IMPLEMENTASI ANTI FACE SPOOFING PADA FACE RECOGNITION MENGGUNAKAN ALGORITMA HAAR CASCADE CLASSIFIER DAN CNN BERBASIS OPENCV

TUGAS AKHIR

Diajukan sebagai syarat menyelesaikan jenjang strata Satu (S-1) di Program Studi Teknik Informatika, Jurusan Teknologi, Produksi dan Industri, Institut Teknologi Sumatera

Oleh :

Akhmad Fahrizal

120140024

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

INSTITUT TEKNOLOGI SUMATERA

LAMPUNG SELATAN

2023

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Serangan face spoofing menjadi salah satu tantangan yang sangat kritis pada sistem face recognition yang dimana pihak yang secara tidak sah mencoba menipu sistem menggunakan media palsu layaknya gambar wajah untuk mengakali pendeteksi wajah. Pada sistem face recognition juga terdapat beberapa yang tidak memadai dan dapat dengan mudah dikelabui oleh gambar wajah. Sehingga, penyerang dapat masuk ke sistem dengan mudah dan mengambil seluruh informasi yang ada pada suatu sistem tanpa perlu otentikasi diri.

Teknologi keamanan sudah sangat berkembang hingga saat ini yang sudah menggunakan sistem pengenalan wajah baik pada smartphone, laptop, dan sebagainya. Diperlukannya pengembangan sistem anti face-spoofing dalam menjaga keamanan pada suatu sistem [1]. Pengenalan wajah ini juga merupakan sistem keamanan biometrik yang dapat digunakan dengan mudah, penggunaan sistem ini juga dipercaya dapat mempercepat proses pengenalan dan otentikasi seseorang tanpa perlu adanya input data diri terlebih dahulu dalam mengakses suatu sistem [2].

Menurut penelitian Sandan Priya (2019) yang membahas perihal face spoofing pada sistem pengenalan wajah menjelaskan bahwa sistem ini memiliki kerentanan terhadap keamanan dengan menggunakan foto palsu yang berisikan wajah pemiliki kunci biometrik tersebut yang memiliki akses pada sistem ini [3]. Dan menurut penelitian Yang Wei (2022) yang membahas tentang Liveness Detection menjelaskan beberapa hal mengenai serangan face spoofing pada umumnya tersebut terjadi seperti menggunakan wajah palsu dalam bentuk gambar maupun video, replay attack yang digunakan pada transmisi kanal data antara akuisisi gambar dan ekstraksi fitur dan juga data yang sudah di inject tersebut digunakan untuk memindahkan data biometrik [4].

Dari pengembangan anti face-spoofing ini dimungkinkan sistem pengenalan wajah dapat membedakan wajah asli maupun yang palsu dalam mengotentikasikan seseorang untuk masuk ke dalam suatu sistem tersebut [5]. Dengan ini, diperlukannya suatu algoritma yang dapat membedakan wajah asli dan palsu dalam mencegah serangan tersebut agar kejahatan seperti ini dapat terhindarkan [6].

Implementasi ini akan mengimplementasikan dua metode yaitu dengan algoritma Haar Cascade Classifier yang dikenal sebagai algoritma dengan performa terbaik dalam pengenalan objek menggunakan yang menggunakan minim sumber daya serta akurasi yang tinggi dalam pengenalan objek secara real time. Algoritma ini juga akan disandingkan dengan Convolutional Neural Network sebagai algoritma penentu yang menggunakan metode deep learning serta Eye Aspect Ratio (EAR) dalam menentukan wajah asli maupun palsu pada pengenalan wajah secara efektif.

Algoritma Haar Cascade Classifier yang digunakan sebagai pendeteksian wajah yang berupa gambar digital ini akan menampilkan fungsi matematika yang berupa kotak serta nilai dari warna RGB dari tiap pixel yang ada dan akan diproses yang menghasilkan beberapa nilai daerah gelap dan terangnya [7]. Pada Haar Cascade Classifier terdapat sebuah fitur yaitu Haar-like feature yang berupa kumpulan fitur khusus yang merepresentasikan citra integral yang merupakan cara tercepat dalam menghitung haar feature [8]. Dengan ini, algoritma yang digunakan dapat menghasilkan performa yang cepat dalam mendeteksi wajah karena hanya bergantung pada jumlah pixel pada suatu kotak yang sudah di crop dan tidak semua pixel pada satu gambar [9]. Sehingga dapat digunakan pada sistem yang memiliki sumber daya yang kecil dan berjalan dengan minimum 15 fps [10].

Algoritma Convolutional Neural Network ini digunakan sebagai memvalidasi wajah asli ataupun palsu melalui citra gambar secara real-time yang menggunakan metode seperti analisis tekstur pada gambar, kualitas gambar, dan citra 3D [11]. Pada Convolutional Neural Network (CNN) bekerja dengan mengambil gambar dan akan dilakukan konvolusi serta subsampling yang diperlukan, lalu memasukkan keluaran yang sudah didapat ke sejumlah lapisan yang sudah terhubung sepenuhnya [12]. Sehingga pada operasi tersebut akan mengalikan kernel konvolusi atau filter dengan input dan ukuran dari kernel tersebut akan lebih kecil dari inputnya, lalu menjumlahkannya untuk mendapatkan nilai tunggal [4].

Oleh karena itu, dari kedua metode yang akan diimplementasikan terdiri dari solusi menggunakan dua algoritma yaitu Haar Cascade Classifier dan CNN. Lalu yang kedua yaitu menggunakan satu algoritma saja yaitu Convolutional Neural Network (CNN). Dapat diharapkan memberikan perlindungan dari sisi keamanan yang lebih baik dalam mendeteksi wajah dan memvalidasi wajah asli atau palsu dalam menghindari resiko serangan yang dapat merugikan sistem serta informasi yang diakses. Dan juga tidak melupakan sisi performa dalam pengenalan wajah pada berbagai kondisi cahaya ruangan

serta peningkatan akurasi dalam pengenalan wajah tersebut walaupun menggunakan sistem yang memiliki sumber daya yang minim.

1.2. Rumusan Masalah

Adapun rumusah masalah pada penelitian ini sebagai berikut :

1. Bagaimana mendeteksi face spoofing pada face recognition tanpa mengurangi performa pendeteksian, tingkat akurasi, serta dapat menggunakan sumber daya yang kecil?

1.3. Tujuan Penelitian

Adapun tujuan penelitian sebagai berikut :

1. Memberikan pencegahan dari serangan face spoofing pada sistem pengenalan wajah dengan algoritma yang efektif dan efisien dalam penggunaan sumber daya serta memiliki tingkat akurasi yang baik.

1.4. Batasan Masalah

Dari uraian yang sudah dijelaskan sebelumnya, terdapat beberapa batasan masalah yang ada yaitu sebagai berikut :

1. Pada pengimplementasian kedua algoritma ini hanya berfokus menggunakan library OpenCV sehingga tidak mencakup ke platform lainnya.
2. Pemodelan Convolutional Neural Network yang dilakukan relatif sederhana dalam menjaga keterbatasan sumber daya dan meminimalisir kompleksitas dalam pengimplementasiannya.
3. Pengujian yang akan dilakukan hanya berfokus pada serangan face spoofing umum seperti foto tanpa mengeksplorasi secara rinci pada jenis serangan spoofing yang lebih rinci.

1.5. Manfaat Penelitian

Adapun manfaat pada penelitian ini yaitu sebagai berikut :

1. Memberikan solusi dalam pencegahan face spoofing pada face recognition menggunakan algoritma Haar Cascade Classifier dan Convolutional Neural Network (CNN).
2. Adanya peningkatan akurasi dalam pendeteksian wajah palsu tanpa terjadinya pengurangan performa.

3. Solusi yang dihasilkan dapat dikembangkan dan diimplementasikan bahkan pada sistem yang memiliki sumber daya kecil.

1.6. Sistematika Penulisan

Sistematika penulisan pada penelitian ini adalah sebagai berikut :

1.6.1. BAB I PENDAHULUAN

Pada bab ini menjelaskan tentang gambaran umum dari penelitian yang akan dilaksanakan yang mencakup dari latar belakang, rumusan masalah, tujuan, Batasan masalah, manfaat penelitian, dan sistematika penelitian.

1.6.2. BAB II TINJAUAN PUSTAKA

Pada bab ini menjelaskan terkait tinjauan pustaka yang berasal dari penelitian sebelumnya yang telah dilakukan dan dasar teori yang mendukung penelitian agar dapat dilaksanakan.

1.6.3. BAB III METODE PENELITIAN

Pada bab ini menjelaskan mengenai alur penelitian, penjabaran Langkah penelitian, alat dan bahan yang akan digunakan, metode tugas akhir, ilustrasi penghitungan metode, dan rancangan pengujian pada penelitian yang akan dilaksanakan.

BAB II
TINJAUAN PUSTAKA

2.1. Tinjauan Pustaka

Penelitian mengenai pencegahan serangan face spoofing pada sistem pengenalan wajah yang sudah banyak digunakan saat ini. Dengan pengelitian ini akan membahas tentang pencegahan serangan face spoofing pada sistem pengenalan wajah menggunakan algoritma Haar Cascade Classifier dan CNN. Berikut tinjauan pustaka sebagai kajian dari penelitian-penelitian sebelumnya yang akan dijabarkan dalam tabel.

Tabel 2.1 Tinjauan Pustaka

No	Nama Penulis dan Tahun Penelitian	Judul Penelitian	Masalah yang Diangkat	Keunggulan atau Keterbatasan	Perbedaan
1	Ali H. Alyousef[1] [2023][13]	Implementing Face Detector using Viola-Jones Method	Implementasi algoritma pendeteksi wajah dengan metode Viola-Jones yang berfokus deteksi wajah dengan Haar-Like features, Adaboost, integral images, dan cascade of classifiers.	Keunggulanny a yaitu metoda Viola-Jones terkenal sebagai algoritma yang efisien dan digunakan secara luas, serta pendeteksian juga memliki nilai akurasi sebesar 60% walaupun metode Viola-Jones asli memiliki nilai 90%.	Terletak pada tingkat akurasi yang 60% dibandingk an Viola-Jones aslinya.

No	Nama Penulis dan Tahun Penelitian	Judul Penelitian	Masalah yang Diangkat	Keunggulan atau Keterbatasan	Perbedaan
2	Yueping Kong[1], Xinyuan Li[2],Guangye Hao[3], Chu Liu[4][2022][5]	Face Anti-Spoofing Method Based on Residual Network with Channel Attention Mechanism	Kerentanan sistem pengenalan wajah seperti serangan face spoofing menggunakan foto ataupun video dari wajah pengguna yang aslinya.	Metode yang diusulkan menggunakan kombinasi residual network yang digunakan untuk mengekstrak perbedaan tekstur antara gambar wajah serta mekanisme channel attention.	Metode pendeteksian anti face spoofing ini menggunakan residual network serta mekanisme channel attention yang merupakan pendekatan yang berbeda dari metode lainnya.
3	Enoch Solomon[1], Krzysztof J. Cios[2] [2023][6]	FASS: Face Anti-Spoofing System Using Image Quality Features and Deep Learning	Penelitian ini menjelaskan masalah utama tentang kerentanan teknologi pengenalan wajah dari serangan face spoofing yang dapat membatasi pengguna.	Metode yang digunakan yaitu random forest dengan fitur kualitas gambar no-references yang diidentifikasi dan menggunakan klasifikasi deep learning.	Dengan menggunakan random forest dan deep learning ini diuji dan dibandingkan dengan sistem anti face spoofing lainnya pada berbagai dataset.

No	Nama Penulis dan Tahun Penelitian	Judul Penelitian	Masalah yang Diangkat	Keunggulan atau Keterbatasan	Perbedaan
4	Muhamad Irsan[1], Satria Ramadhan[2], Silvia Ayunda Murad[3] [2021][14]	Pendeteksian Wajah Menggunaakn Algoritma Convolutional Neural Network Dalam Menghitung Jumlah Mahasiswa	Penelitian ini membahas mengenai perhitungan kehadiran mahasiswa yang saat itu masih dilakukan secara manual yang dapat menyebabkan ketidakakuratan dalam menghitung jumlah kehadiran mahasiswa.	Menggunakan metode Convolutional Neural Network (CNN) sebagai metode deep learning yang digunakan sebagai pendeteksi wajah para mahasiswa serta menghitung jumlah mahasiswa secara akurat. Nilai keakuratan didapatkan sebesar 99% ketika proses training dan nilai akurasi sebesar 98%.	Dalam pendeteksian wajah digunakan model deep learning yaitu CNN yang dapat mendeteksi wajah secara akurat dari jarak 1-6 meter.

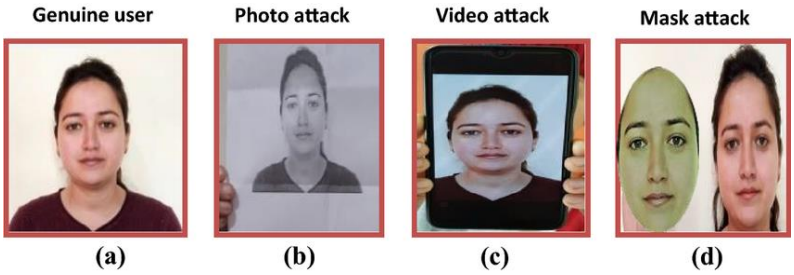
No	Nama Penulis dan Tahun Penelitian	Judul Penelitian	Masalah yang Diangkat	Keunggulan atau Keterbatasan	Perbedaan
5	Prof. Dr. Paul Mccullagh[1] [2023][15]	Face Detection by Using Haar Cascade Classifier	Haar Cascade Classifier adalah algoritma yang populer dalam pendeteksian objek yang pada penelitian ini digunakan sebagai pengenalan wajah. Algoritma ini memiliki beberapa tahap seperti pengumpulan data training, ekstraksi fitur, pelatihan classifier, pembangunan cascade classifier dalam deteksi wajah pada gambar.	Algoritma yang digunakan sudah memiliki tingkat akurasi dan efisiensi yang tinggi dalam gambar hingga video yang dimana algoritma ini juga mudah untuk diimplementasikan dengan performa yang baik pada situasi tertentu. Namun, algoritma ini memiliki keterbatasan dalam pendeteksian wajah pada kondisi pencahayaan yang kurang.	Penelitian ini menggunakan algoritma Haar Cascade Classifier sebagai pendeteksian wajah dikarenakan algoritma ini memiliki tingkat akurasi yang tinggi serta memiliki performa dan efisiensi yang bagus tanpa memakan sumber daya perangkat yang besar sehingga dapat diimplementasikan pada sumber daya yang kecil.

Berdasarkan dari tabel tinjauan pustaka di atas ini yang merupakan penelitian terdahulu terdapat beberapa keterkaitan pada penelitian yang akan dilakukan. Pada penelitian yang dilakukan ini memiliki topik pencegahan serangan anti face spoofing pada sistem pengenalan wajah yang menggunakan algoritma Haar Cascade Classifier sebagai algoritma pengenalan wajah yang memiliki nilai akurasi yang tinggi serta performa yang baik. Serta algoritma Convolutional Neural Network digunakan sebagai algoritma penentuan wajah palsu untuk mencegah anti face spoofing tersebut. Sehingga, dengan menggunakan kedua algoritma ini diharapkan dapat membantu pencegahan serangan face spoofing pada pengenalan wajah yang ada pada suatu aplikasi yang memiliki data sensitif.

2.2. Dasar Teori

Berikut ini merupakan dasar teori dari penelitian tentang Implementasi Anti Face Spoofing :

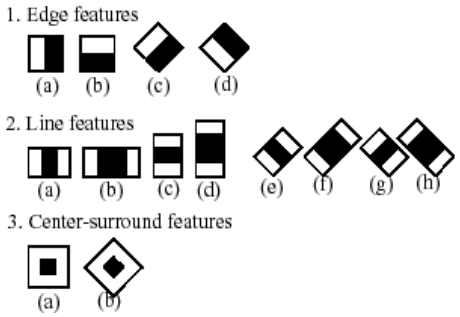
2.2.1. Serangan Face Spoofing



Gambar 2.1 Ilustrasi terhadap serangan face spoofing

Sistem pengenalan wajah sudah ada pada banyak digunakan sebagai sistem keamanan biometrik. Pengenalan wajah ini juga terus berkembang dan sudah mengalami perkembangan yang signifikan, namun terdapat kekurangan seperti rentan terhadap ancaman face spoofing [2]. Dengan adanya keamanan biometrik yang salah satunya menggunakan wajah manusia ini juga tetap ada kerentanan dengan serangan yang ada menggunakan foto ataupun video tanpa adanya wajah asli secara fisik yang dapat mengurangi tingkat keamanan sistem ini[16]

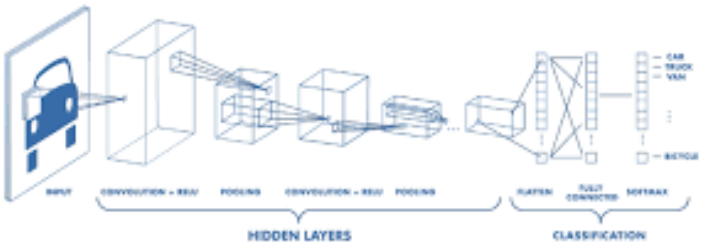
2.2.2. Algoritma Haar Cascade Classifier



Gambar 2.2 Haar-Like Features

Haar Cascade Classifier ini diperkenalkan oleh Paul Viola dan Michael Jones pada tahun 2001 yang menggunakan Haar-Like Features dan metode yang digunakan ini sering disebut sebagai metode Viola-Jones. Metode ini telah diterapkan secara luas pada pendeteksian objek karena dengan keunggulan struktur sederhana serta tingkat deteksi serta kecepatan yang tinggi [17]. Metode Haar-Like Features ini bekerja dengan memproses gambar dalam kotak-kotak yang akan digunakan untuk mendeteksi perbedaan nilai piksel pada tiap kotak dan menentukan daerah gelap serta terang sebagai dasar pengolahan citra. Proses pengolahan Haar-Like features yang digunakan tersebut diorganisir dan diatur dalam cascade classifier untuk meningkatkan hasil yang akurat [18].

2.2.3. Algoritma Convolutional Neural Network (CNN)



Gambar 3.2 Convolutional Neural Network

Convolutional Neural Network (CNN) merupakan algoritma deep learning yang banyak digunakan terutama pada sistem pengenalan objek. Algoritma ini digunakan sebagai salah satu metode untuk mengekstrak fitur wilayah wajah pada suatu gambar. CNN ini juga merupakan jenis arsitektur jaringan saraf tiruan yang sudah memberikan hasil yang terbaik dalam berbagai sistem pengenalan objek [3].

Algoritma ini juga sudah mengalami banyak perkembangan yang sudah diterapkan sebagai sistem pengenalan wajah. CNN bekerja dengan cara

mempelajari bentuk wajah menggunakan dataset yang ada sebagai trainer untuk menghasilkan saraf tiruan dalam memperhitungkan bentuk wajah yang ada. Dengan ini dapat digunakan untuk mendeteksi serta mencegah face spoofing [3].

2.2.4. OpenCV (Open Computer Vision)

Gambar 3.3 OpenCV

Open Computer Vision (OpenCV) merupakan library open-source yang dapat digunakan untuk pengolahan citra gambar. Library ini dapat digunakan sebagai pengenalan objek hingga pengenalan wajah yang menggunakan bahasa python. Fungsi yang menjadikan OpenCV ini banyak digunakan yaitu dapat mendeteksi objek secara real-time menggunakan kamera tanpa memakan sumber daya komputasi yang berlebih [19].

Walaupun OpenCV ini sudah dapat bekerja dengan sumber daya yang kecil, tetapi masih dapat dioptimalkan kembali dengan menerapkan Open Computing Language (OpenCL) Accelerators yang dapat memanfaatkan GPU (Graphical Proccessing Unit) untuk meningkatkan performanya saat mendeteksi suatu objek hingga pengenalan wajah [20].

2.2.5. Citra Gambar Berwarna dan Grayscale

(a) (b)

Gambar 3.4 (a) Gambar berwarna (b) Gambar grayscale

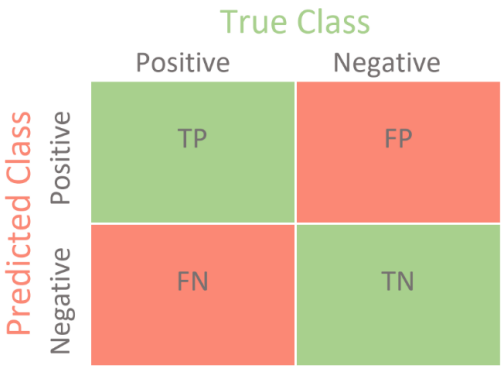
Pada dasarnya, citra gambar merupakan suatu bidang dua dimensi yang secara matematis yaitu fungsi menerus atau continue dari intensitas cahaya pada suatu bidang dua dimensi. Citra gambar ini didapat dengan pantulan cahaya yang menerangi suatu objek dan dipantulkan kembali dari cahaya tersebut. Sehingga

pantulan yang diterima akan ditangkap oleh alat-alat seperti pada manusia, kamera, dan sebagainya [21].

Citra gambar berwarna memiliki kombinasi tiga warna dasar seperti merah, hijau, dan biru yang biasa disebut dengan RGB (Red, Green, Blue). Setiap warna dasar pada suatu citra gambar akan menggunakan penyimpanan sebesar 8 bit atau 1 byte sehingga pada satu piksel warna pada citra gambar menyimpan data warna sekitar 3 byte [21].

Namun pada citra gambar grayscale atau yang biasa disebut dengan gambar monokrom (hitam dan putih) hanya mempunya dua dasar warna yaitu hitam dan putih. Warna hitam memiliki nilai yang rendah dan warna putih memiliki nilai yang sebaliknya yaitu tinggi. Dan tingkat kehalusan warna grayscale ini bergantung pada ukuran memori yang ditampung, apabila memiliki memori yang tinggi maka warna gradasi yang dihasilkan dapat lebih halus [21]. Pada pengenalan wajah juga terdapat metode grayscaling yang bertujuan untuk menentukan area gelap dan terangnya melalui konversi warna dari RGB ke grayscale melalui penghapusan informasi warna pada citra gambar. Hal ini dapat memudahkan dalam pendeteksian objek dengan menentukan area yang gelap dan terang sebagai input dari pendeteksian objek [22].

2.2.6. Confusion Matrix



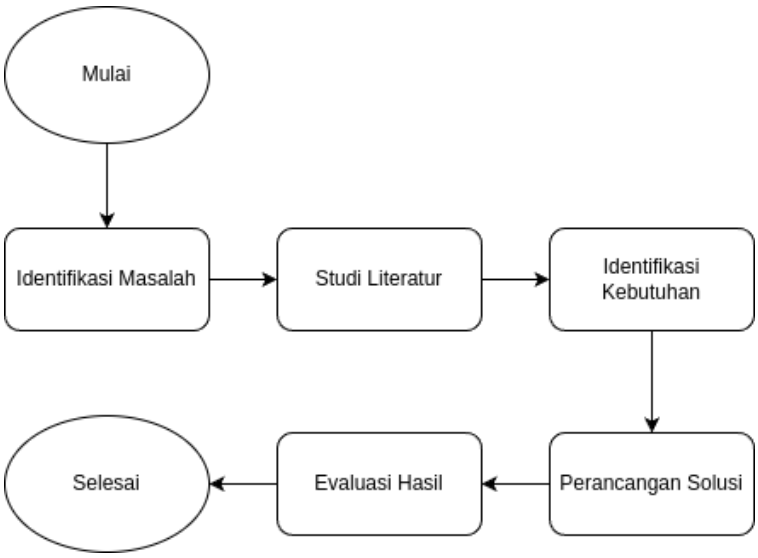
Gambar 3.5 Tabel Confusion Matrix

Confusion matrix merupakan metode yang biasanya digunakan untuk menentukan sebuah set pada data uji penggabungan model data performa dengan nilai kebenaran yang sudah diketahui. Beberapa point sebagai penentu dari confusion matrix yaitu True Positive (TP), False Positive (FP), True Negative (TN), False Negative (FN) [23]. Dengan ini, confusion matrix akan membuat sebuah persegi dengan isi 2 x 2 yang berisikan point penentu tersebut [24].

BAB III
METODE PENELITIAN

3.1. Alur Penelitian

Berikut ini bentuk alur penelitian yang digunakan dalam penelitian yang akan ditampilkan pada gambar 3.1.



Gambar 3.1 Alur Penelitian

3.2. Identifikasi Masalah

Tahapan ini dilakukan untuk mencari masalah yang terjadi pada face recognition terutama dari segi keamanannya. Saat ini terdapat beberapa sistem yang menggunakan face recognition mengalami serangan face spoofing untuk masuk ke dalam sistem tanpa otorisasi. Hal ini tidak merusak sistem yang ada, namun penyerang dapat masuk ke dalam sistem tanpa adanya otorisasi terlebih dahulu.

Dengan ini, diperlukannya sebuah solusi yang dapat memberikan tingkat keamanan yang baik pada face recognition tanpa adanya pengurangan dari sisi performa pada face recognition dalam mendeteksi wajah. Penggunaan algoritma Haar Cascade Classifier dalam mendeteksi wajah ini hanya memerlukan sumber daya yang sedikit sehingga tidak akan mempengaruhi sistem face recognition dalam menentukan wajah asli dan palsu. Namun, diperlukannya algoritma Convolutional Neural Network (CNN) dalam memvalidasi ketika pendeteksian wajah terjadi, sehingga hasil yang dideteksi dapat lebih akurat dalam menentukan wajah asli maupun palsu.

OpenCV (Open Vision Computer) juga digunakan sebagai library face recognition yang memberikan hasil performa terbaik tanpa adanya kendala dari segi performa sehingga dapat digunakan dalam sistem yang kecil.

3.3. Studi Literatur

Studi literatur yang dilakukan untuk mencari teori tentang face recognition serta algoritma yang digunakan baik dari jurnal sebagai acuan pada implementasi solusi ini. Face recognition merupakan sistem pengenalan wajah yang dilakukan sebagai alat otorisasi suatu sistem menggunakan bagian dari tubuh manusia. Bagian tubuh manusia yang digunakan berupa wajah ini merupakan suatu bagian yang dapat digunakan karena wajah dapat dibedakan dari tiap manusia sehingga bagian ini menjadi identifikasi yang unik.

Pada sistem face recognition itu sendiri memiliki kelebihan yang dapat mendeteksi wajah dan membedakannya sesuai dengan bentuk wajah manusia. Namun, terdapat beberapa sistem yang masih dapat mendeteksi wajah dalam berupa foto maupun video tanpa adanya wajah secara fisik[1]. Sehingga, hal ini menjadi kelemahan dari sisi keamanan pada suatu sistem face recognition.

Algoritma Haar Cascade Classifier merupakan algoritma yang sudah lama ada dan sudah banyak digunakan pada sistem face recognition karena dapat digunakan pada sistem dengan sumber daya yang kecil [9]. Untuk menambahkan akurasi serta dapat memvalidasi apakah wajah tersebut asli, maka algoritma tersebut akan disandingkan dengan algoritma Convolutional Neural Network (CNN) dalam mencegah face spoofing. Dan dengan menyandingkan kedua algoritma ini diharapkan dapat meningkatkan akurasi dalam mendeteksi wajah serta menentukan wajah asli ataupun palsu.

3.4. Identifikasi Kebutuhan

Penelitian ini akan membutuhkan alat dan bahan untuk mengimplementasi anti face spoofing menggunakan algoritma Haar Cascade Classifier dan Convolutional Neural Network (CNN). Berikut alat dan bahan yang diperlukan dalam penelitian yaitu sebagai berikut :

3.4.1. Alat

Alat yang diperlukan pada penelitian ini yaitu sebagai berikut :

1. Visual Studio Code, sebagai alat pengimplementasian kode.

2. Library OpenCV, digunakan untuk pemrosesan citra gambar serta pendeteksian wajah.
3. Algoritma Haar Cascade Classifier, algoritma ini digunakan untuk mendeteksi wajah secara akurat yang menggunakan sumber daya kecil.
4. Algoritma Convolutional Neural Network, algoritma ini digunakan untuk validasi wajah asli.

3.4.2. Bahan

Bahan yang digunakan pada penelitian ini yaitu dengan menggunakan dataset Anti-Spoofing Dataset pada laman Kaggle dan pengambilan wajah manusia secara langsung sebagai media training untuk algoritma yang akan digunakan. Dataset Anti-Spoofing yang digunakan sebesar 1.3GB yang diperkirakan sebanyak 51000 set data akan digunakan untuk training dalam menentukan wajah asli ataupun palsu. Data yang diperoleh diklasifikasikan dalam folder dengan penamaan yang berbeda berisikan wajah fisik dan wajah yang ada pada kertas ataupun pada layar.

3.5. Perancangan Solusi

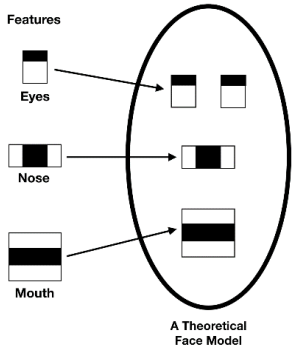
Perancangan anti face spoofing pada face recognition dilakukan dengan langkah pertama yaitu menganalisis terhadap potensi terjadinya serangan face spoofing seperti menggunakan foto palsu. Lalu, pemilihan serta persiapan dataset yang sangat krusial yang harus mencakup variasi wajah asli maupun palsu dalam melatih algoritma yang digunakan. Berikut penjelasan algoritma yang akan digunakan.

3.5.1. Algoritma Haar Cascade Classifier

Algoritma Haar Cascade Classifier digunakan sebagai algoritma yang mendeteksi wajah secara real-time. Algoritma ini juga memanfaatkan library OpenCV (Open Computer Vision) sebagai pengenalan citra gambar. Algoritma yang digunakan juga dapat mendeteksi wajah dari berbagai sudut pandang serta cahaya tanpa mengurangi performa sistem yang digunakan.

Algoritma ini menggunakan metode statistical pada pendeteksian objek. Algoritma ini juga menggunakan metode Haar Like Feature yang dapat didefinisikan pada bentuk seperti koordinat dan ukuran dari feature tersebut. Pada feature ini terbagi menjadi dua bagian, yaitu bagian yang berwarna putih dan hitam. Penggunaan feature ini digunakan karena memiliki pemrosesan yang cepat

dibandingkan dengan pendeteksian objek berdasarkan citra gambar per piksel yang ada. Sehingga, algoritma ini cocok digunakan untuk pendeteksian wajah secara real-time tanpa adanya pengurangan dari performa yang diberikan oleh algoritma ini.



Gambar 3.2 Haar Like Feature dalam mendeteksi wajah

3.5.2. Algoritma Convolutional Neural Network (CNN)

Algoritma Convolutional Neural Network (CNN) yang digunakan sebagai validasi wajah yang telah terdeteksi tersebut asli atau palsu. Penggunaan algoritma ini yang disandingkan dengan algoritma Haar Cascade Classifier dapat meningkatkan akurasi dalam menentukan wajah asli. Model CRMNet yang digunakan pada algoritma CNN ini merupakan suatu model deep-learning pipeline yang dapat mendeteksi wajah asli dan palsu dengan bantuan library Keras, Tensorflow serta OpenCV.

Pada algoritma Convolutional Neural Network (CNN) terdapat beberapa langkah dalam pengenalan objek yang akan dijelaskan sebagai berikut :

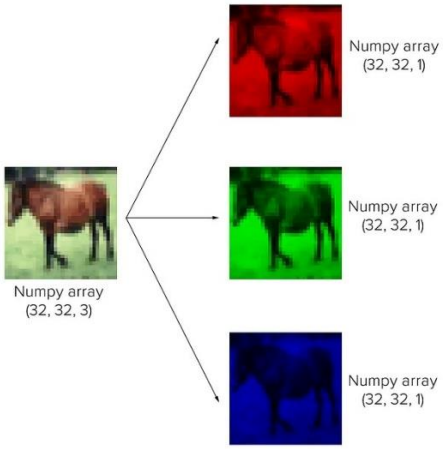
3.5.2.1. Feature Extraction Layer

Langkah ini merupakan proses encoding pada sebuah image yang akan menjadi features berupa angka-angka yang dijadikan sebagai representasi image tersebut atau feature extraction. Feature Extraction Layer ini memiliki dua bagian utama yaitu Convolutional Layer dan Pooling Layer, yang dimana pada penelitian umumnya tidak menggunakan Pooling.

3.5.2.2. Convolutional Layer

Pada Convolutional Layer ini terdiri dari beberapa neuron yang sudah tersusun sesuai panjang dan tinggi dalam bentuk pixel sehingga membentuk sebuah filter. Filter tersebut merupakan hasil dari pemisahan

warna pada suatu gambar menjadi RGB yang awalnya berupa multidimensional array. Proses yang dilakukan juga berupa pergeseran dari filter yang telah dihasilkan dari ketiga warna yang telah dipisahkan. Pergeseran tersebut akan dilakukan operasi "dot" dari input dan nilai dari filter sehingga menghasilkan output yang disebut sebagai activation map atau feature map.



Gambar 3.3 Ilustrasi Convolutional Layer

3.5.2.3. Stride

Stride ini merupakan parameter yang dapat menentukan berapa jumlah pergeseran filter seperti ketika nilai stride adalah 1, maka convolutional filter akan bergeser sebanyak 1 pixel secara horizontal dan vertikal. Dari jumlah pergeseran tersebut apabila nilai stride lebih kecil, maka semakin detail informasi yang telah didapat dari input. Dengan nilai kecil ini terdapat suatu kelemahan yaitu apabila nilai stride kecil maka akan membutuhkan komputasi yang lebih dibandingkan dengan stride besar.

3.5.2.4. Padding atau Zero Padding

Padding atau Zero Padding ini merupakan parameter yang akan menentukan jumlah pixel yang ditambahkan pada tiap sisi dari input yang biasanya berisikan nilai 0. Penggunaan Zero Padding ini ditujukan untuk memanipulasi dimensi output dari convolutional layer. Tujuan utama ditambahkannya Zero Padding ini yaitu untuk meningkatkan performa dari convolutional filter yang akan berfokus pada inti informasi sebenarnya yaitu berada diantara Zero Padding tersebut.

Dalam menghitung dimensi pada feature map, dapat digunakan rumus seperti dibawah ini.

$$output = \frac{W - N + 2P}{S} + 1$$

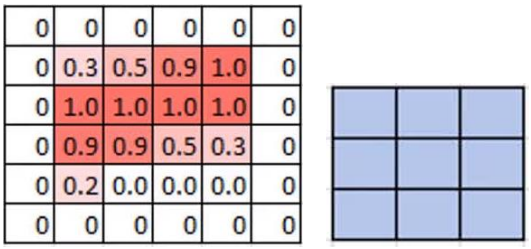
Keterangan :

W = Panjang / Tinggi pada Input

N = Panjang / Tinggi pada Filter

P = Zero Padding

S = Stride



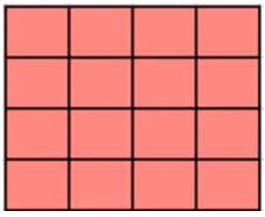
(a) (b)

Gambar 3.4 (a) Input Gambar (b) Filter

Pada gambar 3.4 diberikan input dengan ukuran 4 x 4 dengan padding yang menunjukkan angka 0 (nol) sehingga hanya terdapat 1 (satu) padding saja pada sekitar input gambar serta filter yang diberikan berukuran 3 x 3 sebagai kernel dalam CNN. Dan pergerakan pendeteksian gambar sebanyak 1 piksel sebagai nilai stride. Berikut perhitungan dalam menentukan output zero padding pada algoritma CNN.

$$output = \frac{4 - 3 + 2(1)}{1} + 1 = 4$$

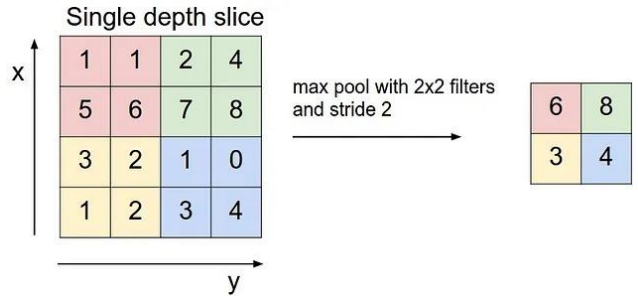
Perhitungan diatas menghasilkan nilai 4 (empat) yang menunjukkan ukuran output dari perhitungan zero padding sebesar 4x4 yang dapat divisualisasikan pada gambar 3.5 berikut.



Gambar 3.5 Output perhitungan Zero Padding

3.5.2.5. Pooling Layer

Pada Pooling Layer memiliki prinsip terdiri dari sebuah filter yang memiliki ukuran dan stride tertentu yang akan bergeser pada seluruh area yang ada pada feature map. Pada umumnya, pooling yang digunakan yaitu Max Pooling dan Average Pooling. Tujuan dari penggunaan Pooling Layer ini untuk mengurangi dimensi dari suatu feature map yang sering disebut sebagai downsampling, yang akan menghasilkan performa komputasi yang cepat karena parameter yang diupdate semakin kecil serta dapat mengatasi overfitting.

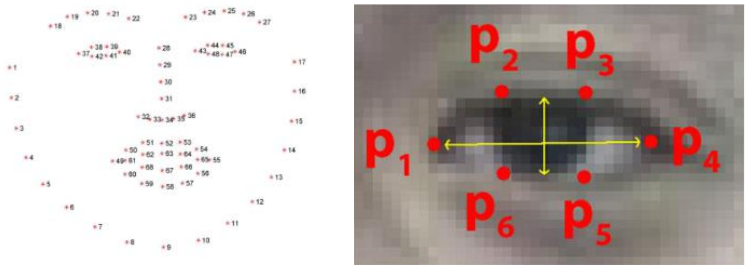


Gambar 3.4 Ilustrasi Pooling Layer

3.5.2.6. Fully-Connected Layer

Fully-Connected Layer merupakan feature map yang telah dihasilkan dari feature extraction layer dalam bentuk multidimensional array sehingga akan dilakukan flatten kembali atau reshape feature map menjadi sebuah vector yang dapat digunakan sebagai input dari fully-connected layer. Fully-Connected Layer ini terdapat beberapa hidden layer, activation function, output layer serta loss function.

Algoritma Convolutional Neural Network (CNN) yang digunakan sebagai validator dari wajah asli atau palsu ini menggunakan metode Eye Aspect Ratio yang berdasarkan dari konsep facial landmarks. Penggunaan metode ini untuk mendeteksi bagian-bagian dari wajah, seperti mata pada metode ini. Fungsi dari metode ini akan menghasilkan titik-titik penting pada sebuah bentuk yang dihasilkan dari prediktor bentuk. Sehingga, fungsi ini akan melakukan proses pendeteksian wajah, dan pendeteksian titik penting pada wajah yang menjadi daerah perhatiannya.



Gambar 3.5 Ilustrasi pendeteksian titik penting pada wajah

Dalam menghitung treshold pada Eye Aspect Ratio dapat digunakan rumus sebagai berikut.

$$EAR = \frac{|p_2 - p_6| + |p_3 - p_5|}{2|p_1 - p_4|}$$

Keterangan :

P = Titik perhatian suatu bentuk.

Berikut ini contoh dari penggunaan persamaan dari EAR (Eye Aspect Ratio) yaitu sebagai berikut.

$$EAR = \frac{|38 - 42| + |39 - 41|}{2|47 - 40|} = 1$$

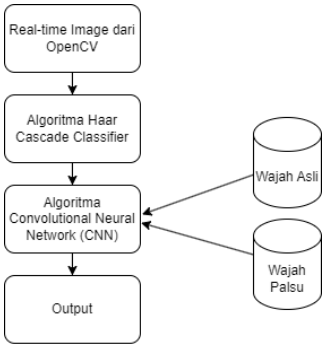
Dari perhitungan diatas menghasilkan angka 1 (satu) yang menandakan kondisi mata saat pendeteksian wajah sedang terbuka. Namun, apabila terdapat kondisi terdeteksi dibawah 1 (satu), maka kondisi mata sedang tertutup.

3.6. Perancangan Solusi

Metode implementasi anti face spoofing pada face recognition ini akan dibagi menjadi dua tahapan yaitu sebagai berikut :

3.6.1. Tahapan 1

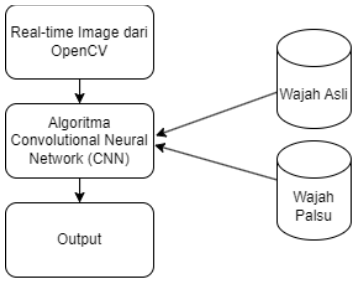
Pada tahapan ini akan dilakukan penerapan algoritma Haar Cascade Classifier sebagai pendeteksian wajah dan library OpenCV sebagai citra gambar secara real-time dan algoritma Convolutional Neural Network (CNN) sebagai algoritma pendeteksi wajah asli ataupun palsu. Dengan menggunakan dataset yang ada, algoritma Haar Cascade Classifier akan menentukan wajah siapa yang sedang terdeteksi dan algoritma Convolutional Neural Network (CNN) akan mendeteksi wajah tersebut palsu atau asli. Dataset yang digunakan sebagai media training algoritma yang akan digunakan.



Gambar 3.4 Alur Kerja Tahapan 1

3.6.2. Tahapan 2

Pada tahapan kedua dilakukan penerapan algoritma Convolutional Neural Network (CNN) serta library OpenCV sebagai tampilan citra gambar secara real-time. Algoritma CNN yang digunakan pada tahapan ini sebagai pendeteksian wajah serta memvalidasi wajah asli ataupun palsu. Dengan penggunaan algoritma ini akan menentukan bagaimana akurasi yang dihasilkan apabila hanya menggunakan satu algoritma saja.



Gambar 3.5 Alur kerja Tahapan 2

3.7. Pengujian

Pengujian yang dilakukan setelah mengimplementasi solusi anti face spoofing yang dilakukan yaitu dengan meguji tingkat akurasi dalam mendeteksi wajah dari berbagai sudut pandang serta kondisi cahaya ruangan. Pengujian yang dilakukan juga dengan menggunakan dataset yang berisikan wajah asli maupun palsu.

Algoritma yang telah diterapkan juga akan dilakukan pengujian baik untuk algoritma Haar Cascade Classifier akan diuji dalam hal pendeteksian wajahnya dan untuk algoritma Convolutional Neural Network (CNN) dilakukan pengujian dalam menentukan wajah asli dan palsu.

Dari kedua tahapan yang telah diterapkan akan diuji dari tingkat ke akuratan serta performa yang diberikan. Pada tahapan satu yang menggunakan algoritma Haar Cascade Classifier dan Convolutional Neural Network (CNN) ini akan diuji akurasi serta

performa serta pada tahapan dua yang hanya menggunakan algoritma Convolutional Neural Network (CNN) akan diuji dengan hal yang sama. Pengujian yang dilakukan akan menggunakan metode Confusion Matrix dalam mengukur tingkat performa serta akurasi dalam pendeteksian wajah.

3.7.1. Confusion Matrix

Confusion Matrix yang digunakan sebagai metode pengujian ini akan mengukur tingkat True Positive, True Negative, False Positive dan False Negative serta akurasi dalam pendeteksian wajah yang akan dilakukan. Berikut tabel confusion matrix yang akan digunakan.

Tabel 3.1 Tabel Confusion Matrix

		Prediksi Algoritma	
		Tidak	Ya
Nilai Aktual	Tidak	True Negative	False Positive
	Ya	False Negative	True Positive

Catatan :

1. Prediksi Algoritma (Tidak : Tidak terdeteksi, Ya : Terdeteksi).
2. Nilai Aktual (Tidak : Tidak ada objek, Ya : Ada Objek).

Sebagai contoh, berikut tabel confusion matrix yang akan digunakan untuk menghitung nilai akurasi, presisi, dan recall.

Tabel 3.1 Tabel Confusion Matrix

		Prediksi Algoritma	
		Tidak	Ya
Nilai Aktual	Tidak	6	2
	Ya	3	9

3.7.2. Akurasi

Perhitungan akurasi diperlukan untuk menentukan suatu rasio yang dihasilkan dari prediksi yang benar. Akurasi juga merupakan nilai yang hampir sama dengan nilai prediksi dengan nilai sebenarnya. Berikut ini rumus dari perhitungan akurasi.

$$Akurasi = \frac{TP + TN}{TP + TN + FP + FN} \times 100\%$$

Berikut ini contoh dari penggunaan rumus akurasi pada confusion matrix yaitu sebagai berikut.

$$Akurasi = \frac{6+9}{6+9+2+3} = \frac{15}{20} = 0{,}75$$

Dari perhitungan diatas menghasilkan nilai akurasi sebesar 0,75 yang jika dikonversikan ke nilai persen menjadi 75%.

3.7.3. Presisi

Presisi merupakan suatu jumlah data yang memiliki kategori positif dan dapat diklasifikasikan secara benar dan dibagi dengan total data yang diklasifikasikan positif. Berikut ini rumus dari perhitungan presisi.

$$Presisi = \frac{TP}{FP+TP} \times 100\%$$

Berikut ini contoh dari penggunaan rumus presisi pada confusion matrix yaitu sebagai berikut.

$$\text{Pr}e\,sisi = \frac{6}{6+2} = \frac{6}{8} = 0{,}75$$

Dari perhitungan diatas menghasilkan nilai presisi sebesar 0,75 yang jika dikonversikan ke nilai persen menjadi 75%.

3.7.4. Recall

Recal merupakan nilai berapa persen data pada suatu kategori positif yang sudah diklasifikasikan dengan benar oleh sistem. Berikut ini rumus dari perhitungan recall.

$$Recall = \frac{TP}{FN+TP} \times 100\%$$

Berikut ini contoh dari penggunaan rumus recall pada confusion matrix yaitu sebagai berikut.

$$Recall = \frac{6}{6+3} = \frac{6}{9} = 0{,}66$$

Dari perhitungan diatas menghasilkan nilai recall sebesar 0,66 yang jika dikonversikan ke nilai persen menjadi 66%.

DAFTAR PUSTAKA

[1] S. Kumar *dkk.*, "Face Spoofing, Age, Gender and Facial Expression Recognition Using Advance Neural Network Architecture-Based Biometric System," *Sensors*, vol. 22, no. 14, Jul 2022, doi: 10.3390/s22145160.

[2] S. Khairnar, S. Gite, K. Kotecha, dan S. D. Thepade, "Face Liveness Detection Using Artificial Intelligence Techniques: A Systematic Literature Review and Future Directions," *Big Data and Cognitive Computing*, vol. 7, no. 1. MDPI, 1 Maret 2023. doi: 10.3390/bdcc7010037.

[3] S. Priya, S. Pawar, dan A. Joshi, "Evaluation of local descriptors and deep CNN features for face anti spoofing," *International Journal of Recent Technology and Engineering*, vol. 8, no. 2 Special Issue 8, hlm. 1644–1648, Agu 2019, doi: 10.35940/ijrte.B1121.0882S819.

[4] Y. Wei, I. K. D. Machica, C. E. Dumdumaya, J. C. T. Arroyo, dan A. J. P. Delima, "Liveness Detection Based on Improved Convolutional Neural Network for Face Recognition Security," *International Journal of Emerging Technology and Advanced Engineering*, vol. 12, no. 8, hlm. 45–53, Agu 2022, doi: 10.46338/ijetae0822_06.

[5] Y. Kong, X. Li, G. Hao, dan C. Liu, "Face Anti-Spoofing Method Based on Residual Network with Channel Attention Mechanism," *Electronics (Switzerland)*, vol. 11, no. 19, Okt 2022, doi: 10.3390/electronics11193056.

[6] E. Solomon dan K. J. Cios, "FASS: Face Anti-Spoofing System Using Image Quality Features and Deep Learning," *Electronics (Switzerland)*, vol. 12, no. 10, Mei 2023, doi: 10.3390/electronics12102199.

[7] D. Mantara Sakti, W. Sudoro Murti, A. Kurniasari, dan J. Rosid, "Face recognition dengan metode Haar Cascade dan Facenet," *Indonesian Journal of Data and Science (IJODAS)*, vol. 3, no. 1, hlm. 30–34, 2022.

[8] K. Diantoro, D. Gustina, S. MERCUSUAR BEKASI Jl Raya Jatiwaringin No, P. Gede, dan J. Barat, "Perancangan Sistem Deteksi Wajah Berbasis Gambar Menggunakan OPENCV," 2019.

[9] N. Muhammad, E. Ariyanto, dan Y. A. S. Yudo, "IMPROVED FACE DETECTION ACCURACY USING HAAR CASCADE CLASSIFIER METHOD AND ESP32-CAM FOR IOT-BASED HOME DOOR SECURITY," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 8, no. 1, hlm. 154–161, Feb 2023, doi: 10.29100/jipi.v8i1.3365.

[10] I. Akil, "FACE DETECTION PADA GAMBAR DENGAN MENGGUNAKAN OPENCV HAAR CASCADE," *INTI Nusa Mandiri*, vol. 17, no. 2, hlm. 48–54, Feb 2023, doi: 10.33480/inti.v17i2.4000.

[11] R. Koshy dan A. Mahmood, "Enhanced deep learning architectures for face liveness detection for static and video sequences," *Entropy*, vol. 22, no. 10, hlm. 1–27, Okt 2020, doi: 10.3390/e22101186.

[12] R. Koshy dan A. Mahmood, "Optimizing deep CNN architectures for face liveness detection," *Entropy*, vol. 21, no. 4, Apr 2019, doi: 10.3390/e21040423.

[13] A. H. Alyousef, "Implementing Face Detector using Viola-Jones Method," *SSRG International Journal of Electrical and Electronics Engineering*, vol. 10, no. 7, hlm. 140–147, Jul 2023, doi: 10.14445/23488379/IJEEE-V10I7P113.

[14] M. Irsan, S. Ramadhan, dan S. A. Murad, "PENDETEKSIAN WAJAH MENGGUNAKAN ALGORITMA CONVOLUTIONAL NEURAL NETWORK DALAM MENGHITUNG JUMLAH MAHASISWA," *Kumpulan jurnaL Ilmu Komputer (KLIK)*, vol. 08, no. 3, 2021.

[15] S. Hashim dan P. Mccullagh, "Face detection by using Haar Cascade Classifier," *Wasit Journal of Computer and Mathematics Science*, vol. 2, no. 1, hlm. 1–8, Mar 2023, doi: 10.31185/wjcm.109.

[16] M. A. Hosen, S. H. Moz, M. M. H. Khalid, S. S. Kabir, dan S. M. Galib, "FACE RECOGNITION-BASED ATTENDANCE SYSTEM WITH ANTI-SPOOFING, SYSTEM ALERT, AND EMAIL AUTOMATION," *Radioelectronic and Computer Systems*, vol. 2023, no. 2(106), hlm. 119–128, 2023, doi: 10.32620/REKS.2023.2.10.

[17] V. Dores, "Identifikasi Masker pada Face Detection dengan Menggunakan Metode Haar Cascade dan CNN," *Jurnal Sistim Informasi dan Teknologi*, Agu 2022, doi: 10.37034/jsisfotek.v4i4.154.

[18] W. Dwiparaswati dan S. V. Hilmawan, "IMPLEMENTASI FACE RECOGNITION SECARA REAL-TIME DENGAN METODE HAAR CASCADE CLASSIFIER MENGGUNAKAN OPENCV-PYTHON."

[19] A. Mishra, K. Bhardwaj, dan V. Sharma, "Smart Attendance System Using OpenCV," *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, vol. 07, no. 01, Jan 2023, doi: 10.55041/ijsrem17489.

[20] J. Song, H. Jeong, dan J. Jeong, "Performance Optimization of Object Tracking Algorithms in OpenCV on GPUs," *Applied Sciences (Switzerland)*, vol. 12, no. 15, Agu 2022, doi: 10.3390/app12157801.

[21] A. S. Budi, H. Maulana, T. Multimedia Digital, F. Sains dan Teknologi, dan J. Teknik Informatika dan Komputer, "Pengenalan Citra Wajah Sebagai Identifier Menggunakan Metode Principal Component Analysis (PCA)," vol. 9, no. 2, 2016.

[22] I. P. Sari, F. Ramadhani, A. Satria, dan D. Apdilah, "Implementasi Pengolahan Citra Digital dalam Pengenalan Wajah menggunakan Algoritma PCA dan Viola Jones," *Hello World Jurnal Ilmu Komputer*, vol. 2, no. 3, hlm. 146–157, Okt 2023, doi: 10.56211/helloworld.v2i3.346.

[23] N. E. Ramli, Z. R. Yahya, dan N. A. Said, "Confusion Matrix as Performance Measure for Corner Detectors," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 29, no. 1, hlm. 256–265, 2022, doi: 10.37934/araset.29.1.256265.

[24] D. Božić, B. Runje, D. Lisjak, dan D. Kolar, “Metrics Related to Confusion Matrix as Tools for Conformity Assessment Decisions,” *Applied Sciences (Switzerland)*, vol. 13, no. 14, Jul 2023, doi: 10.3390/app13148187.