Penerapan Steganografi Pada Autentikasi Biometrik

Muhammad Iqbal 13510064
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13510064@std.stei.itb.ac.id

***Abstract*— Autentikasi berbasis biometrik adalah teknik verifikasi identitas dengan menggunakan karakteristik fisik dari seseorang. Sistem biometrik memiliki risiko keamanan karena banyaknya variasi serangan yang mungkin seperti *Spoofing, Replay Attack,* dan lain-lain. Makalah ini akan membahas metoda berbasis steganografi untuk meningkatkan keamanan dan autensitas dari data itu sendiri.**

***Index Terms*—biometrik, steganografi, encoding, decoding**

I. PENDAHULUAN

Teknik autentikasi berbasis biometrik semakin popular digunakan jika dibandingkan dengan penggunaan autentikasi tradisional seperti kartu identitas, password, dan lain-lain. Salah satu keunggulan dari sistem autentikasi biometrik adalah kemampuan untuk membedakan antara pengguna yang sah dan pengguna palsu yang mencoba untuk mendapatkan hak akses dari pengguna sah tersebut.

Meskipun teknik autentikasi biometrik memiliki berbagai kelebihan dibandingkan teknik autentikasi tradisional, masalah yang muncul dari penjaminan keamanan dan integirtas data biometrik merupakan masalah yang vital. Sebagai contoh, jika data biometrik seseorang seperti gambar dari sidik jari yang tersimpan di database hilang, maka tidak bisa diganti tidak seperti mengganti kartu yang tercuri, lupa password, dan-lain-lain. Selain itu, meskipun data biometrik bersifat unik, namun data ini bukanlah data yang rahasia. Setiap orang meninggalkan sidik jari ketika ia menyentuh sesuatu. Dari sini, dapat muncul berbagai ancaman serangan yang mungkin dilakukan pada sistem, dimulai dari penggunaan sidik jari palsu pada sensor, *replay attack,* serangan yang ditujukan langsung pada template yang disimpan di database. Serangan-serangan ini memiliki kemungkinan untuk mengurangi kredibilitas dari sistem autentikasi biometrik.

Solusi dari masalah ini adalah selain template data biometrik yang ada, sebuah data yang bersifat rahasia juga disisipkan pada setiap data biometrik. Penggunaan teknik steganografi dalam teknik autentikasi biometrik ini dapat meningkatkan keamanan sistem, serta mencegah berbagai variasi ancaman yang mungkin terjadi. Jika kriptografi fokus pada enkripsi pesan menjadi sesuatu yang tidak berarti, maka steganografi fokus pada penyembunyian eksistensi pesan itu sendiri. Penyembunyian pesan ini sangat cocok digunakan untuk mengirimkan informasi biometrik dari *client* ke *server*. Penyisipan data ini mengurangi kemungkinan modifikasi illegal yang dilakukan terhadap data biometrik. Teknik enksipri data bisa diterapkan untuk melindungi data biometrik yang dikirimkan, sehingga data tidak bisa dimodifikasi jika tidak memiliki kunci yang benar. Namun masalah muncul ketika data ini sudah didekripsi untuk masalah autentikasi, data tidak lagi memiliki mekanisme keamanan yang melindunginya sehingga jika ada kemungkinan data dapat di-*intercept* maka enkripsi tidak menyediakan keamanan pada sistem secara keseluruhan. Sedangkan penyisipan data dengan steganografi yang tidak berhubungan dengan enkripsi dan dekripsi menyediakan keamanan sistem secara keseluruhan dan memberikan pertahanan lebih terhadap modifikasi ilegal.

II. DASAR TEORI

A. Steganografi

Steganografi berasal dari bahasa Yunani yaitu kata steganos yang artinya tulisan tersembunyi. Steganografi adalah ilmu dan seni menyembunyikan informasi dengan cara menyisipkan pesan rahasia di dalam pesan lain. Saat ini, steganografi banyak dilakukan pada data digital dengan menggunakan komputer digital, yang biasa disebut dengan steganografi digital. Steganografi mempunyai properti sebagai berikut:

1. Embedded message (hiddentext), yaitu pesan yang disembunyikan.
2. Cover object (covertext), yaitu pesan yang digunakan untuk menyembunyikan embedded message.
3. Stego object (stegotext), yaitu pesan yang sudah berisi pesan embedded message.
4. Stego key, yaitu kunci yang digunakan untuk menyisipkan pesan dan mengekstraksi pesan dari stegotext.

Proses steganografi secara umum dapat dilihat pada gambar berikut:

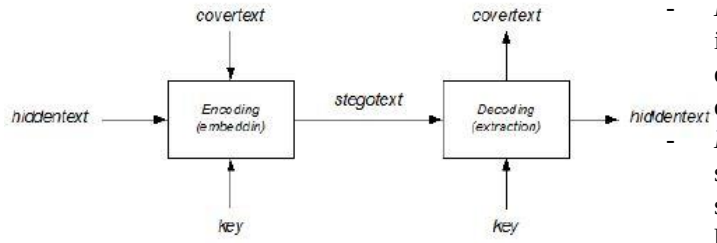

Figure 1 Proses Steganografi

Steganografi dapat dianggap pelengkap kriptografi. Steganografi menyembunyikan keberadaan pesan dengan tujuan untuk menghindari kecurigaan sedangkan kriptografi menyembunyikan isi pesan dengan tujuan agar pesan tidak dapat dibaca. Kriteria steganografi yang bagus adalah sebagai berikut:

1. Imperceptible, yaitu keberadaan pesan rahasia tidak dapat dipersepsi.
2. Fidelity, yaitu mutu cover object tidak jauh berubah akibat embedded.
3. Recovery, yaitu data yang disembunyikan harus dapat diungkapkan kembali.

B. Steganografi pada Citra Digital

Citra digital terdiri atas sejumlah pixel. Citra 200x150 berarti memiliki 200x150 pixel = 30000 pixel. Setiap pixel panjangnya n-bit. Contoh: citra 8 - bit, citra 24-bit, dsb. Nilai pada setiap pixel menyatakan derajat keabuan. Pada citra 24-bit (*real image*), 1 pixel = 24 bit, terdiri dari komponen RGB (Red-Green-Blue). Teknik yang digunakan :

- Spatial (time) domain
  Memodifikasi langsung nilai byte dari cover-object (nilai byte dapat merepresentasikan intensitas/warna pixel atau amplitudo) Memodifikasi langsung nilai byte dari cover object. Contoh: Metode modifikasi LSB
- Transform domain
  Memodifikasi hasil transformasi sinyal dalam ranah frekuensi. Contoh: Metode Spread Spectrum

Pada makalah kali ini teknik yang digunakan adalah spatial domain yaitu metode LSB. Metode LSB memanfaatkan indra visual manusia dalam mengamati perubahan sedikit pada gambar. Caranya dengan mengganti bit LSB pixel dengan bit data. Mengubah bit LSB hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya dan hal ini tidak akan berpengaruh terhadap persepsi.

C. Sistem Autentikasi Biometrik

Setiap sistem autentikasi biometrik terdiri dari empat modul dasar:

- *Enrollment Unit*, modul yang mendaftarkan setiap individual kedalam basis data sistem. Di fase ini, data biometrik dari setiap orang dibaca untuk dihasilkan representasi digitalnya.
- *Feature Extraction Unit*, modul ini memproses sampel input yang digunakan untuk menghasilkan sebuah representasi yang disebut template, yang kemudian disimpan di basis data pusat atau di smartcard yang diberikan pada individu.
- *Matching Unit*, modul ini membandingkan input yang ada dengan template yang tersimpan. Jika sistem melakukan verifikasi identitas, maka modul ini membandingkan input dengan template master yang ada lalu dihasilkan nilai kecocokan.
- *Decision Maker*, modul ini menerima atau menolak pengguna berdasarkan nilai ambang batas keamanan dan nilai kecocokan.

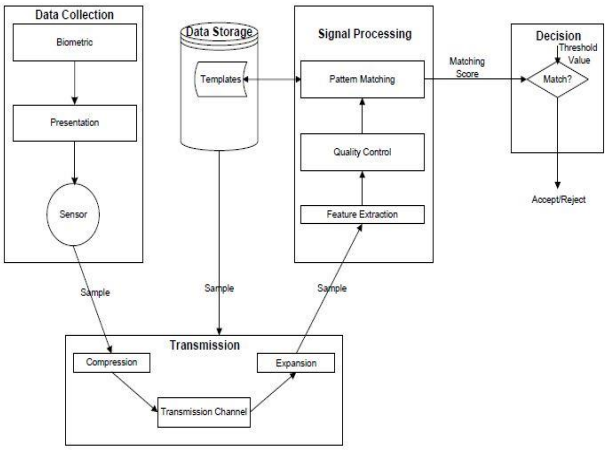

Figure 2 Struktur dasar sistem autentikasi biometrik[5]

Evaluasi performa dari sistem autentikasi biometric tergantung pada dua tipe kesalahan, kesalahan pencocokan dan kesalahan akuisisi data. Kesalahan yang berhubungan dengan kesalahan pencocokkan terdiri dari :

- *False Acceptance Rate*, kesalahan pengukuran biometrik sehingga dua orang berbeda dianggap sebagai orang yang sama.
- *False Rejection Rate*, kesalahan pengukuran biometrik sehingga data dari orang yang sama dianggap berasal dari dua orang yang berbeda.
- *Failure to Capture Rate*, kesalahah sistem dimana sistem tidak bisa menangkap sampel dengan kualitas yang cukup dalam beberapa kali percobaan.
- *Failure to Enroll Rate*, kesalahan dimana sistem biometrik tidak bisa menghasilkan referensi template dengan kualitas yang mencukupi.

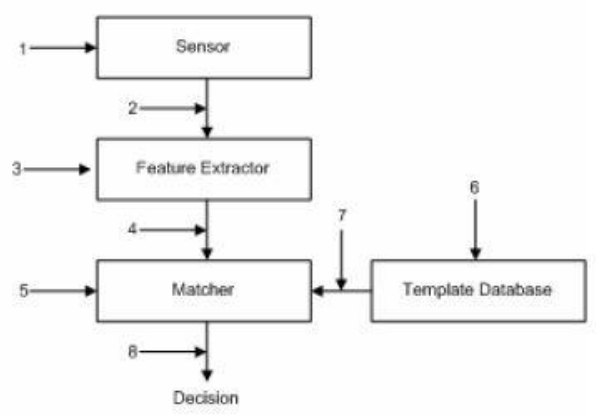

Figure 3 Celah serangan didalam sistem biometrik [4]

Sistem autentikasi biometrik seperti sistem autentikasi lainnya, bukan merupakan sistem autentikasi yang sempurna. Sistem ini memiliki beberapa kelemaha, meskipun biometrik menyediakan data yang unik, namun data ini tidak rahasia dan jika hilang tidak dapat tergantikan.

Biometrik bekerja dengan baik hanya jika dapat memverifikasi dua hal:

- Data biometrik itu datang dari orang yang asli pada waktu verifikasi saat itu.
- Data biometrik ini sesuai dengan biometrik master pada basis data.

Namun berbagai masalah menghambat kemampuan untuk memverifikasi diatas:

- Noise di data yang diperoleh – Noise pada data biometrik yang disebabkan oleh
  sensor rusak, karakteristik fisik yang rusak dan kondisi ruang yang tidak menguntungkan. Hal ini menyebabkan data tidak cocok dan akan ditolak.
- Variasi Intra-kelas - Data yang diperoleh selama otentikasi mungkin berbeda dari data yang digunakan untuk menghasilkan template selama pendaftaran, mempengaruhi proses pencocokan.
- Non-universalitas - Sebuah subset dari pengguna yang tidak memiliki biometrik tertentu.

III. ANALISIS DAN IMPLEMENTASI

Nilai kecocokkan sempurna terjadi apabila sampel yang diambil dari input sensor memiliki kecocokkan sama persis dengan file yang tersimpan didalam basis data pusat. Didalam kebanyakan sistem autentikasi, kecocokkan sempurna merupakan hal yang sangat bagus, namun didalam sistem autentikasi biometrik justru menimbulkan keraguan. Terdapat variansi natural didalam proses penangkapan data oleh sensor yang menyebabkan nilai kecocokkan sempurna hamper mustahil. Ketika hal tersebut terjadi, maka hal tersebut mengindikasikan bahwa seseorang telah mendapatkan template biometrik yang tersimpan didalam basis data dan berniat melakukan replay attack. Solusi potensial untuk menangani maslah ini adalah dengan mengharuskan pengguna untuk menyediakan sampel lain. Jika pengguna tersebut memang benar-benar sah, maka variansi natural akan menyebabkan perbedaan nilai kecocokkan, berbeda jika pengguna palsu yang menggunakannya maka ia tidak memiliki sampel lain sehingga nilai kecocokkan akan tetap sama. Dengan penerapak steganografi, maka penyerang akan mengalami kesulitan yang berarti ketika mencoba mencari celah keamanan sistem.

Metode LSB klasik pada steganografi yang menyisipkan pesan sebagai contoh keedalam cover image dari sidik jari, menggunakan pesan bit stream untuk mengganti least significant bit dari cover image secara sekuensial. Metoda ini menimbulkan beberapa distorsi terhadap kualitas citra yang dihasilkan. Untuk mengatasi hal ini, maka dilakukan juga teknik LSB yang dilakukan tidak secara sekuensial namun secata tersebar sehingga tidak terlalu merusak kualitas dari citra. Pesan rahasia yang disembunyikan disimpan di lokasi yang random dengan menggunakan pseudorandom number generator (PRNG) dengan *seed* adalah password dari pengguna. Algoritma

```
function pseudoRandom(input integer : seed) →integer

DECLARATION
m_w, m_z, result : integer
ALGORITHM
long m_w ← seed;
long m_z ← 211;{choose any number for second seed}
m_z ← 36969 * (m_z & 65535) + (m_z >> 16);
m_w ← 18000 * (m_w & 65535) + (m_w >> 16);
result ← (m_z << 16) + m_w;
→ |result % 25000000| {return absolute result}
```

Proses penyisipan:

- Baca cover image (gambar sidik jari).
- Baca pesan yang akan disisipkan.
- Ambil password dari user
- Generate angka pseudo random berdasarkan password untuk menentukan posisi LSB untuk menyembunyikan pesan.
- Sembunyikan pesan.

Proses akuisisi pesan:

- Baca stegano image.
- Ambil password dari user
- Generate angka pseudo random berdasarkan password untuk menentukan posisi LSB untuk menyembunyikan pesan.
- Ambil pesan

IV. HASIL PENGUJIAN

Dengan menggunakan algoritma yang telah ditentukan

sebelumnya, dilakukan pengujian dengan melakukan penyisipan pesan kedalam contoh sidik jari. Lalu setelah dilakukan penyisipan, dilakukan penghitungan berapa PSNR yang dihasilkan melalui perbandingan kedua citra. Hasilnya dapat dilihat di gambar berikut.

Figure 4 Contoh cover image sidik jari

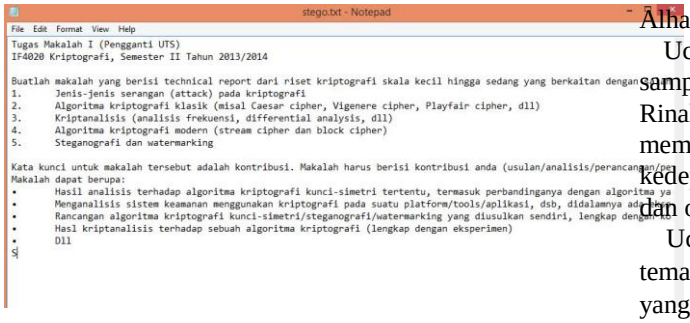

Figure 5 Pesan yang disisipkan

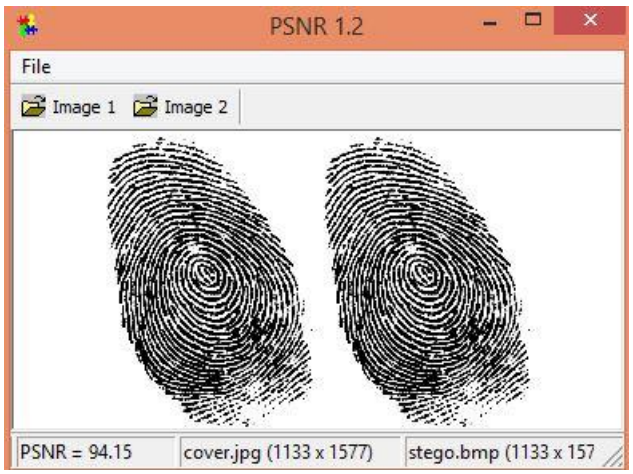

Figure 6 Hasil perhitungan PSNR

Dari hasil diatas, dapat dilihat bahwa nilai PSNR yang dihasilkan cukup tinggi, sehingga dapat disimpulkan bahwa penyisipan pesan tidak merusak kualitas dari citra sidik jari.

V. KESIMPULAN

Dari hasil pengujian yang telah dilakukan, maka dapat disimpulkan beberapa hal berikut:

- Steganografi pada sistem autentikasi biometrik merupakan hal yang sangat penting untuk meningkatkan keamanan dan kredibilitas sistem.
- Penggunaan teknik steganografi yang tepat dibutuhkan agar tidak merusak kualitas citra terlalu buruk sehingga dapat mengalami kesalahan pencocokkan pada sistem autentikasi.
- Metoda penyisipan pesan dengan menggunakan LSB yang tersebar merupakan metoda yang cukup efektif untuk sistem autentikasi biometrik.

VII. ACKNOWLEDGMENT

Penulis ingin mengucapkan terima kasih yang paling besar kepada Allah SWT. Dialah yang senantiasa memberikan kesehatan dan kesempatan bagi penulis sehingga bisa menyusun makalah ini hingga selesai. Alhamdulillah.

Ucapan terima kasih selanjutnya ingin penulis sampaikan kepada dosen mata kuliah IF4020, Bapak Rinaldi Munir. Berkat bimbingan beliau penulis bisa memahami ilmu-ilmu dalam bidang Kriptografi. Semoga kedepannya, ilmu ini akan terus bermanfaat bagi penulis dan orang-orang di sekitarnya.

Ucapan terima kasih terakhir diberikan kepada teman-teman sekelas penulis. Khususnya ucapan terima kasih yang sangat besar kepada rekan sekelompok tugas. Atas kerja samanya, tugas besar dan tugas kecil yang diberikan pada mata kuliah ini bisa dikerjakan dengan baik.

REFERENSI

[1] BIOMETRICS: Personal Identification in Networked Society, A. Jain, S. Pankanti, and R. Bolle, eds., Kluwer, 1999.
[2] B. Schneier, “The Uses and Abuses of Biometrics,” Comm. ACM, vol. 42, no. 8, p. 136, Aug. 1999.
[3] N.K. Ratha, J.H. Connell, and R.M. Bolle, “An Analysis of Minutiae Matching Strength,” Proc. Third Int’l. Conf. Audio- and Video-Based Biometric Person Authentication, pp. 223-228, June 2001.
[4]Jain, A.K.; Uludag, U., “*Hiding biometric data*”, Pattern Analysis and Machine Intelligence, IEEE Transactions on, Volume: 25, Issue: 11, Nov. 2003.
[5]Leniski, *A.C., Skinner, R.C., McGann, S.F. and Elliott, S.J*, “*Securing the biometric model*,” Security Technology, 2003. Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on, 14-16 Oct. 2003.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 18 Maret 2014

ttd

Muhammad Iqbal 13510064