1. Pendahuluan

Dalam beberapa dekade terakhir, teknologi biometrik dengan cepat mendapatkan popularitas dalam memperkuat keamanan tanpa memberikan beban tambahan pada seseorang untuk mengingat kata sandi atau membawa perangkat lain [1, 2]. Sistem biometrik dirancang untuk mengenali individu secara otomatis dengan menganalisis karakteristik individu tersebut, dari perspektif biologis dan/atau perilaku. Di antara sistem yang sering diterapkan, penggunaan sistem pengenalan wajah memiliki peran penting karena penggunaannya yang luas, mulai dari di dalam aplikasi *smartphone* hingga imigrasi [2]. Namun karena penggunaannya yang luas, terdapat peningkatan kekhawatiran terhadap ancaman keamanan yang mencoba melewati sistem, dan salah satu ancaman tersebut adalah serangan *video injection* [3].

Dalam konteks sistem biometrik, serangan *video injection* adalah suatu bentuk serangan yang mencoba menipu sensor sistem, dengan menggunakan video atau gambar yang disuntikkan langsung ke aliran data atau dengan topeng fisik [1, 4]. Untuk mencegah rusaknya kerahasiaan data yang dijaga oleh sistem pengenalan wajah, diperlukan deteksi dini terhadap serangan-serangan tersebut, dan salah satu cara untuk mendeteksinya adalah melalui pembelajaran mesin, khususnya dengan menggunakan algoritma *ensemble learning*. *Ensemble learning* merupakan suatu metode pembelajaran yang menggabungkan beberapa algoritma yang sama (homogen) atau yang berbeda (heterogen) dengan beberapa cara seperti bagging, boosting, dan stacking, sehingga kinerja pengklasifikasi gabungan tersebut akan semakin kuat [5].

Penelitian yang dilakukan oleh Osisanwo dkk. [8] menganalisis kinerja beberapa algoritma klasifikasi seperti *Naive Bayes*, *Decision Tree*, *support vector machine* (SVM), dan *Neural Network* (*Perceptron*). Dalam penelitiannya dijelaskan bahwa semua algoritma yang dianalisa mempunyai kelebihan dan kekurangannya masing-masing, diantaranya adalah dalam beberapa hal algoritma berbasis Decision Tree lebih unggul dari algoritma lainnya dalam mengolah fitur yang tidak terlalu informatif dimana fitur jenis ini sering muncul di dalam data yang berbentuk tabular. Algoritma berbasis *Decision Tree* juga memiliki performa yang lebih baik dibandingkan *Neural Network Perceptron* pada dataset kecil, dan untuk dataset besar, margin performa *Neural Network Perceptron* hanya berkisar 1 - 3 persen lebih baik dibandingkan *Decision Tree*. Oleh karena itu, berdasarkan sifat *ensemble learning* yang menggabungkan algoritma untuk kinerja yang lebih baik, maka penelitian ini menggunakan *ensemble learning*, dan menggabungkan dua algoritma berbasis *Decision Trees* yaitu algoritma *LightGBM*, dan *XGBoost*, kemudian menggunakan model tersebut untuk mendeteksi serangan *video injection* dengan dataset yang berbentuk tabular. Secara teori, algoritma *XGBoost* dan *LightGBM* akan menghasilkan performansi yang baik untuk mendeteksi *video injection* pada dataset yang berbentuk tabular. Selain itu, penggunaan metode *ensemble learning* dalam penggabungan antara kedua algoritma berdasarkan *decision tree* tersebut akan menghasilkan performa yang lebih baik lagi dibanding keduanya secara terpisah.

Topik dan Batasannya

Berdasarkan latar belakang permasalahan yang telah diuraikan, penelitian yang dikerjakan pada tugas akhir ini adalah bagaimana cara untuk membangun sistem pendeteksian *video injection attack* menggunakan *ensemble learning stacking* serta mengukur akurasi dari penerapan sistem deteksi. Metode *ensemble learning stacking* tersebut menggunakan *base estimator* berupa algoritma yang berdasarkan dengan konsep *Decision Tree,* yaitu algoritma XGBoost dan LightGBM.

Batasan masalah dari penelitian tugas akhir ini diantaranya adalah dataset yang digunakan merupakan dataset foto. Dataset ini terdiri dari foto serangan dan foto asli, yang kemudian diperbanyak menggunakan teknik augmentasi data. Dataset didapat dari lab Forestry Universitas Telkom.

Tujuan

Penelitian ini mempunyai beberapa tujuan, diantaranya adalah:

- Melakukan pendeteksian *video injection attack* dengan metode *ensemble learning stacking* yang menggunakan *base classifier* yang berdasarkan *Decision Tree*, yaitu XGBoost dan LightGBM.
- Membandingkan performansi dari metode *ensemble learning stacking* dengan *base classifier* yang berdasarkan *Decision Tree* dengan performansi algoritma dasarnya tersebut.

Organisasi Tulisan

Bagian selanjutnya menjelaskan rincian berikut: Bagian 2 berisi studi yang berkaitan dengan sistem pengenalan wajah serta serangan *video injection*. Bagian 3 berisi rincian arsitektur sistem. Bagian 4 berisi hasil dan pembahasan seputarnya. Dan bagian 5 berisi kesimpulan dan saran untuk penelitian selanjutnya.