Abstract

CCTV cameras, often known as surveillance cameras, are among the most sophisticated security systems now available. Even though surveillance cameras (CCTV) are a security tool, it is common for them to be targeted to conceal a crime caught on camera. Video injection is one of the methods used to compromise surveillance cameras (CCTV). Video injection attacks insert live video feeds, resulting in a loss of data integrity that can impede or even alter the absolute truth. This paper employs the *ensemble learning* approach to recognize video injection attempts on security cameras. *Ensemble learning* utilized here is *random forest* and *support vector machine* (SVM) estimators. The *random forest* estimator-based model yields a f1-score value of 91% and an accuracy of 93% with a total dataset of 600 data, while the *support vector machine* (SVM) estimator yields a f1-score value of 84% and an accuracy of 87% with a total dataset of 12000 data. The accuracy of *random forest* is fairly high and may be used to identify video injection attacks.

Keywords: CCTV, video injection, *random forest, support vector machine* (SVM)