

Sistem Keamanan Untuk Otorisasi Pada *Smart Home* Menggunakan Pengenalan Wajah Dengan *Library OpenCV*

Moh. Eki Riyadani¹, Subiyanto²

^{1,2}Jurusan Teknik Elektro, Fakultas Teknik, Universitas Negeri Semarang, Sekaran, Gunungpati, Kota Semarang, 50229, Indonesia

¹eky.riyadani@students.unnes.ac.id, ²subiyanto@mail.unnes.ac.id

Diterima : 20 Februari 2022

Disetujui 27 Maret 2022

Abstract— Seiring kemajuan industri 4.0 seperti Internet of Things (IoT), Big Data, Cloud Computing, dan Artificial Intelligent (AI) telah mendorong para peneliti untuk berinovasi di berbagai bidang, termasuk sistem keamanan. Sistem keamanan menjadi isu penting karena maraknya pencurian di suatu tempat tinggal. Sistem keamanan diperlukan untuk otorisasi rumah untuk mencegah kejahatan pencurian. Sistem keamanan dibangun menggunakan pengenalan wajah. Penelitian ini mengusulkan untuk mengembangkan sistem keamanan menggunakan Raspberry Pi berbasis pengenalan wajah dengan pemrograman Python dan memanfaatkan OpenCV. Pengujian sistem meliputi pengujian fungsi pelatihan, fungsi pengenalan wajah, fungsi pengiriman citra, fungsi pengambilan keputusan, dan pengujian kinerja sistem, kinerja sistem untuk pengenalan wajah dihitung menggunakan rumus confusion matrix yang menghasilkan sensitivitas 100%, spesifisitas 13%, dan 97% ketepatan.

Keyword—Industrial 4.0, Security System, Facial Recognition, Raspberry Pi, OpenCV, Python

I. PENDAHULUAN

Sistem keamanan menjadi salah satu isu penting yang perlu diulas di lingkungan masyarakat umum. Menurut data dari Badan Pusat Statistik (BPS) pada tahun 2011-2018 tindak kriminal pencurian mengalami peningkatan sebesar 8,23% [1]. Tidak dapat dipungkiri bahwa meningkatnya tindak kriminal pencurian dikarenakan lemahnya sistem keamanan pada rumah yang dimiliki oleh masyarakat.

Selaras dengan berkembangnya tren teknologi industri 4.0 seperti Internet of Things (IoT) dan Artificial Intelligent (AI) mendorong para peneliti untuk melakukan berbagai inovasi termasuk dalam membangun sistem keamanan [2]. Secara umum sistem keamanan yang dimiliki masyarakat umum masih berupa sistem keamanan yang konvensional seperti menggunakan anak

kunci, hal ini dapat menjadi risiko karena anak kunci dapat diduplikasi. Adapun penggunaan Radio Frequency Identification (RFID) sebagai sistem keamanannya [3], namun penggunaan RFID dinilai masih mempunyai kelemahan yaitu potensi rusak atau hilangnya kartu RFID.

Biometrik menjadi salah satu opsi untuk membangun sistem keamanan yang kuat, dikarenakan setiap individu mempunyai keunikan karakter tersendiri seperti karakter sidik jari, suara, iris mata, dan karakteristik wajah [4]. Salah satu biometrik yang dianggap kuat untuk membangun sistem keamanan adalah pengenalan wajah atau yang sering disebut dengan face recognition [4].

Telah banyak algoritma untuk membuat sistem pengenalan wajah, diantaranya algoritma Eigenface yang digunakan pada penelitian [5]. Pada penelitian [6] menggunakan algoritma deep

learning untuk membangun sistem pengenalan wajah. Penelitian [7], [8] menerapkan algoritma Convolutional Neural Network (CNN) yang merupakan salah satu turunan dari deep learning untuk membuat sistem pengenalan wajah. Algoritma deep learning dianggap sebagai algoritma yang efektif untuk face recognition [6], [9], [10].

Pemanfaatan face recognition telah banyak digunakan oleh para peneliti, diantaranya penelitian [11] yang memanfaatkan face recognition sebagai sistem keamanan, serta penelitian [12], [13] face recognition digunakan untuk sistem absensi.

Oleh karena itu pada penelitian ini, peneliti ingin mengajukan suatu ide untuk membangun suatu sistem keamanan yang kuat guna meningkatkan keamanan pada rumah menggunakan sistem pengenalan wajah atau face recognition. Sistem keamanan dengan face recognition ini dikembangkan menggunakan perangkat Raspberry Pi 3 model B, di mana perangkat tersebut merupakan salah satu jenis single board computer dan sekaligus microcontroller yang sangat cocok untuk melakukan tugas komputasi dengan baik [14], serta menggunakan bahasa pemrograman Python dan algoritma deep learning yang tersedia pada OpenCV.

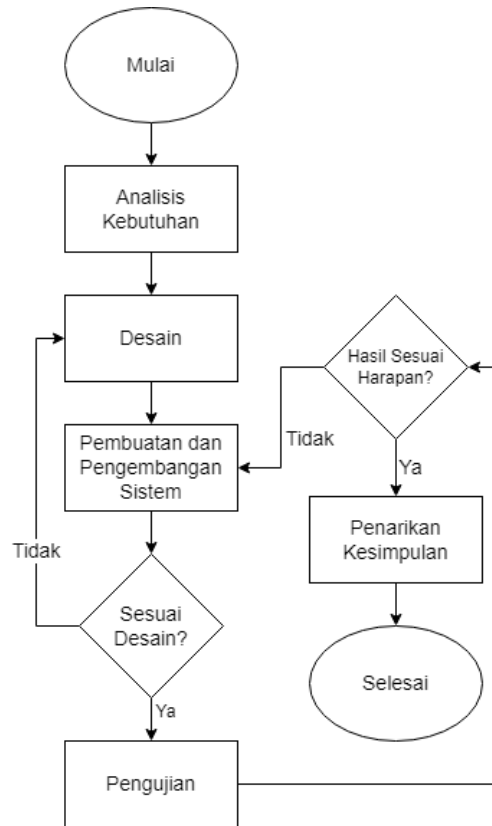
Penelitian ini diharapkan dapat membantu instansi atau masyarakat umum dalam hal meningkatkan keamanan untuk mengurangi tindakan kriminal pada seseorang yang tidak diberi kewenangan mengakses rumah atau gedung. Struktur penulisan pada penelitian ini yaitu abstrak, pendahuluan, metode penelitian, hasil dan pembahasan, serta kesimpulan dan saran.

II. METODE PENELITIAN

A. Desain Penelitian

Secara umum desain penelitian dibagi menjadi studi literatur, analisis permasalahan, perancangan metode pengenalan wajah, implementasi sistem, pengujian, dan simpulan.

Pada Gambar 1. memaparkan desain penelitian yang dilakukan.



Gambar 1. Diagram Alir Desain Penelitian

Pada tahap awal, peneliti melakukan analisis kebutuhan, peneliti melakukan studi literatur dengan mengumpulkan data dari berbagai sumber seperti jurnal penelitian, buku, internet source dan sumber lain yang relevan. Setelah peneliti mendapatkan cukup data dari studi literatur, kemudian peneliti melakukan analisis rancangan dari sistem yang akan dibangun dan analisis kebutuhan alat dan bahan.

Tahap desain dilakukan setelah melakukan analisis kebutuhan. Tahap desain ini merupakan rancangan bagaimana sistem akan berfungsi. Desain sistem meliputi Training Citra Wajah, Deteksi Wajah, Pengenalan Wajah, Fungsi Lock/Unlock Pintu, dan Pengiriman Informasi pada Server.

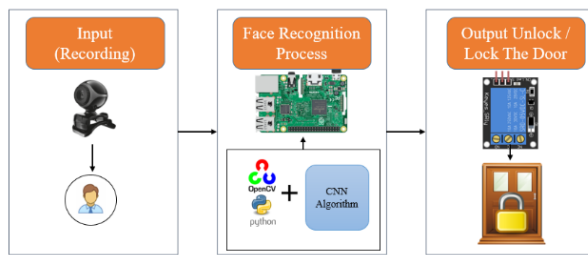
Setelah tahap desain dilakukan, kemudian tahap selanjutnya yaitu pembuatan dan pengembangan sistem yang meliputi persiapan alat dan bahan, perakitan hardware, dan developmen program.

Tahap selanjutnya yaitu pengujian sistem, di mana tahap ini dapat dilakukan ketika sistem yang

telah dibangun sudah sesuai dengan desain yang telah dirancang. Setelah pengujian sistem dilakukan, maka selanjutnya adalah penarikan kesimpulan dari hasil pengujian yang telah dilakukan.

B. Analisis Rancangan Sistem

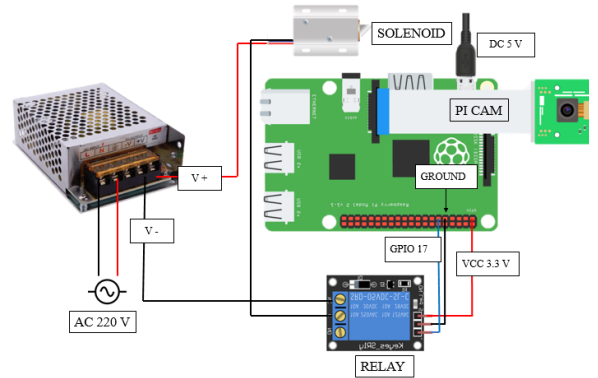
Analisis rancangan desain sistem ini dibagi menjadi tiga bagian, yaitu input, proses, dan output. Gambar 2 merepresentasikan dari rancangan sistem pada penelitian ini.



Gambar 2. Desain Rancangan Sistem

Bagian pertama merupakan input dari sistem di mana pada bagian tersebut terdapat modul kamera yang berfungsi sebagai sensor. Bagian input merupakan proses perekaman citra wajah yang terekam oleh kamera. Bagian kedua merupakan pemrosesan citra wajah yang berhasil terekam kamera untuk dikenali dengan metode yang telah ditentukan. Metode tersebut diprogram pada raspberry pi dengan menggunakan bahasa pemrograman python dengan memanfaatkan library OpenCV. Pada bagian ke tiga merupakan keluaran atau output yang dihasilkan dari pemrosesan gambar wajah pada bagian ke dua. Hasil output tersebut berupa pengambilan keputusan apakah pintu akan terbuka atau tetap terkunci.

Dari analisis rancangan desain sistem, peneliti dapat menentukan desain rancangan hardware untuk membuat sistem keamanan untuk otorisasi pada smart home menggunakan pengenalan wajah. Rancangan desain hardware ditunjukkan pada gambar 3.



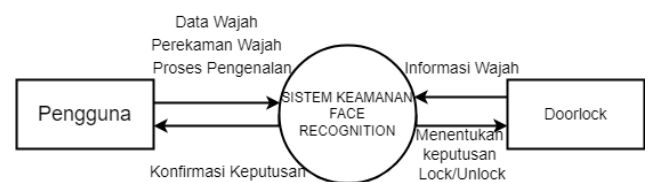
Gambar 3 Diagram Blok Hardware

Kebutuhan alat dan bahan untuk membuat sistem keamanan menggunakan pengenalan wajah dapat dilihat pada tabel 1.

Tabel 1 Kebutuhan Alat dan Bahan

Alat dan Bahan	Fungsi
Raspberry Pi 3 Model B	Sebagai microcontoller
MicroSD card 16 GB	Sebagai Penyimpanan data
Magnetik Solenoid Door Lock	Sebagai aktuator untuk keluaran
Pi Camera	Sensor pada sistem
Relay	Sebagai switch
Power Supply	Sumber daya tegangan

Pada sistem ini meliputi perekaman wajah oleh kamera yang kemudian dilakukan pendeteksian wajah untuk dikenali, setelah itu pengambilan keputusan oleh sistem untuk membuka atau mengunci pintu. Data yang telah didapatkan kemudian dikirim ke server di mana pemilik rumah dapat memantau siapa saja yang telah mengaksesnya. Cara kerja sistem direpresentasikan pada Gambar 4.



Gambar 4. DFD Sistem

Setelah dilakukan analisis perancangan sistem, langkah yang dilakukan selanjutnya adalah perakitan hardware. Pada tahap ini peneliti merealisasikan rancangan desain hardware yang telah diusulkan. Masing-masing komponen dirangkai sesuai dengan desain rancangan sistem yang telah dibuat.

C. Development Program

Pada bagian ini peneliti akan membuat bagaimana sistem pengenalan wajah dibuat dengan membuat program menggunakan bahasa python dan library OpenCV.

1. Instalasi OpenCV

Sebelum dapat menginstal OpenCV pada Raspberry, harus ada prasyarat packages library yang harus diinstal pada raspberry. Berikut merupakan potongan kode untuk menginstal requirement yang dibutuhkan.

Instal requirement yang dibutuhkan untuk menginstal openCV

```
$ sudo apt-get install libhdf5-dev libhdf5-serial-dev libhdf5-103
$ sudo apt-get install libqtgui4 libqtwebkit4 libqt4-test python3-pyqt5
$ sudo apt-get install libatlas-base-dev
$ sudo apt-get install libjasper-dev
```

Instal pip dan python 3

```
$ wget https://bootstrap.pypa.io/get-pip.py
$ sudo python3 get-pip.py
```

Setelah menginstal beberapa requirement yang dibutuhkan, selanjutnya dapat menginstal OpenCV melalui terminal pada Raspberry menggunakan perintah berikut.

```
$ sudo pip install opencv-contrib-python==2.7.0
```

2. Pengkodean Pengenalan Wajah

Pengenalan wajah dibuat menggunakan pengkodean bahasa pemrograman Python. Namun sebelum melakukan pengkodean untuk pengenalan wajah, bagian awal pengkodean perlu dilakukan inisiasi library yang akan dipakai terlebih dahulu. Gambar 4 menunjukkan potongan pengkodean inisiasi library.

```
12 import time
13 import datetime
14 import cv2
15 import os
16 import requests
17 import RPi.GPIO as GPIO
18 import face_recognition
```

Gambar 5 Inisiasi Library

Keterangan

import time untuk menginisiasi waktu

import date time untuk menginisiasi tanggal

import cv2 untuk menginisiasi library OpenCV

import RPI.GPIO untuk menginisiasi pin GPIO

Setelah melakukan inisiasi library, tahap selanjutnya yaitu pengkodean untuk pendeteksian wajah dan pengenalan wajah.

```
51 # load encoding + haarcascade detector
52 print("[INFO] loading encodings + face detector...")
53 data = pickle.loads(open(args["encodings"], "rb").read())
54 detector = cv2.CascadeClassifier(args["cascade"])
55
56 # init kamera + video streaming
57 print("[INFO] mulai video stream...")
58 #vs = VideoStream(src=0).start()
59 vs = VideoStream(usePiCamera=True).start()
60 time.sleep(2.0)
61
62 # start FPS counter
63 fps = FPS().start()
```

Gambar 6 Pengkodean Deteksi Wajah

```
0 # Koordinat box asli dr OpenCV = (x, y, w, h)
1 # Konversi ke (top, right, bottom, left) :
2 boxes = [(y, x + w, y + h, x) for (x, y, w, h) in rects]
3
4 # hitung facial embedding utk setiap wajah dlm box
5 encodings = face_recognition.face_encodings(rgb, boxes)
6 names = []
7
8 # loop setiap facial embeddings
9 for encoding in encodings:
0     # cocokkan dengan known encoding
1     matches = face_recognition.compare_faces(data["encodings"],
2         encoding, tolerance=0.40)
3     name = "Unknown"
4     if True in matches:
5         # initialize dictionary to count the total number of tim
6         # was matched
7         matchedIdxs = [i for (i, b) in enumerate(matches) if b]
8         counts = {}
9
0         # loop over the matched indexes and maintain a count for
1         # each recognized face face
2         for i in matchedIdxs:
3             name = data["names"][i]
4             counts[name] = counts.get(name, 0) + 1
5             name = max(counts, key=counts.get)
6         # update the list of names
7         names.append(name)
```

Gambar 7 Pengkodean Pengenalan Wajah

D. Pengujian Sistem

Setelah melakukan analisis, desain, dan pembuatan sistem, langkah peneliti selanjutnya adalah melakukan pengujian dari setiap elemen sistem seperti pengujian fungsi training, pengujian fungsi pengenalan wajah, pengujian fungsi pengiriman gambar, dan pengujian performa kinerja sistem.

1. Pengujian Fungsi Training

Pengujian fungsi training ini dilakukan untuk menguji apakah sistem yang telah dibuat berjalan sesuai seperti apa yang diharapkan.

Pengujian fungsi ini akan melakukan training citra wajah sebanyak 120 citra. Tabel 2 merepresentasikan pengujian fungsi training.

Tabel 2 Pengujian Fungsi Training.

Pengujian Sistem Pengenalan Wajah			
Nama	Sistem Keamanan Menggunakan Pengenalan Wajah		
Topik	Pengujian Fungsi Training		
No.	Fungsi Pokok	Sesuai	
		Ya	Tidak
1.	Training Dataset	✓	

2. Pengujian Fungsi Pengenalan Wajah

Pada pengujian fungsi pengenalan wajah ini, sistem diharapkan dapat berjalan dengan sebagaimana mestinya, yaitu sistem dapat mendeteksi wajah yang dikenal dan mendeteksi wajah yang tidak dikenal. Tabel 3 merepresentasikan hasil pengujian fungsi pengenalan wajah.

Tabel 3 Pengujian Fungsi Pengenalan Wajah

Pengujian Sistem Pengenalan Wajah			
Nama	Sistem Keamanan Menggunakan Pengenalan Wajah		
Topik	Pengujian Fungsi Pengenalan Wajah		
No.	Fungsi Pokok	Sesuai	
		Ya	Tidak
1.	Mendeteksi Citra Wajah Dikenal	✓	
2.	Mendeteksi Citra Wajah Tidak Dikenal	✓	

3. Pengujian Fungsi Pengunci Pintu

Pengujian fungsi kunci pintu ini dilakukan untuk mengetahui apakah sistem penguncian yang diharapkan dapat bekerja sesuai dengan yang diharapkan atau tidak. Pengujian sistem pengunci ini merupakan pengambilan keputusan dari pengenalan wajah, jika citra wajah dikenali maka sistem pengunci pintu ini akan terbuka, jika tidak maka sistem pengunci

akan tetap terkunci. Tabel 4 menunjukkan hasil dari pengujian fungsi pengunci pintu.

Tabel 4 Pengujian Fungsi Pengunci Pintu

Pengujian Sistem Pengenalan Wajah			
Nama	Sistem Keamanan Menggunakan Pengenalan Wajah		
Topik	Pengujian Fungsi Pengunci Pintu		
No.	Fungsi Pokok	Sesuai	
		Ya	Tidak
1.	Kunci Terbuka Ketika Citra Wajah Dikenali	✓	
2.	Kunci Terbuka Ketika Citra Wajah Tidak Dikenali	✓	

4. Pengujian Fungsi Pengiriman Gambar

Tahap pengujian fungsi pengiriman gambar ini diharapkan sistem dapat mengirim gambar ke server. Tujuannya adalah agar pengguna mengetahui citra wajah yang teridentifikasi dan siapa yang mengakses rumahnya. Tabel 5 menunjukkan hasil pengujian dari fungsi pengiriman gambar.

Tabel 5 Pengujian Fungsi Pengiriman Gambar

Pengujian Sistem Pengenalan Wajah			
Nama	Sistem Keamanan Menggunakan Pengenalan Wajah		
Topik	Pengujian Fungsi Pengiriman Gambar		
No.	Fungsi Pokok	Sesuai	
		Ya	Tidak
1.	Mengirim Citra Ke Server	✓	
2.	Melihat Citra Dikenal	✓	
3.	Melihat Citra Tidak Dikenal	✓	

E. Pengujian Performa

Pengujian performa bertujuan untuk menghitung keakuratan dalam mengidentifikasi citra wajah. Dalam mengevaluasi performa dari algoritma, kita menggunakan acuan Confusion Matrix [15]. Confusion Matrix merepresentasikan prediksi dan kondisi sebenarnya dari data yang dihasilkan oleh algoritma. Berdasarkan Confusion Matrix kita bisa menentukan

Accuracy, Precision, Recall dan Specificity Untuk dapat menentukan hasil dari semua itu akan dicari nilai True Positive, True Negative, False Positive, False Negative dalam pengujiannya [16], [17].

Data yang sudah diperoleh, kemudian dihitung untuk mengetahui citra pelatihan yang digunakan. Selain itu juga data yang diperoleh digunakan untuk mengetahui nilai True positive rate (TPR) atau sensitivity, True Negative Rate (TNR) atau specificity, dan accuracy. Untuk dapat menghitung nilai tersebut dapat direpresentasikan pada persamaan (1) - (3).

$$\text{Sensitivity} = \text{TPR} = \frac{\text{TP}}{\text{TP} + \text{FN}} \quad (1)$$

Keterangan

TPR = Sensitivity : Menggambarkan akurasi data yang diharapkan dengan hasil prediksi

TP : Memprediksi nilai benar dengan kondisi sebenarnya

FN : Mempunyai nilai negatif tetapi diprediksi sebagai nilai positif

$$\text{Specificity} = \text{TNR} = \frac{\text{TN}}{\text{TN} + \text{FP}} \quad (2)$$

Keterangan

TNR = Specificity : Proporsi negatif yang benar diidentifikasi dengan benar .

TN : Prediksi nilai negatif yang benar.

FP : Mempunyai nilai positif tetapi diprediksi sebagai nilai negatif.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{FN} + \text{TN}} \quad (3)$$

Keterangan

Accuracy : Proporsi nilai yang benar baik positif maupun negatif dalam memprediksi.

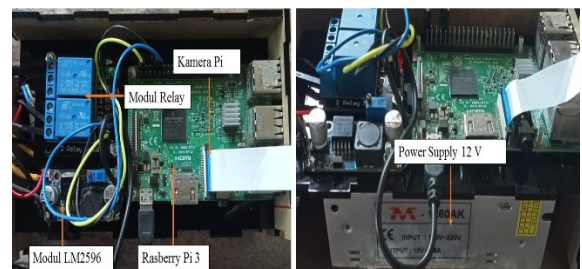
III. HASIL DAN PEMBAHASAN

Pada penelitian ini telah dihasilkan suatu sistem keamanan pada smart home menggunakan pengenalan wajah. Di mana sistem dapat mendeteksi dan mengidentifikasi citra wajah yang

terekam oleh kamera. Kemudian dari hasil identifikasi tersebut, dapat mengambil keputusan untuk melakukan aksi lock/unlock kunci pintu. Citra wajah yang terekam juga dikirimkan ke server.

A. Hasil Pembuatan Hardware

Pada bagian ini, peneliti berhasil membuat hardware dari sistem keamanan pada smart home menggunakan pengenalan wajah. Alat dan bahan yang disiapkan serta rancangan hardware yang dibuat kemudian direalisasikan. Gambar 8 menunjukkan hasil pembuatan hardware yang telah dirancang.



Gambar 8 Hardware Sistem Pengenalan Wajah

B. Hasil Fungsi Training

Dihasilkan pengujian training citra wajah pada dataset yang terdiri dari 120 citra wajah. Pelatihan citra atau training dilakukan untuk memperbaharui pustaka citra wajah yang tersimpan pada dataset serta agar sistem dapat mengenali wajah yang tertangkap kamera. Gambar 9 menunjukkan hasil dari fungsi training.

```

pi@raspberrypi: ~/face_recognition
File Edit Tabs Help
pi@raspberrypi:~$ source ~/.profile
pi@raspberrypi:~$ workon cv
(cv) pi@raspberrypi:~$ cd face1/
bash: cd: face1/: No such file or directory
(cv) pi@raspberrypi:~$ cd /home/pi/face_recognition
(cv) pi@raspberrypi:~/face_recognition $ ./baru.sh
[INFO] quantifying faces...
[INFO] processing image 1/210
[INFO] processing image 2/210
[INFO] processing image 3/210
[INFO] processing image 4/210
[INFO] processing image 5/210
[INFO] processing image 6/210
[INFO] processing image 7/210
[INFO] processing image 8/210
[INFO] processing image 9/210
[INFO] processing image 10/210
[INFO] processing image 11/210
[INFO] processing image 12/210
[INFO] processing image 13/210
[INFO] processing image 14/210
[INFO] processing image 15/210
[INFO] processing image 16/210
[INFO] processing image 17/210
    
```

Gambar 9 Hasil Fungsi Training

Didapatkan juga waktu yang diperlukan untuk proses training citra wajah sebanyak 120 citra. Tabel 4.1 menunjukkan hasil waktu yang dibutuhkan untuk proses training 120 citra.

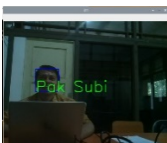
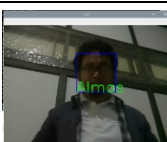
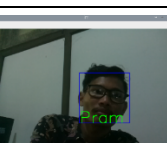
Tabel 6 Pengujian Waktu Training Citra

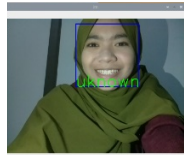
Hasil Pengujian	Waktu Training (Detik)	Jumlah Citra
Training Citra	385,1	120

C. Hasil Fungsi Pengenalan Wajah

Dihasilkan fungsi pengenalan wajah dari sistem keamanan pada smart home ini, fungsi pengenalan wajah berjalan sesuai dengan apa yang diharapkan. Fungsi pengenalan wajah ini berhasil mengidentifikasi citra wajah yang terekam kamera. Tabel 7 menunjukkan hasil fungsi pengenalan wajah.

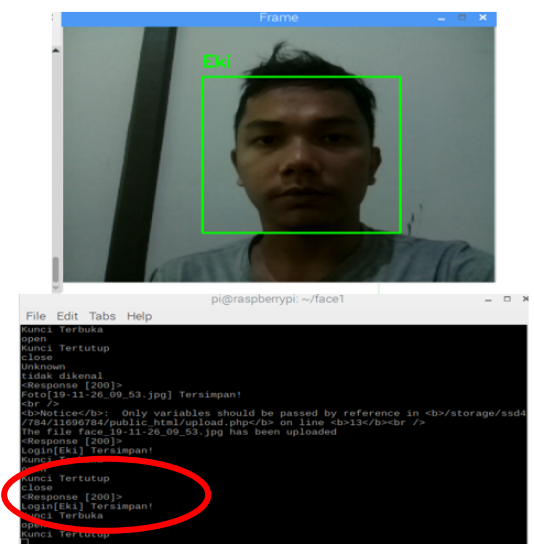
Tabel 7 Hasil Fungsi Pengenalan Wajah

Citra	Nama Citra	Dikenali Sistem	Hasil
	Dina	Dina	Benar
	Eki	Afif	Salah
	Pak Subi	Pak Subi	Benar
	Almas	Almas	Benar
	Pram	Pram	Benar
	Unknown	Unknown	Benar
	Unknown	Unknown	Benar

	Unknown	Unknown	Benar
--	---------	---------	-------

D. Hasil Fungsi Pengunci Pintu

Citra wajah yang teridentifikasi oleh kamera akan diproses oleh sistem untuk pengambilan keputusan apakah kunci akan lock atau unlock. Jika sistem berhasil mengenali citra wajah, maka pengambilan keputusan untuk sistem kunci pintu adalah terbuka/unlock. Sebaliknya, jika sistem tidak dapat mengenali citra wajah, maka sistem kunci pintu akan tetap terkunci / unlock. Gambar 10 menunjukkan fungsi lock / unlock bekerja sebagaimana mestinya.



Gambar 10 Hasil Fungsi Pengunci Pintu

E. Hasil Pengiriman Gambar

Bersamaan dengan pengambilan keputusan oleh sistem bahwa kunci pintu akan terbuka atau tetap terkunci, data informasi kemudian dikirim ke server dan disimpan ke database. Gambar 11 menunjukkan hasil dari fungsi pengiriman gambar ke server. Tercantum informasi sesuai dengan database yang telah dibuat. Nama menunjukkan informasi identifikasi citra, foto menunjukkan file citra yang disimpan, waktu menunjukkan informasi waktu saat citra berhasil terekam, dan status menunjukkan informasi citra dikenali atau tidak dikenali.

id	nama	foto	waktu	status
1	face_22-02-02_21_58.jpg	foto/5ae0de4f35bcb1b6ff62aa50abe6486f	2022-02-02 21:58:47	UNKNOWN
2	face_22-02-08_23_34.jpg	foto/48f3a283d4566feb1aa1bcb082bc9fad	2022-02-08 23:34:38	UNKNOWN
3	Eki		2022-02-09 00:00:42	Eki
4	face_22-02-09_00_04.jpg	foto/412caa26344c613aa69a31a2adcf9a97	2022-02-09 00:04:06	UNKNOWN
5	Eki		2022-02-09 00:23:10	Eki
6	face_22-02-09_09_50.jpg	foto/c091fac230572775926296424002229b	2022-02-09 09:50:11	UNKNOWN

Gambar 11 Hasil Fungsi Pengiriman Gambar

F. Hasil Pengujian Performa

Hasil pengujian performa didapatkan dari percobaan dan pengujian sistem pengenalan wajah. Di mana pada pengujian pengujian sebelumnya dicari nilai True Positive (TP), False Positive (FP), False Negative (FN), dan True Negative (TN).

TP merupakan hasil perekaman sesuai dengan gambar yang di identifikasi (dikenali), TN merupakan nilai negatif yang benar (citra tidak dikenal dan sistem tidak mengenali), FP adalah nilai ketika citra dikenal namun sistem tidak mengenali (error 1), serta FN merupakan citra yang seharusnya tidak dikenal tetapi sistem mengenalinya (error 2). Tabel 8 menunjukkan hasil dari pengujian performa.

Tabel 8 Hasil Pengujian Performa

Nama	Data Pengujian				
	Times	TP	FP	TN	FN
Terdapat Pada Dataset					
Eki	10	10	-	-	-
Dina	10	10	-	-	-
Almas	10	10	-	-	-
Alfi	10	10	-	-	-
Pramudyo	10	7	3	-	-
Tidak Terdapat Pada Dataset					
Sartini	10	-	-	10	-
Maulana	10	-	-	10	-
Arifin	10	-	-	10	-
Sukri	10	-	-	10	-

Yoana	10	-	-	10	-
TOTAL	100	47	3	50	0

Dari hasil yang didapatkan pada tabel 8, didapatkan nilai Accuracy, Specificity, dan nilai Sensitivity yang di tunjukkan pada tabel 9.

Tabel 9 Hasil Pengujian Sensitivity, Specificity, dan Accuracy

Pengujian	Sensitivity (TPR)	Specificity (TNR)	Accuracy
Performa Sistem	100%	13%	97%

IV. SIMPULAN DAN SARAN

Setelah dilakukan penelitian, dapat ditarik kesimpulan dari keseluruhan hasil penelitian ini yang akan dijelaskan pada bab ini, serta dituliskan beberapa saran guna menyempurnakan penelitian yang telah dilakukan.

A. SIMPULAN

Berdasarkan penelitian yang telah dilakukan, pembuatan sistem keamanan untuk otorisasi pada smart home menggunakan Raspberry pi 3 dengan Pi sebagai sensor. pemanfaatan opencv untuk pengenalan wajah dapat diterapkan untuk sistem keamanan pada smart home. Pembuatan sistem menggunakan bahasa pemrograman python dengan algoritma haar cascade untuk pendeteksi wajah. Hasil perekaman citra dikirim ke disimpan ke database yang bertujuan untuk mengetahui siapa saja yang telah mengakses pintu.

Hasil pengujian training 120 gambar wajah pada dataset membutuhkan waktu 385,1 detik. Pada pengujian performa, hasil yang didapatkan untuk sensitivity adalah 100%, specificity 13%, dan accuracy 97%.

Dengan demikian, penelitian ini dapat diimplementasikan untuk sistem keamanan untuk otorisasi pada smart home menggunakan pengenalan wajah.

B. SARAN

Adapun saran untuk penelitian selanjutnya setelah kesimpulan yang telah didapatkan pada penelitian ini, penelitian mengenai sistem

keamanan untuk otorisasi pada smart home menggunakan e pengenalan wajah,

1. Untuk pengembangan sistem face recognition dengan database yang lebih banyak, sebaiknya menggunakan perangkat dengan spesifikasi yang mumpuni, hal ini guna untuk memaksimalkan proses pengolahan data pada sistem serta meminimalkan kendala pada saat pengembangan sistem.
2. Mengembangkan metode pengenalan wajah yang telah ada pada penelitian sebelumnya dengan cara memodifikasi atau mengkolaborasi beberapa algoritma untuk menghasilkan performa yang lebih baik.
3. Untuk sistem keamanan menggunakan face recognition, diharapkan agar sistem dapat mengidentifikasi bahwa yang objek terekam adalah citra wajah, bukan objek lain.

DAFTAR PUSTAKA

- [1] Badan Pusat Statistik, Statistik Kriminal 2018. Jakarta: Badan Pusat Statistik, 2018.
- [2] Y. Lu, "Industry 4.0: A survey on technologies, applications and open research issues," *J. Ind. Inf. Integr.*, vol. 6, pp. 1–10, 2017.
- [3] P. Adole, J. M. Môm, and G. A. Igwe, "RFID Based Security Access Control System with GSM Technology," no. 7, pp. 236–242, 2016.
- [4] E. Pricop, "Biometrics the secret to securing industrial control systems," *Biometric Technol. Today*, vol. 2019, no. 4, pp. 8–10, Apr. 2019.
- [5] F. U. Zhi-peng, "Survey of Deep Learning In Face Recognition," pp. 6–9, 2014.
- [6] I. Masi, Y. Wu, T. Hassner, and P. Natarajan, "Deep Face Recognition: A Survey," *Proc. - 31st Conf. Graph. Patterns Images, SIBGRAPI 2018*, pp. 471–478, 2019.
- [7] H. Zhang, Z. Qu, L. Yuan, and G. Li, "A Face Recognition Method Based on CNN," in *IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, 2017, vol. 1395, no. 1, pp. 544–547.
- [8] Wirtjes and S. Jaceline, "Pengenalan Ekspresi Wajah Menggunakan Convolutional Neural Network (CNN)," *Repos. Institusi USU*, vol. 4, no. 3, pp. 4907–4916, 2019.
- [9] K. Santoso and G. P. Kusuma, "Face Recognition Using Modified OpenFace," *Procedia Comput. Sci.*, vol. 135, pp. 510–517, 2018.
- [10] S. Chen, Y. Liu, X. Gao, and Z. Han, "MobileFaceNets: Efficient CNNs for accurate real-time face verification on mobile devices," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10996 LNCS, pp. 428–438, 2018.
- [11] S. Pandya et al., "Smart Home Anti-Theft System: A Novel Approach for Near Real-Time Monitoring and Smart Home Security for Wellness Protocol," *Appl. Syst. Innov.*, vol. 1, no. 4, 2018.
- [12] I. Jurjawi, "Implementasi Pengenalan Wajah Secara Real Time untuk Sistem Absensi Menggunakan Metode Pembelajaran Deep Learning dengan Pustaka Open CV," Universitas Sumatera Utara, 2020.
- [13] S. Isrofi, J. Hizkia, and S. Ringo, "Sistem Aplikasi Absensi Berbasis Android Menggunakan Otentikasi Wajah Dan Lokasi (Studi Kasus Di CV . Atmosfer IT Consultan)," vol. V, no. September, pp. 11–20, 2021.
- [14] E. Rakhman, RaspberryPi, Mikrokontroler Mungil yang Serba Bisa. Yogyakarta: Andi, 2014.
- [15] D. S. AbdELminaam, A. M. Almansori, M. Taha, and E. Badr, "A deep facial recognition system using computational intelligent algorithms," *PLoS One*, vol. 15, no. 12 December, 2020.
- [16] W. Zhu, N. Zeng, and N. Wang, "Sensitivity, specificity, accuracy, associated confidence interval and ROC analysis with practical SAS® implementations.," *Northeast SAS Users Gr. 2010 Heal. Care Life Sci.*, pp. 1–9, 2010.
- [17] K. J. Bhanushree and M. B. Meenavathi, "Feature Based Face Recognition using Machine Learning Techniques," *Int. J. Recent Technol. Eng.*, vol. 8, no. 6, pp. 1313–1317, 2020.