Survey Paper
Gesture-Based Password Recovery

Team Members:

Vijayadharshni - 21BCE1072

Sharan Kumar - 21BCE1803

Abstract:

In today's digital world, ensuring the security of user credentials is paramount. Traditional password-based authentication systems often suffer from security vulnerabilities and user inconvenience. To address these challenges, we propose a Gesture-Based Password Recovery system that leverages hand gestures for secure and user-friendly password recovery. The system allows users to authenticate themselves by performing predefined hand gestures, which are captured and compared against previously saved gestures. If the current gesture matches the saved gesture, users are granted access to change their password. This approach enhances security by adding a biometric factor to password recovery, while also improving user experience by offering a more intuitive and secure authentication method.

The Gesture-Based Password Recovery system consists of three main components: gesture capture, gesture comparison, and password change. In the gesture capture phase, the system uses a camera to capture the user's hand gestures, which are then processed and analyzed. The gesture comparison phase involves comparing the captured gestures against previously saved gestures using a machine learning model. If the gestures match within a certain threshold, the user is authenticated and can proceed to change their password in the password change phase.

We implemented the Gesture-Based Password Recovery system using Python and OpenCV for gesture capture and processing, TensorFlow for machine learning model development, and Flask for the web interface. We evaluated the system's performance using a dataset of hand gestures and found that it achieves high accuracy and reliability in authenticating users. Our system offers a novel approach to password recovery, enhancing security and usability in digital authentication systems.

Introduction:

In today's digital world, ensuring the security of our personal information is paramount. Traditional text-based passwords, while commonly used, can be challenging to remember and vulnerable to security breaches. To address these issues, we propose a Gesture-Based Password Recovery system. This innovative approach replaces traditional passwords with hand gestures, offering a more secure and user-friendly authentication method.

The Gesture-Based Password Recovery system leverages hand gestures represented as tensors to authenticate users. By capturing and storing hand gestures as tensors during the initial setup, users can later use these gestures to recover their passwords securely. The system compares the current gesture input by the user with the previously stored tensor data. If the gestures match, the user is granted access to change their password, enhancing security and usability.

This project aims to enhance password security and user experience by introducing a biometric factor to the authentication process. By utilizing hand gestures, users can recover their passwords more securely and conveniently, reducing the reliance on traditional text-based passwords. This approach not only improves security but also offers a more intuitive and natural way for users to interact with authentication systems.

In the following sections, we will discuss the methodology, implementation, and evaluation of the Gesture-Based Password Recovery system, highlighting its benefits and potential applications in modern digital systems.

Literature overview:

Paper	Description	Methodology	Advantages and disadvantages
Picture Gesture Authentication: Empirical Analysis, Automated Attacks, and Scheme Evaluation	This study investigates picture gesture authentication, assessing its vulnerabilities through empirical analysis and introducing a novel attack framework based on a selection function concept to crack passwords in previously unseen pictures.	Collection of more than 10,000 picture passwords and Conducting an empirical analysis of picture gesture authentication using the collected dataset. Proposing a novel attack framework designed to crack passwords on previously unseen pictures in a picture gesture authentication system.	Picture gesture authentication offers a user-centric and visually intuitive method, potentially enhancing the user experience compared to traditional text-based passwords. The study's findings of a novel attack framework capable of cracking a considerable portion of picture passwords may highlight security vulnerabilities in this authentication method.
Password Recovery Using Graphical Method	The study employed a user-centric approach, involving 30 participants in testing a prototype implementation of graphical password recovery, with data analysis focused on attempts, timing, patterns, and user feedback.	Graphical password recovery typically involves users selecting or identifying images from a predefined set in a specific sequence or pattern, serving as an alternative method for authenticating or recovering passwords.	Advantages: User-friendly, easy to remember; Disadvantages: Potentially lower security, balancing usability concerns.

Image Based Password Authentication System	The proposed image-based password authentication system aims to overcome vulnerabilities associated with traditional text-based passwords, utilizing a randomized clickable image grid and a unique key generated during registration.	The system generates a unique key for each user during registration, encrypted alongside the username using cryptography. Authentication involves clicking on a randomized image grid, eliminating the need for traditional text-based passwords.	Potential complexity in managing and remembering image-based keys; reliance on user interaction with graphical elements may pose accessibility challenges.
Password Recovery Mechanism Based on Keystroke Dynamics	The paper explores various password recovery mechanisms, including secret questions, hints, One Time Passwords (OTP), and proposes a novel method based on behavioral biometric characteristics, specifically keystroke dynamics data, to enhance security and user identification.	The proposed password recovery mechanism incorporates behavioral biometrics, specifically analyzing keystroke dynamics data, alongside traditional methods like secret questions and hints, to enhance security and accurately identify users during the recovery process.	Improved security through keystroke dynamics data, providing a more robust password recovery mechanism compared to traditional methods. Potential challenges in implementation, user acceptance, and accuracy of keystroke dynamics analysis
Strong Zero-knowledge Authentication Based on Virtual Passwords	The paper introduces a robust zero-knowledge authentication system, SAVP, addressing privacy concerns in web applications	The methodology encompasses studying user habits, exploring password authentication evolution, emphasizing salt integration, and detailing cryptographic mechanisms to establish a robust zero-knowledge authentication system (SAVP).	Enhanced privacy and security through a robust zero-knowledge authentication system (SAVP). Potential complexity in implementation and user adaptation; reliance on cryptographic techniques may require careful maintenance and updates.

Methodologies and approches:

Method 1 - Using our own trained model

To implement a Gesture-Based Password Recovery system, we adopted the following methodologies and approaches:

- Data Preparation:
  We collected a dataset of hand gesture images to train a deep learning model using TensorFlow and Keras. The images were preprocessed using OpenCV to convert them to RGB format, resize them to 224x224 pixels, and normalize the pixel values.

- Model Training:

  We trained a deep learning model using the collected dataset to recognize hand gestures. The model architecture included layers for convolution and pooling, followed by dense layers for classification. The model was trained using the Adam optimizer and categorical cross-entropy loss function.
- Password Setup:

  Users were required to perform specific hand gestures during the setup phase, which were captured and saved as tensors. These gestures served as the user's password for authentication.

- Authentication Process:

  During authentication, users performed the same hand gestures captured during the setup phase. The gestures were processed using the trained model to predict the corresponding gestures.

- Password Recovery:

  If the predicted gestures matched the saved gestures, users were granted access to change their password. The system verified the gestures using a comparison function and allowed users to input a new password.

- Evaluation:

  We evaluated the system's performance by measuring the accuracy of gesture recognition and the effectiveness of the password recovery process. We also assessed the system's security by analyzing its vulnerability to automated attacks.
- User Interaction:

  The system provided a user-friendly interface for capturing gestures and changing passwords. Users interacted with the system through a webcam, and the gestures were displayed in real-time using OpenCV.

By adopting these methodologies and approaches, we developed a secure and user-friendly Gesture-Based Password Recovery system that offers an alternative to traditional text-based passwords.

Model Training:

To develop a gesture recognition model for the Gesture-Based Password Recovery system, we employed the following methodologies and approaches:

- Data Collection and Preprocessing:
  We collected a dataset of hand gesture images, organized into subdirectories based on the gesture labels. Each image was resized to 224x224 pixels and converted to RGB format to ensure consistency and compatibility with the model.

- Model Architecture:
  We designed a convolutional neural network (CNN) using the TensorFlow Keras API. The model consists of multiple convolutional layers followed by max-pooling layers to extract features from the input images. The final layers include dense layers with relu activation for classification.

- Training and Validation:
  We split the dataset into training and validation sets using the train_test_split function from scikit-learn. The training set was used to train the model, while the validation set was used to evaluate its performance and prevent overfitting.

- Model Compilation and Training:
  We compiled the model using the Adam optimizer and sparse categorical crossentropy loss function. The model was trained for 10 epochs with the training data, and the validation data were used to monitor its performance and adjust hyperparameters if necessary.
- Model Evaluation:
  After training, we evaluated the model using the validation set to measure its performance in terms of loss and accuracy. This step helped us assess the model's generalization ability and identify any potential issues.

- Model Saving:
  Finally, we saved the trained model to a file (gesture_model_ai.h5) for future use in the Gesture-Based Password Recovery system.

Method 2: Using mediapipe

To implement real-time hand gesture recognition for the Gesture-Based Password Recovery system, we utilized the following methodologies and approaches:

We employed the MediaPipe library, which provides pre-trained models for hand detection and landmark localization. This library allows us to detect multiple hands in a video stream and accurately locate landmarks (key points) on each hand, such as fingertips and joints.
Hand Detector Class:

We created a custom handDetector class to encapsulate the functionality of the MediaPipe hand detection and landmark localization models. This class provides methods for detecting hands in an image, locating landmarks on the detected hands, and calculating distances between landmarks to recognize gestures.
Gesture Recognition:

Using the handDetector class, we implemented a method to recognize specific hand gestures based on the positions of landmarks. By analyzing the spatial relationships between landmarks, we can determine if a certain gesture, such as a finger being raised, is being performed.
Real-Time Processing:

We integrated the hand gesture recognition functionality into a real-time video processing loop. This loop continuously captures frames from a webcam, detects hands and landmarks in each frame, and recognizes gestures in real time.
Performance Evaluation:

We evaluated the performance of our hand gesture recognition system by measuring the frame rate (fps) of the real-time processing loop. A higher frame rate indicates faster and more responsive gesture recognition, which is crucial for user interaction in the Gesture-Based Password Recovery system.
By employing these methodologies and approaches, we were able to develop a robust and efficient hand gesture recognition system for enhancing the security and user experience of the Gesture-Based Password Recovery system.

Findings and trends

The Gesture-Based Password Recovery project presents several key findings and trends that contribute to the field of password security and authentication methods:

- Biometric Authentication: The use of hand gestures as a biometric authentication method offers a novel approach to password recovery. By leveraging unique physical characteristics, such as hand movements, users can authenticate themselves more securely.

- Usability and User Experience: The project highlights the importance of usability and user experience in authentication systems. Gesture-based authentication provides a more intuitive and natural way for users to interact with the system, enhancing overall user satisfaction.

- Security Enhancements: Compared to traditional text-based passwords, gesture-based authentication offers enhanced security features. The use of hand gestures adds an additional layer of security, making it more difficult for unauthorized users to gain access.

- Challenges in Implementation: Despite its benefits, implementing gesture-based authentication systems comes with challenges. These include data collection and annotation, model complexity, user variability, and security and privacy concerns.

Challenges and gaps:

- Data Collection and Annotation:
  Challenge: Collecting a diverse and representative dataset of hand gestures can be challenging, especially for complex gestures or gestures performed by different individuals.
  Gap: There may be limitations in the dataset's size, diversity, and quality, which can impact the model's performance and generalization to real-world scenarios.

- Model Complexity and Performance:

Challenge: Designing a model that can accurately recognize a wide range of hand gestures while maintaining fast and efficient performance is challenging.

Gap: The selected model architecture may not be optimal for all types of gestures, leading to potential limitations in accuracy or speed.

- User Variability:

  Challenge: Users may perform gestures differently based on factors such as hand size, movement speed, and individual habits, making it challenging to create a universal gesture recognition system.

  Gap: The model may not be robust enough to handle variations in gesture execution, leading to potential authentication failures or usability issues.

- Security and Privacy Concerns:

  Challenge: Ensuring the security and privacy of the gesture-based authentication system is crucial, as gestures could potentially be observed or replicated by unauthorized individuals.

  Gap: There may be vulnerabilities in the system that could be exploited, such as insufficient protection of gesture data or insecure communication channels.

- Usability and User Experience:

  Challenge: Balancing security requirements with usability is challenging, as users may find complex or restrictive gesture patterns difficult or frustrating to use.

  Gap: The system may not be user-friendly or intuitive, leading to potential user resistance or abandonment of the gesture-based authentication method.

- Adaptability and Scalability:

  Challenge: Ensuring that the gesture recognition system can adapt to new gestures or environments and scale to accommodate a large number of users is challenging.

  Gap: The system may be limited in its ability to adapt to new gestures or may require manual intervention to update the gesture database, leading to maintenance challenges.

Future research directions:

- Enhanced Security Features: Research can be conducted to enhance the security features of gesture-based authentication systems. This may include developing more robust gesture recognition algorithms to reduce the risk of false positives and false negatives.

- Usability and User Experience Improvements: Future research can explore ways to improve the usability and user experience of gesture-based authentication systems. This may involve refining gesture recognition interfaces and providing feedback to users to make the authentication process more intuitive and user-friendly.

- Biometric Fusion: Investigating the fusion of multiple biometric modalities, such as hand gestures and facial recognition, could enhance the security and reliability of authentication systems.

- Adversarial Attacks: Research could focus on understanding and mitigating adversarial attacks on gesture-based authentication systems. This may involve developing techniques to detect and defend against attacks that attempt to spoof or deceive the system.

- Privacy and Ethical Considerations: Future research should also address privacy and ethical considerations related to biometric data collection and storage. This may include developing privacy-preserving authentication methods and ensuring compliance with relevant data protection regulations.

- Scalability and Deployment: Research can explore ways to scale gesture-based authentication systems for deployment in real-world settings. This may involve optimizing algorithms for performance and efficiency and addressing deployment challenges in diverse environments.

- Interoperability and Standardization: Establishing interoperability standards for gesture-based authentication systems could facilitate their adoption and integration with existing security frameworks.

- User Education and Awareness: Finally, research can focus on educating users about the benefits and best practices of using gesture-based authentication systems to enhance overall security awareness.

Conclusion:

In conclusion, the Gesture-Based Password Recovery project offers a promising approach to enhancing password security and usability. By leveraging hand gestures as a biometric authentication method, the project aims to address the limitations of traditional text-based passwords, such as complexity and memorability issues.

Through the implementation of a gesture recognition model trained on a diverse dataset of hand gestures, the project demonstrates the potential for a more secure and user-friendly authentication process. However, several challenges and gaps exist, including data collection and annotation difficulties, model complexity, user variability, security and privacy concerns, usability and user experience issues, and adaptability and scalability considerations.

Addressing these challenges and filling the identified gaps will be crucial for the successful deployment and adoption of gesture-based authentication systems. Future work should focus on improving the robustness and accuracy of the gesture recognition model, enhancing user privacy and security, and optimizing the system's usability and scalability.

Overall, the Gesture-Based Password Recovery project represents an innovative approach to password security, with the potential to revolutionize how users authenticate and recover their passwords in a more secure and user-friendly manner.