IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

IMAGE SEGMANTATION ALGORITHMS FOR SECURITY AUTHENTICATION

[1]Mrs.K.Sudhadevi, [2]Madesh.R, [3]Jeeva.v,[4]Krishna Kumar

[1]Assistant Professor, [2]student, [3]student [4] student
Department of Computer Science and Engineering
Paavai Engineering College(Autonomous)
Pacahal,Namakkal,Tamil Nadu .,India

Abstract : A Personal Identification Number (PIN) is a sequence of digits that confirms the identity of a person when it is successfully presented. The maturity of PIN authentication is a result of its continuous usage for years in a wide range of everyday life applications, like mobile phones and banking systems. PIN authentication is susceptible to brute force or even guessing attacks. IPIN uses the technique of hybrid images to blend two keypads with different digit orderings in such a way, that the user who is close to the device is seeing one keypad to enter her PIN, while the attacker who is looking at the device from a bigger distance is seeing only the other keypad. To overcome shoulder-surfing attacks on authentication schemes by proposing Illusion PIN (IPIN), a PIN-based authentication method that operates on touch screen devices. The user's keypad is shuffled in every authentication attempt since the attacker may memorize the spatial arrangement of the pressed digits. The visibility algorithm forms the core of our work and we would like to examine whether it can be used to assess the visibility of images other than hybrid keypads. Visibility algorithm could be used to assess the visibility of general images, but its parameters have to be appropriately tuned for the particular task at hand

***IndexTerms* - Component,formatting,style,styling,insert.**

INTRODUCTION

Visual cryptography is a method for protecting image-based secrets that has a computationfree decoding process. Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc) to be encrypted in such a way that the decryption can be performed by the human visual system without the aid of computers. As network technology has been greatly advanced, much information is transmitted via the Internet conveniently and rapidly. At the same time, the security issue is a crucial problem in the transmission process. In this project we proposed a visual cryptographic system using Color Palettes. In this RSA algorithm Encryption and Decryption provides solution for both individuals and corporations. Using this encryption user can easily encrypt and decrypt text (messages), so you can send emails from home or office in a safe way. The proposed method is a simple, practical and effective cryptographic system. The text information is encrypted and stored in the Color Palettes. Initially user has to give the secret key in order to encrypt the text. Later, when the recipient decrypts the text, the secret key he/she enters is and compared with the stored color palette. And, in case, the secret key the recipient enters matches the stored key, encrypted message will be successfully decrypted

RESEARCH METHODOLOGY

[1] Ankita Karia..,Password-based authentication is the most commonly used method for gaining access to secured systems. Unfortunately, empirical evidence highlights the fact that most passwords are significantly weak and encouraging users to create stronger passwords is a significant challenge. In this research, we propose a theoretically augmented password strength meter design that is guided by the Elaboration Likelihood Model of persuasion (ELM). We evaluate our design by leveraging three independent and complementary methods: a survey-based experiment using students to evaluate the saliency of our conceptual design (proof-of-concept), a controlled laboratory experiment conducted on Amazon M Turk to test the effectiveness of the proposed design (proof-of-value), and a randomized field experiment conducted in collaboration with an online forum in Asia to establish proof-of-use. In each study, we observe the changes in users' behavior in response to our proposed password strength meter. We find that

the ELM augmented password strength meter is significantly effective at addressing the challenges of password-based authentication. Users exposed to this strength meter are more likely to change their password, leading to a new password that is significantly stronger. Our findings suggest that the proposed design of augmented password strength meters is an effective method for promoting secure password behavior among end users.

[2] Aparna M.S,..,Biometric systems input physical or personal human characteristics for identification, authentication, and security purposes. With the advancement in communication and intelligent security systems, biometrics are programmed to validate electronic signatures (E-signatures) for online and offline authentication. This article introduces a dynamic signature verification technique(DSVT) using mutual compliance (MC) between the security system and the 3 biometric device. The security system is responsible for online and offline signature approval using personal inputs from humans. This personal verification is related to the stored online/offline signatures using certificates provided for authentication. The certificate-based authentication is valid within a session for online representation. Contrarily, this authentication is valid for persons under offline conditions. In this mode of segregation, application-level authentication verification is performed. A conventional tree classifier for dynamic signature verification is used for differentiating online and offline signatures.Moreover, the security metrics—such as signing bit, key, and size—are verified for both modes using classifier learning. For the segregated mode, the validation of the above is required to be unanimous to accelerate the dynamicity. The proposed technique's performance is analyzed using the authentication success rate, verification failing ratio, verification time, and complexity.

[3] Nasir Memon…,Present-day smartphones provide various conveniences, owing to high-end hardware specifications and advanced network technology. Consequently, people rely heavily on smartphones for a myriad of daily-life tasks, such as work scheduling, financial transactions, and social networking, which require a strong and robust user authentication mechanism to protect personal data and privacy. In this study, we propose draw-a-deep-pattern (DDP)—a deep learning-based end-to-end smartphone user authentication method using sequential data obtained from drawing a character or freestyle pattern on the smartphone touchscreen. In our model, a recurrent neural network (RNN) and a temporal convolution neural network (TCN), both of which are specialized in sequential data processing, are employed. The main advantages of the proposed DDP are (1) it is robust to the threats to which current authentication systems are vulnerable, e.g., shoulder surfing attack and smudge attack, and (2) it requires few parameters for training; therefore, the model can be consistently updated in realtime, whenever new training data are available. To verify the performance of the DDP model, we collected data from 40 participants in one of the most unfavorable environments possible, where in all potential intruders know how the authorized users draw the characters or symbols (shape,direction, stroke, etc.)

[4] Andreas Bulling…,Recent advances in machine learning and natural language processing have fostered the enormous prosperity of smart voice assistants and their services, e.g., Alexa, Google Home, Siri, etc. However, voice spoofing attacks are deemed to be one of the major challenges of voice control security, and never stop evolving such as deep-learning-based voice conversion and speech synthesis techniques. To solve this problem outside the acoustic domain, we focus on head-wearable devices, such as earbuds and virtual reality (VR) headsets, which are feasible to continuously monitor the bone-conducted voice in the vibration domain. Specifically, we identify that air and bone conduction (AC/BC) from the same vocalization are coupled (or concurrent) and user-level unique, which makes them suitable behavior and biometric factors for multi-factor authentication (MFA). The legitimate user can defeat acoustic domain and even cross- domain spoofing samples with the proposed two-stage Air Bone authentication. The first stage answers whether air and bone conduction utterances are time domain consistent (TC) and the second stage runs bone conduction speaker recognition (BC- SR). The security level is hence increased for two reasons: (1) current acoustic attacks on smart voice assistants cannot affect bone conduction, which is in the vibration domain; (2) even for advanced cross-domain attacks, the unique bone conduction features can detect adversary's impersonation and machine- induced vibration. Finally, Air Bone authentication has good usability (the same level as voice authentication) compared with traditional MFA and those specially designed to enhance smart voice security. Our experimental results show that the proposed Air Bone authentication is usable and secure

PROBLEM DEFNITION

At the time of registration, a user creates a graphical password by first entering a picture he or she chooses. The user then chooses several point-of-interest (POI) regions in thepicture. Each POI is described by a circle (center and radius).For authentication, the user first enters his or her username. The system, then, displays the registered picture. The user, then, has to correctly pick the POIs and type the associated words.

OVERVIEW OF THE PROJECT

At any time, typed words are either shown as asterisks (*) or hidden. In Figures, we show an example of the login screen. For every POI, the user types a word or phrase that would be associated with that POI. If the user does not type any text after selecting a POI, then that POI is associated with an empty string. The user can choose either to enforce the order of selecting POIs (stronger password), or to make the order in significant. In Figures, we show an example of a user creating a graphical password. In this example, the user chooses a picture of his or her kids by pressing "Load Image button". Then the user clicks on the kidsfaces in the order of their ages (order is enforced).User authentication is a fundamental component in most computer security contexts. In this extended abstract, we proposed a simple graphical password authentication system. The system combines graphical and text-based passwords trying to achieve the best of both worlds. It also provides multi-factor authentication in a friendly intuitive system.

We described the system operation with some examples, and highlighted important aspects of the system. This security authentication project integrates advanced image segmentation algorithms with machine learning and cryptographic techniques to create a robust and intelligent system. The project encompasses multiple key components, including image pre processing to standardize input data, segmentation modules utilizing algorithms like U-Net or Mask R-CNN for precise region identification, and feature extraction techniques such as histogram analysis and edge detection. to enhance security, encryption techniques are implemented for secure communication between modules, along with measures to thwart adversarial attacks on the segmentation model

REGISTRATION MODULE

In this Module is used to the user register the information and set the password as a colour or images.

LOGIN MODULE

Authentication module is used to verify the user is authorized or not. When the user login to the system it checks the user entered image and database image, if it is correct the user is authorized user.

ACCESS USER APPLICATION

In this module is used to the user access the application after authentication process, itonly allow the authorized users.

GENERATE SECRET KEY

In this module is used to generate the secret key for every user where the secret key is referred as the image that has been used as the password . This secret key is used to maintain the information of the user with higher security which in case increases the higher security to the users

ENCRYPTION USING COLOUR PALETTE

In this module the user has to register their name and their details. The registered information will be stored in the database. User or administrator tries to check this site and entered correct login username and password. After that, this application checks to redirects 9 the required pages for administrator as well as user. The user has entered their important information, each text has convert to particular Colour. The images are randomly allocated to each text. Then image names only stored to database.

KEY VERIFICATION AND VIEW DATA

In this module the user's secret information are stored into the database, these information displayed only colour palette forma t. After the user is enter the secret key, if there are compare with database, and the information is downloaded. Then the user can view their information .

KEY DECRYPTION

Implement a decryption algorithm based on the extracted features.utilize cryptographic methods to enhance security, such as symmetric or asymmetric key decryption .integrate machine learning-based decryption for adaptive and intelligent authentication importance of key decryption is the core of the security authentication process, transforming extracted features into actionable authentication decisions.

SECURITY MEASURES AND VALIDATION

Integrate encryption techniques to secure communication between modules.implement measures to prevent attacks, such as adversarial attacks on the segmentation model .the testing and validation is to implement a comprehensive testing strategy to validate the accuracy and security of the system.Use diverse datasets for training and testing to ensure generalization.the importance is to rigorous testing ensures the reliability and effectiveness of the entire authentication system.

FEATURE EXTRACTION

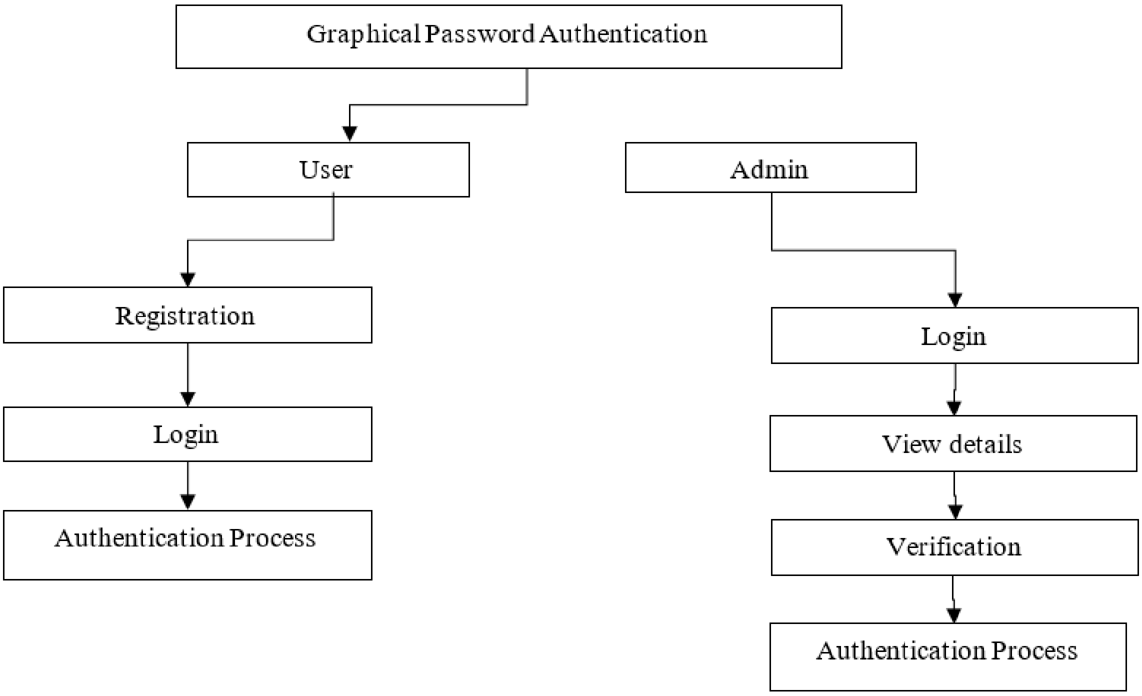
Extract key features from the segmented regions, such as color, texture, or shape characteristics.Use techniques like histogram analysis, edge detection, or texture analysis.importance of this are Feature extraction distills complex information into discriminative elements, facilitating subsequent analysis

PROPOSED SYSTEM

By using the proposed scheme the user can access and save the data in a secured manner which ensures the data privacy. The user has been provided username and password and additionally with an image as a password. The image password enhances the system with better security from which the data can be saved with high security. Each data has been saved on behalf of the image password which consists of n number or colour palettes.

SYSTEM ARCHITECTURE

A system architecture or systems architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. It can provide a plan from which products can be procured, that will work implement the overall system. There have been efforts to formalize languages to describe system architecture; collectively these are called architecture description languages (ADLs)



CONCLUSION

The graphical password authentication system is used to provide the more security for the authentication system. Where the user sets the image as a password and makes the data and the information with higher security. In future work it will be developed in the web application and it will be used for email, password and net banking etc,.,The Pass Points system presents a potential solution to the challenges associated with traditional alphanumeric passwords, which users often find difficult to remember and often create insecure e passwords. Graphical passwords offer a more intuitive and memorable alternative, where users click on images instead of typing alphanumeric characters. This paper has described the Pass Points system, its security features, and an empirical study that compared Pass Points to alphanumeric passwords. The results of the study showed that although the graphical group took longer and made more errors in learning the password, the difference was largely due to a few participants who had difficulty with graphical passwords. In the longitudinal trials, both groups performed similarly in terms of remembering their password, but the graphical group took more time to input their password. Overall, Pass Points appears to be a viable alternative to traditional passwords and warrants further exploration as a means of enhancing password security while maintaining usability.

Acknowledgment

We are gratefull to Mrs.K.Sudhadevi,M.E.,.,Assiatant professor CSE Department Paavai Engineering college(Autonomous) for mentoring us to present this paper successfull

REFRENCES

[1] Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud. Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies, 63:128–152, July 2005.

[2] Daniel V. Klein. Foiling the Cracker: A Survey of, and Improvements to, Password Security. In Proceedings of the 2nd USENIX UNIX Security Workshop, 2020

[3] Eugene H. Spafford. Observing reusable password choices. In Proceedings of the 3rd Security Symposium. Usenix, pages 299–312, 2018

[4] Michael Halvorson, Microsoft Visual Basic Professional, Microsoft Press Second Edition University of Washington in Seattle Jan 1, 2002

[5] Real User Corporation. The science behind passfaces, June 2019.

[6] Robert Morris and Ken Thompson. Password security: a case history. Communications ofthe ACM, 22:594–597, November 2021.

[7]Sigmund N. Porter. A password extension for improved human factors. Computers & Security, 1(1):54– 56, 2019.

.