Vol. 13. No. 02, Mei 2022: 123-129
http://publikasi.mercubuana.ac.id/index.php/jte
p-ISSN: 2086-9479 e-ISSN: 2621-8534

Perancangan Sistem Pengenalan Wajah untuk Keamanan Ruangan Menggunakan Metode *Local Binary Pattern Histogram*

Sunardi[1], Anton Yudhana[1], Muhamad Alwi Talib[2*]

[1]*Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta*
[2]*Magister Informatika, Universitas Ahmad Dahlan, Yogyakarta*
[*]talib2008048037@webmail.uad.ac.id

***Abstrak*— Saat ini telah banyak dikembangkan sistem pengamanan akses masuk ke ruangan dengan verifikasi identitas menggunakan kunci, kartu, dan sebagainya. Namun keterbatasan manusia dalam mengingat benda sehingga kadang terdapat kejadian tertinggal atau terlupa kombinasi angka atau password yang mengakibatkan tidak dapat untuk mengakses ruangan. Teknik verifikasi wajah diperlukan untuk mengakses ruangan dengan teknologi biometrik yang handal dan efisien tanpa harus mengingat objek seperti kunci, kartu, kata sandi, atau pin. Oleh karena itu tujuan penelitian adalah membuat rancang bangun sistem keamanan akses ruangan menggunakan *face recognition* menggunakan metode LBPH berbasis Raspberry Pi. Sistem yang dikembangkan terdiri dari dua bagian, yaitu alat yang dipasang pada Raspberry Pi utama yang menjadi otak kamera dan aplikasi Telegram pada smartphone. Kamera dapat mengenali wajah pengguna dan beberapa orang yang dapat mengakses ruangan. Jika kamera tidak mengenali wajah orang yang terdeteksi maka kamera akan mengambil gambar dan mengirimkannya ke pemilik rumah melalui Telegram sebagai notifikasi untuk tindakan lebih lanjut terhadap kedatangan orang yang tidak dikenal.**

Kata Kunci*— *Haar-cascade, LBPH, Keamanan, Raspberry, Telegram.

DOI: 10.22441/jte.2022.v13i2.010

I. PENDAHULUAN

Sistem pengawasan ruangan menggunakan kamera *Closed Circuit Television* (CCTV) dinilai kurang efektif karena pemilik atau petugas keamanan harus memantau layar untuk mengetahui jika terjadi penyusupan. Disisi lain, telah banyak dikembangkan sistem pengamanan akses masuk ruangan dengan beberapa verifikasi identitas menggunakan kunci, kartu, ataupun pin. Namun keterbatasan manusia dalam mengingat kadang terlupa membawa kunci atau kartu, kadang juga terlupa untuk mengingat kombinasi angka dan huruf pada pin atau password yang menyebabkan tidak dapat mengakses ruangan. Selanjutnya dikembangkan teknik untuk identifikasi atau verifikasi pengguna ruang menggunakan teknologi biometrik sangat handal dan akurat untuk sistem pengamanan pada ruangan [1][2].

II. PENELITIAN TERKAIT

Pendeteksian wajah (*face detection*) dapat dilakukan menggunakan berbagai metode seperti *HOG Face Detector, Deformable Part Model* (DPM), YOLO, dan *Convolutional Neural Network* (CNN). Metode Haar-cascade banyak yang digunakan dalam berbagai penelitian sebelumnya [3][4][5][6][7]. Haar-cascade memanfaatkan *machine learning* untuk mencari fitur-fitur dari citra yang merupakan wajah. Fitur yang disebut dengan haar-feature merupakan kotak-kotak yang terdiri dari warna hitam dan putih yang susunannya mempresentasikan fitur-fitur dari wajah. Citra wajah dikelompokkan berdasarkan sisi yang terang dan sisi yang gelap, contohnya daerah mata cenderung lebih gelap dibandingkan daerah sekitarnya. Haar-cascade banyak digunakan karena komputasi yang cepat tergantung pada jumlah piksel dalam persegi dari suatu citra.

Disisi lain, pengenalan wajah (*face recognition*) dapat dilakukan menggunakan berbagai metode seperti *Principal Component Analysis* (PCA) atau *Eigenface* [8], *Independent Component Analysis* (ICA) [9], *Linear Discriminant Analysis* (LDA) [10], *Support Vector Machines* (SVM) [11], dan *Hidden Markov Models* (HMM) [12]. Metode *Local Binary Pattern Histogram* (LBPH) juga digunakan untuk pengenalan wajah seperti yang dilakukan penelitian sebelumnya [5][13]. Konsep atau cara kerja LBPH adalah nilai intensitas untuk setiap piksel pada interval 0-255 diubah kedalam bentuk biner dengan membandingkannya dengan nilai tengah. Jika nilai lebih besar atau sama dengan nilai tengah maka akan bernilai biner 1, sebaliknya jika lebih kecil dari nilai tengah akan bernilai biner 0. Pada LBPH dilakukan pengolahan citra yang diawali dengan proses *preprocessing* salah satunya dengan mengubah citra asli yang berwarna *Red Green Blue* (RGB) menjadi citra abu-abu (*grayscale*) [14][2]. *Cropping* juga termasuk salah satu pengolahan citra, seperti yang dilakukan oleh Saifullah dkk tahun 2016 [14].

Raspberry Pi banyak digunakan seperti yang dilakukan oleh penelitian-penelitian sebelumnya [15][16][17][18][19] [3][4][5][6][7] [13]. Raspberry Pi adalah komputer seukuran kartu kredit yang mana komponen dari Raspberry Pi hampir serupa dengan komputer pada umumnya, seperti CPU, GPU, RAM, Port USB, Audio Jack, HDMI, Ethernet, dan GPIO.

Penelitian ini membuat rancang bangun keamanan akses ruangan menggunakan *face recognition* berbasis Raspberry Pi menggunakan metode Haar-Cascade dan LBPH. Objek penelitian adalah pintu suatu ruangan. Tujuan penelitian ini adalah membangun sistem disertai dengan pengukuran dan analisis akurasi, kecepatan pengenalan wajah, kecepatan sistem

dalam membuka kunci, dan kecepatan sistem dalam mengirim pemberitahuan berupa pesan melalui Telegram kepada pemilik sebagai notifikasi dan tindak lanjut terhadap kehadiran orang yang tidak dikenal.

III. METODOLOGI PENELITIAN

Langkah awal yang dilakukan dalam penelitian ini adalah akuisisi citra. Akuisisi citra merupakan tahap awal untuk mendapatkan citra digital. Tujuan akuisisi citra untuk menentukan data yang diperlukan dan memilih metode perekaman citra digital [20]. Proses akuisisi citra dapat dilakukan dengan beberapa alat yaitu kamera digital dan kamera thermal [21]. Pada penlitian ini kamera digital yang digunakan berjenis webcam.

Penelitian ini menggunakan Haar-cascade Classifier sebagai algoritma yang digunakan untuk mendeteksi wajah manusia secara *realtime* didukung dengan komputasi yang cepat berdasarkan jumlah piksel dalam persegi pada suatu citra. Metode *Local Binary Pattern Histogram* (LBPH) digunakan untuk pengenalan wajah karena memiliki akurasi tinggi. Penelitian ini dibagi dalam empat bagian, yaitu *Face Detection* menggunakan metode Haar-cascade Classifier, *Face Recognition* menggunakan metode LBPH, dan Perancangan *Hardware*, dan Perancangan *Software* yang akan diuraikan lebih detail seperti berikut.

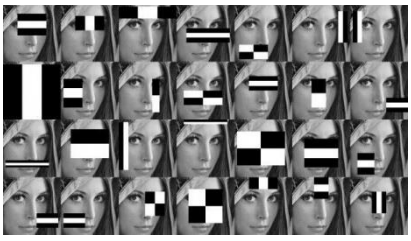
A. *Face Detection*

Deteksi wajah adalah salah satu hal mendasar yang digunakan dalam teknologi pengenalan wajah. OpenCV menyediakan Haar-cascade Classifier yang dapat digunakan untuk mendeteksi wajah pada citra. Pada penelitian ini, Haar-cascade digunakan dalam proses pendeteksian wajah. Alasan menggunakan Haar-cascade adalah karena kecepatan dan akurasi yang tinggi dalam mendeteksi wajah. Haar-cascade Classifier adalah algoritma yang dibuat oleh Paul Viola dan Michael Jones yang dilatih dari banyak citra positif (citra wajah) dan citra negatif (citra tanpa wajah) [22]. Setiap fitur adalah nilai tunggal yang diperoleh dengan mengurangkan jumlah piksel dibawah persegi panjang putih dari jumlah piksel dibawah persegi panjang hitam. Nilai tunggal untuk fitur Haar dihitung menggunakan persamaan berikut:

$$Nilai\ tunggal = hitam - putih = \frac{1}{n}\sum_{hitam}^{n} I(x) - \frac{1}{n}\sum_{putih}^{n} I(x)$$

Dimana n adalah jumlah piksel dan I(x) adalah nilai sebenarnya yang terdeteksi pada sebuah citra.

Citra wajah dikelompokkan berdasarkan sisi yang terang dan sisi yang gelap. Contohnya daerah mata cenderung lebih gelap dibandingkan daerah sekitarnya seperti pada Gambar 1.



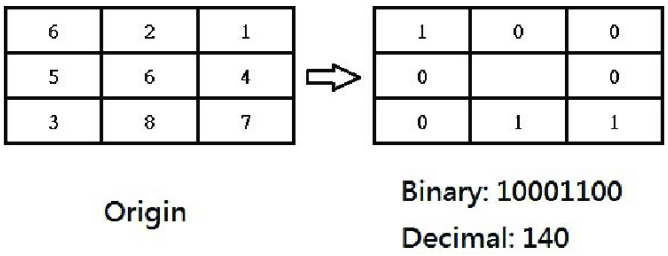
Gambar 1. Haar-cascade Classifier

B. *Face Recognition*

Pengenalan wajah adalah proses mengenali wajah seseorang yang relevan dengan sistem penglihatan. Hal ini telah menjadi alat interaksi manusia-komputer yang penting dalam penggunaannya pada sistem keamanan, kontrol akses, pengawasan video, area komersial dan bahkan digunakan di jejaring sosial seperti Facebook. Setelah perkembangan kecerdasan buatan yang pesat, pengenalan wajah sekali lagi menarik perhatian karena sifatnya yang tidak mengganggu dan menjadi metode utama identifikasi manusia jika dibandingkan dengan jenis teknik biometrik lainnya. Pengenalan wajah dapat dengan mudah diperiksa tanpa sepengetahuan subjek [23].

LBPH adalah salah satu dari tiga algoritma pengenalan wajah bawaan pada *library* OpenCV antara lain *Eigenface*, *Fisherfaces*, dan LBPH. Dibandingan dengan kedua algoritma tersebut, LBPH tidak hanya dapat mengenali muka depan, tetapi juga mengenali muka samping yang lebih fleksibel [24].

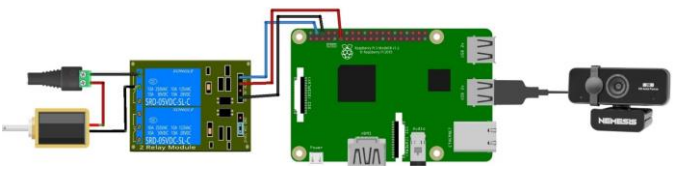
Pada LBPH dilakukan pengolahan citra melalui *preprocessing* salah satunya dengan mengubah citra asli (warna/RGB) menjadi citra abu-abu (*grayscale*). Nilai intensitas tiap piksel pada citra keabuan merupakan nilai tunggal yang berada pada interval 0-255, sedangkan pada citra berwarna perlu tiga nilai intensitas yang berada pada interval 0-255 untuk tiap pikselnya. Semakin mendekati nilai 255 maka derajat keabuan semakin terang [25]. Selanjutnya nilai intensitas untuk setiap pikselnya pada interval 0-255 diubah kedalam bentuk biner dengan membandingkannya dengan nilai tengah yaitu lebih besar atau sama dengan nilai tengah maka akan bernilai biner 1 dan jika lebih kecil dari nilai tengah akan bernilai biner 0. Proses mengubah nilai intensitas setiap piksel pada citra *grayscale* kedalam bentuk biner menggunakan metode LBPH dapat dilihat seperti pada Gambar 2.



Gambar 2. Perubahan Nilai Setiap Piksel Kedalam Bentuk Biner Menggunakan Metode LBPH

C. *Perancangan Hardware*

Pada penelitian ini menggunakan Raspberry Pi 3 model B dengan *circuit diagram* seperti Gambar 3.



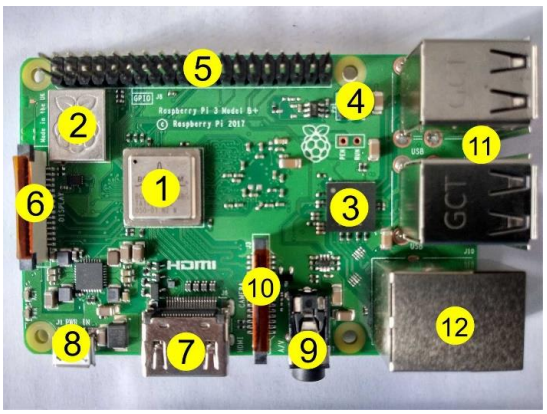
Gambar 3. *Circuit Diagram*

Raspberry Pi dan *solenoid* dihubungkan melalui modul *relay*. Raspberry Pi hanya dapat menyediakan arus sebesar 5 V,

sedangkan *solenoid* membutuhkan 9 V hingga 12 V sehingga adaptor dibutuhkan untuk memberi daya pada *solenoid*. Pin VCC dan GND dari modul *relay* dihubungkan ke 5V dan GND, sedangkan input *relay* terhubungkan ke GPIO 17 pada Raspberry Pi. Pin positif *solenoid* dihubungkan ke kabel positif adaptor 12 V, sedangkan pin negatif *solenoid* dihubungkan ke COM dari *relay*, dan kabel negatif adaptor 12 V dihubungkan ke NO dari *relay*.

Face recognition untuk keamanan ruangan pada penelitian ini menggunakan alat dan bahan yang diuraikan sebagai berikut.

a. Raspberry Pi
Raspberry Pi adalah *System on Chip* (SoC) dengan desain satu papan membawa semua sirkuit penting, seperti *Central Processing Unit* (CPU), *Graphics Processing Unit* (GPU), dan beberapa sirkuit input, output, dan pemrosesan. Ketersediaan fitur seperti pin *General Purpose Input Output* (GPIO) membuat komputer dapat menerima pemrograman *hardware* dan menggerakkan sirkuit elektronik dan mengumpulkan data melalui berbagai cara. Komputer generasi pertama dilengkapi dengan slot kartu SD untuk memungkinkan penginstalan dan penggunaan versi Linux yang sesuai, baik yang disediakan oleh Raspberry Pi Foundation, OS Raspbian, atau salah satu alternatif yang tersedia. Komputer generasi kedua, ketiga, dan keempat memiliki slot kartu MicroSD [25]. Raspberry Pi 3 model B yang digunakan pada penelitian ini dapat dilihat pada Gambar 4.



Gambar 4. Raspberry Pi 3 model B

Komponen yang terdapat pada Raspberry Pi 3 Model B yaitu:

1. RAM 1 GB DDR2 Broadcom BCM2837B0 1.4 GHz
2. Dual-band 802.11 AC Wireless LAN, Bluetooth 4.2
3. Gigabit Ethernet
4. Ethernet POE Power
5. 40 Pin GPIO
6. DSI display screen port
7. HDMI port
8. Power port
9. Audio port
10. Pi Camera port
11. USB Port
12. Ethernet port

b. Kamera
Raspberry Pi dapat menggunakan kamera web atau Pi *Camera*. Seperti pada Gambar 5, penelitian ini menggunakan Webcam Nemesis A95 yang memiliki resolusi 1920x1080 dengan USB *plug and play* yang dapat dikonfigurasi dengan Raspberry Pi. Webcam digunakan sebagai alat untuk menangkap citra yang diproses pada sistem.

Gambar 5. Kamera NYK Nemesis A95

c. Modul *Relay*
Relay adalah perangkat yang dioperasikan secara elektrik. Sederhananya, *relay* adalah saklar otomatis untuk mengendalikan rangkaian arus tinggi maupun arus rendah. Pada penelitian ini menggunakan modul relay *two-channel* seperti pada Gambar 6.

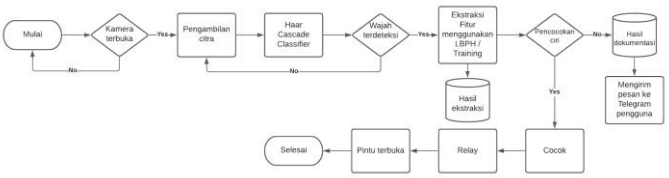
Gambar 6. Modul *Relay*

d. *Solenoid Door Lock*
Gambar 7 adalah *solenoid* yang digunakan pada penelitian ini untuk membuka kunci dan menutup kunci pada pintu secara otomatis sesuai dengan keadaan *relay*.

Gambar 7. *Solenoid Door Lock*

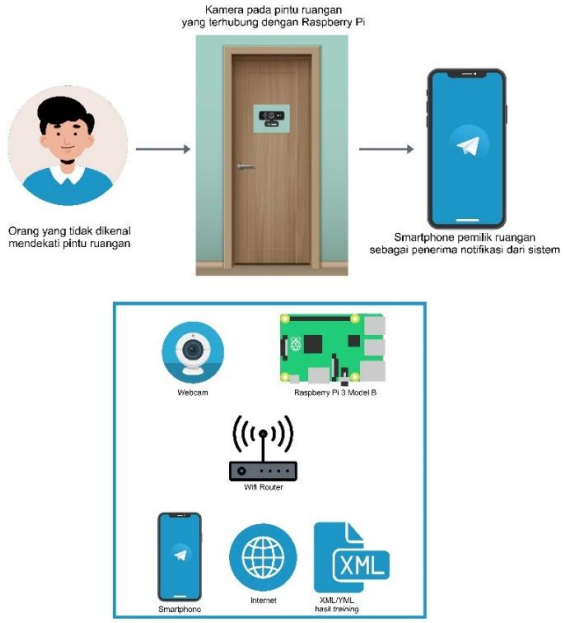
D. Perancangan Software

Penelitian ini menggunakan bahasa pemrograman Python dan aplikasi Telegram pada *smartphone*. Tahap awal penelitian dilakukan *training* dengan menambahkan wajah yang akan dikenali oleh sistem. Ketika alat dinyalakan, sistem akan terus-menerus atau secara *realtime* melakukan pendeteksian. Apabila sistem mendeteksi adanya wajah manusia maka Raspberry Pi akan membuat kamera untuk menangkap citra. Selanjutnya citra dilakukan pencocokan dengan *database*. Apabila citra yang diproses terdapat kecocokan maka Raspberry Pi akan membuat pintu dalam kondisi terbuka. Namun apabila citra yang ditangkap dan diproses tidak ada kecocokan dengan *database* maka Raspberry Pi akan mengirimkan pemberitahuan dan mengirimkan citra melalui aplikasi Telegram pemilik rumah. Gambar 8 adalah diagram alir dari keseluruhan sistem yang diusulkan.



Gambar 8. Diagram Alir Sistem yang Diusulkan

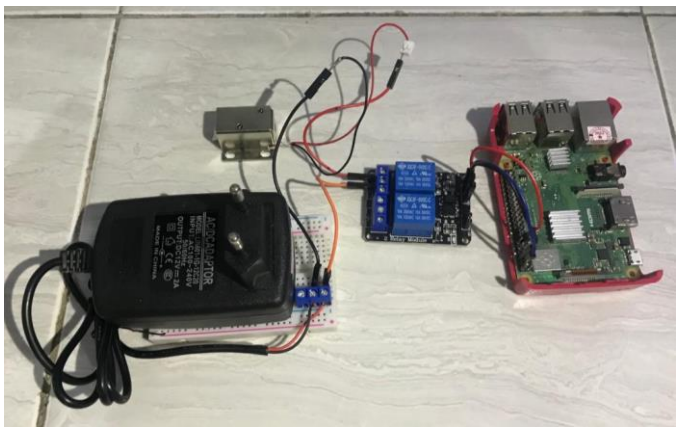
Webcam menangkap citra wajah yang mendekati ruangan. Sistem akan mengenali wajah tersebut dan mencocokkan dengan file hasil *training* berupa file xml/yml apakah dikenal atau dikenal. Jika dikenali maka sistem akan memberi arus kepada *solenoid* melalui *relay* untuk membuka kunci pintu. Akan tetapi, jika tidak dikenali maka sistem akan mengambil citra dan mengirimkan pesan notifikasi melalui Telegram yang ada di *smartphone* pemilik ruangan. Sistem yang dibangun ditunjukkan pada Gambar 9.



Gambar 9. Sistem Pengenalan Wajah untuk Kemanan Ruangan

IV. HASIL DAN ANALISA

Alat atau komponen dirancang sesuai dengan *circuit diagram* pada Gambar 3 agar perangkat dapat berjalan dengan benar. Sistem ini terutama terdiri dari Raspberry Pi sebagai inti sistem untuk mengenali wajah dari citra yang ditangkap oleh webcam dan *solenoid* sebagai pembuka dan pengunci pintu pada ruangan seperti yang ditampilkan pada Gambar 10.



Gambar 10. Implementasi *Hardware*

A. Pengujian Keseluruhan Alat

Proses pertama adalah citra diubah dari RGB menjadi *grayscale.* Citra *grayscale* tersebut kemudian dilakukan pemindaian dengan *Cascade Classifier.*

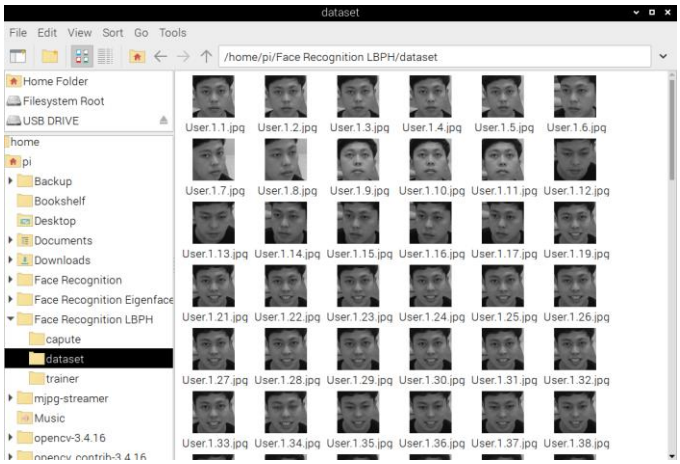
Tahapan pengambilan citra sebagai berikut:

1. Memasukkan nama orang yang akan diberikan otoritas pada sistem.
2. Melakukan konversi gambar dari RGB menjadi *grayscale*. Hal ini dilakukan untuk membuat nilai intensitas pada setiap piksel pada citra menjadi nilai tunggal agar dapat diubah kedalam bentuk biner dengan menggunakan metode LBPH.
3. Mengambil citra wajah sebanyak 100 sampel yang disimpan didalam folder *dataset* dengan jarak kurang dari 0,7 meter dan diambil pada waktu siang dengan intesitas cahaya ruangan cukup terang.

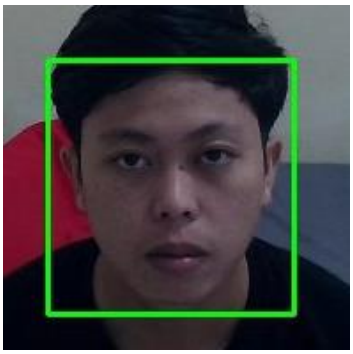
Semua citra wajah yang telah didapatkan akan dilakukan *training* menggunakan metode LBPH. Hasil *training* disimpan kedalam file xml/yml. Gambar 11 menampilkan hasil pengambilan citra wajah untuk *dataset* yang sebelumnya dilakukan konversi dari RGB menjadi *grayscale* lalu dilakukan *cropping* sesuai citra yang terdeteksi berupa wajah. Citra wajah diambil sebanyak 100 sampel untuk dilakukan *training* yang ada pada pada tahap selanjutnya.

Sebanyak 100 sampel citra yang sudah menyelesaikan *training* akan dicocokkan dengan hasil deteksi dari *streaming* kamera. Hasil deteksi tergantung dari tingkat *confidence* dengan *output* dikenali atau tidak dikenali. Setelah kamera mendeteksi wajah pada citra maka otomatis sistem akan mencocokkan citra terhadap hasil *training* yang sebelumnya dilakukan. Jika wajah dikenali maka *solenoid door lock* akan otomatis membuka. Jika wajah tidak dikenali maka sistem akan mengirim hasil citra kepada pemilik rumah melalui aplikasi Telegram. Pada 20 kali

percobaan, jarak terbaik kamera terhadap objek wajah adalah kurang dari 0,7 meter.



Gambar 11. *Dataset* yang Dilakukan *Training*



Gambar 12. Saat Sistem Melakukan Pengenalan Wajah

Pada Gambar 12 sistem akan mengidentifikasi citra dari kamera menggunakan *Haar-cascade Classifier* untuk mengetahui citra tersebut terdeteksi wajah atau bukan wajah. Ini dilakukan dengan memberi tanda bujur sangkar berwarna hijau, lalu citra yang teridentifikasi sebagai wajah akan dicocokkan menggunakan LBPH terhadap file hasil *training*.

Diketahui rata-rata waktu yang dibutuhkan oleh Sistem Pengenalan Wajah untuk Keamanan Ruangan Menggunakan LBPH dari Raspberry Pi 3 B untuk berada pada posisi siap digunakan dari 10 kali percobaan adalah 19,78 detik. Tahap selanjutnya yaitu pengiriman citra. Pengiriman citra dilakukan ketika kamera tidak dapat mengenali wajah yang terdeteksi. Pada proses ini, sistem telah dihubungkan dengan koneksi internet dan mendapat API sertai ID dari akun Telegram agar gambar yang dikirim dari sistem dapat diterima oleh pengguna.

B. Pengujian Alat dengan Variasi Jarak Kurang dari 0,7 meter

Pada proses pengujian ini, pengenalan wajah dilakukan sebanyak 10 kali untuk untuk mengetahui seberapa cepat dan akurat sistem mengenali wajah pada jarak kurang dari 0,7 meter. Tabel 1 adalah hasil pengujian alat di ruangan dengan posisi sistem *standby*.

Tabel 1. Hasil Pengujian Sistem dengan Jarak 0 Sampai 0,7 m

No	Waktu (Detik)	Benar/Salah
1	2.,31	Benar
2	1,84	Benar
3	1,69	Benar
4	1,49	Benar
5	1,06	Benar
6	0,72	Benar
7	0,81	Benar
8	0,96	Benar
9	0,75	Benar
10	1,36	Benar

Berdasarkan data pada Tabel 1 didapat data pengujian yaitu 10 benar terdeteksi dengan akurasi 100% dan waktu yang dibutuhkan sistem dalam mengenali wajah rata-rata adalah 1,30 detik.

C. Pengujian Alat dengan Variasi Jarak Lebih dari 0,7 meter

Pada proses pengujian ini, pengenalan wajah dilakukan sebanyak 10 kali untuk untuk mengetahui seberapa cepat dan akurat sistem mengenali wajah pada jarak lebih dari 0,7 meter dan maksimal 1 meter. Tabel 2 adalah hasil pengujian alat di ruangan dengan posisi sistem *standby*.

Tabel 2. Hasil Pengujian Sistem dengan Jarak 0,7 Sampai 1 m

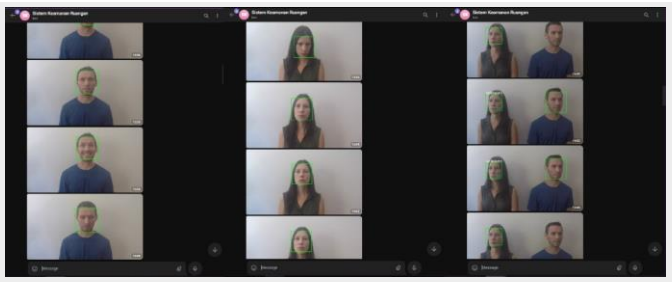
No	Waktu (detik)	Benar/Salah
1	2,51	Salah
2	2,31	Benar
3	2,03	Salah
4	1,97	Benar
5	2,01	Salah
6	1,80	Salah
7	1,42	Benar
8	1,26	Benar
9	1,02	Benar
10	0,92	Benar

Berdasarkan data pada Tabel 2, didapat 6 kali percobaan mendapatkan hasil benar terdeteksi dan 4 salah terdeteksi. Oleh karenanya didapatkan akurasi 60% dan waktu yang dibutuhkan sistem dalam mengenali wajah rata-rata adalah 1,72 detik. Uji coba dengan jarak lebih 1 meter juga dilakukan dengan hasil wajah dapat terdeteksi tetapi sistem tidak dapat mengenali wajah tersebut seperti pada Gambar 13.

Gambar 13. Sistem Tidak Mengenali Wajah dengan Jarak Lebih dari 1 Meter

D. Pengujian Alat dalam Mengirim Pesan ke Telegram

Sistem mendeteksi wajah pada citra maka otomatis sistem akan mencocokkan citra terhadap hasil *training* yang sebelumnya dilakukan. Jika wajah dikenali maka *solenoid door lock* otomatis membuka, sebaliknya jika wajah tidak dikenali maka sistem akan mengirim hasil citra berupa foto yang dikirim kepada pemiik rumah melalui Telegram. Seperti pada Gambar 14, pengujian dilakukan menggunakan tiga sampel wajah yang tidak dikenali oleh sistem yang kemudian sistem akan mengirim pesan berupa citra dari kamera kepada pemilik ruangan melalui Telegram.



Gambar 14. Sistem Mengirim Citra Gambar Melalui Telegram Kepada Pengguna

Pada proses pengujian ini, pengenalan wajah dilakukan setiap sampel video orang tidak dikenali oleh sistem masing-masing sebanyak lima kali untuk mengetahui seberapa cepat sistem dalam mengirimkan pesan melalui Telegram dengan posisi sistem *standby* dan jaringan yang stabil. Tabel 3 adalah hasil pengujian Sistem Pengenalan Wajah Menggunakan Metode LBPH dengan Raspberry Pi 3 B.

Tabel 3. Hasil Pengujian Sistem dalam Mengirim Citra Gambar Melalui Telegram Kepada Pengguna

No	Waktu (detik)		
	Sampel 1	Sampel 2	Sampel 3
1	0,45	2,31	2,42
2	0,47	1,73	1,79
3	0,50	1,32	1,14
4	0,42	0,53	1,25
5	0,56	1,12	1,63

Berdasarkan Tabel 3, pengujian menggunakan sampel 1 didapat data rata-rata waktu yang diperlukan sistem untuk mengirimkan pesan melalui Telegram sampai diterima oleh pengguna adalah 0,48 detik. Sampel 2 didapat data rata-rata waktu yang diperlukan sistem untuk mengirimkan pesan melalui Telegram sampai diterima oleh pengguna adalah 1,4 detik. Sampel 3 didapat data rata-rata waktu yang diperlukan sistem untuk mengirimkan pesan melalui Telegram sampai diterima oleh pengguna adalah 1,65 detik.

V. KESIMPULAN

Berdasarkan hasil perancangan dan pengujian yang telah dilakukan dapat ditarik beberapa kesimpulan sebagai berikut. Waktu yang dibutuhkan Raspberry Pi 3 B untuk menjalankan program sampai ke posisi *standby* adalah 19,78 detik. Dari hasil pengujian pertama sistem pengenalan wajah menggunakan metode LBPH dalam jarak kurang dari 0,7 meter didapatkan keberhasilan deteksi dengan benar memiliki nilai yang paling tinggi yaitu 100%. Pengujian kedua sistem pengenalan wajah menggunakan metode LBPH dalam jarak 0,7 meter sampai 1 meter didapatkan keberhasilan deteksi dengan benar yaitu 60%. Jarak terbaik sistem pengenalan wajah menggunakan metode LBPH adalah kurang dari 0,7 meter dengan intensitas cahaya yang sangat berpengaruh. Dari hasil pengujian ketiga yaitu mengukur seberapa cepat sistem dalam mengirim pesan berupa citra gambar melalui Telegram sampai diterima pengguna. Digunakan tiga sampel video didapatkan data sampel 1 dengan rata-rata 0,48 detik, sampel 2 dengan rata-rata 1,4 detik, dan sampel 3 dengan rata-rata 1,65 detik.

UCAPAN TERIMA KASIH

Ucapan terima kasih diberikan kepada Universitas Ahamad Dahlan yang telah mendukung dalam penyelesaian penelitian ini.

DAFTAR PUSTAKA

[1] A. Yudhana, S. Sunardi, and P. Priyatno, "Perancangan Pengaman Pintu Rumah Berbasis Sidik Jari Menggunakan Metode UML," *J. Teknol.*, vol. 10, no. 2, pp. 131–138, 2018, [Online]. Available: https://dx.doi.org/10.24853/jurtek.10.2.131-138.

[2] A. Yudhana, S. Sunardi, and P. Priyatno, "Development of Door Safety Fingerprint Verification Using Neural Network," *J. Phys. Conf. Ser.*, vol. 1373, no. 1, 2019, doi: 10.1088/1742-6596/1373/1/012053.

[3] N. A. Hussein and I. Al Mansoori, "Smart Door System for Home Security Using Raspberry Pi3," *2017 Int. Conf. Comput. Appl. ICCA 2017*, pp. 395–399, 2017, doi: 10.1109/COMAPP.2017.8079785.

[4] A. Nag, J. N. Nikhilendra, and M. Kalmath, "IOT Based Door Access Control Using Face Recognition," *2018 3rd Int. Conf. Converg. Technol. I2CT 2018*, pp. 1–3, 2018, doi: 10.1109/I2CT.2018.8529749.

[5] Soe Sandar | Saw Aung Nyein Oo, "Development of a Secured Door Lock System Based on Face Recognition Using Raspberry Pi and GSM Module," *Int. J. Trend Sci. Res. Dev.*, vol. 3, no. 5, pp. 357–361, 2019, [Online]. Available: http://www.ijtsrd.com/papers/ijtsrd25280.pdf.

[6] Z. Zhu and Y. Cheng, "Application of Attitude Tracking Algorithm for Face Recognition Based on OpenCV in the Intelligent Door Lock," *Comput. Commun.*, vol. 154, no. 900, pp. 390–397, 2020, doi: 10.1016/j.comcom.2020.02.003.

[7] R. A. Nadafa, S. M. Hatturea, V. M. Bonala, and S. P. Naikb, "Home Security Against Human Intrusion Using Raspberry Pi," *Procedia Comput. Sci.*, vol. 167, no. Iccids 2019, pp. 1811–1820, 2020, doi: 10.1016/j.procs.2020.03.200.

[8] M. Turk and A. Pentland, "Eigenfaces for Recognition," *J. Cogn. Neurosci.*, vol. 3, no. 1, pp. 71–86, Jan. 1991, doi: 10.1162/jocn.1991.3.1.71.

[9] M. S. Bartlett, J. R. Movellan, and T. J. Sejnowski, "Face Recognition by Independent Component Analysis," *IEEE Trans. Neural Networks*, vol. 13, no. 6, pp. 1450–1464, Nov. 2002, doi: 10.1109/TNN.2002.804287.

[10] J. Lu, K. N. Plataniotis, and A. N. Venetsanopoulos, "Face recognition using LDA-based algorithms," *IEEE Trans. Neural Networks*, vol. 14, no. 1, pp. 195–200, 2003, doi: 10.1109/TNN.2002.806647.

[11] B. Heisele, P. Ho, and T. Poggio, "Face recognition With Support Vector Machines: Global Versus Component-based Approach," *Proc. IEEE Int. Conf. Comput. Vis.*, vol. 2, no. July, pp. 688–694, 2001, doi: 10.1109/ICCV.2001.937693.

[12] A. V. Nefian and M. H. Hayes, "Hidden Markov Models for Face Recognition," in *Proceedings of the 1998 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP '98 (Cat. No.98CH36181)*, 1998, vol. 5, no. 4, pp. 2721–2724, doi: 10.1109/ICASSP.1998.678085.

[13] T. K. Vamsi, K. C. Sai, and M. Vijayalakshmi, "Face Recognition Based Door Unlocking System Using Raspberry Pi," *nternational J. Adv. Res.*

Ideas Innov. Technol., vol. 5, no. 2, pp. 1320–1324, 2019, [Online]. Available: https://www.ijariit.com/manuscripts/v5i2/V5I2-1856.pdf.

[14] S. Saifullah, S. Sunardi, and A. Yudhana, "Analisis Perbandingan Pengolahan Citra Asli dan Hasil Croping untuk Identifikasi Telur," *J. Tek. Inform. dan Sist. Inf.*, vol. 2, no. 3, pp. 341–350, 2016, doi: 10.28932/jutisi.v2i3.512.

[15] P. B. Patel, V. M. Choksi, S. Jadhav, and M. B. Potdar, "Smart Motion Detection System Using Raspberry Pi," *Int. J. Appl. Inf. Syst.*, vol. 10, no. 5, pp. 37–40, Feb. 2016, doi: 10.5120/ijais2016451506.

[16] N. Surantha and W. R. Wicaksono, "Design of Smart Home Security System using Object Recognition and PIR Sensor," *Procedia Comput. Sci.*, vol. 135, pp. 465–472, 2018, doi: 10.1016/j.procs.2018.08.198.

[17] S. Desai and V. D. Pawar, "Smart Door Security System Using Raspberry Pi with Telegram," *Int. Res. J. Eng. Technol.*, vol. 6, no. 6, pp. 1400–1404, 2019, [Online]. Available: https://www.irjet.net/archives/V6/i6/IRJET-V6I6338.pdf.

[18] M. Sajjad *et al.*, "Raspberry Pi Assisted Face Recognition Framework for Enhanced Law-enforcement Services in Smart Cities," *Futur. Gener. Comput. Syst.*, vol. 108, pp. 995–1007, 2020, doi: 10.1016/j.future.2017.11.013.

[19] M. I. Pure, A. Ma'arif, and A. Yudhana, "Alat Deteksi Detak Jantung Pada Atlet Maraton Menggunakan Raspberry," vol. 7, no. 2, pp. 282–290, 2021.

[20] Sunardi, A. Yudhana, and S. Saifullah, "Identity Analysis of Egg Based on Digital and Thermal Imaging: Image Processing and Counting Object Concept," *Int. J. Electr. Comput. Eng.*, vol. 7, no. 1, pp. 200–208, 2017, doi: 10.11591/ijece.v7i1.pp200-208.

[21] A. Yudhana, Sunardi, and S. Saifullah, "Segmentation Comparing Eggs Watermarking Image and Original Image," *Bull. Electr. Eng. Informatics*, vol. 6, no. 1, pp. 47–53, 2017, doi: 10.11591/eei.v6i1.595.

[22] P. Viola and M. Jones, "Rapid Object Detection Using a Boosted Cascade of Simple Features," in *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. CVPR 2001*, 1979, vol. 1, no. 10, pp. I-511-I–518, doi: 10.1109/CVPR.2001.990517.

[23] M. Coskun, A. Ucar, O. Yildirim, and Y. Demir, "Face Recognition Based on Convolutional Neural Network," in *2017 International Conference on Modern Electrical and Energy Systems (MEES)*, Nov. 2017, vol. 54, no. 5, pp. 376–379, doi: 10.1109/MEES.2017.8248937.

[24] X. M. Zhao and C. B. Wei, "A Real-time Face recognition System Based on the Improved LBPH Algorithm," *2017 IEEE 2nd Int. Conf. Signal Image Process. ICSIP 2017*, vol. 2017-Janua, pp. 72–76, 2017, doi: 10.1109/SIPROCESS.2017.8124508.

[25] A. Yudhana, S. Sunardi, and S. Saifullah, "Perbandingan Segmentasi Pada Citra Asli dan Citra Komprese Wavelet untuk Identifikasi Telur," *Ilk. J. Ilm.*, vol. 8, no. 3, pp. 190–196, Dec. 2016, doi: 10.33096/ilkom.v8i3.75.190-196.