TITLE: Deep Learning Based Face Recognized Attendance Management System

The Deep Learning Based Face Recognized Attendance Management System is a project designed to modernize attendance tracking in educational institutions and organizations. The system uses Image Processing and Facial Recognition to solve issues like proxy attendance (when someone else marks attendance for another person), time inefficiency, and errors associated with manual methods.

Problem Statement:

Manual attendance systems are prone to vulnerabilities like proxy attendance, take a lot of time, and are prone to errors. While digital methods help, they may face connectivity problems that affect real-time reporting. This system aims to overcome these challenges by utilizing facial recognition technology to improve accuracy and speed.

Proposed Methodology:

Data Preparation: A dataset of known faces is stored, and the face to be recognized is placed in the appropriate folder.

Image Preprocessing: Converts the image to grayscale and applies histogram equalization for better recognition.

Face Encoding: Encodes known faces using the 'findEncodings' function.

Face Recognition: Uses the 'face_recognition' library to locate and encode faces in an image.

Attendance Marking: Recognized faces are matched with the dataset, and attendance is recorded in an Excel sheet.

Deployment: The system is integrated with Django and deployed on PythonAnywhere, making it accessible across multiple platforms like laptops and mobile devices.

System Requirements:

- Operating System: Windows, macOS, or Linux

- Processor: Intel Core i5 or higher

-Memory: 8GB RAM

- Storage: 256GB SSD

- Software Dependencies: Python 3.6+, OpenCV, face_recognition, Django

Conclusion:

The system offers a reliable and advanced alternative to manual attendance methods. It addresses connectivity issues faced in digital attendance systems while ensuring high accuracy, real-time monitoring, and improved efficiency in attendance management through the use of facial recognition technology.

The link for the IEEE paper on Deep Learning Based Face Recognized Attendance Management System: https://ieeexplore.ieee.org/document/10456032

Title: Digital Transaction Cyber-Attack Detection Using Particle Swarm Optimization

The project focuses on using Artificial Intelligence (AI) and Genetic Algorithms (GAs) to detect cyber-attacks in the digital world, emphasizing the need for enhanced cybersecurity given the growing threat landscape.

Abstract:

The digital world plays an essential role in daily life, with advancements in technology and AI used for cyber-attack detection. The project highlights the transformation of human lifestyles, with real-time updates and online interactions becoming part of everyday life. It also addresses security in areas like digital lending, mobile banking, cryptocurrency, and blockchain. A key focus is on using genetic algorithms for cyber-attack detection.

Introduction:

The increasing number of cyber-attacks poses a significant risk in the digital landscape. Network devices connected together are particularly vulnerable to hacking. Cyber threats can quickly disrupt data and demand immediate attention for damage control.

Problem Definition:

A network packet tracing mechanism is implemented using Java, responsible for ensuring the successful delivery of data packets from source to destination. The network layer handles packet routing decisions, with the project focusing on two specific genetic algorithms-Ant Colony Optimization (ACO) and Particle Swarm Optimization (PSO- to optimize packet routing and enhance security.

Proposed Methodology:

Genetic algorithms, inspired by natural selection, are used to solve complex problems efficiently. The algorithm works by:

1. Choosing an encoding type and population size
2. Randomly selecting an initial population
3. Selecting parent chromosomes
4. Applying crossover and mutation processes
5. Evaluating the offspring to find optimal solutions

Ant Colony Optimization (ACO): Inspired by how ants find the shortest path to food, ACO optimizes problems by mimicking the behavior of ants depositing pheromones to guide others.

Particle Swarm Optimization (PSO): Based on the social behavior of bird flocks, PSO solves optimization problems by updating particles' positions based on their own and the swarm's best experience.

Hardware and Software Requirements:

Hardware: Intel Core i5, 8GB RAM, 500GB SSD, Intel IrisXe Graphics, Windows 11

Software: Java

Conclusion:

The project demonstrates the effectiveness of AI in cyber-attack detection by comparing the ACO and PSO algorithms. Continued research and AI advancements, along with regulatory support, will help protect organizations from cyber threats in online transactions. In the future, this model can be applied to real-time online transactions using AI and genetic algorithms.

The link for the IEEE paper on Deep Learning Based Face Recognized Attendance Management System: https://ieeexplore.ieee.org/document/10585244