ANALISA ALGORITMA SISTEM KEAMANAN KOMPUTER MENGGUNAKAN SIDIK JARI DENGAN METODE POIN MINUTIAE PADA HP COMPACT 2210B NOTEBOOK PC

ABSTRAK

Salah satu sistem keamanan komputer yang sedang menjadi kebutuhan masyarakat adalah sistem keamanan komputer dengan menggunakan sidik jari. Teknologi ini dapat dibilang cukup untuk melindungi informasi yang penting, karena setiap manusia memiliki sidik jari yang berbeda-beda / unik. Penggunaan identifikasi seseorang menggunakan sidik jari pada fingerprint reading, retina mata pada retina scan, dan lainnya tidak lain adalah untuk menjaga keamanan suatu tempat atau benda. Penggunaan anggota tubuh sebagai input untuk identifikasi seseorang dalam keamanan disebut penggunaan sistem biometric. Keluaran dari sistem pencitraan sidik jari adalah berupa sebuah image. Image ini tidak langsung digunakan sebagai kunci, namun dikonversi dulu menjadi sebuah graf berbobot yang masing-masing node-nya memiliki "berat" masing-masing. "Berat" inilah yang menurut rancangan pada makalah ini, digunakan sebagai kunci untuk enkripsi dan dekripsi.

Kata Kunci : Sidik, Jari, Keamanan, Biometrik

Dhian Sweetania

Jurusan Sistem Informasi
Universitas Gunadarma
Jl. Margonda Raya 100 Pondok Cina,
Depok 16424
dhian_sweetania@staff.gunadarma.ac.id

1. PENDAHULUAN

1.1. LATAR BELAKANG

Informasi sekarang ini merupakan suatu kebutuhan bagi masyarakat luas. Hal ini secara langsung dapat dilihat dari perilaku masyarakat yang selalu butuh akan informasi yang direalisasikan melalui berbagai hal seperti berlangganan koran, majalah, dan lain-lain. Dengan mudah masyarakat mendapatkan informasi karena informasi berkembang dengan sangat pesat mengikuti perkembangan dunia. Sama halnya dengan teknologi, informasi berkembang seraya mengikuti perkembangan teknologi. Perkembangan informasi membuat informasi itu menjadi hal yang sangat penting dan membutuhkan keamanan untuk melindungi informasi.

Dalam perkembangannya bukan hanya informasi yang menjadi penting, tetapi perkembangan teknologi pun menjadi hal yang sangat penting khususnya teknologi keamanan komputer. Sebagai contoh, sekarang ini manusia berlomba-lomba membangun sebuah sistem untuk melindungi informasi yang mereka miliki dari ancaman virus ataupun orang lain yang berusaha untuk mengambil, memanipulasi ataupun hanya untuk sekedar merusak informasi itu.

Perkembangan teknologi keamanan komputer yang menjadi kuncinya sudah marak diperbincangkan, bahkan teknologi keamanan komputer dapat menjadi suatu peluang usaha bagi programmer yang dapat menciptakan suatu sistem untuk memproteksi suatu data atau informasi dari ancaman virus atau orang lain seperti membuat anti virus maupun suatu proteksi yang ditanamkan di suatu perangkat yang dapat menyimpan informasi seperti notebook dan PC. Salah satu sistem keamanan komputer yang sedang menjadi kebutuhan masyarakat adalah sistem keamanan komputer dengan menggunakan sidik jari. Teknologi ini dapat dibilang cukup untuk melindungi informasi yang penting, karena setiap manusia memiliki sidik jari yang berbeda-beda / unik.

Salah satu perusahaan notebook yang sudah menanamkan suatu sistem keamanan komputer dengan menggunakan sidik jari di dalam produknya adalah HP COMPAQ 2210B NOTEBOOK PC. Dengan ini penulis akan menganalisa bagai mana algoritma dan metode bekerjanya sistem keamanan sidik jari yang berada pada HP COMPAQ 2210B NOTEBOOK PC.

1.2. BATASAN MASALAH

Dalam jurnal ini membahas sebatas perkembangan teknologi sidik jari sebagai alat untuk melindungi atau memproteksi data dan informasi serta metode dan algoritma sistem yang ada dalam teknologi sidik jari yang menggunakan metode kriptografi di dalam HP Compaq 2210b Notebook PC.

1.3. TUJUAN

Tujuan dari jurnal ini adalah untuk menganalisa metode yang digunakan dalam sistem keamanan yang menggunakan sidik jari serta memberikan solusi dalam memilih alat untuk melindungi dan memproteksi data dan informasi penting.

1.4. METODE PENULISAN

Metode penulisan yang digunakan oleh penulis adalah :

1. Merancang algoritma system enkripsi dekripsi biometrika
2. Melakukan proses verifikasi citra sidik jari dengan ekstrasi poin minutiae
3. Penulis juga melakukan penganalisaan terhadap kinerja sistem sidik jari yang berada pada HP Compaq 2210b Notebook PC.

2. TINJAUAN PUSTAKA

2.1. SISTEM BIOMETRIK

Penggunaan identifikasi seseorang menggunakan sidik jari pada *fingerprint reading*, retina mata pada *retina scan*, dan lainnya tidak lain adalah untuk menjaga keamanan suatu tempat atau benda. Penggunaan anggota tubuh sebagai input untuk identifikasi seseorang dalam keamanan disebut penggunaan sistem *biometric*.

Sistem *biometric* adalah studi tentang metode otomatis untuk mengenali manusia berdasarkan satu atau lebih bagian tubuh manusia atau kelakuan dari manusia itu sendiri yang meiliki keunikan. Tujuan utama dari penggunaan sistem *biometric* adalah untuk menjaga keaslian keunikan kunci, karena hampir tidak mungkin pembacaan input sidik jari atau retina orang yang berbeda menghasilkan hasil pembacaan yang sama.

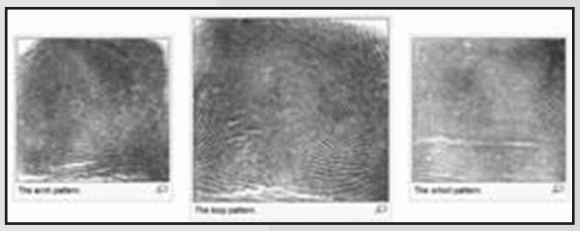
Gambar 1. fingerprint reader

Gambar 2. retina scanner

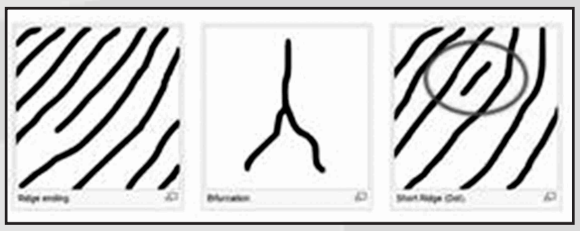
Penggunaan sistem *biometric* memungkinkan keunikan untuk menjaga keamanan suatu tempat atau benda. Hal inilah yang menimbulkan gagasan untuk menggabungkan sistem *biometric* dan salah satu algoritma kriptografi, yang dibahas pada jurnal ini adalah algoritma kriptografi klasik.

Pada jurnal ini, pembahasan yang dilakukan dibatasi pada biometrika sidik jari, sehingga perangkat keras yang digunakan adalah *fingerprint reader*, metode yang digunakanpun sesuai dengan hasil pembacaan biometrika sidik jari.

Prinsip pemprosesan pencitraan sidik jari menggunakan *fingerprint reader* tergolong rumit, namun sudah banyaknya perangkat keras yang digunakan membuat *constraint* tersebut menjadi kabur. Prinsip-prinsip pencitraan tersebut diantara lain adalah *pattern based* dan *minutiae based*. Pada pattern based fingerprint recognition, pola sidik jari dikelompokkan menjadi 3, yaitu arch, loop dan whorl. Sedangkan pada minutiae based juga terdapat 3 klasifikasi pola yaitu ridge ending, bifurfication, dan dot(short ridge).



Gambar 3 klasifikasi pattern based



Gambar 4 klasifikasi minutiae based

Selain prinsip yang digunakan untuk klasifikasi pola di atas, terdapat juga berbagai sistem sebagai sensor fingerprint. Sistem-sistem sensor fingertpint tersebut antara lain optical, ultrasonic dan capacitance sensors.

Pada sensor optical, pencitraan sebuah sidik jari didasarkan pada pembacaan sidik jari menggunakan "sinar terlihat". Cara kerjanya bisa dianalogikan seperti sebuah digital camera yang menangkap gambar melalui sensor. Namun sensor pada sistem optical ini memiliki beberapa layer(tidak akan dibahas lebih lanjut).

Pada sensor ultrasonic, prinsip kerja yang digunakan sama seperti prinsip kerja ultrasonography pada dunia kedokteran, menggunakan gelombang suara frekuensi tinggi untuk pencitraan lapisan epidermal kulit.

Pada sensor capacitance, pencitraan sidik jari didasarkan pada kapasitansi lapisan sidik jari. Lapisan dermal yang bersifat konduktif dan lapisan epidermal yang bersifat non-konduktif memberikan perbedaan untuk dicitrakan pada sistem sensor ini.

$$C = \frac{Q}{V}$$

$$C = \varepsilon_0 \varepsilon_r \frac{A}{d}$$

Pada jurnal ini permasalahan sistem tersebut tidak akan dibahas terlalu dalam melihat pokok pembahasan dari jurnal ini adalah pembangkitkan kunci dari sebuah sistem biometrika, yang dalam hal ini adalah sidik jari. Pada jurnal ini sistem sensor yang digunakan tidak dispesifikkan, namun keluaran dari sistem biometrika tersebut adalah berupa sebuah *image* seperti pada gambar 3. Gambar ini bisa berbentuk format lain namun intinya adalah sebuah image yang merepresentasikan sidik jari orang.

2.1. TEKNIK KRIPTOGRAFI

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematis yang berhubungan dengan aspek keamanan informasi seperti : keabsahan, integritas data, serta autentifikasi data. Kriptografi tidak berarti hanya memberikan keamanan informasi saja, namun lebih ke arah teknik-tekniknya. Ada empat tujuan dari ilmu kriptografi, yaitu :

- privacy, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas
- integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain menyangkut penyisipan, penghapusan, dan pensubtitusian data lain ke dalam data yang sebenarnya
- autentikasi, adalah berhubungan dengan identifikasi, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain
- non-repudiasi, yang berarti begitu pesan terkirim, maka tidak akan dapat dibatalkan.

2.2.1. ENKRIPSI

Proses utama dalam suatu algoritma kriptografi adalah enkripsi dan dekripsi. Enkripsi merubah sebuah plaintext ke dalam bentuk ciphertext. Pada mode ECB (Elekctronic Codebook), sebuah blok pada plaintext dienkripsi ke dalam sebuah blok ciphertext dengan panjang blok yang sama.

Blok cipher memiliki sifat bahwa setiap blok harus memiliki panjang yang sama (misalnya 128 bit). Namun apabila pesan yang dienkripsi memiliki panjang blok terakhir tidak tepat 128 bit, maka diperlukan mekanisme padding, yaitu penambahan bit-bit dummies untuk menggenapi menjadi panjang blok yang sesuai; biasanya padding dilakukan pada blok terakhir plaintext.

Padding bada blok terakhir bisa dilakukan dengan berbagai macam cara, misalnya dengan penambahan bit-bit tertentu. Salah satu contoh penerapan padding dengan cara menambahkan jumlah total padding sebagai byte terakhir pada blok terakhir plaintext. Misalnya panjang blok adalah 128 bit (16 byte) dan pada blok terakhir terdiri dari 88 bit (11 byte) sehingga jumlah padding yang diperlukan adalah 5 byte, yaitu dengan menambahkan angka nol sebanyak 4 byte, kemudian menambahkan angka 5 sebanyak satu byte. Cara lain dapat juga menggunakan penambahan karakter end-of-file pada byte terakhir lalu diberi padding setelahnya.

2.2.2. DEKRIPSI

Dekripsi merupakan proses kebalikan dari proses enkripsi, merubah ciphertext kembali ke dalam bentuk plaintext. Untuk menghilangkan padding yang diberikan pada saat prpses enkripsi, dilakukan berdasarkan informasi jumlah padding yaitu angka pada byte terakhir.

>> Dasar Matematis

Dasar matematis yang mendasari proses enkripsi dan deskripsi adalah relasi antara dua himpunan yaitu yang berisi elemen plaintext dan yang berisi elemen cipertext. Enkripsi dan dekripsi merupakan fungsi transformasi antara himpunan-himpunan tersebut. Apabila elemen-elemen plaintext dinotasikan dengan P, elemen-elemen ciphertext dinotasikan dengan C, sedang untuk proses enkripsi dinotasikan dengan E, dekripsi dengan notasi D, maka secara matematis proses kriptografi dapat dinyatakan sebagai berikut :

Enkripsi : E(P)=C
Dekripsi : D(C)=P atau D(E(P))=P

Pada skema enkripsi konvensional atau kunci simetrik digunakan sebuah kunci untuk melakukan proses enkripsi dan dekripsinya. Kunci tersebut dinotasikan dengan K, sehingga proses kriptografinya adalah :

Enkripsi : EK(P)=C
Dekripsi : DK(C)=P atau DK(EK(P))=P

Sedangkan pada sistem asymmetric-key digunakan kunci umum (public key) untuk enkripsi dan kunci pribadi (private key) untuk proses dekripsinya sehingga kedua proses tersebut dapat dinyatakan sebagai berikut :

Enkripsi : EPK(P)=C
Dekripsi :DSK(C)=P atau DSK(EPK(P))=P

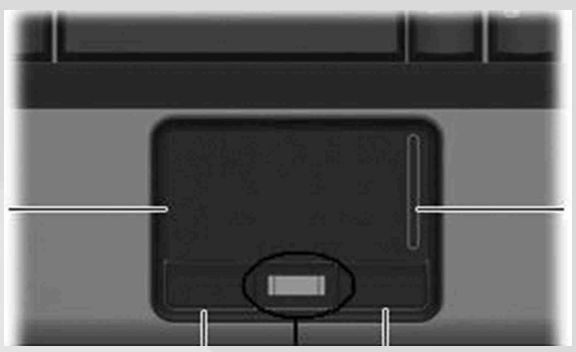
1. PEMBAHASAN

3.1. SEKILAS TENTANG KEAMANAN

HP adalah salah satu perusahaan teknologi informasi terbesar dunia. Hewlett-Packard dibangun oleh dua orang yang bernama Bill Hewlett dan Dave Packard. Bermarkas besar di Palo Alto,

California, Amerika Serikat, perusahaan ini memiliki keberadaan global dalam bidang komputerisasi, percetakan, dan gambaran digital, dan juga menjual perangkat lunak dan pelayanan jasa lainnya.

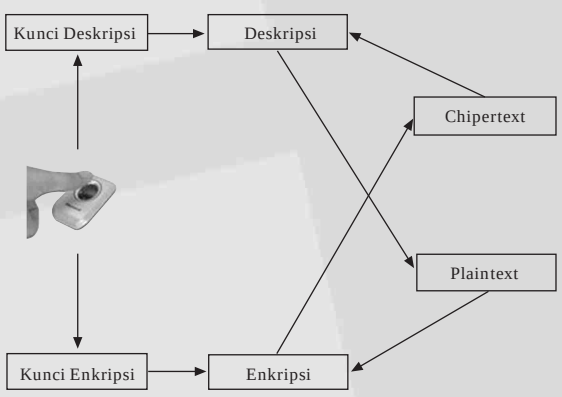
Salah satu produk dari HP adalah HP Compaq 2210b Notebook PC. Di dalamnya terdapat salah satu sistem keamanan computer yaitu sistem keamanan dengan menggunakan sidik jari. Plat tempat memindai sidik jari berada di antara touchpad button dan berfungsi untuk masuk ke dalam windows, tetapi plat sidik jari berbeda dengan password, karena pengguna dapat menggunakan password juga untuk masuk ke dalam windows.



Plat Sidik Jari

Gambar 5. Plat Sidik Jari

3.1. RANCANGAN SISTEM



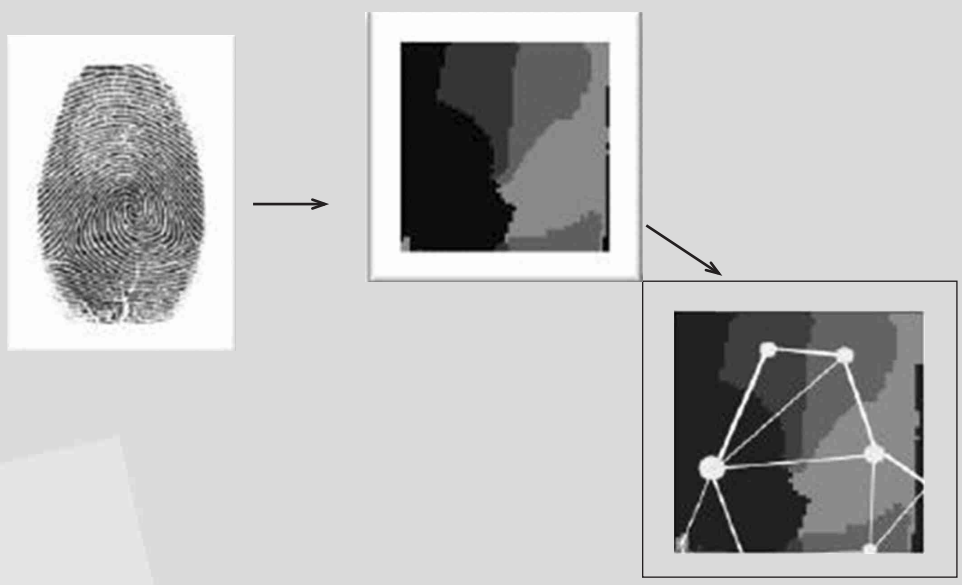
Gambar 6. Rancangan Sistem

Pada gambar di atas, diperlihatkan rancangan sistem enkripsi dan dekripsi menggunakan sistem biometrika. Pembacaan dari perangkat keras sistem biometrika yang unik untuk tiap orang akan menghasilkan satu kunci yang unik pula. Kunci ini akan dikonversi sedemikian hingga menghasilkan sebuah kunci untuk melakukan enkripsi plainteks menjadi cipherteks. Untuk proses dekripsipun juga demikian, kunci unik yang diperoleh dari pembacaan sistem biometrika digunakan sebagai kunci untuk dekripsi cipherteks menjadi plainteks.

Jika dilihat dari cara kerja sistem ini, perubahan kunci yang dibaca dari sistem biometrika tersebut menjadi sebuah string atau bentuk lain adalah sama dengan algoritma enkripsi dan dekripsi biasa. Misalnya enkripsi vigenere cipher menggunakan kunci “apple”, kunci ini dapat dicari menggunakan analisis frekuensi dan teknik lainnya. Pembacaan unik dari sistem biometrika ini juga akan dikonversi menjadi bentuk string pula, namun tidak berbentuk kata-kata yang sering ditemui, bentuknya akan berupa hasil konversi bit-bit dari ascii yang dibaca dari garis-garis sidik jari. Misalnya, hasil pembacaan sistem biometrika tidak berupa kata-kata namun berbentuk abstrak atau bentuk lain yang sulit dipahami dan dilihat *pattern*-nya.

3.1. ALGORITMA SISTEM ENKRIPSI DAN DEKRIPSI

Keluaran dari sistem pencitraan sidik jari adalah berupa sebuah *image*. *Image* ini tidak langsung digunakan sebagai kunci(misalnya dengan dikonversi ke dalam bentuk string, karena sangat sulit untuk menghasilkan hasil pembacaan yang sama), namun dikonversi dulu menjadi sebuah graf berbobot yang masing-masing *node*-nya memiliki “berat” masing-masing. “Berat” inilah yang menurut rancangan pada makalah ini, digunakan sebagai kunci untuk enkripsi dan dekripsi.



Gambar 6 proses konversi dari pencitraan sidik jari ke graf berbobot

Pada gambar 6 diperlihatkan proses konversi sebuah citra sidik jari menjadi sebuah graf berbobot dengan “berat” node yang berbeda-beda. Graf berbobot didefinisikan sebagai G= (V, E, μ, U) dengan V adalah jumlah nodes, E adalah jumlah sisi, μ adalah berat node, dan U adalah berat sisi.

Penentuan berat sisi dan nodes sendiri adalah berdasarkan beberapa parameter seperti titik tengah gravitasi untuk masing-masing region, jarak antar 2 titik tengah gravitasi, garis batas tiap region, dan lainnya.

$$Wn = Area(Ri)\ ,\ i = 1, 2, 3, ..., n$$

Persamaan di atas menunjukkan rumus untuk mencari sebuah berat dari node dengan menggunakan parameter-parameter yang telah disebutkan di atas. Berat tiap region ini yang akan digunakan untuk membuat sebuah kunci.

Dapat juga digunakan berat sebuah sisi untuk menentukan kunci, parameter yang digunakan adalah :

- Adj-P adalah batas antara 2 region yang bersinggungan atau saling bertetangga
- Node-d adalah jarak antarnodes yang dihubungkan oleh sebuah sisi
- Diff-v adalah perbedaan direction dari dua region

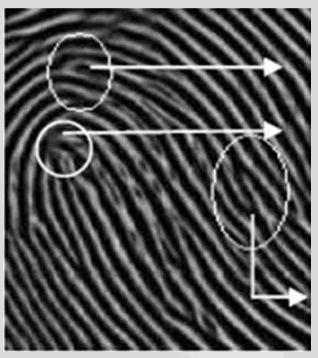
Dari parameter diatas, dibuat persamaan untuk sebuah sisi adalah

$$We = Adj\text{-}p \times Node\text{-}d \times Diff - v$$

Untuk detail penurunan kedua persamaan tidak akan dibahas pada makalah ini. Namun disinilah proses pembuatan kunci unik yang didapat dari sistem biometrika yang digunakan. Himpunan solusi salah satu dari 2 persamaan tersebut digunakan untuk membuat kunci enkripsi dan dekripsi.

3.4 VERIFIKASI CITRA SIDIK JARI DENGAN METODE POIN MINUTIAE

Poin Minutiae adalah sejenis titik yang terbentuk pada sidik jari. Ada beberapa jenis minutiae atau dapat juga disebut dengan ridge, antara lain ridge ending (akhir), ridge crossing (persilangan), dan fitur kecil yang terbentuk dari pecabangan ridge pada sidik jari disebut ridge birfurcation. Pada gambar 7 ditunjukan bentuk dari minutiae sidik jari.



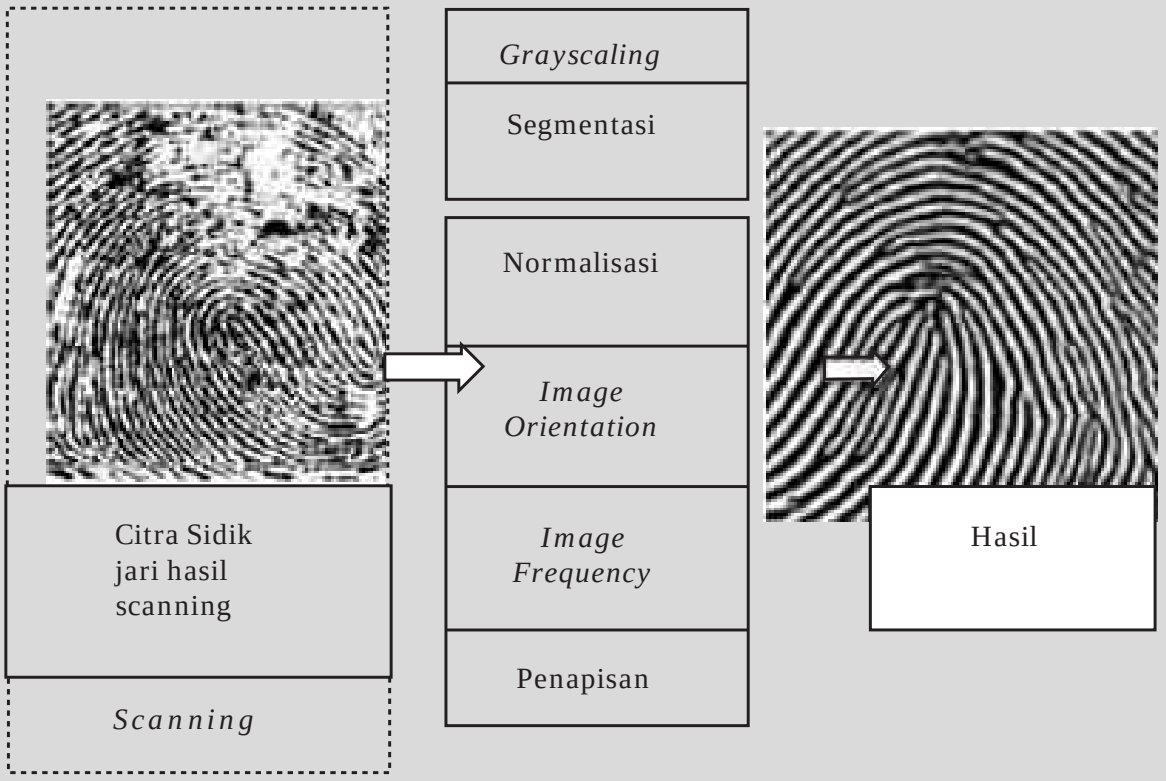
Gambar 7. Ridge Sidik Jari

3.4.1. Proses Verifikasi

Verifikasi merupakan proses pencocokan sejenis dengan identifikasi hanya saja pada proses verifikasi, sidik jari dicocokan satu-satu dimana setiap sidik jari masukkan diperbandingkan dengan satu template sidik jari tertentu yang tersimpan sebelumnya. Keluaran dari program ini adalah apakah proses verifikasi berhasil atau gagal.

3.4.2 Perbaikan Citra

Tahap pertama adalah pemprosesan citra sidik jari. Pada tahap ini citra sidik jari hasil scanning akan ditingkatkan kualitasnya melalui beberapa proses.



Gambar 8. Proses Perbaikan Citra

Proses grayscaling dilakukan dengan mengkonversi citra warna menjadi citra hitam putih dengan merata-rata nilai ketiga elemen warna setiap pixel. Segmentasi merupakan proses untuk memisahkan obyek pada suatu citra dari daerah latar belakangnya. Setelah itu citra yang disegmentasi dinormalisasi dengan menstandarisasi nilai intensitas suatu citra dengan menyesuaikan cakupan derajat keabuan sehingga berada pada cakupan nilai yang diharapkan. Proses Image Orientation and Image Frequency digunakan untuk proses penapisan citra sidik jari. Penapisan yang digunakan adlah penapisan gabor.

$$G(x,y;\theta,f) = \exp\left\{-\frac{1}{2}\left[\frac{x_\theta^2}{\sigma_x^2} + \frac{y_\theta^2}{\sigma_y^2}\right]\right\}\cos(2\pi f x_\theta)$$

Dimana:

$$x_\theta = x\cos\theta + y\sin\theta,$$
$$y_\theta = -x\sin\theta + y\cos\theta,$$

$$E(i,j) = \sum_{u=\frac{-w_x}{2}}^{\frac{w_x}{2}} \sum_{u=\frac{-w_y}{2}}^{\frac{w_y}{2}} G(u,v;\theta(i,j)\,F(i,j))\,N(i-u,j-v)$$

3.4.3. Ekstrasi Minutiae

Ada tiga tahap dalam Image Extraction ini, diantaranya adalah : Binerisasi, Penipisan pola dan deteksi minutiae. Konversi citra pada proses binerisasi dilakukan dengan operasi pengambangan sehingga didapatkan keberadaan obyek berupa alur guratan sidik jari. Penapisan pola bertujuan mengurangi bagian yang tidak perlu. Kemudian citra hasil penipisan dideteksi minutiae menggunakan metode crossing number. Poin minutiae dideteksi dengan memindai tetangga local pada masing-masing pixel ridge pada citra dengan menggunakan ukuran window 3 x 3. Kemudian nilai crossing number dihitung, yang didefinisikan sebagai separuh penjumlahan dari perbedaan antara pasangan-pasangan pixel yang bersebelahan pada eight-neightbourhood.

1. KESIMPULAN

Kesimpulan dari jurnal ini adalah, rancangan sistem enkripsi dan dekripsi menggunakan sistem biometrika. Pembacaan dari perangkat keras sistem biometrika yang unik untuk tiap orang akan menghasilkan satu kunci yang unik pula. Kunci ini akan dikonversi sedemikian hingga menghasilkan sebuah kunci untuk melakukan enkripsi plainteks menjadi cipherteks. Untuk proses dekripsipun juga demikian, kunci unik yang diperoleh dari pembacaan sistem biometrika digunakan sebagai kunci untuk dekripsi cipherteks menjadi plainteks.

Serta menggunakan sidik jari dapat memberikan solusi untuk melindungi dan memproteksi data dan informasi penting.

2. DAFTAR PUSTAKA

[1] http://www.informatika.org/~rinaldi/Kriptografi/2006-2007/Algoritma%20Kriptografi%20Klasik%20(bag%203).ppt , Oktober 2011

[2] http://www.informatika.org/~rinaldi/Kriptografi/2009-2010/kripto09-10.htm , Oktober 2011

[3] http://en.wikipedia.org/wiki/Biometrics, Oktober 2011

[4] James L.Wayman,"A Generalized Biometric Identification System Model", *IEEE*, 1998.

[5] Maintenance and Service Guide, HP Compaq 2210b Notebook PC, 2009.