

# APLIKASI TRANSFORMASI CITRA TANDA TANGAN MENJADI TANDA TANGAN DIGITAL

David Samuel – NIM: 13506081

Program Studi Teknik Informatika, Institut Teknologi Bandung  
Jl. Ganesha 10, Bandung  
E-mail : if16081@students.itb.ac.id

## Abstrak

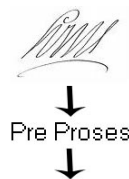
Pengiriman dokumen melalui internet adalah hal yang sering dilakukan. Akan tetapi, seiring dengan semakin pentingnya dokumen yang dikirim, maka diperlukan sebuah mekanisme untuk membuktikan bahwa dokumen elektronik yang dikirim adalah sesuai dengan yang dimaksudkan oleh pengirim. Ada banyak sekali serangan berbahaya yang dapat dilancarkan apabila sebuah dokumen elektronik yang dikirim melalui jaringan tidak disertai dengan sebuah mekanisme untuk melakukan verifikasi dan autentikasi. Salah satunya adalah pengatasnamaan pengiriman sebuah dokumen elektronik oleh seseorang yang tidak bertanggung jawab. Tanda tangan digital adalah salah satu cara untuk melakukan verifikasi dan otentikasi berkas elektronik. Ada banyak teknik yang dapat digunakan dalam menghasilkan tanda tangan digital yang dapat disisipkan pada dokumen, dan semua teknik yang ada memiliki kelebihan dan kekurangan masing-masing.

Seiring dengan kemajuan zaman, manusia menginginkan sebuah mekanisme verifikasi dokumen elektronik dengan cara yang semakin manusiawi dan mendekati kenyataan. Ada beberapa cara yang mulai dikembangkan yang tidak terbatas pada verifikasi dokumen elektronik, yaitu verifikasi menggunakan deteksi iris mata, sidik jari, dan tanda tangan seseorang. Pada makalah ini, dipaparkan kemungkinan untuk mentransformasikan citra tanda tangan sebagai masukan pada sebuah aplikasi autentikasi biometrik tanda tangan sehingga bisa disisipkan ke dalam berkas elektronik sebagai salah satu alat verifikasi dan autentikasi.

**Kata Kunci:** Biometrik, Busur Terlokalisasi, Vektor Eigen, Pola Citra Tanda Tangan

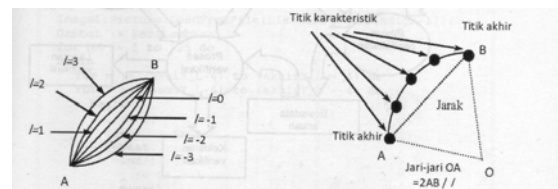
## 1. Pendahuluan

Sistem verifikasi menggunakan biometrika citra tanda tangan dengan metode busur terlokalisasi adalah salah satu cara yang umum digunakan dalam dunia biometrik. Metode pola busur terlokalisasi memanfaatkan kemunculan suatu pola tertentu sebagai ciri. Metode pola busur terlokalisasi dikembangkan dari metode pola busur (*Arc Pattern Method*).



**Gambar 1 Skema Umum Proses Transformasi Citra Tanda Tangan**

Secara umum, metode ini mengambil sebuah pandangan umum menempatkan beberapa buah titik berjarak sama antara titik awal dan titik akhir sebuah busur, yang disebut dengan titik karakteristik, titik-titik karakteristik ini yang akan menyusun pola model yang dipergunakan sebagai karakteristik tanda tangan.



**Gambar 2 Titik Karakteristik pada sebuah busur**

Berdasarkan frekuensi kemiripan titik-titik model pada citra sampel, akan ditentukan keaslian sebuah dokumen elektronik. Untuk pemeriksaan

bahwa dokumen elektronik tidak mengalami perubahan semenjak dikirimkan oleh pengirim, digunakan algoritma hash MD5. Kombinasi algoritma dan citra tanda tangan inilah yang akan menentukan apakah sebuah dokumen elektronik ini asli atau telah mengalami modifikasi.

## 2. Batasan Masalah

Makalah ini membatasi permasalahan yang dibahas mengenai cara identifikasi dengan menggunakan pola busur terlokalisasi, sebagai salah satu metode biometrik verifikasi citra tanda tangan.

Hasil verifikasi akan kemudian dicocokkan dengan 128 bit hasil algoritma hash MD5 yang telah terdapat pada basis data acuan. Dengan demikian, batasan terdapat pada proses pembangunan dan verifikasi dokumen elektronik saja dan tidak menyangkut pembahasan performa dan tingkat kesalahan dari aplikasi transformasi citra tanda digital.

## 3. Algoritma Hash MD5

Algoritma MD5 adalah sebuah hash function yang akan menghasilkan keluaran message digest sepanjang 128 bit.

Langkah-Langkah yang dilakukan adalah:

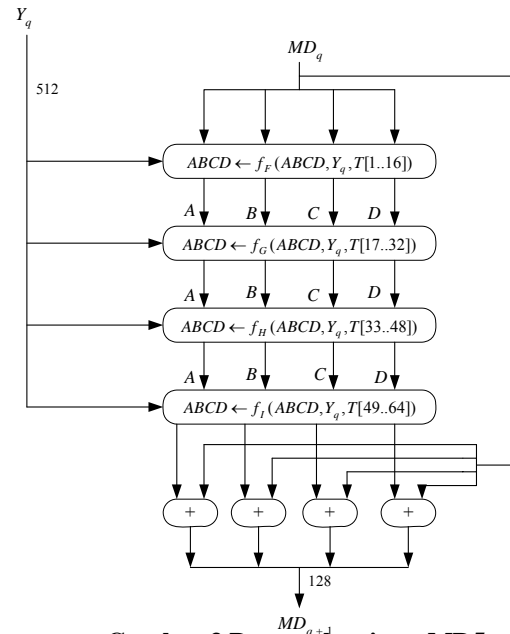
1. Penambahan bit-bit pengganjal
2. Penambahan nilai panjang pesan semula
3. Inisialisasi Penyangga
4. Pengolahan pesan dalam blok berukuran 512 bit

Pada tahap awal, pesan akan ditambah dengan bit-bit pengganjal sehingga panjang pesan kongruen dengan 448 modulo 512. Sehingga nanti pesan akan berukuran kelipatan 512 bit, setelah 64 bit terakhir yang ditambahkan adalah informasi panjang pesan sebelum ditambahkan bit pengganjal.

Inisialisasi penyangga MD5 membutuhkan 4 buah penyangga(buffer) yang masing-masing berukuran 32 bit. Keempat penyangga ini berisi dalam hex sebagai berikut:

A= 0x67452301  
 B= 0xEFCDAB89  
 C= 0x98BADCFE  
 D= 10325467

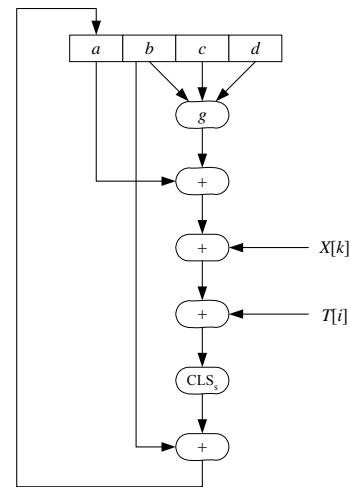
Pengolahan pesan dalam blok berukuran 512 bit oleh algoritma MD5 dapat dilihat pada gambar berikut:



Gambar 3 Proses algoritma MD5

Proses  $H_{MD5}$  terdiri dari 4 buah putaran, dan masing-masing putaran melakukan operasi dasar MD5 sebanyak 16 kali dan setiap operasi dasar memakai sebuah elemen  $T$ . Jadi setiap putaran memakai 16 elemen Tabel  $T$ .

Sedangkan setiap operasi dasar MD5 dapat dilihat pada gambar berikut:



Gambar 4 Operasi Dasar MD5

Fungsi-fungsi dasar MD5

| Nama  | Notasi       | $g(b, c, d)$                          |
|-------|--------------|---------------------------------------|
| $f_F$ | $F(b, c, d)$ | $(b \wedge c) \vee (\sim b \wedge d)$ |
| $f_G$ | $G(b, c, d)$ | $(b \wedge d) \vee (c \wedge \sim d)$ |
| $f_H$ | $H(b, c, d)$ | $b \oplus c \oplus d$                 |
| $f_I$ | $I(b, c, d)$ | $c \oplus (b \wedge \sim d)$          |

**Catatan:** operator logika AND, OR, NOT, XOR masing-masing dilambangkan dengan  $\wedge, \vee, \sim, \oplus$

Nilai  $T[i]$

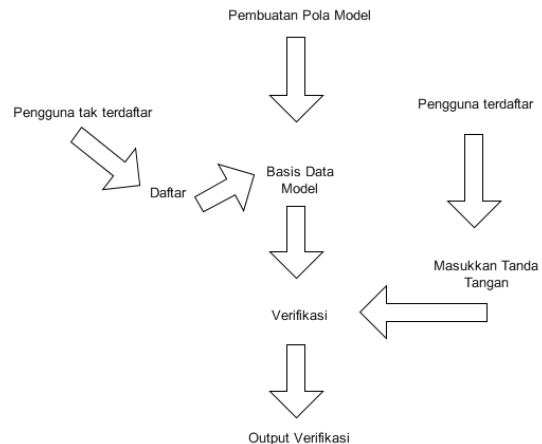
|                  |                  |                  |                  |
|------------------|------------------|------------------|------------------|
| T[1] = D76AA478  | T[17] = F61E2562 | T[33] = FFFA3942 | T[49] = F4292244 |
| T[2] = E8C7B756  | T[18] = C040B340 | T[34] = 8771F681 | T[50] = 432AFF97 |
| T[3] = 242070DB  | T[19] = 265E5A51 | T[35] = 69D96122 | T[51] = AB9423A7 |
| T[4] = C1BDCEE   | T[20] = E9B6C7A  | T[36] = FDE5380C | T[52] = FC93A039 |
| T[5] = E         | T[21] = A        | T[37] = T[37]    | T[53] = T[53]    |
| T[6] = F57C0FAF  | T[22] = D62F105D | T[38] = 4        | T[54] = T[54]    |
| T[7] = 4787C62A  | T[23] = 02441453 | T[39] = 4BDECFA  | T[55] = T[55]    |
| T[8] = A8304613  | T[24] = D8A1E681 | T[40] = T[40]    | T[56] = T[56]    |
| T[9] = FD469501  | T[25] = E7D3FBC  | T[41] = T[41]    | T[57] = T[57]    |
| T[10] = 698098D8 | T[26] = T[25]    | T[42] = 0        | T[58] = T[58]    |
| T[11] = 8B44F7AF | T[27] = 21E1CDE  | T[43] = T[41]    | T[59] = FE2CE6E0 |
| T[12] = FFFF5BB1 | T[28] = 6        | T[44] = 289B7EC6 | T[60] = T[59]    |
| T[13] = 895CD7BE | T[29] = C33707D6 | T[45] = EAA127F  | T[61] = A3014314 |
| T[14] = 6B901122 | T[30] = T[27]    | T[46] = A        | T[62] = T[60]    |
| T[15] = FD987193 | T[31] = F4D50D87 | T[47] = T[43]    | T[63] = T[61]    |
| T[16] = A9E3E905 | T[32] = T[28]    | T[48] = D4EF3085 | T[64] = F7537E82 |
| T[17] = T[15]    | T[33] = 455A14ED | T[49] = T[44]    | T[65] = T[62]    |
| T[18] = T[16]    | T[34] = 04881D05 | T[50] = T[45]    | T[66] = BD3AF235 |
| T[19] = T[17]    | T[35] = D9D4D03  | T[51] = T[46]    | T[67] = T[63]    |
| T[20] = T[18]    | T[36] = T[30]    | T[52] = T[47]    | T[68] = T[64]    |
| T[21] = T[19]    | T[37] = T[31]    | T[53] = T[48]    | T[69] = T[65]    |
| T[22] = T[20]    | T[38] = T[32]    | T[54] = T[49]    | T[70] = T[66]    |
| T[23] = T[21]    | T[39] = T[33]    | T[55] = T[50]    | T[71] = T[67]    |
| T[24] = T[22]    | T[40] = T[34]    | T[56] = T[51]    | T[72] = T[68]    |
| T[25] = T[23]    | T[41] = T[35]    | T[57] = T[52]    | T[73] = T[69]    |
| T[26] = T[24]    | T[42] = T[36]    | T[58] = T[53]    | T[74] = T[70]    |
| T[27] = T[25]    | T[43] = T[37]    | T[59] = T[54]    | T[75] = T[71]    |
| T[28] = T[26]    | T[44] = T[38]    | T[60] = T[55]    | T[76] = T[72]    |
| T[29] = T[27]    | T[45] = T[39]    | T[61] = T[56]    | T[77] = T[73]    |
| T[30] = T[28]    | T[46] = T[40]    | T[62] = T[57]    | T[78] = T[74]    |
| T[31] = T[29]    | T[47] = T[41]    | T[63] = T[58]    | T[79] = T[75]    |
| T[32] = T[30]    | T[48] = T[42]    | T[64] = T[59]    | T[80] = T[76]    |
| T[33] = T[31]    | T[49] = T[43]    | T[65] = T[60]    | T[81] = T[77]    |
| T[34] = T[32]    | T[50] = T[44]    | T[66] = T[61]    | T[82] = T[78]    |
| T[35] = T[33]    | T[51] = T[45]    | T[67] = T[62]    | T[83] = T[79]    |
| T[36] = T[34]    | T[52] = T[46]    | T[68] = T[63]    | T[84] = T[80]    |
| T[37] = T[35]    | T[53] = T[47]    | T[69] = T[64]    | T[85] = T[81]    |
| T[38] = T[36]    | T[54] = T[48]    | T[70] = T[65]    | T[86] = T[82]    |
| T[39] = T[37]    | T[55] = T[49]    | T[71] = T[66]    | T[87] = T[83]    |
| T[40] = T[38]    | T[56] = T[50]    | T[72] = T[67]    | T[88] = T[84]    |
| T[41] = T[39]    | T[57] = T[51]    | T[73] = T[68]    | T[89] = T[85]    |
| T[42] = T[40]    | T[58] = T[52]    | T[74] = T[69]    | T[90] = T[86]    |
| T[43] = T[41]    | T[59] = T[53]    | T[75] = T[70]    | T[91] = T[87]    |
| T[44] = T[42]    | T[60] = T[54]    | T[76] = T[71]    | T[92] = T[88]    |
| T[45] = T[43]    | T[61] = T[55]    | T[77] = T[72]    | T[93] = T[89]    |
| T[46] = T[44]    | T[62] = T[56]    | T[78] = T[73]    | T[94] = T[90]    |
| T[47] = T[45]    | T[63] = T[57]    | T[79] = T[74]    | T[95] = T[91]    |
| T[48] = T[46]    | T[64] = T[58]    | T[80] = T[75]    | T[96] = T[92]    |
| T[49] = T[47]    | T[65] = T[59]    | T[81] = T[76]    | T[97] = T[93]    |
| T[50] = T[48]    | T[66] = T[60]    | T[82] = T[77]    | T[98] = T[94]    |
| T[51] = T[49]    | T[67] = T[61]    | T[83] = T[78]    | T[99] = T[95]    |
| T[52] = T[50]    | T[68] = T[62]    | T[84] = T[79]    | T[100] = T[96]   |

|                  |                  |                  |                  |
|------------------|------------------|------------------|------------------|
| A679438E         | FCEFA3F          | 9                | B                |
| T[16] = 49B40821 | T[31] = 676F02D9 | T[46] = E6DB99E5 | T[64] = EB86D391 |
|                  | T[32] = 8D2A4C8  | T[47] = 1FA27CF8 |                  |
|                  | A                | T[48] = C4AC5665 |                  |

Keluaran dari algoritma MD5 adalah message digest dengan ukuran 128 bit, yang dapat dipakai untuk melakukan perhitungan selanjutnya. Hasil ini akan disimpan dalam basis data acuan untuk kemudian diperiksa kebenarannya dengan citra tanda tangan digital.

#### 4. Gambaran Umum Sistem Verifikasi

Pada tahap pertama pengembangan, dibutuhkan pola model yang akan digunakan sebagai pola model tetap sistem. Pola ini dimasukkan sekali pada saat sistem ini pertama kali dibuat.



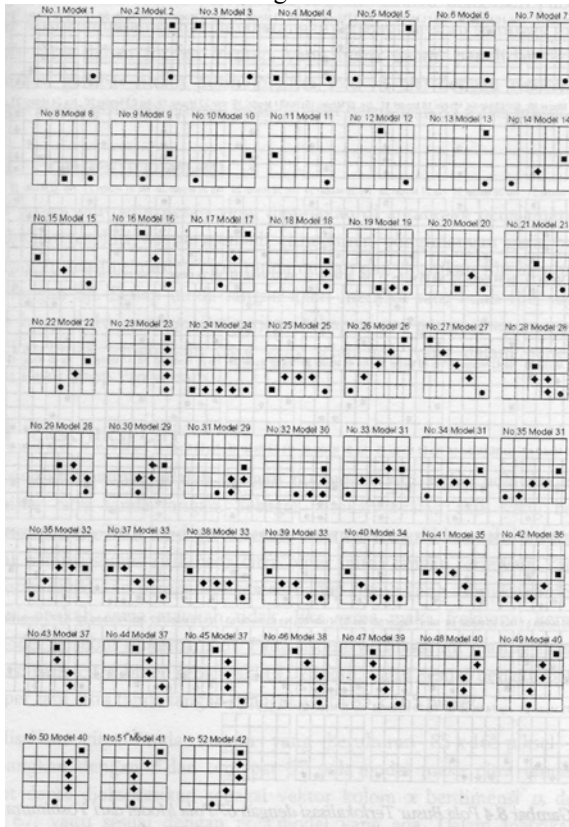
**Gambar 5 Skema Umum Sistem**

Verifikasi tanda tangan dilakukan dengan cara memasukkan nomor identitas yang telah diberikan secara unik kepada masing-masing pengguna, dalam hal ini adalah hasil keluaran algoritma hash MD5, dan pengguna memasukkan citra tanda tangan, dan dilakukan proses perbandingan. Keluaran dari proses verifikasi ini adalah laporan mengenai penerimaan atau penolakan dari tanda tangan masukan.

#### 5. Akuisisi Model Tanda Tangan

Pada proses ini, dikumpulkan sejumlah tanda tangan, untuk mendapatkan pola model tanda tangan secara umum. Area citra tanda tangan dibagi menjadi kotak-kotak berukuran 5x5. Banyaknya pola model

yang digunakan adalah 40, dan batas terkecil cacah keseringan muncul adalah 20 kali sehingga diperoleh 52 pola. 52 pola tanda tangan menurut model pola Yoshumura inilah yang akan dipergunakan sistem untuk ekstraksi citra tanda tangan.



Gambar 6 Pola Busur Terlokalisasi Yoshimura

## 6. Akuisisi Data

Sampel tanda tangan ditulis di atas kertas dengan ukuran 2 cm x 4 cm. Penulisan tanda tangan sampel tidak boleh melebihi daerah persegi panjang ini. Sampel di-scan dengan format citra bitmap, sehingga didapat sebuah citra tanda tangan digital.

Setelah itu pra-pemrosesan dilakukan dengan mengubah gambar menjadi biner, dan area dibagi menjadi kotak berukuran 5x5. Lalu akan dilakukan ekstrak ciri sesuai dengan pola busur terlokalisasi yang telah didapat.

Cara penghitungannya adalah dengan menggerakkan setiap pola model busur terlokalisasi di atas citra tanda tangan. Lingkaran penuh digunakan sebagai patokan. Titik ini digeser secara teratur satu grid secara vertikal atau horizontal, sampai semua titik pada citra biner tanda tangan terlewati. Pada saat proses perbandingan, maka frekuensi kemunculan pola model tersebut ditambahkan.

Misalkan citra tanda tangan berukuran 85x 165 pixel, maka hasil ekstraksi frekuensi kemunculan pola dapat dinyatakan dengan sebuah vektor kolom  $x$  berdimensi  $p$ , dengan  $p$  adalah 52, yaitu jumlah pola model yang ada. Bentuk dalam matriks:

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{52} \end{pmatrix}$$

Dengan elemen-elemen  $x_1$ -  $x_{52}$  adalah frekuensi kemunculan dari masing-masing model sesuai dengan nomor modelnya.

Untuk melakukan pendaftaran tanda tangan, maka setiap pengguna terlebih dahulu harus memasukkan tanda tangan acuan sebanyak  $m$  kali, sehingga matriks vektor yang akan disimpan dalam basis data acuan adalah matriks vektor yang berukuran  $p \times m$  sebagai berikut:

$$x = \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1m} \\ \vdots & \vdots & \ddots & \vdots \\ x_{p1} & x_{p2} & \dots & x_{pm} \end{pmatrix}$$

Jika digunakan 6 buah tanda tangan setiap, maka ukuran matriks vektor acuan akan berukuran 52 x 6. Matriks vektor inilah yang akan disimpan dalam basis data acuan dan akan digunakan dalam proses perbandingan yang akan dilakukan.

## 7. Proses Perbandingan

Proses perbandingan adalah proses yang sangat terkait dengan hasil dari ekstraksi ciri, dan merupakan inti dari keseluruhan proses verifikasi, serta proses yang paling banyak melakukan perhitungan.

Pada basis data acuan yang ada yang berisi record berupa matriks vektor berdimensi  $p \times m$  ini selanjutnya dihitung rata-rata kemunculan setiap model dengan menjumlahkan elemen masing-masing baris kemudian dibagi dengan  $m$ . Persamaan yang digunakan

$$x'_i = \sum_{k=1}^m \frac{x_{ik}}{m}$$

Nilai nilai yang dihasilkan, yaitu  $x'_1, x'_2, \dots, x'_p$  dibentuk menjadi sebuah vektor kolom  $x'$  yang berdimensi  $p$  yang merupakan rata-rata acuan.

Setelah mendapatkan rata-rata acuan, lalu akan dicari sebuah matriks varian dari acuan dengan persamaan sebagai berikut:

$$V = \sum_{j=1}^m (x_j - x') (x_j - x')^t / m$$

- V = varian dari acuan, matriks kuadrat p x p
- M = banyaknya sampel acuan
- x<sub>j</sub> = vektor kolom acuan ke-j
- x' = vektor kolom rata-rata acuan
- t = transpos

Mencari frekuensi kemunculan masing-masing pola model pada citra tanda tangan yang akan dibandingkan sama halnya dengan mencari frekuensi kemunculan pada pola model acuan. Misalkan tanda tangan yang akan dibandingkan adalah Q, maka vektor kolom yang dihasilkan adalah x<sub>q</sub>.

Varian V, rata-rata acuan x' dan vektor kolom frekuensi kemunculan pola tanda tangan yang dibandingkan x<sub>q</sub>, dipergunakan untuk menghitung harga ketidaksamaan dengan persamaan sebagai berikut:

$$D(P_i, Q) = \sum_{k=1}^q \frac{(Z_{kQ} - Z_j^k)^2}{\lambda_k} + \sum_{k=q+1}^p \frac{(Z_{kQ} - Z_j^k)^2}{\lambda_q}$$

$$Z_{kQ} = 1_k^t x_Q$$

$$Z_j^k = 1_k^t x_j$$

D(P<sub>i</sub>, Q) : Nilai ketidaksamaan antara acuan P<sub>i</sub> dengan pembanding Q

Λ = Vektor kolom yang berisi nilai eigen dengan urutan menurun

1<sub>k</sub> = Vektor eigen yang berbentuk vektor kolom dengan urutan disesuaikan dengan nilai eigen yang berhubungan

X<sub>Q</sub> = Vektor kolom yang berisi frekuensi kemunculan pola model pada citra tanda tangan pembanding

- X' = Vektor kolom rata-rata acuan
- T = transpos
- P = dimensi vektor kolom
- Q = Suatu integer dengan syarat 1 < q < p. Konstanta q merupakan nomor pemotongan dari nilai eigen. Tujuan pemotongan adalah untuk menghindari pembagian dengan bilangan yang sangat kecil atau

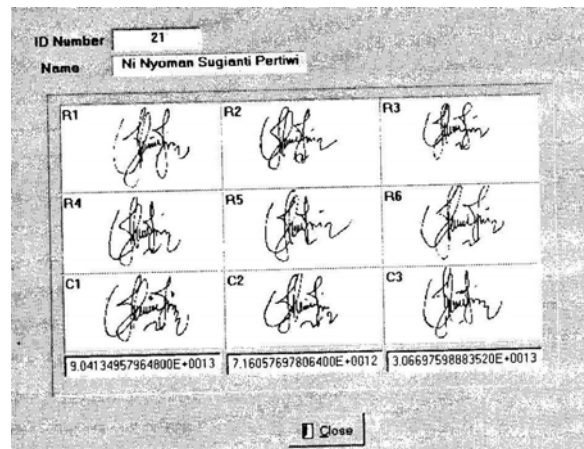
bahkan nol yang bisa menyebabkan kesalahan. Hal ini disebabkan nilai eigen pada batas nomor besar cenderung untuk bernilai sangat kecil bahkan mendekati nol.

Tahap selanjutnya adalah perancangan basis data acuan yang terdiri dari dua pokok penting, yaitu pendaftaran tanda tangan acuan dan penentuan nilai ambang batas yang akan disimpan dalam satu record dengan nomor identitas dari setiap pengguna sistem ini.

### 8. Pengambilan Keputusan

Pada tahap ini, maka akan diambil keputusan apakah tanda tangan yang diuji akan diterima atau ditolak. Nilai ketidaksamaan akan dibandingkan dengan nilai ambang yang telah tersimpan pada basis data acuan yang telah dikalikan dengan nilai kritis. Jika nilai ketidaksamaan kurang dari atau sama dengan nilai hasil kali ambang, maka tanda tangan dianggap asli. Sedangkan jika nilai ketidaksamaannya lebih besar, maka tanda tangan yang diuji tersebut dinyatakan palsu. Apabila d(P<sub>j</sub>, Q<sub>i</sub>) didefinisikan sebagai nilai ketidaksamaan antara tanda tangan acuan oleh partisipan P<sub>j</sub> dengan tanda tangan yang diuji Q<sub>i</sub>, maka berlaku hubungan seperti berikut ini:

d(P<sub>j</sub>, Q<sub>i</sub>) <= nilai ambang x nilai kritis, maka tanda tangan asli, selain itu palsu.



Gambar 7 Proses Verifikasi Citra Tanda Tangan Digital

### 9. Pemilihan Konstanta

1. Kontanta nilai kritis  
Efektivitas dan kerja metode verifikasi akan sangat berpengaruh dari nilai konstanta yang ditetapkan. Konstanta yang akan dipergunakan harus diuji coba terlebih dahulu dengan variasi-variasi yang

dianjurkan oleh pustaka. Konstanta yang mempengaruhi sistem verifikasi tanda tangan menggunakan metode pola busur terlokalisasi ada 2, yaitu:

- a. Konstanta pemotongan nilai eigen (q)  
 Pada perhitungan ketidaksamaan:

$$D(P_i, Q) = \sum_{k=1}^q \frac{(Z^{k_Q} - Z_i^k)^2}{\lambda k} + \sum_{k=q+1}^p \frac{(Z^{k_Q} - Z_i^k)^2}{\lambda q}$$

Terdapat sebuah konstanta yang nilainya ditentukan oleh hasil pengujian. Konstanta ini adalah konstanta pemotongan nilai eigen di mana q adalah bilangan integer yang kurang dari dimensi vektor kolom p.

Digunakan nilai yang dimulai dari 4 sampai pada akhirnya akan memberi pesan kesalahan karena terjadi pembagian dengan nol. Dari hasil pengujian terhadap variasi nilai q akan dipilih satu nilai yang mengakibatkan sistem mengalami kesalahan terkecil, dan akan digunakan sebagai konstanta pemotongan nilai eigen yang permanen dalam melakukan verifikasi.

- b. Konstanta Pengali nilai ambang  
 Konstanta ini merupakan koefisien pengali dari median nilai ketidaksamaan yang diperoleh saat verifikasi tiga tanda tangan pembandingan dengan tanda tangan acuan yang didaftarkan. Pengujian terhadap konstanta pengali nilai ambang dilakukan dari nilai 1,5; 2,0; 2,5; dan 3,0. Nilai ini dipakai agar nilai ambang yang dihasilkan tidak terlalu jauh menyimpang dari nilai C yang didapatkan. Jika konstanta pengali nilai ambang kurang dari 1,5 maka batas penerimaan akan sangat sempit sehingga persentase tidak diterimanya tanda tangan asli akan membesar.

## 10. Kesimpulan

- Verifikasi dengan menggunakan citra tanda tangan digital memiliki potensi untuk dapat digunakan secara luas, mengingat caranya yang semakin natural dan mendekati kenyataan pada kehidupan sehari-hari.
- Tingkat penerimaan dan verifikasi bahwa sebuah citra tanda tangan asli sangat bergantung pada pemilihan konstanta nilai

kritis eigen dan konstanta pengali nilai ambang.

## 11. Daftar Pustaka

- [1] Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.
- [2] Putra, Darma (2009). Sistem Biometrika. Penerbit ANDI, Yogyakarta.
- [3] Riha Z., Mathas V(2000). Biometric Authentication Systems. FI MU, Masaryk.