**Topic**: **Machine Learning Techniques for Biometric and Behavioral Authentication**

Project1 Submitted By: Adrian & Yilake Mengstie

Your Name

BOWIE STATE UNIVERSITY

CTEC402

Fall 2024

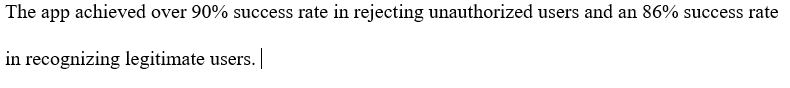
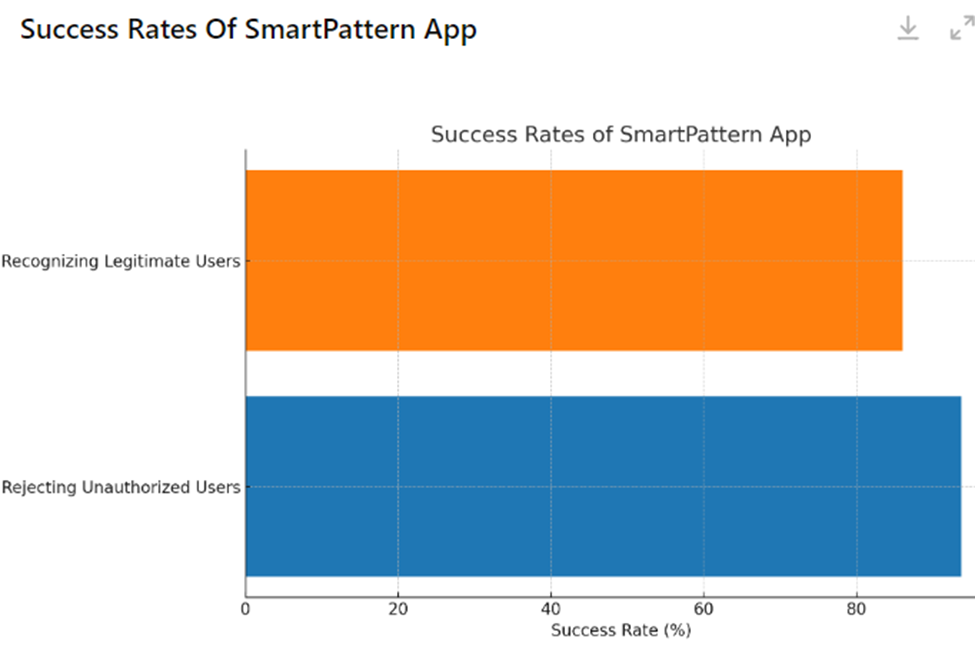
**1. Title: SmartPattern: Behavioral Biometric Authentication in Android Unlock Patterns through Machine Learning**

**1.1**: **Biometric-based authentication system for Android smartphones**

**Purpose:** This study aimed to improve the traditional Android pattern lock mechanism by integrating behavioral biometrics and machine learning.

In addition to providing a layer of defense by analyzing behavioral traits unique to each user that static pattern locks cannot offer, the system also adapts to natural variations in the user's behavior, like drawing the pattern more quickly on some days and slowly on others. This flexibility is a critical distinguishing factor of SmartPattern compared to conventional pattern locks, making it robust and user-friendly. This approach makes authentication secure and adaptable by considering how users interact with their devices and the physical patterns users draw [2].

**Methodology:** SmartPattern collects data by tracking each point's X and Y coordinates in the pattern and the time taken to move between points based on the user's pattern and how they draw it. Once the data is collected. These algorithms construct the behavioral profile of a legitimate user by learning from multiple samples of how the user typically draws a pattern [1]. It checks both the correctness of the pattern and whether the user's behavior while drawing matches the learned profile. By analyzing behavioral traits alongside physical patterns, SmartPattern ensures that only a legitimate user can unlock the device, even if the attacker knows the correct pattern.

**Result:** The app was evaluated with sixty-four users across two phases of testing. The results showed the following success rates [2]: **ChatGPT:** An Android Smart Pattern is a security feature that lets users unlock their devices by drawing a personalized pattern on a 3x3 dot grid, offering a visual alternative to traditional PINs and passwords. While it is easy to set up and use, its security is relatively lower compared to stronger authentication methods. If too many incorrect attempts are made, the device locks temporarily and can be unlocked using a linked Google account or other recovery options. This feature provides a balance of convenience and basic security for everyday device use.

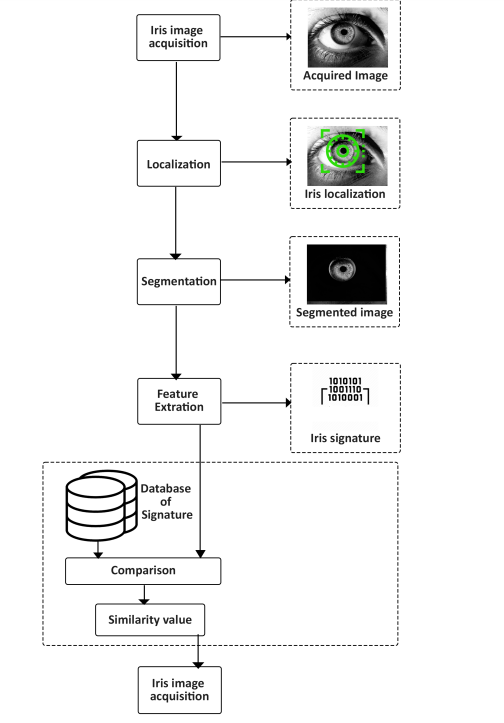
**2. A Comprehensive Overview on Biometric Authentication Systems Using Artificial Intelligence Techniques**

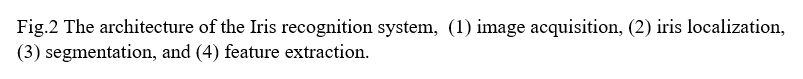
**2.1**: **Iris Recognition Using Machine Learning for Biometric Authentication**

**Purpose:** IRiss recognition is the most accurate biometric authentication method. The proposed method identifies individuals using machine learning and artificial intelligence analysis of iris patterns. In high-security environments like airports, the goal is to expedite and improve the accuracy of authentication processes [1].

**Methodology of The Study**: To obtain an image from the user's iris, the system uses a digital camera, and then the image undergoes various enhancements, including filtering, contrast enhancement, and histogram equalization, to enhance its overall quality. Techniques such as filtering, contrast enhancement, and histogram equalization are applied to improve image clarity. The iris is localized by detecting the boundaries of the iris and pupil using edge detection and fuzzy algorithms to identify key features. Furthermore, PCA (Principal Component Analysis) is another step in extracting the iris's most important statistical features. This step reduces the dimensionality of the data while retaining essential features. After feature extraction, the Support Vector Machine (SVM) algorithm is used to classify iris patterns and match new images to a database for identification [2].

**The Main Output of This Research:** An iris recognition system driven by machine learning achieves high accuracy; thus, it is ideal for use in sensitive settings, such as airport security. The proposed system employs PCA for dimensionality reduction and SVM for classification to deliver fast and reliable biometric authentication. The system maintains consistent performance under varying lighting and environmental conditions. This method links iris data with passenger travel information to realize quicker and more secure airport authentication. In high-security settings using PCA and an SVM, iris recognition delivers reliable and effective biometric authentication [2].



**ChatGpt**: Iris recognition using machine learning for biometric authentication involves capturing a digital eye image, preprocessing it to enhance quality, and then using Principal Component Analysis (PCA) to extract noteworthy features from the iris pattern. These features are then classified using a Support Vector Machine (SVM) algorithm to match the iris to a stored database for identification accurately. This method provides high accuracy, speed, and security, making it ideal for sensitive applications like airport passenger authentication, where fast and reliable identity verification is essential. Machine learning techniques improve the system's robustness against environmental variations, ensuring consistent performance in real-world scenarios.

3. **Title: Visual Altimetric for Robot Authentication**

**Purpose**: Identify and authenticate authorized robots by analyzing their visual characteristics, specifically facial recognition, which is the focus area of this research paper. This method confirms that it is possible to distinguish authorized robots from unauthorized or fake robots. The system assures that the robot’s identity uses facial detection and identification techniques like biometric authentication systems for humans [3].

**Methodology:** A robot face dataset is collected from physical or virtual avatars. Facial detection algorithms are applied to identify key features such as eyes, mouth, and nose. Once face detection is completed, the next step involves face identification, in which various recognition methods are applied to compare the detected face against a pre-stored template in the database. Knowledge-based approaches capture the relationships between facial features, and appearance-based techniques, for instance, PCA (Principal Component Analysis) and SVM (Support et al.), are the most critical steps for this methodology for statistical modeling and comparing the robot’s face for a match. Throughout the process, the system tests the robot’s ability to recognize various conditions, such as changes in lighting, camera angles, and facial expressions. By evaluating these variations, the authors improved the system’s ability to identify authorized users even in challenging environments accurately [3].

**Result**: The research confirmed that like human face recognition systems, robots can also be authenticated with an elevated level of accuracy. This method effectively ensures that authorized robots have the privilege to interact with humans or access restricted systems while unauthorized robots are detected and blocked. Security, human-robot interaction, and access control in robotics environments are some areas where we can implement this system [3].

**ChatGPT**: Visual Artimetrics for Robot Authentication refers to using visual characteristics, such as facial features or body movements, to verify the identity of a robot. Like biometrics for humans (e.g., facial recognition or fingerprint scanning), this technology ensures that the robot attempting to perform a task or access a system is an authorized entity rather than an unauthorized or fake one.

The concept revolves around analyzing a robot’s visual appearance—including its face, gestures, or other identifiable traits—using computer vision algorithms to compare these traits to a stored database of "authorized" robots. The goal is to securely and reliably authenticate robots in environments where identity matters, such as in sensitive areas like security systems, industrial operations, or public services. It can also be applied to virtual avatars in digital worlds.

In this context, " Artimetrics " refers to adapting biometric principles for artificial entities, extending the concept of authentication beyond biological beings to include robots and other non-human systems.

4. **Title**: **Embedded Face and Biometric Technologies for National and Border Security**

4.1 Embedded Face and Biometric Technologies for National and Border Security

**Purpose**:

This research aims to improve national and border security by applying advanced biometric technologies, including facial and iris recognition, for real-time identification of individuals, including undocumented travelers. Automating individual identification in high-traffic areas like airports ensures faster and more accurate processing, enhancing overall security [2].

**Methodology**:

In high-traffic zones, multi-region histograms and a face search engine process facial recognition data extracted from surveillance cameras, including face and iris images. The system, equipped with distributed computing and GPU acceleration, processed large real-time data volumes from high-definition cameras at high speeds [2].

**Output**:

Eleven (11) out of the fifteen (15) people of interest identified during the trial were accurately identified, resulting in an identification rate of 73%. Eleven out of twelve (12) cases of real-time recognition achieved 91% accuracy. The large-scale trial employed biometric data for real-time identification with minimal human intervention [2].

This system processes real-time biometric data from low-resolution images, allowing integration into existing CCTV networks. The system, employing facial recognition technology, tracks individuals across cameras autonomously. Authorities can also trace undocumented travelers, even if they have destroyed their papers, from their point of entry to establish their origin [2].

This system's unique ability to process biometric data in real-time, manage low-resolution images commonly found in surveillance systems, and integrate with existing CCTV networks. The system can identify individuals based on facial features and track them across multiple cameras without direct human oversight. Additionally, it addresses the undocumented traveler problem by allowing authorities to track individuals from entry points to identify their true origin, even if they have destroyed their documents [2].

**ChatGPT**: Face and biometric technologies use unique physical or behavioral traits, such as facial features, fingerprints, or iris patterns, for identification or authentication. These systems are widely applied in areas like security, access control, and identity verification, with facial recognition being a prominent example. Biometric identifiers offer a reliable way to confirm a person's identity by comparing their traits against a digital database. Real-time processing capabilities allow these systems to instantly verify or identify individuals, making them valuable for smartphones, border security, financial services, and other applications. These technologies enhance security, reduce fraud, and streamline access without traditional documentation.

**CITATION**

1. Albalawi, S., Alshahrani, L., Albalawi, N., Kilabi, R., & Alhakamy, A. A. (2022). A comprehensive overview of biometric authentication systems using artificial intelligence techniques. International Journal of Advanced Computer Science and Applications, 13(4), 1-11.
2. B. C. Lovell, A. Bigdeli and S. Mau, "Invited paper: Embedded face and biometric technologies for national and border security," CVPR 2011 WORKSHOPS, Colorado Springs, CO, USA, 2011, pp. 117-122, Doi: 10.1109/CVPRW.2011.5981830. keywords:
3. Torres, J., de los Santos, S., Alepis, E., & Patsakis, C. (2019, February). Behavioral Biometric Authentication in Android Unlock Patterns through Machine Learning. In ICISSP (pp. 146-154)
4. R. V. Yampolskiy and M. L. Gavrilova, "Artimetrics: Biometrics for Artificial Entities," in IEEE Robotics & Automation Magazine, vol. 19, no. 4, pp. 48-58, Dec. 2012, Doi: 10.1109/MRA.2012.2201574.