DeepGuard: A Deepfake Detection Solution

Abstract

DeepGuard is a highly accurate deepfake detection solution developed by computer science students. It combines deep learning algorithms and image processing techniques. The paper highlights its architecture, evaluation results, and potential applications in various domains. Ongoing research and development in deepfake detection are emphasized.
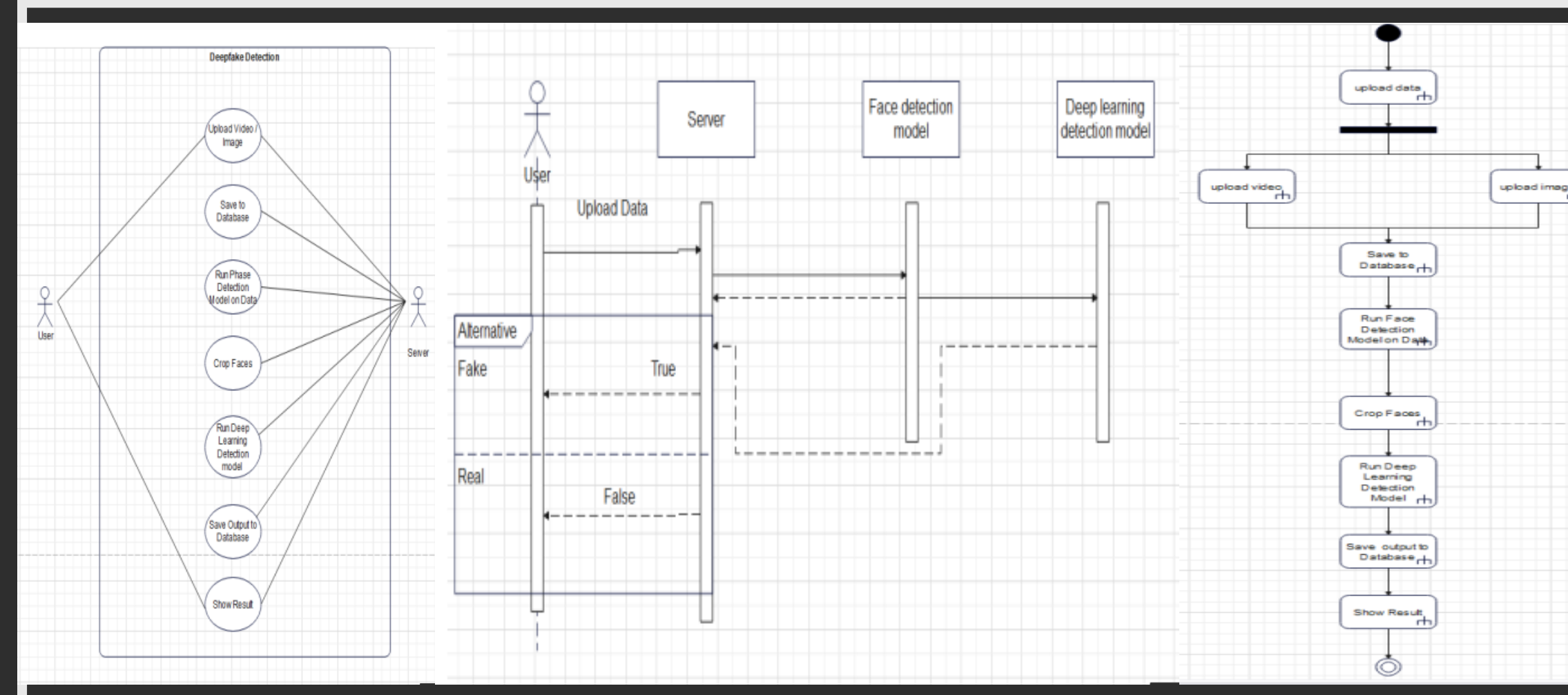
System Analysis

Technologies

Background

Deepfakes are manipulated media created using deep learning techniques, posing risks such as misinformation, privacy invasion, and fraud. Examples include political propaganda, revenge porn, and fraudulent activities. Deepfake detection is crucial for preventing misinformation, protecting privacy, maintaining trust in media, preventing fraud, and safeguarding national security.

Mobile App UI

Results

The performance of the DeepGuard deepfake classification model was evaluated using various metrics to assess its accuracy and effectiveness in detecting deepfake images and videos
• Accuracy (ACC): 95.13%
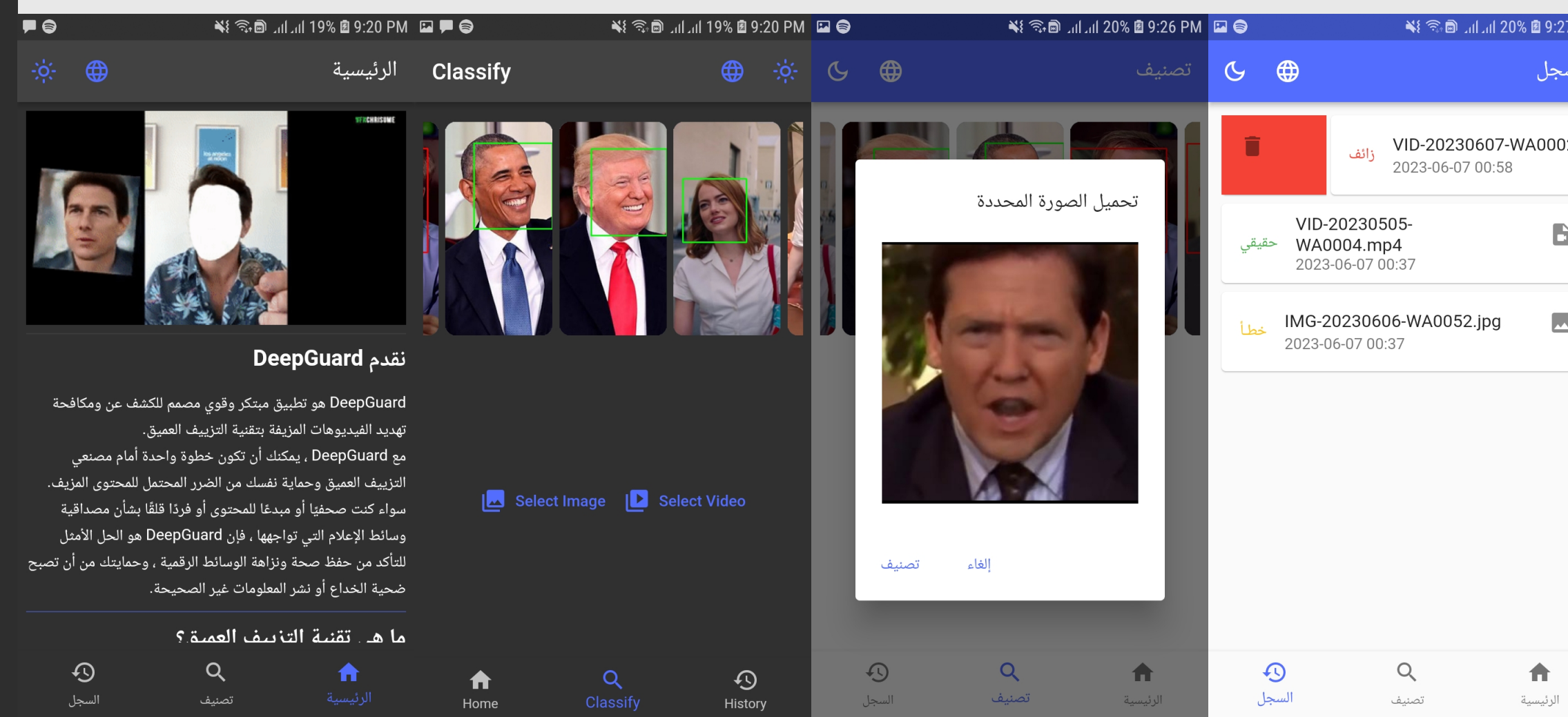• Precision: 96.52%
• Recall (Sensitivity): 94.76%

Objectives

The main objective of a deepfake detection project is to develop accurate algorithms and tools to detect and identify manipulated media, including images and videos, created using deep learning techniques. Specific objectives include developing deep learning models, creating datasets, analyzing deepfake characteristics, exploring additional techniques, developing user-friendly tools, and raising
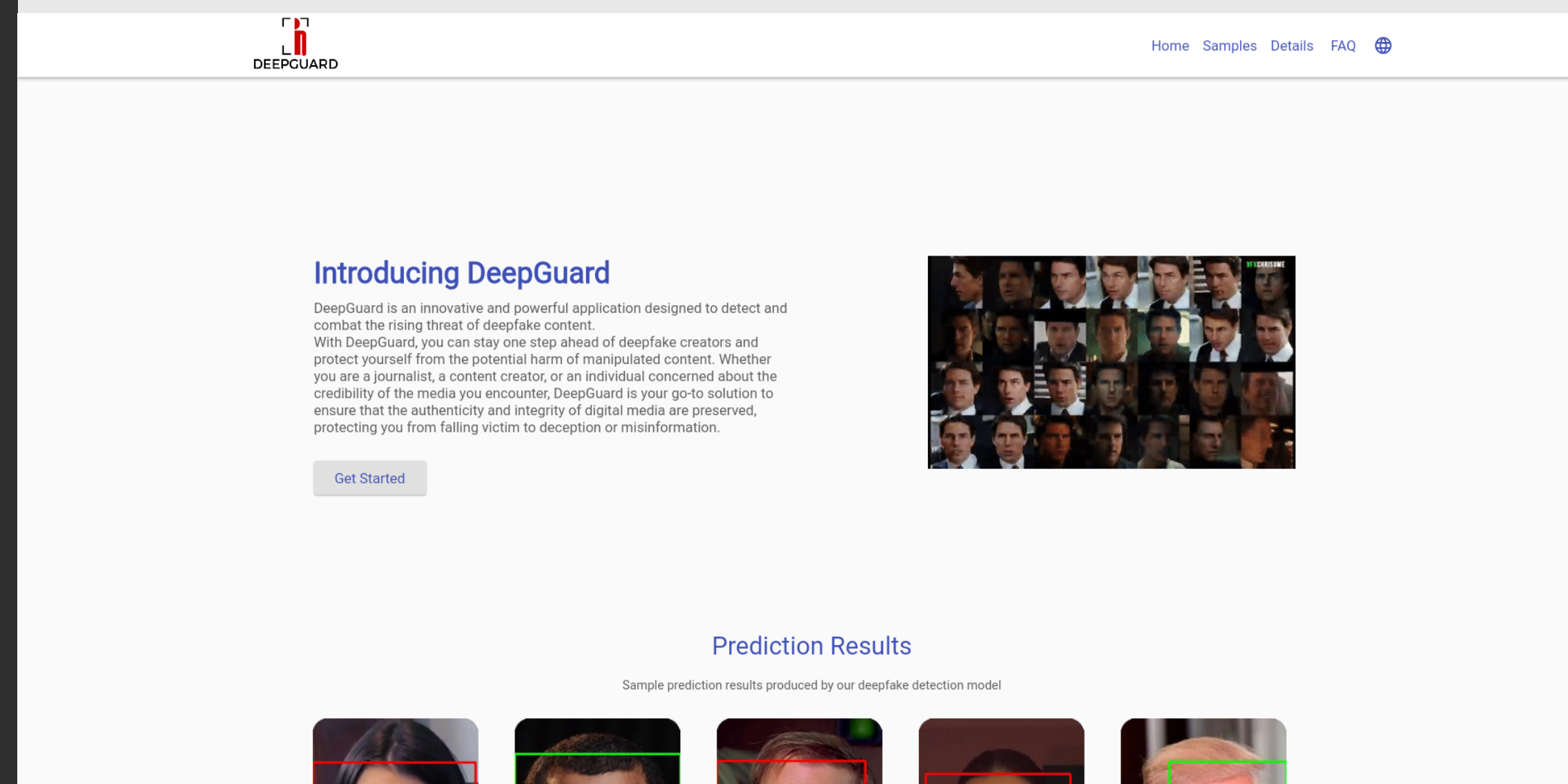
Web App UI

Conclusions

Deepfake detection projects utilize computer vision and AI techniques to identify manipulated media. Techniques include facial landmark detection, image and video forensics, and deep learning to analyse patterns and inconsistencies. Effective deepfake detection is crucial for combating disinformation and enabling informed media consumption.