Jurnal Multimedia & Artificial Intelligence, Volume 4, Nomor 1, Februari 2020

Prototype Desain Keamanan Login Menggunakan Biometrik Wajah dengan Metode *Eigenface*

Prototype of Login Security Design Using Face Biometrics with Eigenface Method

Sugeng Widodo [1], Supatman [2]

[12]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Mercu Buana Yogyakarta,
Jl. Wates Km. 10 Yogyakarta 55753, Indonesia
Email: [1]kalibaru09@gmail.com, [2]supatman@mercubuana-yogya.ac.id
Tanggal submisi: 18-08-2019; Tanggal penerimaan: 12-03-2020

ABSTRAK

Masalah keamanan merupakan masalah utama yang harus di perhatikan apabila menggunakan suatu perangkat yang terhubung dalam jaringan luar atau jaringan internet. Untuk itu *user* sering sekali diminta untuk membuat *password* yang unik dan susah ditebak oleh orang lain. Keamanan *login* menjadi masalah utama apabila menggunakan suatu perangkat yang terhubung dalam jaringan luar atau jaringan internet. Karenanya dilakukan suatu pengamanan data menggunakan biometrik wajah. *Eigenface* adalah suatu metode pengenalan wajah yang berdasarkan pada algoritma *Principal Component Analysis* (PCA). Secara singkat prosesnya adalah citra direpresentasikan dalam sebuah gabungan *vector* yang dijadikan satu matriks tunggal. Dari matriks tunggal ini akan diekstraksi suatu ciri utama yang akan membedakan antara citra wajah satu dengan citra wajah lainnya. Dalam penggunaan sistem *login* biometrik wajah ini adalah *user* mendaftar ke sistem kemudian wajah *user* akan di train sehingga *user* akan dikenali oleh sistem untuk keperluan *login*. Pada saat *user* melakukan *login* maka data wajah *user* akan diproses secara *real time* dan dicocokan dengan data yang ada pada *database* sehingga apabila data cocok maka *user* akan berhasil *login*. Jarak wajah dengan webcam standarnya adalah 50-60 cm, sedangkan tingkat pencahayaan minimal wajah dapat dikenali adalah 5 *lux*, dan sudut kemiringan wajah yang masih dapat dikenali sistem adalah 40°. Pada pengujian tes login ada 15 total data, 13 data berhasil dan 2 data gagal, maka persentase keberhasilanya adalah 86%.

Kata Kunci : *biometrik wajah; eigenface; lux meter; principal component analysis (PCA); real time*

ABSTRACT

Security issues are the main problems that must be considered when using a device which is connected in an outside network or internet network. Thus, users are often asked to create unique passwords that are difficult for others to guess. Login security becomes the main problem when using a device connected to the outside network or internet network. Therefore, there should be an action to conduct a data security using facial biometrics. Eigenface is a face recognition method based on the Principal Component Analysis (PCA) algorithm. The process is that the image is represented in a vector combination made into a single matrix. From this single matrix, a feature will be extracted. It is the main thing that will distinguish one face image and another one. In using this face, biometric login system is the user registers to the system, then, the user's face will be trained so that the user will be recognized by the system for login purpose. When a user logs in, the user's face data will be processed in a real time and matched with the existing data in the database. Hence, if the data match, the user login will be successful. The distance between the face and the webcam is 50-60 cm, meanwhile, the minimum lighting level of the face that can be recognized is 5 lux, and the tilt angle of the face that the system can recognize is 40°. In the last login test, there were 15 total data, 13 data succeeded and 2 data failed. Hence, the percentage of success was 86%.

Keywords : *facial biometrics; eigenface; lux meter; principal component analysis (PCA); real time*

1. PENDAHULUAN

Prototype Desain Keamanan Login Menggunakan Biometrik Wajah dengan Metode *Eigenface*

Teknologi komunikasi dan informasi berkembang dengan pesat dan memberikan pengaruh besar bagi kehidupan manusia. Masalah keamanan merupakan masalah utama yang harus di perhatikan apabila menggunakan suatu perangkat yang terhubung dalam jaringan luar atau jaringan internet. Untuk itu *user* sering sekali diminta untuk membuat *password* yang unik dan susah ditebak oleh orang lain. *Password* adalah kumpulan karakter atau *string* yang digunakan oleh pengguna jaringan atau sebuah sistem operasi yang mendukung banyak pengguna *(multiuser)* untuk memverifikasi identitas dirinya kepada sistem keamanan yang dimiliki oleh jaringan atau sistem tersebut. Saat *user* akan melakukan *programming* atau proses pembuatan sebuah aplikasi sering sekali user menjumpai atau mengharuskan user untuk membuat form login untuk keperluan tertentu. Mengingat banyaknya masalah yang timbul apabila *password* tidak terenkripsi dengan baik maka tidak menutup kemungkinan apabila akun terkena *hack* dari orang-orang yang nakal. Karenanya *user* memerlukan pengamanan tambahan guna melakukan mengantisipasi hal-hal yang tidak diinginkan tersebut. Salah satunya adalah dengan menggunakan biometrik sebagai keamananya. Biometrik merupakan pengenalan identitas seseorang berdasarkan bentuk fisiknya contohnya wajah, sidik jari, garis telapak tangan, retina mata, ataupun suara/wicara manusia itu sendiri. Pengenalan biometrik pada wajah merupakan salah satu bidang penelitian yang penting, dan dimanfaatkan dibidang komersial maupun bidang hukum. Teknik pengenalan wajah pada saat ini mengalami kemajuan berarti. Melalui pengembangan suatu teknik seperti eigenface untuk ekstraksi karakteristik wajah. Variasi dalam pencahayaan dan pose seharusnya diminimalisasi untuk pengenalan wajah secara optimal, dengan demikian *preprocessing* dari *database* dan percobaan harus dilakukan. Dalam penelitian ini akan menggunakan karakteristrik ekstraksi dari wajah, dan menggunakan metodologi *Eigenface Face Recognition*.

1. TINJAUAN PUSTAKA

Penelitian yang dilakukan oleh (Hasmin, 2016) yang berjudul "Aplikasi rekam kehadiran dengan deteksi wajah menggunakan metode *eigenface* pada kejaksaan tinggi sulawesi selatan". Beberapa bagian tubuh manusia bisa menjadi identitas pribadi seseorang yang menjadikan seorang manusia berbeda dengan manusia lainnya diantaranya adalah sidik jari, *DNA*, retina mata dan wajah, tentu saja dibutuhkan perangkat khusus untuk dapat mengenali dan mengubah data tersebut menjadi data yang dapat dikenali manusia, seperti teknologi *finger print* dan pemindai retina.

Biometrik

Setiap individu di dunia memiliki wajah yang unik dan bahkan untuk dua anak kembar yang mata manusia hampir sulit untuk membedakanya. Mungkin sesuatu yang kecil seperti penempatan alis yang sedikit unik, lebarnya mata, atau luasnya hidung. Ada penanda yang pasti untuk dapat mengaktifkan pengenalan biometrik ini dalam sepersekian detik untuk dapat mengenali keunikan setiap individu untuk memeriksa keunikan wajah dari setiap elemen. Dengan cara ini dapat memaksimalkan penggunaan *gadget* untuk menjamin itu untuk dapat memperoleh hak akses penggunaan. Pengakuan orang-orang dalam pemanfaatan kualitas wajah tidak dapat disangkal menyadari pentingnya sistem pengenalan wajah . (Kalyani, 2017).

Eigenface

Pengenalan *Eigenface* berasal dari prefiks bahasa Jerman "*eigen*", yang berarti "sendiri/*individual*". Metode *eigenface* dianggap sebagai teknologi pengenalan wajah otomatis pertama yang pernah diciptakan. Teori ini dikembangkan oleh Turk dan Pentland. Teori ini dikembangkan dengan membagi sebuah citra wajah menjadi data set fitur karakteristik yang disebut *eigenface*.

Eigenface adalah suatu metode pengenalan wajah yang berdasarkan pada algoritma *Principal Component Analysis* (PCA). Secara singkat prosesnya adalah citra direpresentasikan dalam sebuah gabungan *vector* yang dijadikan satu matriks tunggal. Dari

matriks tunggal ini akan diekstraksi suatu ciri utama yang akan membedakan antara citra wajah satu dengan citra wajah lainnya. Citra yang digunakan adalah citra digital dengan format *grayscale* untuk mempermudah komputasinya. Dengan membandingkan antara citra uji dengan citra referensi menggunakan konsep jarak *euclidean*, maka akan didapat kesimpulan apakah suatu citra wajah dikenali atau tidak dikenali. (Kustian, 2017).

Perhitungan Principal Component Analysis (PCA)

PCA adalah teknik statistik yang sudah digunakan secara luas baik dalam hal pengolahan data, pembelajaran mesin, maupun pengolahan citra atau pemrosesan signal. Metode *Principal Component Analysis* (PCA) dibuat pertama kali oleh para ahli statistik dan ditemukan oleh Karl Pearson pada tahun 1901 yang memakainya pada bidang biologi. Pada tahun 1947 teori ini ditemukan kembali oleh Karhunen, dan kemudian dikembangkan oleh Loeve pada tahun l963, sehingga teori ini juga dinamakan *Karhunen-Loeve transform* pada bidang ilmu telekomunikasi. PCA digunakan digunakan untuk menyederhanakan suatu data, dengan cara mentransformasi data secara linier sehingga terbentuk sistem koordinat baru dengan *varians* maksimum. Analisis komponen utama dapat digunakan untuk mereduksi dimensi suatu data tanpa mengurangi karakteristik data tersebut secara signifikan. Analisis komponen utama juga sering digunakan untuk menghindari masalah *multikolinearitas* antar peubah bebas dalam model regresi berganda. Analisis komponen utama merupakan analisis antara dari suatu proses penelitian yang besar atau suatu awalan dari analisis berikutnya, bukan merupakan suatu analisis yang langsung berakhir. Misalnya komponen utama bisa merupakan masukan untuk regresi berganda atau analisis faktor atau analisis gerombol. Analisis komponen utama juga merupakan salah satu teknik statistika multivariat yang dapat menemukan karakteristik data yang tersembunyi. Dalam penerapannya, analisis komponen utama, justru dibatasi oleh asumsi-asumsinya,yaitu asumsi kelinearan model regresi, asumsi keorthogonalan komponen utama, dan asumsi *varians* yang besar memiliki struktur yang penting.

Principal Component Analysis (PCA) merupakan salah satu hasil berharga dari aljabar linear terapan. Prosedur PCA pada dasarnya adalah bertujuan untuk menyederhanakan variabel yang diamati dengan cara menyusutkan (mereduksi) dimensinya. Hal ini dilakukan dengan cara menghilangkan korelasi diantara variabel bebas melalui transformasi variabel bebas asal ke variabel baru yang tidak berkorelasi sama sekali tanpa menghilangkan informasi penting yang ada di dalamnya atau yang biasa disebut dengan *principal component*. Dengan reduksi ini maka waktu komputasi dapat dikurangi dan *kompleksititas* dari citra wajah yang tidak perlu dapat dihilangkan. *Principal Component Analysis* menggunakan vektor-vektor yang disebut dengan *eigenvector* dan nilai-nilai yang disebut dengan *eigenvalue* untuk mendapatkan fitur yang paling signifikan pada dataset. (Kustian, 2017).

Proses Perhitungan *Principal Component Analysis* (PCA) dapat dilakukan dengan langkah-langkah sebagai berikut :

a. Mengambil satu set citra wajah (M). misalkan M berjumlah 10 buah citra wajah.
b. Inisialisasi *r* untuk tiap citra wajah dari *set training r* adalah sebuah *vector* n^2 x 1 berdasarkan *matrix* dari citra wajah yang berukuran NxN.
c. Menghitung rata-rata *vector* citra wajah

$$Y = \frac{1}{M}\sum_{i-1}^{M} r_i \text{ .....} \quad (1)$$

d. Melakukan normalisasi ukuran citra dengan melakukan pengurangan *vector* citra wajah dengan nilai rata-rata tersebut.

$$Q = r_i \text{.....} \quad (2)$$

e. Jika sudah maka langkah selanjutnya adalah menghitung *matrix* kovarian

$$C = \frac{1}{M}\sum_{i-1}^{M} Q_n Q_n^T = AA^T(matriks\ N^2 x N^2). \text{ .....} \quad (3)$$

Dimana :

$$A = [Q_1 Q_2 Q_3 \dots Q_M](matriks\ N^2 x M \text{ .....} \quad (4)$$

f. Jika ukuran *matrix* terlalu besar maka pencarian *matrix* kovarian menjadi :

$$C = A^T A \text{ .....} \quad (5)$$

g. Menghitung *eigenvalue* (λ) dan *eigenvector* (x) dari *matrix* kovarian

$$C = A^T A \text{.....} \quad (6)$$

h. Menghitung *eigenvector* sebanyak M dari *matrix* kovarian

$$C = AA^T \text{.....} \quad (7)$$

Dengan persamaan :

$$U_i = A.x_1 \text{.....} \quad (8)$$

i. Melakukan normalisasi terhadap u.
j. Mengumpulkan *eigenvector* sebanyak K.

2. METODOLOGI PENELITIAN

Perancangan Tabel

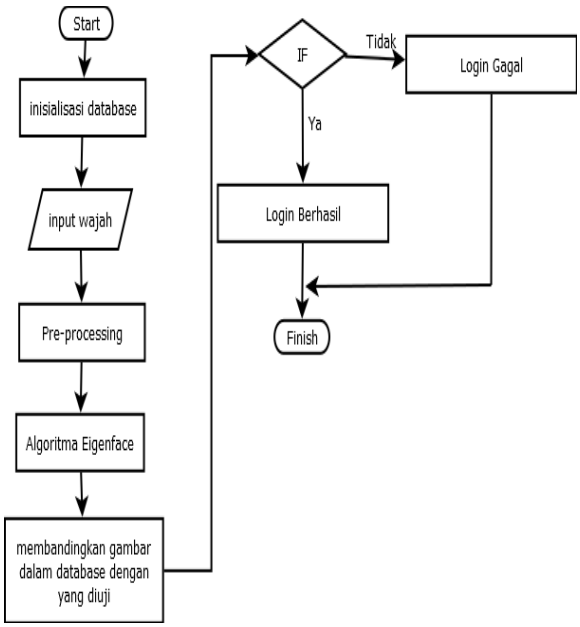
Tabel Biodata digunakan untuk proses mendaftar anggota baru dan juga berfungsi untuk data *login*. Struktur tabel biodata dapat dilihat pada Tabel 1.

Tabel 1. Tabel Biodata

Nama Field	Type	Length	Keterangan
ID	Int	10	Primary key
Nama	Varchar	30	
Tanggal	Date	-	
JamMasuk	Time	-	
Keterangan	Varchar	20	

Desain Sistem

Perangkat lunak akan melakukan *pre-processing*, kemudian mengekstraksi karakteristik wajah menggunakan *eigenface* lalu menyimpan nilai *matrix* untuk proses identifikasi. Pencarian karakteristik gambar akan melalui *pre-processing* kemudian gambar akan diproses menggunakan *eigenface* gambar akan dicari nilai *matrix* yang lebih kecil dan disimpan sebagai karakteristik. Alur sistem keseluruhan dijelaskan pada Gambar 1.

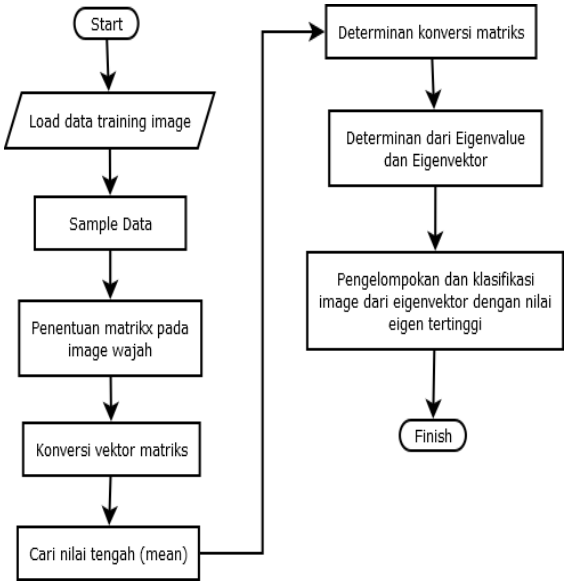


.

Gambar 1. Flowchart Sistem Keseluruhan

Desain Algoritma Identifikasi Image

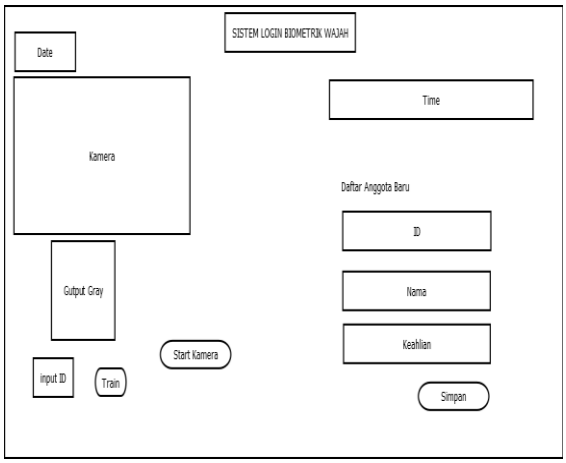
Desain Algoritma Identifikasi *Image* dengan *Eigenface* dapat dilihat pada Gambar 2.



Gambar 2. Desain Algoritma Identifikasi *Image* dengan *Eigenface*

Desain Antar Muka

Perancangan antarmuka diperlukan untuk mempermudah pengguna menggunakan sistem biometrik wajah ini. Sistem ini memiliki satu tampilan *front end* yang terdiri dari beberapa menu diantaranya adalah menu daftar anggota, menu *train* dan menu login.



Gambar 3. Halaman utama (front *end*)

3. PEMBAHASAN

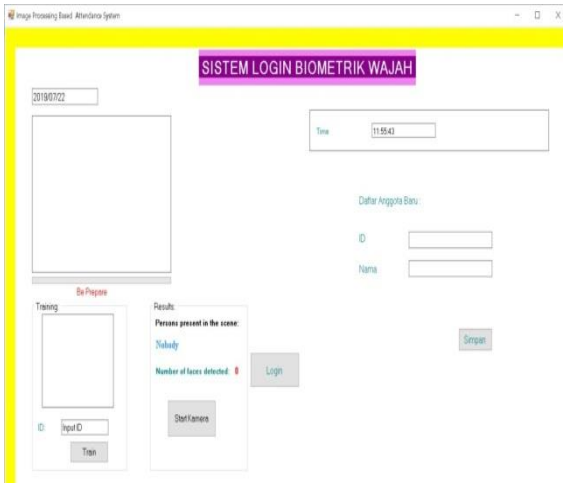
Analisis dan pembahasan akan menjelaskan mengenai hasil dari penelitian *prototype* desain keamanan login menggunakan biometrik wajah yang telah diproses dari hasil pengujian.

Hasil Penelitian

Hasil Pengujian yang dilakukan pada sistem keamanan login biometrik wajah dengan metode *eigenface* menunjukan unjuk kerja sistem yang sesuai dengan data yang didapat.

Hasil Implementasi Desain Program

Implementasi desain sistem adalah pengkodean sistem agar sesuai dengan desain sistem yang telah didesain sebelumnya.



Gambar 4. Halaman Utama *(Front End)*

Analisis dan Pembahasan

Analisis sistem dilakukan dengan melakukan proses pendaftaran *user*, kemudian melakukan proses *train* atau pengenalan wajah, semakin banyak wajah di *train* maka akan semakin baik sistem mengenali, sebelum *image* disimpan kedalam *database*, *image* akan melalui proses *grayscaling* yaitu mengubah *image* RGB menjadi image *grayscale* untuk mendapatkan vector ciri dan mendapatkan jarak *distance* yang nantinya akan digunakan pada proses pengenalan wajah.

Setelah didapatkan nilai grayscale kemudian image akan melalui tahap thresholding, yaitu untuk mengubah citra berderajat keabuan menjadi citra biner atau hitam putih. Intensitas pixel citra hasil grayscale dibandingkan dengan nilai ambang (threshold). Jika nilai pixel lebih besar dari nilai ambang, maka pixel akan direpresentasikan dengan warna putih. Dan sebaliknya jika nilai *pixel* lebih kecil maka akan direpresentasikan dengan warna hitam. Setelah proses *grayscale* dan *threshold* terpenuhi maka image akan disimpan kedalam database.

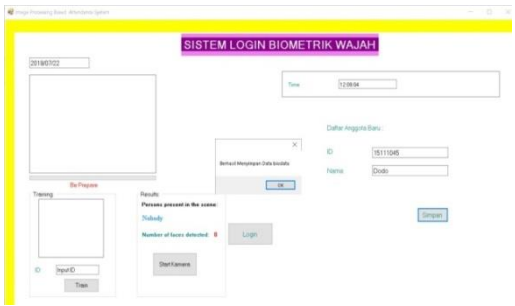
Dilanjutkan dengan tes *login* pada aplikasi. Proses *login* akan membandingkan citra yang ada dalam database dengan citra tes yang akan dibandingkan dengan menggunakan algoritma *eigenface* untuk mencari nilai citra yang terdekat pada database dengan nilai citra tes.

Uji Fungsionalitas

Pada uji fungsionalitas sistem akan dilakukan proses *train* (pengenalan wajah) dan proses tes *login* yaitu proses pencocokan wajah yang ada dalam *database* dengan wajah baru saat proses *login*.

Proses Tambah Anggota

Proses tambah anggota dapat dilihat pada Gambar 5.



Gambar 5. Proses tambah anggota

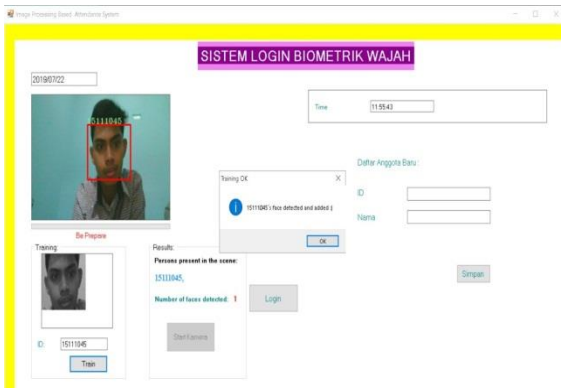
Proses tambah anggota akan disimpan pada *database* MySQL. Untuk lebih jelasnya lihat Gambar 6.

	ID	Nama	Tanggal	jamMasuk	keterangan
Ubah Salin Hapus	1506110	Beatrice K. Ingulima	2019-08-07	09:20:33	Berhasil
Ubah Salin Hapus	1900001	Laode hartono	2019-08-06	00:00:00	
Ubah Salin Hapus	15011059	Teguh Supriono	2019-08-06	12:04:15	Berhasil
Ubah Salin Hapus	15021064	M. hasbi	0000-00-00	00:00:00	
Ubah Salin Hapus	15021069	M. Anjas	2019-08-06	12:09:31	Berhasil
Ubah Salin Hapus	15021087	Syofiyan	2019-08-06	12:30:15	Berhasil
Ubah Salin Hapus	15021151	Nur kholik	2019-08-06	11:24:15	Berhasil
Ubah Salin Hapus	15031027	Dedek satria wijaya	2019-08-06	13:03:38	Berhasil
Ubah Salin Hapus	15071055	Indah Rahmayanti	0000-00-00	00:00:00	
Ubah Salin Hapus	15071060	Nur Chasanah	0000-00-00	00:00:00	
Ubah Salin Hapus	15081125	M. Noval K	2019-08-06	19:03:52	Berhasil
Ubah Salin Hapus	15111006	David Saputra	0000-00-00	00:00:00	

Gambar 6. Data anggota disimpan pada *database*

Proses Train Wajah

Proses *train* wajah dilakukan dengan melakukan lima kali *train* yaitu saat posisi wajah menghadap ke depan, kanan, kiri, atas dan bawah. guna agar sistem lebih mengenal detail wajah. Pada proses *train* wajah dilakukan uji coba dengan *lux light meter* nilai 19 *lux*. Proses *train* wajah dapat dilihat pada Gambar 7.



Gambar 7. Proses Train Wajah

Proses Tes Login

Pada proses tes login akan di lakukan proses pencocokan secara *real time* antara citra wajah dengan data citra wajah yang ada pada *database*. Proses pengujian tes wajah akan dilakukan dengan berbagai pose, diantaranya yaitu pose saat menghadap ke depan, kanan, kiri, atas, dan bawah. Dan akan dilakukan dengan berbagai tingkat pencahayaan dengan parameter yang digunakan yaitu *lux light meter* (satuan *lux*). Proses tes *login* dapat lihat pada tabel-tabel dibawah ini:

Pengukuran jarak standar yang dapat digunakan untuk proses login. Pengukuran jarak standar dapat dilihat pada Tabel 2.

Tabel 2. Jarak Standar

No	Jarak (*Centi Meter*)	Keterangan
1	20 cm	Tidak teridentifikasi
2	30 cm	Tidak teridentifikasi
3	40 cm	Tidak teridentifikasi
4	50 cm	Teridentifikasi
5	60 cm	Teridentifikasi
6	70 cm	Tidak teridentifikasi
7	80 cm	Tidak teridentifikasi
8	90 cm	Tidak teridentifikasi
9	100 cm	Tidak teridentifikasi

Keterangan:
Dari percobaan jarak wajah dan webcam yang didapat maka jarak standarnya adalah 50-60 cm.

Tingkat kemiringan (sudut) wajah, mengukur sudut wajah dilakukan dengan menggunakan busur derajat sebagai alat ukur. Tingkat sudut wajah saat menengok akan sangat berpengaruh dalam penentuan *matching* sistem saat *login*. Tingkat sudut wajah yang telah diukur dapat dilihat pada Tabel 3.

Tabel 3. Tes Sudut Kemiringan Wajah

No	Posisi Wajah	Tingkat Kemiringan	Keterangan
1	Lurus depan	0°	Berhasil
2	Menghadap kanan	10°	Berhasil
		20°	Berhasil
		30°	Berhasil
		40°	Berhasil
		50°	Gagal
3	Menghadap kiri	10°	Berhasil
		20°	Berhasil
		30°	Berhasil
		40°	Berhasil
		50°	Gagal
4	Menghadap atas	10°	Berhasil
		20°	Berhasil
		30°	Berhasil
		40°	Berhasil
		50°	Gagal
5	Menghadap bawah	10°	Berhasil
		20°	Berhasil
		30°	Berhasil
		40°	Berhasil
		50°	Gagal

Keterangan:
Dari tes sudut kemiringan maka dapat disimpulkan yaitu sudut kemiringan yang masih dapat mengenali wajah adalah 40°.

Tes *gesture* wajah dan *accessoris*, gesture wajah user yang berubah-ubah akan di tes *login* dalam sistem beserta *accessoris* yang digunakan sehingga nantinya akan didapatkan data hasil. Tabel Tes *gesture* wajah dan *accessoris* dapat dilihat pada Tabel 4. Dan Tabel 5.

Tabel 4. Tes *Gesture* Wajah dan *Accerssoris*

No	*Gesture* dan *Accesoris*	Keterangan
1	Senyum	Berhasil
2	Tertawa	Berhasil
3	Memejamkan mata	Berhasil

Tabel 5. Tes Gesture Wajah dan Accerssoris (Lanjutan)

No	*Gesture* dan *Accesoris*	Keterangan
4	Menjulurkan lidah	Berhasil
5	Mengerutkan kening	Berhasil
6	Mata melotot	Berhasil
7	Mulut manyun	Berhasil
8	Pipi menggembung	Berhasil
9	Memakai kacamata	Gagal
10	Memakai peci	Berhasil
11	Memakai masker	Gagal

Keterangan:
Total alat adalah 11 data, diantaranya 9 data berhasil dan 2 data gagal. Maka hasil dari percobaan login pada gesture dan accessoris wajah, gagal pada kondisi saat wajah memakai kacamata dan memakai masker.

Pengujian *login* dengan *lux light meter* dapat dilihat pada Tabel 6.

Tabel 6. Tes Tingkat Pencahayaan

No	Tingkat Pencahayaan	Keterangan
1	1 *lux*	Gagal
2	3 *lux*	Gagal
3	5 *lux*	Berhasil
4	10 *lux*	Berhasil
5	15 *lux*	Berhasil
6	19 *lux*	Berhasil
7	25 *lux*	Berhasil
8	46 *lux*	Berhasil
9	70 *lux*	Berhasil
10	152 *lux*	Berhasil
11	212 *lux*	Berhasil
12	241 *lux*	Berhasil

Keterangan:
Dari tes tingkat pencahayaan maka dapat disimpulkan apabila tingkat pencahayaan dibawah 5 *lux* maka wajah tidak terdefinisi.

Percobaan tes *login*, pada percobaan ini akan dilakukan guna untuk mengetahui seberapa akurat aplikasi dapat mengenali wajah *user*. Percobaan tes *login* dapat dilihat pada Tabel 7.

Tabel 7. Tes Login

No	Nim (ID)	Status
1	15111045	Berhasil
2	15031027	Berhasil
3	15021069	Berhasil
4	15021154	Berhasil
5	15021087	Berhasil
6	15011059	Berhasil
7	15021064	Gagal
8	18021018	Berhasil
9	17081172	Berhasil
10	17021089	Berhasil
11	15111058	Berhasil
12	18031008	Gagal
13	15111027	Berhasil
14	15111059	Berhasil
15	15111018	Berhasil

Keterangan:
Pada 15 kali percobaan, didapat data 13 kali berhasil dan 2 kali gagal. Maka diperoleh 86%.

4. KESIMPULAN

Dari penelitian yang dilakukan, kesimpulan yang dapat diambil adalah jarak wajah dengan webcam standarnya adalah 50-60 cm, sedangkan tingkat pencahayaan minimal wajah dapat dikenali adalah 5 *lux*, dan sudut kemiringan wajah yang masih dapat dikenali sistem adalah 40°.

Pengujian gesture dan accessories wajah didapatkan total data 11 data, 9 data berhasil dan 2 data gagal, yaitu pada kondisi saat wajah memakai kacamata dan memakai masker.

Pada pengujian tes login ada 15 total data, 13 data berhasil dan 2 data gagal, maka persentase keberhasilanya adalah 86%.

5. UCAPAN TERIMA KASIH

Terimakasih Kepada seluruh dosen Informatika, FTI, Universitas Mercu Buana Yogyakarta dan Teman-Teman FTI 2015.

DAFTAR PUSTAKA

Agustina, I., Fauziah, & Gunaryati, A. 2016. Biometrik pola suara dengan jaringan saraf tiruan. *JURNAL TEKNIK INFORMATIKA VOL 9 NO. 2*, Hal: 140-147, ISSN: 1979-9160.

Andarinny, A. A., Widodo, C. E., & Adi, K. 2017. Perancangan sistem identifikasi biometrik jari tangan menggunakan Laplacian of Gaussian dan ektraksi kontur. *Youngster Physics Journal*, Hal: 304-314, ISSN: 2302 - 7371.

Apriadi, A., Michrandi, S., & Azmi, F. 2016. Perancangan otentikasi sidik jari pada biometrik payment design of authentication fingerprint for biometric payment. *e-Proceeding of Engineering*, Hal: 824-830, ISSN : 2355-9365.

Auliannisa, Rizkia Dwi; Suratman, Fiky Yosef; Rizal, Achmad. 2017. Deteksi Katarak Menggunakan Metode Transformasi Hough Berbasis Android. *e-Proceeding of Engineering : Vol.4, No.3*, Hal: 3310-3319, ISSN: 2355-9365.

Barri, M. W., Lumenta, A. S., & Wowor, A. 2015. Perancangan Aplikasi SMS GATEWAY Untuk Pembuatan Kartu Perpustakaan di Fakultas Teknik Unsrat. *E-journal Teknik Elektro dan Komputer*, Hal : 23-28, ISSN : 2301-8402.

Firman, A., Wowor, H., & Najoan, X. 2016. Sistem Informasi Perpustakaan Online Berbasis Web. *E-journal Teknik Elektro dan Komputer*, Hal : 29-36, ISSN : 2301-8402.

Hasmin, E. 2016. Aplikasi rekam kehadiran dengan deteksi wajah menggunakan metode eignface pada kejaksaan tinggi sulawesi selatan. Seminar Nasional *Teknologi Informasi dan Multimedia 2016*, Hal: 411-416, ISSN: 2302-3805.

Kalyani. 2017. Various Biometric Authentication Techniques: A Review. Journal *of Biometrics & Biostatistics*, Hal: 1-5, ISSN: 2155-6180.

Kustian, N. 2017. Analisis komponen utama menggunakan metode eigenface terhadap pengenalan citra wajah. jurnal *teknologi*, Hal : 44-48, ISSN : 2085 – 1669.

Masrani, H., Ilhamsyah, & Ruslianto, I. 2018. Aplikasi pengenalan pola pada huruf tulisan tangan menggunakan jaringan saraf tiruan dengan metode ekstraksi fitur geometri. *Jurnal Coding, Sistem Komputer Untan*, Hal: 69-78, ISSN: 2338-493X.

Nugroho, E. 2009. *Biometrika Mengenal Sistem Identifikasi Masa Depan.* Yogyakarta: C.V ANDI OFFSET.

Nugroho, H. 2017. Image Enhancement Pada Screen Capture CCTV Dengan Menggunakan Metode Histogram Ekualisasi. *KINETIK*, hal: 99-106, ISSN: 2503-2259.

Pamungkas, P. D., & Hariri, F. R. 2016. Pengenalan Citra Tanda Tangan Menggunakan Metode. *Citec Journal*, Hal: 269-279, ISSN: 2460-4259.

Yahya, & Nur, M. A. 2018. Pengaruh Aplikasi C# dalam Proses

Perhitungan Numerik. *Jurnal* Informatika *dan Teknologi*, hal: 79 – 87, e-ISSN 2614-8773.