

Perancangan Sistem Identifikasi Wajah dengan Teknik *Feature-Based* pada Aplikasi *Safety Box*

Wahyu Artotomo¹, V. Vekky R. Repi¹, Novi Azman²

¹Program Studi Teknik Fisika, Fakultas Teknik dan Sains, Universitas Nasional, Jakarta

²Program Studi Teknik Elektro, Fakultas Teknik dan Sains, Universitas Nasional, Jakarta

Korespondensi: vekky_repi@yahoo.com

Abstrak. Identifikasi wajah dapat digunakan sebagai pelengkap untuk fungsi keamanan. Pada penelitian ini akan dilakukan pengidentifikasian wajah sebagai akses keamanan pada aplikasi *safety box* dimana sistemnya meliputi pendeteksian wajah, operasi geometri pengolahan citra (pemotongan dan penskalaan citra), perbaikan citra, proses identifikasi wajah menggunakan *Speeded-Up Robust Features* (SURF) dan eksekusi menggunakan solenoid sebagai fungsi pengaman pada aplikasi *safety box*. Dari hasil percobaan di peroleh hasil identifikasi dengan persentasi 50% menggunakan wajah yang identik dengan *database* sedangkan pada pengujian lainnya yang menggunakan wajah yang tidak identik dengan *database* memiliki hasil identifikasi dengan persentasi 0% dari 50 data perbandingan. Persentasi ini di dapat berdasarkan hasil nilai poin kesamaan yang di anggap wajah teridentifikasi untuk mengakses *safety box* dimana pada penelitian ini batasan nilai poin kesamaan yang di anggap teridentifikasi adalah ≥ 7 . Dari hasil penelitian ini disimpulkan bahwa sistem identifikasi ini berhasil karena hanya pada wajah yang identik dengan *database* yang berhasil teridentifikasi oleh sistem sehingga bisa mengakses pengunci pada *safety box* sedangkan pada wajah yang tidak identik pada *database* tidak teridentifikasi oleh sistem.

Kata Kunci : Identifikasi wajah, *safety box*, pengolahan citra, *Speeded-Up Robust Features*, *database*.

PENDAHULUAN

Perkembangan teknologi di dunia semakin pesat, hal ini dikarenakan tuntutan pasar dunia yang semakin membutuhkan teknologi yang handal dalam menunjang segala kebutuhan baik untuk masa kini ataupun perkembangan di masa depan. Suatu bidang yang memiliki dampak dari perkembangan zaman adalah sistem identifikasi. Identifikasi bagian tubuh merupakan konsep terbaru dan yang sering digunakan adalah proses identifikasi dengan wajah. Hal ini dikarenakan setiap orang memiliki ciri-ciri khas pada masing-masing wajah. Sistem keamanan suatu objek pada saat ini lebih banyak memanfaatkan tenaga manusia dari pada sistem otomatis. Sistem keamanan dengan alarm telah banyak diterapkan untuk mendeteksi adanya pencuri. Tetapi sistem tersebut tidak bisa membedakan antara pemilik dan pencuri, sehingga tingkat keamanan sangat rendah [1]-[4]. Penggunaan identifikasi wajah pada penelitian ini dengan tujuan untuk mengenali wajah pemilik dan membedakannya dengan wajah pencuri. Pada penelitian ini, objek yang akan di beri sistem keamanan adalah aplikasi *safety box*, dimana pengidentifikasian wajah adalah konsep keamanan pada aplikasi *safety box* tersebut.

METODE PENELITIAN

Spesifikasi Alat

Sistem ini disusun dengan menggunakan alat-alat bantu berupa perangkat keras dan perangkat lunak sebagai penunjang pada sistem ini. semua alat-alat ini memiliki fungsinya masing-masing sesuai dengan posisi dan tujuan alat ini digunakan. berikut adalah alat-alat beserta spesifikasinya yang digunakan pada penelitian ini:

- Perangkat keras
 - *Personal Computer* (PC) dengan spesifikasi *Processor Intel Core i3-2330M*
 - 2.2 GHz, RAM 6 GB
 - Kamera eksternal M-TECH 5MP

- Mikrokontroler Arduino Uno r3
 - *Relay* Heli Shun 5 vdc
 - *Solenoid* 12 vdc
 - *Adapter* 12 vdc
 - Kotak *safety box*
 - Kabel-kabel penghubung
- Perangkat lunak
- Sistem operasi *Windows 7 Professional* 64-bit.
 - MATLAB R2013a

Penelitian Secara Umum

Dalam bidang penelitian pemrosesan wajah (*face processing*), pendeteksian wajah manusia (*face detection*) adalah salah satu tahap awal yang sangat penting di dalam proses pengenalan wajah (*face recognition*). Sistem pengenalan wajah digunakan untuk membandingkan satu citra wajah masukan dengan suatu database wajah dan menghasilkan wajah yang paling cocok dengan citra tersebut apabila ada kecocokan. Sedangkan autentikasi wajah (*face authentication*) digunakan untuk menguji keaslian/kesamaan suatu wajah dengan wajah yang telah diinput sebelumnya.

Bidang penelitian yang juga berkaitan dengan pemrosesan wajah adalah lokalisasi wajah (*face localization*) yaitu pendeteksian wajah dengan asumsi hanya ada satu wajah di dalam citra. Sistem pengenalan citra wajah dibagi menjadi dua jenis, yaitu *feature-based* dan sistem *image-based*. Pada sistem *feature-based* digunakan ciri yang diekstraksi dari komponen citra wajah seperti mata, hidung dan lain-lain yang kemudian dimodelkan secara geometris hubungan antara ciri-ciri tersebut. Sedangkan pada sistem *image-based* menggunakan informasi mentah dari piksel citra yang kemudian direpresentasikan dalam metode tertentu, misalnya seperti *Principal Component Analysis* (PCA) atau transformasi wavelet yang digunakan untuk klasifikasi identitas citra [1-3].

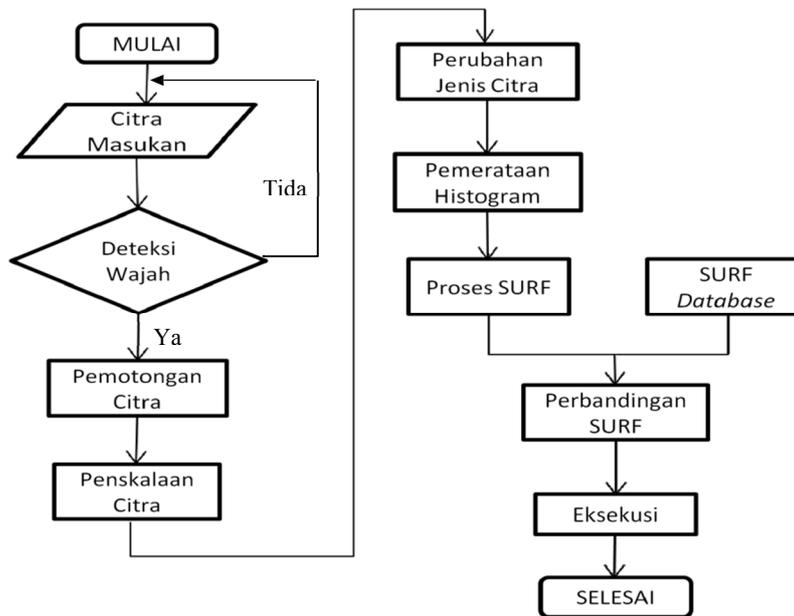
Metode atau teknik pengenalan wajah yang umum telah dilakukan sebelumnya, antara lain menggunakan algoritma *eigenface* oleh Turk and Pentland pada tahun 1991, dengan distribusi Gaussian dan Clustering oleh Sung and Poggio pada tahun 1994, dengan Support Vector Machine oleh Osuna dkk pada tahun 1997, dan dengan Statistic dan Wavelet oleh Schneiderman pada tahun 2000. beberapa masalah yang mungkin terjadi yakni perubahan skala, perubahan posisi, perubahan cahaya, perubahan detil dan ekspresi wajah. Gambar di bawah adalah bentuk sistem pengenalan wajah yang menggunakan *feature-based* dan *image based* [4-6].

Gambar 1 menunjukkan alur penelitian secara umum dari penelitian ini. Sebelum sistem secara keseluruhan dijalankan, maka harus dibuat *database* sebagai pembanding dengan data uji. *Database* itu sendiri akan di proses terlebih dahulu dan di simpan sebelum proses identifikasi wajah ini berjalan. Proses penyimpanan *database* ini dilakukan di luar identifikasi wajah atau tersendiri. Jumlah citra pada *database* ini adalah lima puluh. Hal ini dikarenakan *database* sebagai data perbandingan dengan data uji sehingga diperbanyak agar mampu berinteraksi citra uji yang tak menentu atau tidak tetap [7-10]. Gambar 2 merupakan alur penelitian dari penyimpanan citra (*database*).

Terlihat pada gambar 3.2 bahwa proses penyimpanan citra *database* sebenarnya hampir sama dengan sistem identifikasi wajah namun yang membedakan adalah hasil dari proses *Speeded-Up Robust Features* (SURF) sebagai metode pengenalan fitur akan di simpan di dalam suatu *database* dan apabila ada citra masukan yang dianggap sebagai citra uji maka data dari citra uji itu akan dibandingkan dengan *database* sebagai proses identifikasi wajah yang dikenali atau tidak [11].

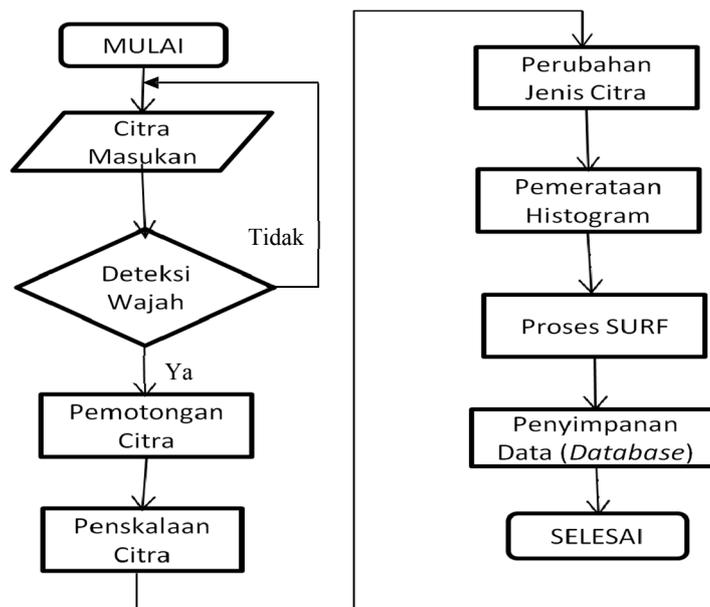
Pada proses awal akan dilakukan proses pengambilan citra menggunakan kamera M-TECH berkualitas 5MP. Setelah itu citra akan di proses pendeteksian wajah, apabila terdeteksi lebih dari satu wajah sistem tidak dapat dilanjutkan karena dianggap gangguan. Setelah tahap proses deteksi wajah, citra akan di normalisasikan dengan beberapa proses mulai dari pemotongan citra, perubahan skala dan perbaikan citra. Lalu pada tahap identifikasi wajah akan

dilakukan perbandingan fitur menggunakan metode *Speeded-Up Robust Features (SURF)* antara data uji dan *database* [12]. Setelah dibandingkan maka akan di dapat nilai poin kesamaan yang akan di kategorikan dalam identifikasi wajah berupa dikenali atau tidak dikenali sesuai dengan yang telah di tentukkan sebelumnya. Dari hasil identifikasi wajah akan dijadikan sebagai dasar eksekusi kepada *safety box* yang mana apabila wajah dikenali maka *safety box* akan otomatis terbuka sedangkan bila tidak dikenali maka *safety box* tetap dalam keadaan terkunci.



GAMBAR 1. Perancangan sistem identifikasi wajah.

Proses yang pertama adalah proses deteksi wajah, yaitu proses yang bertujuan mengidentifikasi adanya wajah dalam citra, pendeteksian ini digunakan untuk membantu sistem dalam pengidentifikasian wajah. Proses selanjutnya adalah pemotongan citra, yaitu citra masukan yang telah di deteksi bagian wajahnya akan di potong pada bagian wajah sehingga bagian di luar wajah yang tidak di deteksi akan di hilangkan sehingga citra baru akan menampilkan bagian wajah saja.



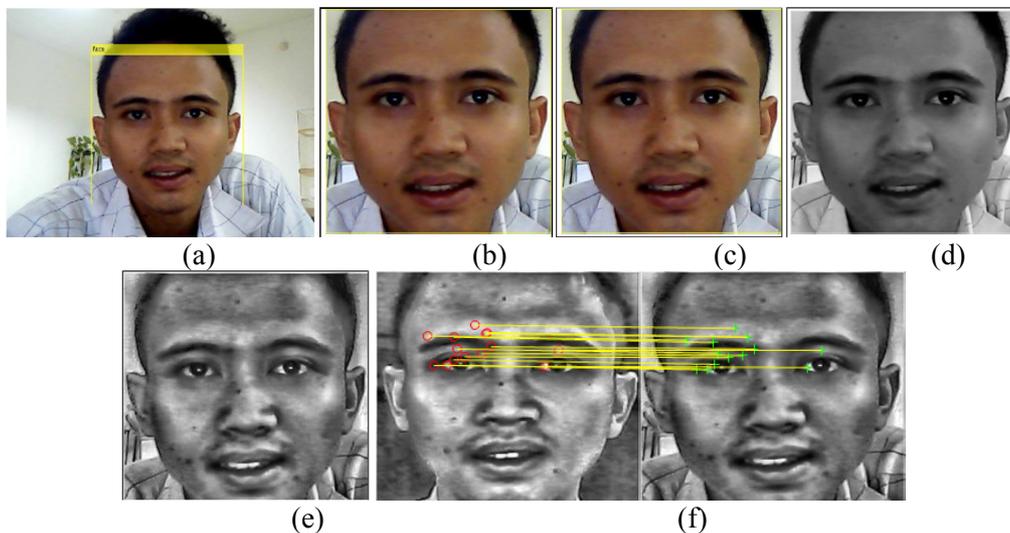
GAMBAR 2. Diagram alir penyimpanan database.

Setelah proses pemotongan citra, citra baru akan dilakukan proses pengubahan skala. Hal ini dilakukan karena setelah pemotongan citra, skala citra mengalami perubahan bervariasi. Variasi

ini terjadi karena letak wajah saat pengambilan memiliki besar skala yang berbeda-beda maka dari itu dilakukan penskalaan atau mengubah skala pada citra agar memiliki besar skala yang sama dengan citra database.

Setelah citra melakukan tahap penskalaan, citra akan di normalisasikan dengan mengubah jenis citra dari citra RGB menjadi *grayscale*. perubahan ini dilakukan untuk memperkecil nilai-nilai piksel. Pada tahap selanjutnya, citra akan di ekualisasi histogram. Ekualisasi di sini menggunakan CLAHE. Seperti yang telah di jelaskan pada bab 2 bahwa *Contrast Limited Adaptive Histogram Equalization* (CLAHE) berfungsi untuk membedakan *noise* dengan cara membatasi kontras.

Metode CLAHE ini merupakan metode ekualisasi histogram pada semua rentang dinamiknya sebagai gabungan dari histogram lokal masing-masing citra. Hal ini bertujuan agar gambar yang dihasilkan memiliki informasi yang lebih baik. Proses selanjutnya adalah *matching features*. Proses ini membutuhkan 2 citra untuk melihat fitur kesamaan dari kedua citra tersebut. Kedua citra tersebut adalah citra uji dan citra *database*. citra uji di dapat saat sistem menerima masukan, sedangkan citra *database* adalah beberapa citra yang telah disiapkan sebagai dasar pembandingan dengan citra uji nanti [10-12]. Hasil dari setiap proses ditampilkan pada gambar 3.



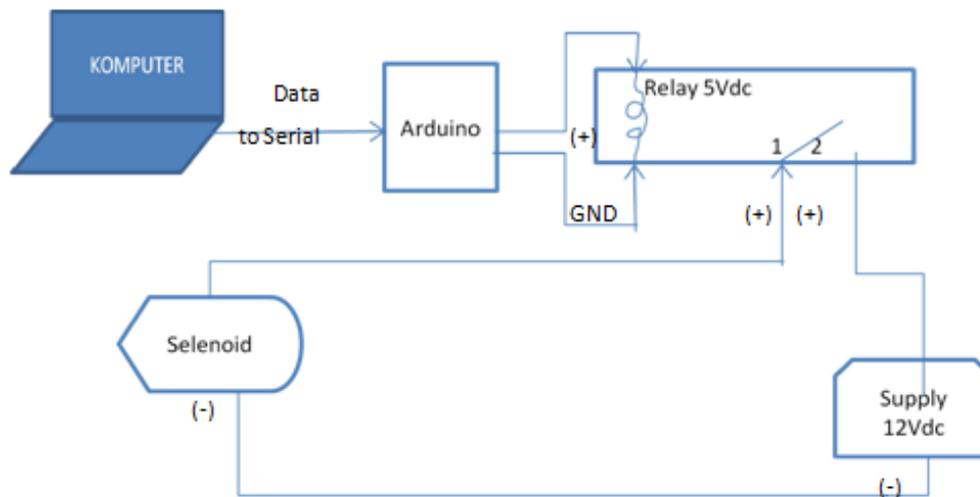
GAMBAR 3. Hasil dari tiap proses sistem pendeteksian wajah yang dirancang: (a) Citra masukan dari kamera yang telah terdeteksi; (b) Pemotongan citra; (c) Penskalaan citra; (d) Citra RGB to Gray; (e) Citra hasil proses CLAHE; (f) Proses *matching features* pada dua citra.

Pada tahap klasifikasi di proses *matching features*, dibutuhkan beberapa syarat [13]. Syarat ini harus memiliki parameter lebih karena syarat klasifikasi sistem ini bukan hanya terdeteksi wajah atau ada beberapa kesamaan poin fitur saja namun harus memiliki batasan nilai poin kesamaan dalam identifikasi wajah untuk dapat mengakses keamanan pada aplikasi *safety box* ini, batasan nilai poin kesamaan ini akan saya tentukan dengan menggunakan percobaan di bawah ini. Dari beberapa percobaan dengan citra uji dan citra database yang mana database di buat hingga 50 masukan dengan variasi mimik muka berbeda-beda untuk mengetahui responsif dengan mimik yang berbeda. Pengujian dilakukan dengan 50 citra pada *database* yang memiliki mimik dan kondisi yang berbeda dan akan di dapat nilai poin kesamaan yang akan dijadikan parameter untuk klasifikasi identifikasi wajah. Hasil pengujian disajikan oada Tabel 1.

Berdasarkan Tabel 1, rata-rata poin kesamaan bernilai 8 poin kesamaan dengan nilai yang sering muncul adalah 10 dan nilai tertinggi adalah 16. Oleh karena itu dapat ditentukan bahwa nilai poin kesamaan minimal 7, maka wajah dikatakan saling mengenali. Parameter nilai rata-rata di anggap cukup mewakili sebagai parameter saling mengenali dalam identifikasi wajah. Selanjutnya adalah tahap eksekusi, yaitu dimana hasil keluaran dari identifikasi wajah akan di proses pada mikrokontroler lalu untuk mengeksekusi solenoid sebagai aktuator yang akan dimanfaatkan sebagai penguncian pada aplikasi *safety box* ini. Tahap pada proses ditunjukkan pada gambar 4.

TABEL 1. Pengujian sebagai Klasifikasi Identifikasi Wajah

Pengujian									
No	Hasil	No	Hasil	No	Hasil	No	Hasil	No	Hasil
1	10	11	5	21	7	31	10	41	7
2	9	12	16	22	3	32	4	42	1
3	8	13	10	23	2	33	4	43	8
4	6	14	10	24	0	34	8	44	5
5	8	15	14	25	7	35	10	45	10
6	2	16	10	26	5	36	13	46	3
7	6	17	8	27	2	37	14	47	6
8	4	18	11	28	2	38	6	48	4
9	4	19	11	29	4	39	7	49	5
10	1	20	7	30	3	40	13	50	1



GAMBAR 4. Skema Koneksi Mikrokontroler Dan Aktuator

Eksekusi dapat dilakukan apabila pin penghubung selenoid dan *supply* tersambung. Untuk penyambungannya digunakan mikrokontroler yang tersambung pada pin COM dimana apabila identifikasi wajah memiliki keluaran outputan 1 maka akan memberikan arus listrik dengan tegangan ± 5 Vdc. Mengingat *relay* yang digunakan 5 Vdc juga maka apabila pin COM di aliri arus listrik dengan tegangan 5 Vdc maka pin lain pada *relay* khususnya pada pin hubungan *supply* dan selenoid akan tersambung begitu pula sebaliknya bila tidak ada tegangan maka selenoid akan tetap dalam keadaan semula dimana keadaan semula berarti selenoid dalam keadaan *normally close* atau dengan kata lain selenoid dalam keadaan mengunci pada *safety box* dan *safety box* akan dapat terbuka apabila selenoid mendapatkan energi untuk menarik pengunci yang dihubungkan pada *safety box*.

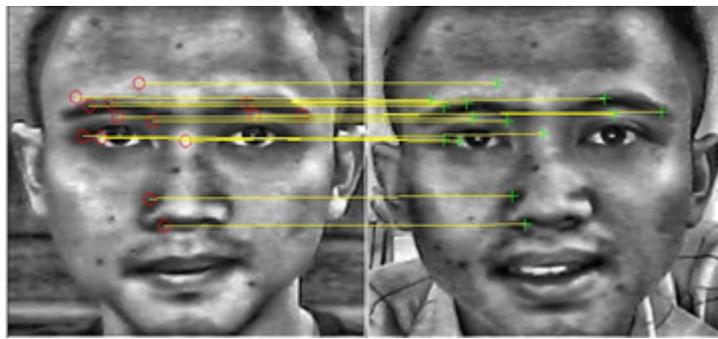
ANALISA DAN PEMBAHASAN

Citra yang akan di ujikan berjumlah 4 terlihat pada gambar 5, dengan memiliki peran masing-masing dalam pengujian dan *database* yang digunakan berjumlah 50 dengan bermacam-macam variasi mimik wajah dan sudut pandang citra

Pada Pengujian I ini menggunakan citra uji yang identik dengan citra *database*. Gambar 6 terlihat banyaknya poin kesamaan di antara citra tersebut. Angka di atas gambar yang berjumlah 14 adalah nilai poin kesamaan poin antara dua citra tersebut. Gambar kiri adalah salah satu citra *database* dan gambar kanan adalah citra uji. Fitur yang memiliki kesamaan poin dominan pada bagian mata dan sekitarnya. gambar uji pada pengujian I terdeteksi sehingga *safety box* akan terbuka dengan selenoid sebagai kunci telah tertarik karena program identifikasi wajah menganggap salah satu perbandingan gambar uji dan gambar *database* teridentifikasi sama dan mikrokontroler menjalankan arus listriknya untuk menyambungkan pin *supply* dan selenoid yang awalnya terputus.

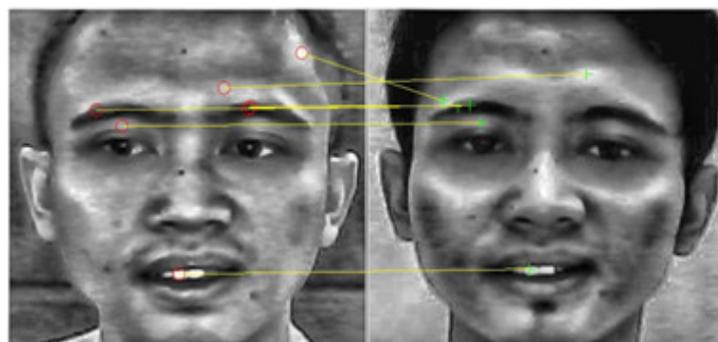


GAMBAR 5. Citra Uji secara Berurutan dari Kiri ke Kanan



GAMBAR 6. Hasil Pengujian I

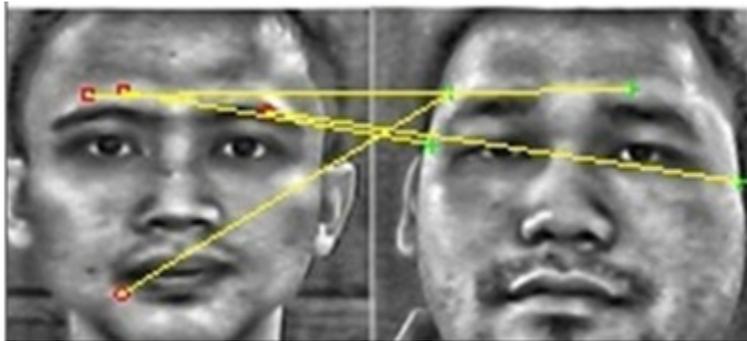
Pada gambar 7, adalah pengujian II ini menggunakan citra uji yang identik dengan *database*. citra identik ini memiliki pencahayaan berbeda dengan citra *database* yaitu 125 lux karena citra pada *database* 80-100 lux. Hal ini dilakukan untuk mengetahui apakah dengan gambar uji ini dapat membuka *safety box* yang terkunci atau tidak.



GAMBAR 7. Hasil Pengujian II

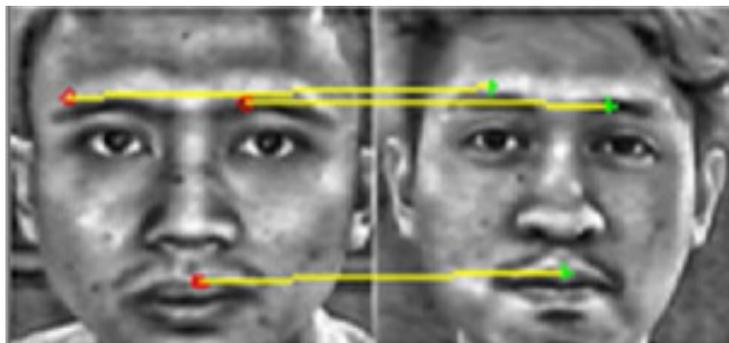
Pengujian II ini dikatakan teridentifikasi wajahnya dengan database mengingat perbandingan citra uji dan citra pada *database* ketiga memiliki nilai poin kesamaan 7 yang mana telah ditentukan bahwa batasan nilai poin kesamaan yang masuk dalam kategori teridentifikasi dengan citra *database* bernilai ≥ 7 . Oleh karena itu maka aplikasi *safety box* akan terbuka karena gambar teridentifikasi sehingga program akan memberikan sinyal citra teridentifikasi kepada mikrokontroler Arduino sehingga mikrokontroler akan menjalankan arus listrik ke relai untuk membuka pin *supply* dan solenoid sehingga *supply* dapat mengaliri arus listrik ke solenoid untuk membuka kunci pada *safety box*.

Pada gambar 8, adalah pengujian III ini dikatakan tidak teridentifikasi wajahnya dengan database mengingat perbandingan gambar uji dan gambar database ketiga hanya memiliki nilai poin kesamaan tertinggi 4 yang mana telah ditentukan bahwa batasan nilai poin kesamaan yang masuk dalam kategori teridentifikasi dengan gambar database bernilai ≥ 7 . Oleh karena itu maka box akan tetap dalam keadaan tertutup dan tidak dapat di akses karena gambar tidak teridentifikasi sehingga program akan memberikan sinyal gambar tidak teridentifikasi kepada mikrokontroller Arduino sehingga mikrokontroller tidak menjalankan arus listrik ke relai sehingga pin *supply* dan selenoid masih dalam keadaan terputus sehingga *supply* tidak dapat mengaliri arus listrik ke selenoid dan kunci masih dalam keadaan terkunci sehingga *safety box* tidak bisa di buka.



GAMBAR 8. Hasil Pengujian III

Sedangkan pada gambar 9 adalah pengujian IV ini menggunakan citra uji yang berbeda dengan *database*. Pengujian IV ini dikatakan tidak teridentifikasi wajah dengan database mengingat perbandingan citra uji dan citra *database* ke-19 hanya memiliki nilai poin kesamaan tertinggi 4 yang mana telah ditentukan bahwa batasan nilai poin kesamaan yang masuk dalam kategori teridentifikasi dengan citra pada *database* bernilai ≥ 7 . Oleh karena itu maka *safety box* akan tetap dalam keadaan tertutup.



GAMBAR 9. Hasil Pengujian IV

Pada hasil pengujian I memiliki nilai poin kesamaan dengan nilai rata-rata 8, nilai yang sering muncul 10, nilai tertinggi 16 dan nilai terendah 0. Pada pengujian I ini, *box* dapat terbuka karena telah melewati batasan nilai identifikasi wajah sehingga selenoid sebagai pengunci dapat terbuka dimana nilai kesamaan poin 7 ada di beberapa proses perbandingan gambar uji dan *database*.

Pada hasil pengujian II memiliki nilai poin kesamaan dengan nilai rata-rata 3, nilai yang sering muncul 2, nilai tertinggi 7 dan nilai terendah 0. Pada pengujian II ini, *safety box* dapat terbuka karena telah melewati batasan nilai identifikasi wajah sehingga selenoid sebagai pengunci dapat terbuka dimana nilai kesamaan poin 7 ada di beberapa proses perbandingan citra uji dan citra pada *database* meskipun nilai tertinggi hanya 7 karena pada syarat identifikasi 7 masuk dalam kategori teridentifikasi.

Pada hasil pengujian III memiliki nilai poin kesamaan dengan nilai rata-rata 2, nilai yang sering muncul 1, nilai tertinggi 4 dan nilai terendah 0. Pada pengujian III ini, *safety box* tidak dapat terbuka karena wajah tidak teridentifikasi sehingga solenoid tidak bisa membuka kunci pada *safety box*. Hal yang menyebabkan *safety box* tetap dalam keadaan terkunci adalah nilai poin kesamaan yang tidak dapat memenuhi syarat sebagai wajah yang teridentifikasi. nilai terbesar dari pengujian III ini adalah 4, oleh karena itu *safety box* tetap dalam keadaan terkunci karena nilai ini tidak dapat memenuhi syarat teridentifikasi yang bernilai 7 poin kesamaan. Hal yang menyebabkan nilai ini kecil adalah citra uji tidak identik dengan citra pada *database*.

Pada hasil pengujian IV memiliki nilai poin kesamaan dengan nilai rata-rata 1, nilai yang sering muncul 0, nilai tertinggi 2 dan nilai terendah 0. Pada pengujian IV ini, *safety box* tidak dapat terbuka karena wajah tidak teridentifikasi sehingga solenoid tidak bisa membuka kunci pada *safety box*. Hal yang menyebabkan *safety box* tetap dalam keadaan terkunci adalah nilai poin kesamaan yang tidak dapat memenuhi syarat sebagai wajah yang teridentifikasi. nilai terbesar dari pengujian IV ini adalah 4, oleh karena itu *safety box* tetap dalam keadaan terkunci karena nilai ini tidak dapat memenuhi syarat teridentifikasi yang bernilai 7 poin kesamaan. Hal yang menyebabkan nilai ini kecil adalah citra uji tidak identik dengan citra pada *database*. Hasil ini sama dengan hasil pengujian III.

KESIMPULAN

Keberhasilan identifikasi wajah ini dilandaskan dengan persentasi tingkat pengenalan 50% dari 50 perbandingan data antara data uji dan *database* pada pengujian I dan memiliki persentasi 8% pada pengujian II karena pengujian I dan pengujian II menggunakan wajah yang saling identik dengan *database* dapat mencapai batasan nilai poin kesamaan identifikasi wajah yang bernilai ≥ 7 , sedangkan pada pengujian lainnya yaitu pengujian III dan pengujian IV memiliki persentasi identifikasi wajah 0% karena wajah yang tidak saling identik dengan *database*.

DAFTAR PUSTAKA

- [1] Bayu Setya, Hendriawan Akhmad dan Susetyoko Ronny. "Penerapan Face Recognition dengan Metode Eigenface dalam Intelligent Home Security", 2011.
- [2] Seprihahara. "Sistem Pengenalan Wajah (Face Recognition) Menggunakan Metode Hidden Markov Model (HMM)", 2012.
- [3] Shakhnarovich Geogory and Moghaddam Baback. "Face Recognition in Subspaces", 2011.
- [4] Stan Z Li and Anil K. Jain "Handbook of Face Recognition", 2011.
- [5] Rojas Q, Mario, David Masip, and Jordi Vitria. "Automatic Detection of Facial Feature Points via HOGs and Geometric Prior Models", 2010.
- [6] Ahti Noviatu Rahman Dwi. "Teknik Pengenalan Wajah dengan Algoritma PCA Berbasis Seleksi Eigenvector", 2011.
- [7] Mubarak, Shah. *Fundamentals of Computer Vision*, Orlando, 1997.
- [8] Hantoro Tan Felix, Indra Laksana Laksamana, Marcos H, Budiharto Widodo. "Pengembangan Sistem Absensi Face Recognition dengan Metode LDA", 2013
- [9] Anandito Rio. Pengolahan Citra untuk Peningkatan Visualisasi Citra Negatif Film Gigi x-ray Paranomik, 2012.
- [10] Putro, Dwisnanto, M. "Sistem Deteksi Wajah dengan Menggunakan Metode Viola-Jones", Seminar Nasional "Science, Engineering and Technology", 2012.
- [11] Gunawan Alexander A S, Gerardus Pascal, Gazali Wikaria. "Pendeteksian Rambu Lalu Lintas dengan Algoritma Speeded Up Robust Features (SURF)", 2013.
- [12] Geng Du, Fei Su and Anni Cai. *Face Recognition using SURF features*. Beijing, China, 2009.
- [13] Ditha Tania Ken. "Pengenalan Gambar Menggunakan Sebagian Data Gambar", 2010.