

**RANCANG BANGUN SISTEM PENGENALAN WAJAH
UNTUK AKSES LOGIN MENGGUNAKAN WEBCAM
DENGAN METODE *MINKOWSKI DISTANCE* BERBASIS
DESKTOP**

SKRIPSI

oleh:
MOCH. ILYAS FIQRI HABIBULLAH
NIM. 10650048



**JURUSAN TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2014**

**RANCANG BANGUN SISTEM PENGENALAN WAJAH
UNTUK AKSES LOGIN MENGGUNAKAN WEBCAM
DENGAN METODE *MINKOWSKI DISTANCE* BERBASIS
DESKTOP**

SKRIPSI

oleh:
MOCH. ILYAS FIQRI HABIBULLAH
NIM. 10650048



**JURUSAN TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2014**

**RANCANG BANGUN SISTEM PENGENALAN WAJAH UNTUK AKSES
LOGIN MENGGUNAKAN WEBCAM DENGAN METODE *MINKOWSKI*
DISTANCE BERBASIS DESKTOP**

SKRIPSI

**Diajukan kepada:
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
Untuk Memenuhi Salah Satu Persyaratan dalam
Memperoleh Gelar Sarjana Komputer (S.Kom)**

**Oleh:
MOCH. ILYAS FIQRI HABIBULLAH
NIM. 10650048**

**JURUSAN TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2014**

LEMBAR PERSETUJUAN

**RANCANG BANGUN SISTEM PENGENALAN WAJAH UNTUK AKSES
LOGIN MENGGUNAKAN WEBCAM DENGAN METODE *MINKOWSKI*
DISTANCE BERBASIS DESKTOP**

SKRIPSI

Oleh :

Nama : Moch. Ilyas Fiqri Habibullah

NIM : 10650048

Jurusan : Teknik Informatika

Fakultas : Sains dan Teknologi

Telah diperiksa dan disetujui untuk diuji :

Tanggal : 10 Juli 2014

Dosen Pembimbing I

Dosen Pembimbing II

Dr. Suhartono, M.Kom

Dr. Muhammad Faisal, M.T

NIP. 19680519 200312 1 001

NIP. 19740510 200501 1 007

Mengetahui,

Ketua Jurusan Teknik Informatika

Dr. Cahyo Crysdian

NIP. 19740424 200901 1 008

LEMBAR PENGESAHAN

**RANCANG BANGUN SISTEM PENGENALAN WAJAH UNTUK AKSES
LOGIN MENGGUNAKAN WEBCAM DENGAN METODE *MINKOWSKI*
DISTANCE BERBASIS DESKTOP
SKRIPSI**

Oleh :

Moch. Ilyas Fiqri Habibullah

NIM. 10650048

Telah dipertahankan di depan dewan penguji skripsi
dan dinyatakan diterima sebagai salah satu persyaratan
untuk memperoleh gelar sarjana komputer (S.Kom)

Tanggal : 9 September 2014

| Susunan Dewan Penguji: | Tanda Tangan |
|--|---------------------|
| 1. Penguji Utama : <u>Yunifa Miftachul Arif, M.T</u> NIP. 19830616 201101 1 004 | () |
| 2. Ketua Penguji : <u>Fachrul Kurniawan, M.MT</u> NIP. 19771020 200901 1 001 | () |
| 3. Sekretaris : <u>Dr. Suhartono, M.Kom</u> NIP. 19680519 200312 1 001 | () |
| 4. Anggota Penguji : <u>Dr. Muhammad Faisal, M.T</u> NIP. 19740510 200501 1 007 | () |

Mengetahui,
Ketua Jurusan Teknik Informatika

Dr. Cahyo Crysdiان

NIP. 19740424200901 1 008

PERSEMBAHAN

*Tidak Ada Daya dan Upaya, Melainkan Atas Kehendak,
Allah Semata*

*Kebaikan yang kita raih adalah semata-mata karena Ramat
dari Allah*

*Allhamdulillah Ku persembahkan kepada Allah Subhanahu wa Ta'ala atas
Berkat Rahmat dan Kasih Sayang-Nya, Sehingga skripsi ini terselesaikan.*

*Terima kasih kepada kedua orang tuaku (ABAH wa UMY) yang tak henti-
hentinya berdoa, memohon agar anaknya ini selalu diberi kesehatan dan
kelancaran dalam menjalankan studi.*

*Tak lupa kepada kedua adik-adikku (Muhammad Rifqi Ari Fullah dan Ahmad
Farhan Maulana Hasyim) yang memberikan keceriaan saat di rumah.*

Terima kasih guru-guruku, pembimbingku, dan teman-temanku.

*Terima kasih untuk pendamping setia yang selalu menemani, Calon Ibu dari
anak-anakku kelak, semoga menjadi penyejuk, pembawa keceriaan dalam
keluarga yang Sakinah, Mawaddah, wa Rohmah.*

Insyallah

MOTTO

خير الناس انفعهم لالناس

“Sebaik-baik Manusia

Adalah

*Yang Paling Bermanfaat Bagi
Manusia Lainnya”*

**HALAMAN PERNYATAAN
KEASLIAN PENELITIAN**

Saya yang bertandatangan di bawah ini:

Nama : Moch. Ilyas Fiqri Habibullah

NIM : 10650048

Fakultas/Jurusan : Sains dan Teknologi / Teknik Informatika

Judul Penelitian : *Rancang Bangun Sistem Pengenalan Wajah Untuk Akses Login Menggunakan Webcam Dengan Metode Minkowski Distance Berbasis Desktop*

Menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri, bukan merupakan pengambilan data, tulisan atau pikiran orang lain yang saya akui sebagai hasil tulisan atau pikiran saya sendiri, kecuali dengan mencantumkan sumber cuplikan pada daftar pustaka. Apabila dikemudian hari terbukti atau dapat dibuktikan skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, 16 September 2014
Yang membuat pernyataan,

Moch. Ilyas Fiqri Habibullah
NIM. 10650048

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Alhamdulillah rabbil 'Alamin penulis panjatkan kehadiran Allah Subhanahu wa Ta'ala yang telah memberikan Rohmat, Hidayah, dan Ridho-Nya, sehingga penulis dapat menyelesaikan studi di Jurusan Teknik Informatika Universitas Islam Negeri Maulana Malik Ibrahim Malang sekaligus menyelesaikan skripsi ini dengan baik dan lancar.

Selanjutnya penulis menghaturkan ucapan terima kasih kepada semua pihak yang telah memberikan doa, harapan, dan semangat untuk terselesaikannya skripsi ini. Ucapan terima kasih, penulis sampaikan kepada :

1. Prof. Dr. H. Mudjia Rahardjo, M.Si selaku rektor UIN Maulana Malik Ibrahim Malang, yang telah banyak memberikan pengetahuan dan pengalaman yang berharga.
2. Dr. drh. Hj. Bayyinatul Muchtaromah, M.Si selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Dr. Cahyo Crysdiand selaku ketua Jurusan Teknik Informatika Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Dr. Suhartono M.Kom dan Dr. Muhammad Faisal M.T selaku dosen pembimbing skripsi, yang telah banyak memberikan pengarahan dan pengalaman yang berharga.
5. Segenap civitas akademika jurusan Teknik Informatika, terutama seluruh dosen, terima kasih atas segenap ilmu dan bimbingannya.
6. Abah tercinta H. Achmad Hasyim dan Umy tercinta Hj. Siti Umilah yang senantiasa memberikan doa, semangat, tenaga, biaya, dan restunya kepada penulis dalam menuntut ilmu di kampus tercinta.
7. Semua pihak yang ikut membantu dalam menyelesaikan skripsi ini baik berupa materiil maupun moril.

Peneliti menyadari bahwa dalam penyusunan skripsi ini masih terdapat kekurangan dan peneliti berharap semoga skripsi ini bisa memberikan manfaat kepada para pembaca khususnya bagi peneliti secara pribadi. *Amin Ya Rabbal 'Alamin.*

Wassalamu'alaikum Wr. Wb.

Malang, 10 Juli 2014

Moch. Ilyas Fiqri Habibullah

DAFTAR ISI

| | |
|--|-------------|
| HALAMAN JUDUL | i |
| HALAMAN PENGAJUAN | ii |
| LEMBAR PERSETUJUAN | iii |
| LEMBAR PENGESAHAN | iv |
| HALAMAN PERSEMBAHAN | v |
| MOTTO | vi |
| HALAMAN PERNYATAAN..... | vii |
| KATA PENGANTAR..... | viii |
| DAFTAR ISI..... | ix |
| DAFTAR TABEL | xi |
| DAFTAR GAMBAR..... | xii |
| ABSTRAK | xiii |
| ABSTRACT | xiv |
| | |
| BAB I PENDAHULUAN | |
| 1.1 Latar Belakang..... | 1 |
| 1.2 Rumusan Masalah..... | 5 |
| 1.3 Tujuan Penelitian | 6 |
| 1.4 Manfaat Penelitian..... | 6 |
| 1.5 Batasan Masalah | 7 |
| 1.6 Sistematika Penulisan | 7 |
| | |
| BAB II TINJAUAN PUSTAKA | |
| 2.1 Definisi Wajah..... | 10 |
| 2.2 Login..... | 11 |
| 2.3 Webcam | 12 |
| 2.4 Image Processing | 15 |
| 2.5 Eigenface | 19 |
| 2.6 Minkowski Distance | 20 |
| 2.7 OpenCV | 21 |
| 2.8 Database..... | 23 |
| 2.9 Bahasa Pemrograman | 26 |
| 2.10 Penelitian Terkait..... | 29 |
| | |
| BAB III METODE PENELITIAN | |
| 3.1 Rancangan Penelitian..... | 33 |
| 3.1.1 Objek Penelitian | 35 |
| 3.1.2 Tahapan Penelitian | 36 |
| 3.1.3 Tempat dan Waktu | 37 |
| 3.1.4 Jenis Penelitian..... | 37 |
| 3.1.5 Sumber dan Jenis Data | 38 |
| 3.1.6 Metode Analisis/Penjelasan Data..... | 38 |

| | | |
|------------------------------------|--|-----------|
| 3.2 | Instrumen Penelitian | 39 |
| 3.3 | Kerangka Konsep..... | 39 |
| 3.4 | Rancangan Database..... | 45 |
| BAB IV HASIL DAN PEMBAHASAN | | |
| 4.1 | Perangkat Penelitian | 47 |
| | 4.1.1 Perangkat Keras..... | 47 |
| | 4.1.2 Perangkat Lunak..... | 48 |
| 4.2 | Implementasi Sistem..... | 48 |
| | 4.2.1 Interface Sistem..... | 48 |
| | 4.2.2 Implementasi Alur Program..... | 54 |
| | 4.2.3 Implementasi Minkowski Distance..... | 61 |
| 4.3 | Uji Coba Sistem..... | 63 |
| | 4.3.1 Analisis Data | 64 |
| | 4.3.2 Percobaan Login..... | 66 |
| 4.4 | Integrasi Islam | 73 |
| BAB V KESIMPULAN DAN SARAN | | |
| 5.1 | Kesimpulan..... | 79 |
| 5.2 | Saran | 79 |
| DAFTAR PUSTAKA | | 81 |
| LAMPIRAN..... | | 84 |

DAFTAR TABEL

| | |
|---|----|
| Tabel 2.1 Contoh Perhitungan Minkowski Distance | 21 |
| Tabel 3.1 Struktur Tabel Login..... | 45 |
| Tabel 3.2 Struktur Tabel Log | 46 |
| Tabel 3.3 Struktur Tabel View Datalog | 46 |
| Tabel 4.1 Contoh Citra Acuan | 65 |
| Tabel 4.2 Hasil Percobaan dengan Citra Acuan 75lux | 67 |
| Tabel 4.3 Hasil Percobaan dengan Citra Acuan 100lux | 69 |
| Tabel 4.4 Hasil Percobaan dengan Citra Acuan 200lux | 71 |



DAFTAR GAMBAR

| | |
|--|----|
| Gambar 3.1 Blok Diagram Sistem | 40 |
| Gambar 3.2 Alur Penyimpanan Data Template | 41 |
| Gambar 3.3 Alur Proses Pencocokan | 43 |
| Gambar 4.1 Tampilan PyQt4 | 49 |
| Gambar 4.2 Tampilan Form Login | 49 |
| Gambar 4.3 Tampilan Form Daftar | 50 |
| Gambar 4.4 Tampilan Form Admin | 51 |
| Gambar 4.5 Tampilan Form Tambah Akun | 52 |
| Gambar 4.6 Tampilan Form Data Log | 53 |
| Gambar 4.7 Tampilan Form Data Akun | 54 |
| Gambar 4.8 Pengecualian Pengisian Semua Baris Data | 55 |
| Gambar 4.9 Pengecualian Kesamaan Username | 56 |
| Gambar 4.10 Pilihan Ekspresi Wajah | 56 |
| Gambar 4.11 Hasil Simpan Gambar | 57 |
| Gambar 4.13 Tampilan Berhasil Login | 59 |
| Gambar 4.14 Tampilan Gagal Login | 60 |
| Gambar 4.15 Grafik Percobaan dengan Citra Acuan 75lux | 68 |
| Gambar 4.16 Grafik Percobaan dengan Citra Acuan 100lux | 70 |
| Gambar 4.17 Grafik Percobaan dengan Citra Acuan 200lux | 72 |

ABSTRAK

Habibullah, Moch. Ilyas Fiqri. 2014. **Rancang Bangun Sistem Pengenalan Wajah Untuk Akses Login Menggunakan Webcam Dengan Metode Minkowski Distance Berbasis Desktop.** Skripsi. Jurusan Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Pembimbing: (I) Dr. Suhartono M.Kom (II) Dr. Muhammad Faisal M.T

Kata Kunci: *Pengenalan Wajah, Minkowski Distance, Eigenface, OpenCV, Python, Login.*

Wajah adalah salah satu ciri biometrik pada manusia. Tidak ada satupun wajah yang sama di dunia ini meskipun ada kemiripan. Sehingga dibuatlah sistem pengenalan wajah untuk akses login menggunakan webcam dengan metode minkowski distance berbasis desktop. Sistem ini dibuat bertujuan untuk meningkatkan keamanan akun. Untuk mendapatkan akses login, maka pengguna tidak hanya memasukkan *username* dan *password* saja, namun juga dengan melakukan pencocokan wajah. Dengan menggunakan *minkowski distance*, maka sistem dapat mengenali wajah pengguna akun dengan melakukan perhitungan nilai jarak kemiripan.

Pada percobaan yang dilakukan dapat dijelaskan bahwa perbedaan intensitas cahaya mengakibatkan akurasi ketepatan yang berbeda. Akurasi terbaik didapatkan pada kondisi intensitas cahaya citra masukan dengan citra acuan adalah hampir sama.

ABSTRACT

Habibullah, Moch. Ilyas Fiqri. 2014. **Design and Build Face Recognition System For Login Access Using Webcam Implemented *Minkowski Distance Method Basic On Desktop***. *Thesis*. Department of Informatics, Faculty of Science and Technology, State Islamic University Maulana Malik Ibrahim Malang.

Promotor: (I) Dr. Suhartono, M.Kom
(II) Dr. Muhammad Faisal, M.T

Face is one of more human biometric characteristic. Nobody have same face in the world although somebody have resemble face. So the writer had made face recognition system for login access using webcam implemented minkowski distance method basic on desktop. This system has been made for increase security account. To get login access, user not only enter username and password, but also do face verification. Using minkowski distance, so system can identify face of user account with counting value of distance similarity.

On the experimentation, can be explained that difference of light intensity result in diffence of exact accuration. The best accuration of system is got from same condition of light intensity between input image and reference image.

Keywords: *Face Recognition, Minkowski Distance, Eigenface, OpenCV, Python, Login*

المجزة

حبيب الله، محمد إلياس فكري. ٢٠١٤. علم هندسة النظام تعرف الوجوه للدخول يستخدم الكاميرا بالطريقة مسافة Minkowski أساس أجهزة الكمبيوتر المكتبية. البحث. شعبة هندسة المعلوماتية، كلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج
المربي (١) الدكتور سهرطنا، الماجستير (٢) الدكتور محمد فيسل، الماجستير

الكلمات الرئيسية: تعرف الوجوه، مسافة Minkowski، Eigenface، OpenCV، Python، تسجيل

الوجوه هي في عداد الصفات خاصة على الانسان. لا شيء الوجوه مساو في هذا الدنيا رغم أن تشبه. لخلق علم هندسة النظام تعرف الوجوه للدخول يستخدم الكاميرا بالطريقة مسافة Minkowski أساس أجهزة الكمبيوتر مكتبية. هذا النظام خلق مقصود إلى تعزيز أمان المحاسبة. أن يحصل الانضمام الدخول، إذا كتيب لا فقط يدخل اسماء المستخدمين و كلمات السر سجع، لكن يركب أيضا. مع يستخدم مسافة Minkowski، إذا النظام يستطيع تحديد الوجوه من جانبه يحسب الدرجات مسافة التشابهات.
على بوتقة التي كان حمل يستطيع وصف أن فرق كشافة النور أفضى إلى دقة التي مختلف. أفضل دقة مكتشف على شروط كشافة النور مرئيات التقييمات مع مرئيات المزج هي تقريبا قريب.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Islam mengajarkan kepada pengikutnya untuk senantiasa menjaga apa yang telah Allah titipkan atau berikan di dunia. Nikmat berupa iman, kesehatan, badan, harta dan keluarga adalah segelintir contoh banyaknya pemberian nikmat dari Allah untuk kita jaga dan perlakukan sebaik-baiknya. Pemberian dari Allah tersebut adalah hak atau kebenaran untuk dimanfaatkan dan dipergunakan secara benar oleh orang yang mendapat karuniaNya. Sejatinya setiap manusia telah diberikan masing-masing haknya di dunia. Namun hakekat manusia yang memiliki nafsu yang mana tanpa dijaga oleh akalnya, dapat menjadikan manusia mengambil sesuatu yang bukan merupakan haknya.

Sebagaimana Allah melarang manusia mengambil yang bukan haknya dalam Al-Qur'an surah An-Nur ayat 27 yang berbunyi:

يٰۤاَيُّهَا الَّذِيْنَ ءَامَنُوْا لَا تَدْخُلُوْا بُيُوْتًا غَيْرَ بُيُوْتِكُمْ حَتّٰى تَسْتَأْذِنُوْا وَّتُسَلِّمُوْا عَلٰى
 اٰهْلِهَا ذٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُوْنَ ﴿٢٧﴾

Artinya: “Hai orang-orang yang beriman, janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Yang demikian itu lebih baik bagimu, agar kamu (selalu) ingat.” (QS. An-Nur:27)

Dari ayat tersebut telah jelas bahwa Allah melarang manusia untuk memasuki rumah yang bukan haknya tanpa mendapat izin dari orang yang berhak atas rumah tersebut. Begitu pula pada masa teknologi sekarang ini dalam kehidupan sehari-hari. Telah banyak aktifitas manusia sehari-hari yang berhubungan dengan data pribadi, keuangan, pekerjaan dan aktifitas lain yang menggunakan akses sistem komputer untuk menjalankannya. Maka diperlukan sebuah pengamanan akses pada masing-masing akun agar tidak disalahgunakan oleh sembarang orang. Hakekatnya, setiap manusia dilarang memasuki atau mengakses akun orang lain tanpa izin orang yang memilikinya. Karena akun tersebut juga merupakan hak setiap orang yang memilikinya.

Keamanan sebuah akun atau *account* adalah hal yang sangat penting. Untuk mengamankan sebuah akun, biasanya diberikan sebuah *username* dan *password*. *Username* dan *password* inilah yang digunakan untuk mengakses atau memanfaatkan akun tersebut.

Username adalah serangkaian nama unik (tidak boleh sama antara satu dengan yang lain) yang mengidentifikasi seseorang pada sistem komputer. Sedangkan *password* adalah kata sandi yang digunakan untuk membuktikan persetujuan identitas atau memperoleh akses dari sebuah sistem komputer yang harus dirahasiakan dari mereka yang tidak diperbolehkan untuk mengaksesnya. Penggunaan *password* sebenarnya telah digunakan pada peradaban kuno yang mana pada zaman itu terdapat penjaga dalam suatu daerah yang akan menantang dan memberikan ujian kepada orang atau sekelompok orang yang ingin masuk. Mereka akan memperbolehkan seseorang untuk masuk apabila mengetahui

password atau kata sandinya. Pada zaman modern ini, *password* atau kata sandi digunakan untuk mengakses ke dalam sistem komputer yang terlindungi. Sehingga dengan mengetahui *password* tersebut, maka pengguna dapat mendapatkan akses untuk masuk ke dalam sistem.

Hakekatnya sebuah *password* diciptakan untuk mengamankan akun seorang pengguna. Namun biasanya *password* yang digunakan terlalu lemah atau menggunakan karakter yang sama pada setiap akun yang dimiliki sehingga menjadi rentan terhadap pembajakan. Ilmuwan komputer dari Inggris menyebut Indonesia menjadi negara yang menggunakan *password* paling mudah ditebak.

Seperti yang dilansir oleh *Daily Mail*, Josep Bonneau, ilmuwan komputer dari Universitas Cambridge, Inggris, melakukan penelitian terhadap 69,3 juta sampel pengguna akun situs Yahoo! di berbagai negara termasuk Indonesia. Setelah dianalisis, Bonneau mengklaim bahwa 15% dari kata *password* yang digunakan pemilik akun Yahoo! di Indonesia lebih mudah ditebak hanya dengan menggunakan bahasa lokal yang sama. Bonneau menyatakan pula bahwa dibandingkan pengguna komputer berusia muda, ternyata pengguna berusia lanjut, atau yang berada di atas 55 tahun, justru memiliki *password* yang lebih kuat. Untuk itu, masih menurut Bonneau, penggunaan *password* yang memiliki kombinasi lebih sulit diperlukan untuk menjaga akun mereka. Selain itu penggantian password secara rutin juga akan membuat akunnya lebih terproteksi. Hal ini mungkin merepotkan bagi sebagian orang bila setiap saat tertentu harus rutin mengganti password demi keamanan akun yang dimilikinya (Bonneau Josep, 2012).

Oleh karena kemungkinan pembobolan akun tersebut, maka penulis tertarik mengajukan solusi dari permasalahan di atas dengan menambahkan pengenalan wajah pada saat melakukan *login* ke dalam sebuah akun. Pengenalan Wajah yang merupakan salah satu ciri biometrik telah banyak dikembangkan untuk sistem yang mendukung aspek keamanan (Marito, 2010). Pengenalan wajah ini menggunakan metode *minkowski distance* untuk mencocokkan wajah pengguna. Metode ini dipilih karena merupakan salah satu metode yang berfungsi untuk mencocokkan atau mengukur jarak kemiripan dari suatu citra masukan dengan citra yang menjadi *template* atau acuan.

Diharapkan dari pembuatan sistem ini dapat meningkatkan keamanan sebuah akun agar tidak mudah dibajak oleh orang lain. Dengan menambahkan pengenalan wajah pengguna, maka pengguna lain tidak hanya memasukkan username dan password saja, namun juga harus ada masukan citra wajah pada saat *login*.

Allah berfirman dalam surah Al-Muthaffifin ayat 24 yang berbunyi:

تَعْرِفُ فِي وُجُوهِهِمْ نَضْرَةَ النَّعِيمِ

Artinya: “Kamu dapat mengetahui dari wajah mereka kesenangan mereka yang penuh kenikmatan.”(QS. Al-Muthaffifin:24)

Dari ayat diatas menunjukkan bahwa wajah memiliki identitas. Setiap wajah memiliki karakteristik yang berbeda pada manusia. Hal inilah yang menuntun penulis untuk membuat Rancang Bangun Sistem Pengenalan Wajah Untuk Akses Login Menggunakan Webcam Dengan Metode Minkowski Distance Berbasis Desktop untuk mengidentifikasi wajah dari pengguna sebuah akun.

Metode yang digunakan dalam mencocokkan wajah adalah dengan menggunakan metode *minkowski distance*. Penggunaan metode *minkowski distance* adalah untuk mencari kemiripan dua buah citra yaitu citra yang menjadi masukan dan citra yang menjadi template atau acuan.

Bahasa pemrograman yang digunakan untuk membangun aplikasi adalah dengan menggunakan bahasa pemrograman *python*. *Python* adalah bahasa pemrograman multiguna dengan filosofi perancangan yang berfokus pada tingkat keterbacaan kode. *Python* diklaim sebagai bahasa yang menggabungkan kapabilitas, kemampuan dengan sintaksis kode yang sangat jelas, dan dilengkapi dengan fungsionalitas pustaka standar yang besar serta komprehensif.

Kedepannya diharapkan penelitian ini dapat memberikan manfaat untuk meningkatkan keamanan sebuah akun menjadi lebih baik lagi dari pada hanya menggunakan username dan password saja untuk melakukan login. Serta dapat dikembangkan dengan membuat sistem-sistem baru yang memiliki tingkat akurasi tinggi dalam mendeteksi dan mengenali wajah.

1.2 Rumusan Masalah

Bagaimana merancang dan membangun sistem yang dapat mengenali wajah seseorang menggunakan alat pengambil gambar *webcam* untuk digunakan sebagai akses *login* menggunakan metode *minkowski distance* sebagai metode pengenalan wajah berbasis aplikasi *desktop*?

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah:

1. Menerapkan dan mengimplementasikan metode *minkowski distance* ke dalam sistem dengan bahasa pemrograman *python*
2. Membangun sistem yang dapat mendeteksi dan mengenali wajah menggunakan webcam sebagai syarat untuk mendapatkan akses login ke dalam sistem.
3. Menambahkan pengenalan wajah pada sistem untuk akses login

1.4 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Bagi Peneliti
Meningkatkan kualitas pengetahuan di bidang ilmu pengolahan citra digital dan menambah pengetahuan dalam membangun aplikasi berbasis desktop menggunakan bahasa pemrograman *python*.
2. Bagi Pengembang Sistem Lain
Menjadi salah satu tambahan referensi dalam mengembangkan sistem dengan pengenalan wajah untuk akses *login* ke dalam sistem menggunakan bahasa pemrograman *python* dan library *OpenCV*.
3. Bagi Pengguna Sistem
Dapat menambahkan rasa aman kepada pengguna sistem dengan ditambahkan pengenalan wajah untuk akses *login* ke dalam sistem dan merupakan salah satu upaya untuk mengurangi pembobolan akun.

1.5 Batasan Masalah

Adapun batasan masalah pada penelitian ini adalah:

1. Kamera yang digunakan beresolusi standar VGA yang terpasang pada perangkat komputer laptop.
2. Intensitas pencahayaan yang digunakan sebesar 75lux, 100lux dan 200lux pada saat memasukkan data maupun proses *login*
3. Wajah pengguna tidak membelakangi kamera pada saat *login*.
4. Sistem hanya menangani masalah akses *login*.
5. Jarak *webcam* dengan wajah pada saat *login* sebesar 50cm

1.6 Sistematika Penulisan

Sebagai gambaran pembahasan pada penelitian ini, perlu diberikan perincian sistematika penulisan dalam laporan penelitian ini. Berikut gambaran sistematika penulisan pada laporan ini:

BAB I PENDAHULUAN

Bab ini berisi Latar Belakang, Rumusan masalah, Tujuan Penelitian, Manfaat Penelitian, Batasan Masalah dan Sistematika Penulisan laporan skripsi. Bab ini menjelaskan masalah yaitu keamanan akun yang melatarbelakangi dilakukannya penelitian ini kemudian dijelaskan pemberian solusi dari permasalahan tersebut yaitu dengan penambahan pengenalan wajah pada saat *login* untuk memperoleh hak akses akun.

BAB II TINJAUAN PUSTAKA

Bab ini berisi penjelasan teori-teori yang ada kaitannya atau berhubungan dengan penelitian yang dilakukan. Teori tersebut meliputi alat atau sarana yang akan digunakan dalam penelitian seperti *webcam*, bahasa pemrograman *python*, *library openCV* dan lain sebagainya. Selain itu dijelaskan pula mengenai metode yang digunakan pada penelitian ini yaitu metode *minkowski distance* yang merupakan metode untuk melakukan pencocokan pada wajah pada saat melakukan login.

BAB III METODE PENELITIAN

Bab ini menguraikan secara lebih rinci metode-metode yang digunakan dalam penelitian. Dijelaskan pula alasan mengapa memilih metode tersebut dalam penelitian ini. Metode tersebut meliputi pemilihan alat yang digunakan dalam penelitian serta langkah-langkah yang diterapkan. Langkah-langkah dalam penelitian dijelaskan secara lebih rinci bagaimana alur sistem bekerja. Mulai dari mendesain tampilan sistem, database, masukan yang digunakan dan sampai pada keluaran sistem yaitu berupa pengambilan keputusan oleh sistem.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini dijelaskan hasil dari penelitian yang dilakukan. Dilakukan pengujian pada sistem yang telah dibuat sehingga menghasilkan perhitungan akurasi ketepatan pengenalan wajah oleh sistem. Pengujian dilakukan pada

bentuk wajah yang berbeda-beda. Selain itu sistem diuji dengan membandingkan citra acuan dengan beberapa citra yang berbeda. Kemudian dijelaskan dan dibahas secara rinci hasil dari pengujian sistem tersebut.

BAB V KESIMPULAN DAN SARAN

Pada bab ini dijelaskan kesimpulan yang diambil setelah dilakukan pengujian pada penjelasan bab sebelumnya serta saran untuk perbaikan pada pengembangan sistem selanjutnya.



BAB II

TINJAUAN PUSTAKA

2.1 Definisi Wajah

Menurut kamus besar bahasa Indonesia, pengertian wajah atau muka adalah bagian depan dari kepala, pada manusia meliputi wilayah dari dahi hingga dagu, termasuk rambut, dahi, alis, mata, hidung, pipi, mulut, bibir, gigi, kulit, dan dagu (Badan Pengembangan dan Pembinaan Bahasa, 2014). Tidak ada satupun wajah di dunia ini yang serupa mutlak, meskipun pada kembar identik sekalipun.

Allah menciptakan manusia berbeda-beda antara satu dengan yang lainnya. Sebagaimana firmanNya surah Al-Hujurat ayat 13:

يٰۤاَيُّهَا النَّاسُ اِنَّا خَلَقْنٰكُمْ مِّنْ ذَكَرٍ وَّاُنْثٰى وَجَعَلْنٰكُمْ شُعُوْبًا وَّقَبَاۤىِٕلٍ لِتَعَارَفُوْۤا ۗ اِنَّ اَكْرَمَكُمْ عِنْدَ اللّٰهِ اَتْقٰىكُمْ ۗ اِنَّ اللّٰهَ عَلِيْمٌ خَبِيْرٌ ﴿١٣﴾

Artinya: “Hai manusia, Sesungguhnya Kami menciptakan kamu dari seorang laki-laki dan seorang perempuan dan menjadikan kamu berbangsa - bangsa dan bersuku-suku supaya kamu saling kenal-mengenal. Sesungguhnya orang yang paling mulia diantara kamu disisi Allah ialah orang yang paling taqwa diantara kamu. Sesungguhnya Allah Maha mengetahui lagi Maha Mengenal.” (QS. Al-Hujurat:13)

Ayat di atas menjelaskan bahwa manusia memang diciptakan berbeda antara satu dengan yang lainnya agar saling mengenal. Memberikan penjelasan pula bahwa perbedaan di antara manusia itu adalah rahmat atau kemudahan yang Allah berikan. Perbedaan seperti halnya berbeda wajah, berbeda sidik jari, berbeda iris

mata, berbeda warna kulit, berbeda suara, berbeda bahasa dan sebagainya. Dapat dibayangkan apabila semua manusia memiliki ciri-ciri yang sama. Maka manusia tidak dapat membedakan antara satu dengan yang lainnya. Manusia tidak akan memiliki identitas yang melekat kepada dirinya. Salah satu contoh identitas yang telah disebutkan sebelumnya adalah wajah.

Wajah adalah salah satu dari ciri biometrik pada diri manusia sebagai identitas yang melekat pada orang yang memilikinya. Terdapat elemen-elemen penentu terbentuknya wajah seperti bentuk mata, alis, hidung, mulut dan elemen-elemen lain yang semua itu membentuk sebuah pola yang kemudian dinamakan wajah.

2.2 *Login*

Login adalah proses untuk mengakses komputer dengan memasukkan identitas pengguna baik berupa *username*, *password* atau data lain guna mendapatkan hak akses menggunakan sumber daya komputer tujuan (Ismail, 2012). *Username* dan *password* sering digunakan untuk memperoleh hak akses akun atau disebut dengan *login*.

Username adalah susunan karakter yang menggambarkan identitas pemilik akun. Pemilik akun memiliki kebebasan dalam menentukan karakter untuk menjadi *username*. Biasanya *username* adalah nama dari pengguna akun tersebut. *Password* adalah susunan karakter yang menjadi sandi untuk memperoleh akses *login*. Susunan karakter *password* hampir sama dengan *username* yaitu bebas ditentukan

oleh pengguna. Namun *password* bersifat rahasia dan tidak boleh diberikan kepada orang lain. Karena *password* merupakan syarat untuk memperoleh hak akses akun.

Dalam penelitian ini ditambahkan pengenalan wajah pengguna menggunakan webcam pada saat login. Sehingga terdapat 3 masukan dari pengguna pada saat login yaitu *username*, *password* dan citra wajah. Citra wajah dimasukkan ke dalam sistem dengan diambil menggunakan *webcam*. *Webcam* menghasilkan citra yang kemudian menjadi masukan untuk dicocokkan dengan citra acuan. Citra masukan harus sama dengan citra acuan atau memiliki kemiripan sehingga akses *login* dapat diberikan. Apabila perbandingan kedua citra menghasilkan perbedaan yang besar, maka akses *login* tidak akan diberikan.

2.3 Webcam

Dikutip dari situs Internet dan Teknologi bahwa pengertian dari *webcam* atau kamera web adalah sebutan bagi kamera *real-time* (berarti keadaan pada saat ini) yang gambarnya dapat diakses atau dilihat melalui *world wide web*. *Webcam* adalah perangkat berupa kamera sebagai pengambil citra/gambar yang dikendalikan oleh sebuah komputer atau oleh jaringan komputer (<http://id.shvoong.com>, 2014).

Menurut salah satu situs edukasi, (<http://idkf.bogor.net/yuesbi/e-DU.KU/edukasi.net/>, 2014), bahwa jenis-jenis *webcam* dibagi atas:

1. *Serial and Parallel port Webcam*

Webcam jenis ini sudah jarang ditemukan lagi karena sudah tidak ada yang memproduksi dan jauh tertinggal di masa sekarang ini. Selain itu, kamera jenis ini menghasilkan kualitas gambar yang rendah atau kurang jelas

dan *frame rate* yang rendah pula. Kamera jenis ini tidak akan mampu untuk digunakan mendeteksi wajah atau bahkan mengenali wajah.

2. USB Webcam

Webcam jenis ini merupakan solusi bagi pengguna baru atau amatir yang biasa digunakan untuk melakukan *chatting* atau *video call* dalam dunia internet. Mendukung fasilitas PnP (*Plug and Play*) dan dapat dihubungkan ke *port* USB tanpa harus mematikan komputer, namun syaratnya sistem operasi komputer harus mendukung fasilitas USB *port*. Namun dirasa sistem komputer saat ini telah banyak yang mendukung fasilitas USB *port*.

3. Firewire and Card Based Webcam

Firewire adalah salah satu teknologi *video capture device* yang diperlukan bagi kamera yang mendukungnya. *Webcam* jenis ini sering digunakan untuk menangkap video dengan kualitas yang cukup baik seperti penggunaan pada CCTV untuk merekam kejadian di depan kamera secara *real time* dan terus-menerus. Pada umumnya *Webcam* yang membutuhkan *video capture device* harganya mahal, akan tetapi dapat menghasilkan *frame rate* tinggi, yaitu 24 sampai 30 *frame per second* (*fps*).

4. Network and Wireless Camera

Network Camera adalah perangkat kamera yang tidak memerlukan sama sekali fasilitas komputer untuk mengontrol kamera dan tidak menggunakan media kabel sebagai penghubung, karena kamera jenis ini dapat langsung terhubung ke jaringan melalui *modem* dengan koneksi *wireless*. Pengiriman gambar dan suara langsung menuju jaringan LAN atau

jaringan telepon menggunakan *modem* yang terpasang pada perangkat kamera.

Bagian serta kelengkapan dari perangkat *Webcam* (<http://idkf.bogor.net/yuesbi/e-DU.KU/edukasi.net/>, 2014).

Webcam terdiri atas sebuah lensa, sirkuit elektronik dan sensor gambar. Sensor gambar tersebut dapat berupa CCD dan CMOS. Selain itu *Webcam* pada umumnya juga dilengkapi dengan berbagai peralatan tambahan untuk mendukung kerja yang maksimal atau mempermudah penggunaan *webcam* oleh pengguna. Berikut adalah beberapa perangkat tambahan tersebut:

1. Kabel Data

Kabel data adalah sebuah kabel yang dapat menghubungkan komputer dengan *webcam* maupun jenis perangkat *periferal* lainnya sebagai media pengiriman data. Namun pada jenis *wireless webcam* tidak menggunakan kabel data sebagai media pengiriman data.

2. Tombol Snapshot

Tombol ini dipergunakan untuk mengambil gambar serta untuk menyimpannya ke dalam bentuk citra.

3. Pengaturan Fokus

Pada beberapa *webcam* dilengkapi dengan pengaturan fokus. Ini digunakan untuk pengaturan fokus lensa agar gambar yang dihasilkan lebih jelas dan terfokus.

4. Lensa Kamera

Tentu saja sebuah *webcam* harus dilengkapi lensa kamera. Lensa di sini mewakili fungsi seperti mata manusia yang digunakan untuk melakukan pengambilan video ataupun gambar.

2.4 *Image Processing*

Mengutip dari pernyataan Jain (1989), seorang profesor dari jurusan Ilmu Komputer dan Teknik di Universitas Michigan, beliau menyatakan bahwa *Image processing* atau pengolahan citra adalah proses pengolahan gambar berbentuk dua dimensi oleh perangkat komputer digital. Sedangkan proses pengambilan atribut-atribut berupa gambar dengan *input* dan *output* yang juga berupa gambar adalah merupakan pengertian *image processing* menurut Gonzalez dan Woods (2001) yang merupakan penulis buku *Digital Image Processing*.

Image processing adalah suatu proses mengolah dan menganalisis citra atau gambar yang banyak melibatkan persepsi visual. Proses tersebut mempunyai ciri data masukan atau *input* dan informasi keluaran atau *output* yang berbentuk citra dengan citra keluaran mempunyai kualitas lebih baik dari citra masukan (Munir, 2004).

Dari pengertian *image processing* menurut beberapa pakar di atas, maka dapat disimpulkan bahwa *image processing* adalah suatu proses memperbaiki atau mengubah atribut-atribut citra dengan masukan berupa citra dan dengan keluaran yang juga berupa citra sehingga menghasilkan citra baru yang sesuai dengan proses yang dilakukan.

Jenis-jenis Pengolahan Citra (Yang Jianwei, dkk., 2003)

1. Perbaikan Citra (*Image Restoration*)

Jenis ini bertujuan untuk memperbaiki bagian-bagian dari citra yang kurang sesuai untuk ditingkatkan kualitasnya sehingga menjadi lebih baik.

Contoh-contoh operasi perbaikan citra:

- a. Perbaikan kontras gelap/terang
- b. Perbaikan tepian objek (*edge enhancement*)
- c. Penajaman (*sharpening*)
- d. Pemberian warna semu (*pseudocoloring*)
- e. Penapisan derau (*noise filtering*)

2. Peningkatan Kualitas Citra (*Image Enhancement*)

Peningkatan kualitas citra adalah pemrosesan sebuah citra yang ditujukan untuk menghasilkan kondisi tertentu pada citra, metode yang dapat dilakukan berbeda-beda tergantung pada citra yang akan diproses serta kondisi yang diharapkan.

Tujuan dari teknik peningkatan kualitas citra adalah untuk melakukan pemrosesan terhadap citra agar hasilnya mempunyai kualitas yang relatif lebih baik dari citra awal. Baik di sini memiliki pengertian bahwa peningkatan kualitas yang sesuai dengan keinginan.

3. Registrasi Citra (*Image Registration*)

Registrasi Citra adalah proses penempatan objek berupa raster atau image citra yang belum mempunyai acuan sistem koordinat ke dalam sistem koordinat dan proyeksi tertentu.

Registrasi citra terdiri dari dua tahap proses, yaitu :

- a. *Spatial Transformation* yang merupakan pemetaan letak piksel yang dikoreksi pada bidang citra acuan.
- b. *Gray-level Interpolation* yang merupakan pemberian nilai intensitas piksel sesuai dengan nilai intensitas piksel bersangkutan, dan pemberian nilai intensitas piksel-piksel yang kosong berdasarkan interpolasi intensitas piksel-piksel yang berdekatan / tetangga (*nearest neighbour method*).

4. Pemampatan Citra (*Image Compression*)

Pemampatan citra adalah proses meminimasi jumlah bit yang diperlukan untuk merepresentasikan suatu citra digital atau aplikasi kompresi data yang dilakukan terhadap citra digital dengan tujuan untuk mengurangi redundansi dari data-data yang terdapat dalam citra sehingga dapat disimpan atau ditransmisikan secara efisien. Tujuan dari proses ini adalah agar citra keluaran yang dihasilkan jumlah bitnya berukuran lebih kecil dari citra masukan sehingga mempermudah dan mempercepat proses pengiriman citra. Namun dengan proses ini biasanya juga mengurangi kualitas dari citra itu sendiri. Penggunaan teknik yang tepat dapat mengurangi ukuran bit citra tanpa harus mengurangi kualitas dari citra itu sendiri.

5. Pemilahan Citra (*Image Segmentation*)

Pemilahan citra adalah suatu proses yang membagi-bagi sebuah citra menjadi unsur-unsur pokok dari citra itu sendiri. Pemilahan citra (*image segmentation*) bertujuan untuk memilih dan mengisolasi (memisahkan)

suatu objek dari keseluruhan citra untuk diambil objek tertentu yang menggambarkan keseluruhan citra itu sendiri.

Secara umum, proses Pemilahan citra (*image segmentation*) terbagi menjadi tiga kelompok :

- a. Segmentasi berdasarkan klasifikasi (*classification based segmentation*) yaitu dapat berupa klasifikasi warna, bentuk tertentu dan sebagainya.
- b. Segmentasi berdasar daerah tepi (*edge based segmentation*) yaitu dibedakan berdasarkan batas tepi dari perbedaan unsur citra dalam suatu gambar sehingga membentuk suatu pola garis.
- c. Segmentasi berdasar daerah (*region based segmentation*) yaitu dibedakan berdasarkan daerah citra dengan unsur citra yang sama pada sebuah gambar.

Pemilahan citra pada penelitian ini digunakan untuk memilah citra wajah pada saat pengambilan citra menggunakan *webcam*. Pemilahan citra tersebut menggunakan *library openCV* untuk menghasilkan hanya citra wajah saja yang akan diproses dalam tahap selanjutnya oleh sistem. Secara otomatis sistem akan memotong bagian citra yang dideteksi sebagai wajah, kemudian dijadikan masukan oleh sistem. Baik itu masukan sebagai citra acuan atau masukan sebagai citra ketika pengguna akan *login*.

6. Pengenalan Citra (Image Recognition)

Pengenalan citra adalah teknik pengenalan suatu pola tertentu pada citra sesuai dengan aturan-aturan tertentu yang diinginkan. Pola tersebut dapat berupa unsur tertentu seperti warna, bentuk dan sebagainya.

Dalam proses ini, sistem diprogram untuk dapat mengenali pola-pola tertentu yang ada pada citra. Seperti halnya pada kamera digital yang dapat mengenali pola senyuman, pola wajah dan sebagainya.

Pada penelitian ini, proses pengenalan citra digunakan untuk mengenali pola bentuk wajah pengguna akun untuk dijadikan sebagai akses *login*.

2.5 *Eigenface*

Algoritma atau algoritme dalam kamus besar bahasa Indonesia adalah urutan-urutan logis dari intruksi atau langkah untuk pengambilan keputusan dalam pemecahan masalah (Badan Pengembangan dan Pembinaan Bahasa, 2014). Sedangkan kata *eigenfaces* berasal dari bahasa jerman "*eigenwert*" dimana "*eigen*" artinya karakteristik dan "*wert*" artinya nilai. *Eigenface* adalah salah satu algoritma *vector* pengenalan wajah yang berdasarkan pada (*Principle Component Analysis*) PCA yang dikembangkan di Massachuset Institueb of Thecnology (MIT). *Principle Component Analysis* (PCA) sering juga disebut sebagai metode Karhunen - Loeve yang secara matematis dilakukan dengan mencari *vector eigen* dari metrik kovarian sekumpulan citra wajah. *Eigenface* juga merupakan kumpulan dari *eigenvector* yang digunakan

untuk masalah *computer vision* pada pengenalan wajah manusia (Hanif, 2009).

Prinsip dasar dari pengenalan wajah adalah dengan mengutip informasi unik wajah tersebut kemudian di-*encode* dan dibandingkan dengan hasil *decode* yang sebelumnya dilakukan. Dalam metode *eigenface*, *decoding* dilakukan dengan menghitung *eigenvector* kemudian direpresentasikan dalam matrik yang berukuran besar. *Eigenvector* juga dinyatakan sebagai karakteristik wajah oleh karena itu metode ini disebut dengan *eigenface*. Setiap wajah direpresentasikan dalam kombinasi *linear eigenface*. Prinsip dasar dari metode *eigenface* adalah bagaimana caranya untuk mengekstrak informasi yang relevan dari sebuah citra wajah lalu mengubahnya ke dalam satu set kode yang paling efisien, dan membandingkan kode wajah ini dengan database berisi beragam wajah yang telah dikodekan secara serupa (Semuil, 2011).

Untuk menghasilkan *eigenface*, sekumpulan citra digital dari wajah manusia diambil pada kondisi pencahayaan yang sama kemudian diproses pada resolusi yang sama (misal $a \times b$), kemudian citra tadi diperlakukan sebagai vektor dimensi $a \times b$ dimana komponennya diambil dari nilai piksel citra (Dewi, 2012).

2.6 *Minkowski Distance*

Kemiripan dua buah citra dapat dihitung dengan jarak. Semakin mirip dua buah citra maka semakin kecil jaraknya. Begitu pula sebaliknya. Semakin

berbeda dua buah citra, maka jaraknya semakin besar. Untuk menghitung kemiripan dua buah citra, digunakan perhitungan *minkowski distance*.

Minkowski distance adalah sebuah metrik pada ruang *euclidean* yang mana merupakan generalisasi dari jarak *euclidean* dan jarak *manhattan*.

Rumus dari *Minkowski Distance* adalah:

$$dist = \left(\sum_{k=1}^n |p_k - q_k|^r \right)^{\frac{1}{r}}$$

Tabel 2.1 Contoh Perhitungan Minkowski Distance

| | Biaya | Waktu | Berat | Insentif |
|---------|-------|-------|-------|----------|
| Objek A | 0 | 3 | 4 | 5 |
| Objek B | 7 | 6 | 3 | -1 |

Titik A dengan koordinat {0,3,4,5} dan titik B dengan koordinat {7,6,3,-1}

Maka perhitungan *minkowski distance* dari kedua titik tersebut dengan $r=3$ adalah:

$$\begin{aligned} d_{BA} &= \left(|0-7|^3 + |3-6|^3 + |4-3|^3 + |5+1|^3 \right)^{\frac{1}{3}} \\ &= \sqrt[3]{343 + 27 + 1 + 216} = \sqrt[3]{587} = 8.373 \end{aligned}$$

2.7 OpenCV

Open Source Computer Vision library adalah library open source multi platform berlisensi BSD (Berkeley Software Distribution) yang bersifat gratis

untuk digunakan baik di kegiatan akademik maupun komersial. OpenCV adalah library Open Source untuk Computer Vision untuk C/C++, namun juga terdapat library yang memungkinkan openCV digunakan menggunakan bahasa pemrograman python. OpenCV didesain untuk aplikasi real-time, memiliki fungsi-fungsi akuisisi yang baik untuk image/video. OpenCV juga menyediakan interface ke Integrated Performance Primitives (IPP) Intel sehingga bisa mengoptimasi aplikasi Vision jika menggunakan prosesor Intel (Krisna Gunawan. 2013).

Fitur-fitur yang dimiliki OpenCV antara lain :

- Manipulation data citra (alokasi, copying, setting, konversi).
- Citra dan video I/O (file dan kamera based input, image/video file output).
- Manipulasi Matriks dan Vektor beserta rutin-rutin aljabar linear (products, solvers, eigenvalues, SVD).
- Data struktur dinamis (lists, queues, sets, trees, graphs).
- Pemroses Citra fundamental (filtering, edge detection, corner detection, sampling and interpolation, color conversion, morphological operations, histograms, image pyramids).
- Analisis struktur (connected components, contour processing, distance transform, various moments, template matching, Hough transform, polygonal approximation, line fitting, ellipse fitting, Delaunay triangulation).

- Kalibrasi kamera (calibration patterns, estimasi fundamental matrix, estimasi homography, stereo correspondence).
- Analisis gerakan (optical flow, segmentation, tracking).
- Pengenalan obyek (eigen-methods, HMM).
- Graphical User Interface (display image/video, penanganan keyboard dan mouse handling, scroll-bars).
- Pelabelan citra (line, conic, polygon, text drawing)
OpenCV juga terdiri dari 3 library, yaitu:
 - CV : untuk algoritma Image processing dan Vision
 - Highgui : untuk GUI, Image dan Video I/O
 - CXCORE : Untuk struktur data, support XML dan fungsi-fungsi grafis (Kristanto, 2012).

2.8 Database

Pengertian Database

Menurut jurnal ilmiah yang dikeluarkan oleh Reva Siti Ardhiva bahwa pengertian *database* atau basis data adalah kumpulan data yang disimpan secara sistematis atau teratur di dalam komputer dan dapat diolah, diproses atau dimanipulasi menggunakan perangkat lunak (program aplikasi) tertentu untuk menghasilkan suatu informasi. Konsep dasar database adalah kumpulan dari catatan, atau potongan dari pengetahuan. Sebuah database memiliki penjelasan terstruktur dari jenis fakta yang tersimpan di dalamnya: penjelasan ini disebut skema. Ada banyak cara untuk mengorganisasi skema,

atau memodelkan struktur database: ini dikenal sebagai database model atau model data (Reva Siti Ardhiva, 2014).

Model yang umum digunakan sekarang adalah model relasional, yang menurut istilah yaitu mewakili semua informasi dalam bentuk tabel yang saling berhubungan dimana setiap tabel terdiri dari baris dan kolom (definisi yang sebenarnya menggunakan terminologi matematika). Dalam model ini, hubungan antar tabel diwakili dengan menggunakan nilai yang sama antar tabel (Hansen, dkk., 1996).

Dilihat dari jenisnya, basis data dibagi menjadi dua yaitu:

1. Basis data *flat-file*. Basis data *flat-file* ideal untuk data berukuran kecil dan dapat diubah dengan mudah. Pada dasarnya, *database* ini tersusun dari sekumpulan *string* dalam satu atau lebih *file* yang dapat diurai untuk mendapatkan informasi yang disimpan. Basis data *flat-file* baik digunakan untuk menyimpan daftar atau data yang sederhana dan dalam jumlah kecil. Basis data *flat-file* akan menjadi sangat rumit apabila digunakan untuk menyimpan data dengan struktur kompleks walaupun dimungkinkan pula untuk menyimpan data semacam itu. Salah satu masalah menggunakan basis data jenis ini adalah rentan pada korupsi data karena tidak adanya penguncian yang melekat ketika data digunakan atau dimodifikasi.
2. Basis data relasional. Basis data ini mempunyai struktur yang lebih logis terkait cara penyimpanan. Kata "relasional" berasal dari kenyataan bahwa tabel-tabel yang berada di basis data dapat dihubungkan satu

dengan lainnya. Basis data relasional menggunakan sekumpulan tabel dua dimensi yang masing-masing tabel tersusun atas baris (tupel) dan kolom (atribut). Untuk membuat hubungan antara dua atau lebih tabel, digunakan key (atribut kunci) yaitu *primary key* di salah satu tabel dan *foreign key* di tabel yang lain. Saat ini, basis data relasional menjadi pilihan karena keunggulannya. Beberapa kelemahan yang mungkin dirasakan untuk basis data jenis ini adalah implementasi yang lebih sulit untuk data dalam jumlah besar dengan tingkat kompleksitasnya yang tinggi dan proses pencarian informasi yang lebih lambat karena perlu menghubungkan tabel-tabel terlebih dahulu apabila datanya tersebar di beberapa tabel (McLeod, dkk., 1998).

Proses memasukkan dan mengambil data ke dan dari media penyimpanan data memerlukan perangkat lunak yang disebut dengan sistem manajemen basis data (*database management system* | DBMS). DBMS merupakan sistem perangkat lunak yang memungkinkan user untuk memelihara, mengontrol, dan mengakses data secara praktis dan efisien. Dengan kata lain semua akses ke basis data akan ditangani oleh DBMS. Ada beberapa fungsi yang harus ditangani DBMS yaitu mengolah pendefinisian data, dapat menangani permintaan pemakai untuk mengakses data, memeriksa sekuriti dan integriti data yang didefinisikan oleh DBA (*Database Administrator*), menangani kegagalan dalam pengaksesan data yang

disebabkan oleh kerusakan sistem maupun disk, dan menangani unjuk kerja semua fungsi secara efisien (McNurlin, dkk., 1998).

Pengertian DBMS menurut Sudirman yang mengutip dari beberapa ahli berikut ini:

1. Menurut C.J. Date : DBMS adalah merupakan *software* yang menangani seluruh akses pada *database* untuk melayani kebutuhan pengguna.
2. Menurut S, Attre : DBMS adalah *software*, *hardware*, *firmware* dan prosedur-prosedur yang mengatur *database*. *Firmware* adalah *software* yang telah menjadi modul yang tertanam pada *hardware* (ROM).
3. Menurut Gordon C. Everest : DBMS adalah manajemen yang efektif untuk mengorganisasi sumber daya data (Sudirman, 2009).

Fungsi DBMS :

1. Definisi data dan hubungannya
2. Memanipulasi data
3. Keamanan dan integritas data
4. Security dan integritas data
5. Recovery/perbaikan dan concurency data
6. Data dictionary
7. Unjuk kerja / performance (Winoto, 2014)

2.9 Bahasa Pemrograman

Bahasa pemrograman, atau sering diistilahkan juga dengan bahasa komputer atau bahasa pemrograman komputer, adalah instruksi atau perintah standar untuk memerintahkan atau menjalankan komputer. Bahasa pemrograman ini merupakan suatu himpunan dari aturan *sintaks* dan *semantik* yang dipakai untuk mendefinisikan program komputer. Bahasa ini memungkinkan seorang *programmer* dapat menentukan secara persis data mana yang akan diolah oleh komputer.

Menurut tingkat kedekatannya dengan mesin komputer, bahasa pemrograman terdiri dari:

1. Bahasa Mesin, yaitu memberikan perintah kepada komputer dengan memakai kode bahasa biner, contohnya 01100101100110
2. Bahasa Tingkat Rendah, atau dikenal dengan istilah bahasa rakitan (*Assembly*), yaitu memberikan perintah kepada komputer dengan memakai kode-kode singkat (kode *mnemonic*), contohnya MOV, SUB, CMP, JMP, JGE, JL, LOOP, dan sebagainya.
3. Bahasa Tingkat Menengah, yaitu bahasa komputer yang memakai campuran instruksi atau perintah dalam kata-kata bahasa manusia dan instruksi yang bersifat simbolik, contohnya {, }, ?, <<, >>, &&, ||, dan sebagainya.
4. Bahasa Tingkat Tinggi, yaitu bahasa komputer yang memakai instruksi berasal dari unsur kata-kata bahasa manusia, contohnya begin, end, if, for, while, and, or, dan sebagainya.

Sebagian besar bahasa pemrograman digolongkan sebagai Bahasa Tingkat Tinggi, hanya bahasa C yang digolongkan sebagai Bahasa Tingkat Menengah dan *Assembly* yang merupakan Bahasa Tingkat Rendah (usu.ac.id, 2013).

Bahasa Pemrograman *Python*

Python adalah bahasa pemrograman *interpretatif* multiguna dengan filosofi perancangan yang berfokus pada tingkat keterbacaan kode. *Python* diklaim sebagai bahasa yang menggabungkan kapabilitas, kemampuan, dengan sintaksis kode yang sangat jelas, dan dilengkapi dengan fungsionalitas pustaka standar yang besar serta komprehensif.

Python mendukung multi paradigma pemrograman, utamanya; namun tidak dibatasi; pada pemrograman berorientasi objek, pemrograman imperatif, dan pemrograman fungsional. Salah satu fitur yang tersedia pada *python* adalah sebagai bahasa pemrograman dinamis yang dilengkapi dengan manajemen memori otomatis. Seperti halnya pada bahasa pemrograman dinamis lainnya, *python* umumnya digunakan sebagai bahasa skrip meski pada praktiknya penggunaan bahasa ini lebih luas mencakup konteks pemanfaatan yang umumnya tidak dilakukan dengan menggunakan bahasa skrip. *Python* dapat digunakan untuk berbagai keperluan pengembangan perangkat lunak dan dapat berjalan di berbagai *platform* sistem operasi.

Saat ini kode *python* dapat dijalankan di berbagai *platform* sistem operasi, beberapa diantaranya adalah:

1. Linux/Unix
2. Windows
3. Mac OS X
4. Java Virtual Machine
5. OS/2
6. Amiga
7. Palm
8. Symbian

Beberapa keunggulan python, antara lain :

1. *Syntax* yang sederhana.
2. Memiliki library yang sangat banyak.
3. Mendukung OOP.
4. *Syntax* dicek perbaris, sehingga memudahkan pembacaan kembali dan penulisan ulang.
5. Memiliki banyak fasilitas pendukung, sehingga mudah mengoperasikan.
6. *Open source* (gudanglinux.com, 2013).

2.10 Penelitian Terkait

Penelitian terkait yang dilakukan oleh Yusron Rijal dan Riza Dhian Ariefianto. Keduanya adalah mahasiswa lulusan S1 Jurusan Sistem Komputer, Sekolah Tinggi Manajemen Informatika & Teknik Komputer Surabaya. Penelitian oleh keduanya dilakukan pada tahun 2008 yang berjudul “Deteksi Wajah Berbasis

Segmentasi Model Warna Menggunakan Template Matching Pada Objek Bergerak”. Penelitian dilakukan dengan menggunakan media webcam sebagai alat untuk mendeteksi wajah. Wajah yang terdeteksi kemudian diproses melalui tahapan-tahapan tertentu. Metode digunakan adalah *template matching* yaitu metode yang digunakan untuk menentukan area-area warna kulit yang merupakan wajah. Area-area tersebut nantinya akan menjadi citra baru yang kemudian diubah ke dalam bentuk greyscale. Setelah citra greyscale terbentuk, barulah dicocokkan dengan citra acuan yang sebelumnya telah dibuat. Dengan begitu akan didapat hasil keluaran berupa sistem dapat mendeteksi wajah atau tidak.

Kesimpulan dari penelitian yang dilakukan oleh Yusron Rijal dan Riza Dhian Ariefianto adalah bahwa dari pengujian sistem secara keseluruhan, prosentase akurasi dari sistem pendeteksian wajah tersebut sebesar 65% dengan kecepatan rata-rata proses sebesar 4 detik. Proses segmentasi sangat bergantung pada kondisi pencahayaan. Akibatnya, nilai ambang pada suatu kondisi pencahayaan dengan kondisi pencahayaan yang lain bisa jadi berbeda. Sedangkan Prosentase akurasi penggunaan *template matching* sebagai penentu wajah mencapai 70,5%. Akan tetapi cara tersebut menurutnya memiliki kelemahan karena proses dilakukan pada bidang 2 dimensi. Akibatnya, apabila terdapat area bukan wajah yang memiliki bentuk seperti *template* akan dinyatakan sebagai wajah (Yusron Rijal dan Riza Dhian Ariefianto, 2008).

Penelitian terkait dari Mohamad Aditya Rahman yang merupakan seorang mahasiswa Jurusan Teknik Elektronika, Politeknik Elektronika Negeri Surabaya,

Kampus PENS-ITS Sukolilo, Surabaya. Meneliti tentang “Sistem Pengenalan Wajah Menggunakan Webcam Untuk Absensi Dengan Metode Template Matching”. Penelitian yang dilakukan oleh Mohamad Aditya Rahman ini dilatarbelakangi oleh penggunaan password atau kartu yang merupakan teknik identifikasi konvensional menurutnya tidak cukup handal dalam mengenali identitas seseorang karena karena sistem keamanan dapat ditembus ketika password dan kartu tersebut digunakan oleh pengguna yang tidak berwenang. Sehingga peneliti tersebut membuat sebuah sistem identifikasi yang didasarkan pada karakteristik alami manusia yaitu sistem yang dapat mengenali wajah untuk tujuan absensi atau pendataan.

Namun metode yang dilakukan pada penelitian ini berbeda dengan penelitian penulis, yaitu menerapkan teknik template matching dalam melakukan pattern recognition pada karakter yang ingin dikenali dan membandingkan antara input pattern dengan template yang disimpan. Terdapat dua jenis proses recognition yang diterapkan dalam mengenali karakter yaitu Image Correlation dan Feature Extraction.

Dari hasil pengujian sistem absensi yang dibuat tersebut, dengan 4 macam pose dan 2 macam pencahayaan maka didapatkan data bahwa pada pencahayaan yang normal hasil capture citra wajah dapat ditangkap oleh webcam dengan jelas sehingga dapat mudah di cocokkan dengan data base citra wajah dan didapatkan keseluruhan data sesuai dengan database. Namun pada pengujian dengan pencahayaan tinggi didapatkan terdapat error dikarenakan hasil capture yang

kurang jelas karena faktor cahaya. Sistem dikatakan error bila data yang dikeluarkan data base tidak sesuai dengan data hasil capture citra wajah (Mohamad Aditya Rahman, 2010).

Penelitian terkait juga dilakukan oleh Febry Santo yang merupakan seorang Mahasiswa Jurusan Teknik Elektro, Universitas Diponegoro Semarang. Meneliti tentang “Pengenalan Iris Mata Menggunakan Metode Pencirian Independent Components Analysis (ICA) dan Jarak Minkowski”. Penelitian dilakukan pada tahun 2014. Objek yang diteliti pada penelitian tersebut adalah citra iris mata. Iris mata adalah salah satu ciri biometrik pada manusia selain wajah, sidik jari dan lain-lain. Metode yang digunakan adalah *Independent Components Analysis* (ICA) dan Metode *Minkowski Distance* sebagai metode pencocokannya.

Hasil yang didapat pada penelitian tersebut adalah tingkat keberhasilan pengenalan pada pengujian menggunakan 2 citra latih lebih tinggi daripada hanya menggunakan 1 citra latih, yaitu 83,33% untuk 2 citra latih dan 64,44% untuk 1 citra latih. Hal tersebut disebabkan variasi iris mata dari citra uji membutuhkan sejumlah citra latih dengan variasi yang mirip untuk dapat dikenali dengan baik oleh sistem pengenalan iris mata. Pada penggunaan variasi koefisien Minkowski 3,4 dan 5 menghasilkan tingkat pengenalan yang lebih besar yaitu sebesar 83,33% dibandingkan dengan penggunaan 1 dan 2 koefisien Minkowski yang memiliki tingkat pengenalan masing-masing sebesar 77,78% dan 82,22%. Hal ini disebabkan semakin kecilnya nilai Jarak Minkowski maka semakin baik tingkat pengenalannya (Santo, 2014).

BAB III

METODE PENELITIAN

Sugiyono mengatakan bahwa “Metode penelitian diartikan sebagai cara ilmiah untuk mendapatkan data dengan tujuan dan kegunaan tertentu” (Sugiyono, 2012). Sedangkan menurut Bakker, ”Metodologi penelitian adalah cara-cara yang mengatur prosedur penelitian ilmiah pada umumnya, sekaligus pelaksanaannya terhadap masing-masing ilmu secara khusus” (Nyoman, 2010). Dari pendapat kedua ahli tersebut dapat disimpulkan bahwa metode ilmiah adalah prosedur secara ilmiah untuk mendapatkan data sehingga memenuhi tujuan penelitian.

3.1 Rancangan Penelitian

Dalam melaksanakan penelitian ini, tentunya dibutuhkan rancangan-rancangan penelitian yang akan dilakukan. Penelitian dirancang agar lebih terstruktur pengerjaannya dari awal memulai penelitian sampai akhir selesainya penelitian. Selain itu, rancangan penelitian juga berguna untuk mempermudah dan memberikan arah secara jelas tentang penelitian yang dilakukan. Rancangan penelitian ini terdiri dari langkah-langkah atau tahapan-tahapan yang akan dilakukan. Langkah-langkah tersebut antara lain:

1. Mengumpulkan Referensi

Tahapan pertama ini adalah mengumpulkan referensi sebanyak-banyaknya mengenai materi yang akan diteliti. Materi tersebut didapatkan

dari berbagai sumber ilmu antara lain buku, jurnal penelitian, internet dan sebagainya. Tahapan ini berguna untuk mematangkan materi dan meluaskan wawasan penulis mengenai seluk-beluk penelitian yang akan dilakukan. Referensi yang banyak dan benar akan mempermudah dalam melaksanakan penelitian dalam tahapan selanjutnya. Referensi juga menjadi bahan pertimbangan bagi penulis untuk membangun sistem login dengan pengenalan wajah menggunakan bahasa pemrograman python.

2. Persiapan penelitian

Persiapan penelitian dilakukan sebelum memulai penelitian. Dalam penelitian ini mempersiapkan seperangkat komputer yang dilengkapi dengan *webcam*. Memasang *software* pendukung ke dalam komputer yaitu *eclipse* yang telah dipasang *python* dan *library openCV* serta memasang DBMS *MySQL* sebagai tempat penyimpanan data.

3. Pelaksanaan Penelitian

Penelitian dilaksanakan setelah semua persiapan dilakukan. Memulai penelitian dengan merancang program secara rinci sampai pada pelaksanaan akhir dari penelitian yaitu pembuatan laporan.

4. Perancangan Program

Pada tahapan ini, program dirancang secara jelas. Perancangan program dilakukan guna mempermudah dalam pembuatan program. Program diharapkan dapat sesuai dengan tujuan penelitian.

5. Pembuatan program

Pada tahapan ini, pembuatan program mulai dilaksanakan. program dibuat sesuai dengan rancangan yang telah dibuat sebelumnya. Pembuatan program dilaksanakan

6. Evaluasi Program

Tahap ini adalah tahap pengujian pada program yang telah dibuat. Program dipastikan kesesuaiannya dengan rancangan yang telah dibuat sebelumnya. Memastikan kembali hasil dari program disesuaikan dengan tujuan dari penelitian. Pada tahapan ini juga dilakukan pengukuran akurasi atau ketepatan program dalam mengenali wajah.

7. Pembuatan Laporan

Pada tahapan ini dibuat laporan penelitian yang dilakukan. Laporan disusun sesuai dengan pelaksanaan penelitian yang dilakukan dilapangan.

3.1.1 Objek Penelitian

Objek yang akan diteliti dalam penelitian kali ini adalah citra wajah pengguna sebuah akun untuk digunakan sebagai akses login. Objek tersebut berupa citra gambar yang diambil menggunakan webcam dari wajah pengguna pada saat mendaftar akun dan pada saat melakukan login. Dari citra wajah tersebut dilakukan proses grayscale kemudian diproses menggunakan library OpenCV sehingga menghasilkan matrik. Matrik tersebut kemudian dicocokkan dengan metode minkowski distance sehingga

menghasilkan nilai jarak kemiripan. Nilai jarak kemiripan inilah yang menjadi parameter objek penelitian yang akan dilakukan.

3.1.2 Tahapan Penelitian

Tahap awal dalam melakukan penelitian adalah dengan membuat rancangan sistem. Dalam merancang sistem tentunya memerlukan langkah-langkah atau tahapan yang harus dilalui. Antara lain membuat dan merancang database, membuat desain tampilan sistem dan sebagainya.

Langkah selanjutnya yaitu mengimplementasikan metode ke dalam sistem. Membuat sistem sesuai dengan alur dengan menerapkan metode minkowski distance sebagai metode untuk mencocokkan wajah. Metode adalah inti dari sistem tersebut. Apabila metode tidak dapat diterapkan, maka sistem yang dibuat tidak akan sesuai dengan tujuan penelitian.

Setelah sistem dibuat, maka langkah selanjutnya adalah pengujian sistem. Variabel yang akan diukur dalam hal ini adalah jarak kemiripan antara citra wajah pengguna pada saat login dengan citra acuan yang ada dalam database. Semakin kecil jarak yang dihasilkan oleh pencocokkan tersebut, maka kedua citra tersebut dikatakan semakin mirip. Sebaliknya bila jarak yang dihasilkan semakin besar, maka dikatakan kedua citra semakin tidak mirip.

3.1.3 Tempat dan Waktu

Penelitian dilaksanakan di dua tempat yaitu Laboratorium Jurusan Teknik Informatika Universitas Islam Negeri Maulana Malik Ibrahim Malang, Perum Villa Bukit Tidar A2 737. Penelitian dimulai pada bulan Mei 2014.

3.1.4 Jenis Penelitian

Jenis penelitian yang dilakukan dalam hal ini adalah penelitian yang bersumber pada jumlah data yang digunakan, berhubungan dengan angka dan statistik, atau bisa disebut penelitian kuantitatif. Penelitian kuantitatif adalah penelitian ilmiah yang sistematis terhadap bagian-bagian dan fenomena serta hubungan-hubungannya.

Tujuan penelitian kuantitatif adalah mengembangkan dan menggunakan model-model matematis, teori-teori dan/atau hipotesis yang berkaitan dengan fenomena alam. Proses pengukuran adalah bagian yang sentral dalam penelitian kuantitatif karena hal ini memberikan hubungan yang fundamental antara pengamatan empiris dan ekspresi matematis dari hubungan-hubungan kuantitatif.

Melalui beberapa uji coba terhadap sistem, maka akan didapat hasil pengukurannya yaitu antara lain akurasi ketepatan pengenalan wajah. Hal inilah yang akan menjadi hasil akhir nanti yang akan menentukan keberhasilan penggunaan metode minkowski distance pada sistem untuk mengenali wajah pengguna.

3.1.5 Sumber dan Jenis Data

Data yang digunakan dalam penelitian kali ini adalah *capture* wajah dari pengguna sebuah akun. Data didapat melalui uji coba yang dilakukan setelah sistem selesai dibuat. Uji coba dilakukan dengan menyimpan *capture* wajah pengguna. Data berupa *capture* wajah dari pengguna tersebut kemudian disimpan ke dalam database yang dijadikan acuan atau *template* ketika sistem akan mencocokkan wajah pada saat pengguna login.

3.1.6 Metode Analisis / Penjelasan Data

Data yang telah diambil yaitu gambar wajah pengguna akan disimpan dalam *database* sebagai *template* atau acuan. Pengaturan cahaya pada wajah saat login harus disesuaikan dengan baik. Hal ini dimaksudkan agar gambar yang dihasilkan lebih baik dengan *noise* yang sedikit. Sehingga sistem dapat mengenali wajah pengguna dalam pencocokkan wajah ketika pengguna melakukan login.

Sistem akan menampilkan hasil dari pencocokkan wajah apabila sesuai dengan *template* atau acuan. Apabila sistem nantinya tidak dapat menemukan wajah yang tepat, maka pengguna tidak dapat masuk ke dalam sistem.

Nilai jarak kemiripan yang dihasilkan sistem dalam mengenali wajah berdasarkan pada beberapa faktor seperti pose wajah ketika login, tingkat intensitas cahaya dan lain-lain yang dapat mempengaruhi sistem dalam menentukan keputusan pencocokkan data.

3.2 Instrumen Penelitian

Variabel bebas atau input yang akan digunakan dalam penelitian ini adalah citra wajah pengguna yang berupa gambar capture pada saat melakukan login. Setiap akan melakukan login, pengguna harus menempatkan wajah di depan webcam agar sistem dapat mengidentifikasi wajah pengguna. Sistem akan mengambil wajah pengguna ketika tombol login diklik.

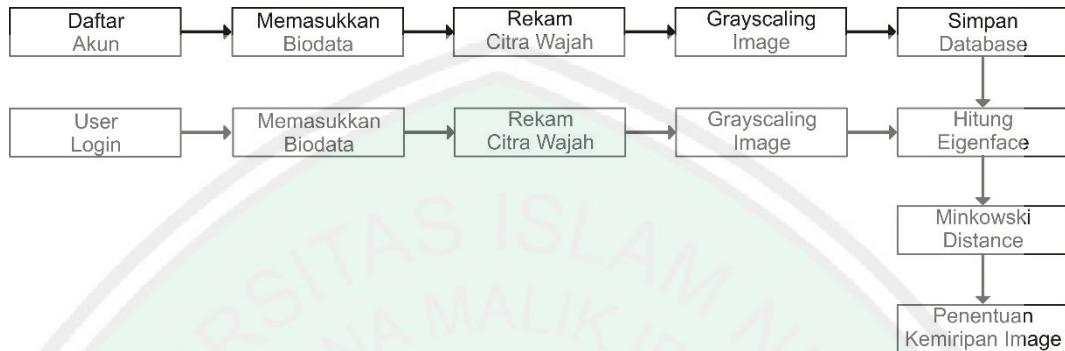
Variabel proses dalam hal ini adalah proses pencocokan wajah oleh sistem yaitu mencocokkan variabel bebas dengan *template* wajah yang ada dalam *database*. Sistem mengimplementasikan metode minkowski distance ketika melakukan pencocokkan wajah.

Variabel terikat atau output dalam hal ini adalah hasil perhitungan jarak kemiripan antara citra masukan dengan citra acuan. Pengguna dapat login apabila jarak kemiripan antara dua buah citra kecil. Sedangkan pengguna tidak dapat login apabila jarak kemiripan yang dihasilkan besar. Ukuran kecil dan besar jarak kemiripan secara detail akan ditentukan setelah penelitian selesai dan dilakukan uji coba untuk menentukan batas yang tepat antara kecil dan besar tersebut.

3.3 Kerangka Konsep

Konsep dari penelitian ini adalah menambahkan proses pengenalan wajah pada saat login dengan menerapkan metode minkowski distance untuk mencocokkan wajah. Konsep ini berbeda dengan konsep sebelumnya yang mana sistem kebanyakan hanya meminta memasukkan data berupa username dan password saja untuk dapat memperoleh akses ketika login.

Berikut akan digambarkan blok diagram dari sistem yang akan dibuat:



Gambar 3.1 Blok Diagram Sistem

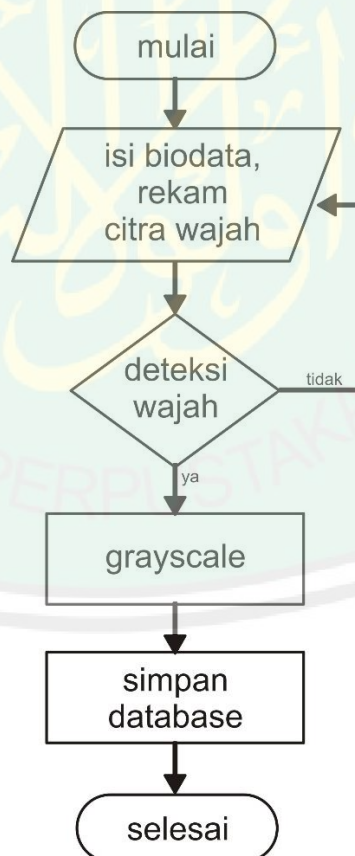
Keterangan:

1. Daftar Akun : Pengguna mendaftar membuat sebuah akun dalam sistem
2. User Login : Suatu kondisi dimana pengguna akan melakukan proses *login*
3. Memasukkan Biodata : Pengguna memasukkan biodata lengkap sesuai persyaratan yang dibuat sistem
4. Rekam Citra Wajah : Pengguna merekam citra wajah untuk dimasukkan ke dalam sistem
5. Grayscale Image : Gambar hasil rekaman pengguna yang berupa matrik RGB, diubah ke dalam matrik *grayscale* atau keabuan
6. Simpan *Database* : Hasil masukan pengguna berupa biodata, citra wajah keabuan disimpan dalam *database*.
7. Hitung Eigenface : Menghitung nilai *eigenface* dari citra wajah yang berupa citra keabuan

8. Minkowski Distance : Menghitung jarak kemiripan antara citra masukan pengguna ketika mendaftar dengan citra masukan pengguna ketika melakukan *login*
9. Penentuan Kemiripan Image : Dari hasil perhitungan jarak kemiripan, akan ditentukan apakah image mirip atau tidak, yang kemudian digunakan untuk memutuskan pengguna dapat *login* atau tidak.

Alur Diagram

- Alur Penyimpanan Data *Template*

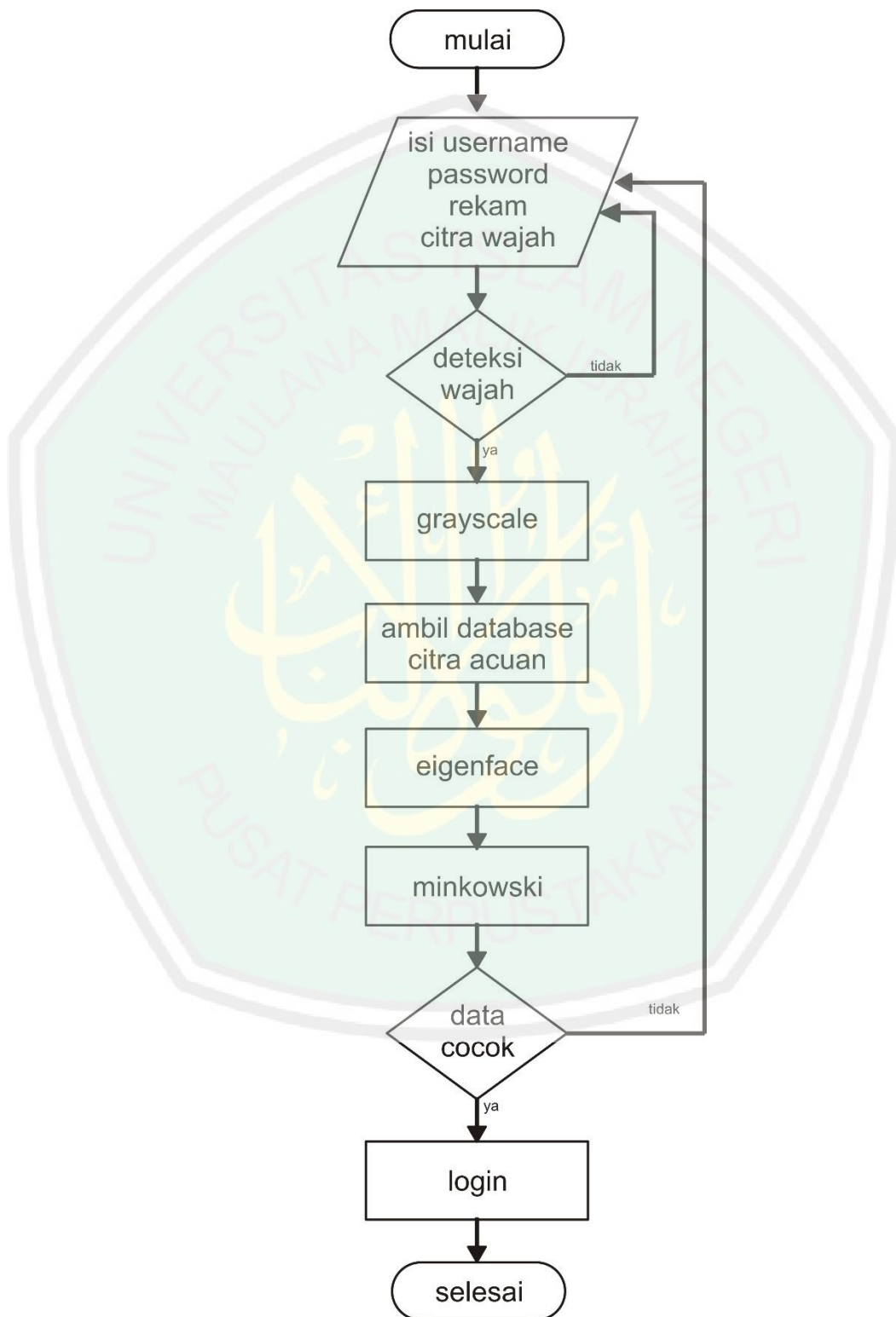


Gambar 3.2 Alur Penyimpanan Data *Template*

Keterangan :

1. Isi biodata, rekam citra wajah : pengguna mendaftar akun adalah dengan memasukkan data biodata ke dalam sistem sesuai dengan isian yang telah disediakan. Pengguna juga memasukkan data berupa citra wajah untuk digunakan sebagai citra acuan yang akan disimpan ke dalam database sistem.
2. Deteksi Wajah : kondisi apabila wajah terdeteksi oleh sistem, maka sistem melanjutkan dengan melakukan proses *grayscale*. Apabila tidak terdeteksi maka proses akan kembali ke awal.
3. *Grayscale* : proses konversi citra yang berupa matrik RGB menjadi citra keabuan.
4. Simpan database : citra hasil *grayscale* kemudian disimpan ke dalam database

- Alur Proses Pencocokan



Gambar 3.3 Alur Proses Pencocokan

Keterangan :

1. Isi username, password, rekam citra wajah : pengguna memasukkan username, password dan citra wajah untuk melakukan proses login
2. Deteksi Wajah : kondisi apabila wajah terdeteksi oleh sistem, maka sistem melanjutkan dengan melakukan proses *grayscale*. Apabila tidak terdeteksi maka proses akan kembali ke awal.
3. *Grayscale* : proses konversi citra yang berupa matrik RGB menjadi citra keabuan.
4. Ambil Database Citra Acuan : Mengambil data citra acuan dalam database
5. Eigenface : proses perhitungan nilai eigen antara citra masukan dengan citra acuan.
6. Minkowski : proses perhitungan jarak kemiripan antara citra masukan dengan citra acuan.
7. Data cocok : suatu kondisi apabila pencocokan citra dianggap cocok atau mirip, maka dilanjutkan dengan proses login. Apabila dianggap tidak cocok maka kembali ke proses awal.
8. Login : proses masuk ke dalam sistem setelah citra masukan dianggap cocok oleh sistem.

Dari alur diagram diatas dapat dijelaskan bahwa masukan yang digunakan adalah citra wajah pengguna akun. Pengguna menempatkan wajah di depan *webcam* agar dapat terdeteksi. Kemudian sistem akan melakukan

proses pendeteksian wajah menggunakan *library OpenCV* sehingga secara otomatis wajah dapat terdeteksi. Apabila tidak ditemukan bentuk wajah, maka sistem akan mengulangi langkah masukan sebelumnya. Apabila sistem dapat menemukan bentuk wajah, maka proses selanjutnya adalah mengubah citra ke dalam bentuk *grayscale* atau derajat keabuan. Setelah itu sistem mengambil citra acuan dari *database* berdasarkan *username* pengguna dan kemudian dilakukan perhitungan *eigenface* antara citra acuan dan citra masukan. Barulah kemudian dilakukan pencocokan kedua citra tersebut menggunakan *minkowski distance*. Apabila wajah cocok maka pengguna dapat *login*. Apabila tidak cocok, maka proses kembali dari awal masukan.

3.4 Rancangan *Database*

Database pada penelitian ini digunakan untuk menyimpan data berupa akun pengguna dan data *log* pengguna. *Database* dibuat dengan 3 tabel di dalamnya yaitu tabel *login*, tabel *log* dan tabel *datalog*. Tabel *login* adalah tabel yang berisi biodata pengguna seperti: *id*, nama, *email*, *username* dan *password*. Tabel *log* adalah tabel yang berisi data catatan *log* pengguna pada saat *login* yaitu berisi *username*, waktu, status dan lama pemrosesan sistem dalam mengenali wajah. Serta tabel *datalog* adalah tabel *view* yang digunakan untuk menampilkan data pada tabel *login* dan tabel *log* yang memiliki kesamaan data pada kolom *username*.

Berikut lebih jelasnya akan dijelaskan pada tabel:

Tabel 3.1 Struktur Tabel *Login*

| Kolom | Tipe |
|--------------|--------------|
| id | Integer |
| nama | Varchar (50) |
| email | Varchar (50) |
| username | Varchar (50) |
| password | Varchar (50) |

Tabel 3.2 Struktur Tabel *Log*

| Kolom | Tipe |
|--------------|--------------|
| username | Varchar (50) |
| waktu | DateTime |
| status | Varchar (50) |
| lama | Double |

Tabel 3.3 Struktur Tabel View Datalog

| Kolom | Tipe |
|--------------|--------------|
| nama | Varchar (50) |
| email | Varchar (50) |
| username | Varchar (50) |
| waktu | DateTime |
| status | Varchar (50) |
| lama | Double |

BAB IV

HASIL DAN PEMBAHASAN

Bab ini akan membahas proses uji coba sistem yang telah dibuat berdasarkan prosedur pembuatan yang telah dijelaskan pada bab sebelumnya, untuk mengetahui tingkah keberhasilan sistem dalam mendeteksi maupun mengenali wajah seseorang menggunakan metode minkowski distance.

4.1 Perangkat Penelitian

Setelah desain sistem telah dibuat seperti pada bab sebelumnya, maka sistem kemudian diprogram sesuai dengan desain yang telah ditetapkan. Pembuatan sistem menggunakan perangkat-perangkat keras maupun perangkat-perangkat lunak untuk mendukung terselesaikannya pembuatan sistem. Berikut ini dijelaskan perangkat-perangkat yang digunakan pada saat pembuatan.

4.1.1 Perangkat Keras

Perangkat keras yang digunakan pada saat pembuatan sistem adalah seperangkat komputer dengan spesifikasi antara lain:

1. *Platform : Laptop*
2. *Processor : Intel Core i3 CPU M350 @2.27GHz*
3. **RAM : 3 GB**
4. **HDD : 500GB**
5. **VGA : ATI Radeon HD 5450**

6. *Webcam : USB 2.0 Camera Standard*

4.1.2 Perangkat Lunak

Selain perangkat keras yang digunakan untuk mendukung sistem, digunakan juga perangkat-perangkat lunak antara lain:

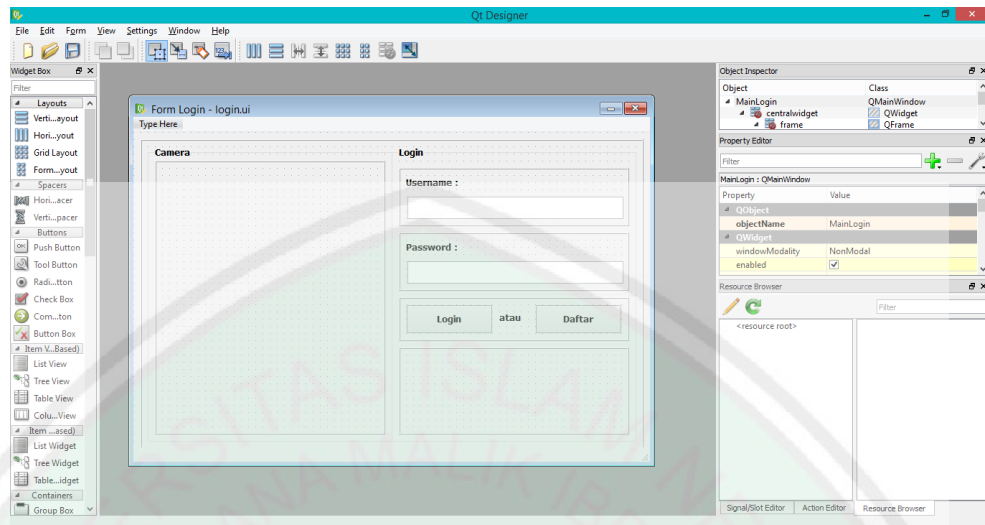
1. Sistem Operasi : *Windows 8.1 32bit*
2. *Eclipse Juno 2013*
3. *Xampp Versi 1.7.4*
4. *Python 2.7*
5. *OpenCV Versi 2.4.8*

4.2 Implementasi Sistem

Sistem kemudian dibuat dengan menggunakan perangkat-perangkat yang telah disebutkan di atas. Sistem yang dibuat bukanlah sistem informasi besar yang menangani banyak operasi dan alur yang kompleks. Namun sistem login ini hanya menangani login dengan penambahan pengenalan wajah. Sehingga tidak ditentukan tingkatan atau perbedaan akun seperti admin atau akun biasa. Semua akun memiliki tingkatan yang sama. Berikut dijelaskan lebih jelas hasil dari pembuatan tersebut.

4.2.1 Interface Sistem

Interface sistem login ini dibuat menggunakan *PyQt4* yang merupakan salah satu *library* pada *python 2.7*. Dengan menggunakan *PyQt4* akan memudahkan dalam membuat *interface* karena berbasis GUI yaitu hanya dengan *drag* dan *drop item-item* pada program untuk membuat tampilan. Berikut adalah tampilan *PyQt4* dalam membuat *interface* program:

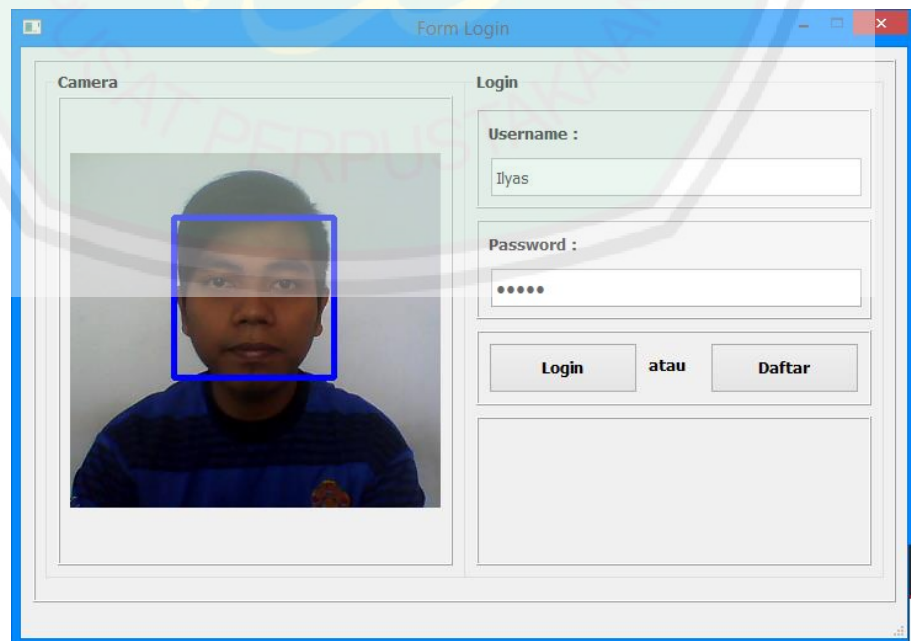


Gambar 4.1 Tampilan *PyQt4*

Terdapat beberapa *form* pada pembuatan sistem *login*. *Form* tersebut antara lain:

1. *Form Login*

Form login adalah *form* untuk melakukan *login* atau masuk ke dalam sistem komputer. Berikut adalah tampilan *form login*:



Gambar 4.2 Tampilan *Form Login*

2. *Form* Daftar

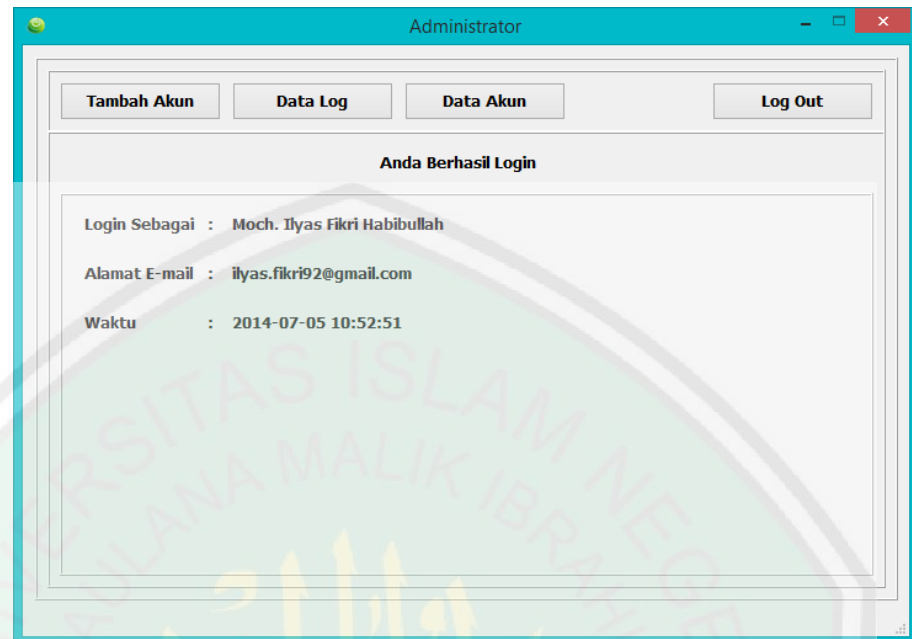
Form daftar adalah *form* untuk melakukan pendaftaran akun. Bagi pengguna yang belum memiliki akun dalam sistem, maka harus mendaftar akun terlebih dahulu pada *form* ini untuk membuat akun. Berikut adalah tampilan *form* daftar:



Gambar 4.3 Tampilan *Form* Daftar

3. *Form* Admin

Form admin adalah *form* yang pertama kali ditampilkan pada saat *login* telah berhasil dilakukan. *Form* ini menampilkan identitas dan data *log* pengguna pada saat *login* ke dalam sistem. Berikut adalah tampilan *form* admin:



Gambar 4.4 Tampilan *Form Admin*

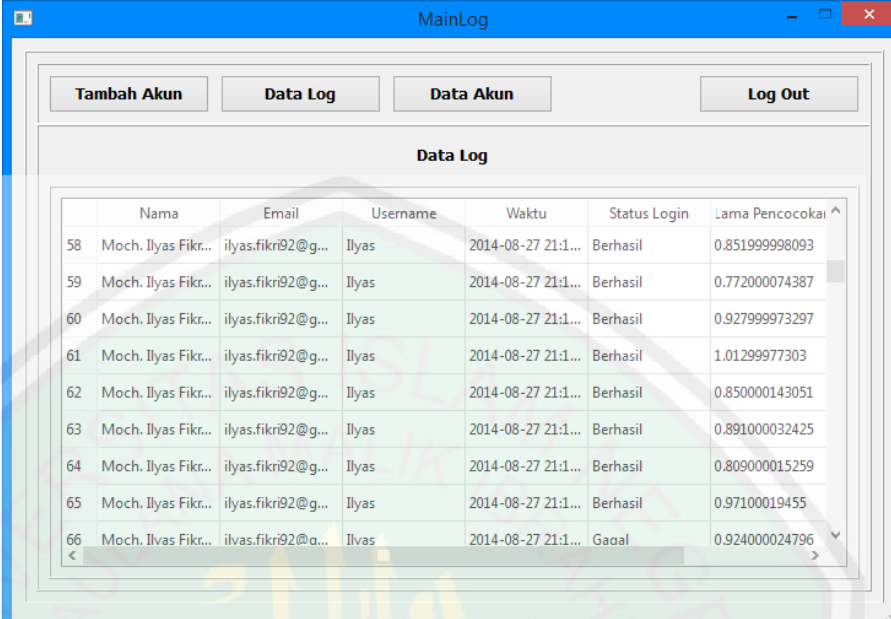
4. *Form Tambah Akun*

Form tambah akun adalah *form* yang hampir sama dengan *form* daftar yaitu *form* yang digunakan untuk menambahkan akun pada sistem. *Form* tambah akun ini dapat digunakan oleh pengguna yang telah *login* atau masuk ke dalam sistem. Berikut adalah tampilan dari *form* tambah akun:

Gambar 4.5 Tampilan *Form* Tambah Akun

5. *Form* Data Log

Form data log adalah *form* yang digunakan untuk menampilkan data pengguna yang *login*. Terdapat tabel *log* pada *form* data log. Tabel *log* tersebut mempunyai 4 kolom yaitu kolom nama, *email*, *username* dan waktu. Masing-masing kolom berisi informasi mengenai data pengguna akun yang *login* pada waktu tertentu. Berikut adalah tampilan *form* data log:

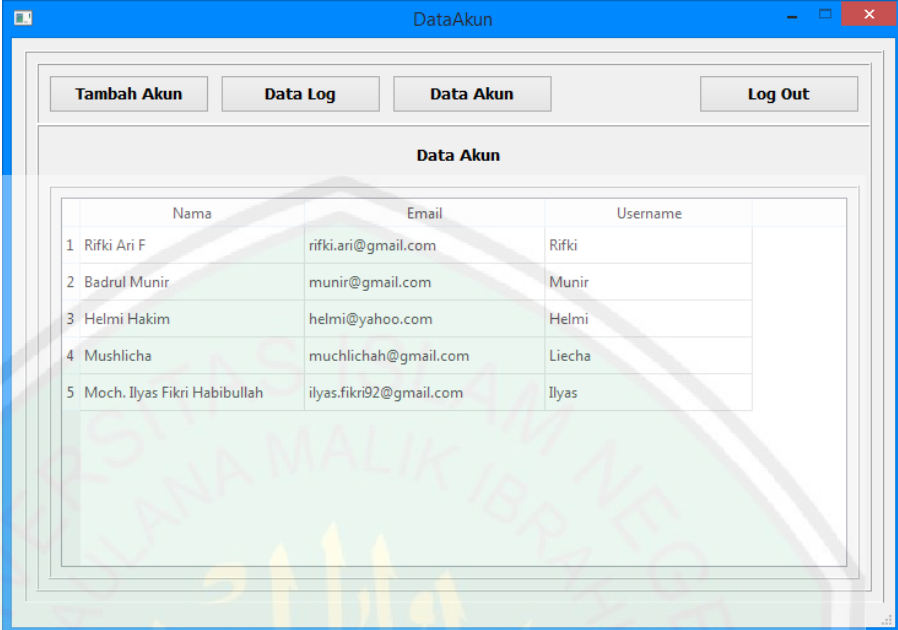


| | Nama | Email | Username | Waktu | Status Login | Lama Pencocokan |
|----|---------------------|--------------------|----------|--------------------|--------------|-----------------|
| 58 | Moch. Ilyas Fikr... | ilyas.fikri92@g... | Ilyas | 2014-08-27 21:1... | Berhasil | 0.851999998093 |
| 59 | Moch. Ilyas Fikr... | ilyas.fikri92@g... | Ilyas | 2014-08-27 21:1... | Berhasil | 0.772000074387 |
| 60 | Moch. Ilyas Fikr... | ilyas.fikri92@g... | Ilyas | 2014-08-27 21:1... | Berhasil | 0.927999973297 |
| 61 | Moch. Ilyas Fikr... | ilyas.fikri92@g... | Ilyas | 2014-08-27 21:1... | Berhasil | 1.01299977303 |
| 62 | Moch. Ilyas Fikr... | ilyas.fikri92@g... | Ilyas | 2014-08-27 21:1... | Berhasil | 0.850000143051 |
| 63 | Moch. Ilyas Fikr... | ilyas.fikri92@g... | Ilyas | 2014-08-27 21:1... | Berhasil | 0.891000032425 |
| 64 | Moch. Ilyas Fikr... | ilyas.fikri92@g... | Ilyas | 2014-08-27 21:1... | Berhasil | 0.809000015259 |
| 65 | Moch. Ilyas Fikr... | ilyas.fikri92@g... | Ilyas | 2014-08-27 21:1... | Berhasil | 0.97100019455 |
| 66 | Moch. Ilyas Fikr... | ilyas.fikri92@g... | Ilyas | 2014-08-27 21:1... | Gagal | 0.924000024796 |

Gambar 4.6 Tampilan *Form Data Log*

6. *Form Data Akun*

Form data akun adalah *form* yang digunakan untuk menampilkan data akun yang telah terdaftar dalam sistem. Semua akun yang terdaftar pada sistem akan ditampilkan pada *form* ini. Berikut adalah tampilan dari *form data akun*:



| | Nama | Email | Username |
|---|------------------------------|-------------------------|----------|
| 1 | Rifki Ari F | rifki.ari@gmail.com | Rifki |
| 2 | Badrul Munir | munir@gmail.com | Munir |
| 3 | Helmi Hakim | helmi@yahoo.com | Helmi |
| 4 | Mushlichah | muchlichah@gmail.com | Liecha |
| 5 | Moch. Ilyas Fikri Habibullah | ilyas.fikri92@gmail.com | Ilyas |

Gambar 4.7 Tampilan *Form* Data Akun

4.2.2 Implementasi Alur Program

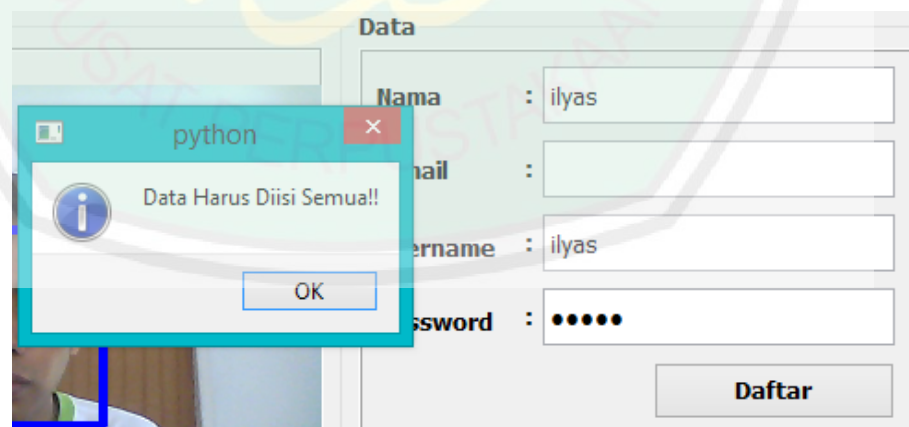
1. Pendaftaran Akun

Seorang pengguna sistem akan diperbolehkan melakukan proses *login* atau masuk ke dalam sistem komputer apabila telah mempunyai akun yang terdaftar dalam sistem. Maka dari itu, setiap pengguna harus melakukan pendaftaran akun terlebih dahulu ke dalam sistem sebagai media pengenalan oleh sistem kepada pengguna tersebut. Hal ini bertujuan agar sistem dapat mengenali penggunanya ketika pengguna tersebut akan mengakses sistem di lain waktu.

Kebanyakan sistem dalam mengenali penggunanya dengan menggunakan *username* dan *password* yang merupakan gabungan karakter yang disusun sedemikian rupa oleh pengguna sebagai kata

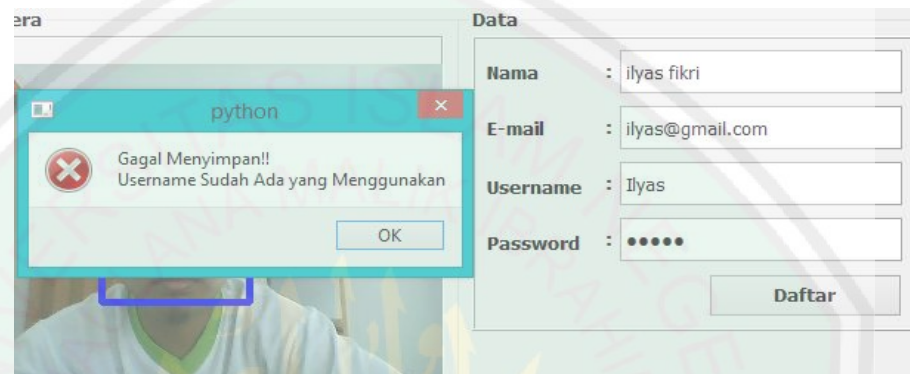
kunci atau syarat untuk masuk ke dalam sistem komputer. Namun pada sistem ini ditambahkan pengenalan wajah sebagai syarat tambahan untuk masuk ke dalam sistem. Oleh karena itu, pada saat pendaftaran akun juga ditambahkan masukan berupa citra wajah yang nantinya akan dijadikan sebagai citra acuan. Pada gambar 4.3 dan gambar 4.5 pada halaman sebelumnya menampilkan 2 kolom yang harus diisi pada saat pendaftaran akun. Kolom tersebut yaitu kolom data dan kamera. Pada kolom data terdapat beberapa baris yang harus diisi yaitu nama, *email*, *username* dan *password*. Terdapat juga tombol daftar yang digunakan untuk menyimpan masukan pada baris tadi ke dalam *database*.

Agar tidak terjadi kesalahan pada saat memasukkan data, maka diberikan pengecualian atau *exceptions* pada program. Semua baris harus diisi dengan lengkap agar data dapat disimpan dalam *database*.



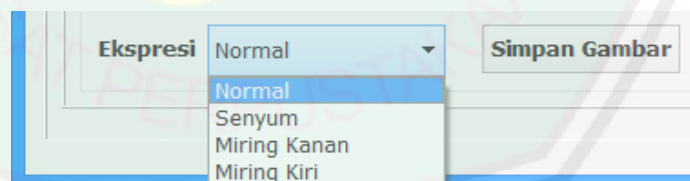
Gambar 4.8 Pengecualian Pengisian Semua Baris Data

Selain itu, username juga tidak boleh sama antara pengguna satu dengan pengguna yang lain. Dikarenakan sistem akan kesulitan dalam membedakan pengguna apabila memiliki username yang sama.



Gambar 4.9 Pengecualian Kesamaan *Username*

Pada kolom kamera, terdapat bagian yang menampilkan kamera untuk menangkap citra wajah dan bagian berupa pilihan ekspresi wajah dengan tombol simpan wajah untuk menyimpan citra wajah.



Gambar 4.10 Pilihan Ekspresi Wajah

Tombol simpan gambar adalah tombol untuk menyimpan citra wajah setelah pilihan ekspresi dipilih.

Citra wajah akan disimpan dalam *harddisk* komputer pada direktori `E:\Wajah\username`. "*username*" adalah nama *folder* berdasarkan *username* pengguna disesuaikan dengan masukan pada

baris *username* kolom data. Sebelum memasukkan citra wajah, maka baris *username* tersebut harus diisi terlebih dahulu. *Folder* yang sebelumnya tidak ada, akan dibuat berdasarkan *username* dan tinggal memasukkan data apabila sebelumnya sudah ada. Nama *file* yang tersimpan ke dalam *folder* berdasarkan pada pilihan ekspresi wajah berekstensi .pgm



Gambar 4.11 Hasil Simpan Gambar

2. Proses Login

Proses *login* adalah proses pengguna untuk masuk ke dalam sistem komputer setelah melakukan pendaftaran akun. Pada gambar 4.2 di halaman sebelumnya menunjukkan 3 syarat yang harus dipenuhi oleh pengguna untuk dapat masuk ke dalam sistem yaitu *username* harus benar, *password* harus benar dan wajah harus cocok.

Sistem akan mencocokkan *username* dan *password* yang dimasukkan oleh pengguna pada saat *login* dengan *username* dan *password* pengguna pada saat mendaftar yang telah tersimpan di dalam *database Login* dengan tabel *login*. Apabila *username* dan *password* sudah benar, maka akan dipanggil *method* pencocokan. Sedangkan

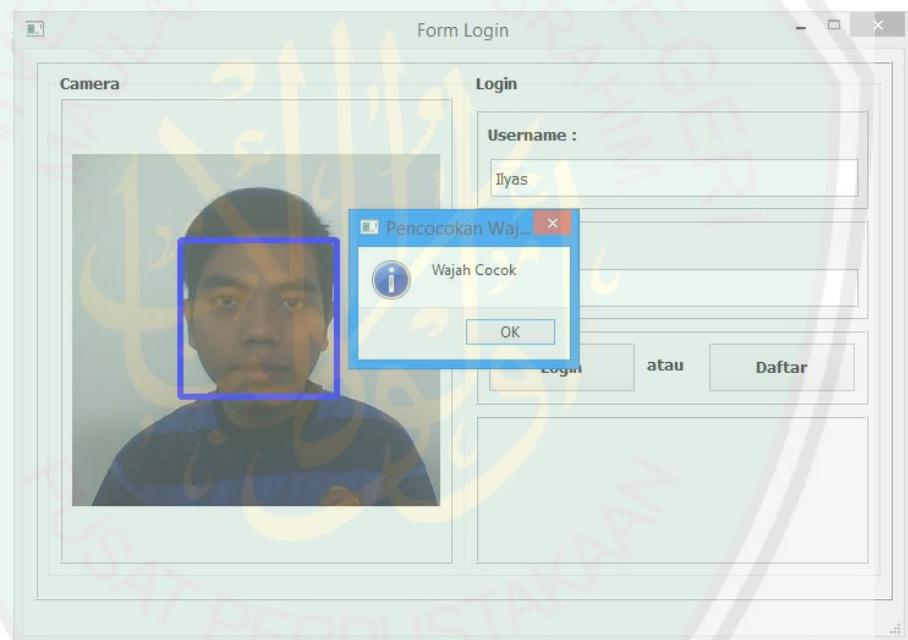
apabila *username* atau *password* tidak sesuai dengan yang ada di dalam *database*, maka pengguna tidak dapat masuk atau *login* dan harus mengulang proses dari awal.

Di dalam *method* pencocokan diimplementasikan metode *minkowski distance*. Metode ini digunakan untuk mencocokkan citra masukan dengan citra acuan. Metode ini adalah langkah akhir dari program yang akan menentukan pengguna dapat masuk atau tidak.

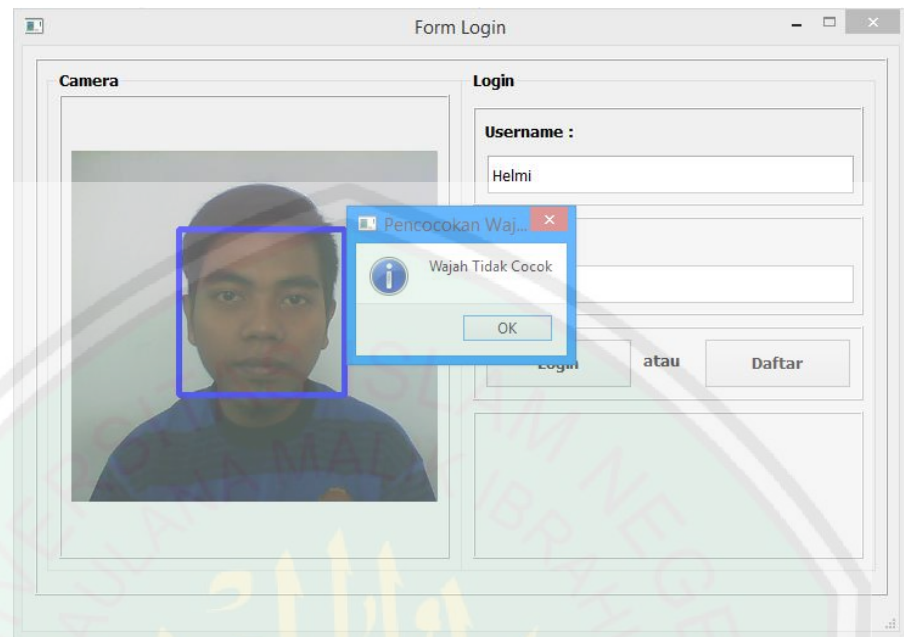
Terdapat variabel jarak pada kode yang telah dibuat yang merupakan hasil dari perhitungan menggunakan metode *minkowski distance*. Semakin kecil nilai jarak, maka sistem mendeteksi semakin mirip antara citra masukan dengan citra acuan.

Setelah itu diberikan kondisi yang akan menentukan langkah sistem selanjutnya. Kondisi tersebut antara lain adalah hasil perhitungan menggunakan metode *minkowski distance* yaitu letak atau direktori citra acuan yang paling mirip dengan citra masukan dan nilai jaraknya yang mana seperti pada gambar 4.11 di atas menunjukkan direktori dengan nama *folder* "Ilyas". Apabila nama folder hasil perhitungan metode *minkowski distance* sama dengan *username* yang dimasukkan dan nilai jaraknya dibawah 1500, maka pengguna diperbolehkan masuk ke dalam sistem atau *login*. Namun apabila hasilnya tidak sama dan nilai kemiripannya di atas 1500, maka akan muncul keterangan bahwa wajah tidak cocok.

Sistem tidak akan memperbolehkan login apabila wajah yang menjadi masukan dengan wajah yang menjadi acuan berbeda. Sedangkan angka 1500 adalah nilai ambang batas yang penulis berikan terhadap nilai jarak kemiripan. Suatu citra dapat dibilang mirip apabila nilai kemiripannya di bawah 1500. Hal ini berdasarkan pada beberapa uji coba penulis lakukan. Berikut adalah tampilan program pada saat *login*:



Gambar 4.13 Tampilan Berhasil *Login*



Gambar 4.14 Tampilan Gagal Login

3. Menampilkan Data

Ketika pengguna sudah berhasil *login* atau masuk ke dalam sistem, maka sistem akan menampilkan data dari pengguna seperti pada gambar 4.4 di halaman sebelumnya. Data tersebut antara lain: nama, *email* dan waktu ketika melakukan *login*.

Selain data tersebut di atas, ditampilkan pula data berupa tabel datalog seperti pada gambar 4.6 dan data tabel login seperti pada gambar 4.7. Tabel datalog ditampilkan dengan menekan tombol data log yang ada pada menu bagian atas, sedangkan tabel login ditampilkan setelah tombol data akun ditekan pada menu bagian atas. Pengguna juga dapat keluar dengan menekan tombol *logout*.

4.2.3 Implementasi Minkowski Distance

Metode minkowski distance diimplementasikan ke dalam sistem pada *method* pencocokan yang telah disinggung sebelumnya. Metode ini digunakan untuk menghitung nilai kemiripan antara citra masukan dan citra acuan. Citra masukan dan citra acuan adalah gambar wajah pengguna yang berupa matrik. Berikut akan dicontohkan bagaimana sistem mengimplementasikan metode *minkowski distance* untuk menghasilkan nilai jarak kemiripan citra:

Sistem memiliki pengguna dengan *username* “Helmi”, “Liecha” dan “Ilyas”. Masing-masing pengguna telah memasukkan citra acuan ke dalam sistem.

Contoh citra acuan yang ada dalam *database*:



(A)

(B)

(C)

Masing-masing citra menghasilkan nilai matrik 3x3. Citra A memiliki nilai matrik $\{(2,3,2),(3,4,1),(1,3,1)\}$, citra B memiliki nilai matrik $\{(3,4,2),(5,6,3),(2,2,1)\}$ dan citra C memiliki nilai matrik $\{(8,9,7),(9,1,8),(7,6,6)\}$. Citra A disimpan pada direktori dengan nama “Helmi”, citra B disimpan pada direktori dengan nama “Liecha” dan citra C disimpan pada direktori dengan nama “Ilyas”. Kemudian salah satu pengguna

ingin *login* ke dalam sistem dengan memasukkan *username*, *password* dan citra masukan ke dalam sistem.

Contoh citra masukan dengan *username* “Ilyas”:



(D)

Citra D menghasilkan nilai matrik $\{(8,8,7),(9,2,8),(7,8,7)\}$. Kemudian sistem akan menghitung nilai jarak kemiripan antara citra masukan dan citra acuan yang ada dalam database. Sehingga akan disimpulkan citra acuan mana yang lebih mirip dengan citra masukan. Berikut adalah perhitungan yang dilakukan sistem menggunakan metode *minkowski distance*:

$$\begin{aligned}
 AD &= \sqrt[3]{(|2-8|^3 + |3-8|^3 + |2-7|^3 + |3-9|^3 + |4-2|^3 + |1-8|^3 + |1-7|^3 + |3-8|^3 + |1-7|^3)} \\
 &= \sqrt[3]{(6^3 + 5^3 + 5^3 + 6^3 + 2^3 + 7^3 + 6^3 + 5^3 + 6^3)} \\
 &= \sqrt[3]{(216 + 125 + 125 + 216 + 8 + 343 + 216 + 125 + 216)} \\
 &= \sqrt[3]{1590} \\
 &= 11,672
 \end{aligned}$$

$$\begin{aligned}
 BD &= \sqrt[3]{(|3-8|^3 + |4-8|^3 + |2-7|^3 + |5-9|^3 + |6-2|^3 + |3-8|^3 + |2-7|^3 + |2-8|^3 + |1-7|^3)} \\
 &= \sqrt[3]{(5^3 + 4^3 + 5^3 + 4^3 + 4^3 + 5^3 + 5^3 + 6^3 + 6^3)} \\
 &= \sqrt[3]{(125 + 64 + 125 + 64 + 64 + 125 + 125 + 216 + 216)}
 \end{aligned}$$

$$= \sqrt[3]{1124}$$

$$= 10,397$$

$$CD = \sqrt[3]{(|8-8|^3 + |9-8|^3 + |7-7|^3 + |9-9|^3 + |1-2|^3 + |8-8|^3 + |7-7|^3 + |6-8|^3 + |6-7|^3)}$$

$$= \sqrt[3]{(0^3 + 1^3 + 0^3 + 0^3 + 1^3 + 0^3 + 0^3 + 2^3 + 1^3)}$$

$$= \sqrt[3]{(0+1+0+0+1+0+0+8+1)}$$

$$= \sqrt[3]{11}$$

$$= 2,224$$

Dari hasil perhitungan di atas, maka sistem akan menyimpulkan bahwa citra acuan yang paling mirip dengan citra masukan adalah citra C. Sistem kemudian mencocokkan kesamaan nama direktori dengan *username* yang pengguna masukkan ketika *login*. Citra C berada pada direktori “Ilyas” dan *username* yang dimasukkan adalah “Ilyas”, sehingga keduanya cocok. Kemudian akan dilihat nilai kemiripannya. Nilai kemiripan antara citra C dan citra D atau CD adalah 2,224 yaitu lebih kecil dari nilai ambang batas sebesar 1500 sehingga benar. Maka sistem akan memperbolehkan pengguna untuk *login* pada kondisi yang dicontohkan di atas.

4.3 Uji Coba Sistem

Setelah selesai merancang dan membangun aplikasi *login* dengan penambahan pengenalan wajah ini, maka perlu dilakukan pengujian terhadap aplikasi. Uji coba dilakukan untuk mengetahui akurasi dan ketepatan sistem dalam mengenali wajah. Dalam uji coba ini dilakukan dalam beberapa kondisi yang

berbeda pada saat login. Kondisi tersebut yaitu intensitas cahaya yang berbeda pada saat memasukkan data maupun pada saat melakukan login. Berdasarkan pada penelitian yang dilakukan oleh Tri Mulyono dkk., maka penulis melakukan uji coba untuk menghitung akurasi sistem yaitu dengan dilakukan perhitungan kesalahan (*error rate analysis*). Kesalahan yang dianalisa terdiri dari dua bentuk kesalahan yaitu *False Acceptance Rate* (FAR) dan *False Rejection Rate* (FRR). FAR adalah kesalahan sistem dalam memperbolehkan pengguna yang salah untuk masuk atau *login*. Sedangkan FRR adalah kesalahan sistem dalam menolak pengguna yang benar untuk masuk atau *login*. (Tri Mulyono, dkk., 2012)

4.3.1 Analisis Data

Data yang digunakan sebagai bahan uji coba adalah berupa citra wajah. Citra wajah didapat dari pengambilan wajah pengguna pada saat mendaftar dan melakukan login. Pada saat mendaftar, pengguna harus memasukkan citra wajah dengan beberapa ekspresi wajah yang berbeda. Pilihan ekspresi wajah sudah ditentukan seperti pada gambar 4.10 yaitu:













1. Normal
2. Senyum
3. Miring Kanan $\pm 15^\circ$
4. Miring Kiri $\pm 15^\circ$

Selain dengan ekspresi wajah yang berbeda, juga dilakukan pengambilan data dengan intensitas cahaya yang berbeda pada setiap sesi pengambilan. Sumber cahaya adalah berupa lampu sebesar 15watt. Intensitas cahaya yang ditentukan adalah sebesar 75lux, 100lux dan 200lux yang

dihasilkan dari variasi jarak wajah dari lampu sebesar 220cm, 100cm dan 60cm. Sehingga setiap pengguna memasukkan masukan 12 citra masukan dengan rincian 4 ekspresi x 3 variasi intensitas cahaya.

Berikut ini adalah beberapa contoh data citra wajah acuan dengan posisi atau ekspresi yang berbeda-beda:

Tabel 4.1 Contoh Citra Acuan

| | 75lux | 100lux | 200lux |
|-----------------|---|--|---|
| Normal |  |  |  |
| Senyum |  |  |  |
| Miring Kanan |  |  |  |
| Miring Kiri |  |  |  |

4.3.2 Percobaan *Login*

Percobaan dilakukan dengan beberapa kondisi yang berbeda. Sebagaimana pada pembahasan sebelumnya, syarat untuk dapat login atau masuk ke dalam sistem adalah username harus benar, password harus benar dan wajah harus cocok. Diasumsikan bahwa username dan password pengguna sudah benar, maka dilakukan pengujian untuk menghitung FAR dan FRR pada sistem.

Percobaan dilakukan dengan menempatkan wajah lurus di depan kamera dengan jarak yang konstan atau tetap yaitu sebesar 50cm antara wajah dengan webcam. Kemudian dilakukan percobaan login dengan intensitas pencahayaan yang berbeda pada citra masukan dan dengan intensitas pencahayaan yang berbeda pada citra acuan. Percobaan dibagi menjadi beberapa sesi yaitu:

1. Citra acuan intensitas 100lux, citra masukan intensitas 100lux
2. Citra acuan intensitas 100lux, citra masukan intensitas 200lux
3. Citra acuan intensitas 100lux, citra masukan intensitas 300lux
4. Citra acuan intensitas 200lux, citra masukan intensitas 100lux
5. Citra acuan intensitas 200lux, citra masukan intensitas 200lux
6. Citra acuan intensitas 200lux, citra masukan intensitas 300lux
7. Citra acuan intensitas 300lux, citra masukan intensitas 100lux
8. Citra acuan intensitas 300lux, citra masukan intensitas 200lux
9. Citra acuan intensitas 300lux, citra masukan intensitas 300lux

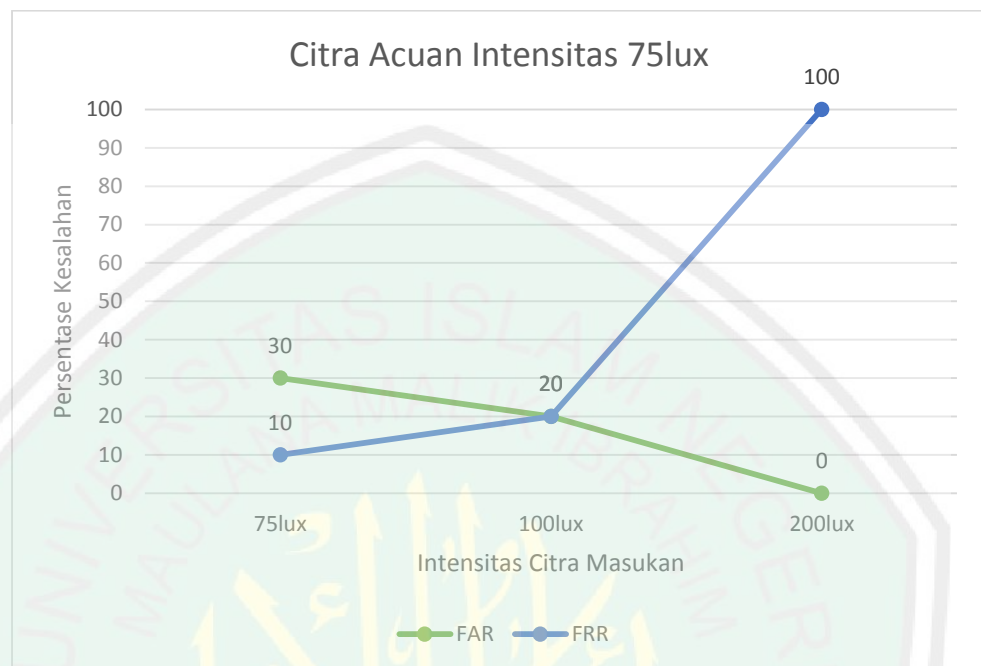
Setiap sesi dilakukan percobaan sebanyak 20 kali yang mana 10 kali percobaan untuk menghitung FAR dan 10 kali percobaan untuk menghitung FRR sehingga total keseluruhan percobaan yang dilakukan adalah 180 kali. FAR adalah persentase kesalahan sistem dalam menerima pengguna yang seharusnya salah menjadi benar sehingga pengguna dapat login. Sedangkan FRR adalah persentase kesalahan sistem dalam menolak pengguna yang seharusnya benar menjadi salah sehingga pengguna tidak dapat login.

Berikut adalah hasil dari percobaan yang telah dilakukan:

Tabel 4.2 Hasil Percobaan dengan Citra Acuan 75lux

| Citra Masukan | FAR | FRR | Akurasi |
|---------------|-----|------|---------|
| 75lux | 30% | 10% | 80% |
| 100lux | 20% | 20% | 80% |
| 200lux | 0% | 100% | 50% |

Berikut adalah grafik dari percobaan dengan citra acuan 75lux:



Gambar 4.15 Grafik Percobaan dengan Citra Acuan 75lux

Dari hasil percobaan menggunakan citra acuan 75lux seperti pada tabel dan grafik di atas menunjukkan bahwa kesalahan dalam menerima pengguna yang salah menjadi benar atau FAR lebih kecil dari pada kesalahan dalam menolak pengguna yang benar menjadi salah atau FRR. Terutama kesalahan pada percobaan dengan intensitas cahaya sebesar 200lux yang menunjukkan kesalahan mencapai 100%. Hal ini dikarenakan perbedaan yang sangat mencolok antara citra acuan dengan citra masukan sehingga menghasilkan nilai jarak kemiripan yang besar atau di atas ambang batas yang ditentukan yaitu 1500. Sedangkan persentase FAR menjadi 0% atau sempurna dikarenakan tidak satupun citra masukan yang dianggap benar oleh sistem dengan perbedaan jarak yang sangat besar tersebut.

Sedangkan hasil pada percobaan login dengan intensitas cahaya 75lux dan 100lux menunjukkan kesalahan yang minimal pada FRR dengan persentase 10% yaitu pada percobaan 75lux. Namun persentase FAR mencapai 30% pada kondisi ini dikarenakan sistem mendeteksi banyak kesamaan pada wajah atau jarak kemiripan yang dihasilkan di bawah 1500.

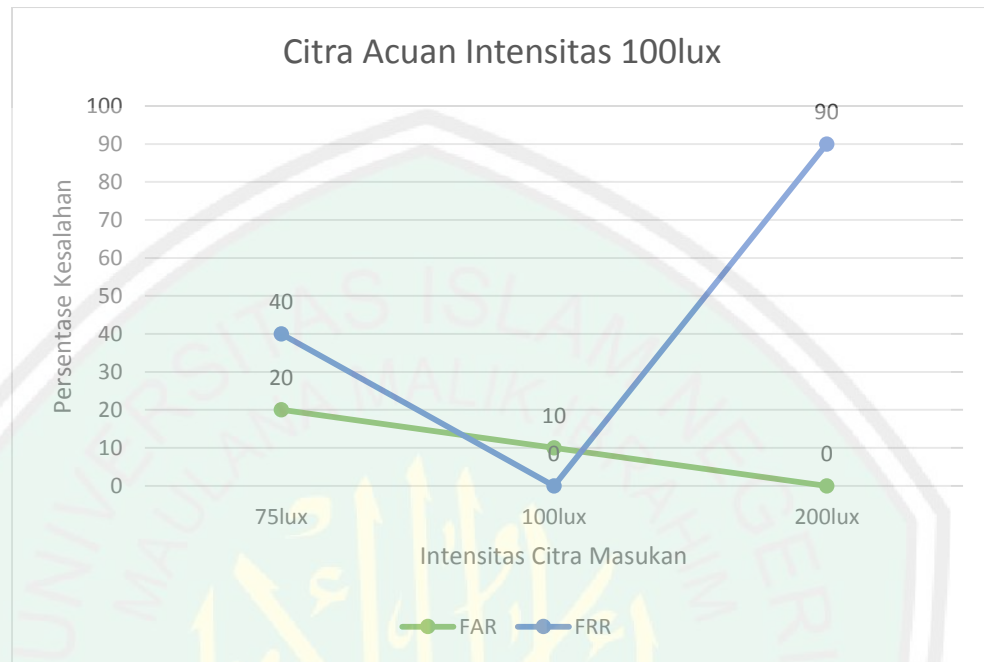
Maka dapat disimpulkan bahwa dengan citra acuan yang diambil dengan intensitas cahaya 75lux akan menghasilkan akurasi mencapai 80% apabila dilakukan percobaan login dengan intensitas cahaya 75lux dan 100lux yang mana intensitas cahayanya tidak terlalu berbeda dengan citra acuan.

Sedangkan pada percobaan dengan citra acuan menggunakan intensitas 100lux menghasilkan persentase sebagai berikut:

Tabel 4.3 Hasil Percobaan dengan Citra Acuan 100lux

| Citra Masukan | FAR | FRR | Akurasi |
|---------------|-----|-----|---------|
| 75lux | 20% | 40% | 70% |
| 100lux | 10% | 0% | 95% |
| 200lux | 0% | 90% | 55% |

Berikut adalah grafik dari percobaan dengan citra acuan 100lux:



Gambar 4.16 Grafik Percobaan dengan Citra Acuan 100lux

Dari hasil percobaan dengan citra acuan 100lux seperti pada tabel dan grafik di atas menunjukkan bahwa kesalahan FRR terbesar yaitu pada percobaan dengan intensitas cahaya 200lux yang mencapai 90%. Pengguna yang benar akan kesulitan login ke dalam akun apabila data acuannya memiliki intensitas 100lux dengan percobaan login pada intensitas citra acuan sebesar 200lux. Begitu pula percobaan login dengan intensitas citra masukan sebesar 75lux dengan persentase kesalahan sebesar 40% pada percobaan. Namun tidak ada kesalahan dalam proses login apabila intensitas citra masukan juga sebesar 100lux yang menghasilkan FRR sebesar 0%.

Sementara nilai FAR terbesar yaitu pada percobaan dengan intensitas cahaya 75lux. Cahaya yang sedikit lebih redup dari citra acuan membuat

akurasi sistem berkurang dengan hasil nilai kemiripan yang relatif kecil menyebabkan sistem melakukan kesalahan 20%. Pada hasil percobaan dengan citra acuan dan citra masukan yang sama intensitas cahayanya menghasilkan FAR sebesar 10%. Sedangkan pada percobaan dengan intensitas cahaya sebesar 200lux menghasilkan FAR 0%. Seperti halnya percobaan dengan citra acuan 75lux, sistem sama sekali tidak melakukan kesalahan FAR dikarenakan nilai jarak kemiripan yang sangat besar. Sehingga semua percobaan yang dilakukan dengan pengguna yang salah, tidak satupun yang dapat masuk ke dalam sistem.

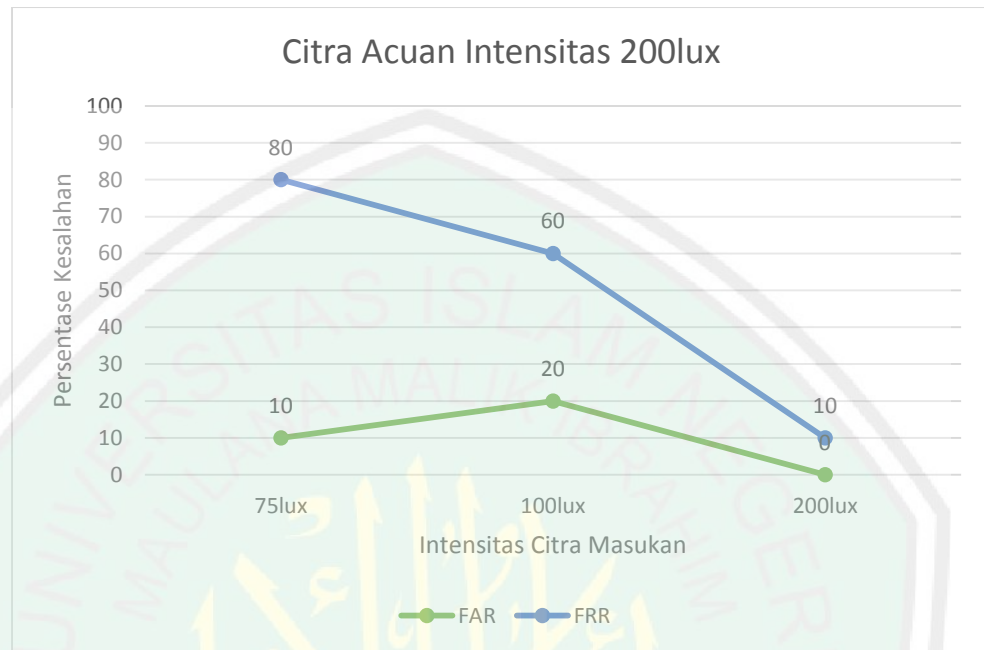
Dapat disimpulkan bahwa akurasi terbaik untuk melakukan proses login dengan citra acuan intensitas 100lux adalah melakukan percobaan pada intensitas cahaya 100lux yang mana pada percobaan yang dilakukan dapat menghasilkan akurasi sebesar 95%.

Sedangkan pada percobaan menggunakan citra acuan intensitas 200lux menghasilkan persentase sebagai berikut:

Tabel 4.4 Hasil Percobaan dengan Citra Acuan 200lux

| Citra Masukan | FAR | FRR | Akurasi |
|---------------|-----|-----|---------|
| 75lux | 10% | 80% | 55% |
| 100lux | 20% | 60% | 60% |
| 200lux | 0% | 10% | 95% |

Berikut adalah grafik dari percobaan dengan citra acuan 200lux:



Gambar 4.17 Grafik Percobaan dengan Citra Acuan 200lux

Dari hasil percobaan dengan citra acuan intensitas 200lux seperti pada tabel dan grafik di atas menunjukkan bahwa akurasi terendah yaitu sebesar 55% dengan nilai FAR sebesar 10% dan nilai FRR sebesar 80% didapat dari percobaan dengan intensitas cahaya 75lux. Perbedaan citra acuan dengan citra masukan yang terlalu besar menyebabkan sistem hanya 2 kali berhasil mengenali dengan benar wajah pengguna namun berhasil menolak pengguna yang salah sebanyak 9 kali. Hal ini disebabkan nilai jarak kemiripan yang besar sehingga sistem menolak pengguna yang salah pada hampir semua percobaan yang dilakukan.

Sedangkan pada hasil percobaan dengan intensitas cahaya sebesar 100lux menghasilkan nilai FAR dan FRR masing-masing sebesar 20% dan

60%. Sistem dapat mengenali wajah sedikit lebih baik pada kondisi ini dengan persentase akurasi 60%.

Pada hasil percobaan dengan intensitas yang sama dengan citra acuan yaitu sebesar 200lux, menghasilkan tingkat akurasi yang tinggi mencapai 95% dengan nilai FAR dan FRR masing-masing sebesar 0% dan 10%. Pada kondisi ini, nilai jarak kemiripan antara citra acuan dengan citra masukan tidak terlalu besar, sehingga didapatkan hasil yang maksimal.

Dari keseluruhan percobaan yang telah dijelaskan hasilnya pada penjelasan di atas maka dapat disimpulkan bahwa intensitas cahaya sangat berpengaruh dalam menentukan keberhasilan sistem mengenali wajah. Perbedaan yang terlalu jauh antara intensitas citra acuan dengan intensitas citra masukan menghasilkan akurasi yang rendah. Sedangkan percobaan dengan intensitas yang hampir sama antara citra masukan dengan citra acuan menghasilkan kesalahan sistem yang semakin kecil, sehingga persentase akurasinya menjadi semakin tinggi.

Persentase FAR dan FRR dari keseluruhan percobaan yang dilakukan adalah sebesar 8,89% untuk FAR dan 44,44% untuk FRR.

4.4 Integrasi Islam

Pada sub bab ini akan dijelaskan integrasi atau hubungan antara penelitian yang dilakukan dengan kajian keislaman. Penelitian berkaitan dengan upaya untuk menjaga hak milik dari gangguan orang lain yang tidak berhak. Islam mengharuskan ummatnya untuk menjaga setiap apa yang Allah

anugerahkan untuk dilindungi dan dirawat sebagai amanah. Sebagaimana Allah memberikan tubuh sebagai liang berteduhnya ruh yang merupakan hak setiap hamba untuk dijaga dari gangguan hamba lain yang ingin menggangukannya. Sudah sepantasnya setiap hamba, ada kemauan dan usaha untuk menjaga dan semakin memperbaiki penjagaannya agar apa yang menjadi haknya tidak mudah diambil oleh orang lain. Sebagai contoh dalam peperangan, sudah seharusnya perlengkapan untuk berperang seperti senjata, perisai dan lain sebagainya diperbaiki dengan ditambah semakin banyak atau dibaguskan kualitasnya.

Sebagaimana sebuah hadits shohih yang diriwayatkan oleh Bukhori Muslim yang berbunyi: *Aku mendengar Rosulullah SAW bersabda “Barang siapa terbunuh karena membela hartanya, maka Ia mati syahid”* (HR. Tirmidzi Nomor.1338). Hadits ini berbicara tentang keutamaan memelihara harta. Harta yang dimaksud tidaklah harus selalu diartikan sebagai uang, properti atau kekayaan fisik lainnya. Namun juga dapat diartikan semua yang manusia miliki adalah harta.

Sebuah *account* atau akun adalah harta yang juga harus selalu dijaga, karena mungkin saja sebuah akun akan sama nilainya dengan informasi atau harta yang ada di dalamnya. Sebagai contoh adalah akun tabungan di sebuah bank. Maka nilai akun tersebut akan sebanding dengan jumlah uang yang ada di dalamnya. Sudah menjadi kewajiban sebuah bank yang mendapat amanah dari nasabahnya untuk menjaga keamanan akun nasabahnya dari ancaman orang lain yang tidak mempunyai hak atas akun tersebut. Penambahan

pengenalan wajah untuk login pada penelitian ini adalah salah satu upaya atau *ikhtiar* yang menurut penulis dapat digunakan untuk lebih mengamankan sebuah akun. Akan sangat berguna apabila diproduksi secara massal sebuah sistem komputer yang dapat mengenali ciri biometrik manusia dengan sangat akurat, sehingga pengamanan sebuah akun atau akses login dapat lebih ditingkatkan.

Upaya penambahan pengenalan wajah untuk akses login ini adalah sekaligus untuk mengurangi terjadinya kezaliman. Zalim adalah bahasa Arab yang mempunyai pengertian meletakkan sesuatu bukan pada tempatnya. Jadi, segala sesuatu yang diletakkan bukan pada tempatnya adalah termasuk kezaliman, dan yang melakukan kezaliman disebut dengan zalimin. Salah satu sumber hukum yang menjadi acuan yaitu sebuah hadits dari Abu Dzar Al Ghifari radhiyallahuanhu, dari Rasulullah shallallahu'alaihi wa sallam sebagaimana beliau riwayatkan dari Rabbnya Azza Wajalla bahwa, Allah berfirman: *“Wahai hambaku, sesungguhnya aku telah mengharamkan kezaliman atas diri-Ku dan Aku telah menetapkan haramnya (kezaliman itu) diantara kalian, maka janganlah kalian saling berlaku zalim. ...”* (HR. Muslim No. 4674).

Hadits di atas secara tegas menyebutkan larangan perbuatan zalim. Bahkan Allah SWT telah mengharamkan perbuatan zalim untuk diri-Nya sendiri dan tentu mengharamkan perbuatan kezaliman dilakukan oleh semua manusia pada umumnya. Allah juga berfirman dalam Al-Quran Surah Qaaf ayat 29 yang berbunyi:

مَا يُبَدَّلُ الْقَوْلُ لَدَيَّ وَمَا أَنَا بِظَلَّامٍ لِلْعَبِيدِ ﴿٦٦﴾

Artinya: “Keputusan di sisi-Ku tidak dapat diubah dan aku sekali-kali tidak Menganiaya hamba-hamba-Ku.”

Ayat di atas menunjukkan bahwa mustahil Allah SWT menzalimi hamba-hamba-Nya. Kalaulah ada seorang hamba terkena kezaliman, itu adalah karena ulah manusia itu sendiri, seperti firman-Nya di dalam Al-Qur’an Surah Yunus ayat 44 yang berbunyi:

إِنَّ اللَّهَ لَا يَظْلِمُ النَّاسَ شَيْئًا وَلَكِنَّ النَّاسَ أَنفُسَهُمْ يَظْلِمُونَ ﴿٤٤﴾

Artinya: “Sesungguhnya Allah tidak berbuat zalim kepada manusia sedikitpun, akan tetapi manusia Itulah yang berbuat zalim kepada diri mereka sendiri.”

Bahkan dalam ayat lain Allah justru menjanjikan akan memberi pahala yang besar kepada hamba-Nya yang melakukan amal kebajikan, walau hanya sebesar biji *zarrah*. Sebagaimana dalam Surah An-Nisa’ ayat 40 yang berbunyi:

إِنَّ اللَّهَ لَا يَظْلِمُ مِثْقَالَ ذَرَّةٍ وَإِن تَكُ حَسَنَةً يُضْعِفْهَا وَيُؤْتِ مِنْ لَدُنْهِ أَجْرًا

عَظِيمًا ﴿٤٠﴾

*Artinya: “Sesungguhnya Allah tidak Menganiaya seseorang walaupun sebesar *zarrah*, dan jika ada kebajikan sebesar *zarrah*, niscaya Allah akan melipat gandakannya dan memberikan dari sisi-Nya pahala yang besar.”*

Maksudnya adalah Allah tidak akan mengurangi pahala orang-orang yang mengerjakan kebajikan walaupun sebesar zarah, bahkan kalau orang tersebut berbuat baik pahalanya akan dilipat gandakan oleh Allah.

Penjelasan ayat Al-Qur'an maupun Hadits di atas menjelaskan secara jelas bahwa Allah melarang manusia berlaku zalim. Mustahil Allah mezalimi hamba-hamba-Nya. Kezaliman yang terjadi itu adalah karena ulah hamba itu sendiri. Allah menjanjikan pahala kepada orang yang berlaku sebaliknya yaitu kebajikan walaupun kebajikan itu hanya sebesar biji *zarah*.

Perilaku membobol akun seseorang atau menggunakan hak aksesnya tanpa seizin pemilik akun, juga termasuk perilaku yang zalim. Karena menempatkan hak akses bukan pada tempatnya. Sehingga perilaku membobol akun atau menggunakan hak akses login seseorang tanpa izin itu dapat dikategorikan sebagai kezaliman. Sehingga dengan ditambahkan pengamanan pada sistem login menggunakan pengenalan wajah, dapat mengurangi tindak kezaliman. Tentunya dipastikan dengan baiknya kualitas sistem yang dibangun benar-benar dapat menambah tingkat keamanan akun seseorang dari kebobolan.

Tentu dengan jelasnya sumber hukum di atas yang menjadi acuan manusia untuk tidak berlaku zalim, maka setiap manusia juga perlu menanamkan kesadaran di dalam diri untuk mengutamakan kejujuran dalam berperilaku. Karena perilaku jujur adalah merupakan kewajiban bagi setiap manusia. Sebagaimana dalam kitab shahih Bukhori dan Muslim disebutkan sebuah hadits dari Ibnu Mas'ud Radhiallahu'anhu dari Rasulullah

Shallallahu'alaihi wasallam bahwa beliau Shallallahu'alaihi wasallam bersabda:

عن عبد الله بن مسعود رضي الله عنه قال : قال رسول الله صلى الله عليه وسلم : عَلَيْكُمْ بِالصِّدْقِ فَإِنَّ الصِّدْقَ يَهْدِي إِلَى الْبِرِّ وَإِنَّ الْبِرَّ يَهْدِي إِلَى الْجَنَّةِ وَمَا يَزَالُ الرَّجُلُ يَصْدُقُ وَيَتَحَرَّى الصِّدْقَ حَتَّى يُكْتَبَ عِنْدَ اللَّهِ صِدْقًا وَإِيَّاكُمْ وَالْكَذِبَ فَإِنَّ الْكَذِبَ يَهْدِي إِلَى الْفُجُورِ وَإِنَّ الْفُجُورَ يَهْدِي إِلَى النَّارِ وَمَا يَزَالُ الرَّجُلُ يَكْذِبُ وَيَتَحَرَّى الْكَذِبَ حَتَّى يُكْتَبَ عِنْدَ اللَّهِ كَذَابًا رواه مسلم

Artinya: Abdullah bin Mas'ud berkata: "Bersabda Rasulullah : Kalian harus jujur karena sesungguhnya jujur itu menunjukkan kepada kebaikan dan kebaikan itu menunjukkan kepada jannah. Seseorang senantiasa jujur dan berusaha untuk jujur sehingga ditulis di sisi Allah sebagai orang yang jujur. Dan jauhilah oleh kalian dusta karena sesungguhnya dusta itu menunjukkan kepada keburukan dan keburukan itu menunjukkan kepada neraka. Seseorang senantiasa berdusta dan berusaha untuk berdusta sehingga ditulis disisi Allah sebagai seorang pendusta" (HR Muslim Nomor.6586)

Hadits di atas menerangkan bahwa berlaku jujur akan membawa kebaikan. Berlaku jujur untuk tidak mengambil hak orang lain adalah kebaikan. Sehingga dengan menambahkan pengenalan wajah untuk akses login agar seseorang tidak mudah masuk atau membobol akun orang lain adalah juga merupakan usaha untuk kebaikan. Usaha untuk mencegah terjadinya kezaliman dan memaksa orang lain berlaku jujur dalam keseharian.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil dan pembahasan pada bab sebelumnya, maka dapat disimpulkan sebagai berikut:

1. Metode minkowski distance dapat diimplementasikan ke dalam sistem dengan baik menggunakan bahasa pemrograman python, sehingga sistem dapat mendeteksi dan mengenali wajah pengguna akun.
2. Sistem dapat mengenali wajah pengguna dengan tingkat akurasi yang berbeda pada masing-masing percobaan yang dilakukan. Akurasi tertinggi didapatkan pada percobaan dengan menggunakan intensitas yang sama antara citra masukan dengan citra acuan yaitu pada percobaan dengan intensitas cahaya 75lux yang menghasilkan persentase FAR sebesar 30% dan FRR 10% sehingga menghasilkan akurasi sebesar 80%. Pada percobaan dengan intensitas cahaya 100lux menghasilkan persentase FAR sebesar 10% dan FRR 0% sehingga menghasilkan akurasi sebesar 95%. Pada percobaan dengan intensitas cahaya 200lux menghasilkan persentase FAR sebesar 0% dan FRR 10% sehingga menghasilkan akurasi sebesar 95%.

5.2 Saran

1. Penelitian lanjutan perlu dilakukan untuk meningkatkan akurasi pengenalan wajah. Karena akan banyak pengguna dengan wajah yang mirip apabila sistem diberlakukan secara masal. Tingkat error yang tinggi pada kondisi-kondisi tertentu perlu dilakukan perbaikan agar sistem dapat lebih akurat dalam mengenali wajah.
2. Perlu dilakukan perbaikan agar sistem dapat mendeteksi dan mengenali wajah dengan baik meskipun terdapat perbedaan yang mencolok antara citra masukan dengan citra acuan.

DAFTAR PUSTAKA

Al Quran al Karim

Al Hadits Nabi Muhammad Shallallahu ‘Alaihi wa Sallam

Bonneau, Josep. 2012. <http://memobee.com/index.php?do=c.news&idn=6617> diakses pada tanggal 27 Februari 2014

Nasution, Marito. 2010. Rekayasa Sistem Pengenalan Wajah Untuk Proses Log In Sistem Informasi Menggunakan Algoritma Eigenface. *Skripsi*. Medan: Universitas Sumatera Utara

Akbar, Yaumil. 2012. Analisis Identifikasi Rambu-Rambu Lalu Lintas Dengan Pengolahan Citra Digital Menggunakan Metode Template Matching. *Skripsi*. Bandung

Hermawan, Margito. Indra Fajar. 2013. Pengenalan Wajah Dengan Metode Template Matching Sebagai Sistem Starter Sepeda Motor Berbasis Mikrokontroler Atmega 16. *Skripsi*. Surabaya: Institut Teknologi Sepuluh November.

Kamus Besar Bahasa Indonesia. 2014. <http://kbbi.web.id/wajah>. Diakses pada 27 Februari 2014

Ismail, Akmal. 2012. Aplikasi Standard Pelayanan Minimal Dinas Kesehatan Kabupaten Bojonegoro. *Buku Panduan*. Bojonegoro: Tim SDK Kesehatan

Situs Internet dan Teknologi. 2014. <http://id.shvoong.com>. Diakses pada 27 Februari 2014

Situs Edukasi dan Wacana Global. 2014. <http://idkf.bogor.net/yuesbi/e-DU.KU/edukasi.net/SMK/TIK/Webcam/materi2.html> diakses pada 7 Juni 2014

Anil, K. Jain. 1989. *Fundamental of Digital Image Processing*. Prentice Hall: University of Michigan

Gonzalez dan Woods. 2001. *Digital Image Processing*. California: Addison-Wesley Publishing Company

Munir, Rinaldi. 2004. *Pengolahan Citra digital dengan Pendekatan Algoritmik*. Bandung: Informatika Bandung

- Jianwei Yang, Lifeng Liu, Tianzi Jiang. 2003. *A modified Gabor filter design method for fingerprint image enhancement*. National Laboratory of Pattern Recognition. Institute of Automation: Chinese Academy of Sciences
- Leksono, Bowo. 2011. Aplikasi Metode Template Matching untuk Klasifikasi Sidik Jari. *Skripsi*. Semarang: Universitas Diponegoro Semarang
- Pratt, William K. 1991. *Digital Image Processing Second Edition*. New York: John Wiley & Sons, Inc.
- Kamus Besar Bahasa Indonesia. 2014. <http://kbbi.web.id/algorithm> diakses pada 7 Juni 2014
- Fatta, Hanif al. 2009. *Rekayasa Sistem Pengenalan Wajah*. Yogyakarta: CV Andi Offset.
- Tjiharjadi, Semuil. 2011. *Pengenalan Wajah Pelanggan Toko*. Yogyakarta: Seminar Nasional Aplikasi Teknologi Informasi.
- Situs Akademi Pendidikan UNAIR. 2012. <http://erlindamettadewi-fst09.web.unair.ac.id>. Diakses pada 1 Maret 2014
- Gunawan, Krisna. 2013. *Perancangan Sistem Pengenalan Wajah Berbasis Algoritma Principal Component Analysis (PCA)*. *Skripsi*. Bandung: JBPTUNIKOMPP
- Kristanto, Hanny. 2012. *Automatic Mobile Robot Menggunakan Data Kamera Sebagai Pengambil Gambar Jalan Robot*. *Skripsi*. Surabaya: STIKOM
- Reva, Sita Ardhiva. 2014. *Pengembangan Data Warehouse pada Sistem Keuangan*. *Jurnal Ilmiah*. PTIK NR
- Hansen, Gary W. dan Hansen, James V.. 1996. *Database Management and Design*, 2nd ed. New Jersey: Prentice Hall.
- McLeod, Raymond. 1998. *Management Information System*, 7-th ed., New Jersey: Prentice Hall.
- McNurlin, Barbara C dan Sparague, Ralph H Jr.. 1998. *Information Systems Management in Practice*, 4th ed. New Jersey: Prentice Hall.
- Sudirman. 2009. *Macam-macam DBMS(Database Management System)*. *Tulisan Ilmiah*.

- Situs Komputer dan Teknologi. 2014. <http://www.wahyuwinoto.com/2012/04/pengertian-fungsi-dan-komponen-dalam.html>. Diakses pada 1 Maret 2014
- Situs Akademi Pendidikan Universitas Sumatera Utara. 2013. <http://repository.usu.ac.id>. Diakses pada 1 Maret 2014
- Situs Komputer dan Teknologi. 2013. <http://gudanglinux.com/glossary/python/>. Diakses pada 1 Maret 2014
- Rijal, Yusron. Riza, Dhian Ariefianto. 2008. Deteksi Wajah Berbasis Segmentasi Model Warna Menggunakan Template Matching Pada Objek Bergerak. *Skripsi*. Surabaya: Sekolah Tinggi Manajemen Informatika & Teknik Komputer Surabaya
- Mohamad Aditya Rahman. 2010. Sistem Pengenalan Wajah Menggunakan Webcam Untuk Absensi Dengan Metode Template Matching. *Skripsi*. Surabaya: Politeknik Elektronika Negeri Surabaya
- Santo, Febry. 2014. Pengenalan Iris Mata Menggunakan Metode Pencirian Independent Components Analysis (ICA) dan Jarak Minkowski. *Skripsi*. Semarang: Universitas Diponegoro Semarang
- Sugiyono. 2012. Metode Penelitian Kuantitatif Kualitatif dan R&D. Bandung: Alfabeta
- Nyoman. 2010. Teori, Metode dan Teknik Penelitian Sastra. Yogyakarta: Pustaka Pelajar
- Mulyono Tri, Adi Kusworo, Gernowo Rahmat. 2012. Sistem Pengenalan Wajah Dengan Metode Eigenfacedan Jaringan Syaraf Tiruan (JST). *Karya Ilmiah*. Semarang: Universitas Diponegoro

LAMPIRAN

1. Kutipan Kode Program

a. Pendaftaran Akun

```
if self.nama.text() != '' and
self.email.text() != '' and
self.username_2.text() != '' and
self.password_2.text() != '':
try:
    myCursor.execute ("INSERT INTO login
(nama,email,username,password) VALUES
(%s,%s,%s,%s)", [self.nama.text(),
self.email.text(),
self.username_2.text(),
self.password_2.text()])
    alertPopup = QtGui.QMessageBox()
    alertPopup.setText("Sukses Disimpan")
    alertPopup.setIcon(alertPopup.Information
)
    alertPopup.exec_()
    db.name().commit()
    self.nama.setText("")
    self.email.setText("")
    self.username_2.setText("")
    self.password_2.setText("")
```

b. Pengecualian pengisian data

```
else:
    alertPopup = QtGui.QMessageBox()
    alertPopup.setText("Data Harus Diisi
Semua!!")
```

```

alertPopup.setIcon(alertPopup.Information)
alertPopup.exec_()

```

c. Pengecualian Pengisian Username

```

except mdb.Error, e:
    print "Error %d: %s" % (e.args[0],
e.args[1])
    db.name().rollback()
    alertPopup = QtGui.QMessageBox()
    alertPopup.setText("Gagal
Menyimpan!!\nUsername Sudah Ada yang
Menggunakan")
    alertPopup.setIcon(alertPopup.Critical)
    alertPopup.exec_()

```

d. Menyimpan Gambar

```

ekspresi = self.comboBox.currentText()
namafolder = self.username_2.text()
newpath = ((r'E:\Wajah%s') % namafolder)
if not os.path.exists(newpath):
    os.makedirs(newpath)
cv.SaveImage("masukan.jpg", self.ambil)
im = cv2.imread("masukan.jpg")
gray_image = cv2.cvtColor(im,
cv2.COLOR_BGR2GRAY)
cv2.imwrite("E:\Wajah\\"+str(self.username_
2.text())+"\\ "+str(ekspresi)+".pgm",gray_im
age, (90,90))
[a, b]= read(r'E:\Wajah', (90, 90))

```

```

save_model("read.xml", [a, b])
[evalues, evector, mean_image,
shifted_images] = pca(asRowMatrix(a), b)
save_model("value.xml", [evalues, evector,
mean_image, shifted_images])
alertPopup = QtGui.QMessageBox()
alertPopup.setText("Sukses Disimpan!")
alertPopup.setIcon(alertPopup.Information)
alertPopup.exec_()

```

e. Proses Login

```

key = self.password.text()
user = self.username.text()
myCursor.execute ("select * from login")
data = myCursor.fetchall()
for data in data:
    nama = data[3]
    password = data[4]
    print nama, password
    if (user == nama) or (key == password):
        self.pencocokan()

```

f. Implementasi Minkowski Distance

```

selisih = np.asarray(w - w_masuk)
mutlak = np.absolute(selisih)
jarak = (np.sum(mutlak**3, axis=1))**1/3
minimal = min (jarak)
jarak_minimal = jarak.argmin()
mirip = paths[jarak_minimal]

```

```

mirip2
=os.path.basename(os.path.dirname(mirip));
wajah = self.username.text()
if (mirip2==wajah)and(minimal<1500):
alertPopup = QtGui.QMessageBox()
alertPopup.setText("Wajah Cocok")
alertPopup.setIcon(alertPopup.Information)
alertPopup.setWindowTitle("Pencocokan
Wajah")
alertPopup.exec_()
else:
alertPopup = QtGui.QMessageBox()
alertPopup.setText("Wajah Tidak Cocok")
alertPopup.setIcon(alertPopup.Information)
alertPopup.setWindowTitle("Pencocokan
Wajah")
alertPopup.exec_()

```

g. Menampilkan Data

```

myCursor.execute ("select * from datalog
order by waktu desc limit 1")
data = myCursor.fetchall()
for data in data:
    print data[0]
    self.sebagai.setText(data[0])
    self.email.setText(data[1])
    self.tanggal.setText(str(data[3]))

myCursor.execute("SELECT * FROM datalog
order by waktu desc")
baris=myCursor.fetchall()

```

```
self.tablelog.setRowCount(len(baris))
self.tablelog.setColumnCount(6)
for i in range (len(baris)):
    for j in range (6):
        item = Qt.QTableWidgetItem('%s' %
            (baris[i][j]))
        self.tablelog.setItem(i, j, item)

myCursor.execute("SELECT * FROM login order
by id desc")
baris= myCursor.fetchall()
self.tableakun.setRowCount(len(baris))
self.tableakun.setColumnCount(3)
for i in range (len(baris)):
    for j in range (3):
        item = Qt.QTableWidgetItem('%s' %
            (baris[i][j + 1]))
        self.tableakun.setItem(i, j, item)
```