

FACE IDENTIFICATION USING IMAGE PROCESING WITH THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) METHOD

Eunike R. Runtuwene¹, Sondy C. Kumajas^{*2}, Quido C. Kainde³

^{1,2,3}Informatics, Engineering Faculty, Universitas Negeri Manado, Indonesia
Email: ¹17210149@unima.ac.id, ²sondykumajas@unima.ac.id, ³quidokainde@unima.ac.id

(Article received: June 21, 2024; Revision: July 13, 2024; published: August 06, 2024)

Abstract

Cybercrime is a criminal act that utilizes technology, from devices to internet networks. The purpose of cybercrime cases is to harm others by committing theft, hacking, fraud, spreading viruses, and other digital crimes. In every cybercrime case there are usually traces of activity left behind, in the form of traces of activity (history) related can be used as evidence, both in the form of electronic evidence (in the form of electronic physical devices or storage media) and digital evidence (such as document files, history files, or log files containing relevant data). The National Institute of Standards and Technology (NIST) method is a method that is often used in digital forensics to overcome cybercrime cases. The National Institute of Standards and Technology (NIST) method is a method that aims for investigations in finding related information, in order to provide structured information, and process the information obtained. NIST refers to general principles such as collection, examination, analysis, reporting. Using the NIST (National Institute of Standards and Technology) method, the process at each stage is Data Collection is the process of collecting user data and face images through an easy-to-use user interface, Examination is the stage of processing images to detect faces using the Haar Cascade algorithm, Analysis is the process of training a face recognition model (LBPH) and applying it to recognize faces in images or videos. Reporting is the stage of displaying face recognition results and related information to the user through the GUI.

Keywords: *Digital Forensic, Image Processing, NIST Method.*

IDENTIFIKASI WAJAH MENGGUNAKAN IMAGE PROCESSING DENGAN METODE NATIONAL INSTITUTE OF SANDARDS AND TECHNOLOGY (NIST)

Abstrak

Cybercrime adalah tindakan kriminal yang memanfaatkan teknologi, mulai dari perangkat hingga jaringan internet. Adapun tujuan kasus cybercrime adalah merugikan orang lain dengan melakukan pencurian, peretasan, penipuan, penyebaran virus, serta kejahatan digital lainnya. Dalam setiap kasus cybercrime biasanya terdapat jejak aktivitas yang ditinggalkan, berupa jejak aktivitas (history) terkait bisa dijadikan barang bukti, baik berupa barang bukti elektronik (berupa perangkat fisik elektronik atau media penyimpanan) maupun barang bukti digital (seperti file dokumen, file history, atau file log yang mengandung data relevan). Metode National Institute of Standards and Technology (NIST) adalah metode yang sering digunakan dalam digital forensic unruk mengatasi kasus cybercrime. Metode National Institute of Standards and Technology (NIST) merupakan metode yang bertujuan untuk investigasi dalam mencari informasi terkait, agar dapat memberikan informasi terstruktur, serta mengolah sebuah informasi yang didapat. NIST mengacu pada prinsip-prinsip umum seperti collection, examination, analysis, reporting. Dengan menggunakan metode NIST (National Institute of Standards and Technology), maka proses pada setiap tahapan yaitu Pengumpulan Data (Data Collection) adalah proses mengumpulkan data pengguna dan gambar wajah melalui antarmuka pengguna yang mudah digunakan, Pemeriksaan (Examination) adalah tahapan Memproses gambar untuk mendeteksi wajah menggunakan algoritma Haar Cascade, Analysis adalah proses melatih model pengenalan wajah (LBPH) dan menerapkannya untuk mengenali wajah dalam gambar atau video. Reporting adalah tahapan menampilkan hasil pengenalan wajah dan informasi terkait kepada pengguna melalui GUI.

Kata kunci: *Digital forensik, Metode NIST, Pengolahan Citra.*

1. PENDAHULUAN

Perkembangan teknologi merupakan kemajuan bidang ilmu pengetahuan dan rekayasa yang menghasilkan penemuan baru, aplikasi yang lebih baik yang dapat membantu menyelesaikan berbagai permasalahan dalam kehidupan manusia. Namun, dalam perkembangan teknologi, selain sisi positif ternyata diikuti juga dengan berkembangnya sisi negatif dari perkembangan teknologi atau lebih dikenal dengan istilah *Cyber Crime*. *Cyber Crime* merupakan suatu kejahatan yang dilakukan dengan menjadikan komputer atau jaringan komputer sebagai alat, sasaran dan tempat terjadinya kejahatan, termasuk di dalamnya adalah pornografi, penipuan secara online, pembulian, penipuan identitas, dan lain-lain [1]. Kejahatan yang beredar dalam internet, ataupun jaringan, aplikasi dan perangkat digital atau kejahatan dalam dunia maya tidak bisa dianggap remeh karena dampak yang diberikan dalam kehidupan masyarakat. Contoh nyata kejahatan dunia maya (*cybercrime*) yang terjadi salah satunya adalah alat bukti CCTV (*Closed-Circuit Television*) yang dimodifikasi setelah kejadian perkara di lokasi [2].

Dalam suatu kasus kejahatan *cybercrime* akan meninggalkan jejak aktivitas kejahatan. Jejak aktivitas (*history*) yang terkait dapat dijadikan barang bukti, dapat berupa barang bukti elektronik (berupa bentuk fisik dari perangkat elektronik tersebut atau dapat berupa media simpan (*storage device*)) dan barang bukti digital (berupa file dokumen, *file history*, atau *file log* yang berisikan data-data terkait yang dapat di jadikan sebagai informasi pendukung pengambil keputusan) [3]. Bukti elektronik dan bukti digital harus di tangani sesuai dengan prosedur yang tepat dan legal agar bukti yang di hasilkan dari hasil investigasi forensik digital dapat di jadikan bukti yang handal dan legal dalam proses litigasi *cybercrime* [4].

Image Processing merupakan suatu proses yang dilakukan dengan sebuah citra yang di proses oleh komputer sehingga menghasilkan sebuah citra dengan kualitas yang lebih baik dari sebelumnya juga bisa mendapatkan informasi dari citra tersebut. Citra yang dimaksud dalam penelitian ini adalah gambar statis yang berasal dari sensor vision atau webcam [5]. Pengolahan citra (*image processing*) mempunyai keterkaitan yang erat dengan disiplin ilmu yang jika sebuah disiplin ilmu dinyatakan dalam bentuk proses suatu input menjadikan output, maka pengolahan citra memiliki input berupa citra serta output berupa citra [6]. Pengolahan citra digital adalah ilmu yang mempelajari hal-hal berkaitan dengan perbaikan kualitas terhadap suatu gambar (meningkatkan kontras, perubahan warna, restorasi citra), transformasi gambar (translasi, rotasi transformasi, skala, geometrik), melakukan pemilihan citra ciri (*feature images*) yang optimal untuk tujuan analisis, melakukan penyimpanan data yang sebelumnya dilakukan reduksi dan kompresi, transmisi data, dan waktu proses data [7].

Dalam dunia digital yang sudah berkembang sangat pesat banyak terjadinya kejahatan-kejahatan digital yang sering kita temui seperti pencurian data lewat sosial media, penipuan-penipuan, dan lain sebagainya. Maka digital forensik sangat berperan sekali dalam penanganan kasus seperti itu [8]. Tapi digital forensik bukanlah teknik tunggal bayak teknik yang digunakan beroperasi pada digital. Teknik yang diterapkan pada kasus bergantung pada jenis informasi yang berguna untuk memahami apa yang terjadi.

Digital forensik adalah salah satu cabang ilmu yang bertujuan untuk memperoleh informasi dan menyelidiki barang bukti digital agar bisa dipertanggungjawabkan di pengadilan sebagai barang bukti yang sah di mata hukum. Barang bukti digital sendiri berarti hasil dari barang bukti elektronik yang berasal dari personal computer, mobile phone, notebook, server, maupun alat bantu teknologi yang dapat dikategorikan sebagai media penyimpanan dan dan dapat dianalisa sebagai sebuah barang bukti [9].

Teknik identifikasi wajah merupakan hasil dari adanya perkembangan teknologi yang semakin maju. Namun yang menjadi permasalahan, kemampuan komputer yang mengidentifikasi wajah manusia tidaklah mudah. Sehingga, membutuhkan sebuah program untuk mengetahui data/informasi seseorang.[10]. Dengan begitu identifikasi wajah dan pencocokan data/informasi seseorang bisa dengan mudah diproses oleh komputer.

Identifikasi wajah adalah salah satu aplikasi utama dari bidang pengolahan citra dan kecerdasan buatan yang telah menarik perhatian luas karena potensinya dalam berbagai sektor, seperti keamanan, pengawasan, dan interaksi manusia-komputer [11]. Identifikasi wajah yang efektif harus mampu mengenali wajah dengan akurasi tinggi meskipun terdapat variasi dalam sudut wajah, ekspresi, dan kondisi pencahayaan. Untuk mencapai kendalan dan akurasi yang tinggi, diperlukan pendekatan yang terstruktur dan terbukti efektif. [12].

Pendekatan *National Institute of Standards and Technology (NIST)* dalam pengolahan citra menawarkan kerangka kerja yang komprehensif untuk pengembangan sistem identifikasi wajah yang andal [13]. *NIST* menyediakan pedoman dan standar yang bertujuan untuk memastikan keandalan sistem, akurasi pencocokan, validasi, dan referensi yang baik. Dengan mengikuti pedoman ini, sistem identifikasi wajah dapat diuji dan divalidasi dengan cara yang sistematis dan transparan.

Penelitian ini menggunakan bahasa pemrograman *python* dengan library *OpenCV*, menyediakan platform yang kuat dan fleksibel untuk tugas pemrosesan gambar termasuk deteksi wajah. Untuk tugas yang lebih maju dan komputasi intensif, *python* dan *openCV* menyediakan lingkungan yang lebih sesuai [14]. Penelitian ini mengimplementasikan metode identifikasi wajah berdasarkan pendekatan *NIST* dalam pengolahan

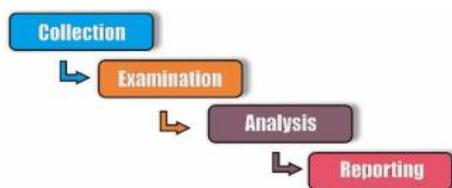
citra. Metode ini mencakup serangkaian tahapan mulai dari akuisisi citra wajah hingga pencocokan data dengan basis data.

Evaluasi sistem dilakukan dengan memperhatikan variasi sudut wajah, ekspresi, dan kondisi pencahayaan yang berbeda. Selain itu, penelitian ini juga mengintegrasikan metode *NIST* dalam analisis digital forensik menggunakan teknik pengolahan citra dengan OpenCV-Python. Metode *NIST* mencakup empat tahapan: *Collecting*, *Examination*, *Analysis*, dan *Reporting*, yang beradaptasi untuk memastikan bahwa setiap langkah dalam proses identifikasi dilakukan secara optimal [15]. Tujuan dari penelitian ini, untuk menganalisa sebuah program yang dibuat untuk mengidentifikasi wajah menggunakan image processing dan mencocokkan data yang telah diidentifikasi untuk sebuah pembuktian metode *NIST*.

2. METODE PENELITIAN

2.1. Metode National Institute of Standards and Technology (NIST)

Pendekatan *National Institute of Standards and Technology (NIST)* dalam pengolahan citra menawarkan kerangka kerja yang komprehensif untuk pengembangan sistem identifikasi wajah yang andal. Dalam konteks pengolahan citra pada penelitian ini menggunakan *OpenCV* seperti dibawah ini, dengan 4 tahapan.



Gambar 1. Metode National Institute of Standards and Technology (NIST)

Pertama, *Collecting* (Pengumpulan Data) merupakan pengumpulan informasi, data atau sampel yang relevan dengan tujuan yang diinginkan. Dalam konteks *NIST*, ini bisa berarti mengumpulkan data empiris atau informasi tentang teknologi baru, fenomena, atau masalah yang sedang dipelajari. Pengumpulan yang tepat dan representatif lah langkah awal penting untuk memastikan bahwa analisis yang akan datang berdasarkan pada informasi yang akurat.

Kedua, tahap *Examination* (Pemeriksaan Data). Setelah data atau informasi dikumpulkan, tahap berikut memeriksa atau menganalisisnya secara lebih mendalam. Ini mungkin melibatkan identifikasi pola, tren, anomaly, atau aspek-aspek lain yang relevan. Di dalam *NIST*, ini bisa berarti pemeriksaan terhadap teknologi, produk, atau proses tertentu untuk memahami karakteristik dan fitur-fitur yang ada. Pengambilan dan penyaringan data pada bagian tertentu dari sumber data. Berfokus pada gambar dan sehingga data yang diambil dari *realtime* (video

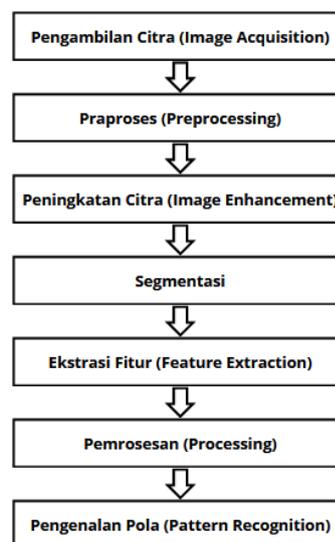
kamera) adalah capture gambar wajah dari seseorang yang memiliki data tersebut.

Ketiga, proses *Analysis Data*. Proses ini melibatkan pemahaman lebih dalam tentang informasi yang dikumpulkan dan diperiksa. Ini bisa mencakup penggunaan metode statistik, perbandingan dengan standar atau norma yang ada, dan penarikan kesimpulan berdasarkan data yang tersedia. Di *NIST*, tahap analisis akan mencakup evaluasi lebih lanjut terhadap teknologi atau fenomena yang dipelajari, dengan tujuan untuk mengidentifikasi masalah atau potensi perbaikan.

Keempat yaitu *Reporting* (pembuatan laporan) di tahap ini kita akan membuat laporan hasil yang ditetapkan dari tahap-tahap sebelumnya. Hasil dari tahap-tahap sebelumnya kemudian dirangkum dan dilaporkan. Ini bisa berupa laporan ilmiah, standar, panduan, atau hasil lainnya yang memiliki nilai bagi komunitas yang tertarik. Pelaporan melibatkan penyajian hasil dari analisis data.

2.2. Image Processing

Image Processing atau Pengolahan Citra adalah cabang ilmu yang berkaitan dengan memanipulasi gambar menggunakan algoritma dan analisis citra untuk mendapatkan informasi baru atau memperbaiki kualitas gambar dengan menggunakan komputer.



Gambar 2. Tahapan Image Processing

Pengambilan Citra (Image Acquisition): Proses ini melibatkan pengambilan gambar. Pengambilan gambar dapat menggunakan kamera digital atau scanner. Cara lain adalah mengimpor gambar yang ada ke komputer.

Praproses (Preprocessing): Citra yang diperoleh mungkin mengandung noise atau artefak lainnya. Dalam langkah ini, citra yang diambil dari kamera akan dikonversi untuk mempermudah proses berikutnya.

Peningkatan Citra (Image Enhancement): Tujuan dari langkah ini untuk meningkatkan kualitas citra dengan meningkatkan kontras, kecerahan, atau

ketajaman gambar. Proses ini melibatkan peningkatan kualitas visual gambar. Kualitas visual gambar dapat dilakukan dengan beberapa cara. Cara terpopuler adalah peningkatan kontras, pengurangan berbagai noise, serta menghilangkan artefak.

Segmentasi: Proses ini adalah membagi gambar menjadi beberapa segmen. Masing-masing segmen sesuai dengan objek atau fitur tertentu dalam gambar.

Ekstraksi Fitur (Feature Extraction): Ekstraksi fitur merupakan bagian dari proses pengurangan dimensi. Pengurangan ini adalah pembagian kumpulan data mentah awal untuk direduksi menjadi kelompok yang lebih mudah dikelola demi kemudahan pengolahan. Karakteristik terpenting dari kumpulan data besar ini adalah bahwa data tersebut memiliki sejumlah besar variabel yang membutuhkan banyak sumber daya komputasi untuk diproses.

Pemrosesan (Processing): Gambar dapat dipulihkan dengan berbagai cara. Biasanya, teknik ini melibatkan penghapusan degradasi dari gambar. Tekniknya adalah pengaburan, noise, dan distorsi. Metode utama restorasi image adalah *inverse filtering* dan *deconvolution*. *Inverse filtering* atau pemfilteran terbalik adalah metode cepat dan sederhana yang menerapkan kebalikan dari fungsi degradasi pada

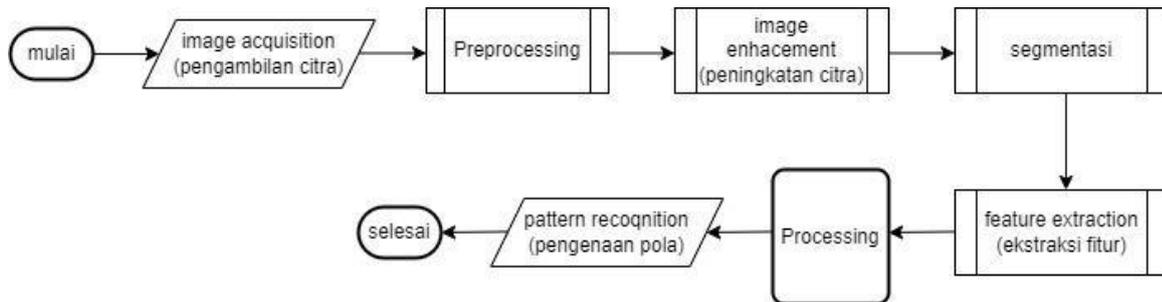
citra yang terdegradasi. Sedangkan *dekonvolusi* merupakan metode yang lebih maju dan tangguh. Metode ini menggunakan algoritma iteratif untuk memperkirakan citra asli dan fungsi degradasi dari citra yang terdegradasi.

Pengenalan Pola (Pattern Recognition): Pengenalan pola merupakan proses yang melibatkan algoritma pembelajaran mesin. Arti lainnya adalah klasifikasi data berdasarkan pengetahuan yang telah diperoleh. Pengenalan pola mengacu pada informasi statistik yang diambil dari pola atau representasinya. Salah satu aspek penting dari pengenalan pola adalah potensi penerapannya.

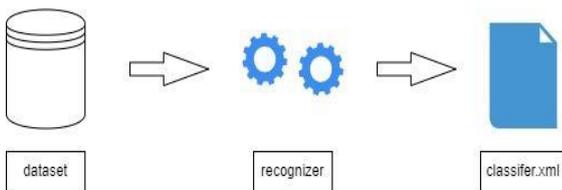
3. HASIL DAN PEMBAHASAN

3.1. Image Processing

Image processing atau pengolahan citra digital adalah cabang ilmu yang berkaitan dengan manipulasi gambar menggunakan algoritma dan analisis citra untuk mendapatkan informasi baru atau memperbaiki kualitas gambar dengan menggunakan komputer. Berikut adalah flowchart dari image processing.



Gambar 3. Flowchart Image Processing



Gambar 4. Ilustrasi Training Classifier

Pengambilan Citra (Image Acquisition):

Langkah pertama adalah mendapatkan citra digital dari kamera dengan menggunakan *OpenCV*.

```
cap = cv2.VideoCapture(0)
ret, frame = cap.read()
```

'cap' digunakan untuk menangkap video dari kamera, dan 'cap.read()' mengambil satu frame dari aliran video.

Praproses (Preprocessing):

Citra yang diperoleh mungkin mengandung noise atau artefak lainnya. Dalam langkah ini, citra yang diambil dari kamera dikonversi menjadi skala abu-abu (*grayscale*) untuk mempermudah proses berikutnya.

```
gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
```

Konversi ke skala abu-abu (*grayscale*) adalah bentuk praproses yang mengurangi kompleksitas komputasi dengan menghilangkan informasi warna.

Peningkatan Citra (Image Enhancement):

Tujuan dari langkah ini untuk meningkatkan kualitas citra dengan meningkatkan kontras, kecerahan, atau ketajaman gambar. Ini dapat dilakukan dengan menerapkan filter atau teknik transformasi.

Segmentasi: Dalam langkah ini, citra dibagi menjadi beberapa bagian yang lebih kecil atau lebih terdefinisi. Tujuannya adalah untuk mengidentifikasi objek atau area tertentu dalam citra.

```
for (x, y, w, h) in faces:
    cropped_face = frame[y:y+h, x:x+w]
```

Haar cascade digunakan untuk mengkoordinat wajah dalam citra, dan koordinat tersebut digunakan untuk memotong bagian wajah.

Ekstraksi Fitur (*Feature Extraction*): Proses ini melibatkan mengidentifikasi fitur-fitur penting dari citra yang akan digunakan untuk pengenalan.

```
clf = cv2.face.LBPHFaceRecognizer_create()
#Training classifier with faces and ids
clf.train(faces, ids)
clf.write("classifier.xml")
```

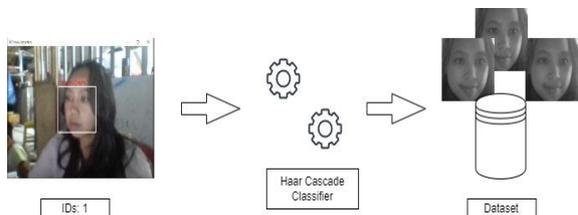
Dalam hal ini, fitur wajah diekstraksi menggunakan Local Binary Patterns Histogram (LBPH).

LBPH digunakan untuk men ekstrakstksi tekstur lokal dari wajah.

Pemrosesan (*Processing*): Disinilah langkah khusus diterapkan pada citra untuk mencapai tujuan tertentu. Langkah pemrosesan melibatkan penyimpanan citra wajah yang terdeteksi dan memproses setiap frame dari video untuk mendeteksi wajah.

```
cv2.imwrite("captured_image.jpg",
cropped_face)
```

Citra wajah yang telah dipotong disimpan ke disk untuk pelatihan lebih lanjut atau untuk digunakan dalam pengenalan wajah.

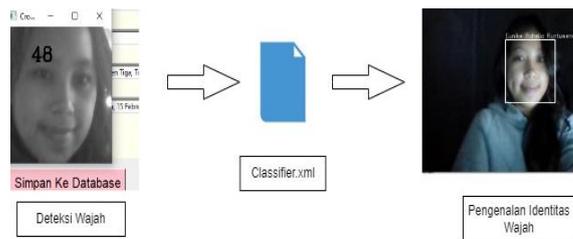


Gambar 5. Ilustrasi Dataset

Pengenalan Pola (*Pattern Recognition*): Dalam langkah ini, fitur-fitur yang diekstraksi digunakan untuk mengidentifikasi atau mengklasifikasi pola tertentu dalam citra. Ini mencakup pengenalan wajah, deteksi objek, atau klasifikasi objek. Dalam hal ini, model LBPH digunakan untuk mendeteksi identitas wajah.

```
id, pred = clf.predict(gray[y:y+h, x:x+w])
confidence = int(100 * (1 - pred / 300))
if confidence > 74:
    # Recognized face
else:
    # Unknown face
```

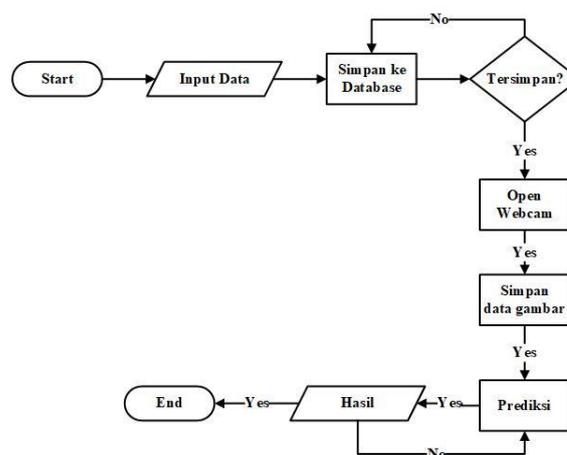
Model LBPH yang telah dilatih digunakan untuk memprediksi identitas wajah berdasarkan citra yang dipotong dan fitur yang diekstraksi.



Gambar 6. Ilustrasi Pengenalan Wajah

Setiap langkah dalam pemrosesan citra memiliki tujuan khusus dan memainkan peran penting dalam keseluruhan sistem pengenalan identitas wajah.

Dalam penelitian ini perancangan sistem yang bisa kita lihat pada gambar flowchart berikut.



Gambar 7. Flowchart Perancangan Sistem

Hasil perancangan sistem berdasarkan flowchart diatas, sebagai berikut:

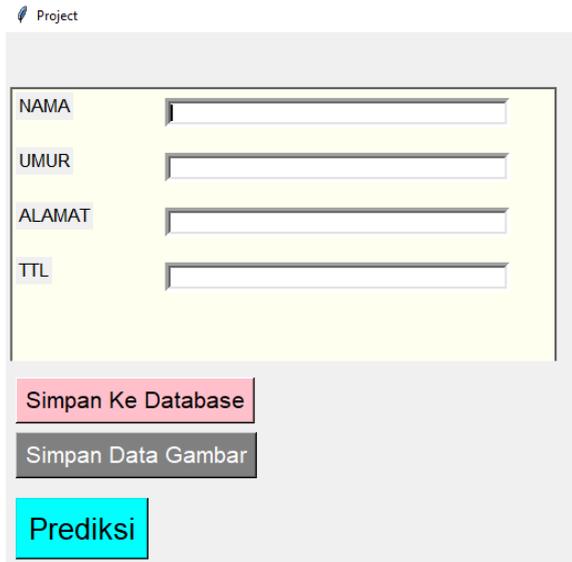
Start: Pengguna membuka file yang berjudul ‘gui_input’

Name	Date modified	Type	Size
data	19/05/2024 1:56	File folder	
3183.jpg	23/08/2017 3:32	JPG File	576 KB
classifier.xml	19/05/2024 2:31	Microsoft Edge H...	71,246 KB
dataset.py	17/05/2024 15:47	Python File	2 KB
detection.py	16/05/2024 19:15	Python File	2 KB
face_p.sql	16/05/2024 15:27	SQL-Script	2 KB
gui_input.py	17/05/2024 16:37	Python File	12 KB
haarcascade_frontalface_default.xml	07/05/2024 4:46	Microsoft Edge H...	909 KB
save.py	07/05/2024 5:22	Python File	1 KB

Gambar 8. gui_input.py

Dengan membuka file “gui_input” pengguna dapat mengakses sistem dan akan lanjut ke langkah selanjutnya.

Input data: Kemudian pengguna memasukkan data yang diperlukan. Data ini berupa informasi pengguna atau parameter lainnya yang diperlukan untuk proses selanjutnya.



Gambar 9. Tampilan antarmuka pengguna (GUI)

Tahap ini untuk membuat sebuah jendela utama sebuah sistem yang didalamnya berelamen GUI seperti tombol, label, dan entri untuk menginput data diri. Dirancang dengan menggunakan library GUI Python Tkinter untuk membangun sebuah interface yang efisien.

Simpan ke database: Data yang di input disimpan dalam database. Ini memastikan data berhasil tersimpan dan dapat diakses.

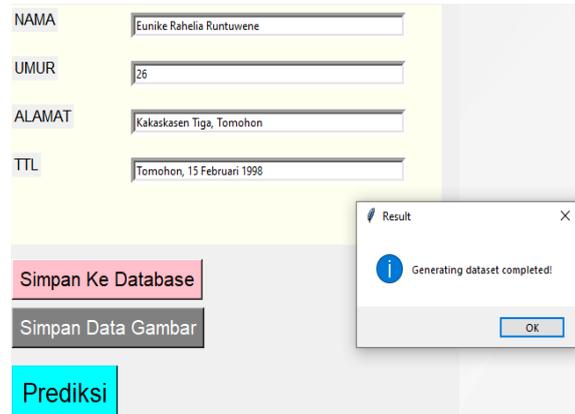
```

classifier.xml
D:\EUN > strips - classifier.xml
1  <?xml version="1.0"?>
2  <opencv_storage>
3  <opencv_lbpfaces>
4  <threshold>1.7976931348623157e+308</threshold>
5  <radius>1</radius>
6  <neighbors>8</neighbors>
7  <grid_x>8</grid_x>
8  <grid_y>8</grid_y>
9  <histograms>
10 <_ type_id="opencv-matrix">
11 <rows>14</rows>
12 <cols>16384</cols>
13 <dt>f</dt>
14 <data>
15 1.7361112e-03 0. 0. 0. 1.7361112e-03 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
16 0. 0. 0. 6.94444450e-03 0. 0. 0. 1.7361112e-03 0. 0. 0. 0. 0. 0. 0. 0.
17 0. 0. 0. 1.5972239e-02 1.7361112e-03 1.38888890e-02
18 1.56250000e-02 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
19 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
20 0. 7.6388881e-02 8.68055597e-03 1.7361112e-03 0. 0. 0. 0. 0. 0. 0. 0.
21 1.7361112e-03 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
22 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
23 0. 0. 0. 0. 0. 0. 8.68055597e-03 0. 0. 0. 1.7361112e-03
24 1.7361112e-03 0. 0. 0. 1.56250000e-02 1.7361112e-03 0. 0.
25 1.07638880e-01 1.7361112e-03 1.38888890e-02 1.04166670e-02 0.
26 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
27 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
28 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
29 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
30 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
31 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
32 0. 3.4722225e-03 8.68055597e-03 0. 4.34027798e-02
33 3.4722225e-03 1.7361112e-03 0. 0. 0. 0. 3.4722225e-03 0.
34 0. 0. 0. 0. 0. 0. 3.4722225e-03 1.7361112e-03 0. 0.
    
```

Gambar 10. file classifier.xml model pengenalan wajah terlatih

Di tahap ini digunakan untuk melatih model pengenalan wajah. Fungsi ini membaca gambar dari direktori, mengkonversikan ke format numpy dan melatih model LBPH (Local Binary Pattern Histogram) yang disediakan oleh OpenCV yang kemudian akan tersimpan sebagai file "classifier.xml". Hasil dari tahap train classifier adalah file 'classifier.xml' yang berisi model pengenalan wajah terlatih.

Apakah sudah tersimpan?: Sistem memeriksa apakah data yang diinput sudah berhasil disimpan ke dalam database, Jika belum tersimpan (no), maka sistem akan kembali mencoba menyimpan data ke database, Jika sudah tersimpan (yes), maka sistem akan melanjutkan kelangkah berikutnya.



Gambar 11. Simpan ke database

Ini adalah langkah validasi untuk memastikan data sudah disimpan.

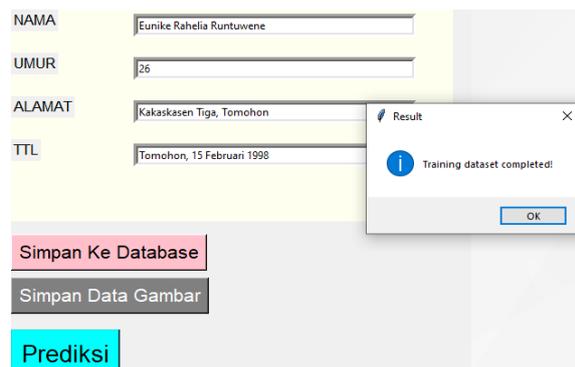
Open webcam: Sistem membuka akses ke webcam. Langkah ini memungkinkan pengguna menangkap gambar dari webcam.



Gambar 12. mengakses kamera dan mendeteksi wajah

Langkah ini membuka akses ke perangkat keras (webcam) untuk menangkap gambar. Penting untuk mendapatkan data visual untuk proses prediksi.

Simpan data gambar: Gambar yang diambil dari webcam disimpan kedalam sistem. Ini bisa berupa penyimpanan lokal atau penyimpanan kedalam database.



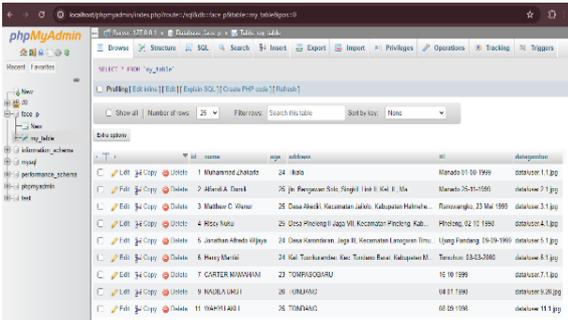
Gambar 13. Berhasil menyimpan data gambar

Gambar diatas adalah proses pengisian data form dan proses menyimpan data gambar berhasil.



Gambar 14. Dataset

Capture gambar wajah disimpan dalam direktori 'data' atau penyimpanan lokal.



Gambar 15. Database

Data diri yang di input akan disimpan dalam table 'my_table' di database 'face_p'.

Prediksi: Sistem melakukan berdasarkan data gambar yang disimpan. Prediksi ini bisa menggunakan model machine learning atau algoritma lainnya yang sudah dilatih sebelumnya.



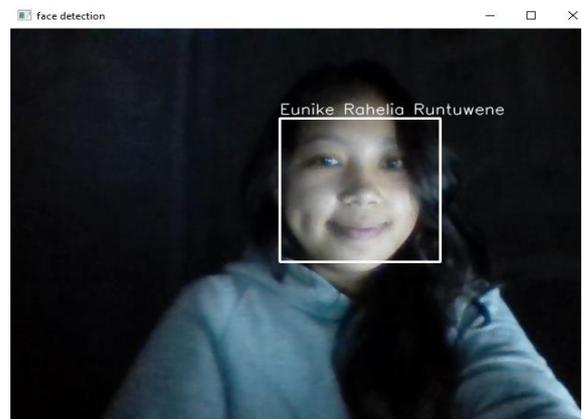
Gambar 16. Graycale

Membaca dan mengkonversi gambar: `Image.open(image).convert ('L')` yang digunakan untuk membuka file besar dan mengkonversinya menjadi abu-abu (grayscale).



Gambar 17. menampilkan gambar pada Tkinter

Apakah prediksi berhasil?: Sistem memeriksa hasil dari prediksi. Hasil ini bisa berubah output prediksi, seperti klarifikasi, deteksi objek, atau lain hasilnya.



Gambar 18. berhasil melakukan deteksi wajah

Deteksi wajah (face detection). Fungsi dari 'detect_face' digunakan untuk mendeteksi dan mengenali wajah secara *real-time*. Fungsi ini mengambil *capture* dari *webcam* setelah itu mendeteksi wajah, dan membandingkan dengan model yang sudah dilatih.

Hasil/Selesai: Semua langkah telah selesai dilakukan dan proses berakhir.



Gambar 19. Hasil

Setelah menghubungkan ke database *MySQL* agar bisa menyimpan data informasi yang telah diinput ke dalam sebuah database, yang pada saat ini menggunakan database *MySQL* sebagai tempat untuk menyimpan data dan menggunakan *PhpMyAdmin* agar memudahkan mengakses database *MySQL*.

3.2. Penerapan Metode *National Institute Of Standards And Technology (NIST)*

Collecting (Pengumpulan Data): Merupakan pengumpulan informasi, data atau sampel yang relevan dengan tujuan yang diinginkan. Dalam konteks *NIST*, ini bisa berarti mengumpulkan data empiris atau informasi tentang teknologi baru, fenomena, atau masalah yang sedang dipelajari. Pengumpulan yang tepat dan representatif lah langkah awal penting untuk memastikan bahwa analisis yang akan datang berdasarkan pada informasi yang akurat. Data primer yang diperoleh langsung dari narasumber Prodi Teknk Informatika Unima. Dengan melakukan wawancara langsung mau pun melalui platform media social whatsapp. Adapun hasil yang didapat adalah Nama, Umur, Alamat, dan Tempat Tanggal Lahir yang di ambil. Data sekunder. Yang tersedia di jejaring internet, adapun data yang diperoleh penulis seperti buku, jurnal, artikel, draft maupun sumber lain tentang image processing, digital forensic, metode national institute of standart dan technology (*NIST*), *python* dan juga *deep learning AI*. Koding mengumpulkan data pengguna melalui GUI (nama, umur, alamat,t1).

```
t1 = tk.Entry(canvas1, width=50, bd=5)
t2 = tk.Entry(canvas1, width=50, bd=5)
t3 = tk.Entry(canvas1, width=50, bd=5)
...
```

Selanjutnya, pengambilan gambar dari webcam menggunakan *Opencv* dan menyimpan ke sistem file.

```
cap = cv2.VideoCapture(0)
...
ret, frame = cap.read()
...
cv2.imwrite(file_name_path, face)
```

Data yang dikumpulkan, termasuk jalur file gambar, di simpan ke dalam database *MySQL*.

```
sql = "INSERT INTO my_table (id, name, age,
address, ttl, datagambar) VALUES (%s, %s, %s,
%s, %s, %s)"
```

Examination (Pemeriksaan Data): Setelah data atau informasi dikumpulkan, tahap berikut memeriksa atau menganalisisnya secara lebih mendalam. Ini mungkin melibatkan identifikasi pola, tren, anomaly, atau aspek-aspek lain yang relevan.

```
face_classifier =
cv2.CascadeClassifier("haarcascade_frontalface_defau
lt.xml")
gray = cv2.cvtColor(frame,
cv2.COLOR_BGR2GRAY)
faces = face_classifier.detectMultiScale(gray, 1.3, 5)
```

```
for (x, y, w, h) in faces:
    cropped_face = frame[y:y+h, x:x+w]
```

Pemeriksaan melibatkan pemrosesan awal dari data yang dikumpulkan untuk memastikan kualitas dan kesesuaian data sebelum dianalisis lebih lanjut. Ini mencakup konversi ke grayscale, deteksi wajah, dan *cropping* wajah dari citra keseluruhan

Analysis: Analisis melibatkan pemahaman lebih dalam tentang informasi yang dikumpulkan dan diperiksa. Ini bisa mencakup penggunaan metode statistik, perbandingan dengan standar atau norma yang ada, dan penarikan kesimpulan berdasarkan data yang tersedia. Di *NIST*, tahap analisis akan mencakup evaluasi lebih lanjut terhadap teknologi atau fenomena yang dipelajari, dengan tujuan untuk mengidentifikasi masalah atau potensi perbaikan.

```
clf = cv2.face.LBPHFaceRecognizer_create()
clf.train(faces, ids)
clf.write("classifier.xml")
```

Pada tahap ini, data yang telah dikumpulkan dan diperiksa dianalisis untuk mengidentifikasi pola atau fitur penting. Ini melibatkan pelatihan model pengenalan wajah menggunakan data wajah yang telah dikumpulkan dan menyimpan model terlatih untuk digunakan nanti. Melibatkan interpretasi data untuk menarik kesimpulan yang berarti.

```
id, pred = clf.predict(gray[y:y+h, x:x+w])
confidence = int(100 * (1 - pred / 300))
```

Melatih pengenalan wajah menggunakan *LBPH (Local Binary Pattern Histogram)*. Model yang telah dilatih digunakan untuk mengenali wajah dalam gambar atau frame video.

Reporting (Pelaporan Data): Hasil dari tahap-tahap sebelumnya kemudian dirangkum dan dilaporkan. Ini bisa berupa laporan ilmiah, standar, panduan, atau hasil lainnya yang memiliki nilai bagi komunitas yang tertarik.

```

a1 = tk.Label(canvas3, text="Nama = ",
font=("Arial", 14))
b1 = tk.Label(canvas3, text=datanama[0][0],
font=("Arial", 14))
...
img = Label(canvas3, image=photo, width=200,
height=200)
img.image = photo
img.place(x=0, y=5)

```

Di *NIST*, laporan ini mungkin mengandung rekomendasi, pedoman, atau temuan yang dapat di gunakan oleh industry atau komunitas yang relevan. Pelaporan melibatkan penyajian hasil dari analisis data. Dalam konteks ini, ini bisa berupa menampilkan hasil deteksi dan pengenalan wajah pada antarmuka pengguna (*GUI*) dan memberikan informasi yang relevan mengenai individu yang dikenali termasuk detail pengguna yang cocok dan gambar wajah yang diambil.

```

messagebox.showinfo('Result', 'Training dataset
completed!!!')
messagebox.showinfo('Result', 'Generating
dataset completed!!!')

```

Kotak Pesan digunakan untuk memberi tahu pengguna tentang penyelesaian tugas seperti pelatihan dataset dan pembuatan dataset.

4. DISKUSI

Dengan menerapkan Metode *NIST* maka akan mempermudah peneliti dalam menemukan barang bukti kejahatan digital. Penelitian ini menghasilkan prosedur forensik dalam melakukan investigasi aplikasi untuk mendapatkan barang bukti yang telah dihapus. Dilakukan dengan cara membaca file database yang sebelumnya telah di backup melalui aplikasi yang terenskripsi yang menyimpan sesi percakapan yang sudah dihapus [1]. Sistem dapat mendeteksi wajah manusia dalam keadaan non-frontal dan dapat mendeteksi adanya beberapa wajah dalam suatu citra. [2]. Hasil dari penelitian, bahwa proses identifikasi objek pada citra digital menggunakan teknik pengelompokan atau clustering melakukan pembagian terhadap pixel-pixel pada citra digital kedalam beberapa kelompok berdasarkan kelompok warna yang terbentuk dari objek tersebut [3].

Penelitian ini menghasilkan barang bukti dari implementasi tahapan-tahapan pada metode *National Institute of Standards and Technology (NIST)*, hasil ini menunjukkan dengan menggunakan metode *NIST* dapat diperoleh barang bukti berupa informasi yang digunakan oleh pelaku untuk melakukan kejahatan. [4]. Penelitian ini memiliki tujuan khusus untuk membuktikan ketajaman tools forensic dalam mengungkap keaslian sebuah bukti digital untuk di

Analisa. Kesimpulan dari penelitian ini bahwa tools yang digunakan dalam proses identifikasi forensic terhadap file video (analisis citra digital) terbukti efektif digunakan [5].

Dari keseluruhan proses dan tahapan penelitian yang sudah dilakukan, didapatkan bahwa program yang di buat dan dikembangkan memiliki keunggulan dibandingkan dengan beberapa penelitian terdahulu. Keunggulan yang ditawarkan adalah untuk mendeteksi wajah seseorang dengan hanya gambar/foto dari beberapa angle (bukan hanya depan, tapi juga kanan dan kiri tampak wajah), dengan menggunakan metode *National Institute of Standards and Technology (NIST)* dapat mengetahui keberhasilan dari program yang dikembangkan, dan mengetahui tools yang digunakan untuk mengidentifikasi dan mencocokkan data terbukti efektif.

5. KESIMPULAN

Penelitian yang menggunakan teknik pengolahan citra dengan kerangka kerja yang sistematis memberikan berbagai manfaat teoritis yang signifikan. Model algoritma yang digunakan adalah *OpenCV* untuk mendeteksi dan mengenali wajah dan dengan menggunakan deteksi wajah Haar cascades dan pengenalan wajah LBPH, model ini dapat dilatih dengan gambar wajah yang diambil dari webcam dan digunakan untuk mengenali wajah secara real-time. Algoritma ini bisa diimplementasikan dalam sistem yang memerlukan autentikasi berbasis wajah atau aplikasi lain yang melibatkan pengenalan wajah. Implementasi program pengenalan wajah menggunakan *OpenCV* dan Tkinter ini menunjukkan bagaimana teknologi dapat digunakan untuk mengumpulkan, memproses, menganalisis, dan melaporkan data wajah dengan cara yang terstruktur dan efisien.

Mengikuti tahapan *NIST (National Institute of Standards and Technology)*, program yaitu: Pengumpulan Data (*Data Collection*) adalah proses mengumpulkan data pengguna dan gambar wajah melalui antarmuka pengguna yang mudah digunakan, Pemeriksaan (*Examination*) adalah tahapan Memproses gambar untuk mendeteksi wajah menggunakan algoritma *Haar Cascade*, Analysis adalah proses melatih model pengenalan wajah (*LBPH*) dan menerapkannya untuk mengenali wajah dalam gambar atau video. *Reporting* adalah tahapan menampilkan hasil pengenalan wajah dan informasi terkait kepada pengguna melalui *GUI*.

UCAPAN TERIMA KASIH

Selesainya penelitian ini tentu saja karena adanya dukungan serta bantuan dari berbagai pihak. Maka, dari itu pada kesempatan ini penulis mengucapkan terimakasih kepada Rektor Universitas Negeri Manado (UNIMA), Dekan Fakultas Teknik UNIMA, Koordinator Prodi Teknik Informatika

UNIMA, Dosen-dosen Prodi Teknik Informatika UNIMA, serta Dosen Pembimbing Akademik dan Pembimbing Skripsi. Terimakasih juga penulis ucapkan kepada orangtua dan teman-teman.

DAFTAR PUSTAKA

- [1] K. A. Mulia Fitriana, "Penerapan Metode National of Standards and Technology (NIST) dalam Analisis Forensik Digital untuk Penanganan Cybercrime," *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, pp. 29-39, 2020.
- [2] D. Mualfah dan R. . A. Ramadhan, "Analisis Forensik Metadata Kamera CCTV Sebagai Alat Bukti Digital," *Digital Zone: Jurnal Teknologi Informasi & Komunikasi*, vol. 11, pp. 257-267, 2020.
- [3] R. U. Imam Riadi, "ANALISIS FORENSIK DIGITAL PADA FROZEN SOLID STATE DRIVE DENGAN METODE NATIONAL INSTITUTE OF JUSTICE (NIJ)," *Elinvo (Electronics, Informatics, and Vocational Education)*, pp. 70-82, 2018.
- [4] M. Riskiyadi, "INVESTIGASI FORENSIK TERHADAP BUKTI DIGITAL DALAM MENGUNGKAP CYBERCRIME," *CyberSecurity dan Forensik Digital*, vol. 3, pp. 12-21, 2020.
- [5] Y. D. Juju Jumadi, "PENGOLAHAN CITRA DIGITAL UNTUK IDENTIFIKASI OBJEK MENGGUNAKAN METODE HIERARCHICAL AGGLOMERATIVE CLUSTERING," *Jurnal Sains dan Teknologi*, pp. 148-156, 2021.
- [6] G. P. Agung Rilo Pambudi, "DETEKSI KEASLIAN UANG KERTAS BERDASARKAN WATERMARK DENGAN PENGOLAHAN CITRA DIGITAL," *JIP (Jurnal Informatika Polinema)*, pp. 69-74, 2020.
- [7] H. S. Nadzir Zair Munantri, "APLIKASI PENGOLAHAN CITRA DIGITAL UNTUK IDENTIFIKASI UMUR POHON," *TELEMATIKA*, pp. 97-104, 2019.
- [8] A. S. Nur Iman, "Analisa Perkembangan Digital Forrensik dalam Penyelidikan Cybercrime di Indoneia (Systematic Review)," *IncomTech: Jurnal Telekomunikasi dan Komputer*, pp. 186-192, 2019.
- [9] B. Raharjo, "SEKILAS MENGENAI FORENSIK DIGITAL," *Jurnal Sositeknologi*, pp. 384-387, 2013.
- [10] H. A. Khairunnisak Nur Isnaini, "ANALISIS FORENSIK UNTUK MENDETEKSI KEASLIAN CITRA DIGITAL MENGGUNAKAN METODE NIST," *JURNAL RESISTOR*, pp. 72-81, 2020.
- [11] R. T. Hasan dan A. B. Sallow, "Face Detection and Recognition Using OpenCV," *JSCDM*, vol. 2, pp. 86-97, 2021.
- [12] A. N. Mushlihudin, "ANALISIS FORENSIK PADA WEB PHISING MENGGUNAKAN METODE NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY," *CYBERNETICS*, pp. 79-92, 2020.
- [13] Y. H. M. Zikri Andrekha, "Deteksi Warna Manggis Menggunakan Pengolahan Citra dengan Opencv Python," *Jurnal Vocational Teknik Elektronika dan Informatika*, pp. 27-33, 2021.
- [14] C. R. Ira Arituddiniyaha, "Deteksi Katarak Pada Mata Menggunakan Image Processing," *Jurnal Elektronik Ilmu Komputer Udayana*, pp. 145-152, 2023.
- [15] G. S. Varsha K. Patil, "Comparative Approach for Face Detection in Python, OpenCV and Hardware," *Journal of Emerging Technologies and Innovative Research (JETIR)*, pp. 675-681, 2023.