DefakeBox@Edge: Real-Time Deepfake Detection on Embedded AI for Cybercrime Surveillance

Sweethijaya S
Student Department of Information Technology, Easwari Engineering College, Ramapuram, Chennai, India

Varshini M
Student Department of Information Technology, Easwari Engineering College, Ramapuram, Chennai, India

Saranya S
Assistant Professor, Department of Information Technology, Easwari Engineering College, Ramapuram, Chennai, India

Abstract:

Deepfake technology is a growing threat within the fields of digital forensics and anti-cybercrime, since fake videos have the ability to deceive investigations and delegitimize surveillance infrastructures. Conventional cloud-based detection strategies often suffer from latency, high computational requirements, and privacy issues. Addressing these concerns, this work presents DefakeBox, a handheld device driven by edge-based artificial intelligence designed exclusively to detect deepfakes in surveillance videos in real time. MATLAB is utilized in model training, signal preprocessing, and visualization while optimal lightweight models run directly on embeddable hardware to enable on- device inference. This setup ensures low-latency performance, offline functionality, and enhanced data privacy and makes it appropriate for permanent monitoring via CCTV or USB camera feeds. Alerts are issued via LCD display and buzzer and event logging supported by an ATmega328-based microcontroller for forensic evidence documentation. What is unique about DefakeBox is its handheld, affordable design that converges real-time edge intelligence and reliability and gives law enforcement agencies a powerful weapon against AI-based manipulation of videos.

Keywords:

Deepfake Detection, Edge AI, Embedded System, Video Surveillance, Cybersecurity, Digital Forensics, Real-Time Monitoring.