

## Analisis Keamanan Akses Ruang Verifikasi Pengenalan Wajah dan Sidik Jari

Ramadhani Ulansari

Program Studi Teknik Informatika, Fakultas Teknologi Informasi

Universitas Respati Indonesia

Jl. Bambu Apus I No. 3 Cipayung, Jakarta Timur 13890

Email: ramadhani.ulansari@fti.urindo.ac.id

### Abstrak

Analisis keamanan akses ruang verifikasi pengenalan wajah dan sidik jari merupakan pengembangan dari penulisan karya ilmiah sebelumnya, dimana penulisan karya ilmiah sebelumnya adalah membuat perancangan keamanan akses ruang hanya dengan menggunakan satu verifikasi yaitu pengenalan wajah. Keamanan akses ruang dengan menggunakan satu verifikasi yaitu pengenalan wajah dirasakan kurang sempurna karena keamanan sangat bergantung sekali terhadap struktur wajah, tingkat cahaya sekitar ruangan, kefokusan kamera, dan posisi wajah ketika menghadap kamera. Penambahan verifikasi sidik jari dirasakan sangat tepat untuk menambahkan keakuratan sistem keamanan, hal ini terlihat dari hasil keakuratan dari dua verifikasi pada hasil penulisan. Tujuan penelitian menganalisis keamanan akses ruang verifikasi pengenalan wajah dan sidik jari. Metode yang digunakan pada analisis keamanan akses ruang verifikasi pengenalan wajah dan sidik jari yaitu studi pustaka dengan banyak membaca referensi dari karya ilmiah, serta metode analisis perancangan alat yang telah dibuat sebelumnya hal ini digunakan untuk membandingkan hasil keakuratan verifikasi pengenalan wajah dan sidik jari dimana hasil yang didapatkan untuk verifikasi menggunakan sidik jari lebih sedikit tingkatan erornya, metode verifikasi ini juga disebut dengan metode biometrik. Dapat disimpulkan verifikasi pengenalan wajah amat sangat tergantung pada ketepatan posisi wajah didepan kamera serta sangat dipengaruhi oleh kondisi cahaya, posisi wajah dan tekstur wajahnya. penggunaan verifikasi sidik jari lebih baik dari pada penggunaan verifikasi wajah walaupun dipengaruhi oleh ketepatan posisi jempol pada alat sidik jari (*finger print*) namun penggunaan sidik jari tidak dipengaruhi oleh kondisi ruangan. jumlah kegagalan lebih sedikit, Sehingga penggunaan akses keamanan menggunakan dua verifikasi dianggap lebih baik.

**Kata kunci:** Keamanan Akses Ruang, Pengenalan Wajah, Sidik Jari.

### PENDAHULUAN

Manusia diciptakan oleh Allah SWT dengan kesempurnaan, memiliki bagian-bagian tubuh yang dapat dijadikan identitas khusus, ilmu yang mempelajari identitas tubuh manusia seperti seperti wajah, suara, DNA, sidik jari, retina mata, telapak tangan, pola tanda tangan, dan pola ketikan disebut metode biometrik. Dengan kemajuan teknologi bagian-bagian tubuh bisa dijadikan identitas yang unik dari diri seseorang sehingga dapat dimanfaatkan sebagai alat keamanan. Analisis keamanan ini merupakan pengembangan dari penulisan karya ilmiah sebelumnya yaitu perancangan akses keamanan ruang dengan menggunakan verifikasi pengenalan wajah. (Ramadhani Ulansari, 2014). Penambahan akses keamanan dari satu verifikasi menjadi dua verifikasi dirasakan lebih tepat dibandingkan hanya menggunakan satu verifikasi, hal ini dapat dibuktikan dari hasil percobaan yang dilakukan kepada tiga objek yang berbeda sebanyak tiga kali pengambilan foto dan pencocokan wajah dalam beberapa kondisi gelap dan terang serta

posisi wajah pada saat menghadap alat verifikasi kedepan, kekanan, dan kekiri. Untuk verifikasi sidik jari-pun dilakukan kepada tiga objek yang sama dengan posisi jempol yang ditempelkan pada alat sidik jari (*finger print*) dibuat berbeda. (Ramadhani Ulansari 2014)

### TUJUAN PENELITIAN

Menganalisis keamanan akses ruang verifikasi pengenalan wajah dan sidik jari.

### METODE PENELITIAN

Analisis keamanan akses ruang verifikasi pengenalan wajah dan sidik jari dilakukan beberapa metode yaitu :

- **Persiapan Rancangan**

Persiapan rancangan meliputi penyiapan komponen-komponen yang dibutuhkan seperti Arduino UNO, Protoboard, Motor Servo, Finger Print, Laptop dan akrilik sebagai maket nantinya.

- **Analisis Rancangan Sistem dan Desain Sistem**

Analisis rancangan sistem dan desain sistem keamanan akses ruang menggunakan verifikasi wajah dan sidik jari dilakukan dengan beberapa tahapan seperti mencari informasi sebanyak-banyaknya dari tulisan karya ilmiah, internet, buku-buku yang menambah informasi terkait dengan tema penelitian.

• **Pengujian Perancangan**

Tahap pengujian rancangan dilakukan dengan menguji rangkaian yang telah di rangkai pada protoboard, dengan cara mengupload program pada software Arduino 1.0.6 kedalam mikrokontroler Arduino hingga mendapatkan output yang diinginkan.

• **Penulisan Penelitian**

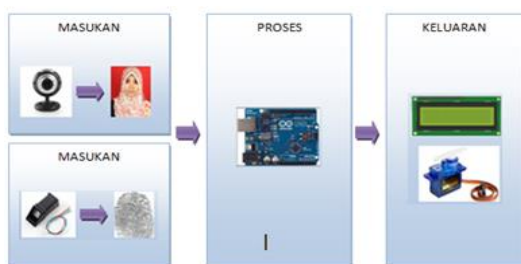
Setelah pengujian rancangan selesai dengan output yang diinginkan, tahap selanjutnya barulah memulai penulisan, perancang gambar rangkaian menggunakan software fritzing.

**HASIL DAN PEMBAHASAN**

Hasil analisis dan pembahasan keamanan akses ruang verifikasi wajah dan sidik akan dijelaskan sebagai berikut :

• **Analisis Rancangan secara Blok Diagram**

Rancangan keamanan akses ruang verifikasi pengenalan wajah dan sidik jari terdiri dari tiga blok diagram yaitu blok masukan, blok proses, dan blok keluaran seperti terlihat pada gambar 1 dibawah ini .



**Gambar 1 Blok Diagram Rancangan keamanan akses ruang verifikasi pengenalan wajah dan sidik jari**

Penjelasan blok masukan, blok proses, dan blok keluaran akan dijelaskan pada paparan berikut :

**Rancangan Blok Masukan**

Rancangan blok masukan berfungsi untuk mendata setiap komponen yang digunakan sebagai media masukan yang akan di proses sehingga menghasilkan Output sesuai yang diharapkan. Blok masukann pada perancangan seperti berikut:

⇒ **Kamera**

Blok masukan menggunakan dua buah alat salah satunya menggunakan web kamera. Web kamera digunakan untuk menangkap suatu objek wajah seseorang dan menghasilkan citra wajah sebagai pengenalan dari wajah seseorang tersebut. Citra wajah diambil secara realtime dengan menggunakan program OpenCv, kecocokan citra wajah ini diambil dari data training yang sudah di simpan pada folder OpenCv sebelumnya, folder ini terletak pada drive C: . (Maulana Rahmat Hakim, 2013)

⇒ **Sidik Jari**

Blok masukan yang kedua adalah sidik jari yang di ambil dari alat *finger print*. Alat *finger print* berfungsi sebagai pembaca bentuk dari ulir pada jari dan kemudian di convert ke dalam data digital. Sensor pada finger print bekerja dengan otaku tama berupa chip DSP yang melakukan *rendering* kemudian mengkalkulasi *feature finding* dan terakhir *searching* pada data yang sudah ada dan dilengkapi dengan LED merah pada lensa yang akan menyala sebagai indikator ketika pengambilan gambar berlangsung.

**Rancangan Blok Proses**

Setelah mendapatkan masukan berupa pengenalan wajah dan sidik jari selanjutnya proses akan berjalan, blok proses merupakan kondisi dimana telah mendapatkan masukan selanjutnya akan diolah agar menghasilkan keluaran sesuai harapan. Blok proses pada perancangan ini adalah mikrokontroler Arduino UNO (Atmega328).

**Rancangan Blok Keluaran**

Blok keluaran berupa terbukannya akses pintu dengan cara berputarnya motor servo dan keluaranya text pada LCD dijelaskan seperti berikut :

⇒ **LCD (Liquid Crystal Display)**

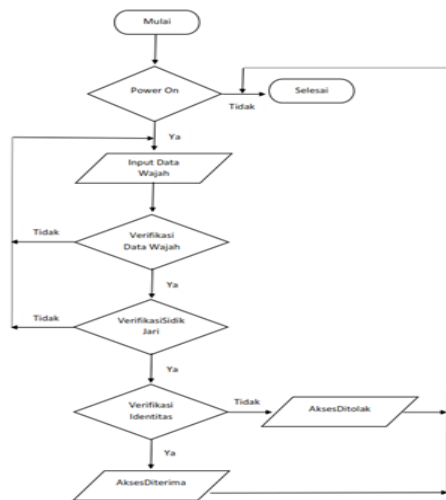
Pada perancangan akses keamanan menggunakan verifikasi biometrik dan sidik jari, LCD (*Liquid Crystal Display*) digunakan untuk menampilkan text output jika hasil dari proses inputan pengenalan wajah dari webcam dan sidik jari cocok, makanya seseorang atau objek tersebut dapat membuka pintu dan LCD ini menampilkan sidik jari cocok pintu terbuka.

⇒ **Motor Servo**

Motor Servo pada blok keluaran berfungsi untuk menggerakkan pintu pada maket hal ini ditandai berdasarkan logika program yang ia dapat sehingga ketika proses dari inputan pengenalan wajah dan sidik jari cocok, maka pintu (motor servo) akan terbuka dan jika tidak maka pintu (motor servo) tidak bergerak.

• **Analisis Diagram Alur Keamanan Akses Ruang Verifikasi Wajah dan Sidik Jari**

Perancangan keamanan akses ruang menggunakan verifikasi pengenalan wajah dan sidik jari dapat di analisis melalui flowchat seperti berikut :



**Gambar 2 Diagram Alur Keamanan Akses Ruang Verifikasi Pengenalan Wajah dan Sidik Jari**

Gambar 2 Diagram Alur keamanan akses ruang verifikasi pengenalan wajah dan sidik jari dimulai dengan melakukan konfigurasi OpenCV, load image training, konfigurasi perangkat keras (power On) kemudian inputkan data wajah secara realtime melalui web kamera selanjutnya akan dilakukan proses pencocokan data training wajah yang sudah tersimpan apakah wajah yang di ambil secara realtime sesuai dengan pengambilan data training atau tidak, jika sudah sesuai maka proses verifikasi selanjutnya yaitu sidik jari dapat di lanjutkan jika tidak maka akan kembali ke proses meminta input pengenalan wajah. Langkah selanjutnya yaitu verifikasi keamanan menggunakan sidik jari seperti proses pencocokan sidik jari dengan cara menepelkan jari dalam hal ini jempol pada alat sidik jari (*finger print*) pengambilan data berupa pembaca bentuk ulir pada jari dan kemudian di

convert ke dalam data digital. Jika cocok maka arduino akan menerima data berupa logika (1) yang kemudian akan menampilkan text pada layar LCD sidik jari benar, dan motor servo bergerak membuka pintu, dan jika proses identitas tidak cocok maka arduino akan menerima logika (0) yang kemudian akan menampilkan text pada layar LCD sidik jari salah, pintu tetap tertutup.

• **Tahapan Ujicoba**

Langkah- langkah pengujian uji coba alat keamanan akses ruang verifikasi pengenalan wajah dan sidik jari adalah sebagai berikut:

**Cara Pengoprasian Pengenalan wajah**

Tahapan dalam pengoprasian wajah adalah sebagai berikut :

- ⇒ Tahap Konfigurasi.
- ⇒ Tahap Pengenalan Wajah.
- ⇒ Tahap Autentikasi.

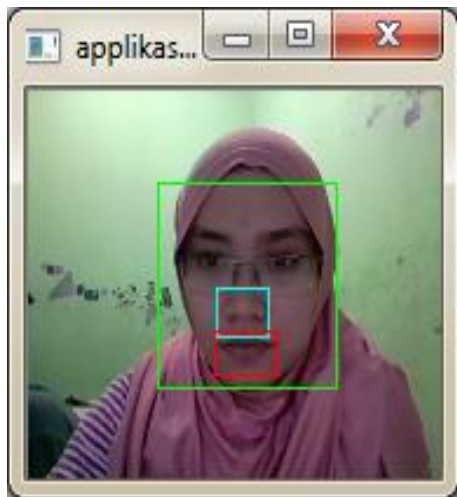
**Cara Pengoprasian Alat**

Tahapan dalam pengoprasian alat adalah sebagai berikut :

- ⇒ Menghubungkan adaptor melalui socket DC untuk mengaktifkan aktifator, dengan daya sebesar 12 volt.
- ⇒ Menghubungkan kabel serial Arduino Uno ke laptop.
- ⇒ Menghubungkan semua peralatan (LCD, Finger Print, Motor Servo) yang dibutuhkan ke mikrokontroler Arduino UNO.
- ⇒ Scan sidik jari melalui finger print ketika wajah sudah terdeteksi sesuai.

**Tahapan Konfigurasi Pengenalan wajah**

Tahapan konfigurasi menggunakan program visual studi 2010 yang diintegrasikan dengan OpenCv kemudian diintegrasikan kembali ke mikrokontroler Arduino UNO. Hal ini terlihat pada gambar 3 konfigurasi pengenalan wajah dibawah ini.



**Gambar 3 Konfigurasi Pengenalan Wajah**

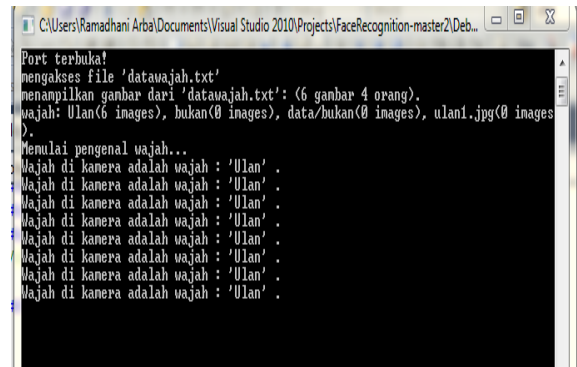
Peroses pengenalan wajah dilakukan dengan menguji kecocokan data yang sudah tersimpan pada direktori file wajah, area wajah yang dicocokkan dimulai dari seluruh wajah bagian hidung, mulut dan lebar wajah. Hasil dari pencocokan data wajah, dikirimkan melalui port arduino untuk melanjutkan pada tahapan selanjutnya, jika terlihat pesan seperti gambar 4 dibawah ini menandakan bahwa arduino sudah terintegrasi pada visual studio 2010.



**Gambar 4 Proses Integrasi OpenCv**

**Tahapan Autentikasi**

Proses tahapan autentifikasi program dapat menentukan dan mengambil sebuah keputusan apakah wajah yang terdeteksi sesuai dengan data yang tersimpan pada direktori yang telah disimpan sebelumnya. Hal ini dapat menentukan apakah objek (wajah) tersebut dapat melanjutkan ke tahap selanjutnya yaitu mecocokkan sidik jari atau tidak. Gambar 5 proses Autentikasi seperti gambar dibawah ini:



**Gambar 5 Proses Autentikasi**

Setelah semua tahapan dalam proses awal yaitu tahapan konfigurasi, tahapan pengenalan wajah, dan tahapan autentifikasi kini waktunya tahapan pengoprasian alat sidik jari (*finger print*), untuk 3 (tiga) tahapan sebelumnya pun mikrokontroler Arduino harus sudah dalam kondisi On (adaptor dan kabel USB harus sudah terpasang). Setelah data objek wajah dinyatakan sama dengan data wajah yang telah tersimpan pada Folder, tahap selanjutnya adalah melakukan pencocokan sidik jari seperti pada gambar 6 dibawah ini :



**Gambar 6 Pencocokan Sidik Jari**

**Hasil Analisis Pada Ujicoba Perancangan**

Hasil analisis pada ujicoba perancangan akses ruang verifikasi pengenalan wajah dan sidik jari terbagi menjadi dua yang akan dijelaskan pada paparan dibawah ini :

⇒ **Hasil Ujicoba Verifikasi Pengenalan Wajah**

Untuk mengetahui hasil dari implementasi suatu sistem apakah keluaran sudah benar atau tidak, maka ujicoba dilakukan terhadap tiga orang berbeda (Ulan, Ryan, Adri) hasil ujicoba seperti berikut :

→ Hasil Ujicoba Kepada Objek A (Ulan)

Hasil ujicoba objek A pada tabel 1 dilakukan percobaan sebanyak lima kali untuk tiap-tiap posisi wajah pada saat pencocokan dengan dua kondisi ruang, dimana pada saat kondisi ruangan gelap total kegagalan sebanyak sepuluh kali dan pada saat kondisi terang total kegagalan sebanyak lima kali dengan persentase kegagalan seperti yang tertera pada tabel 1.





**Tabel 1 Hasil Ujicoba Kepada Objek A (Ulan)**

No	ID_Wajah	Jumlah Foto	Kondisi ruangan	Posisi Wajah pada saat pencocokan	Jumlah Keberhasilan	Jumlah Gagal	Persentase kegagalan
1	Ulan	5	Gelap		2	3	60%
					2	3	60%
					1	4	80%
1	Ulan	5	Terang		4	1	20%
					3	2	40%
					3	2	40%

→ Hasil Ujicoba Kepada Objek B (Ryan)

Hasil ujicoba objek B pada tabel 2 dilakukan juga percobaan sebanyak lima kali untuk tiap-tiap posisi wajah pada saat pencocokan dengan dua kondisi ruang, dimana pada saat kondisi ruangan gelap total kegagalan sebanyak sepuluh kali dan pada saat kondisi terang total kegagalan sebanyak empat kali dengan persentase kegagalan seperti tertera pada tabel 2 dibawah ini.







**Tabel 2 Hasil Ujicoba Kepada Objek B (Ryan)**

No	ID_Wajah	Jumlah Foto	Kondisi ruangan	Posisi Wajah pada saat pencocokan	Jumlah Keberhasilan	Jumlah Gagal	Persentase kegagalan
1	Ryan	5	Gelap		1	4	80%
					2	3	60%
					2	3	60%
1	Ryan	5	Terang		5	0	100%
					4	1	20%
					2	3	60%

→ Hasil Ujicoba Kepada Objek C (Adri)

Hasil ujicoba objek C pada tabel 3 dilakukan percobaan sebanyak lima kali untuk tiap-tiap posisi wajah pada saat pencocokan dengan dua kondisi ruang, dimana pada saat kondisi ruangan gelap total kegagalan sebanyak sepuluh kali dan pada saat kondisi terang total kegagalan sebanyak sebelas kali persentase kegagalan seperti tertera pada tabel 3.

**Tabel 3 Hasil Ujicoba Kepada Objek C (Adri)**










No	ID_Wajah	Jumlah Foto	Kondisi ruangan	Posisi Wajah	Jumlah Keberhasilan	Jumlah Gagal	Persentase kegagalan
1	Adry	5	Gelap		1	4	80%
					3	2	40%
					1	4	80%
					1	4	80%
1	Adry	5	Terang		2	3	100%
					1	4	20%
					1	4	60%
					1	4	60%

Dari hasil ujicoba perancangan terlihat bahwa untuk penggunaan verifikasi pengenalan wajah sangat dipengaruhi oleh ketepatan posisi wajah didepan kamera serta sangat dipengaruhi oleh kondisi cahaya, posisi wajah dan tektur wajah. Wajah harus sangat tepat menghadap ke kamera sedikit saja tidak tepat maka bisa jadi alat akan men-deteksi objek sebagai orang lain dan akses tidak dapat terbuka.

**Hasil Ujicoba Verifikasi Sidik Jari**

Setelah dilakukan ujicoba pengenalan wajah, berikut hasil ujicoba verifikasi sidik jari kepada tiga objek (A,B,C) terlihat pada tabel 2 dibawah ini.

**Tabel 4 Hasil Ujicoba Verifikasi Sidik Jari**

No	ID_Sidik Jari	Jumlah percobaan	Posisi Jempol Pada saat pencocokan & Keberhasilan			Posisi Jempol Pada saat pencocokan & Kegagalan			Persentase kegagalan		
											
	Ulan	5	5	3	4	0	2	1	0%	40%	20%
	Ryan	5	5	4	3	0	1	2	0%	20%	40%
	Adry	5	4	3	4	1	2	1	20%	40%	20%

Dari hasil ujicoba sebanyak lima kali percobaan pada setiap posisi pencocokan sidik jari didapatkan hasil jumlah keberhasilan pada saat objek A melakukan ujicoba yaitu 12 kali keberhasilan, pada objek B sebanyak 12 kali keberhasilan, pada objek C sebanyak 11 kali dengan jumlah kegagalan pada objek A sebanyak 3, objek B sebanyak 3, dan objek C sebanyak 4 kali. mengalami kegagalan persentase kegagalan seperti tertera pada tabel 4. Sehingga disimpulkan penggunaan verifikasi sidik jari lebih baik dari pada penggunaan verifikasi wajah walaupun dipengaruhi oleh ketepatan posisi jempol pada alat sidik jari (*finger print*) namun penggunaan sidik jari tidak dipengaruhi oleh kondisi cahaya ruangan. Sehingga penggunaan akses keamanan menggunakan dua verifikasi dianggap lebih baik daripada hanya menggunakan satu verifikasi pengenalan wajah saja, untuk itu dirasakan amatlah tepat penambahan akses keamanan ruang dengan alat sidik jari (*finger print*).

**KESIMPULAN**

Dapat disimpulkan verifikasi pengenalan wajah amat sangat tergantung pada ketepatan posisi wajah didepan kamera serta sangat dipengaruhi oleh kondisi cahaya, posisi wajah dan tektur wajahnya. penggunaan verifikasi sidik jari lebih baik dari pada penggunaan verifikasi wajah walaupun dipengaruhi oleh ketepatan posisi jempol pada alat sidik jari (*finger print*) namun penggunaan sidik jari tidak dipengaruhi oleh kondisi ruangan. jumlah kegagalan lebih sedikit, Sehingga penggunaan akses keamanan menggunakan dua verifikasi dianggap lebih baik.

**DAFTAR PUSTAKA**

Alfi Syahri. 26 September 2013. Desain Sistem Kontrol Vending mesin Berbasis FPGA dengan pendekatan finite state Mechine.  
 Ramadhani Ulan sari. 2014. Perancangan Akses Keamanan Menggunakan dua buah Verifikasi Biometrik Pengenalan Wajah dan Sidik Jari.  
 Ramadhani Ulan sari. 2012. Perancangan dan Analisis Modul Sistem tertanam menggunakan Mikrokontroler Arduino UNO.  
 Maulanan Rahmat Hakim. 2013. Keamanan Akses Keamanan Ruang menggunakan Verifikasi Wajah.  
 Widodo, Romy Budhi. 2009. Embeded System menggunakan mikrokontroler dan pemrograman C. Yogyakarta : A