# 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.

Seorang penyerang dapat dengan mudah melakukan metode serangan spoof atau serangan face spoofing dengan mengunduh foto wajah pengguna dan menggunakannya untuk mem-bypass proses otentikasi [1]. Serangan face spoofing menggunakan berbagai macam dimensi mulai dari serangan 2D hingga topeng 3D [2]. Serangan 2D dibagi menjadi beberapa kategori: serangan foto, serangan topeng, dan serangan replay. Pada serangan 2D, penyerang umumnya mendapatkan foto pengguna yang memiliki akses ke media sosial pengguna. Pada serangan 3D, penyerang memodifikasi foto pengguna ke dalam bentuk 3D yang dapat digunakan. Dalam kasus yang jarang terjadi, penyerang menggunakan alat printer 3D berkualitas tinggi untuk melakukan face spoofing [2]. Deteksi face spoofing dibagi menjadi dua teknik, yaitu teknik berbasis perangkat keras dan teknik berbasis fitur [1]. Pada teknik berbasis perangkat keras, akan ditambahkan alat yang dapat membantu proses pendeteksian, seperti alat pengukur suhu atau pendeteksi iris mata. Perangkat lunak dikembangkan untuk mendeteksi pemalsuan wajah dengan menggunakan teknik berbasis fitur. Teknik ini dapat diklasifikasikan menjadi berbasis frekuensi, berbasis tekstur, dan berbasis gerakan [2].

Untuk mengklasifikasikan serangan face spoofing, digunakan dataset foto wajah asli dan foto wajah yang dimodifikasi sesuai dengan kasus nyata yang ada. Untuk mengklasifikasikan serangan spoofing wajah, penelitian ini membuat dan menggunakan dataset foto wajah asli dan foto wajah yang diambil dari sembilan orang berbeda, lalu dimodifikasi sesuai dengan kasus nyata yang ada. Dataset terdiri dari 5400 gambar dari beberapa kategori wajah asli dan serangan spoofing. Penelitian ini bertujuan untuk mengembangkan model pembelajaran mesin yang kuat untuk mendeteksi pemalsuan wajah pada sistem pengenalan wajah dengan menggunakan Ensemble Learning. Ensemble Learning Ensemble learning merupakan sistem klasifikasi gabungan yang bertujuan untuk memperkuat kemampuan prediksi dibandingkan dengan hanya menggunakan satu metode klasifikasi saja [3]. Perbandingan antara dua model machine learning yaitu Support Machine Vector dan SVM-Bagging dilakukan pada penelitian ini untuk mengetahui model yang paling efektif dalam mendeteksi pemalsuan wajah.

**Topik dan Batasannya**

Topik pada penelitian ini adalah bagaimana performansi dari algoritma support vector machine dalam mendeteksi face spoofing dan meningkatkan akurasinya dengan menggunakan metode ensemble learning jenis bagging. Batasan masalah pada penelitian ini adalah dataset wajah dengan lima kategori berbeda yang sudah dibuat. Penelitian ini terbatas menggunakan serangan face spoofing yang tidak mendeteksi wajah secara real-time.

**Tujuan**

Tujuan pada peneliatan ini adalah untuk melakukan deteksi pada serangan face spoofing dan analisis akurasi pada metode Support Machine Vector dan K-Nearest Neighbors dalam mendeteksi serangan face spoofing dari dataset yang sudah dibuat dengan cara menggunakan metode ensemble learning, yaitu metode SVM-Bagging dan KNN-Bagging.

**Organisasi Tulisan**

Setelah bagian pendahuluan ini, akan dilanjutkan ke bagian kedua yaitu studi terkait. Pada bagian studi terkait dibahas literature review yang mendukung penelitian ini. Selanjutnya pada bagian ketiga, akan dijelaskan bagaimana sistem yang dibangun, mulai dari tahapan hingga model deteksi. Pada bagian keempat yaitu evaluasi, akan dibahas hasil dari penelitian ini. Terakhir pada bagian lima, akan dipaparkan kesimpulan dari penelitian yang sudah dilakukan.

## 2. Studi Terkait

### Face Spoofing

Face spoofing adalah aktivitas ilegal dimana penyerang berupaya menyamar sebagai pengguna yang terdaftar untuk mendapatkan akses ke dalam suatu sistem [2]. Penyerangan ini terjadi pada sistem biometrik yang menggunakan fitur face recognition. Face spoofing dapat dibagi menjadi dua kategori penyerangan yaitu 2D dan 3D [2]. Pada penyerangan 2D akan digunakan foto atau gambar dari pengguna yang memiliki akses dengan cara melakukan pencetakan gambar atau menggunakan perangkat lain untuk menampilkan foto atau gambar dari pengguna. Sedangkan, penyerangan 3D menggunakan foto/gambar dari pengguna lalu dibentuk menyerupai wajah asli [2].

Untuk melakukan deteksi pada face spoofing dibagi menjadi dua yaitu, teknik berbasis perangkat keras dan teknik berbasis fitur [1]. Pada teknik berbasis perangkat keras akan ditambahkan alat yang dapat membantu proses pendeteksian misalnya alat pengukur suhu atau detektor iris pada mata. Untuk teknik berbasis fitur akan dikembangkan sebuah software yang dapat mendeteksi face spoofing. Teknik ini dapat diklasifikasikan menjadi tiga yaitu, berbasis frekuensi, tekstur, dan gerakan [1].