

SISTEM PENGENALAN WAJAH UNTUK KEAMANAN *FOLDER* MENGGUNAKAN METODE *TRIANGLE FACE*

Putra Prima Arhandi¹, Ulla Delfana Rosiani², Atika Prasetyawati³, Priska Choirina⁴

^{1,2} Prodi Teknik Informatika, Jurusan Teknologi Informasi, ³ Politeknik Negeri Malang
putraprima@gmail.com¹, ullarosi@gmail.com², atikaprasetyawati11@gmail.com³,
priskachoirina17@gmail.com⁴

Abstrak

Keamanan ruangan atau *folder* yang baik memiliki sistem penguncian yang baik yaitu memiliki kemungkinannya kecil terjadi pembobolan sehingga perlu ditambahkan sistem keamanan yang sulit untuk dimanipulasi oleh orang tertentu. Sistem keamanan yang digunakan pada sistem ini menggunakan teknologi biometrika pengenalan wajah yaitu dengan menggunakan ciri – ciri fisik manusia yang memiliki karakteristik yang berbeda – beda yang selalu melekat pada manusia. Dalam aplikasinya, pengenalan wajah dilakukan dengan menggunakan sebuah kamera atau *webcam* untuk menangkap wajah seseorang yang kemudian akan dibandingkan dengan wajah yang sebelumnya telah disimpan di dalam *database* tertentu. Dalam penelitian ini, sistem dirancang dengan deteksi wajah menggunakan metode *Triangle Face*. Identifikasi wajah dilakukan dengan mendeteksi fitur – fitur pada wajah seperti jarak antar mata, jarak mata kanan ke hidung, jarak mata kiri ke hidung, jarak mata kanan ke mulut dan jarak mata kiri ke mulut yang akan membentuk segitiga serta ukuran lebar dan tinggi wajah. Dari perancangan sistem yang telah dijelaskan diatas didapatkan hasil bahwa sistem pengenalan wajah menggunakan metode *Triangle Face* ini memiliki keakuratan yang baik yaitu 82,6%, sehingga dapat dikatakan sistem ini cukup aman untuk diaplikasikan dalam mengakses ruang folder komputer.

Kata kunci : *sistem pengenalan wajah, webcam, folder, triangle face*

1. Pendahuluan

Folder merupakan sebuah ruang pada komputer yang digunakan untuk menyimpan data – data berharga yang tidak sembarang orang dapat membuka untuk mencari suatu data pribadi, hanya orang tertentu yang dapat membuka folder tersebut terutama pemilik komputer atau *PC*. Selain itu, saat ini banyak terjadi kasus pencurian komputer atau *PC*, dimana komputer tersebut terdapat data – data penting yang disimpan didalamnya. Sehingga dalam hal ini dibutuhkan sistem keamanan pada komputer agar tidak sembarang orang dapat mencuri data – data yang tersimpan didalamnya.

Sistem keamanan saat ini banyak digunakan untuk memberikan keamanan pada data yang berharga agar tidak dapat digunakan oleh sembarang orang, namun dalam hal ini masih banyak sistem keamanan yang menggunakan *password* (Miftah, 2016). Dengan perkembangan teknologi informasi saat ini, penggunaan *password* atau kata sandi dapat dirusak (*hack*) oleh orang yang tidak bertanggung jawab. Teknik biometrika merupakan sebuah teknologi yang biasa digunakan untuk fitur keamanan menggunakan ciri – ciri fisik tubuh manusia yang khas seperti berupa pengenalan wajah (*face recognition*), sidik jari (*finger print*), retina dan

pupil yang memiliki karakteristik yang berbeda – beda diantaranya tidak dapat hilang, sulit dipalsukan dan selalu melekat pada manusia (Siregar, 2014). Sehingga teknik biometrik ini aman untuk digunakan sebagai sistem keamanan dengan tambahan metode untuk mencapai keakuratan dan keamanan yang tepat.

Metode *Triangle Face* dapat digunakan sebagai pendukung autentikasi *face recognition* yang memiliki keakuratan lebih baik yaitu mencapai 90% (Miftah, 2016), karena menggunakan fitur – fitur wajah yang membentuk segitiga pada wajah (mata, hidung dan mulut). Dari fitur tersebut akan dicari nilai jarak antar mata, jarak mata ke mulut, mata ke hidung, lebar wajah serta tinggi wajah. Jarak ini yang nantinya akan dijadikan pembeda antara orang satu dengan orang lain (Siregar, 2014).

2. Landasan Teori

2.1 Folder

Folder merupakan ruangan – ruangan pada sebuah komputer yang berfungsi sebagai tempat penyimpanan berkas – berkas (*file*) yang berupa teks, gambar, video, kode, program dan sebagainya. *Folder* pada dasarnya dapat diakses oleh siapa saja. Oleh sebab itu, tingkat keamanan data – data yang

terdapat di dalamnya harus dijaga agar tidak sembarang orang dapat mengaksesnya.

Keamanan *folder* merupakan salah satu cara untuk memberikan suatu sistem keamanan yang berguna untuk mengamankan data atau *file* yang bersifat rahasia dan penting yang ada di dalamnya salah satu penerapannya dengan memberikan *password* berupa huruf/angka atau sandi. Dimana dalam hal ini, sebuah software dapat mengunci *folder* (*directory*) beserta *file*, karena untuk membuka *folder* tersebut harus memasukkan *password* yang telah tersimpan sebelumnya (Siregar, 2014).

2.2 Pengolahan Citra Digital

Pada tahun 1960-an diluncurkan komputer yang mampu melakukan pengolahan citra. Komputer tersebut adalah pemicu cepatnya perkembangan teknologi pengolahan citra digital. Pada tahun 1964 terjadi proses pengolahan citra berupa perbaikan kualitas citra bulan dari distorsi di laboratorium Jet Propulsion (Putra, 2010).

Pengolahan citra digital mengacu pada pemrosesan setiap data 2 dimensi. Citra digital merupakan sebuah larik (*array*) yang berisi nilai – nilai *real* maupun kompleks yang direpresentasikan dengan deretan bit tertentu, dimana pengolahan citra digital digunakan sebagai teknologi pengamanan suatu sistem yang mengalami kemajuan sangat pesat. Sebagai contoh pemanfaatan sidik jari, iris, wajah, dan biometrika yang lainnya untuk sistem identifikasi seseorang (Putra, 2010).

2.3 Verifikasi dan Identifikasi

Aplikasi pengenalan wajah meliputi verifikasi dan identifikasi. Verifikasi merupakan sebuah pengenalan wajah yang digunakan untuk memastikan kebenaran dari wajah yang ingin dikenali. Sedangkan identifikasi merupakan sebuah pengenalan yang ditujukan untuk mengenali wajah tertentu yang dibandingkan dengan database untuk mengetahui wajah siapa orang tersebut (Fahmi, 2012).

2.4 Metode *Triangle Face*

Triangle Face merupakan salah metode yang digunakan untuk mengenali wajah seseorang pada suatu citra digital. Metode ini dapat mengenali seseorang dengan mendeteksi fitur – fitur wajah yang terdapat pada citra masukan seperti mata, hidung, mulut, serta lebar dan tinggi citra yang akan membentuk segitiga sehingga disebut *Triangle Face*. Setelah fitur – fitur tersebut ditemukan, maka akan dicari jarak antar fitur untuk dijadikan pembandingan fitur wajah manusia satu dengan yang lain seperti (Chiunsun):

- a. Jarak mata kiri – mata kanan (Mki - Mka).
- b. Jarak mata kanan – mulut (Mka - Mu).
- c. Jarak mata kiri – mulut (Mki - Mu).
- d. Jarak mata kanan – hidung (Mki - H).
- e. Jarak mata kiri – hidung (Mki - H).

Secara garis besar, metode ini akan melalui beberapa tahapan dalam pengenalan wajah seperti:

1. Deteksi Wajah

Tahap awal dalam pengenalan wajah adalah menentukan yang mana wajah orang yang akan dikenali untuk dianalisa. Kemudian dilakukan pemotongan area wajah untuk mempersempit ruang dalam pengolahan citra serta untuk menentukan ciri yang akan digunakan. Pada fase ini diambil nilai – nilai yang terdapat dalam koordinat tersebut untuk membentuk segi empat yang mengelilingi wajah (*bounding box*) menggunakan *Haar Cascade Classifier*.

Haar Classifier ini merupakan sebuah fungsi matematika yang berbentuk kotak atau persegi yang memiliki sifat komputasi yang bergantung pada jumlah pixel (Sajati,2015).



Gambar 1. Dataset Database Wajah

2. Pencarian Posisi Mata

Pencarian fitur wajah dilakukan pendeteksian tepi – tepi area wajah, area wajah membentang dari sisi atas wajah sampai sisi bawah wajah. Dalam menentukan fitur mata dilakukan menggunakan *Haar Classifier*.

3. Pencarian Posisi Hidung

Dalam pencarian posisi hidung, dilakukan sama seperti tahap pencarian posisi mata, menggunakan algoritma *Haar Cascade*.

4. Pencarian Posisi Mulut

Dalam pencarian posisi mulut, dilakukan dengan mempersempit area pencarian posisi mulut dalam wajah.

5. Penentuan titik ukur

Setelah didapatkan fitur – fitur wajah, maka langkah selanjutnya adalah menentukan titik ukur fitur yang digunakan untuk menemukan titik – titik pusat koordinat pixel x dan y pada tiap fitur wajah.

6. Pengukuran jarak antar fitur

Setelah menemukan titik pusat koordinat tiap fitur wajah, maka akan dilakukan pengukuran jarak antar fitur seperti yang telah disebutkan di atas fitur – fitur yang akan dicari jaraknya dengan menggunakan persamaan seperti berikut:

$$F_i = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \quad (1)$$

7. Normalisasi

Normalisasi digunakan untuk menghilangkan pengaruh perbedaan ukuran citra objek ketika dilakukan pengukuran pada penentuan titik ukur tiap fitur. Normalisasi dapat dilakukan menggunakan persamaan seperti berikut:

$$f_i = \frac{F_i}{\sum_{i=1}^n F_i} \quad (2)$$

Pada persamaan normalisasi diatas nilai normalisasi didapatkan dari hasil ukur tiap masing – masing fitur dibagi dengan penjumlahan semua fitur yang digunakan pada setiap citra wajah (Choirina, 2015).

2.5 Euclidean Distance

Euclidean Distance untuk mengukur tingkat kemiripan antara data latih dan data tes. Fitur – fitur wajah yang akan diidentifikasi yaitu mata, hidung, dan mulut dengan menggunakan persamaan Euclidean:

$$D(A, B) = \sqrt{\sum_{i=0}^n (|A_i - B_i|)^2} \quad (3)$$

Keterangan :

D(A,B) = Euclidean Distance antara A

dan B

A= Vektor ciri data tes

B= Vektor ciri data latih

n = Panjang vektor A dan B

2.6 EmguCV

EmguCV merupakan sebuah *cross platform library* yang terdapat pada OpenCV yang digunakan sebagai pemrosesan gambar dengan bahasa yang kompatibel dengan .NET seperti C#, VB, VC++, IronPython dan sebagainya.

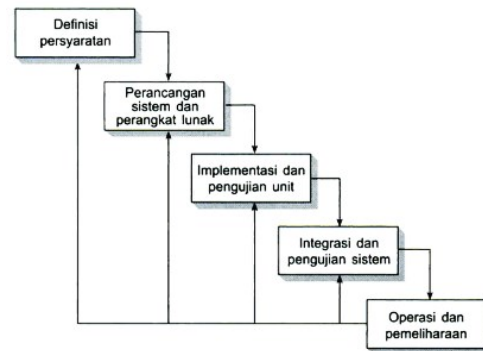
EmguCV ditulis dalam bahasa C# yang dapat dikompilasi yang pada platform mendukung termasuk iOS, Android, Windows Phone, Mac OS X dan Linux (Sommerville, 2003).

3. Metode Penelitian

3.1 Tahapan Penelitian

Metode pembuatan sistem ini menggunakan model *Waterfall*. Model ini mengambil kegiatan proses dasar seperti spesifikasi, pengembangan, validasi, dan evolusi sebagai fase – fase proses yang

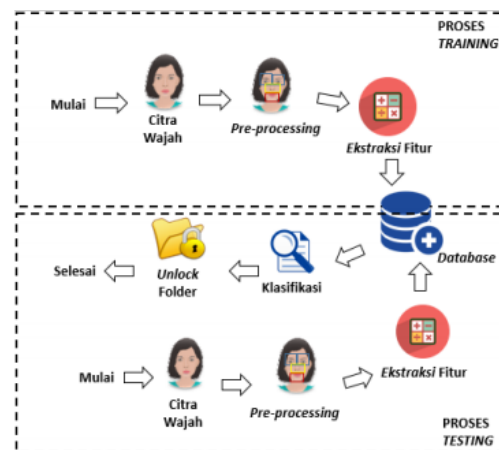
berbeda seperti spesifikasi persyaratan, perancangan perangkat lunak, implementasi, pengujian, dan seterusnya. Adapun tahapan – tahapan berikut ini:



Gambar 2. Model Waterfall.

3.2 Pengolahan Data

Pengolahan data merupakan pengolahan yang digunakan untuk keamanan *folder* menggunakan pengolahan citra. Pengolahan data ini terdiri dari proses *training* dan proses *testing*. Berikut adalah alur dari proses *training* dan *testing*.



Gambar 3. Proses Pengolahan Data

3.3 Metode Pengujian

3.3.1 Pengujian Performansi

Dalam proses pengujian performansi meliputi pengujian pendeteksi jarak kamera pada objek, pengujian deteksi wajah dan fitur wajah

a. Pengujian jarak kamera pada objek wajah

Pada pengujian ini hanya dilakukan pada wajah yang pendeteksiannya tepat pada area wajah yang tegak lurus dengan ketinggian *webcam*.

Tabel 1, Pengujian pendeteksi wajah

Objek	Jarak wajah (cm)			
	30	40	50	60

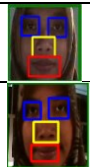
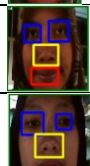

1	√	√	√	-
2	√	√	-	-
3	√	√	-	-
4	√	√	√	√
5	√	√	√	√
6	√	√	-	-
7	-	√	√	-
8	√	√	-	√
9	√	-	√	√
10	-	√	-	-
Rata-rata	80%	90%	90%	40%

Dari pengujian diatas dapat dianalisa dan disimpulkan bahwa pada tabel 1 terdapat perbedaan ukuran pada pegujian ini, dikarenakan perbedaan jarak objek dari kamera, semakin dekat jarak wajah ke kamera, maka dalam sistem deteksi akan semakin terdeteksi dengan baik.

b. Pengujian deteksi fitur

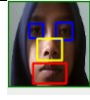


Selanjutnya adalah pengujian jarak terhadap fitur – fitur wajah, karena sistem ini dibutuhkan pendeteksian fitur wajah yang baik untuk melakukan pengukuran nilai – nilai dari fitur wajah.

Tabel 2, Pengujian deteksi fitur pada jarak (30 cm)

Jarak	Wajah	Mata	Hidung	Mulut
30 cm		√	√	√
		√	√	√
		√	√	-


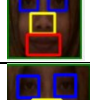

Pengujian pada jarak 30 cm terdapat fitur yang tidak terdeteksi, hal ini dikarenakan jarak terlalu dekat seperti pada Tabel 3.

Tabel 3, Pengujian deteksi fitur pada jarak (40 cm)

Jarak	Wajah	Mata	Hidung	Mulut
40 cm		√	√	√
		√	√	√
		√	√	√


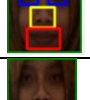

Berbeda dengan pengujian jarak 30 cm, pada jarak 40 cm dapat mendeteksi fitur dengan baik.

Tabel 4 Pengujian deteksi fitur pada jarak (50 cm)

Jarak	Wajah	Mata	Hidung	Mulut
50 cm		√	√	√
		√	√	√
		√	√	√

Pada deteksi fitur jarak 50 cmsama halnya seperti pendeteksian pada jarak 40 cm, yaitu dapat mendeteksi fitur dengan baik.

Tabel 5 Pengujian deteksi fitur pada jarak (60 cm)

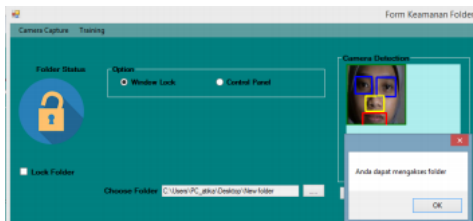
Jarak	Wajah	Mata	Hidung	Mulut
60 cm		√	√	-
		√	√	√
		-	-	-

Pengujian pada jarak 60 cm tidak dapat mendeteksi fitur dengan baik dibandingkan dengan jarak 30 cm – 50 cm.

c. Pengujian klasifikasi pada sistem keamanan folder

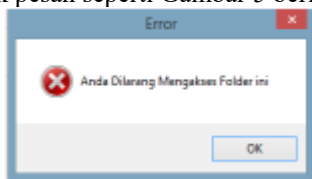
Pada pengujian klasifikasi sistem, dilakukan untuk menguji kebenaran sistem untuk mencapai tujuan. Dalam hal ini terdapat pengujian benar dan pengujian salah, yang artinya pada pengujian benar, maka orang tersebut kemungkinan benar pemilik PC sehingga dapat mengakses

folder yang dituju, seperti pada Gambar 4 berikut:



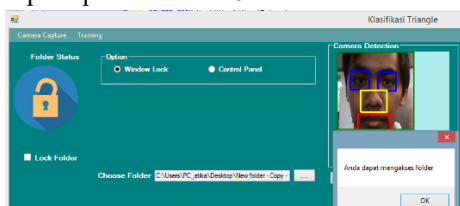
Gambar 4. Pengujian Benar

Namun, terdapat pula pengujian benar, yaitu seseorang (bukan pemilik PC) tidak dapat mengakses folder, sehingga akan nampak pesan seperti Gambar 5 berikut:



Gambar 5. Pengujian Benar

Pada pengujian yang menghasilkan kesalahan, hal ini artinya seseorang (bukan pemilik PC) dapat mengakses folder, seperti pada Gambar 6 berikut:



Gambar 6. Pengujian Salah

d. Pengujian keakurasian dan kesalahan

Dari hasil pengujian pengenalan pada sistem secara keseluruhan ditemui kasus yang dapat dikatakan salah yang tidak diinginkan dalam tujuan sistem namun juga terdapat kebenaran seperti yang diinginkan oleh tujuan sistem. Dalam pengujian menggunakan 23 sampel dari 5 orang diperoleh hasil bahwa terdapat diantaranya adalah dalam proses pengenalan yang merupakan seseorang yang dikenali sebagai pemilik dapat membuka folder dengan ini hasil ini adalah benar dan bukan sebagai pemilik tidak dapat membuka folder.

$$\text{Keakuratan} = \frac{\text{Hasil Benar}}{\text{Banyaknya Pengujian}} \times 100\%$$

Tabel 6, Tingkat Keakuratan

Jarak	Keakuratan
30 cm	82,6 %
40 cm	60,8%
50 cm	60,8%

Dalam hasil pengujian juga terdapat kesalahan, dimana seseorang yang seharusnya tidak dikenali sebagai pemilik, dapat dikenali sebagai pemilik dan dapat membuka folder. Hal ini dapat diperhitungkan menggunakan persamaan berikut:

$$\text{Kesalahan} = 100\% - \text{Keakuratan}$$

Dari persamaan diatas, maka akan menghasilkan tingkat kesalahan seperti pada Tabel 3.7 berikut:

Tabel 7, Tingkat Kesalahan

Jarak	Kesalahan
30 cm	17,4%
40 cm	38,2%
50 cm	38,2%

4. Kesimpulan dan Saran

4.1 Kesimpulan

Dari hasil penilitan yang telah dilakukan, maka dapat disimpulkan:

- Proses deteksi wajah menggunakan *Haar Cascade Classifier* tergolong cukup baik.
- Batas optimum jarak deteksi objek wajah dengan *webcam* adalah 30 cm – 50 cm
- Tingkat ketepatan deteksi fitur – fitur pada wajah sangat berpengaruh terhadap proses klasifikasi.
- Metode *Triangle Face* dengan penambahan fitur – fitur lainnya memiliki tingkat keakurasian terbesar pada jarak 30 cm yaitu 82,6% dan terdapat kesalahan terbesar pada jarak 40 cm dan 50 cm yaitu 38,2% yang artinya ketika dilakukan tes klasifikasi, wajah orang tersebut dapat membuka folder (bukan pemilik *PC*).

4.2 Saran

Berdasarkan penelitian ini, ada beberapa hal yang disarankan yaitu:

- Pada proses klasifikasi dapat digunakan metode klasifikasi yang memiliki tingkat keakurasian baik
- Dapat ditambahkan jumlah fitur – fitur wajah yang digunakan agar lebih detail dalam dan tingkat keakurasiannya semakin baik.

Daftar Pustaka:

- Chiunsun Lin, Kuo-Chin Fan."Human Face Detection Using Geometri Triangle Relationship".Institute of Computer Science and Information, Taiwan.
- Choirina, Priska."Deteksi jenis berdasarkan citra wajah jarak jauh dengan metode Haar Cascade Classifier".Studi Kasus: Politeknik Negeri Malang,2015.
- Fahmi Aziz, Danu."Simulasi Akses Ruangan Pada Sistem Pengenalan Wajah Menggunakan Metode Triangle Face".Jurnal Universitas Jember.2012.
- Miftah, Muhammad."Pengamanan Laptop Menggunakan Pengenalan Wajah Berbasis Triangle Face".Jurnal Universitas Dian Nuswantoro Semarang.2016.
- Putra, Darma."Pengolahan Citra Digital", 1st ed., Yogyakarta:Andi.2010.pp. 3-4
- Sajati, Haruno.(2015, September). Deteksi Obyek Menggunakan Haar Cascade Classifier [Online] Available : <http://jati.stta.ac.id/2015/09/deteksi-obyek-menggunakan-haar-cascade.html>
- Siregar, Hani Febrina Rasyad."Penerapan Face Recognition pada Keamanan Folder Menggunakan Metode Eigenface".Jurnal Universitas Sumatera Utara Medan, 2014.
- Sommerville, Ian."Software Engineering", 6th ed., Jakarta: Erlangga.2003.pp. 43 - 44