Vcamdetector: A Novel Dataset and Webcam Spoofing Detection System in Intelligent Proctoring Systems in Assessment Platform

Amadasun Osamuyimen

National Open University of Nigeria

Abstract

The rapid growth of online learning and online examination systems has created unprecedented challenges to academic integrity. Webcam spoofing is one of the principal vulnerabilities of smart proctoring systems, where examinees use virtual camera software to substitute live feeds with recorded videos or manipulated data, thus avoiding monitoring systems. This paper presents VCamDetector, a big dataset and detection framework specifically designed to identify virtual camera software in proctoring environments. We introduce a novel multi-modal approach combining device fingerprinting, video stream analysis, and behavioral pattern detection to discriminate genuine physical webcams against virtual camera applications. Our dataset contains over 5,000 video samples from 15 physical camera devices and 9 popular virtual camera software applications, which are labeled with 52 discriminative features across four categories: device-level signatures, stream properties, performance measures, and metadata patterns. We contrast various machine learning approaches and achieve 96.8% accuracy using our ensemble classifier, with an appreciable gain in performance compared to existing methods. Our findings indicate virtual cameras possess distinctive signatures in frame timing consistency, resource usage patterns, and hardware enumeration attributes. The VCamDetector dataset and system provide an effective framework for safeguarding intelligent proctoring systems against webcam spoofing attacks to maintain academic integrity for online education.

Keywords: Webcam Spoofing Detection; Virtual Camera Identification; Intelligent Proctoring; Academic Integrity; Online Examination Security; Device Fingerprinting; Deepfake Prevention