

# PENERAPAN METODE FACE-ARG (ATTRIBUTED RATIONAL GRAPH) UNTUK KEAMANAN BERTRANSAKSI VIA SMART CARD DENGAN PENGENAL WAJAH

LYCO ADHY PURWOKO (13508027)

Jurusan Teknik Informatika Institut Teknologi Bandung  
jalan Ganesha 10 Bandung  
e-mail : gondesadhy@yahoo.com

## ABSTRAK

Seiring dengan kemajuan teknologi yang berkembang dengan pesatnya, kemudahan dalam bertransaksi jual-beli pun semakin meningkat. Masyarakat hanya perlu membawa sebuah kartu kecil (smart card) yang simpel dan praktis untuk melakukan transaksi jual beli. Namun, hal tersebut tidak seaman yang dibayangkan. Masih banyak celah yang bisa dimanfaatkan oleh oknum yang tidak berwenang. Untuk mengatasi permasalahan tersebut, diperlukan adanya sistem pengamanan yang aman dan sulit untuk dimanipulasi. Yaitu adalah sistem pengaman menggunakan identifikasi biometrik metode Face-ARG (Attributed Rational Graph). Tetapi metode itu masih ada titik kurang efektifan dalam pencarian image dalam basis data. Untuk mengatasinya, ketika dalam bertransaksi pun keadaan pengambilan gambar yang nantinya akan dicocokkan di basis data yang ada, akan dikondisikan seakurat mungkin.

**Kata kunci:** Pengenalan wajah, metode Face-ARG (Attributed Rational Graph), basis data, transaksi, smart card, sistem pengaman.

## 1. PENDAHULUAN

Perkembangan teknologi saat ini sudah berkembang dengan pesatnya. Banyak teknologi-teknologi baru yang telah ditemukan oleh para ahli teknologi, bahkan hal-hal yang dianggap orang jaman dulu adalah suatu hal yang mustahil, sekarang ini sudah dapat dibuktikan atas penemuan-penemuan ilmuan saat ini.

Perkembangan teknologi yang pesat saat ini tentunya tidak terlepas dari perkembangan dunia komputer yang sangat pesat dan cepat. Baik perkembangan dunia komputer yang mengarah ke hal yang positif maupun ke hal yang negatif. Hal ini dikarenakan ada beberapa oknum yang dengan sengaja menggunakan teknologi komputer

untuk melakukan hal-hal yang negatif dan dapat merugikan orang banyak.

Salah satu teknologi komputer yang berkembang saat ini adalah teknologi pembayaran belanja menggunakan sebuah kartu yang memiliki identitas unik (barcode). Sehingga dengan teknologi tersebut, masyarakat dimanjakan untuk berbelanja tanpa membawa uang yang berlebihan dan memberatkan, hanya perlu membawa sebuah kartu yang praktis dan simpel (smart card). Dan juga dapat mencegah tindak kriminal pencurian karena meskipun kartu tersebut sampai jatuh ke tangan orang yang tidak tepat, orang tersebut tidak dapat langsung menggunakan seenaknya karena setiap kartu tersebut memiliki sebuah chip kecil (*Internal Circuit* kecil yang tertanam pada kartu) dan si pengguna harus memasukan sebuah sandi yang hanya diketahui oleh si pemilik (PIN).

Namun seiring dengan perkembangan teknologi yang sangat pesat dan kemampuan orang indonesia umumnya tentang teknologi terutama tentang IT, keamanan yang dirancang tersebut (transaksi melalui kartu) tidak dapat berlangsung lama. Dalam hanya hitungan beberapa bulan, sistem keamanan tersebut sudah dapat dimanipulasi oleh oknum-oknum yang tidak bertanggung jawab. Sehingga kartu atau tanpa kartu tersebut (e-bay via internet), seorang oknum bisa mendapatkan sandi dari si pemilik dan dapat menduplikasi chip (Jaringan terpadu) yang juga menyimpan sebuah data unik juga.

Untuk menjawab permasalahan tersebut, solusi yang tepat saat ini salah satunya adalah sistem pengaman menggunakan teknologi identifikasi biometrik. Identifikasi biometrik adalah teknologi yang yang berdasar pada karakteristik alami manusia yang tentunya setiap personal memiliki karakteristik alami yang berbeda-beda. Yaitu yang meliputi karakteristik fisiologis dan karakteristik perilaku, yang meliputi wajah, sidik jari, telapak tangan, iris dan retina mata, suara, DNA dan tanda tangan. Teknologi biometrik ini memiliki beberapa keunggulan dibandingkan dengan teknologi sistem pengaman konvensional lainnya, karena teknologi identifikasi biometrik ini tidak mudah untuk ditiru apalagi dicuri oleh oknum yang tidak berwenang. Karena pada dasarnya idenifikasi biometrik ini adalah pengidentifikasian seseorang melalui karakteristik

fisiologis tiap individu yang berbeda dan pasti beda dengan orang lain serta melekat. Sehingga akan susah untuk ditiru oleh orang lain. Wajah sebagai salah satu yang dapat digunakan untuk sistem pengaman berbasis identifikasi biometrik ini. Telah banyak pengaplikasian teknologi ini, sebagai contohnya untuk mencari orang hilang atau buronan polisi yang hanya diketahui data foto dirinya agar dapat diketahui keberadaannya dalam berbagai ekspresi rupa. Berbagai metode telah dikembangkan oleh beberapa ahli untuk mengenali wajah dengan benar, cepat dan akurat. Namun seiring berjalannya waktu, muncul permasalahan – permasalahan baru mengenai metode-metode tersebut. Mulai dari permasalahan sukarnya pengenalan wajah karena perbedaan posisi, pencahayaan yang kurang, hingga ketika ada sesuatu yang menutupi sebagian wajah. Salah satu metode yang sudah bekerja dengan baik yang dapat mengenali wajah walaupun dalam kondisi ekspresi yang berbeda-beda adalah metode *Face-ARG (Attributed Rational Graph)* – (Bo-Gun Park, et al. 2005; B.G. Park, et al. 2003).

Pada metode *Face-ARG* ini proses kerjanya adalah suatu gambar wajah akan ditransformasi menjadi struktur *Attributed Rational Graph (ARG)* yang terdiri dari himpunan node yang memiliki relasi binary di dalamnya dengan melalui proses pencocokan gambar dari dua buah wajah dengan cara mentransformasikan suatu gambar wajah menjadi sebuah bentuk graf yang terdiri dari himpunan node dan edge yang saling berhubungan.

Namun, metode ini juga ada sedikit kelemahannya. Kelemahan utamanya adalah metode ini dalam melakukan proses pencocokan hanya bisa dilakukan antara graf dari 2 gambar saja dan pencocokan harus dilakukan untuk semua wajah yang tersimpan di basis datanya. Sehingga apabila data yang terdapat pada basis data tersebut besar, maka waktu yang diperlukan untuk pencarian akan semakin lama. Selain itu, perbedaan ukuran image, variasi ekspresi dan latar juga mempengaruhi proses pencarian itu sendiri. Sedangkan untuk pengaplikasian pada makalah ini, yaitu sistem pengaman dalam bertransaksi menggunakan pengenalan wajah, akan dikondisikan agar foto yang dihsailkan ketika proses pengambilan gambar ketika bertransaksi memiliki kondisi yang serupa dengan data yang pertama kali diambil pada database yang ada.

## 2. TINJAUAN PUSTAKA

### 2.1 Sejarah

#### 2.1.1 Identifikasi Biometrik

Penggunaan teknologi identifikasi biometrik bukanlah sebuah teknologi baru. Karena sudah lama juga identifikasi biometrik konvensional digunakan, seperti tangan dan sidik jari.

Teknologi biometrik mengalami perkembangan pesat setelah diimplementasikan secara meluas dalam kerja bidang elektronik. Pemerintahan elektronik digunakan oleh pemerintah sebagai salah satu langkah untuk meningkatkan efisiensi dan efektivitas kinerja

pemerintahan dalam relasi internal dan eksternal negara. Selain itu penggunaan pemerintahan elektronik ini juga dimaksudkan untuk menunjang pelayanan publik kepada masyarakat. Banyak negara kemudian mengadopsi sistem pemerintahan elektronik ini untuk peningkatan kinerjanya.

Pada akhirnya sistem ini turut digunakan sebagai salah satu alat interaksi antarnegara dalam ruang lingkup internasional. Karena di dalam sistem ini informasi yang diakses merupakan data-data yang bersifat rahasia dan sensitif, tercipta suatu tantangan keamanan yang signifikan. Proteksi internasional terhadap data sensitif membawa perubahan pada sistem pengamanan data tersebut untuk mengantisipasi potensi pelanggaran yang dilakukan agen pemerintah maupun masyarakat dalam mengakses informasi tersebut.

Penggunaan sistem elektronik baru ini membuat seluruh penggunaannya, yaitu agen pemerintah dan masyarakat, untuk menggunakan media elektronik. Pemerintah menyesuaikan diri dengan pola kebiasaan masyarakat yang selalu menggunakan interaksi fisik untuk membangun kepercayaan antara masyarakat dan pemerintah yang menggunakan internet sebagai dasar dari sistem kinerja mereka. Salah satu dari upaya peningkatan kepercayaan terhadap penggunaan teknologi pemerintahan elektronik ini adalah sistem keamanan yang dapat mengimbangnya, yaitu sistem pemindaian biometrik.

#### 2.1.2 Smart Card

Kartu pintar ditemukan dan dipatenkan pada 1970-an. Ada beberapa perselisihan tentang siapa "penemu" asli kartu ini termasuk Jürgen Dethloff dari Jerman, Arimura dari Jepang, dan Roland Moreno dari Perancis. Penggunaan masal pertama kali dari kartu ini adalah untuk pembayaran telepon di Perancis pada 1983.

### 2.2 Transaksi Jual-Beli Via Smart Card

Transaksi jual-beli pada jaman sekarang ini, seiring dengan berkembangnya teknologi yang berkembang dengan pesatnya. Selalu memberikan kemudahan dan memanjakan masyarakat pada umumnya. Salah satunya yang dibahas pada makalah ini adalah penggunaan smart card untuk transaksi jual beli baik secara langsung (fisik) maupun tidak langsung (non-fisik) yang sistem transaksinya menggunakan sebuah rangkaian terintegrasi kecil yang ada pada kartu tersebut yang fungsinya sebagai identitas kartu tersebut yang artinya juga mengidentifikasi si pemilik kartu itu sendiri serta ditambah sistem pengaman dengan masukan sandi yang hanya diketahui oleh si pemilik.

#### 2.3 Metode Face-ARG

Pada tahun 2005 Bo-Gun Park et al, mempunyai sebuah usulan yaitu sebuah metode baru dalam proses pencocokan gambar dari dua buah wajah dengan tingkat keberhasilan

lebih baik dibandingkan dengan metode lainnya. Metode yang digunakannya adalah *Face ARG (Attributed Rational Graph)* yang mentransformasikan gambar suatu wajah menjadi bentuk suatu graph yang terdiri dari himpunan node dan edge yang saling berhubungan.

Teori dasar dari metode ARG sendiri telah dijelaskan dalam paper B.G. Park et al, (2003). Di dalam paper tersebut dijelaskan bahwa setelah dua buah gambar diekstrak menjadi bentuk graf yang akan dicocokkan agar diperoleh sebuah graf dengan prioritas terbaik. Kemudian dilakukan pendeteksian terhadap fitur – fitur yang harus dihilangkan agar diperoleh graf yang saling berkorespondensi.

Ekstraksi dari suatu model image menjadi sebuah bentuk ARG dilakukan dengan menggunakan *straight line segment* (Sang Ho Park, et al., 2000), dimana objek yang dihasilkan adalah sama walaupun dilakukan proses RTS (*Rotation, Translation, Scale*).

### 3. PEMBAHASAN

#### 3.1 Sistem Smart Card

##### 3.1.1 Smart Card Sentuh

Kartu pintar sentuh memiliki chip keemasan dengan diameter sekitar setengah inci. Pada saat dimasukan ke pembaca kartu, chip berhubungan dengan penghubung elektronik yang dapat membaca informasi dari chip dan menuliskannya kembali.

Standar ISO/IEC 7816 dan ISO/IEC 7810 mendefinisikan:

- Bentuk fisik
- Posisi dan bentuk penghubung elektronik
- Sifat kelistrikan
- Protokol Komunikasi
- Format perintah yang dikirimkan ke kartu dan tanggapan balik dari kartu
- Ketahanan kartu
- fungsi

Kartu ini tidak memiliki baterai, energi disediakan oleh pembaca kartu.

##### 3.1.2 Smart Card Non-Sentuh

Kartu ini berkomunikasi dengan pembaca kartu dengan cara teknologi induksi RFID (dengan kecepatan pertukaran data dari 106 sampai 848 kbit/detik). Kartu ini hanya perlu didekatkan dengan pembaca kartu untuk menyelesaikan transaksi. Kartu ini banyak digunakan untuk sistem transportasi masal yang membutuhkan proses yang cepat atau tanpa menggunakan tangan.

Standar untuk kartu ini adalah ISO/IEC 14443. Standar ini mendefinisikan dua tipe kartu non-sentuh yang dapat berkomunikasi sampai jarak 10 cm. Standar lainnya adalah ISO 15693 yang mengijinkan komunikasi sampai jarak 50 cm.

Kartu non-sentuh yang digunakan luas berada di Hong Kong dengan kartu Octopus dan di Paris dengan Kartu Calypso/Navigo, yang ada sebelum ISO/IEC 14443.

#### 3.2.3 Kelebihan dan Kekurangan Smart card

##### 3.2.3.1 Kelebihan Smart Card

- Memiliki kemampuan untuk digunakan dalam berbagai fungsi aplikasi (multifungsi)
- Meringkas sejumlah uang kedalam bentuk yang praktis dan mudah dibawa kemana saja
- mempunyai bentuk yang simpel

##### 3.2.3.2 Kekurangan Smart Card

Seiring dengan perkembangan teknologi, keamanan dalam bertransaksi menggunakan smart card (kartu kredit, kartu debit) tidak bisa dijamin lagi keamanannya. Sekarang chip yang tertanam dalam kartu tersebut dapat diduplikasi dan sandi dari kartu tersebut juga dapat diperoleh dengan permainan manipulasi komputisasi sehingga kartu tersebut dapat digunakan oleh oknum yang tidak berwenang untuk kepentingan pribadinya yang tentu saja merugikan pemilik kartu sebenarnya.

#### 3.2 Pengenalan Wajah Dengan Metode Face-ARG

Suatu gambar wajah yang telah diambil dan ditransformasikan ke dalam bentuk ARG akan memiliki himpunan node-node dan relasi binary di dalamnya. Gambar wajah ARG dapat didefinisikan dalam bentuk :

$$Face - ARG : G = (V, R, F), \quad (1)$$

Dimana  $V = \{v_1, \dots, v_n\}$  adalah himpunan node dari suatu graf,  $R = \{rij | v_i, v_j \in V, i \neq j\}$  adalah himpunan relasi binary dari vektor-vektor yang terdapat dalam node.

$F = \{Ri | i = 1, \dots, N\}$  himpunan dari relasi ruang vektor dari node. Relasi ruang vektor  $Ri = \{rij | j = 1, \dots, N, j \neq i\}$ , untuk  $i = 1, \dots, N$ . Merepresentasikan himpunan relasi vektor antara node  $v_i$  dengan node-node lain di dalam  $V$ . Dapat disimpulkan bahwa jika terdapat dua buah wajah yang sama maka relasi ruang vektor yang terdapat dalam bentuk ARG kedua wajah tersebut seharusnya juga sama, dengan membandingkan relasi ruang vektor dari dua gambar wajah maka akan dapat dievaluasi tingkat kesamaan dari kedua gambar tersebut.

Untuk mendeskripsikan objek secara invariant agar dapat melakukan proses RTS (*Rotasi, Traslasi, Scale*) maka digunakan enam tipe ukuran yang berbeda,

$$rij(1) = \theta, \quad rij(2) = \theta c, \quad rij(3) = \theta m \quad (2)$$

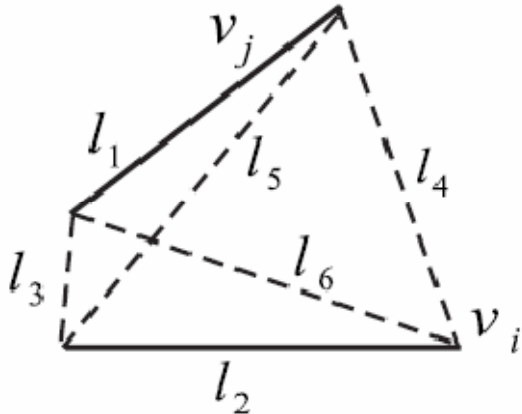
$$rij(4) = DR, \quad rij(5) = mij,x, \quad rij(6) = mij,y, \quad (3)$$

Dimana  $rij(1)$  adalah sudut antara dua segment aris  $v_i$  dan  $v_j$ .  $rij(2)$  adalah complement sudut dari sudut terkecil di

dalam vektor.  $r_{ij}$  (3) adalah sudut antara titik tengah dari  $v_i$  terhadap  $v_j$ ,  $r_{ij}$  (4) adalah rasio jarak yang dihitung dengan persamaan

$$DR = \frac{l_1+l_2}{(l_3+l_4+l_5+l_6)} \quad (4)$$

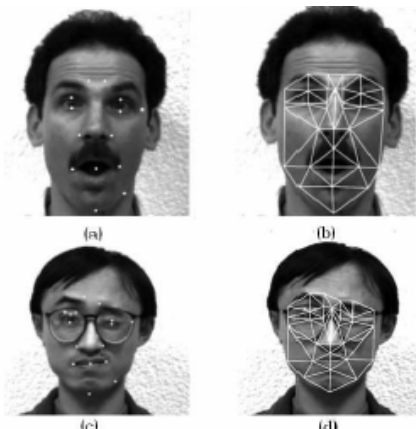
Dimana  $l(i)$  untuk  $i = 1,2,\dots,6$  dijelaskan seperti gambar 1



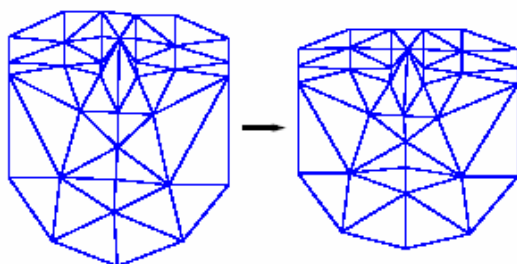
Gambar 1. Rasio jarak dari DR

$r_{ij}$  (5) dan  $r_{ij}$  (6) adalah koordinat dari titik tengah vektor  $m_{ij}$ , yang merupakan vektor dari dua titik tengah  $v_i$  dan  $v_j$ .

Pola yang diberikan oleh Face-ARG berupa kordinat – kordinat yang diberikan pada wajah sehingga membentuk suatu graf yang nantinya akan dinyatakan dalam bentuk vektor baris. Sebagai contoh dapat dilihat pada gambar2[6].



Gambar2 . pasangan kordinat-kordinat pada image wajah



Gambar 3. Contoh graf yang dihasilkan oleh gambar 2

Dari graf yang dihasilkan akan diperoleh vektor jarak yang menyatakan hubungan antar node yang saling berkorespondensi dalam graf yang dihasilkan oleh masing-masing image. Sehingga dapat disimpulkan apabila suatu image masuk vektor graf yang dihasilkan juga harus sama dengan vektor yang dihasilkan oleh image yang sama yang disimpan dalam basis data, dengan cara membandingkan tingkat kesamaan antar graf yang dihasilkan oleh setiap image. Tingkat kesamaan antara dua *face* Face-ARG,  $g_1$  dan  $g_2$  dengan pasangan node yang berkorespondensi sebanyak  $N$  dapat dihitung, dengan persamaan

$$S(G^{G1 \leftrightarrow G2}) = \sum_{i=1}^N D(R_i) \cdot W_i = \sum_{i=1}^N W_i \cdot \left[ \prod_{j=1, j \neq i}^N p(r_{ij}^{G2} - r_{ij}^{G1}) \cdot \gamma_{ij} \right] \quad (5)$$

Dimana  $D(R_i)$  adalah fungsi untuk menghitung perbedaan antara relasi ruang vektor  $R_i^{G1}$  dan  $R_i^{G2}$ .  $p(r_{ij}^{G2} - r_{ij}^{G1})$  adalah probabilitas error pada relasi ruang vektor dan  $\omega_i$  dan  $\gamma_{ij}$  adalah faktor berat dari fitur  $v_1$  dan faktor berat dari relasi biner antara fitur  $v_i$  dan  $v_j$ . Diasumsikan error pada relasi vektor adalah Gaussian dan elemen-elemen yang ada adalah independen. Untuk  $r_{ij}$  pada tiap persamaan dimodelkan dengan distribusi gussian dengan persamaan

$$P(\Delta = (r_{ij}(5), r_{ij}(6)) - (r_{ij}(5), r_{ij}(6))) = \begin{cases} \frac{1}{\sqrt{2\pi\sigma_e}} \cdot \exp\left(-\frac{\Delta^2}{2\sigma_e^2}\right), & \text{if } |\Delta| < D_{thres}, \\ P_c = \frac{1}{\sqrt{2\pi\sigma_e}} \cdot \exp\left(-\frac{D_{thres}^2}{2\sigma_e^2}\right), & \text{otherwise} \end{cases} \quad (6)$$

(7)

Proses pencocokan yang paling baik dan efektif dari kedua wajah yang diuji kesamaannya dapat diidentifikasi dengan menghitung nilai kesamaan tertinggi dari keduanya yang berada di atas nilai threshold. Nilai treshold tersebut didefinisikan sebagai batas pengenalan akhir dari kedua face-ARG.

$$Face - ID = \arg_{GM \in FDB} \max S(G^{GM \leftrightarrow GT}) \quad (8)$$

Kesulitan yang akan dihadapi bila menggunakan metode Face-ARG adalah apabila image wajah yang dimasukkan sama tetapi memiliki ekspresi wajah yang berbeda, latar yang berbeda atau ukurannya yang berbeda seperti pada gambar 4[3], hal ini akan mengakibatkan FACE-ARG menjadi metode yang kurang efektif karena diperlukannya basis data yang besar untuk menyimpan

semua kemungkinan yang akan terjadi dengan wajah tersebut. Seperti untuk menyimpan satu wajah dengan berbagai ekspresi, kemudian waktu yang diperlukan untuk proses pencarian pola wajah yang tepat juga menjadi berlangsung relatif lama. Karena apabila image yang akan dibandingkan berada pada basis data yang memiliki data banyak, maka waktu pencariannya pun akan berlangsung relatif lama karena metode face-arg ini melakukan pengenalan wajah dengan melakukan perbandingan hanya terbatas antara 2 image saja setiap pengecekannya. Sehingga apabila basis data memiliki 100 gambar dengan berbagai ekspresi wajah yang berbeda, maka proses pencocokan yang harus dilakukan adalah 4950 perbandingan



**Gambar 4. Contoh image dengan berbagai ekspresi yang disimpan dalam basis data (Jiao Feng, Gao, Wen, et al., 2002).**

### 3.3 Sinkronisasi Kerja

Pada sinkronisasi kerja pada sistem ini sebenarnya hampir sama dengan sistem kerja smart card yang digunakan untuk transaksi pada umumnya. Namun terdapat letak perbedaan ketika pengecekan keabsahan dari pemilik kartu tersebut. Apabila pada smart card pada umumnya pengecekan hanya dilakukan melalui peng-*input*-an sandi yang hanya diketahui si pemilik yang tentu saja sistem seperti ini, orang lain dapat mencari tahu sandi tersebut agar bisa menggunakan kartu tersebut atau dengan memanipulasi sandi kartu tersebut. Untuk mencegah hal yang seperti demikian, sistem pengecekan menggunakan pengenalan wajah yang tiap orang memiliki wajah yang berbeda dan sulit untuk ditiru orang lain.

Mekanisme kerja pada smart card yang digunakan untuk transaksi menggunakan sistem pengamanan pengenalan wajah memiliki 2 tahapan, yaitu :

- Peng-identifikasian smart card baik smart card tipe sentuh yang menggunakan pembaca kartu maupun kartu non-sentuh yang menggunakan teknologi induksi RFID
- Setelah melakukan penidentifikasi bahwa smart card tersebut digunakan untuk transaksi jual-beli, kemudian dilakukan pengecekan keabsahan kepemilikan kartu tersebut dengan pengenalan wajah yang menggunakan metode Face-ARG ini.

Pada saat pengecekan keabsahan ini yang menggunakan pengenalan wajah, dalam pengambilan gambar dilakukan dalam kondisi yang sekondusif mungkin. Maksudnya adalah keadaan pengambilan gambar dilakukan dengan kondisi ekspresi wajah yang seakurat mungkin disamakan dengan data image yang tersimpan pada basis data yang ada, agar basis data yang digunakan tidak memerlukan data yang begitu banyak dan besar. Sehingga pengecekan pengenalan wajah dengan metode Face-ARG ini memakan waktu se-efektif mungkin dan sesingkat mungkin. Dan pengecekan keabsahan melalui identifikasi biometrik dengan pengenalan wajah ini dapat bekerja singkat dan akurat, sehingga sistem keamanan transaksi via smart card menggunakan pengenalan wajah ini dapat terjaga keamanannya dari pihak-pihak yang tidak bertanggung jawab.

## 4. KESIMPULAN

Untuk menjaga keamanan ketika bertransaksi via smart card, akan memberikan efek yang lebih aman apabila sistem keamanannya diubah. Dari yang biasanya hanya menggunakan sebuah sandi yang dimasukan oleh si pemilik ketika akan bertransaksi digantikan oleh sistem identifikasi biometrik menggunakan pengenalan wajah melalui metode Face-ARG (Attributed Rational Graph). Karena apabila sistem pengamanannya menggunakan identifikasi biometrik (pengenalan wajah) maka sulit bagi oknum-oknum yang tidak bertanggung jawab untuk memanipulasi serta menirunya, sehingga keamanan bertransaksi via smart card akan lebih aman. Sistem pengenalan wajah yang digunakan adalah dengan metode Face-ARG (Attributed Rational Graph) adalah setiap image wajah yang masuk akan direpresentasikan dalam bentuk vektor graph yang nantinya akan disesuaikan dengan vektor graf dari satu image lain yang dengan melihat tingkat kesesuaiannya, setiap pencocokan yang dilakukan dengan metode Face-ARG (Attributed Rational Graph) hanya dapat dilakukan untuk dua image, sehingga diperlukan waktu dan proses yang lama untuk setiap image diidentifikasi. Untuk meng-efisienkan waktu proses, pengambilan gambar yang dilakukan ketika melakukan transaksi untuk pengecekan keabsahan dari pemilik kartu, kondisi yang ada dibuat sekondusif mungkin agar meminimalisir perbedaan kondisi ekspresi wajah sehingga data image yang di dalam basis data pun tidak memerlukan data yang banyak sehingga proses pengecekan dapat berlangsung lebih cepat.

## REFERENSI

- [1] Bo-Gun Park, Kyoung-Mu Lee, and Sang-Uk Lee. (2005). "Face Recognition Using Face-ARG Matching", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 27, No. 12, December 2005.
- [2] B.G. Park, K.M. Lee, S.U. Lee, and J.H. Lee. (2003). "Recognition of Partially Occluded Objects Using Probabilistic ARG-Based Matching." Computer Vision and

Image Understanding, Vol. 90, No. 3, pp. 217-241, June 2003.

- [3] Jiao Feng, Gao, Wen, et al. (2002). "A Face Recognize Method Based on Local Feature Analysis", The 5th Asian Conference on Computer Vision, January 2002, Melbourne, Australia.
- [4] Kusumadewi, Sri. (2003). "Artificial Intelligence: Teknik dan Aplikasinya", Graha Ilmu, Yogyakarta.
- [5] Li, Xiaoxing, Mori Greg, HaoZhang. (2005). "Expression-Invariant Face Recognition with Expression Classification",
- [6] Sang Ho Park, Kyoung Mu Lee, and Sang Uk Lee. (2000). "A Line Feature Matching Technique Based On an Eigenvector Approach," Computer Vision and Image Understanding, Vol. 77, No. 3, pp. 263-283, March 2000.
- [7] Penggunaan biometrik dalam pemerintahan elektronik. [http://id.wikipedia.org/wiki/Pemindai\\_biometrik#Penggunaan\\_biometrik\\_dalam\\_pemerintahan\\_elektronik](http://id.wikipedia.org/wiki/Pemindai_biometrik#Penggunaan_biometrik_dalam_pemerintahan_elektronik). Tanggal akses 19 Desember 2009.
- [8] Pengertian dan macam – macam jenis Smart card. [http://id.wikipedia.org/wiki/Smart\\_card#sejarah](http://id.wikipedia.org/wiki/Smart_card#sejarah). Tanggal akses 19 Desember 2009.