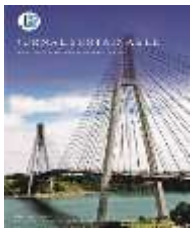


Jurnal Sustainable: Jurnal Hasil Penelitian dan Industri Terapan
Vol. 08, No. 02, hal. 48- 56, Oktober 2019
Jurnal Sustainable: Jurnal Hasil Penelitian Dan Industri Terapan
ISSN 2615-6334 (Online)
ISSN 2087-5347 (Print)

Smart Home Security menggunakan *Face Recognition* dengan Metode *Eigenface* Berbasis Raspberry Pi

Rudi Kurniawan[1,*],Antoni Zulius[2]
[1]Program Studi Ilmu Teknik, Fakultas Teknik, Universitas Sriwijaya
[1,2]Program Studi Rekayasa Sistem Komputer, Fakultas Komputer, Universitas Bina Insan Lubuklinggau
[*]Corresponding Author: rudi.kurniawan@univbinainsan.ac.id

Abstract—One of the biometric technologies that have been implemented in many security systems besides retinal recognition, fingerprint recognition and iris is facial recognition. On the hardware side itself, face recognition uses a camera to capture a person's face then compared to the data that has been stored in a particular database. There are several methods of facial recognition, namely neural networks, adaptive neuro fuzzy, and eigenface. Specifically in this study the method that will be explained is the eigenface method, and uses a web cam to capture images in real time. The advantage of this method is that the computation is very fast and simple compared to the use of methods that require a lot of learning, such as artificial network requirements. Broadly speaking, the process of this application is the camera to capture faces, then an RGB value is obtained. Using the initial processing, resize, RGB to Grayscale, and histogram equalization for light alignment. The eigenface method functions to calculate the eigenvalue, and the eigenvector that will be used as a feature in making recognition. From the experiments and tests carried out, the tool can recognize facial images with a success rate of up to 90% at a distance of 25 cm with an average success of 72.5%. This proves this tool is quite good in face recognition.
Keywords—*Image Processing, Raspberry Pi, Face Recognition, Grayscale*.

Intisari—Salah satu teknologi biometrik yang telah banyak diimplementasikan dalam sistem security selain pengenalan retina, pengenalan sidik jari dan iris mata adalah pengenalan wajah (*Face Recognition*). Dalam sisi perangkat kerasnya sendiri pengenalan wajah menggunakan sebuah kamera untuk menangkap wajah seseorang kemudian dibandingkan dengan wajah sebelumnya yang telah disimpan di dalam database tertentu. Beberapa metode pengenalan wajah yaitu *neural network*, *neuro fuzzy* adaptif, dan *eigenface*. Secara khusus dalam penelitian ini metode yang akan dijelaskan adalah metode *eigenface*, dan menggunakan *web cam* untuk menangkap gambar secara *real time*. Kelebihan dari metode ini adalah dalam hal komputasinya yang sangat cepat dan sederhana dibandingkan dengan penggunaan metode yang memerlukan banyak pembelajaran seperti jaringan syarat tiruan. Secara garis besar proses dari aplikasi ini adalah kamera melakukan *capture* pada wajah, kemudian didapat sebuah nilai RGB. Dengan menggunakan pemrosesan awal, dilakukan *resize*, RGB ke *Grayscale*, dan histogram equalisasi untuk perataan cahaya. Metode *eigenface* berfungsi untuk menghitung *eigenvalue*, dan *eigenvector* yang akan digunakan sebagai fitur dalam melakukan pengenalan. Dari percobaan dan pengujian yang dilakukan, alat dapat mengenali citra wajah dengan tingkat keberhasilan sampai 90% pada jarak 25 cm dengan rata-rata keberhasilan sebesar 72.5 %. Hal ini membuktikan alat ini cukup baik dalam pengenalan wajah.
Kata kunci—*Pengolahan citra, Raspberry Pi, Face Recognition, Grayscale*.

ISSN 2615-6334 (Online)
ISSN 2087-5347 (Print)

I. PENDAHULUAN

Kejahatan atau kriminalitas merupakan perbuatan seseorang yang dapat diancam hukuman penjara berdasarkan KUHP atau undang undang serta peraturan lainnya yang berlaku di Indonesia. Sistem keamanan yang ada selama ini masih kurang sempurna, hal itu bisa dilihat dari banyaknya tingkat kejahatan yang terjadi baik ditempat umum maupun perumahan semakin berkembang khususnya tindak kejahatan pencurian dan perampokan.

Kunci memegang peranan yang sangat penting dalam sistem keamanan. Pada saat ini banyak pencuri yang berhasil memasuki rumah yang kosong, terutama pada saat hari raya atau libur panjang telah tiba**.** Sistem kunci pintu rumah yang ada sekarang ini sebagian besar masih menggunakan kunci mekanik konvensional**. N**ormalnya pemilik rumah tersebut hanya menggunakan gembok pagar atau rantai.

Berdasarkan dari kasus yang ada, maka harus dipikirkan sebuah sistem baru yang berfungsi untuk mencegah tindak pembobolan dan pencurian rumah karena lemahnya tingkat pengaman kunci atau gembok. Sehingga terciptalah gagasan inovasi sistem *smart home security* menggunakan *face recognition* dengan metode *eigenface* berbasis *Raspberry Pi,* tentunya memiliki keamanan yang lebih baik dibandingkan pengaman kunci atau gembok. Dapat dikatakan bahwa sistem ini adalah sebuah kunci elektronik yang otomatis. Sistem ini diharapkan dapat menanggulangi terjadinya tindak pencurian pada rumah-rumah yang sering ditinggalkan oleh penghuninya.

Beberapa penelitian yang sudah dilakukan yang berkaitan dengan keamanan rumah mengunakan pengenalan wajah antara lain dengan judul "*Face Recognition* Untuk Sistem Pengaman Rumah Menggunakan Metode HOG dan kNN Berbasis *Embedded*" membahas tentang bagaimana mengimplementasikan alat keamanan pintu dengan pola pengenalan wajah menggunakan metode HOG dan kNN. Pada alat yang dirancang menggunakan unit proses berbasis modul Raspberry Pi. Perbedaan mendasar dengan topik yang peneliti bahas adalah pada metode yang digunakan, yaitu peneliti menggunakan metode HOG dan kNN. Melalui hasil pengujian, didapat akurasi sebesar 87.5 % [1].

Sebuah penelitian membahas tentang bagaimana membangun sebuah prototipe keamanan rumah dengan pola pengenalan wajah. Pada alat yang dirancang, unit proses yang digunakan berbasis modul Raspberry Pi. Perbedaan mendasar dengan topik yang peneliti bahas adalah pada metode yang digunakan, yaitu peneliti menggunakan gabungan metode pengenalan wajah antara lain metode *eigenfaces, fisherfaces* dan *Local Binary Patterns Histogram* (LBPH). Peneliti tidak mencantumkan aspek akurasi dalam penelitiannya. Sehingga tidak didapati informasi akurasi *prototype* sistem yang dirancang [2].

Penelitian lain membahas tentang bagaimana mengimplementasikan alat keamanan pintu dengan pola pengenalan wajah menggunakan metode *fisherface*. Pada alat yang dirancang tersebut menggunakan unit proses berbasis modul mikrokontroler arduino uno R3. Perbedaan mendasar dengan topik yang peneliti bahas adalah pada unit proses dan metode yang digunakan, yaitu peneliti menggunakan unit proses mini komputer Raspberry Pi dan metode *eigenface*. Melalui hasil pengujian, didapat akurasi sebesar 80 % [3].

Sebuah penelitian mengimplementasi-kan alat keamanan rumah dengan pola pengenalan wajah menggunakan metode *Principal Component Analysis*. Pada alat yang dirancang tersebut menggunakan unit proses berbasis modul mikrokontroler arduino uno R3. Perbedaan mendasar dengan topik yang peneliti bahas adalah pada metode yang digunakan, yaitu peneliti menggunakan metode *Principal Component Analysis*. Melalui hasil pengujian, didapat akurasi sebesar 88 % [4].

Penelitian dengan judul "Perancangan dan Implementasi Keamanan Pintu Berbasis Pengenalan Wajah Dengan Metode *Eigenface*" membahas tentang bagaimana mengimplementasikan keamanan pintu dengan pola pengenalan wajah menggunakan metode *Eigenface*. Pada alat yang dirancang tersebut menggunakan unit proses berbasis modul Raspberry Pi. Perbedaan mendasar dengan topik yang peneliti bahas adalah pada unit output yang digunakan, yaitu menggunakan kendali motor servo untuk menggerakkan kunci, sedangkan peneliti menggunakan *solenoid door lock* yang menggunakan kunci otomatis berdasarkan prinsip elektromagnetik. Melalui hasil pengujian, didapat akurasi sebesar 90 % [5].

Penelitian yang berjudul "Penerapan Algoritma *Gabor Wavelet* Sebagai Keamanan Rumah Dengan Mengidentifikasi Wajah Berbasis *Webcam*" membahas tentang bagaimana menerapkan algoritma *Gabor Wavelet* dalam pengenalan wajahnya. Untuk unit *input* digunakan *webcam* dan tingkat akurasi yang dicapai mencapai 90 % [6]

Penelitian dengan judul "Penerapan *Face Recognition* dengan Metode *Eigenface* pada *Intelligent Car Security*" membahas tentang bagaimana mengimplementasikan keamanan pintu Mobil dengan pola pengenalan wajah menggunakan metode *Eigenface*. Pada alat yang dirancang tersebut menggunakan unit proses berbasis modul Mikrokontroler Arduino Uno. Perbedaan mendasar dengan topik yang peneliti bahas adalah pada unit output yang digunakan, yaitu objek yang dijadikan keamanan pintu adalah pada pintu mobil, sedangkan peneliti menggunakan pintu rumah yang didasari pada prinsip *smart home security*. Peneliti dalam penelitian ini tidak mencantumkan akurasi dari pola pengenalan wajah yang dilakukan [7].

Penelitian dengan judul "Rancang Bangun Sistem Biometrik Pengenalan Wajah Menggunakan *Principal Component Analysis*" menjelaskan bagaimana merancang sistem keamanan pintu secara sistem biometrik pengenalan wajah menggunakan *Principal Component Analysis* (PCA). Secara umum terdapat dua metode yang digunakan, yaitu metode *Haar Cascade* untuk proses deteksi wajah dan metode PCA (*eigenface*) untuk proses pengenalan wajah. Pengujian dilakukan pada jarak 30 cm dengan tingkat akurasi sebesar 83,33 % [8].

Penelitian dengan judul "*Face Recognition Using Eigenface Approach*" menjelaskan bagaimana melakukan pengenalan wajah melalui pendekatan metode *eigenface*. Algoritma yang digunakan dalam pengenalan wajah menggunakan *Principal Component Analysis* (PCA) yang mengacu pada metode *eigenface*. Pada penelitian ini menjelaskan pendekatan (metode) *eigenface* merupakan pendekatan PCA paling mudah dan efektif yang digunakan dalam pengenalan wajah. Metode ini mentransformasikan wajah ke dalam bentuk set kecil karakter penting [9].

Atas dasar penelitian sebelumya, peneliti melakukan penelitian *smart home security* dengan menggunakan metode *eigenface*. Dalam sistem ini, sistem bekerja dengan mengekstraksi wajah yang telah dideteksi menggunakan metode *Eigenface*, mengaplikasikan *face recognition* dengan metode *eigenfaces* ebagai sarana pengenalan wajah antara pemilik rumah dan pencuri secara *real-time*. Pemilik rumah dan pencuri dimasukkan ke dalam *class* yang berbeda sehingga akan lebih mudah dalam pengenalan. Diharapkan dengan aplikasi ini dapat membuat suatu sistem yang handal dan aman. Selanjutnya sistem akan membuka *solenoid door lock* dan menyalakan LED berwarna hijau jika citra wajah baru yang dideteksi dikenali oleh sistem sebagai penghuni rumah. Namun apabila sistem tidak mengenali citra wajah baru tersebut, maka *solenoid door lock* akan tetap terkunci, LED akan menyala merah, *buzzer* akan berbunyi, dan sms notifikasi akan dikirim ke nomor pemilik rumah.

ISSN 2615-6334 (Online)
ISSN 2087-5347 (Print)

II. METODOLOGI PENELITIAN

A. Eigenface

Metode *Eigenface* ditemukan oleh Matthew A Turk dan Alex P. Pentland dari MIT pada tahun 1991 [10]. Tujuan utama dari metode *eigenface* adalah untuk mendapatkan karakteristik citra dengan menggunakan karakteristik wajah, tetapi dengan menggunakan rumus transformasi matematika.

1) Tahapan Perhitungan Eigenface

Menyiapkan *database* dengan membuat suatu himpunan *X* yang terdiri dari seluruh *training image*.

$$X = [x_1, x_2, ..., x_n] \quad (1)$$

Mencari nilai *mean* gambar (μ)

$$\mu = \frac{1}{n}\sum_{i=n}^{n} x_i \quad (2)$$

Menghitung matriks *covarians* (S) dimana (x_i - μ) adalah selisih antara *training image* dengan mean dari wajah.

$$s = \frac{1}{n}\sum_{i=1}^{n}(x_i - u)(x_i - u)^T \quad (3)$$

Menghitung eigenvalues (λt) dan eigenvector v_i dari S.

$$Sv_i = \lambda_i v_i \quad (4)$$

Mengurutkan *eigen vector* secara menurun dengan *eigenvalue*. K *principal componen* adalah *eigen vector* yang sesuai dengan *eigenvalue* nilai K terbesar. Memproyeksikan semua sampel pelatihan ke sub ruang PCA.

$$Y = WT\ (x - \mu) \quad (5)$$

Dimana $W = (v_1, v_2, v_3, v_4, v_5, ... , v_k)$. Memproyeksikan citra uji ke dalam subruang PCA.

$$X = Wy + \mu \quad (6)$$

Menemukan nilai terdekat antara gambar pelatihan yang diproyeksikan dan gambar uji yang diproyeksikan.

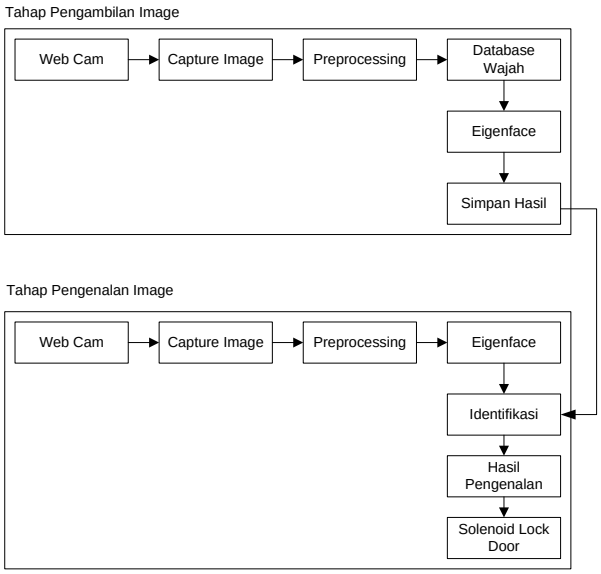
2) Vektor

Melalui persamaan (4), vektor akan digunakan karena jika menggunakan matriks perhitungannya akan sangat besar dan lambat. Menggunakan vektor menyebabkan ukuran gambar relatif kecil jika dibandingkan dengan menggunakan Bitmap. Dengan menggunakan vektor, perhitungan akan sangat berkurang dari urutan jumlah *pixel* dalam gambar dengan urutan jumlah gambar dalam training set. Dalam prakteknya, training set, training set gambar wajah akan sangat relatif kecil dan perhitungan menjadi sangat mudah dikelola.

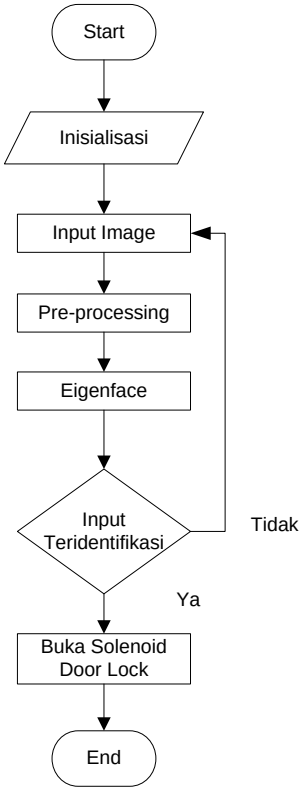
B. Cara Kerja Sistem

Didalam sistem pengenalan wajah ini dibagi menjadi dua tahap, yaitu tahap pengambilan gambar dan tahap pengenalan. Didalam tahap pengambilan ini, *image* yang diambil akan dijadikan *database* lalu akan disimpan hasilnya. Setiap *image* berukuran (640x480) pixel. Pada *pre-processing*, sendiri ada empat tahapan antara lain : *cropping*, *resize*, *grayscale*, dan *histogram equalization*. Setelah melalui proses itu lalu *image* akan melalui tahap *eigenface* yang proses matematikanya telah dibahas sebelumnya.

Kemudian tahapan yang kedua, merupakan tahapan pengenalan, kedua matriks dari *image* dibandingkan. *Threshold* yang merupakan batas kemiripan yang sudah dilakukan sebelumnya. Jika *image* tersebut melampaui batas *threshold* yang sudah ditentukan sebelumnya maka *image* tersebut tidak akan dikenali. Gambar 1 menyajikan diagram blok sistem dan gambar 2 menyajikan diagram alir sistem pengenalan wajah.



Gambar 1. Blok Diagram Sistem



Gambar 2. Diagram Alir Sistem

C. Perancangan Sistem

1) Spesifikasi Alat

1. Kamera Web Cam Logitech C270
   Berfungsi sebagai media untuk meng-*capture* wajah.
2. Mini PC (Raspberry Pi)
   Sebagai unit proses sistem
3. *Solenoid Lock Door*
   Sebagai pengunci pintu
4. *Relay*
   Sebagai Saklar penggerak solenoid
5. *Speaker*
   Berfungsi sebagai bel rumah

2) Perancangan Mekanik

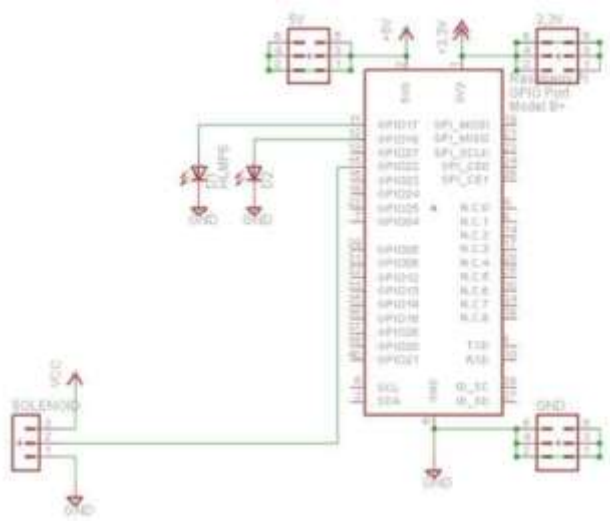
Pada perancangan sistem ini dirancang sebuah mekanik atau *prototype* seperti rumah pribadi dimana untuk pengambilan wajah manusia yang akan diidentifikasi menggunakan *web camera*. Format pengambilan gambar berupa JPEG dengan ukuran 640x480 pixel. *Design* keamanan pintu rumah ini akan diterapkan sebagai *output* dari pengambilan citra wajah manusia yang memenuhi hak akses pada pintu masuk rumah. Gambar 3 menyajikan *prototype design* pintu rumah.

Gambar 3. Design Tampak Depan

3) Perancangan Elektronik

Perancangan modul Raspberry Pi ini berfungsi untuk mengontrol semua kinerja sistem mulai dari pemrosesan pengolahan citra, menjalankan modul *solenoid*, dan memberikan *output* indikator LED1 dan LED2. Gambar 4 menyajikan rangkaian elektronik keseluruhan.

ISSN 2615-6334 (Online)
ISSN 2087-5347 (Print)



Gambar 4. Rangkaian Sistem Keseluruhan

Tabel 1 dibawah ini menyajikan konfigurasi pin pada Raspberry Pi yang digunakan untuk konfigurasi GPIO.

Tabel 1. Konfigurasi GPIO pada Raspberry Pi

Pin	Nama	Keterangan
11	GPIO 17	Indikator Pintu Tertutup
12	GPIO 18	Indikator Pintu Terbuka
15	GPIO 19	Relay Untuk Solenoid

III. PENGUJIAN DAN PEMBAHASAN

A. Pengujian

Pengujian merupakan salah satu langkah penting yang harus dilakukan untuk mengetahui apakah sistem yang dibuat telah sesuai dengan yang direncanakan, hal itu dapat dilihat dari hasil yang diperoleh dalam pengujian sistem. Selain untuk mengetahui apakah sistem sudah bekerja dengan baik sesuai dengan yang diharapkan, pengujian juga bertujuan untuk mengetahui kelebihan dan kekurangan dari sistem yang dibuat. Sebelum melakukan pengukuran, maka dipersiapkan terlebih dahulu alat-alat yang diperlukan dalam melakukan pengukuran.

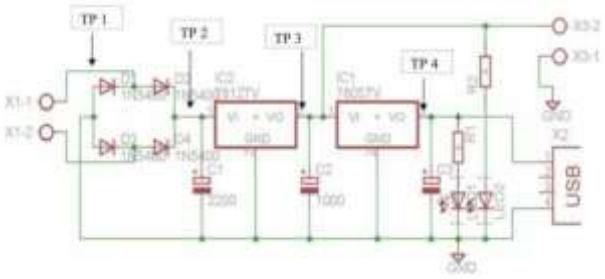
Dimulai dari rangkaian *power supply* sebagai catu daya, PIR sebagai *sensor object*, *camera* sebagai media untuk *Capture* atau menangkap gambar dan rangkaian *driver solenoid* untuk mengaktifkan solenoid. Setiap unit atau bagian di uji berdasarkan *input* dan *output* yang diberikan apakah sesuai dengan yang diharapkan atau tidak, jika tidak sesuai maka kemungkinan akan mengganggu kinerja alat nantinya.

Berikut langkah-langkah dan pokok pembahasan yang akan di lakukan dalampangujian sebagai berikut :

1. Pengujian Catu Daya
2. Pengujian *Driver Solenoid*
3. Pengujian Tingkat Akurasi Data

1) Pengujian Catu Daya

Pengujian rangkaian catu daya ini dilakukan dengan cara mengukur nilai tegangan keluaran dari *power supply* guna mengetahui tegangan keluaran yang dihasilkan apakah nilai tegangan keluaran telah sesuai dengan keinginan yang kita butuhkan untuk men-*supply* tegangan ke semua rangkaian lainnya. Sesuai dengan *schematic* rangkaian *power supply* yang dibuat menghasilkan tegangan keluaran 5Vdan 12V DC. Gambar 5 berikut menyajikan titik pengukuran yang dilakukan pada rangkaian *power supply* :



Gambar 5. Titik Pengukuran Tegangan Catu Daya

Tabel 2 berikut menyajikan hasil pengukuran catu daya dengan menggunakan multimeter.

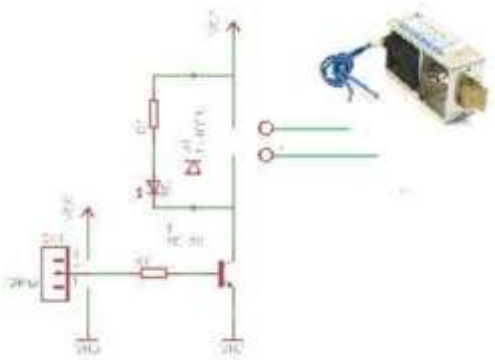
Tabel 2. Titik Pengukuran Catu Dayu

Titik Ukur	Hasil Ukur	Ket
TP.1	12 Vac	Input 12 V Trafo
TP.2	16 Vdc	Output Dioda Brigde
TP.3	12 Vdc	Output Regulator 7812
TP.4	5 Vdc	Output Regulator 7805

2) Pengujian Driver Solenoid

Pengujian *driver solenoid* dilakukan untuk mengetahui apakah *driver* dapat bekerja sebagaimana mestinya sesuai dengan yang

diinginkan. Gambar 6 berikut menyajikan titik-titik pengujian *driver solenoid*.



Gambar 6. Titik Pengukuran Driver Solenoid

Tabel 3 berikut menyajikan hasil pengukuran dengan menggunakan multimeter.

Tabel 3. Titik Pengukuran Catu Dayu

TP 1	TP 2 (V_{BE})	TP 3 (V_{CE})	TP 4	Kondisi
5 V	0.75 V	0.04 V	12 V	On
0 V	0 V	4.8 V	0 V	Off

Dari data pengukuran rangkaian *driver solenoid* yang ada pada tabel diatas, dapat dianalisakan bahwa untuk titik pengukuran 1 merupakan tegangan yang didapatkan dari sumber yaitu sebesar 5 Volt dimana pada kondisi ini transistor berada pada posisi saturasi atau *on* yang dapat bekerja karena menghasilkan tegangan *basis* (V_{BE}) sebesar 0,75 Volt. Adapun syarat picu dari transistor untuk tersebut untuk menarik kontak menjadi aktif yaitu minimal harus memiliki tegangan sebesar 0,7 Volt.

Sedangkan pada saat transistor tidak diberi tegangan sumber atau Vin = 0 Volt maka transistor berada pada posisi *cut off* atau pada kondisi tidak aktif dikarenakan tegangan basis (V_{BE}) yang dihasilkan mempunyai nilai tegangan sebesar 0 Volt atau kurang dari syarat picu yaitu 0,7 Volt.

3) Pengujian Tingkat Akurasi Data

Pada pengujian di tahap ini, dilakukan dengan cara menguji pendeteksian kamera dalam *range* jarak sejauh 25 cm dari posisi kamera menuju wajah target. Dalam pengujian sebanyak 10 kali, kamera dapat mendeteksi wajah dengan baik sebanyak 9 kali pendeteksian dengan 1 kali gagal dalam mendeteksi. Tabel 4 menyajikan data hasil pengujian dengan jarak 25 cm

Tabel 4. Pengujian Jarak 25 cm

Jarak	Jumlah Percobaan	Hasil Pembacaan	
		Terdeteksi	Tidak
25 cm	1	Ya	Tidak
	2	Ya	
	3	Ya	
	4	Ya	
	5		
	6	Ya	
	7	Ya	
	8	Ya	
	9	Ya	
	10	Ya	

Pada pengujian di tahap ini, dilakukan dengan cara menguji pendeteksian kamera dalam *range* jarak sejauh 25 cm dari posisi kamera menuju wajah target. Dalam pengujian sebanyak 10 kali, kamera dapat mendeteksi wajah dengan baik sebanyak 9 kali pendeteksian dengan 1 kali gagal dalam mendeteksi.

Sehingga diperoleh tingkat keberhasilan seperti berikut :

$$Tingkat\ keberhasilan = \frac{terdeteksi}{jumlah\ percobaan} \times 100\%$$

$$= \frac{9}{10}\ x\ 100\ \%$$

$$= 90\ \%$$

Tabel 5 menyajikan data hasil pengujian dengan jarak 50 cm.

Tabel 5. Pengujian Jarak 50 cm

Jarak	Jumlah Percobaan	Hasil Pembacaan	
		Terdeteksi	Tidak
50 cm	1		Tidak
	2	Ya	
	3		Tidak
	4		Tidak
	5	Ya	
	6	Ya	
	7	Ya	
	8	Ya	

ISSN 2615-6334 (Online)
ISSN 2087-5347 (Print)

	9	Ya
	10	Ya

Pada tahap pengujian dengan jarak 50 cm ini, terjadi penurunan keefektifan dari pembacaan kamera. Adapun hasil pembacaannya sebagai berikut :

$$Tingkat\ keberhasilan = \frac{terdeteksi}{jumlah\ percobaan} \times 100\%$$

$$= \frac{7}{10}\ x\ 100\ \%$$

$$= 70\ \%$$

Tabel 6 menyajikan data hasil pengujian dengan jarak 75 cm.

Tabel 6. Pengujian Jarak 75 cm

Jarak	Jumlah Percobaan	Hasil Pembacaan	
		Terdeteksi	Tidak
76 cm	1	Ya	
	2		Tidak
	3		Tidak
	4	Ya	
	5	Ya	
	6	Ya	
	7	Ya	
	8	Ya	
	9	Ya	
	10	Ya	

Pada tahap pengujian dengan jarak 75 cm ini, terjadi penurunan keefektifan dari pembacaan kamera. Adapun hasil pembacaannya sebagai berikut:

$$Tingkat\ keberhasilan = \frac{terdeteksi}{jumlah\ percobaan} \times 100\%$$

$$= \frac{8}{10}\ x\ 100\ \%$$

$$= 80\ \%$$

Tabel 7 menyajikan data hasil pengujian dengan jarak 100 cm.

Tabel 7. Pengujian Jarak 100 cm

Jarak	Jumlah Percobaan	Hasil Pembacaan	
		Terdeteksi	Tidak
100 cm	1		Tidak
	2	Ya	
	3	Ya	
	4	Ya	
	5		Tidak
	6		Tidak
	7	Ya	
	8	Ya	
	9		Tidak
	10		Tidak

Pada tahap pengujian dengan jarak 75 cm ini, terjadi penurunan keefektifan dari pembacaan kamera. Adapun hasil pembacaannya sebagai berikut:

$$Tingkat\ keberhasilan = \frac{terdeteksi}{jumlah\ percobaan} \times 100\%$$

$$= \frac{5}{10}\ x\ 100\ \%$$

$$= 50\ \%$$

Berdasarkan pada perhitungan diatas, dapat dipersentasikan tingkat keberhasilan dan tingkat kegagalan dalam melakukan pendeteksian wajah menggunakan kamera *webcam* yaitu sebagai berikut :

Tabel 8 menyajikan data tingkat keberhasilan hasil pendeteksian kamera.

Tabel 8. Tingkat Keberhasilan Keseluruhan

Pengujian	Pengujian		Persentase	
	Terdeteksi	Tidak Terdeteksi	Berhasil	Tidak Berhasil
Tahap 1	9	1	90 %	10 %
Tahap 2	7	3	70 %	30 %
Tahap 3	8	2	80 %	20 %
Tahap 4	5	5	50 %	50 %
Total	29	11	72, 5 %	27,5 %

IV. KESIMPULAN

Penggunaan metode *eigenface* dalam *smart home security* dengan *face recognition* menunjukkan hasil akurasi dengan rata-rata sebesar 72,5 %. dari hasil percobaan, jarak antara wajah yang akan dikenali dengan web cam sangat berpengaruh terhadap proses pendeteksian wajah dengan jarak efektif sejauh 25 cm dengan akurasi maksimum sebesar 90 %. Sistem berhasil melakukan pengenalan meskipun posisinya berbeda-beda, karena yang digunakan adalah nilai dari *eigenface* tiap citra wajah yang dibandingkan. Pengguanaan *class* untuk pengelompokan data pemilik rumah dan bukan pemilik rumah

sangat efektif digunakan dalam proses verifikasi antara pemilik atau pencuri. Tingkat keberhasilan pengenalan wajah sangat dipengaruhi oleh deteksi wajah, pemrosesan awal, dan penghitungan dengan PCA (*eigenface*) sebelumnya.

UCAPAN TERIMA KASIH

Ucapan terimakasih dari penulis kepada pihak yang telah memberikan dukungan dalam penulisan artikel ini antara lain: Ketua Program Studi Ilmu Teknik Universitas Sriwijaya Palembang, Dekan Fakultas Teknik, Ketua LPPM Universitas Sriwijaya Palembang, Ketua Program Studi Rekayasa Sistem Komputer Universitas Bina Insan Lubuklinggau, Ketua LPPM Universitas Bina Insan Lubuklinggau.

REFERENSI

[1] B. Septian Aditya Wijayanto, F. Utaminingrum, dan I. Arwani, "Face Recognition Untuk Sistem Keamanan Rumah Menggunakan Metode HOG dan kNN Berbasis *Embedded*," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer.*, vol. 3, no. 3, hlm. 2774–2781, Maret 2019.

[2] I. Nyoman Piarsa, K. Suar Wibawa, "Prototype Deteksi dan Pengenalan Wajah Pada Sistem Monitoring dan Kontrol Visual Keamanan Rumah," *Seminar Nasional Sains dan Teknologi (Senastek) IV*, , hlm. 1–7, 2017.

[3] B. Maryuni S, F. Eko Purnomo, dan M. Faiq Ilman Fahmi, "Sistem Keamanan Pintu Berbasis Pengenalan Wajah Menggunakan Metode *Fisherface*," *Jurnal Ilmiah Inovasi.*, vol. 17, no. 1, hlm. 43–48, April 2017.

[4] S. Monika, A. Rakhman, dan Lindawati, "Pengaman Rumah Dengan Sistem Face Recognition Secara Real TimeMenggunakan Metode Principal Component Analysis," *Prosiding SNATIF Ke-4*, ISBN:978-602-1180-50-1, hlm. 395–401, 2017.

[5] D. Indra Bramantio, E. Susanto, dan R. Nugraha, "Pengenalan dan Implementasi Keamanan Pintu Berbasis Pengenalan Wajah Dengan Metode Eigenface," *Jurnal Penelitian dan Pengembangan Telekomunikasi, Kendali, Komputer, Elektrik, dan Elektronika (Tetrika)*, vol. 1, No. 2, hlm. 111–114, Juli 2016.

[6] Setiawan A., "Penerapan Algoritma Gabor Wavelet Sebagai Keamanan Rumah Dengan Mengidentifikasi Wajah Berbasis Webcam" *Ekspora Informatika*, vol. 5 No. 2, hlm. 194–202, Maret 2016

[7] Sehman, "Penerapan *Face Recognition* Dengan Metode *Eigenface* Pada *Intelligent Car Securuty*," *Seminar Nasional "Inovasi dalam Desain dan Teknologi"*, ISSN : 2089-1121, hlm. 342–348, 2015.

[8] Nicco. dan Fahruzi I, "Rancang Bangun Sistem Biometrik Pengenalan Wajah Menggunakan *Principal Component Analysis*," *Jurnal Integrasi*, vol. 6, no. 1, ISSN: 2085-3858, hlm. 64-71, 2014.

[9] Slavkovic M. and Jevtic D, "Face Recognition Using Eigenface Approach," *Serbian Journal of Electrical Engineering*, Vo. 9 No. 1 February 2012 DOI: 10.2298/SJEE1201121S, hlm. 121-130, 2012.

[10] Matthew A. Turk and Alex P. Pentland, *Face Recognition Using Eigenface*, IEEE, 1991.