SISTEM VERIFIKASI ONLINE MENGGUNAKAN BIOMETRIKA WAJAH

I Nyoman Piarsa , Riza Hisamuddin

Staff Pengajar Teknik Elektro, Fakultas Teknik, Universitas Udayana
Kampus Bukit Jimbaran, Bali, 80361
Email: manpits@ee.unud.ac.id

Abstrak

Sistem verifikasi online menggunakan biometrika wajah adalah sebuah sistem kontrol keamanan akses web yang menggunakan biometrika wajah. Sistem verifikasi bertujuan untuk menerima atau menolak identitas yang diklaim oleh seseorang. Sistem ini dibagi dalam dua proses penting yaitu proses pendaftaran dan proses pengenalan. Proses pendaftaran adalah proses dimana seorang pengguna mendaftarkan dirinya dalam suatu web dan kemudian melakukan pendaftaran wajah, data wajah yang telah terdaftar akan digunakan untuk proses selanjutnya yaitu proses pengenalan. Proses pedaftaran wajah menggunakan pendeteksian wajah yang menggunakan library OpenCV. Proses verifikasi menggunakan sistem pengenalan yang menggunakan metode *Eigenface*.

Hasil dari penelitian ini didapatkan bahwa, biometrika dapat diterapkan dan digunakan sebagai sistem verifikasi yang berbasiskan web secara online. Metode eigenface dalam proses pengenalan dapat digunakan sebagai sistem keamanan tambahan dengan menggunakan nilai ambang 1,2 dan penggunaan 4 *eigenface*. Pemilihan nilai ambang dan *eigenface* dapat disesuaikan dengan kebutuhan keamanan yang diinginkan. Nilai ambang dan penggunaan *eigenface* bersifat berlawanan arah dimana semakin kecil nilai ambang dan semakin besar penggunaan *eigenface* maka keakuratan sistem semakin akurat, dan sebaliknya sistem keakuratan sistem menjadi berkurang.

Kata kunci: keamanan, verifikasi, wajah, biometrika, metode *eigenface*

1 PENDAHULUAN

Proses pengenalan wajah diawali oleh proses pendeteksian wajah. Proses pendeteksian wajah memiliki peran yang sangat penting dalam sistem pengenalan wajah karena proses pengenalan akan lebih akurat setelah wajah dalam suatu gambar ataupun video telah terdeteksi. Pendeteksian wajah melalui video ataupun *webcam* dapat digunakan pula untuk mengumpulkan wajah yang lebih bervariasi karena pengambilan gambar wajah dilakukan pada saat wajah terdeteksi, kemudian menyimpan wajah yang telah terdeteksi. Jika pendeteksian dilakukan secara terus-menerus maka variasi wajah yang tersimpan pun akan semakin bervariasi sehingga akan membantu dalam proses pengenalan wajah. Sistem pengenalan bertujuan memecahkan identitas seseorang. Terdapat dua tipe sistem pengenalan, yaitu sistem verifikasi dan identifikasi. Sistem verifikasi bertujuan untuk menerima atau menolak identitas yang diklaim oleh seseorang, sedangkan sistem identifikasi bertujuan untuk memecahkan identitas seseorang. Sedangkan biometrika adalah identifikasi dari karakteristik fisik atau perilaku seseorang.

Standar sistem keamanan *web* saat ini menggunakan teknologi kriptografi yaitu penggunaan SSL (*Secure Sockets Layer*) yang telah banyak digunakan pada banyak *web* khususnya *web* yang menyediakan jasa *e-commers* di dalamnya ataupun *web* yang menyediakan jasa *mailing list*. Permasalahan yang dihadapi adalah bagaimana implementasi fitur sistem biometrika pendeteksian dan pengenalan wajah manusia dapat digunakan sebagai salah satu sistem keamanan tambahan pada sistem kontrol keamanan akses *web* yang umumnya hanya menggunakan *user name* dan *password*.

2 TINJAUAN PUSTAKA

2.1 Sistem Biometrika

Sebuah sistem biometrika adalah sistem pengenalan yang bekerja dengan mengambil data biometrika dari individu tertentu, mencari fitur dari data yang diperoleh dan membandingkan fitur ini dengan fitur yang ada dalam basis data. Dalam konteks aplikasi, sebuah sistem biometrika dapat bekerja dalam dua cara yaitu verifikasi dan identifikasi.

Verifikasi, sistem mengesahkan identitas seseorang dengan membandingkan data biometrika yang diperoleh dengan data biometrikanya sendiri yang telah disimpan sebelumnya dalam basis data. Dalam sistem seperti ini pengguna biasanya memberikan identitasnya, seperti PIN (Personal Identification Number), username, kartu pintar dan lain-lain.

Dalam mode identifikasi, sistem mengenali individu dengan mencari data semua pengguna di dalam basisdata untuk mencari satu kecocokan. Dalam hal ini sistem melakukan pembandingan satu-ke-banyak tanpa meminta identitas dari pengguna.

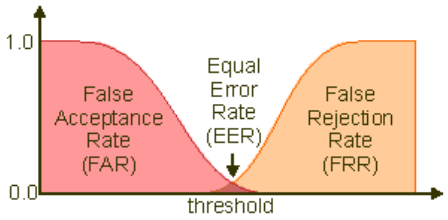
Perlu diketahui bahwa pengukuran biometrika dari individu yang sama yang diambil pada waktu yang berbeda hampir tidak pernah identik. Inilah alasan mengapa digunakan nilai ambang sebagai toleransi.

Sistem biometrika didesain dengan menggunakan lima modul utama sebagai berikut:

1. Modul sensor (sensor modul), merupakan modul untuk pengumpulan data atau akuisisi data, yang mengambil (*captured*) data biometrika dari pengguna, dan mengolahnya menjadi bentuk yang layak untuk proses pengolahan berikutnya.
2. Modul pemisahan ciri (*feature extraction* modul), yaitu modul untuk menghasilkan ciri unik dari bometrika yang digunakan yang dapat membedakan antara satu orang dengan yang lainnya. Modul ini akan mengubah data dari modul sensor kedalam bentuk yang diperlukan oleh modul pencocokan.
3. Modul pencocokan (*matching* modul), yaitu modul untuk menentukan tingkat kesamaan/ ketidaksamaan antara ciri biometrika yang diuji dengan ciri biometrika acuan pada basisdata
4. Modul keputusan (*decision* modul), yaitu modul untuk memutuskan apakah pengguna yang diuji sah atau tidak sah berdasarkan skor hasil pencocokan. Sah atau tidak sahnya pengguna diputuskan berdasarkan suatu nilai ambang (*threshold*).
5. Modul penyimpanan data (*storage* modul), merupakan modul untuk mendaftarkan/ menyimpan ciri biometrika pengguna ke dalam basisdata acuan. Basisdata ini yang akan digunakan sebagai acuan saat proses pengenalan

2.2 Kesalahan-Kesalahan dalam Sistem Biometrika

Sebuah sistem verifikasi biometrika dapat membuat dua macam kesalahan: (i) kesalahan dalam menerima orang yang tidak terdaftar (*false acceptance rate FAR*), (ii) kesalahan dalam menolak orang yang telah terdaftar dalam basis data (false rejection rate FRR). FAR dan FRR saling berlawanan. Kenyataannya FAR dan FRR adalah fungsi dari nilai ambang t. Jika t dinaikkan, untuk membuat sistem lebih toleran terhadap variasi input dan derau, maka FAR meningkat. Sebaliknya, jika t diturunkan untuk membuat sistem lebih aman, maka FRR meningkat.



Gambar-1. Kurva FAR, FRR dan EER

(http://www.bioid.com/sdk/docs/About_EER.htm)

Untuk mengukur kesalahan tersebut diturunkan sebuah formulasi yang disebut dengan False Acceptance Rate (FAR) dan False Rejection Rate (FRR) sebagai berikut:

$$FRR = \frac{\text{jumlah penguna asli ditolak sistem(FR)}}{\text{Jumlah seluruh pengujian}}$$

$$FAR = \frac{\text{jumlah penguna palsu yang diterima sistem (FA)}}{\text{Jumlah seluruh pengujian}}$$

Untuk penentuan total error rate digunakan formula Error Rate (ER) yang mengkombinasikan kedua rasio di atas sebagai berikut:

ER = FAR + FRR

Pada sebuah sistem verifikasi ideal nilai FRR dan FAR diupayakan sekecil mungkin. Untuk itu perlu ditentukan sebuah nilai threshold yang menjadi batas kapan perlu diambil sebuah keputusan. Umumnya nilai threshold yang diambil adalah nilai pada saat mencapai Equal Error Rate (ERR) yaitu pada saat FAR = FRR.

Kebutuhan akan keakuratan suatu sistem biometrika sangat bergantung pada aplikasinya. Sebagai contoh dalam aplikasi forensik seperti identifikasi kriminal, salah satu hal utama adalah FRR (bukan FAR), yaitu kita tidak ingin salah mengidentifikasi seorang kriminal meskipun dengan resiko terjadi kesalahan yang cukup besar dalam verifikasi. Di sisi yang lain FAR menjadi hal yang paling penting dalam aplikasi keamanan tingkat tinggi, dimana tujuan utamanya untuk untuk menolak para penipu (meski dengan resiko pengguna yang sah juga ditolak oleh sistem karena tingginya FRR)

2.3 Pemrosesan Wajah

Deteksi wajah dapat dipandang sebagai masalah klasifikasi pola dimana inputnya adalah citra masukan dan akan ditentukan output yang berupa label kelas dari citra tersebut. Dalam hal ini terdapat dua label kelas, yaitu wajah dan nonwajah.

Pendeteksian wajah (*face detection*) adalah salah satu tahap awal yang sangat penting sebelum dilakukan proses pengenalan wajah (*face recognition*). Bidang-bidang penelitian yang berkaitan dengan pemrosesan wajah (*face processing*) adalah :

1. Pengenalan wajah (face recognition) yaitu membandingkan citra wajah masukan dengan suatu database wajah dan menemukan wajah yang paling cocok dengan citra masukan tersebut.
2. Autentikasi wajah (face authentication) yaitu menguji keaslian atau kesamaan suatu wajah dengan data wajah yang telah diinputkan sebelumnya.

3. Lokalisasi wajah (face localization) yaitu pendeteksian wajah namun dengan asumsi hanya ada satu wajah di dalam citra
4. Penjejakan wajah (face tracking) yaitu memperkirakan lokasi suatu wajah di dalam video secara real time.
5. Pengenalan ekspresi wajah (facial expression recognition) untuk mengenali kondisi emosi manusia.

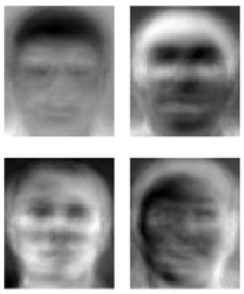
Tantangan yang dihadapi pada masalah deteksi wajah disebabkan oleh adanya faktor-faktor berikut :

1. Posisi wajah. Posisi wajah di dalam citra dapat bervariasi karena posisinya bisa tegak, miring, menoleh atau dilihat dari samping.
2. Komponen-komponen pada wajah yang bisa ada atau tidak ada, misalnya kumis, jenggot dan kacamata.
3. Ekspresi wajah. Penampilan wajah sangat dipengaruhi oleh ekspresi wajah seseorang, misalnya tersenyum, tertawa, sedih, berbicara dan sebagainya.
4. Terhalang objek lain. Citra wajah dapat terhalangi sebagian oleh objek atau wajah lain, misalnya pada citra berisi sekelompok orang.

Kondisi pengambilan citra. Citra yang diperoleh sangat dipengaruhi oleh faktor-faktor seperti intensitas cahaya ruangan, arah sumber cahaya, dan karakteristik sensor dan lensa kamera.

2.4 Metoda Pengenalan Wajah Eigenface

Eigenface adalah kumpulan dari eigencectors yang digunakan dalam bidang kecerdasan buatan untuk menangani problem dari pengenalan wajah manusia. Pendekatan menggunakan eigenvectors untuk pengenalan telah digunakan oleh Sirovich dan Kirby (1987) dan digunakan kembali oleh Matthew Turk and Alex Pentland dalam pengklasifikasian wajah. Eigencectors ini berasal dari covariance matriks dari distribusi data acak wajah manusia pada dimensi yang tinggi pada ruang vektor. Metoda ini mentranformasikan citra wajah kedalam sebuah kumpulan karakteristik fitur citra yang dinamakan eigenface, dengan mengunakan Principal Component Analysis untuk proses training citra (Turk dan Pentland, 1991).



Gambar-2. Citra Eigenfaces

(http://en.wikipedia.org/wiki/Eigenface)

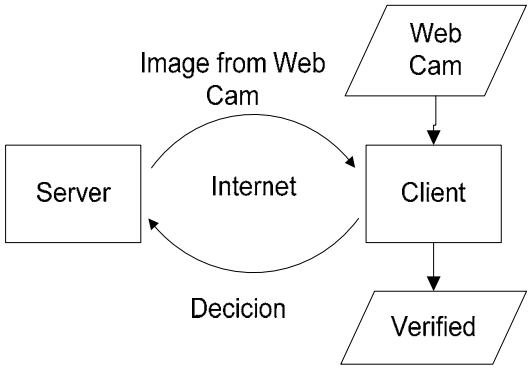
2.5 *Principal Components Analysis* (PCA)

Hotelling mengajukan sebuah teknik untuk mengurangi dimensi sebuah ruang yang direpresentasikan oleh variabel statistik $x_1,x_2,\ldots,x_n$, dimana variabel tersebut biasanya saling berkorelasi satu dengan yang lain sehingga terdapat sebuah himpunan variable baru yang memiliki sifat yang relatif sama dengan variabel sebelumnya dimana dikehendaki himpunan variabel baru tersebut memiliki jumlah variabel (dimensi) yang lebih sedikit dari variabel sebelumnya. Hotelling menyebut metoda tersebut sebagai *Principal Component Analysis* (PCA) atau Transformasi Hotelling dan Transformasi Karhunen-Loeve. Transformasi Karhunen-Loeve banyak digunakan untuk memproyeksikan atau mengubah suatu kumpulan data berukuran besar menjadi bentuk representasi data lain dengan ukuran yang lebih kecil. Transformasi Karhunen-Loeve terhadap sebuah ruang data yang besar akan menghasilkan sejumlah vektor basis ortonormal ke dalam bentuk kumpulan vektor eigen dari suatu matriks kovarian tertentu, yang dapat secara optimal merepresentasikan distribusi data.

3 MODEL SISTEM

Secara umum proses dari sistem verifikasi *online* menggunakan biometrik wajah dilakukan melalui tiga tahapan proses yaitu, proses pengiriman data citra *user* dari *client* ke *server*, proses pendeteksian wajah dan proses pengenalan wajah. Diagram umum dari sistem verifikasi *online* menggunakan biometrik wajah dapat dilihat pada gambar berikut.

Secara umum, pengenalan biometrika wajah adalah sistem pengenalan diri dengan menggunakan biometrika wajah. Sistem verifikasi melakukan pencocokan 1:M terhadap user yang bersesuaian, dengan M menyatakan banyaknya citra wajah yang telah terdaftar pada server.

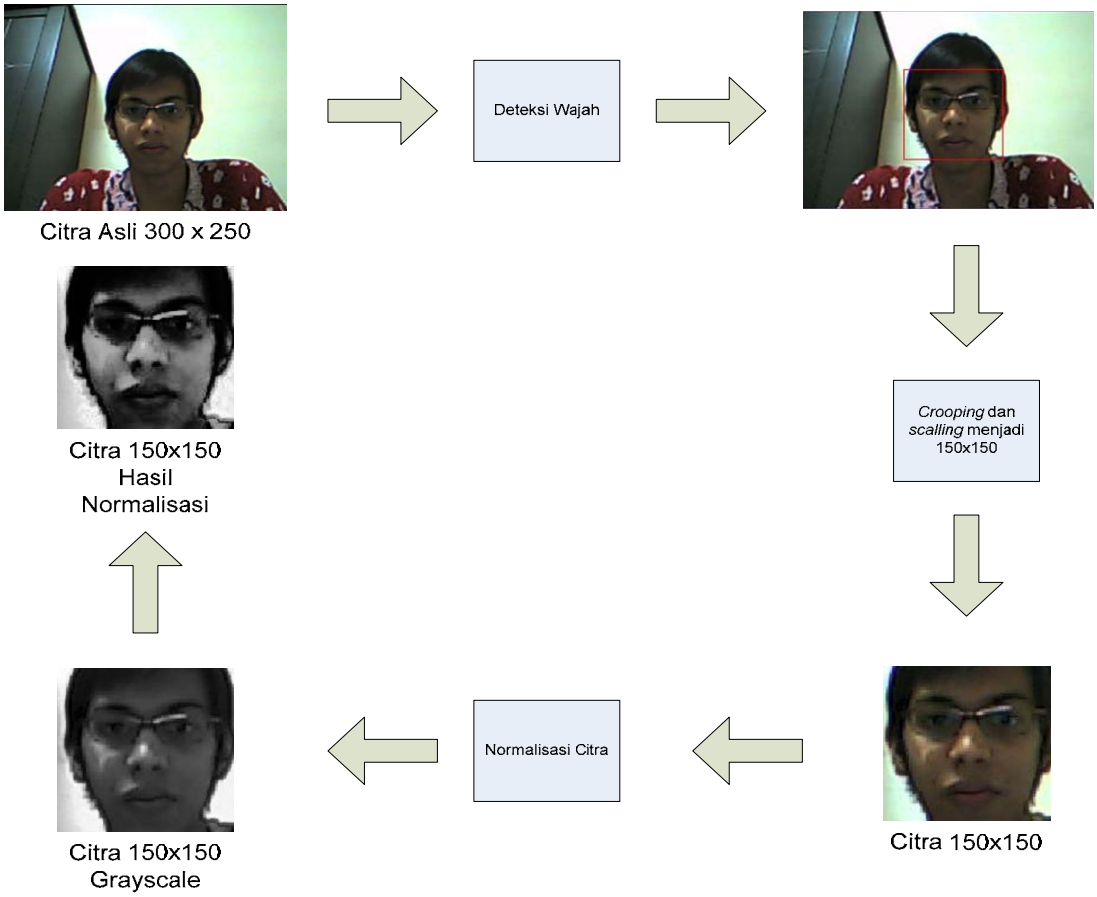


Gambar-3. Diagram Pendetaksian Wajah Berbasis Web

Secara umum, pengenalan biometrika wajah adalah sistem pengenalan diri dengan menggunakan biometrika wajah. Sistem verifikasi melakukan pencocokan 1:M terhadap user yang bersesuaian, dengan M menyatakan banyaknya citra wajah yang telah terdaftar pada server.

Modul pendeteksian wajah merupakan tahapan awal dari proses pengenalan wajah, pendeteksian wajah penting dilakukan agar memberikan hasil yang lebih optimal pada proses pengenalan wajah. Proses pendeteksian wajah menggunakan library OpenCV, wajah yang terdeteksi kemudian dilakukan proses pemotongan citra pada bagian wajah sesuai dengan kordinat yang didapat dari proses deteksi sebelumnya dan dilakukan proses penskalaan ukuran citra menjadi 150x150 pixel, proses normalisasi dan proses penyimpanan wajah hasil proses. Normalisasi menggunakan metode Histogram Equalization bertujuan untuk menyeragamkan tingkat kecerahan wajah akibat perbedaan pencahayaan saat pengambilan data wajah. Proses normalisasi citra dan penskalaan menjadi bagian yang penting pada proses pengenalan karena untuk menghasilkan satu kumpulan eigenface dibutuhkan kumpulan gambar wajah manusia yang memiliki ciri yang sama seperti memiliki tingkat pencahayaan yang sama dan memiliki ukuran yang sama.

..



Gambar-4. Diagram Proses Deteksi Wajah

Modul pengenalan wajah merupakan modul akhir dari sistem verifikasi online menggunakan biometrika wajah. Pengenalan wajah menggunakan metode Eigenface. Sistem pengenalan akan membandingkan fitur citra yang diuji dengan fitur citra sampel dengan cara mencari bobot minum dan kemudian nilai bobot ini dibandingkan dengan nilai ambang yang telah ditentukan sebelumnya, jika nilai bobot ini lebih kecil atau sama dengan nilai ambang maka citra uji berhasil dikenali dan akan diberikan hak akses untuk mengakses suatu sistem dibelakang sistem verifikasi online menggunakan biometrika wajah.

Penentuan nilai ambang (T) merupakan hal yang sangat penting dalam sistem pengenalan karena nilai tersebut akan mempengaruhi tingkat keberhasilan sistem. Oleh karena itu, diperlukan penentuan nilai ambang yang tepat untuk mengoptimalkan kinerja

suatu sistem pengenalan. Nilai T akan berpengaruh pada nilai FAR dan FRR dari sistem verifikasi. Pemilihan nilai T sebenarnya sangat tergantung pada bidang apa aplikasi sistem pengenalan diri diterapkan. Untuk aplikasi-aplikasi keamanan, T yang dipilih adalah T yang memberikan nilai FAR dan FRR sekecil-kecilnya.

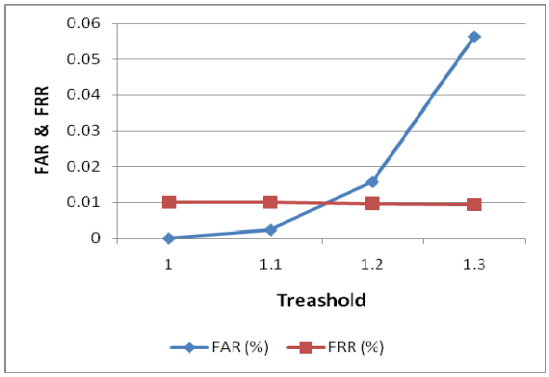
4 HASIL DAN PEMBAHASAN

4.1 Hasil Pengukuran Kinerja Sistem Menggunakan 101 Citra Uji Pengguna dan 10 Eigenface

Pengukuran kinerja sistem dengan menggunakan 101 citra uji pengguna dengan 10 citra sampel pada masing-masing pengguna dengan kombinasi rentang nilai ambang 1,0 sampai 1,3 dan penggunaan 10 eigenface, seperti tabel 1 di bawah ini.

Tabel-1. Hasil pengujian 101 pengguna menggunakan 10 eigenface

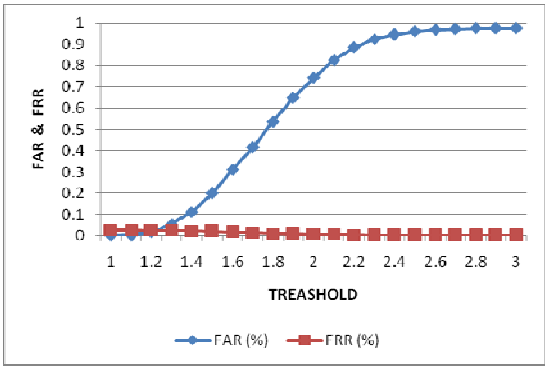
FA	FR	FAR (%)	FRR (%)	Thres hold	Waktu (detik)
0	101	0	0.00990099	1	2260
23	101	0.00225	0.00990099	1.1	2369
160	98	0.01568	0.00960690	1.2	2423
573	95	0.05617	0.00931281	1.3	2315



Gambar-5. Kurva Karakteristik 101 pengguna Penggunakan 10 eigenface

Tabel-2. Hasil pengujian 40 pengguna menggunakan 10 eigenface

FA	FR	FAR (%)	FRR (%)	Treshold	Waktu (detik)
0	40	0	0.025	1	340.84
3	40	0.00188	0.025	1.1	356.67
26	39	0.01625	0.02438	1.2	365.86
88	38	0.055	0.02375	1.3	366.36
181	36	0.11313	0.0225	1.4	366.47
323	32	0.20188	0.02	1.5	366.56
500	27	0.3125	0.01688	1.6	366.58
667	22	0.41688	0.01375	1.7	366.72
861	16	0.53813	0.01	1.8	366.94
1038	13	0.64875	0.00813	1.9	367.31
1184	8	0.74	0.005	2	367
1320	6	0.825	0.00375	2.1	367.36
1414	4	0.88375	0.0025	2.2	367.38
1478	1	0.92375	0.00063	2.3	367.33
1512	0	0.945	0	2.4	367.42
1536	0	0.96	0	2.5	368.14
1548	0	0.9675	0	2.6	368.77
1553	0	0.97063	0	2.7	369.31
1559	0	0.97438	0	2.8	370.08
1560	0	0.975	0	2.9	370.22
1560	0	0.975	0	3	370.23



Gambar-6. Kurva Karakteristik 40 pengguna menggunakan 10 eigenface

4.2 Hasil Pengukuran Kinerja Sistem Menggunakan 40 Citra Uji Pengguna dan 10 Eigenface

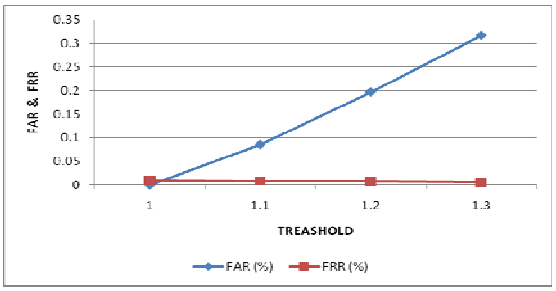
Pengukuran kinerja sistem dengan menggunakan 40 citra uji pengguna dengan 10 citra sampel pada masing-masing pengguna dengan kombinasi rentang nilai ambang 1.0 sampai 3.0 dan penggunaan 10 *eigenfac*, seperti terlihat dalam tabel 2 berikut ini.

4.3 Hasil Pengukuran Kinerja Sistem Menggunakan 101 Citra Uji Pengguna dan 4 Eigenface

Pengukuran kinerja sistem dengan menggunakan 101 citra uji pengguna dengan 10 citra sampel pada masing-masing pengguna dengan kombinasi rentang nilai ambang 1.0 sampai 1.3 dan penggunaan 4 eigenface, seperti tabel 3 di bawah ini.

Tabel-3. Hasil pengujian 101 pengguna dengan 4 eigenface

FA	FR	FAR (%)	FRR (%)	Threshold	Waktu (detik)
0	101	0	0.0099	1	2183
880	90	0.08627	0.00882	1.1	2194
2015	76	0.19753	0.00745	1.2	2208
3236	65	0.31722	0.00637	1.3	2211



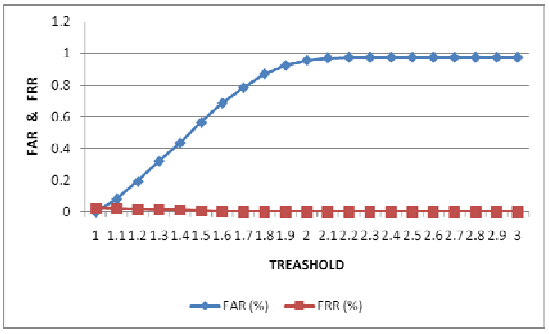
Gambar-7. Karakteristik 101 pengguna dengan 4 eigenface.

4.4 Hasil Pengukuran Kinerja Sistem 40 Citra Uji Pengguna dan 4 Eigenface

Pengukuran kinerja sistem dengan menggunakan 40 citra uji pengguna dengan 4 citra sampel pada masing-masing pengguna dengan kombinasi rentang nilai ambang 1.0 sampai 3.0 dan penggunaan 4 eigenface.

Tabel-4. Hasil pengujian 40 pengguna 4 eigenface

FA	FR	FAR (%)	FRR (%)	Threshold	Waktu (detik)
0	40	0	0.025	1	356.77
134	36	0.08375	0.0225	1.1	356.63
309	28	0.19313	0.0175	1.2	353.72
515	23	0.32188	0.01438	1.3	353.02
698	19	0.43625	0.01188	1.4	347.34
904	13	0.565	0.00813	1.5	346
1100	7	0.6875	0.00438	1.6	346.99
1256	2	0.785	0.00125	1.7	347.02
1395	0	0.87188	0	1.8	347.02
1480	0	0.925	0	1.9	347.3
1531	0	0.95688	0	2	347.49
1554	0	0.97125	0	2.1	348
1560	0	0.975	0	2.2	348
1560	0	0.975	0	2.3	347.53
1560	0	0.975	0	2.4	348.24
1560	0	0.975	0	2.5	348.05
1560	0	0.975	0	2.6	348.05
1560	0	0.975	0	2.7	349.31
1560	0	0.975	0	2.8	348.99
1560	0	0.975	0	2.9	348.59
1560	0	0.975	0	3	348



Gambar-8. Kurva Karakteristik 40 pengguna menggunakan 4 eigenface

5 KESIMPULAN

Sistem verifikasi online menggunakan biometrika wajah yang menggunakan metode eigenface dalam proses pengenalan dapat digunakan sebagai sistem keamanan tambahan dengan menggunakan nilai ambang 1.1 dan penggunaan 4 eigenface. Nilai ambang dan penggunaan eigenface bersifat berlawanan arah dimana semakin kecil nilai ambang dan semakin besar penggunaan eigenface maka keakuratan sistem semakin akurat, dan sebaliknya keakuratan sistem menjadi tidak akurat. Penggunaan eigenface sangat mempengaruhi akurasi sistem, pemilihan eigenface dapat disesuaikan dengan kebutuhan keamanan yang diinginkan. Penggunaan metode *eigenface* yang rentan terhadap pencayahaan dianggap kurang cocok digunakan sebagai sistem pengenalan dalam sistem verifikasi *online*, karena seorang pengguna sistem harus dapat terferifikasi pada kondisi lingkungan yang memiliki tingkat pencahayaan yang berbeda dari lingkungan pada saat pendaftaran.

6 DAFTAR PUSTAKA

[1] Achmad, Balsa dkk., 2005, *Teknik Pengolahan Citra Digital Menggunakan Delph*, Ardi Publishing:Yogyakarta.

[2] Baldwin, R, 2004, *Understanding Base64 Data*, http://www.developer.com/java/ other/article. php/3386271.,Diakses tanggal 20 Januari 2009.

[3] Lindsay, I Smith, 2002, *A Tutorial on Principal Components Analysis*. http:// mail.iiit.ac. in/~mkrishna/PrincipalComponents.pdf. Diakses tanggal 01 November 2008.

[4] M, Turk; A, Pentland. 1991, *Eigenfaces for Recognition*, *Journal of Cognitive Neuroscience*, vol. 3, no. 1, pp. 71-86. http://www.cs.ucsb.edu/~mturk/Papers/jcn.pdf. Diakses tanggal 01 November 2008.

[5] M, Turk; A, Pentland, 1991, ***Face Recognition Using Eigenfaces***. *Proc of Computer Vision and Pattern Recognition*, hal 586–591, IEEE. http://www.cs.wisc.

edu/~dyer/cs540/handouts/mturk-CVPR91.pdf. Diakses tanggal 01 November 2008.

[6] PISSARENKO, Dimitri, 2002, ***Eigenface-based Facial Recognition***. http://www.geocities.com/dapissarenko/2002_12_01_eigenfaces.pdf. Diakses tanggal 01 Agustus 2008

[7] Nixon, Mark S; Aguado, Alberto S., 2008, *Feature Extraction and Image Processing*, http://books.google.co.id/books?id=jXmJqzQgdY8C Diakses tanggal 17 Febuari 2009.

[8] Anonim, *About EER*. http://www.bioid.com/sdk/docs/About_EER.htm. Diakses tanggal 15 Febuari 2009.

[9] Anonim, *Base64*, http://en.wikipedia.org/wiki/Base64. Diakses tanggal 20 Januari 2009.

[10] Anonim *Eigenface*, http://en.wikipedia.org/wiki/ Eigenface. Diakses tanggal 13 Desember 2008.

[11] Anonim **,** *Euclidean Distance*, http://en.wikipedia. org/wiki/Euclidean_distance. Diakses tanggal 13 Desember 2008.

[12] Anonim, *Histogram Equalization*, http://en.wikipedia.org/wiki/Histogram_equalization. Diakses tanggal 13 Desember 2008.

[13] Anonim, *Grayscale*. http://en.wikipedia.org/wiki/Greyscale. Diakses tanggal 20 Januari 2009

[14] Anonim, *HTTP*. http://id.wikipedia.org/wiki/HTTP. Diakses tanggal 20 Januari 2009.

[15] Anonim **,** *OpenCV*, http://en.wikipedia.org/wiki/OpenCV, Diakses tanggal 20 Januari 2009.

[16] Anonim**,** *RGB Color Model*, http://en.wikipedia org/wiki/Rgb. Diakses tanggal 20 Januari 2009.