IMPLEMENTASI FACE RECOGNITION MENGGUNAKAN METODE HAAR-CASCADE CLASSIFIER UNTUK SISTEM KEAMANAN PINTU

Rahmat Irianto[1], Sidik Prabowo, S.T., M.T.[2], Rahmat Yasirandi, S.T., M.T.[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung

[1]rahmatirianto@students.telkomuniversity.ac.id, [2]pakwowo@telkomuniversity.ac.id, [3] batanghitam@telkomuniversity.ac.id

Abstrak

Paper ini berisikan hasil uji coba implementasi system keamaan pintu berbasis teknologi dengan menggunakan Face Recognition dengan metode haar-cascade classifier dan notifikasi menggunakan aplikasi telegram yang diterapkan pada miniatur pintu dengan menggunakan Raspberry Pi 2 sebagai microcontroller utama. Dimana bila ingin membuka kunci selenoid wajah user harus terlebih dahulu didaftarkan kedalam dataset. Berdasarkan hasil uji coba yang telah dilakukan bahwa system dapat 100% membedakan wajah yang telah terdaftar pada dataset dengan wajah yang tidak terdaftar pada dataset.

Kata kunci: **Dataset, Face Recognition, PIN, Raspberry Pi 2.**

Abstract

This paper contains the results of a trial of implementing a technology-based security system using Face Recognition with the haar-cascade classifier method and notifications using a telegram application that is applied to miniature doors using Raspberry Pi 2 as the main microcontroller. Where if you want to unlock the selenoid face the user must first be registered into the dataset. Based on the results of trials that have been done that the system can 100% distinguish faces that have been registered in the dataset with faces that are not registered in the dataset.

1. PENDAHULUAN

Latar Belakang

Perkembangan teknologi sangat pesat dan sudah memasuki aspek aspek kehidupan manusia, salah satunya adalah keamaan. Secara garis besar sebuah sistem keamanan dapat dibagi menjadi 3 bagian besar yaitu, what you have seperti kunci, id card, token dll, kemudian what you know seperti password dan juga what you are seperti biometric security[7].

kelemahan dari sistem keamanan berbasis what you have seperti kunci, id card, token, dll adalah bisa dicuri, kelupaan, diduplikasi [7][9]. Kemudian kelemahan sistem keamanan berbasis what you know seperti pin tau password adalah kebanyakan orang mengunakan password yang simpel agar mudah diingat, sehinggal mudah di tebak,sedangkan password yang panjang dan berubah rubah cenderung susah diingat [7][9] dan walaupun password yang digunakan sudah cukup aman, masih ada metode seperti social engineering dan keyloger [1]. Karenanya biometric security sendiri memiliki keunggulan karena tujuan dari biometric security sendiri adalah untuk membuat authenticator dan pemilik akses tidak terpisahkan, sesuatu yang tidak bisa dilakukan oleh password ataupun token/kunci dikarenakan password ataupun token/kunci dapat dipinjamkan ataupun dicuri [7]. Biometrik juga telah digunakan untuk merujuk pada bidang teknologi yang ditujukan untuk identifikasi individu berdasarkan sifat biologis mereka, seperti yang didasarkan pada pemindaian retina, pola iris, sidik jari atau pengenalan wajah(face recognition) [2].

Terdapat beberapa jenis biometric security, face recognition, fingger print, voice dan lain lain, namun yang paling sering digunakan pada saat ini adalah face recognition dan fingger print. Metode fingger print memiliki beberapa kelemahan bila dibandingkan dengan face recognition yaitu fingger print biasanya hanya menggunakan 1 dari 10 jari yang dimiliki, sedangkan manusia hanya memiliki 1 wajah. Fingger print bukan sesuatu yang sangat private dikarenakan kita selalu meninggalkan finger print hampir dimana saja berbeda dengan wajah manusia dimana kita tidak meninggalkan jejak wajah. Dan juga fingger print membutuhkan kontak dengan alat sedangkan face recognition tidak sehingga dapat menguntungkan pada area yang wajib bersih/steril [8].

Face recognition adalah suatu metode untuk mengenali suatu citra wajah tertentu dengan membandingkan gambar yang didapatkan dengan gambar dataset yang telah tersimpan sebelumnya. Jurnal ini berisi tentang face recognition dengan metode Haar-Cascade classifier untuk mengidentifikasi pemilik akses dan juga memberikan notifikasi kepada aplikasi telegram.

Topik dan Batasannya

Permasalahan yang dijadikan dalam penelitian ini adalah sebagai berikut,

1. Berapa hasil akurasi untuk user yang bisa membuka kunci selenoid dan tidak ?
2. Berapa hasil confident yang dibutuhkan agar sistem dapat membedakan user terdaftar dan yang tidak ?

Batasan masalah dalam penelitian tugas akhir ini adalah sebagai berikut :

1. Sample dataset yang digunakan dalam penelitian ini berjumlah 300 citra untuk 3 orang, 100 citra pada masing masing sampel wajah/orang.
2. Pengambilan dataset dan uji coba digunakan pada tempat yang memiliki cukup cahaya untuk sistem dapat mengenali sebuah wajah.
3. Jarak webcam pada saat pengambilan dataset dan uji coba ± sama.
4. Algoritma yang digunakan adalah algoritma Haar cascade classifier untuk face detection dan algoritma LBPH (Local Binary Patterns Histogram) untuk melakukan face recognisi.
5. Menggunakan Raspberry pi sebagai microcontroller utama dan arduino mega sebagai secondary microcontroller.
6. Pengambilan dataset dan juga uji coba dilakukan pada tempat yang sama dan dalam kondisi cahaya yang sama.
7. Camera yang digunakan adalah logitec c170.

Tujuan

Berdasarkan rumusan masalah maka tujuan dari tugas akhir ini adalah mengetahui hasil akurasi sistem dalam membedakan orang yang bisa membuka kunci dan yang tidak, serta mengetahui tingkat confidet system dalam membedakan user terdaftar pada dataset dengan yang tidak terdaftar.

2. STUDI TERKAIT

2.1. Similar Works

Pada saat ini telah ada beberapa penelitian yang berkaitan dengan system keamanan pintu, salah satunya seperti penelitian pada paper [3]. Dimena penelitian tersebut berisi penelitian tentang system keamanan pintu dengan menggunakan finger print dan juga PIN dan pertanyaan sebagai alat untuk mengidentifikasi seseorang yang di izinkan mengakses pintu, yang kemudian notifikasi akan diberikan pada sebuah halaman website khusus.

Kemudian pada paper [4] melakukan penelitian tentang system keamanan pintu dengan memanfaatkan PIN dan face recognition sebagai alat identifikasi user, dimana pada penelitian ini bila PIN yang di inputkan salah maka, secara otomatis system akan mengaktifkan kamera untuk menjalankan face recognition, dan notifikasi akah diberikan pada email khusus yang terdaftar.

Perbedaan dengan penelitian pada paper ini adalah, pada penelitian ini menggunakan Face recognition dengan metode Haar-cascade classifier sebagai alat untuk mengidentifikasi sesorang, yang bila mana pada saat user terdaftar atau tidak terdaftar mengakses alat maka user terdaftar ataupun tidak sama sama akan diambil gambarnya untuk kemudian dikirimkan pada aplikasi telegram.

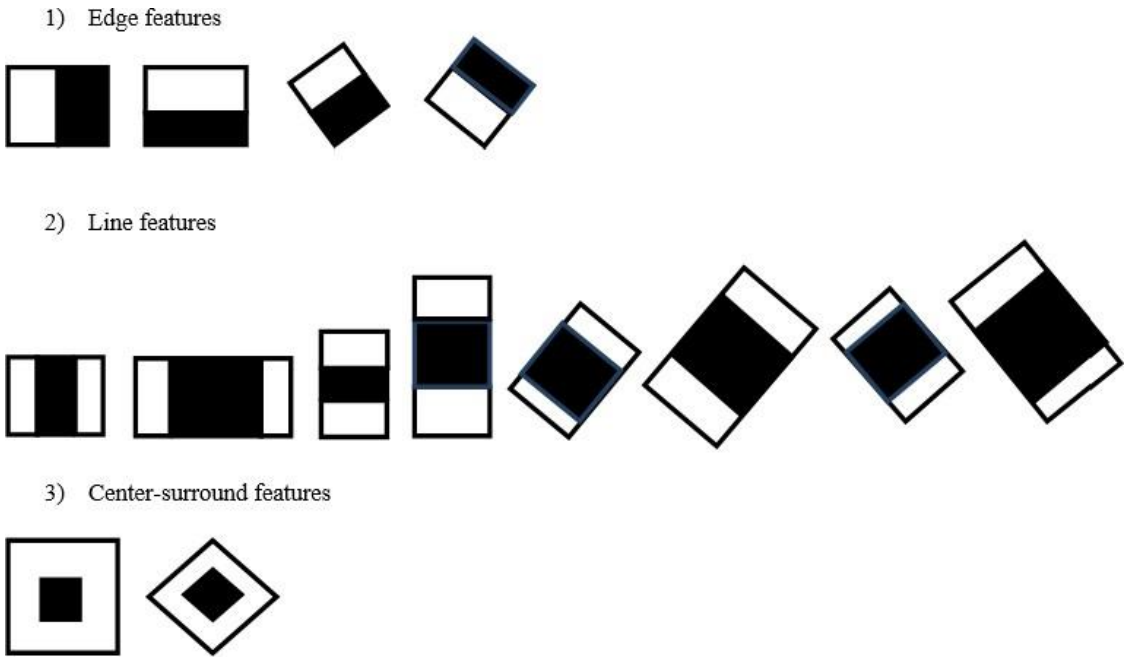
2.2. Face Recognition

Istilah biometrik juga telah digunakan untuk merujuk pada bidang teknologi yang muncul yang ditujukan untuk identifikasi individu berdasarkan sifat biologis mereka, seperti yang didasarkan pada retina scan, iris-pattern, finger print atau face recognition [2]. Face recognisi sendiri masih memiliki beberapa masalah dan juga membutuhkan beberapa Batasan Batasan tertentu agar dapat bekerja secara optimal. Menemukan wajah didalam sebuah gambar sedangkan posisi, orientasi, latar belakang dan ukuran wajah adalah variabel, adalah tugas yang sangat sulit dan banyak algoritma telah dikerjakan untuk menyelesaikan masalah ini. Masalah lain dengan deteksi wajah terjadi setiap kali wajah tertutup sebagian, seperti jenggot, kacamata, gaya rambut atau topi, karena banyak informasi tetap tersembunyi [2].

2.3. *Haar Cascade Classifier*

Haar like feature atau yang juga dikenal dengan Haar cascade classifier adalah salah satu dari sekian banyak metode yang digunakan untuk menelakukan face detection dan juga face recognition. Haar cascade classifier sendiri pertama kali digagas oleh Paul Viola dan Michael Jhon dalam jurnalnya yang berjudul “Rapid Object Detection using a Bossted Cascade of Simple Features”[5]. Haar like features adalah rectangular (persgi) features, dimana yang dinilai adalah jumlah pixel dari tiap persegi dan bukan berdasarkan nilai dari setiap pixel pada sebuah image [5]. Haar like features sendiri adalah gabungan

daripada kotak hitam dan putih.

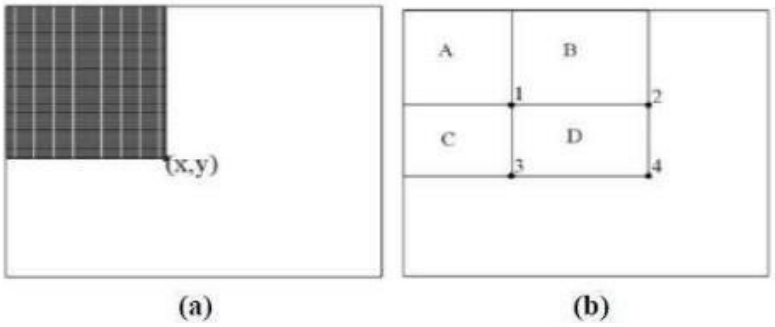


Gambar 1. Haar Like Features [6]

Cara untuk mengetahui adanya feature Haar pada suatu image dengan cara mengurangi jumlah rata rata pixel pada daerah gelap dengan rata rata jumlah pixel pada daerah terang (menggunakan rumus dibawah).

$$f(x) = SumBlackrectangle - SumWhiterectangle \quad . \; . \; . \; . \; .[1]$$

jika hasil perbedaannya berada diatas nilai threshold maka dianggap bahwa terdapat feature haar pada suatu gambar. Kotak pada haar like features dapat dihitung menggunakan integral image. Secara umum integral image adalah menambahkan nilai nilai pixel secara bersamaan.



Gambar 2. Integral Image[6]

Pada gambar 2(a) dapat dilihat bahwa nilai yang terdapat pada lokasi pixel (x,y) berisi semua nilai dari daerah kiri atas hingga titik (x,y). Dimana bila ingin mendapatkan nilai pixel didalam kotak D (gambar 2b) dapat dilakukan dengan cara menggunakan rumus dibawah.

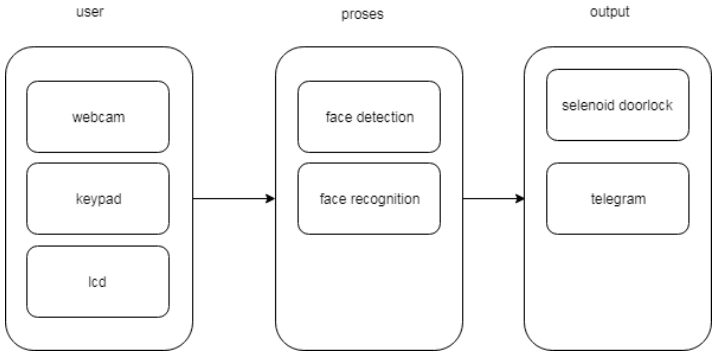
$$D = (A+B+C+D) - (A+B) - (A+C) + A \quad . \quad . \quad . \quad . \quad . \quad [2]$$

2.4. *Telegram*

Telegram adalah sebuah aplikasi messaging yang memungkinkan pengguna untuk mengirimkan pesan, gambar, video, dokumen, dan lainnya tanpa menetapkan besarnya size file yang dikirimkan serta mampu mengirimkan lokasi. Telegram juga menyediakan sebuah API (Application Programming Interface atau Antarmuka Pemrograman Aplikasi) berupa Telegram Bot API yang memungkinkan siapa saja untuk membuat bot mereka sendiri untuk

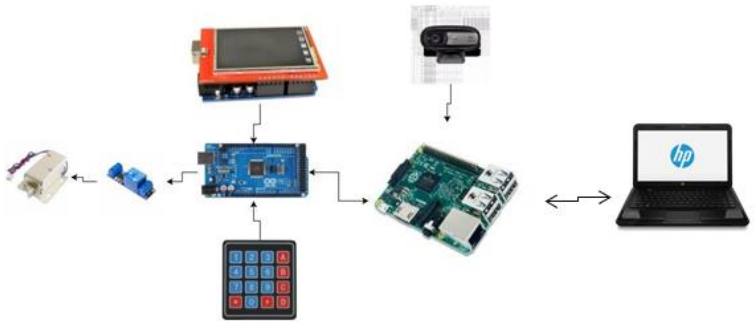
3. PERANCANGAN SISTEM

Perancangan sistem keamanan akses pintu menggunakan face recognition ini mengacu berdasarkan blok diagram pada gambar 3 . Dimana untuk bagian input terdiri keypad agar user dapat menekan tombol sebagai input inisialisasi proses face detection dan face recognition, dan juga webcam untuk mengambil citra wajah. Bagian proses terjadi didalam laptop yang digunakan untuk memproses pendeteksian dan mencocokan wajah dari database, dimana hasil dari face recognisi ini memberikan output pada selenoid doorlock selaku actuator buka dan tutupnya pintu, dan juga hasil face recognisi menentukan hasil pesan yang dikirim pada aplikasi telegram. Sebuah solenoid door lock sebagai actuator buka dan tutupnya pintu.



Gambar 3. Blok diagram sistem

3.1. Perancangan Alat



Gambar 4 perancangan alat

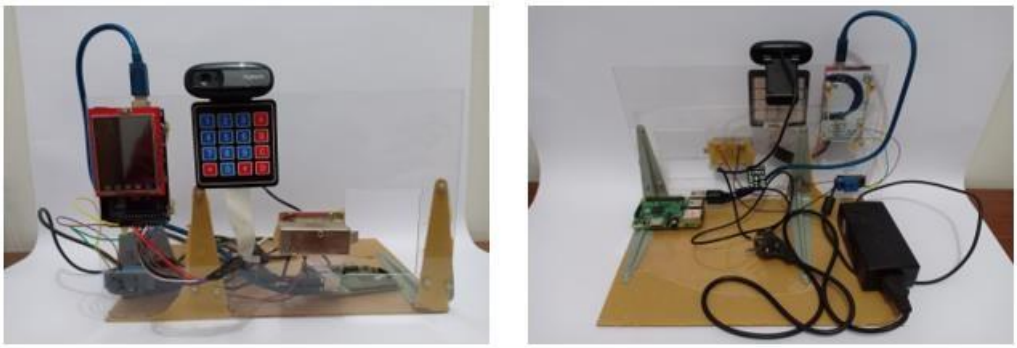
Gambar 4 menunjukkan skematik dari sistem elektronik pada sistem ini. Perancangan sistem elektronik dari sistem keamanan pintu menggunakan face recognition berbasis raspberry pi ini menggunakan alat dan bahan sebagai berikut:

1) Selenoid doorlock sebagai actuator terkunci dan terbukanya pintu. Solenoid door lock yang digunakan pada sistem ini digerakkan dengan tegangan 11V DC sehingga untuk sumber salah satu kaki dihubungkan pada adaptor 12v dan satu kaki dihubungkan dengan relay dimana dipasangkan ke ground adaptor 12v dan Raspberry Pi 2.

2) Modul relay yang digunakan ini merupakan modul dengan 1 Channel, berfungsi pemutus otomatis tegangan pada sistem. Pemilihan modul relay karena telah memiliki pin power, ground dan input dimana power dan ground sebagai sumber tegangan dan grounding, pin input disambungkan ke pin digital 14 pada Raspberry Pi 2 sebagai pengatur keadaan relay
3) Arduino mega sebagai penerima input dari keypad serta pengatur lcd.
4) Keypad untuk user memberikan input
5) Lcd untuk memberikan feedback pada user
6) Webcam sebagai pengambil citra wajah. WebCam yang digunakan pada perancangan ini adalah Logitech c170, dengan spesifikasi kamera 5 megapiksel serta memiliki auto fokus.
7) Raspberry pi 2 sebagai pengaktif webcam dan penerima hasil olah citra yang dihasilkan laptop.
8) Laptop sebagai yang menjalankan face detection dan face recognition kemudian memberiank hasil face recognition kepada raspberry pi 2. Laptop yang digunakan pada penelitin ini adalah HP 1000 notebook pc.

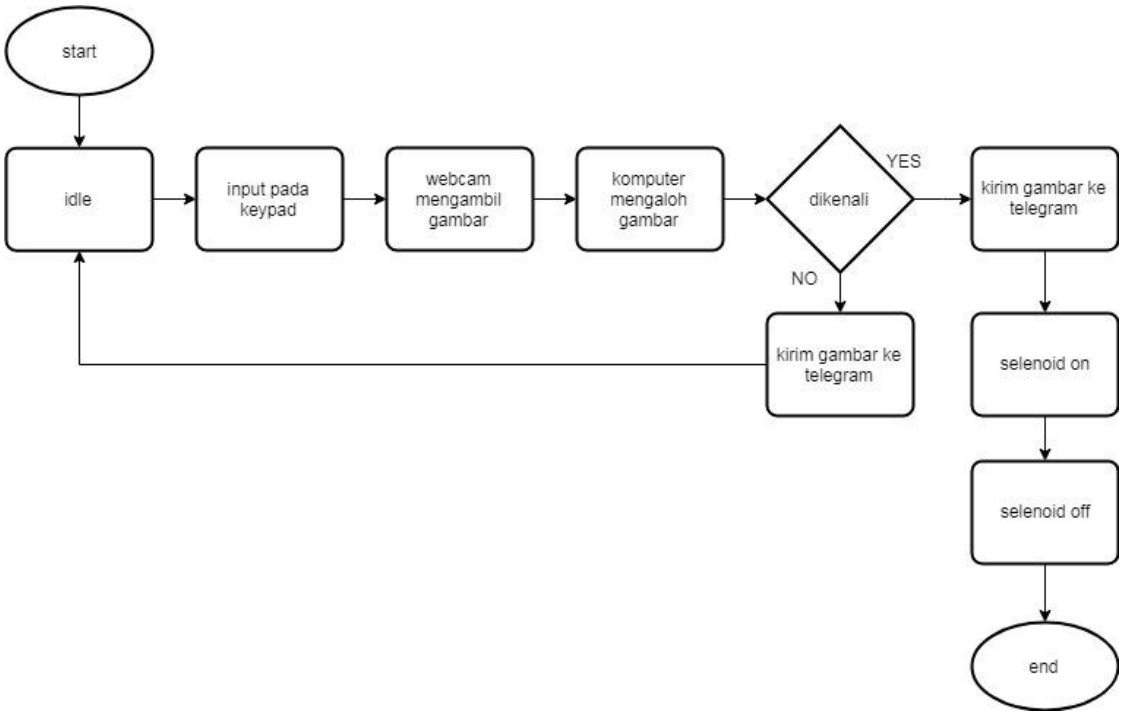
3.2. Miniatur pintu

Perancangan dan pembuatan miniatur pintu ini hanya membuat bagian pintu tanpa membuat kondisi satu ruangan. Mulai dari kerangka penyangga hingga keadaan pintu. Miniatur dapat dilihat pada gambar 5.



Gambar 5. a.tampak depan b.tampak belakang

3.3. Flowchart system



Gambar 6. Flowchart Sistem

Berdasarkan gambar 6 maka dapat dijabarkan bahwa flowchart system sebagai berikut idle adalah keadaan dimana system tidak melakukan tindakan apapun. Kemudian user memberikan input pada

keyboar. Kemudai webcam akan megambil gambar citra yang berada di depan kamera. Yang kemudian citra yang didapatkan oleh webcam akan diteruskan kepada kamputer. Kemputer kemudian menjalankan program face detection untuk mendeteksi wajah, serta menjalankan program face recognition untuk membedakan gambar wajah yang didapatkan, yang kemudian akan dicocokan sesuai dengan dataset yang telah dibuat sebelumnya. Bila citra wajah yang didapatkan sesuai dengan dataset (dikenali) maka, mengirimkan gambar kepada aplikasi telegram, kemudian selenoid terbuka selama 5 detik, kemudian selenoid terkunci kembali. Dan apabila citra wajah tidak sesuai dengan dataset maka sistem akan mengirimkan gambar kepada aplikasi telegram dan kemudian kembali pada posisi idle.

4. HASIL PENGUJIAN

Dari uji coba yang telah dilakukan, didapatkan hasil dan data sebagai berikut:

- System dapat mengirimkan notifikasi pada aplikasi telegram, baik untuk user yang terdaftar pada dataset ataupun user yang tidak terdaftar pada dataset.

Gambar 7. hasil notifikasi pada aplikasi telegram

- System dapat mengambil gambar wajah subjek dan menyimpanya kedalam dataset dengan baik.

Gambar 8. Contoh gambar pada data set

Tabel I

DATA WAKTU HASIL UJI COBA DALAM SATUAN DETIK

ID	DATASET (dtk)	TRAIN (dtk)
1	25.95	10.53
2	30.40	21.05
3	22.32	30.51

- Dari table I diatas dapat disimpulkan bahwa rata rata waktu yang dibutuhkan system untuk mengambil 100 gambar subjek, untuk disimpan menjadi dataset adalah:

$$\frac{25.95 + 30.40 + 22.32}{3} = 26{,}22$$

Dengan demikian dapat disimpulkan bahwa waktu yang dibutuhkan system untuk mengambil 1 gambar subjek untuk dataset adalah $\frac{26.22}{100} = 0.26$ atau setara dengan ±3 gambar setiap 1 detik. Dapat dilihat pula waktu train yang dibutuhkan oleh system untuk mentrain gambar subjek padadataset terus bertambah hal ini dikarenakan jumlah data set yang bertambah setiap kali system meregistrasi atau menambahkan dataset baru kedalam dataset.

Tabel II

DATA HASIL UJI COBA PENGENALAN WAJAH

ID	MENGENALI
1	YA
2	YA
3	YA

- Uji pengenalan wajah dilakukan terhadap masing masing subjek secara bergantian, subjek menghadap kamera dengan jarak yang ± sama dengan saat pengambilan gambar untuk dataset, subjek tidak bergerak dan dengan kondisi cahaya yang memadai bagi webcam untuk mendapatkan citra wajah. Dapat dilihat pada table 2 bahwa system dapat mengenali wajah pengguna sesuai dengan wajah yang telah disimpan pada dataset.

Tabel III

DATA HASIL UJI COBA MEMBEDAKAN USER TERDAFTAR DENGAN TIDAK TERDAFTAR

UNKNOWN	BISA MEMBEDAKAN
1	YA
2	YA

- Uji coba membedakan user terdaftar dengan user tidak terdaftar dilakukan dengan cara yang sama seperti pada uji pengenalan wajah, hanya saja yang membedakan adalah wajah subjek adalah wajah yang tidak didaftarkan pada dataset (unknown). Hasilnya sistem dapat membedakan dengan baik user yang sudah terdaftar dengan yang tidak terdaftar.

Tabel IV

DATA HASIL UJI COBA NILAI CONFIDENT

USER	NILAI CONFIDENT
TERDAFTAR	70,26& - 80,76%
TIDK TERDFTAR	55,5% - 66,6%

- Uji coba nilai confident dilakukan untuk dapat melihat nilai batas confident bagi user yang terdaftar pada dataset dengan user yang tidak terdaftar pada dataset agar dapat menentukan nilai confident bagi user yang terdaftar pada data set dan juga user yang tidak terdaftar pada dataset. Pada tabel IV dapat dilihat bahwa berdasarkan hasil ujicoba bahwa nilai confident terendah bagi user terdaftar pada dataset adalah 70,26% dan nilai tertingginya adalah 80,76% sedangkan, nilai confident terendah bagi user tidak terdaftar pada dataset adalah 55,5% dan nilai tertingginya adalah 66,6%. Oleh sebab itu dapat dikatakan bahwa 67% - 70% adalah nilai tengah confident bagi user terdaftar pada dataset dan user tidak terdaftar pada dataset. Dimana bila nilai confident lebih rendah dari 67% dianggap tidak terdaftar (unknown) dan bila diatas 70% dianggap user terdaftar.

Tabel V
DATA HASIL UJI COBA MEMBUKA PINTU OLEH UNKNOWN

UNKNOWN	BERHASIL TERBUKA/TIDAK
1	TIDAK
1	TIDAK
1	TIDAK
1	TIDAK
1	TIDAK
2	TIDAK
2	TIDAK
2	TIDAK
2	TIDAK
2	TIDAK

- Tabel V adalah hasil uji coba membuka pintu oleh user unknown. Dilakukan dengan cara 2 user unknown mencoba membuka pintu dengan masing masing user unknown mencoba membuka sebanyak 5 kali.

Tabel VI
DATA HASIL UJI COBA MEMBUKA PINTU OLEH USER TERDAFTAR

ID USER	BERHASIL TERBUKA/TIDAK
1	BERHASIL TERBUKA
1	BERHASIL TERBUKA
1	BERHASIL TERBUKA
1	BERHASIL TERBUKA
1	BERHASIL TERBUKA
2	BERHASIL TERBUKA
2	BERHASIL TERBUKA
2	BERHASIL TERBUKA
2	BERHASIL TERBUKA
2	BERHASIL TERBUKA
3	BERHASIL TERBUKA
3	BERHASIL TERBUKA
3	BERHASIL TERBUKA
3	BERHASIL TERBUKA
3	BERHASIL TERBUKA

- Tabel VI adalah hasil uji coba membuka pintu oleh user yang telah didaftarkan pada dataset (user terdaftar). Uji coba dilakukan dengan cara 3 user terdaftar mencoba membuka pintu dengan masing masing user mencoba sebanyak 5 kali.

5. Kesimpulan dan Saran

5.1. Kesimpulan

Dari hasil pengujian yang dilakukan maka dapat disimpulkan bahwa sistem dapat bekerja dengan baik bila dikarenakan akurasi yang cukup tinggi selama kondisi ideal pada batasan masalah terpenuhi. Kemudian sistem dapat mengkategorikan user dengan nilai confident lebih rendah dari 67% adalah user unknown sedangkan user dengan nilai confident diatas 70% sebagai user terdaftar pada dataset, sehingga sistem akan membukakan kunci selenoid untuk memberikan akses.

5.2. Saran

Adapun saran untuk kedepannya adalah sebagai berikut:

Pengembangan dari penelitian ini yaitu dengan mencoba untuk menggunakan algoritma face recognision yang lebih ringan agar dapat diproses menggunakan raspberry atau dengan menggunakan microcontroler yang lebih powerfull dibandingkan dengan raspberry pi 2. Kemudian mencoba dengan menggunakan kamera high resolution untuk dapat menaikan nilai confident bagi yang terdaftar.

Daftar Pustaka

[1] Frank Ortmier and Matthias Trojan, " Biometric Authentication Through a Virtual Keyboard for Smartphone". International Journal of Computer Science Information Technology (IJCIST), Vol. 4 No. 5, October 2012.

[2] M.Daris Femilia and Dr.A.Anthony Irudhayaraj, " Biometric System ". 3rd International Conference on Electeonic Computer Technology april 8-10 2011, kanyakumari. India. 2011 IEEE.

[3] G. Sowjanya and S. Nagaraju, " Design and Implementation of Door Access and Security System Based on IoT ". 2016 Interntionl Conference on Inventive Computation Technologies (ICICT) aug 26-27 2016, Ciombatore, India. 2016 IEEE.

[4] Naser Abbas Hussein and Inas Al Mansoori," Smart Door System for Home Security Using Raspberry pi 3 ". 2017 International Conference on Computer and Application (ICCA) sept 6-7 2017, Doha, United Arab Emirates. 2017 IEEE.

[5] P. Viola and M. Jones, " Rapid Object Detection Using a Boosted Cascade of Simple Feature ". Proceedings of The 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. CVPR 2001, dec 8-14, Kauai, HI, USA, 2001 IEEE

[6] R. Lienhart and J. Maydt, " An Extended Set of Haar-like Features for Rapid Object Detection ", International Conference on Image Processing, sept 22-25 2002, Rochester, NY, USA. 2002 IEEE

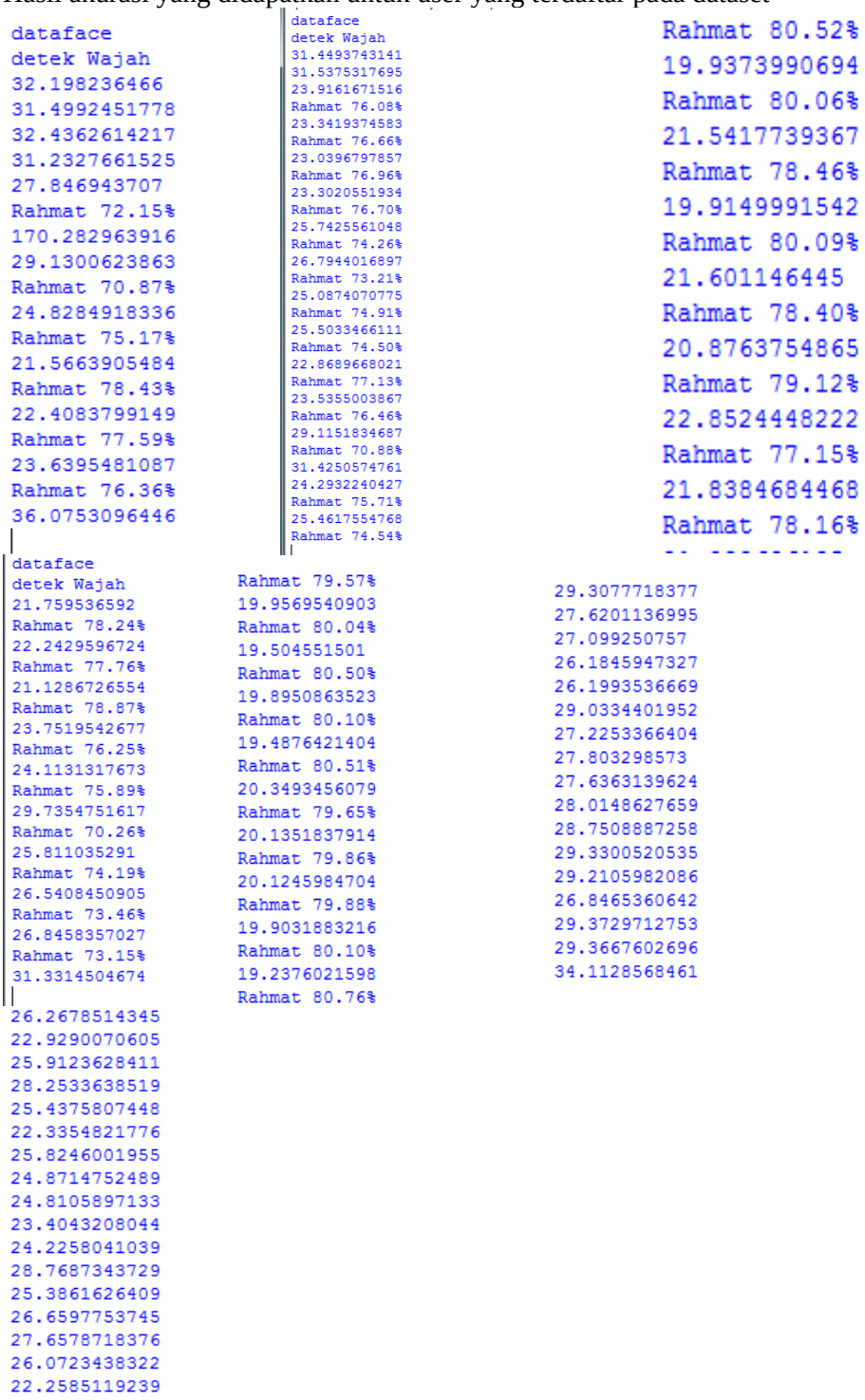
[7] L. O'Gorman, " Comparing Password, Tokens, and Biometrics for User Authentication ", Proceedings of The IEEE (Volume: 91, Issue 12, Dec 2013). IEEE

[8] Csaba Otti, " Comparasion of Biometric Identification Methods ", IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI), may 12-14 2016, Timisoara, Romania. 2016 IEEE

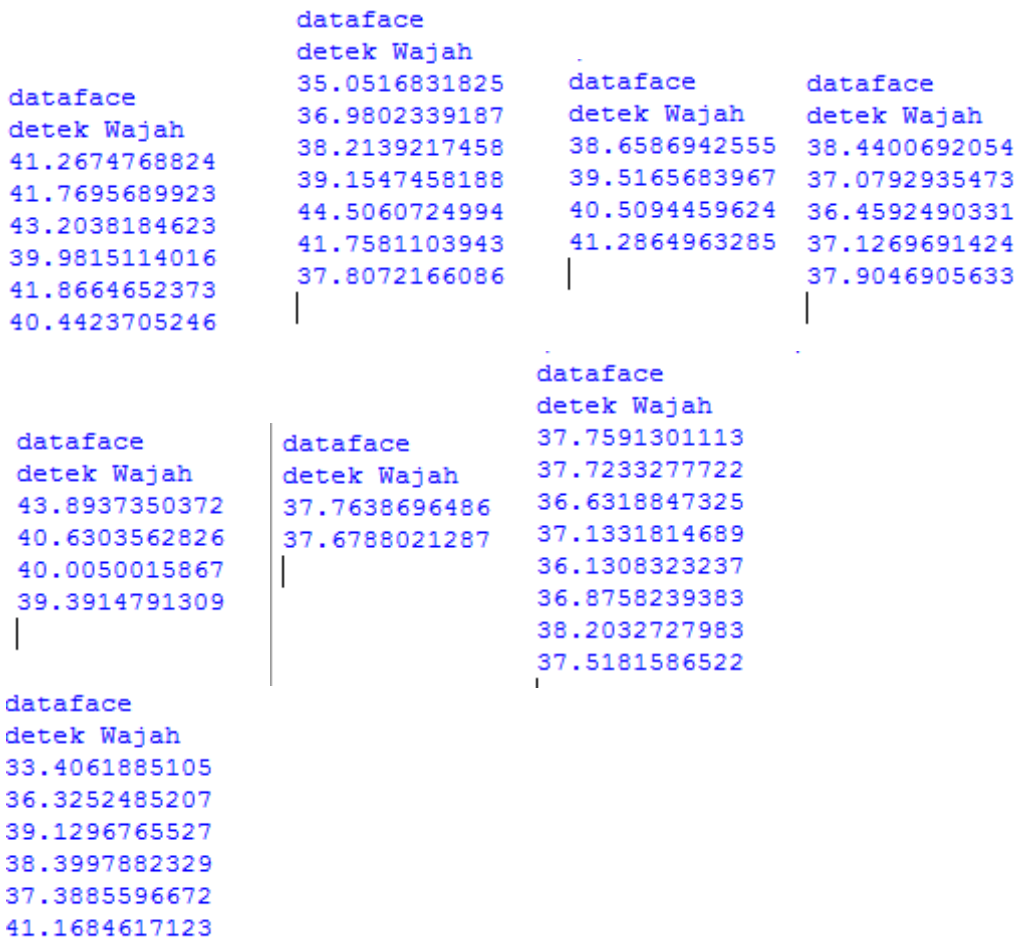
[9] S. Pankanti, R. M. Bolle, A. Jain, “Biometrics: The future of identification,”special issue of *Computer*, Vol. 33, no. 2, Feb. 2000.

LAMPIRAN

- Hasil akurasi yang didapatkan untuk user yang terdaftar pada dataset



- Hasil akurasi untuk user tidak diketahui (unknown)



- Waktu yang dibutuhkan oleh user terdaftar dari mulai memberikan input pada keyboard hinga selenoid terbuka

USER	WAKTU
1	13.88
	06.94
	03.08
	02.84
	06.81
2	20.54
	18.96
	04.46
	03.50
	05.42

- Tabel hasil uji coba unknown berhasil membuka kunci selenoid

PERCOBAAN KE	BERHASIL/TIDAK
1 (UNKNOWN 1)	TIDAK
2 (UNKNOWN 1)	TIDAK
3 (UNKNOWN 1)	TIDAK
4 (UNKNOWN 1)	TIDAK
5 (UNKNOWN 1)	TIDAK
6 (UNKNOWN 2)	TIDAK
7 (UNKNOWN 2)	TIDAK
8 (UNKNOWN 2)	TIDAK
9 (UNKNOWN 2)	TIDAK
10 (UNKNOWN 2)	TIDAK