Penerapan Algoritma Ensemble Learning Berdasarkan Decision Tree Based Model untuk Mendeteksi Serangan Video Injection

Muhammad Naufal Abdillah[1], Vera Suryani[2],

[1,2]Fakultas Informatika, Universitas Telkom, Bandung
[1]@students.telkomuniversity.ac.id, [2]@telkomuniversity.ac.id

Abstract

In the last few decades, biometric detection technology has quickly gained popularity in strengthening security without placing additional burdens on a person to remember passwords or carry other forms of devices, and among the frequently implemented systems, the use of facial recognition system has a prominent role due to its wide use, ranging from smartphone systems to immigration control. However, due to its widespread use, there is an increasing concern about security threats that try to bypass the system, and one of these threats is a video injection attack, which is a form of attack that tries to deceive the sensors of the system, by using a video or image that is injected directly into the data stream or with a physical mask. To prevent damage, it is necessary to have an early detection of these attacks, and one way to detect them is through machine learning, specifically by using ensemble learning algorithms. This paper employs the ensemble learning algorithm by combining the XGBoost algorithm, along with the LightGBM. The ensemble model yields an f1-score value of 0.9217 with an accuracy of 92.5%, while the base estimators yield lower performance.

Keywords: facial recognition, video injection, ensemble learning, XGBoost, LightGBM