PERANCANGAN DAN IMPLEMENTASI PROTOTIPE SISTEM KEAMANAN RUMAH BERBASIS PENGENALAN WAJAH MENGGUNAKAN METODE FISHERFACE DENGAN PUSAT KENDALI TELEGRAM PADA RASPBERRY PI

(DESIGN AND IMPLEMENTATION OF HOME SECURITY PROTOTYPE SYSTEM BASED ON FACE RECOGNITION USING FISHERFACE METHOD WITH TELEGRAM CONTROL CENTER ON RASPBERRY PI)

Danish Ario Wirawan[1], Nur Ibrahim, S.T., M.T.[2], Ramdhan Nugraha, S.Pd., M.T.[3]
[1]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
[2,3]Fakultas Teknik Elektro, Universitas Telkom
[1]**danishaw@telkomuniversity.ac.id**, [2]**nuribrahim@telkomuniversity.co.id**, [3]**ramdhan@telkomuniversity.ac.id**

Abstrak

Salah satu sistem keamanan berbasis biometrik adalah pengenalan wajah yang mengidentifikasi berdasarkan perbedaan ciri wajah. Oleh karena itu, setiap orang mempunyai ciri wajah masing-masing yang dapat digunakan sebagai kata sandi. Melalui penelitian ini kunci rumah dapat dikelola dengan menggunakan sebuah sistem keamanan rumah berbasis pengenalan wajah. Prototipe ini memiliki 2 sistem yaitu sistem otomasi dan sistem keamanan. Pada sistem otomasi ini, aplikasi *Telegram* dapat mengontrol modul relay untuk mengontrol lampu dan kunci rumah. Sedangkan pada sistem keamanan dapat mengontrol modul relay berdasarkan wajah yang dikenali. Jika diluar penghuni rumah mencoba masuk, maka sistem akan memberikan peringatan kepada pemilik rumah melalui *telegram*. Pengenalan wajah menggunakan *OpenCV* yang berbasis *library open source* untuk *computer vision* dan menggunakan metode *Fisherface* untuk ekstraksi ciri serta metode klasifikasi yang memakai bahasa pemrogaman *Python*. Secara keseluruhan tingkat akurasi sistem pada penelitian ini mencapai 98,5%. Hasil yang didapatkan dari penelitian ini menunjukkan bahwa kondisi cahaya terang dengan ekspresi senyum memiliki tingkat performansi yang terbaik, pencapaian tingkat akurasi sebesar 100% keberhasilan dengan rata-rata nilai confidence 20,06547 dan 2.6883 detik untuk rata-rata waktu komputasi.

Kata kunci : ***Raspberry Pi, Face Recognition, OpenCV, Fisherface, Telegram***

Abstract

One of the biometric-based security systems is face recognition, based on differences in facial characteristics. Therefore everyone has their own characteristics that can be used as a password. Through this research, home locks can be managed using home security system based on facial recognition. This prototype has 2 systems, the automation system and the security system. In this automation system, Telegram applications can control relay modules to control lights and house key. The security system can control relay modules based on recognizable faces. If stranger trying to enter the house, the system will give a warning to the homeowner via telegram. Face recognition uses OpenCV based open source library for computer vision and uses the Fisherface method for extraction of features and classification methods that use the Python programming language. Overall the successful rate of the system reach 98.5%. The experiment of this research shows that bright light condition with smile expression gave the best result with 100% success with an average confidence value of 20.06547 and 2.6883 seconds for the average computing time.

Keywords: ***Raspberry Pi, Face Recognition, OpenCV, Fisherface, Telegram***

1. Pendahuluan [10 pts/Bold]

Dewasa ini, hampir semua orang menggunakan listrik sebagai energi utama dalam kehidupan sehari-hari. Ketergantungan terhadap energi listrik membuat orang terkadang lupa untuk mematikan alat – alat listrik yang tidak terpakai dalam waktu yang lama, sehingga mengakibatkan energi listrik terbuang percuma. Pada akhirnya, biaya yang harus dibayar setiap bulan menjadi tinggi. Otomasi menjadi solusi penting untuk mengatasi masalah tersebut.

Tugas akhir ini berfokus pada alat yang dapat menghidupkan atau mematikan peralatan listrik secara otomatis, dengan pengenalan wajah secara *real-time* menggunakan *raspberry pi* yang merupakan sebuah mini komputer dengan memanfaatkan fungsi *GPIO(General Purpose Input Output)* yang berisi pin – pin sebagai *interface* fisik antara *raspberry pi* dengan saklar yang bertugas menghidupkan atau mematikan lampu. Untuk pengenalan wajah menggunakan *OpenCV* sebagai *library* pengolahan citra yang di dalamnya terdapat algoritma *fisherface*.

2. Dasar Teori /Material dan Metodologi/perancangan

2.1 Internet of Things

Ada beberapa definisi dari Internet of Things, Casagras (Coordination and support action for global RFID-related activities and standardization) mendefinisikan Internet of Things sebagai sebuah infrastruktur jaringan global, yang menghubungkan benda-benda fisik dan virtual melalui eksploitasi data capture dan kemampuan komunikasi [1].

Cara kerja dari Internet of things cukup mudah. Setiap benda harus memiliki sebuah IP Address. IP Address adalah sebuah identitas dalam jaringan yang membuat benda tersebut bisa diperintahkan dari benda lain dalam jaringan yang sama. Selanjutnya, IP address dalam benda-benda tersebut akan dikoneksikan ke jaringan internet. Setelah sebuah benda memiliki IP address dan terkoneksi dengan internet, pada benda tersebut juga dipasang sebuah sensor. Sensor pada benda memungkinkan benda tersebut dapat mengolah informasi itu sendiri, bahkan berkomunikasi dengan benda-benda lain yang memiliki IP address dan terkoneksi dengan internet juga. Akan terjadi pertukaran informasi dalam komunikasi antara bendabenda tersebut. Setelah pengolahan informasi selesai, benda tersebut dapat bekerja dengan sendirinya, atau bahkan memerintahkan benda lain juga untuk ikut bekerja [2].

2.2 Face Recognition

Face Recognition atau pengenalan wajah adalah salah satu teknologi biometrik yang memungkinkan untuk memverifikasi wajah seseorang melalui sebuah gambar digital dengan mencocokkan tekstur lekuk wajah dengan data wajah yang tersimpan di database. Tidak seperti teknologi biometrik yang lain, *face recognition* dapat digunakan pada kasus yang melibatkan banyak orang sekaligus, misal dalam pencarian orang hilang atau dalam kasus DPO (Daftar Pencarian Orang). Ada 3 tahap dalam melakukan *Face Recognition* menurut [3] yaitu :

a. *Face detection* : pada tahap ini adalah mendeteksi apakah ada wajah pada gambar atau video yang diinputkan
b. *Feature extraction* : setelah wajah terdeteksi dilakukan ekstraksi ciri untuk memperoleh ciri – ciri dari wajah
c. *Face recognition* : tahap terakhir adalah pengenalan wajah dengan membandingkan wajah yang sudah diketahui cirinya dengan wajah yang ada di database

Skenario pengenalan wajah dapat diklasifikasikan menjadi 2 tipe menurut [4] yaitu :

a. *Face verification* (“apakah aku adalah yang aku katakan sebagai aku ?”) adalah pencocokan satu-ke-satu yang membandingkan sebuah citra wajah query dengan citra wajah template yang telah diklaim benar. Untuk mengevaluasi kemampuan verifikasi, verification rate (paramater dimana pengguna yang sah diberi akses) dibandingkan dengan false accept rate (parameter dimana pengguna palsu diberi akses), kemudian diplot ke dalam kurva ROC. Sistem verifikasi yang baik adalah sistem yang memiliki perbandingan yang seimbang antara kedua parameter tersebut pada pengoperasiaanya
b. *Face identification* (“siapakah aku ? ”) adalah pencocokan satu-ke-banyak yang membandingkan sebuah citra wajah query dengan semua template yang terdapat dalam basis data untuk menentukan identitas dari citra query. Identifikasi dilakukan dengan mencari wajah dalam basis data yang memiliki tingkat kemiripan tertinggi dengan citra query. Fitur subjek uji yang telah dinormalisasi dibandingkan dengan fitur-fitur lainnya dalam basis data dan angka kecocokan akan diperoleh untuk setiap perbandingan. Dari angka kecocokan tersebut akan diperoleh citra yang memiliki tingkat kemiripan tertinggi yang kemungkinan adalah identitas yang dicari.

2.3 Fisherface

Salah satu metode dalam pengenalan wajah yang dikembangkan oleh Peter N. Belhumeur, João P. Hespana dan David J. Kreigman pada tahun 1997 dengan menggabungkan *Principal Component Analysist (PCA)* dengan *Fisher’s Linear Discriminant* (*FLD*). Metode ini memiliki keunggulan dalam mengenali ekspresi wajah dibanding metode pengenalan wajah yang lain. *PCA* digunakan pada awal metode untuk mereduksi matriks citra masukan, kemudian

hasil dari reduksi *PCA* akan digunakan pada *FLD* untuk direduksi menjadi matriks yang lebih sederhana lagi. *PCA* digunakan untuk memaksimalkan jarak semua pola pada data latih sedangkan *FLD* digunakan untuk meminimalkan jarak pola yang termasuk ke dalam kelas yang sama (misalnya wajah seseorang) [4].

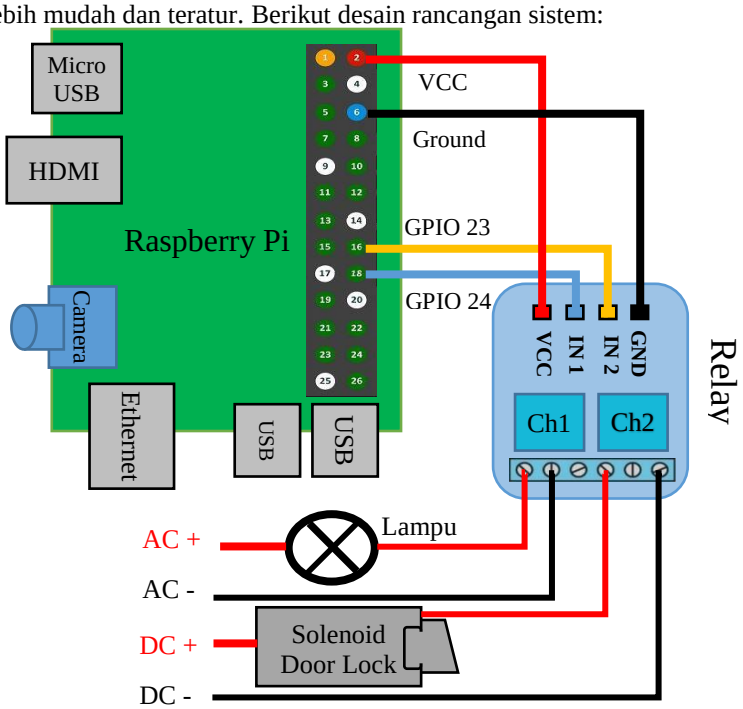
Penelitian yang dilakukan oleh Shan, Cao, Gao, dan Zhao [2], metode *fisherface* pada pengenalan wajah memiliki keunggulan pada aspek perubahan cahaya dan *minor* ekspresi dibandingkan dengan metode *eigenface*, sehingga metode *fisherface* akan lebih mampu jika diterapkan secara langsung, karena setiap hari kondisi cahaya di ruangan tidak menentu dan seringkali berubah. Oleh karena itu, metode *fisherface* dipilih dalam penelitian ini, karena sistem bersifat *real-time* dan tidak tergantung dengan kondisi cahaya yang ditangkap oleh kamera. Selain itu metode *fisherface* bekerja dengan cara mereduksi dimensi, sehingga dapat mengurangi waktu komputasi. Seorang peneliti bernama Alan Brooks dan Li Gao [5], pernah mengembangkan sebuah penelitian yang membandingkan dua algoritma yaitu *eigenface* dan *fisherface*. Penelitian ini difokuskan pada perubahan pose wajah apakah mempengaruhi akurasi pengenalan wajah. Pada *Eigenface* kompleksitas komputasi lebih sederhana daripada *fisherface*. Dari segi efektifitas karena perubahan pose, *fisherface* memberikan hasil yang lebih baik, bahkan dengan data yang lebih terbatas. Teknik *eigenface* juga lebih sensitif terhadap pencahayaan dibandingkan dengan *fisherface*.

Konstruksi *fisherface* adalah pembuatan suatu set *fisherface* dari suatu set gambar training dengan menggunakan perhitungan *Principal Component Analysis* (PCA) dan *Fisher's Linear Discriminant* (FLD).

3. Rancangan Sistem

3.1 Gambaran Umum Sistem

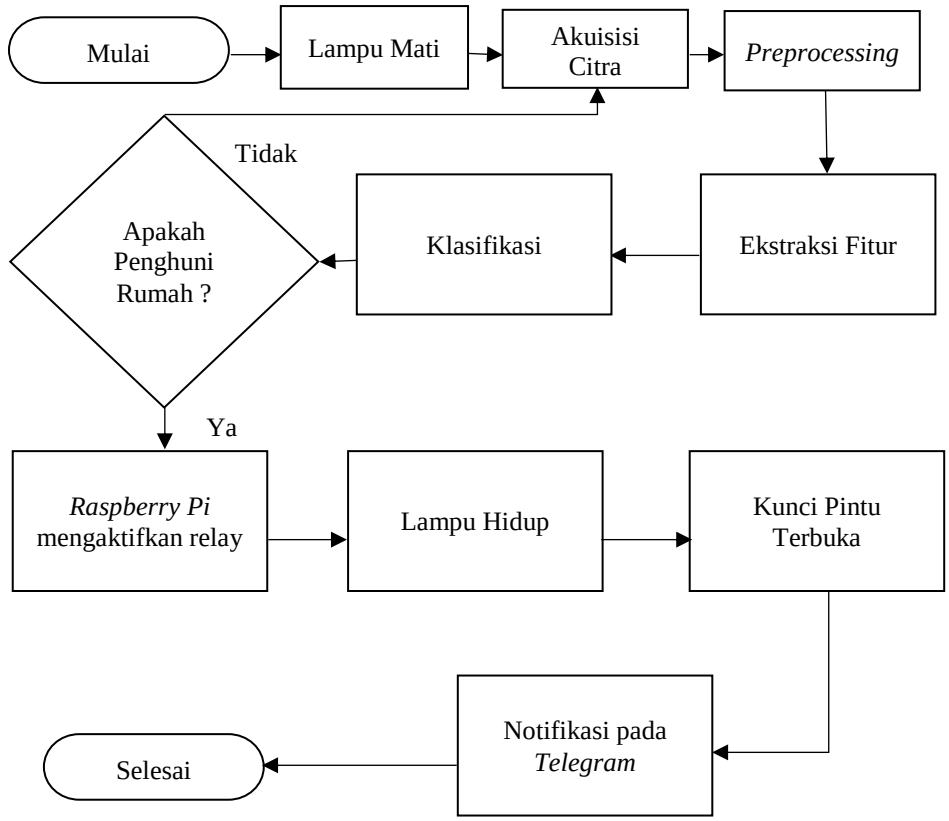
Sebelum memulai untuk pemasangan komponen, terlebih dahulu membuat desain rancangan sistem agar dalam pemasangan komponen lebih mudah dan teratur. Berikut desain rancangan sistem:



Gambar 1. Desain Rancangan Sistem

Untuk menghubungkan *raspberry pi* dengan sebuah saklar dibutuhkan *jumper female to male* yang ditancapkan melalui pin – pin pada GPIO ke pin saklar. Dalam membuat sistem ini hanya diperlukan 4 buah pin GPIO yang memiliki fungsi berbeda yaitu :

1. Pin 2 : dihubungkan ke pin vcc pada saklar untuk memberikan daya sebesar 5 volt.
2. Pin 6 : dihubungkan ke pin gnd pada saklar yang berfungsi sebagai *ground.*
3. Pin 16 (GPIO23) : dihubungkan ke pin IN1 pada saklar berfungsi sebagai input saklar pada *channel* 1 yang terhubung pada lampu yang dikontrol berdasarkan input yang dimasukkan.
4. Pin 18 (GPIO24) : dihubungkan ke pin IN2 pada saklar berfungsi sebagai input saklar pada *channel* 2 yang terhubung dengan kunci pintu solenoid, berfungsi untuk mengontrol kunci pintu berdasarkan input yang dimasukkan.



Gambar 2. Diagram Alir Sistem Keseluruhan

Gambar di atas merupakan diagram alir yang menjelaskan setiap tahap saat sistem bekerja. Proses pertama adalah lampu dinyatakan mati kemudian *Raspberry Pi* akan melakukan akuisisi citra menggunakan modul *Pi Camera* menghasilkan citra uji yang akan melewati *preprocessing* dan menghasilkan citra *grayscale.* Citra *grayscale* akan diambil fitur/cirinya dalam proses ektraksi fitur yang kemudian akan diklasifikasikan dengan citra yang berada dalam database citra latih. Proses selanjutnya adalah menentukan apakah citra uji sesuai dengan penghuni rumah yang sudah ditentukan di dalam sistem. Jika tidak sesuai, maka sistem akan kembali lagi pada proses akuisisi citra. Jika sesuai dengan penghuni rumah, maka *raspberry pi* akan mengaktifkan saklar sehingga lampu akan hidup dan kunci akan terbuka serta memberikan notifikasi ke *telegram* bahwa benar penghuni rumah mengaktifkan sistem.

3.3 Bot Telegram

Untuk melakukan kontrol dan menerima pemberitahuan dari sistema maka dibuat *BOT* pada aplikasi *Telegram yang* dapat dibuat sendiri sesuai keinginan pembuatnya. Untuk membuat *BOT* pada aplikasi telegram harus mencari *user BOT* dengan nama '*BotFather'*. *BotFathe*r itu sendiri adalah satu - satunya *BOT* untuk memerintah dan mengelola semua *BOT* yang akan dibuat. *BotFather* memiliki banyak fungsi misalnya membuat *BOT*, menghapus *BOT*, mengubah nama, mengubah deskripsi dan hal lainnya.

Gambar 3. BotFather

Pembuatan *BOT* pada aplikasi telegram cukup mengikuti perintah yang ada. Pertama ketik command *'/newbot'*, kemudian akan diminta untuk menulis nama *BOT* yang diinginkan contohnya *"Rumah Pintar Bot",* lalu masukan *username* untuk *BOT* tersebut contohnya *"rupin_bot*". Setelah itu maka kita akan diberikan token dari BOT tersebut. Token ini memiliki fungsi yang sangat penting yaitu untuk mengakses *HTTP API* dari *BOT* tersebut. Dengan kata lain

BOT dapat dikendalikan hanya dengan bermodalkan token tersebut. Oleh karena itu token tersebut jangan sampai orang lain tahu dan menjadi rahasia pemilik *BOT*.

3.4 Parameter Pengujian

Parameter yang digunakan dalam penelitian ini adalah sebagai berikut :

1. Akurasi keseluruhan, parameter ini digunakan untuk mengetahui tingkat akurasi dengan cara menghitung wajah yang terdeteksi benar.

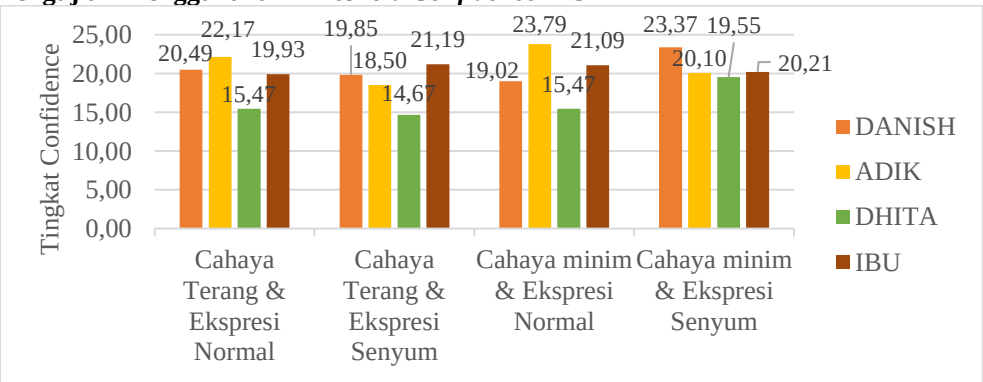
$$\text{Akurasi keseluruhan} = \frac{\text{Jumlah wajah yang terdeteksi benar}}{\text{Jumlah pengujian}} \times 100\%$$

2. Waktu Komputasi pemindaian wajah, parameter ini digunakan untuk mengetahui waktu yang dibutuhkan oleh sistem dalam memindai wajah yang telah diklasifikasikan. Waktu penghitungan dimulai saat sistem mulai mendeteksi wajah hingga program berhasil mengontrol saklar.
3. Waktu komputasi kontrol, parameter ini digunakan untuk mengetahui waktu yang dibutuhkan oleh sistem untuk dapat mengontrol lampu setelah wajah berhasil terdeteksi. Waktu penghitungan dimulai saat pendeteksian wajah berhasil mengontrol saklar kemudian saklar mengontrol lampu dan mendapat notifikasi kembali dari sistem.
4. Kondisi Cahaya, parameter ini sangat mempengaruhi keberhasilan sistem dalam mengenali wajah. Kondisi cahaya yang diuji terbagi menjadi 2, yaitu:
   a) Kondisi cahaya terang
      Sistem diuji saat pagi hari yang cerah dengan jam menunjukkan pukul 10.00 hingga 12.00 WIB.
   b) Kondisi cahaya minim
      Sistem diuji saat sore hari menjelang petang dengan jam menunjukkan pukul 17.00 hingga 18.00 WIB.
5. *Threshold Confidence*
   Nilai *confidence* didapat dari hasil klasifikasi oleh *Euclidean distance* (E_{min}). Semakin kecil jarak minimum yang diperoleh, maka semakin besar kesamaan (*similarity*) gambar masukan dengan gambar pada *training set*. Sebuah wajah dikatakan cocok jika jarak minimumnya lebih kecil dari nilai batas yang diterapkan (*threshold confidence)*. Nilai batas diperoleh dari hasil pengujian-pengujian hingga ditemukan satu nilai yang memuaskan.

4. Hasil Pengujian

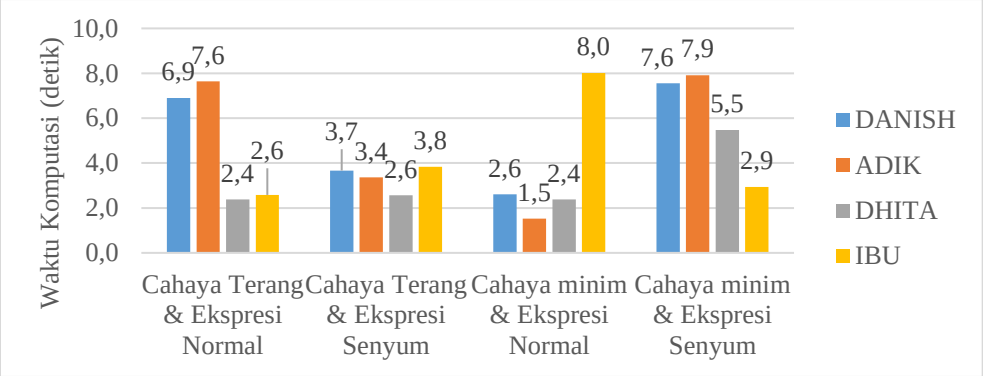
Pengujian dilakukan dengan ekspresi yang berbeda dan kondisi cahaya yang juga berbeda. Selain itu dilakukan perubahan nilai *confidence* yaitu 25 dan 30 untuk mengetahui performansi sistem untuk mengenali tiap *user* yang diperbolehkan mengakses saklar. Secara keseluruhan, tingkat keberhasilan sistem dalam mengenali wajah pengguna sebesar 98.75% dengan rata-rata nilai *confidence* sebesar 20.57 dan 4.11 detik waktu komputasi. Berikut adalah grafik hasil pengujian.

4.1 Hasil Pengujian Menggunakan *Threshold Confidence* <25



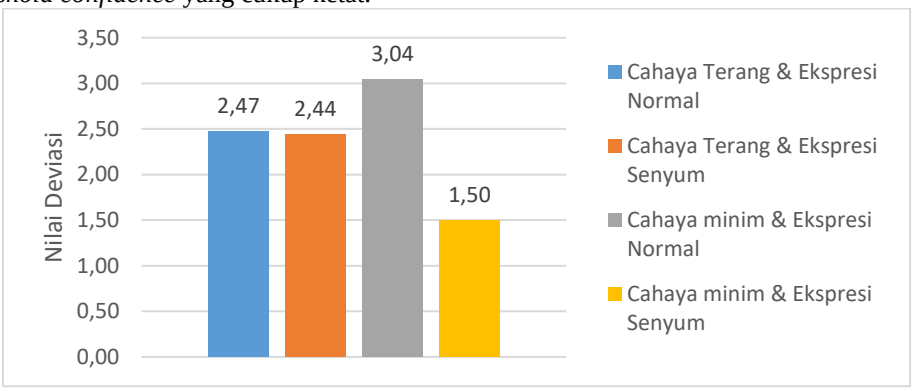
Gambar 4. Hasil Pengujian Berdasarkan Tingkat *Confidence*

Berdasarkan gambar di atas pengujian di kondisi cahaya terang dan ekspresi senyum pada *threshold confidence* <25 diperoleh nilai rata-rata *confidence* terbaik, hal ini karena fitur citra terlihat lebih jelas dan unik dibandingkan dengan ekspresi normal.



Gambar 5. Hasil Pengujian Berdasarkan Waktu Komputasi

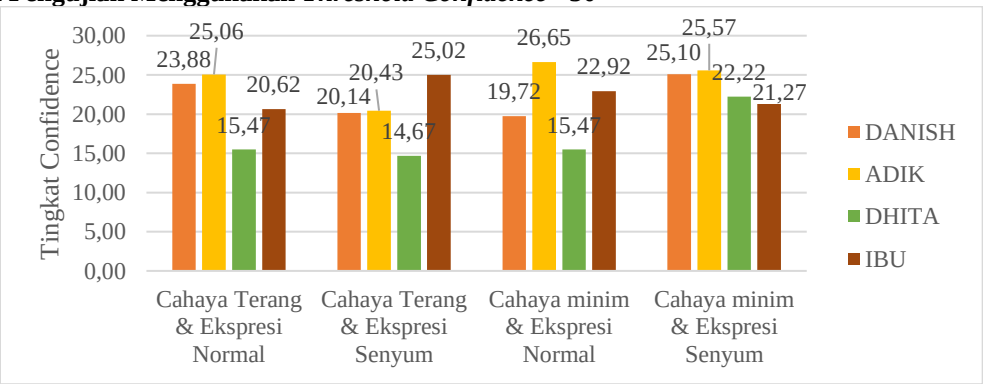
Gambar di atas menunjukkan pengujian di kondisi cahaya minim dengan ekspresi senyum pada *threshold confidence* <25 memperoleh waktu komputasi paling lama, hal ini karena fitur citra kurang terlihat dengan jelas disertai *threshold confidence* yang cukup ketat.



Gambar 6. Nilai Deviasi Berdasarkan Rata-Rata Nilai *Confidence*

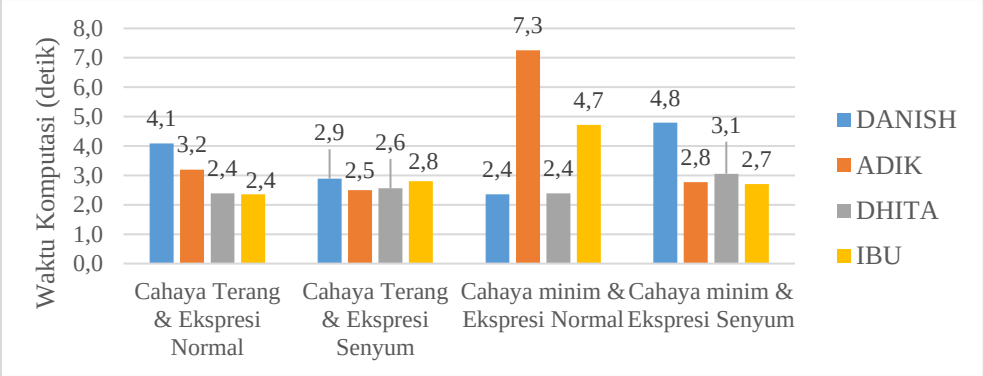
Berdasarkan gambar 6, nilai deviasi paling tinggi di dapat pada kondisi cahaya minim dengan ekspresi normal sedangkan nilai deviasi paling rendah di dapat pada kondisi cahaya minim dengan ekspresi senyum

4.2 Hasil Pengujian Menggunakan *Threshold Confidence* <30



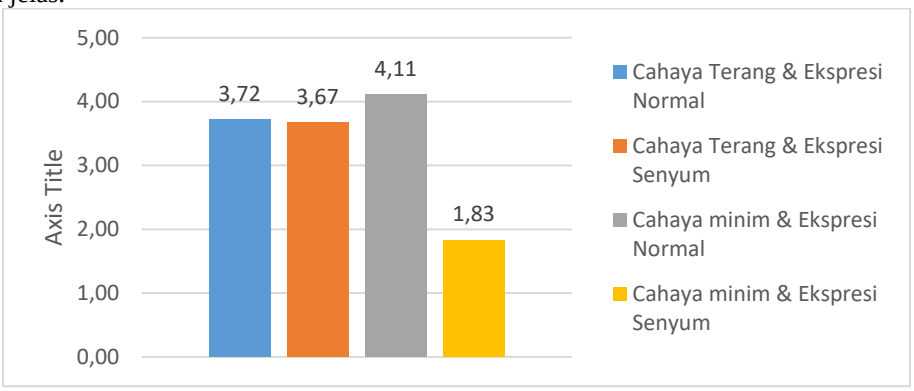
Gambar 7. Hasil Pengujian Berdasarkan Tingkat *Confidence*

Berdasarkan gambar 7, pengujian di kondisi cahaya terang dan ekspresi senyum pada *threshold confidence* <30 diperoleh nilai rata-rata *confidence* terbaik sedangkan di kondisi cahaya mminim dan ekspresi senyum memperoleh nilai rata-rata *confidence* terburuk.



Gambar 8. Hasil Pengujian Berdasarkan Waktu Komputasi

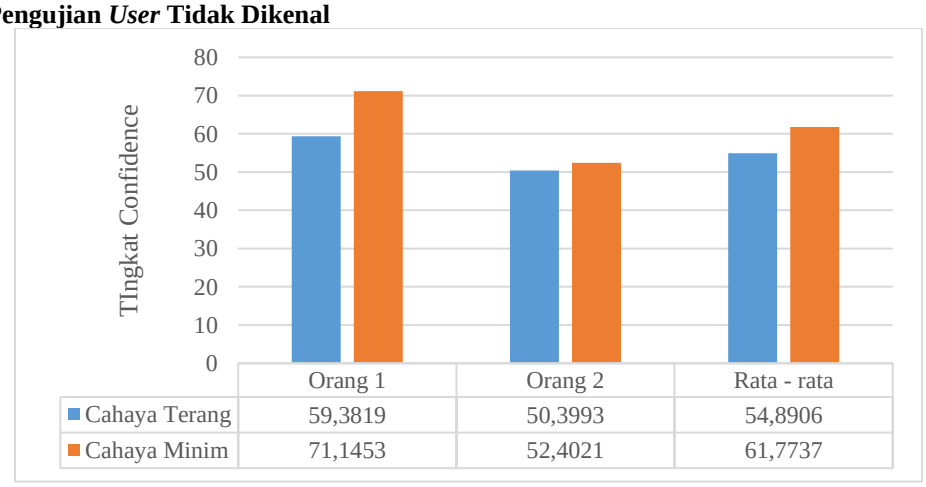
Gambar di atas menunjukkan pengujian di kondisi cahaya terang ekspresi senyum pada *threshold confidence* <30, diperoleh waktu kondisi tercepat. Hal ini karena nilai *threshold confidence* yang lebih longgar dan fitur citra terlihat lebih jelas.



Gambar 9. Nilai Deviasi Berdasarkan Rata-Rata Nilai *Confidence*

Berdasarkan gambar 9, nilai deviasi paling tinggi di dapat pada kondisi cahaya minim dengan ekspresi normal sebesar 4.11, sedangkan nilai deviasi paling rendah di dapat pada kondisi cahaya minim dengan ekspresi senyum sebesar 1,83.

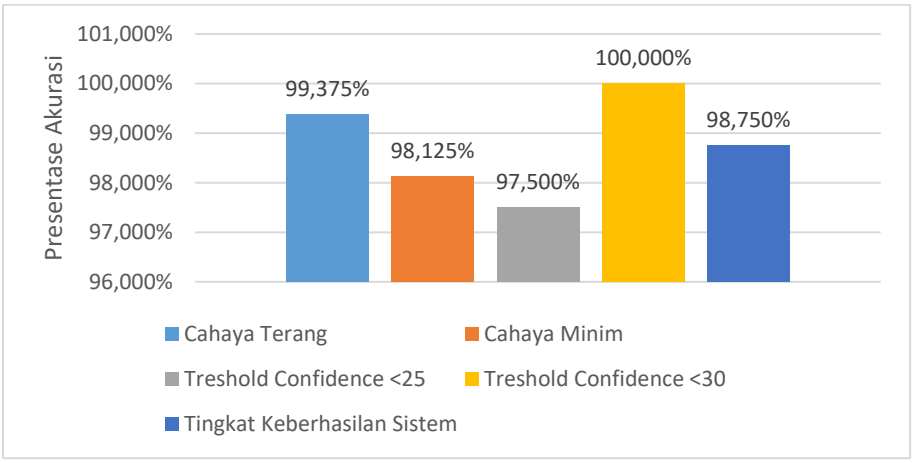
4.3 Hasil Pengujian *User* Tidak Dikenal



Gambar 10. Hasil Pengujian *User* Tidak Dikenal

Gambar 10 menunjukkan tidak ada satupun *user* yang tidak dikenali berhasil masuk ke sistem, dengan rata – rata *confidence* pada kondisi cahaya terang adalah 54,8906 dan untuk kondisi cahaya minim adalah 61,7737.

4.4 Tingkat Keberhasilan



Gambar 11. Tingkat Keberhasilan

Berdasarkan gambar 11, tingkat keberhasilan yang paling baik didapat pada *threshold confidence* <30 dengan akurasi sebesar 100%, sedangkan tingkat keberhasilan yang paling buruk adalah saat kondisi cahaya minim dengan akurasi sebesar 97,50%.

5. Kesimpulan

Berdasarkan analisis hasil pengujian pada tugas akhir ini, dapat ditarik kesimpulan:

1. Perancangan sistem otomasi lampu beserta kunci rumah dan sistem keamanan rumah yang telah dibuat, bekerja dengan baik dan mampu memberikan tingkat akurasi mencapai 98,75% .
2. Performansi *raspberry pi* dalam melakukan proses pengolahan citra, yang paling baik untuk sistem keamanan rumah berdasarkan tingkat keberhasilan dan rata-rata waktu komputasi tercepat adalah di kondisi cahaya terang dan berekspresi senyum dengan batas *confidence* <30 menghasilkan tingkat akurasi sebesar 100% dan rata- rata waktu komputasi sebesar 2,69 detik.
3. Pengujian pada kondisi cahaya terang secara keseluruhan menghasilkan performa yang lebih baik dengan tingkat akurasi sebesar 99,375% dan 3,48 detik untuk rata - rata waktu komputasi dibandingkan kondisi cahaya minim sebesar 98,125% dan 4,75 detik untuk rata - rata waktu komputasi.

6. Saran

Mengingat masih terdapat kekurangan pada tugas akhir ini, maka penulis memiliki beberapa saran yang diharapkan dapat bermanfaat untuk pengembangan selanjutnya dari topik ini.

1. Pengembangan riset sebaiknya menggunakan versi *Raspberry Pi* yang terbaru agar waktu komputasi lebih cepat.
2. Sebaiknya dilakukan pengujian dengan membandingkan pengaruh penggunaan kamera infrared dengan kamera non infrared.
3. Pengembangan riset dengan menyimpan data latih melalui aplikasi smartphone.

Daftar Pustaka:

[1] E. F. P. CASAGRAS, CASAGRAS Final Report: RFID and the Inclusive Model for the Internet of Things, CASAGRAS, 2009.

[2] L. Wahyunita, Aplikasi HomeChat pada aplikasi Intenet of Things Smartphone sebagai komunikasi Peralatan Elektronik Rumah Tangga dengan Manusia, Yogyakarta: Department Math and Science Gadjah Mada University, 2015.

[3] R. C. Wenyi Zhao, Face Processing Advanced Modeling Method, Academic Press, 2006.

[4] S. Shan, B. Cao, W. Gao and D. Zhao, "Extended Fisherface For Face Recognition From A Single Example Image Per Person," in *IEEE International Symposium on Circuits and Systems*, Phoenix-Scottsdale, 2002.

[5] A. Brooks and L. Gao, Face Recognition: Eigenface and Fisherface, Final Project Report, 2004.