Pengembangan Model Image Classification pada Serangan Face Spoofing Menggunakan Metode Ensemble Learning

Muhamad Raihan Ramadhan[1], Dr. Vera Suryani, S.T., M.T.[2]

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

Abstrak

Face spoofing adalah serangan terhadap sistem biometrik dengan menggunakan identitas palsu dari pengguna yang memiliki akses. Serangan ini dapat dilakukan dengan menggunakan foto wajah pengguna yang telah dicetak atau serangan replay dengan menggunakan perangkat lain yang menampilkan wajah pengguna. Metode pencegahan serangan ini dapat dilakukan dengan mendeteksi data yang masuk melalui sistem biometrik. Oleh karena itu, dibutuhkan sebuah sistem yang dapat memprediksi pemalsuan wajah dengan lebih baik. Penelitian ini menggunakan dua metode machine learning: Support Machine Vector (SVM), K-Nearest Neighbors (KNN) dan Bagging dengan SVM dan KNN. Dataset dikumpulkan dari sembilan orang yang berbeda dan terdiri dari lima kategori yang berbeda, yaitu gambar asli, print attack, replay attack, mask attack, dan mask attack dengan lubang pada bagian mata. Setelah melalui tahap preprocessing dan pelatihan model dengan menggunakan dataset tersebut, didapatkan akurasi metode SVM tanpa metode Bagging sebesar 90.52%. Akurasi baru diperoleh setelah menambahkan metode tersebut sebagai estimator dasar ke dalam metode Bagging, untuk SVM-Bagging, yaitu 91.21%. Sedangkan untuk KNN tanpa Bagging sebesar 87.36%. Setelah dilakukan KNN-Bagging mendapati penurunan menjadi 86.90%.

Kata kunci : face spoofing, support vector machine, k-nearest neighbors, bagging

Abstract

Face spoofing is an attack on a biometric system using a fake identity from a user with access. This attack can be carried out using a printed photo of the user's face or a replay attack using another device that displays the user's face. The prevention method for this attack can be done by detecting incoming data via the biometric system. Therefore, a system that can better predict face spoofing is needed. This research use two machine learning methods: Support Machine Vector (SVM), K-Nearest Neighbors (KNN) and Bagging with SVM and KNN. The dataset was collected from nine different people and consisted of five different categories there are actual image, print attack, replay attack, mask attack, and mask attack with a hole in the eye. After going to the preprocessing phase and model training using the dataset, the following accuracy SVM method without the Bagging method was obtained for 90.52%. The new accuracy was obtained after adding that method as a base estimator into the Bagging method, for SVM-Bagging, 91.21%. While for KNN without Bagging it is 87.36%. After doing KNN-Bagging, it decreased to 86.90%.

Keywords: face spoofing, support vector machine, k-nearest neighbors, bagging

1. Pendahuluan

Latar Belakang

Dalam perkembangan teknologi saat ini, sistem otentikasi biometrik telah menjadi sebuah inovasi dalam meningkatkan sistem keamanan. Sebelumnya, sistem otentikasi tradisional yang banyak digunakan seperti PIN, password, dan kartu identitas memiliki kerentanan yang cukup besar. Kerentanan yang biasanya dialami oleh sistem otentikasi tradisional antara lain hilangnya kartu identitas atau praktik brute force pada PIN atau password. Oleh karena itu, sistem otentikasi biometrik dikembangkan untuk menangkap karakteristik unik individu. Penggunaan sistem biometrik memfokuskan proses otentikasi pada sesuatu yang melekat pada pengguna, misalnya sidik jari dan wajah [1]. Meskipun sistem biometrik dianggap aman karena menggunakan karakteristik unik dari seseorang, sistem ini tetap memiliki kerentanan. Kerentanan pada sistem biometrik umumnya terjadi pada sistem pengenalan wajah. Sistem pengenalan wajah rentan terhadap serangan spoof [1].

Serangan face spoofing memiliki dampak yang parah pada sektor keamanan. Keberhasilan pengungkapan sistem biometrik oleh orang yang tidak berwenang dapat mengakibatkan hilangnya data atau penggunaan identitas palsu untuk aktivitas ilegal. Ketidakmampuan sistem biometrik untuk mengidentifikasi wajah pengguna dapat menyebabkan hilangnya kepercayaan pengguna. Menimbulkan keraguan terhadap sistem biometrik dapat menyebabkan kerugian finansial yang berdampak pada proses bisnis. Oleh karena itu, pengembangan model pendeteksian pemalsuan wajah yang tangguh sangat diperlukan untuk menjaga integritas sistem biometrik.