FUNGSI HASH BIOMETRIK SEBAGAI SISTEM KEAMANAN KARTU TANDA PENDUDUK

Irfan Afif (13507099)

Mahasiswa Program Studi Teknik Informatika
Institut Tenologi Bandung
Jl. Ganesha no. 10, Bandung
e-mail: irfan_afif@yahoo.com

Abstrak – Keamanan kartu tanda penduduk yang digunakan di Indonesia masih sangat kurang. Hal ini terbukti dengan adanya kasus-kasus penyalah gunaan kartu tanda penduduk seperti kepemilikian lebih dari satu kartu tanda penduduk ataupun penggunaan kartu tanda pemilik oleh pihak lain selain pemilik. Dari masalah itu tercetus sebuah solusi dengan memasukkan data biometrik pemilik kartu ke dalam kartu tanda penduduk. Data biometrik pemilik tersebut nantinya dapat disimpan dalam kartu tanda penduduk dengan berbagai macam cara. Salah sau cara yang mungkin adalah dengan menggunakan fungsi hash. Jadi, data biometrik yang didapat diubah menjadi message digest dengan fungsih hash, sehingga data biometrik disimpan dengan besar data yang sama. Pencocokan dilakukan dengan memasukkan data input yang telah diubah menjadi message digest dengan fungsi hash yang sama lalu dicocokkan dengan message digest pada kartu. Metode ini diharapkan dapat meningkatkan sistem kemanan kartu tanda penduduk.

Kata kunci: Fungsi hash, biometrik, kartu tanda penduduk, message digest

1. PENDAHULUAN

Identitas merupakan suatu hal yang sangat penting yang melekat pada diri seseorang. KTP (Kartu Identitas Penduduk) merupakan bukti identitas legal dari seseorang yang dikeluarkan oleh pemerintah. Jadi, pemerintah mengakui keberadaan dan kewarganegaraan melalui KTP ini. Siapapun yang memiliki KTP akan dianggap sebagai warga negara Indonesia dan mendapat perlakuan serta layanan dari pemerintah. Walaupun begitu, pada kenyataannya mudah untuk membuat ataupun memalsukan KTP. Salah satu hal yang mengkhawatirkan adalah adanya warga negara asing yang dengan mudah mendapat KTP dan menikmati hak sebagai warga negara Indonesia. Hal ini tentu saja sangat merugikan pemerintah.

KTP juga merupakan bukti identitas dari seseorang. Seseorang dinyatakan ada jika memiliki KTP. Hal yang membedakan satu otang dengan yang lain adalah informasi yang ada pada dirinya. KTP juga menyimpan informasi diri seseorang dan informasi diri itu diaggap sebagai informasi yang legal dan benar. Jadi saya dapat menjadi orang lain jika saya dapat memodifikasi informasi diri saya yang tercantum di dalam KTP yang saya miliki. Ha ini dapat dimanfaatkan oleh orang-orang yang ingin melakukan kejahatan. Salah satu contohnya adalah orang yang ingin menghindari pajak. Seseorang bisa saja membuat KTP ganda yang memiliki informasi berbeda dan membeli sebidang tanah dengan KTP yang menyimpan informasi tersebut. Oleh karena itu dia yang informasi dirinya dinyatakan dengan KTP lain dapat terhindar dari pajak.

Untuk dapat mengatasi haltersebut, diperlukan suatu sistem keamanan pada KTP. Saat ini pemerintah Indonesia sedang membuat suatu proyek untuk membuat e-KTP, yaitu KTP yang miliki chip di dalamnya. Dengan KTP yang memiiki chip ini, sistem keamanan pada KTP dapat ditingaktkan.

Salah satu cara untuk meningkatkan keamanan dari KTP adalah dengan menggunakan data biometrik pemilik. Data biometrik merupakan data yang berada di tubuh dan dapat diukur. Dengan, data biometrik ini, dapat ditentukan apakah pembawa ktp adalah pemiliknya ataupun apakah seseorangyang ingin membuat KTP telah memiikiKTP atau belum.

Untuk mengefisiensikan penyimpanan data di dalam chip kartu, kita dapat menggunakan fungsi hash. Data yang disimpan diubah menjadi suatu data yang berukuran sama dan berbeda untuk setiap masukan. Dengan cara ini, kita dapat mengefisiensikan ruang penyimpanan yang berada di chip tersebut.

2. LANDASAN TEORI

2.1 Fungsi Hash

Fungsi hash adalah sebuah fungsi matematik yang mengubah suatu data masukan yang memiliki panjang beragam menjadi suatu keluaran yang memiliki panjang data yang sama. Suatu fungsi hash berlaku sebagai berikut:

$$h = H(M)$$

Keluaran dari suatu fungsi hash disebut sebagai nilai hash atau message digest.

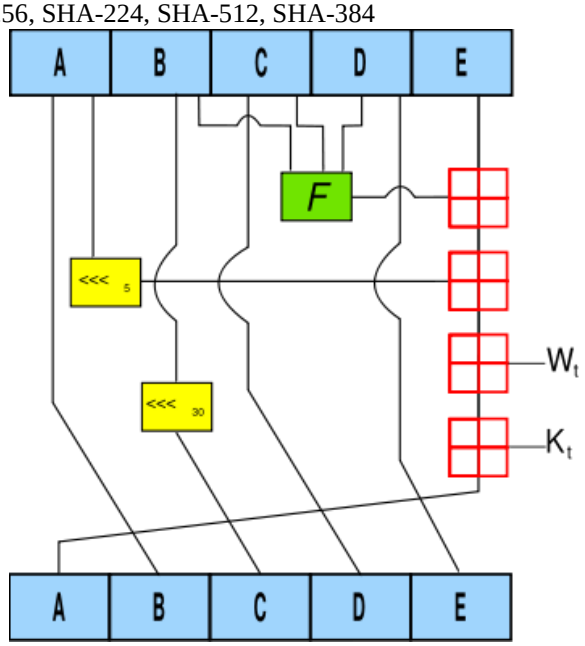
Fungsi hash dapat menghasilkan dua message digest yang sama dari dua masukan yang berbeda. Keunikan message digest yang dihasilkan juga merupakan factor penting dalam suatu fungsi hash dan hal ini masih terus menjadi bahan yang terus diteliti hingga sekarang.

Fungsi hash bersifat satu arah. Artinya kita dapat membentuk suatu message digest dari suatu masukan tetapi kita tidak dapat mendapatkan informasi masukan dari message digest. Hal ini dapat memberikan keuntungan dan kerugian. Keuntungannya adalah kita dapat menggunakan fungsi hash dengan aman tanpa harus merasa takut datanya diambil. Tetapi karena hal ini kita tidak dapat bertukar informasi dengan menggunakan fungsi hash. Oleh karena inilah fungsi hash sering digunakan sebagai pengecek keaslian suatu dokumen digital, bukan untuk bertukar data.

Fungsi hash banyak digunakan dalam penyimpanan data base karena menghasikan keluaran yang panjangnya sama sehingga mudah di simpan. Sebagai contoh adalah penyimpanan password, biasanya password disimpan dalam bentuk message digest. Hal ini memberikan keuntungan, yaitu kerahasiaan password tetap terjaga dan panyimpanan data menjadi mudah.

Diantaran fungsi hash, ada yang disebut sebagai fungsi hash kriptografi. Fungsi hash kriptografi memiliki nilai keamanan tambahan sehingga sering digunakan untuk keperluan ilmu kriptografi. Salah satu contoh kegunaan fungsi hash kriptografi adalah sebagai tanda tangan digital. Salah satu kelebihan fungsi hash kriptografi adalah message digest yang dihasilkan relative berbeda untuk data yang berbeda. Perubahan kecil pada masukan menyebabkan message digest yang dihasilkan juga ikut berubah, bahkan jauh dari message digest awal.

Amerika serikat memiliki lembaga yang mengeluarkan standar untuk fungsi hash yang bernama National Institute of Standards and Technology. Lembaga tersebut telah mengeluarkan lima standar algoritma fungsi hash, yaitu SHA-1 dan SHA-2 yang terdiri dari SAH-256, SHA-224, SHA-512, SHA-384



Gambar 1. Iterasi SHA - 1

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Max message size (bits)	Word size (bits)	Rounds	Operations	Collisions found
SHA-0		160	160	512	$2^{64} - 1$	32	80	+,and,or,xor,rot	Yes
SHA-1		160	160	512	$2^{64} - 1$	32	80	+,and,or,xor,rot	None (2^{52} attack)
SHA-2	*SHA-256/224*	256/224	256	512	$2^{64} - 1$	32	64	+,and,or,xor,shr,rot	None
	SHA-512/384	512/384	512	1024	$2^{128} - 1$	64	80	+,and,or,xor,shr,rot	None

tabel 1. Perbandingan Algoritma Hash yang dikeluarkan oleh National Institute of Standards and Technology

2.2 Biometric

Biometrik adalah suatu metode untuk mengenali mausia melalui fisik yang dimiliki orang tersebut ataupun perilaku yang ia miliki. Biometrik sering digunakan sebagai metode access control ataupun untuk mengenali identitas seseorang. Karakter biometrik terbagi menjadi dua, yaitu:

- Fisiologi, hal ini terkait dengan bentuk tubuh ataupun karakter lain yang terdapat di tubuhnya. Contohnya adalah sidik jari, pola retinadan dna.
- Segala sesudatu yang berhubungan dengan perilaku seseorang. Contohnya adalah kecepatan mengetik, ritme mengetik, dan suara.

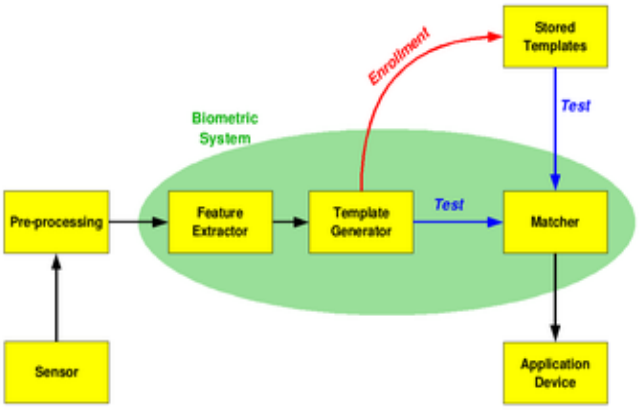
Biometrik dapat digunakan dengan dua cara, yaitu:

1. Verifikasi, membandingkan secara langsung untuk memastikan bahwa seseorang merupakan pemilik biometrik tersebut. Dengan cara ini kita dapat memastikan identitas seseorang.
2. Identifikasi, dengan cara membandingkan suatu biometrik dengan database biometrik yang kita miliki. Cara ini digunakan untuk menentukan siapa pemilik biometrik tersebut.

Ketika data biometrik seseorang diambil untuk pertama kali, maka pemilik data sedang melewati tahap yang disebut enrollment. Tahap ini sangatlah penting karena data yang diambil pada saat enrollment menjadi data yang nantinya akan dibandingkan dengan biometrik yang ingin digunakan. Pada tahap ini sistem harus mengambil semua data yang diperlukan.

Performansi suatu biometrik diukur dengan menggunakan istilah – istilah berikut:

- False accept rate or false match rate (FAR or FMR), merupakan kemungkinan sistem menerima masukan yang tidak valid.
- False reject rate or false non-match rate (FRR or FNMR), merupakan kemungkinan sistem menolak masukan yang valid.
- qual error rate or crossover error rate (EER or CER), merupakan rata-rata ketika jumlah FAR dan FRR sama.
- Failure to enroll rate (FTE or FER), kemungkinan sistem gagal membuat template data dari suatu enrolment.
- Failure to Capture Rate (FCR), kemungkinan sistem gagal mendeteksi biometric ketika diberikan inputan yang benar.
- Template capacity, jumlah maksimal template yang dapat dibuat sistem.



Gambar 2. diagram sistem biometrik

2.3 Smart Card

Smart card disebut juga sebagai chip card ataupun integrated circuit card.Smart card merupakan kartu yang berukuran kecil, besarnya kira-kira seperti kartu tanda penduduk dan dilengkapi dengan sirkuit terintegrasi (IC). Smart card dibagi menjadi dua jenis, yaitu:

1. Memory card, merupakan smart cardyang hanya memiliki memori yang bersifat tetap (volatile).
2. Microprocessor card, memiliki memori yang bersifat tidak tetap (non volatile) dan komponen lainnya. Smart card jenis ini biasanya terbuat dari polyvinyl chloride, kadang - kadang acrylonitrile butadiene styrene atau polycarbonate.

Smart card dapat digunakan untuk identifikasi, autentikasi, penyimpanan data atau pemrosesan aplikasi. Saat ini, smar card banyak digunakan. Contoh-contoh penggunaan smart card adalah:

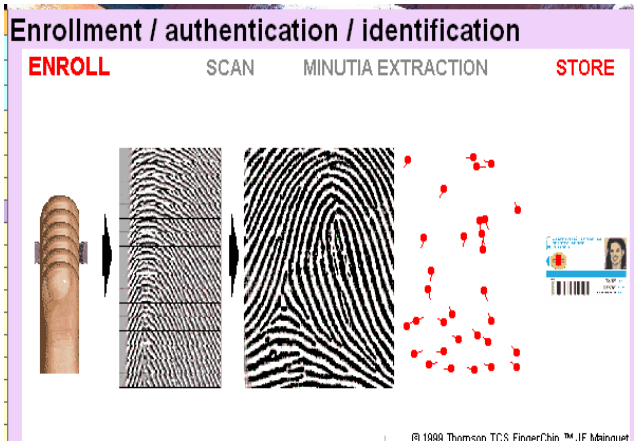
- Kartu SIM Card.
- Kartu credit.
- Kartu ATM.
- Kartu untuk membuka kunci ruangan.
- Kartu debet.
- Kartu telepon.

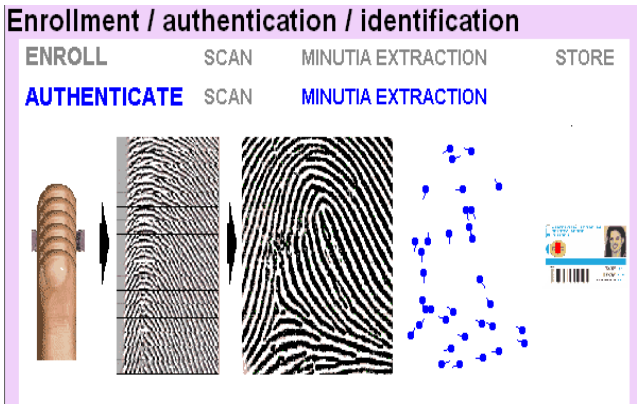
3. Pengujian Fungsi Hash Biometrik Sidik Jari

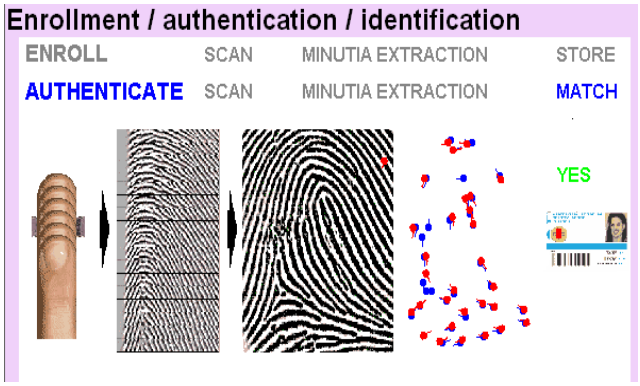
Pada bagian ini, akan dilakukan pengujian untuk menerapkan fungsi hash pada data biometrik sidik jari yang disimpan. Pengujian dilakukan menggunakan biometrik sidik jari. Hal ini dikarenakan biometrik sidik jari merupakan biometrik yang paling mudah digunakan. Sidik jari dapat digunakan sebagai biometrik karena sifatnya yang unit. Sidik jari setiap orang relatif berbeda. Ketika kulit telapak tangan mengalami luka, sidik jari tidak akan berubah jika kulit tidak mengalami cacat permanen.

Pengambilan gambar fingerprint untuk digunakan sebagai data biometrik merupakan tahapan yang dianggap paling penting. Di luar sana banyak pembaca sidk jari yang beredar. Pada prinsipnya, pengambilan sidik jari adalah membedakan bagian yang menonol dan cekungan yang berada pada jari.

Ketika pola gambar sidik jari didapatkan pada enrollment, maka akan dibuat template untuk menyimpan data. Data tersebut biasanya disimpan dalam bentuk gambar ataupun vector dan titik perubahan lekukan pada pola sidik jari. Berikut adalah proses pengambilan dan pencocokan sidik jari:







Gambar 4. Proses penggunaan pola sidik jari

Berikut adalah penjelasan dari gambar tersebut:

1. Gambar pertama merupakan enrollment. Sidik jari di ambil datanya, lalu diubah menjadi titik-titik berarah (template). Titik-titik berarah tersebut merupakan lekukan pada sidik jari. Setelah template selesai dibuat, template dimasukkan ke dalam chip.
2. Ketika ingin memvalidasi kepemilikan kartu, seseorang memasukkan sidik jari. Hasil masukkan sidik jari tersebut diubah ke dalam bentuk titik berarah, kemudian hasilnya tersebut dicocokkan dengan template yang berada di dalam kartu.
3. Terjadi pencocokan pola sidik jari. Pola template diputar beberpa kali untuk mengecek kesamaan pola sidik jari.

3.1 Pengujian Fungsi Hash SHA-1 pada pola sidik jari

Untuk pengujian kali ini dilakukan dengan membuat japlet dalam bahasa java dengan menggunakan Netbeans. Asumsi yang digunakan adalah format data yang digunakan untuk menyimpan pola sidik jari berupa gambar yang nantinya dapat dicocokkan.

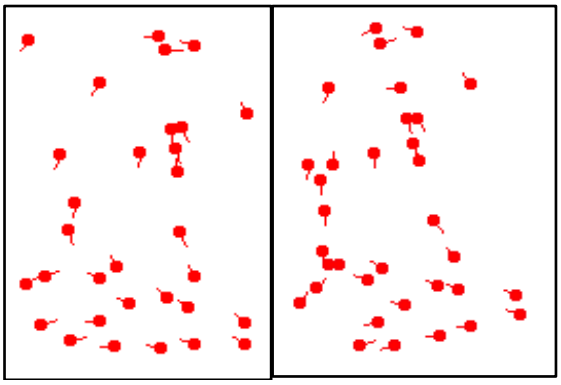
Algoritma fungsi hash yang digunakan adalah algoritma SHA1. SHA1 merupakan salah satu algoritma hash yang dikeluarkan oleh National Institute of Standards and Technology.

Berikut adalah algoritma SHA1 yang digunakan:

```
Initialize variables:
h0 = 0x67452301
h1 = 0xEFCDAB89
h2 = 0x98BADCFE
h3 = 0x10325476
h4 = 0xC3D2E1F0

Pre-processing:
append the bit '1' to the message
```

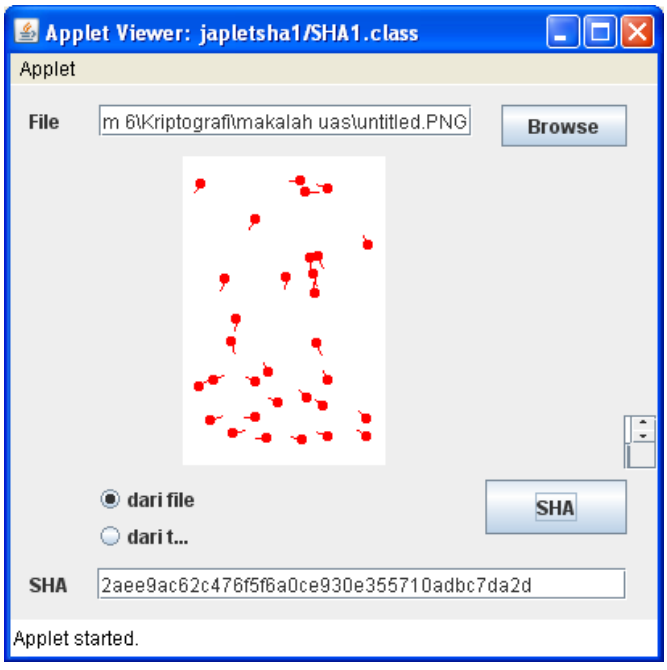
```
append 0 ≤ k < 512 bits '0', so that
the resulting message length (in bits)
   is congruent to 448 ≡ −64 (mod 512)
append length of message (before pre-
processing), in bits, as 64-bit big-
endian integer

Process the message in successive 512-
bit chunks:
break message into 512-bit chunks
for each chunk
    break chunk into sixteen 32-bit
big-endian words w[i], 0 ≤ i ≤ 15

    Extend the sixteen 32-bit words
into eighty 32-bit words:
    for i from 16 to 79
        w[i] = (w[i-3] xor w[i-8] xor
w[i-14] xor w[i-16]) leftrotate 1

    Initialize hash value for this
chunk:
    a = h0
    b = h1
    c = h2
    d = h3
    e = h4

    Main loop:
    [25]
    for i from 0 to 79
        if 0 ≤ i ≤ 19 then
            f = (b and c) or ((not b)
and d)
            k = 0x5A827999
        else if 20 ≤ i ≤ 39
            f = b xor c xor d
            k = 0x6ED9EBA1
        else if 40 ≤ i ≤ 59
            f = (b and c) or (b and d)
or (c and d)
            k = 0x8F1BBCDC
        else if 60 ≤ i ≤ 79
            f = b xor c xor d
            k = 0xCA62C1D6

        temp = (a leftrotate 5) + f + e
+ k + w[i]
        e = d
        d = c
        c = b leftrotate 30
        b = a
        a = temp

    Add this chunk's hash to result so
far:
    h0 = h0 + a
    h1 = h1 + b
    h2 = h2 + c
    h3 = h3 + d
    h4 = h4 + e

Produce the final hash value (big-
endian):
digest = hash = h0 append h1 append h2
append h3 append h4
```

Program menerima masukan gambar pola sidik jari dan mengeluarkan message digest. Data masukan yang digunakan adalah dua pola sidik jari yang sama, tetapi berbeda waktu inputnya. Hal ini menghasilkan pola yang sedikit berbeda. Berikut adalah masukan yang akan digunakan:



Gambar 5. Masukan data pengujian

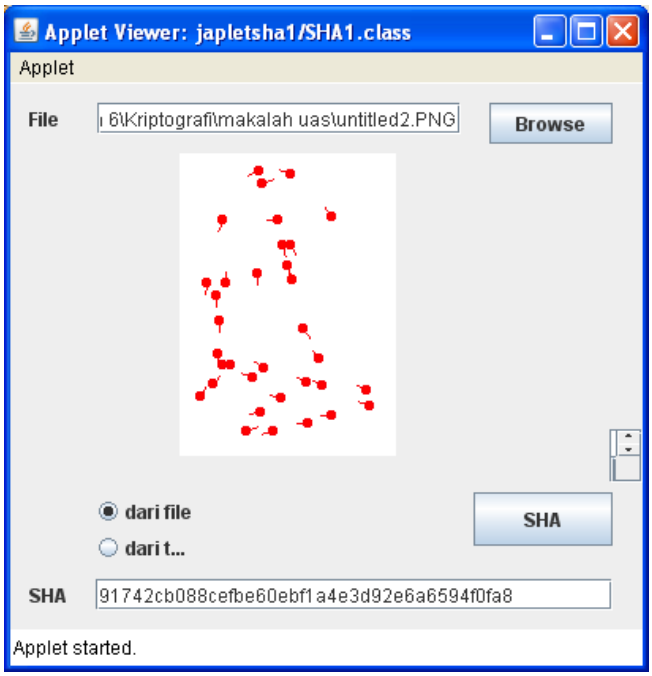
Berikut adalah cuplikan gambar dari program tersebut.



Gambar 6. cuplikan gambar program masukan pertama

Keluaran program:

MD : 2aee9ac62c476f5f6a0ce930e355710adbc7da2d



Gambar 6. cuplikan gambar program masukan kedua

Keluaran program:

MD : 91742cb088cefbe60ebf1a4e3d92e6a6594f0fa8

Message digest yang dihasilkan dari program ini yang nantinya akan disimpan dalam kartu tanda penduduk.

4. Analisis

Berikut adalah analisis penulis dalam penggunaan fungsih hash untuk menyimpan data biometrik.

Keuntungan:

- Besar ruang penyimpanan yang dibutuhkan jauh lebih kecil. Sebagai perbandingan, penyimpanan dalam bentuk gambar menghabiskan ruang 2 kilo byte sedangkan dengan message digest membuthkan ruang 40 karakter. Jika satu karakter menghabiskan 1 byte, maka ruang yang dibutuhkan hanya sekitar 40 byte.

Kekurangan:

- Membutuhkan waktu komputasi yang lebih lama.Walaupun dengan teknologi sekarang fungsi hash tersebut relatif cepat untuk diselesaikan.

Permasalahan:

- Permasalahn muncul ketika data biometrik akan digunakan. Pencocokan pola dilakukan dengan mencocokkan gambar. Keuntungan dengan pencocokkan gambar adalah gambar dapat menangani kesalahan sampai galat tertentu. Hal ini sangat penting karena pemasukan data pola sidik jari tidak selalu sama. Selain itu jika ada pergeseran aaupun sedikit rotasi, gambar dapat menyesuaikan keadaan ini. Sedangkan pada message digest, bersifat satu arah sehingga data gambar tidak dapat diambil kembali. Selain itu fungsi hash SHA 1 akan mengalami perubahan besar walaupun data mengalami perubahan sedikit saja. Hal ini menyebabkan pencocokan dengan data menjadi mustahil, karena input yang diterima relatif sedikit berbeda.

5. Kesimpulan

Berdasarkan hasil pencarian data dan analisis mengenai pemanfaatan fungsi hash biometrik sebagai sistem keamanan kartu tanda penduduk, didapatkan kesimpulan sebagai berikut:

1. Data biometrik dapat digunakan untuk sistem keamanan pada kartu tanda penduduk karena mampu memverifikasi dan mengidentifikasi pemilik kartu tanda penduduk.
2. Algoritma SHA1 menghasilkan message digest yang berbeda dengan maukan yang berbeda walaupun perbedaannya hanya sedikit.
3. Fungsi hash tidak dapat digunakan untuk menyimpan data biometrik pada kartu tanda penduduk. Penggunaan fungsi hash membuat data biometrik tidak dapat dibandingkan atau dicocokkan.

DAFTAR PUSTAKA

[1] Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

[2] http://pagesperso-orange.fr/fingerchip/biometrics/identify.htm
Waktu akses: 15 Mei 2010 pukul 08.18

[3] http://en.wikipedia.org/wiki/SHA-1
Waktu akses: 16 Mei 2010 pukul 13.18

[4] http://en.wikipedia.org/wiki/Biometrics
Waktu akses: 16 Mei 2010 pukul 13.30

Surat Pernyataan

Saya yang bertanda tanda tangan dibawah ini menyatakan bahwa makalah yang saya buat ini tidak mengandung unsur plagiasi

Irfan Afif
13507099