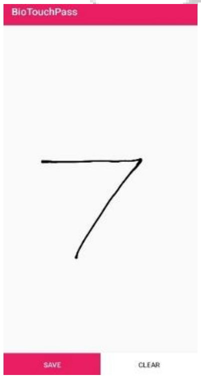
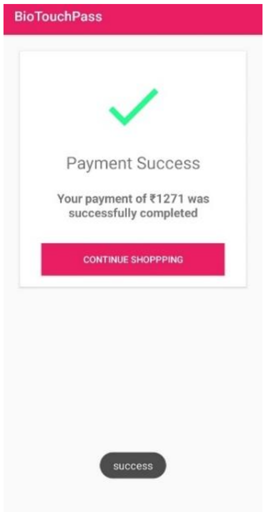


Fig. 6 Authentication of 4-digit Handwritten Passcode

Enter the registered Hand Written Password to finish the payment with the step verification method successfully. When entering the registered password for verification the brightness of the screen will increase and decrease. To create a look-a-like 8-digit password combination. To confuse anyone who can see the password while entering it. While increasing in brightness enter the correct registered value whereas enter the random value for decreased brightness. After the successful payment, the product is purchased.


BioTouchPass

Payment Success

Your payment of ₹1271 was successfully completed

Fig 7 Displaying the Payment Successful Pop-up Screen after Purchase

If the password is wrong or incorrect, the web application will cancel the payment. Thus, the workflow of the project is explained. Fig. 7 represents the Payment Successful popup screen after purchase.

IV. CONCLUSION

This research paper explored the feasibility and effectiveness of a new authentication method called "Handkey-Bio Lock," which leverages handwritten passwords to authenticate touchscreens using a character recognition algorithm Optical (OCR). Through further exploration and implementation of this approach, we discovered several important findings and implications for the field of touchscreen authentication and security [14]. Above all, this investigation demonstrated the feasibility of using handwritten passwords as a means of authentication on touchscreen devices. By leveraging the unique biometric characteristics of each individual's handwriting, Handkey-Bio Lock offers a promising alternative to traditional alphanumeric passwords or biometric methods such as fingerprints, and hand or face recognition. Handwritten passwords, which are inherently variable and complex, can improve security while remaining intuitive for users to create and remember. Additionally, the implementation of the OCR algorithm highlights the importance of robust and accurate character recognition during authentication.

The effectiveness of Handkey-Bio Lock depends on the ability of the OCR algorithm to accurately interpret handwritten characters under a variety of conditions, including different handwriting styles, sizes, and orientations. Through meticulous optimization and improved OCR techniques, we have achieved promising results in accurately translating handwritten passwords into digital representations for authentication purposes. In addition to its technical feasibility, the Handkey-Bio Lock offers several notable advantages in terms of ergonomics and user experience. Unlike traditional alphanumeric passwords, which can be difficult to enter on touchscreen devices, handwritten passwords provide a more natural and intuitive means of authentication. Users can leverage their handwriting habits and preferences, delivering a seamless and personalized authentication experience. Additionally, handwritten passwords are inherently easy to remember and unique, which can improve security while minimizing the risk of forgotten passwords or unauthorized access.

From a security perspective, Handkey-Bio Lock introduces a new layer of authentication that complements existing methods and mitigates common vulnerabilities associated with touchscreen devices. By combining handwriting biometrics with OCR-based identification, Handkey-Bio Lock improves the resilience of authentication systems against traditional threats such as brute force attacks, password mining, and web browsing. Additionally, the dynamic nature of handwritten passwords with a variable element can prevent automated attacks and unauthorized access attempts. The Handkey-Bio Lock authentication method offers a promising paradigm shift in touchscreen security, leveraging handwritten passwords and OCR algorithms to improve both security and user experience. Through extensive investigation and implementation, we have demonstrated the technical feasibility, usability, and security benefits of this innovative approach. As touchscreen devices continue to proliferate in a variety of sectors, Handkey-Bio Lock is poised to become a compelling solution for secure and intuitive authentication in the digital age.

REFERENCES

[1] Kiran, K. C. (2023). Analyzing Capacitive Touchscreen Data Towards User Authentication, Identification, and Gender Classification. Southern Connecticut State University.

[2] Alamleh, H., AlQahtani, A. A. S., & Al Smadi, B. (2023, April). Secure Mobile Payment Architecture Enabling Multi-factor Authentication. In 2023 Systems and Information Engineering Design Symposium (SIEDS) (pp. 19-24). IEEE.

[3] Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. (2020). Deepfakes and beyond A survey of face manipulation and fake detection. Information Fusion, 64, 131-148.

[4] Faundez-Zanuy, M., Fierrez, J., Ferrer, M. A., Diaz, M., Tolosana, R., & Plamondon, R. (2020). Handwriting biometrics: Applications and future trends in e-security and e-health. Cognitive Computation, 12, 940-953.

[5] Faundez-Zanuy, M., Mekyska, J., & Impedovo, D. (2021). Online handwriting, signature, and touch dynamics: tasks and potential applications in the field of security and health. Cognitive Computation, 13, 1406-1421.

[6] Faundez-Zanuy, M., Fierrez, J., Ferrer, M. A., Diaz, M., Tolosana, R., & Plamondon, R. (2020). Handwriting biometrics: Applications and future trends in e-security and e-health. Cognitive Computation, 12, 940-953.

[7] Marullo, S., Pozzi, M., Malvezzi, M., & Prattichizzo, D. (2022). Analysis of postures for handwriting on touch screens without using tools. Scientific reports, 12(1), 296.

[8] Min, S. R., Jung, Y. J., Yoon, T. H., Jung, N. H., & Kim, T. H. (2020). Comparison of Muscle Activity Between Handwriting and Touchscreen Use in Younger Adults and the Elderly. International Journal of Contents, 16(1), 57-64.

[9] Dhieb, T., Njah, S., Boubaker, H., Ouarda, W., Ayed, M. B., & Alimi, A. M. (2020). Towards a novel biometric system for forensic document examination. Computers & Security, 97, 101973.

[10] Sharma, P., & Jasuja, O. P. (2024). Forensic examination of digitally captured handwriting review of contemporary tools and techniques. International Journal of Electronic Security and Digital Forensics, 16(3), 357-371.

[11] Sharma, D., Parashar, V., & Parashar, A. (2024). Identification of Personality Traits by Machine Learning Analysis of Signatures and Handwriting. SN Computer Science, 5(5), 497.

[12] Kumar, R., & Awasthi, S. (2024). Mobile Handwritten Signature Verification and Identification Using PCA for RemoteAuthentication.

[13] Akhundjanov, U. (2024). ADVANCEMENTS IN HANDWRITTEN SIGNATURE VERIFICATION. Journal of technical research and development, 1(1).

[14] Lakshmi, A. A., Reddy, G. S., Reddy, M. S., & Kathirisetty, N. (2024, January). Offline Signature Forgery Detection Based on Geometric Measures Using Tensorflow Model. In 2024 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC) (pp. 1-7). IEEE.