Analisis dan Implementasi Tanda Tangan Digital dengan Memanfaatkan Steganografi pada *E-Mail*

Filman Ferdian - 13507091[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]*if17091@students.if.itb.ac.id*

***Abstract*—Tanda tangan digital adalah suatu teknik yang digunakan untuk melakukan otentikasi dan menjamin kerahasiaan data. Penggunaanya banyak diterapkan pada distribusi perangkat lunak, transaksi keuangan, pengiriman berkas, dsb. Salah satu media penerapannya adalah pada *E-Mail.* Steganografi adalah suatu teknik untuk menyembunyikan suatu pesan pada pesan lainnya. Teknik ini digunakan untuk menyamarkan tanda tangan digital ke dalam suatu gambar**

Pada makalah ini, kita akan melakukan analisis dan implementasi dari tanda tangan digital yang disisipkan pada suatu gambar dalam *E-Mail*. Tanda tangan digital diterapkan dengan metode kombinasi fungsi *Hash* menggunakan algoritma SHA1 menghasilkan *Message Digest* dan metode kriptografi kunci-publik terhadap *Message Digest* menggunakan algoritma RSA. Hasil tanda tangan digital yang memiliki ukuran tetap disisipkan pada suatu gambar dengan metode modifikasi LSB. Hasil akhir gambar akan ditempelkan pada *E-Mail.*

***Key Words*—Tanda Tangan Digital, *E-Mail*, Steganografi, SHA1, RSA**

I. PENDAHULUAN

Dalam era teknologi informasi yang berkembang sangat pesat, penggunaan tanda tangan sudah banyak diterapkan secara digital melalui tanda tangan digital. Tanda tangan digital mulai berkembang seiring munculnya kebutuhan otentikasi suatu data atau berkas yang digunakan secara digital. Penggunaannya juga bertujuan untuk menghindari pemalsuan ataupun gangguan. Saat ini, pemanfaatan tanda tangan digital sudah banyak diterapkan pada distribusi perangkat lunak, transaksi keuangan, pengiriman berkas, dsb.

Definisi tanda tangan digital adalah suatu skema matematika untuk menunjukkan keaslian pesan digital atau dokumen. Sebuah tanda tangan digital yang valid memberikan alasan untuk percaya bahwa penerima pesan yang dibuat oleh pengirim yang diketahui, dan bahwa itu tidak diubah dalam perjalanan.

Keberadaan *E-Mail* sebagai salah satu media yang banyak digunakan untuk mentransfer tulisan, dokumen atau *file* secara digital memunculkan kebutuhan terkait otentikasi. Suatu *E-Mail* khusus terkadang membutuhkan jaminan keaslian terkait data yang dikirim melalui media jaringan tersebut. Salah satu metode yang dapat digunakan untuk menyelesaikan permasalahan ini adalah tanda tangan digital. Suatu *E-Mail* yang telah disisipi oleh tanda tangan digital akan memberikan kemudahan antara pengirim dan penerima untuk menjamin keaslian data.

Penggunaan tanda tangan digital pada pengiriman *E-Mail* dapat dilakukan dengan menggunakan skema enkripsi terhadap pesan yang akan dikirim dengan suatu kunci atau dengan menggunakan kombinasi fungsi *Hash* dengan kriptografi kunci-publik. Pada metode enkripsi, hasil yang dihasilkan akan sesuai dengan besar pesan yang dikirimkan. Metode ini juga sangat bergantung dengan kunci yang digunakan. Sementara pada metode *Hash*, hasil tanda tangan digital hasilnya sama berapapun besar pesan. Metode ini juga memanfaatkan kriptografi kunci-publik yang diterapkan pada hasil fungsi *hash* terhadap dokumen.

Penggunaan tanda tangan digital berupa tulisan hasil enkripsi ataupun fungsi *Hash* akan menghasilkan dokumen dengan tanda tangan yang terlihat secara jelas karena ditulis dengan kode yang terlihat. Hal ini dapat memunculkan potensi gangguan dengan menghilangkan tanda tangan sehingga dokumen yang diterima dapat dianggap memang tidak dilengkapi tanda tangan digital. Penelitian oleh Ripandy sempat berusaha untuk menyisipkan *Message Digest*, yaitu tanda tangan digital pada *E-Mail*, berupa QR *Code* [1]. Pada penelitian kali ini, kita akan mencoba memanfaatkan steganografi untuk menyamarkan *Message Digest* yang akan digunakan sebagai tanda tangan digital.

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Penerapan steganografi dapat dilakukan pada beragam media salah satunya adalah gambar.

Pada makalah ini, *Message Digest* akan disisipkan dalam suatu gambar yang akan ditempelkan pada *E-Mail*. Metode tanda tangan digital yang akan digunakan adalah kombinasi antara fungsi *Hash* dan kriptografi kunci-publik. Fungsi *Hash* yang akan digunakan adalah SHA1.

Sementara, algoritma kunci-publik yang digunakan adalah RSA. Untuk Steganografi pada citra digital, metode yang akan digunakan adalah modifikasi LSB.

Hasil makalah ini akan memberikan suatu metode baru untuk melakukan otentikasi dan menjamin keaslian pesan pada *E-Mail* dengan tanda tangan digital. Selain itu, tanda tangan digital yang disisipkan tidak akan mudah diketahui karena disisipkan pada komponen lain pada pesan berupa gambar dengan teknik steganografi.

II. LANDASAN TEORI

Sebelum membahas penggunan tanda tangan digital pada *E-Mail*, terlebih dahulu dijelaskan beberapa konsep yang berkaitan dengan makalah ini.

II.1 TANDA TANGAN DIGITAL

Tanda tangan digital adalah suatu nilai kriptografis yang bergantung pada pesan dan pengirim pesan (Hal ini kontras dengan tanda tangan pada dokumen kertas yang bergantung hanya pada pengirim dan selalu sama untuk semua dokumen). Dua metode yang dapat digunakan pada tanda tangan digital antara lain:

1. Enkripsi pesan
2. Menggunakan kombinasi fungsi *hash* dan kriptografi kunci-publik

Pembahasan akan difokuskan pada teknik tanda tangan digital dengan menggunakan kombinasi fungsi *hash* dan kriptografi kunci-publik. Mula-mula pesan (*M*) ditransformasi oleh fungsi *hash* (*H*) menjadi pesan ringkas (*h*). Pesan ringkas tersebut dienkripsi dengan kunci privat (*SK*) pengirim pesan:

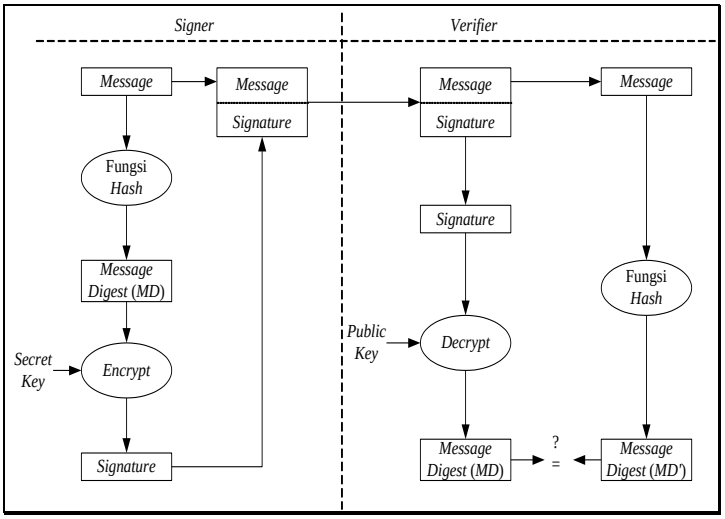
$$S = E_{SK}(h)$$

Hasil enkripsi (S) inilah yang disebut tanda-tangan digital. Tanda-tangan digital dapat ditambahkan (*append*) pada pesan atau terpisah dari pesan dan dikirim secara bersamaan. Di tempat penerima, tanda-tangan diverifikasi untuk dibuktikan keotentikannya dengan cara berikut:

1. Tanda-tangan digital S didekripsi dengan menggunakan kunci publik (*PK*) pengirim pesan, menghasilkan pesan-ringkas semula, *h*, sebagai berikut:

$$h = D_{PK}(S)$$

2. Pengirim kemudian mengubah pesan (*M*) menjadi pesan ringkas (*h'*) dengan menggunakan fungsi hash satu-arah yang sama dengan fungsi hash yang digunakan oleh pengirim.
3. Jika *h' = h*, berarti tanda-tangan yang diterima otentik dan berasal dari pengirim yang benar.



Gambar 1 Proses Penandatanganan dan Verifikasi [2]

II.2 FUNGSI *HASH*

Fungsi *hash* adalah fungsi yang menerima masukan string yang panjangnya sembarang dan mengkonversinya menjadi string keluaran yang panjangnya tetap (umumnya berukuran jauh lebih kecil daripada ukuran string semula). Jika string menyatakan pesan (*message*), maka sembarang pesan (*M*) berukuran sembarang dikompresi oleh fungsi *hash* (*H*) melalui persamaan:

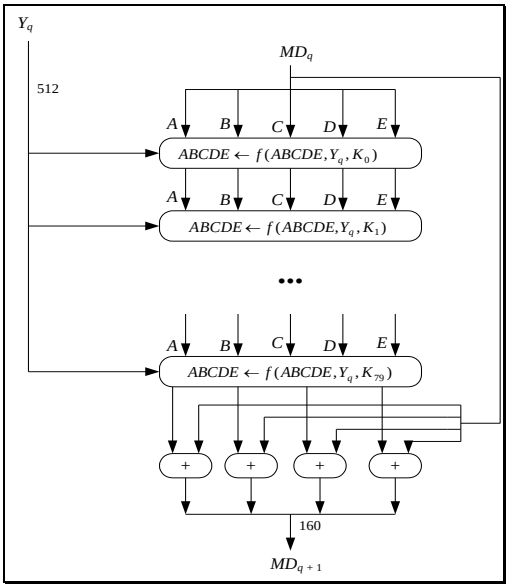
$$h = H(M)$$

Keluaran fungsi hash disebut juga nilai *hash* atau pesan-ringkas (*message digest*). Nilai *h* adalah nilai *hash* atau *message digest* dari fungsi *H* untuk pesan *M*. Fungsi hash satu-arah adalah fungsi *hash* yang bekerja dalam satu arah: pesan yang sudah diubah menjadi pesan-ringkas tidak dapat dikembalikan lagi menjadi pesan semula. Contoh fungsi *hash* satu-arah adalah MD5 dan SHA. MD5 menghasilkan pesan-ringkas yang berukuran 128 bit, sedangkan SHA menghasilkan pesan-ringkas yang berukuran 160 bit.

Salah satu keluarga dari algoritma SHA adalah algoritma SHA-1. Langkah-langkah pembuatan *Message Digest* antara lain:

1. Penambahan *padding bits*.
2. Penambahan nilai panjang pesan semula.
3. Inisialisasi penyangga MD.
4. Pengolahan pesan dalam blok berukuran 512 bit.

Proses pengolahan pesan dilakukan sebanyak 80 putaran dengan masing-masing putaran memiliki skema penambahan bilangan.



Gambar 2 Skema Pemrosesan Pesan 512 bit SHA-1

II.3 KRIPTOGRAFI KUNCI-PUBLIK

Pada kriptografi kunci-publik, masing-masing pengirim dan penerima mempunyai sepasang kunci:

1. Kunci public (*e*): untuk mengenkripsi pesan
2. Kunci privat (*d*): untuk mendekripsi pesan

Proses Enkripsi (*E*) terhadap pesan (*m*) dan Dekripsi (*D*) terhadap *ciphertext* (*c*) menggunakan rumus berikut:

$$E_e(m) = c \text{ dan } D_d(c) = m$$

Salah satu algoritma algoritma kunci-publik yang banyak digunakan dalam tanda tangan digital adalah RSA. Algoritma RSA adalah algoritma kriptografi kunci-publik yang dikembangkan oleh tiga peneliti MIT yaitu Ron Rivest, Adi Shamir, dan Len Adleman, pada tahun 1976. RSA memiliki beberapa properti antara lain:

1. Pembangkitan kunci:
   a. Pilih dua bilangan prima, p dan q (rahasia)
   b. Hitung n = pq dan O(n) = (p – 1)(q – 1)
   c. Pilih sebuah bilangan bulat (*e*) untuk kunci public yang relatif prima terhadap O(n)
   d. Hitung kunci dekripsi (*d*) dengan persamaaan

$$ed = 1 \pmod{O(n)}$$

2. Enkripsi
   Proses diawali dengan membagi pesan menjadi blok-blok plainteks. Hitung blok cipherteks c_i untuk blok plainteks p_i dengan persamaan:

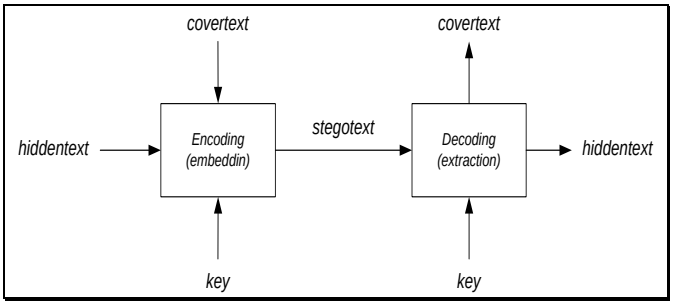
$$c_i = m_i^e \bmod n$$

3. Dekripsi
   Proses dekripsi dilakukan dengan menggunakan persamaan:

$$m_i = c_i^d \bmod n$$

II.4 STEGANOGRAFI

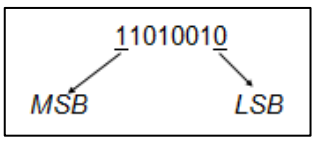
Steganografi adalah ilmu dan seni menyembunyikan (*embedded*) informasi dengan cara menyisipkan pesan rahasia di dalam pesan lain. Pesan dan media penyisipan pesan dapat berupa teks, gambar, audio dan video. Steganografi saling melengkapi kriptografi dengan menyembunyikan keberadaan pesan yang telah dienkripsi. Hal ini bertujuan untuk menghindari kecurigaan.



Gambar 3 Skema Steganografi

Pada steganografi citra digital, terdapat dua macam teknik yang dapat digunakan yaitu *Spatial Domain* dan *Transform Domain*. *Transform Domain* memodifikasi hasil transformasi sinyal dalam ranah frekuensi. Salah satu metode yang dapat digunakan adalah *Spread Spectrum*. Sementara, *Spatial Domain* memodifikasi langsung nilai *byte* dari media penyisipan pesan. Salah satu metodenya adalah metode modifikasi LSB.

Metode modifikasi LSB memanfaatkan kelemahan indra visual manusia dalam mengamati perubahan sedikit pada gambar. Cara steganografi dilakukan dengan mengganti bit LSB (*Least Significant Byte*) pixel dengan bit data. Proses pengubahan bit LSB hanya mengubah nilai *byte* satu lebih tinggi atau lebih rendah dari nilai sebelumnya sehingga tidak berpengaruh signifikan terhadap persepsi visual.



Gambar 4 Contoh Struktur bit

Untuk memperkuat teknik penyembunyian data, bit-bit data rahasia tidak digunakan mengganti byte-byte yang berurutan, namun dipilih susunan byte secara acak. Pembangkit bilangan acak-semu (PRNG: *pseudo-random number generator*) digunakan untuk membangkitkan bilangan acak. Umpan (*seed*) untuk bilangan acak berlaku sebagai kunci (*stego-key*).

III. ANALISIS

Konsep yang dibutuhkan dalam membangun sistem ini terdiri dari teknik tanda tangan digital dan steganografi. Tanda tangan digital dirancang menggunakan teknik kombinasi fungsi *Hash* dan kriptografi kunci publik. Teknik ini menghasilkan panjang hasil tanda tangan digital yang sama besarnya seberapapun ukuran dari pesan asli. Hal ini memberikan kemudahan dalam penyisipan dalam proses steganografi. Sementara, teknik steganografi yang digunakan adalah *Spartial Domain* karena cukup sederhana. Selain itu, hasil perubahan *byte* tidak akan memberikan pengaruh visual yang besar.

Fungsi *Hash* yang digunakan dalam sistem ini adalah SHA-1. SHA-1 menghasilkan pesan ringkas sepanjang 160 bit. Pesan ringkas (*Message Digest*) sepanjang 160 bit ini akan menjadi masukkan untuk pemrosesan kriptografi kunci-publik.

Untuk proses enkripsi pesan ringkas digunakan suatu kunci privat. Dengan cara ini, maka kerahasiaan pesan dan otentikasi dapat dicapai sekaligus. Ide ini ditemukan oleh Diffie dan Hellman. Proses pembangkitan kunci juga akan dilakukan secara acak sehingga kunci yang dihasilkan dapat dijamin keunikannya. Hasil dari proses enkripsi adalah tanda tangan digital berupa string sepanjang 160 *bit* yang akan diproses dengan teknik steganografi.

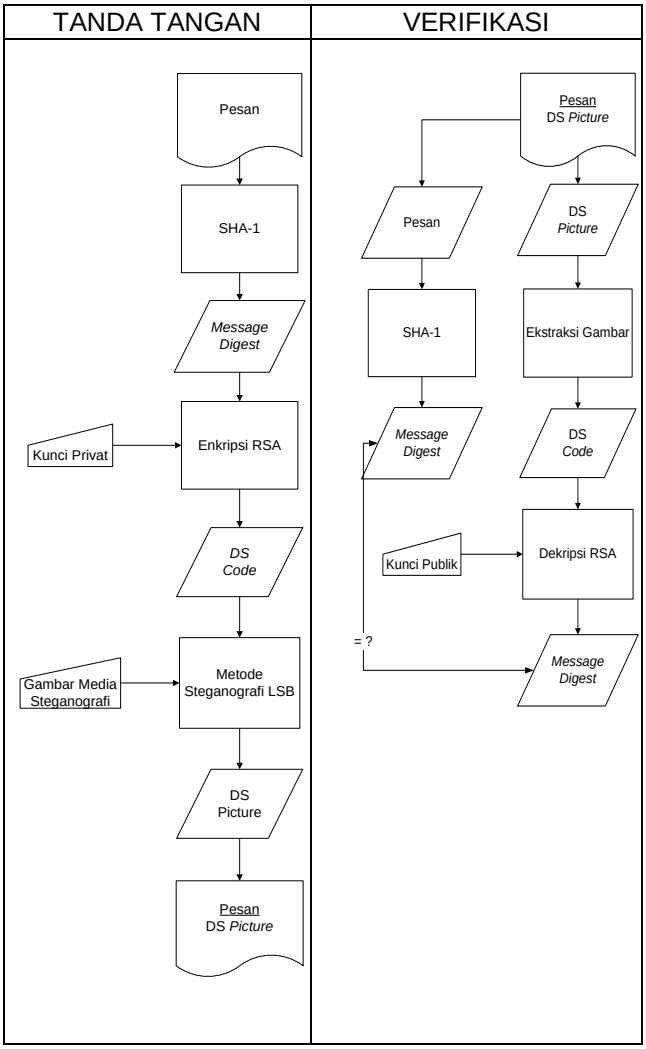
Teknik Steganografi yang digunakan sangat sederhana. Proses penyisipan pesan secara steganografi dilakukan dengan langsung menyisipkan setiap *bit* dari tanda tangan digital ke dalam suatu gambar. Posisi peletakkan tidak akan diacak dengan pertimbangan hasil 160 bit sudah merupakan bilangan yang acak setelah diproses melalui fungsi *Hash* serta algoritma enkripsi RSA. Proses penyisipan akan dilakukan setiap 1 *bit*. Dengan satu *pixel* terdiri dari 3 *byte* maka dibutuhkan ukuran gambar minimal sebesar 54 *pixel*. Proses steganografi dapat divariasikan dengan menambahkan pembangkitan posisi secara acak. Hal ini akan meningkatkan keamanan. Selain itu, tanda tangan digital berupa string sepanjang 160 *bit* ini juga dapat dienkripsi terlebih dahulu.

Proses verifikasi dari data yang dikirim dengan tanda tangan digital dilakukan dengan memisah antara pesan yang terdiri dari pesan utama dan tanda tangan digital. Pesan utama akan diproses dengan menerapkan fungsi *Hash* sehingga akan didapatkan kembali *Message Digest* (MD). Selama pesan tidak dirubah, maka MD yang dihasilkan adalah MD yang sama ketika pesan dienkripsi. Hal ini akan menjamin keaslian dari data. Sementara data tanda tangan digital berupa gambar akan diproses sehingga menghasilkan *Message Digest*. Kedua MD yang diproses pada saat verifikasi akan dibandingkan. Jika hasilnya sama maka *file* tersebut asli. Jika suatu pesan yang diterima tidak memiliki gambar berisi tanda tangan digital maka keaslian dari *E-Mail* dapat dipastikan salah.

Pemrosesan terhadap gambar yang berisi tanda tangan digital diawali dengan ekstraksi terhadap gambar. Proses ekstraksi hanya mengambil *bit* akhir dari setiap *byte* yang disisipi secara urut dan dirangkai menjadi tanda tangan digital berupa string sepanjang 160 *bit*. Hasil ini akan didekripsi dengan menggunakan kunci publik pengirim. Kunci publik mengirim dapat disebarkan kepada semua pembaca pesan. *Hasil* dari dekripsi dengan teknik RSA adalah *Message Digest* yang akan dibandingkan dengan hasil fungsi *hash* dari pesan yang diterima.

Prinsip otentikasi terdapat pada tanda tangan digital yang diterima. Jika isi tanda tangan digitial yang diterima tidak dapat didekripsi maka bisa jadi pengirim tidak memiliki kunci untuk melakukan enkripsi. Hal ini menunjukkan bahwa pengirim tersebut bukanlah pengirim yang legal terhadap *E-Mail* tersebut.

Secara umum, hasil analisis berupa suatu skema pemrosesan yang akan diterapkan adalah sebagai berikut:



Gambar 5 Skema Pemrosesan Pesan

IV. IMPLEMENTASI

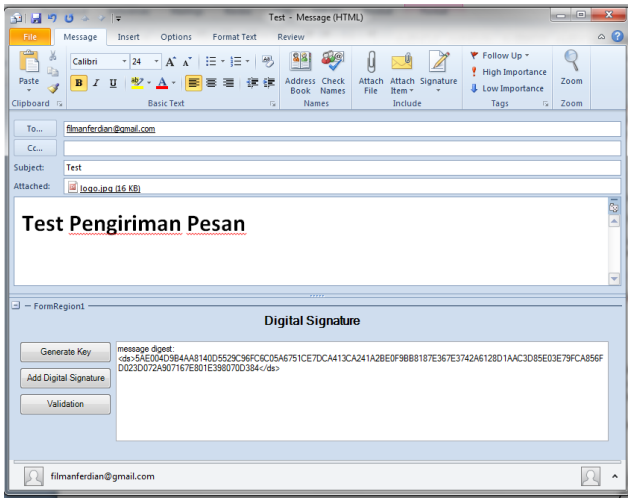
Implementasi dari sistem ini dilakukan sebagai *add-ins* pada aplikasi *E-Mail* berbasis *desktop*. Peletakkan gambar sebagai tanda tangan digital dapat diletakkan dengan tiga cara, antara lain:

1. Langsung di dalam pesan
2. *Attachment* pesan
3. *Hyperlink* ke gambar

Pada aplikasi ini, penggunaan gambar akan diletakkan sebagai *attachments*. Namun, pada beberapa aplikasi *E-Mail* gambar bisa diletakkan langsung di dalam pesan tersebut.

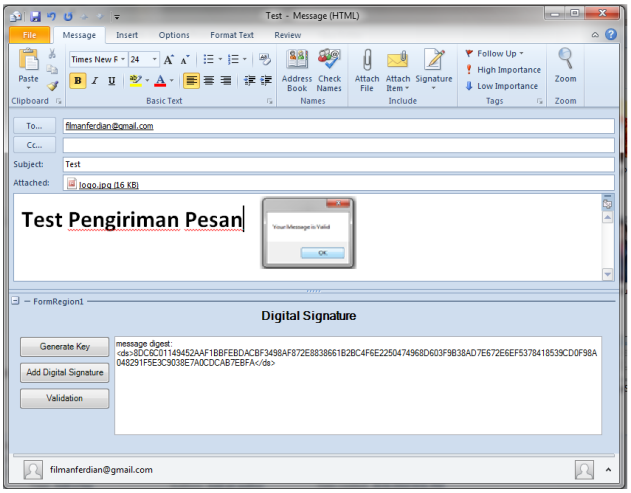
Implementasi dari komponen-komponen disusun sesuai konsep yang direncanakan dengan urutan terdiri dari pembangkit kunci secara acak, fungsi *hash*, enkripsi dan dekripsi kunci-publik serta penyisipan dan ekstraksi steganografi. Sementara, proses verifikasi dilakukan pada *inbox E-Mail*. Pengguna tinggal menekan tombol validasi untuk mengecek keberadaan *E-Mail.*

Hasil Implementasi menunjukkan bahwa aplikasi yang dibangun dapat disesuaikan dengan konsep yang direncanakan. Namun, hasil penerapan pada posisi gambar bisa dibilang kurang optimal karena gambar harus di-*attach* ke dalam pesan. Hal ini dapat menimbulkan kecurigaan oleh pembaca yang melakukan gangguan pada aplikasi karena setiap *E-Mail* yang memiliki tanda tangan digital selalu memiliki *attachments*.



Gambar 6 Proses Peletakkan Tanda Tangan

Pada gambar, dapat dilihat bahwa terdapat *attachment* berupa logo yang berisi gambar sebagai media meletakkan hasil penyisipan tanda tangan ke dalam gambar.



Gambar 7 Proses Verifikasi dari Tanda Tangan

Pesan validasi langsung disampaikan dalam jendela aplikasi dengan kotak pesan yang menyatakan pesan valid atau pesan tidak valid.

Sebagai saran pengembangan berikutnya, gambar sebaiknya disisipkan lansung pada pesan. Namun, perlu dilakukan survey terhadap aplikasi lingkungan implementasi yang mampu meletakkan gambar sebagai *attachments*.

V. KESIMPULAN

Pemanfaatan tanda tangan digital dapat divariasikan dengan teknik steganografi. Sistem ini membutuhkan komponen tanda tangan digital yang dapat memanfaatkan teknik kombinasi fungsi *hash* dan kriptografi kunci publik. Sementara, teknik steganografi yang dapat digunakan sangat beragam. Gambar merupakan salah satu media yang efektif sebagai penyimpanan. Teknik steganografi yang digunakan bisa mulai dari yang paling sederhana yaitu penyisipan tanpa pengacakan posisi karena hasil tanda tangan digital dengan kombinasi fungsi *hash* dan kriptografi kunci-publik sudah menjadi bilangan yang acak. Eskalasi teknik steganografi dapat meningkatkan kualitas dari tanda tangan digital.

Penggunaan kombinasi tanda tangan digital dan steganografi menjamin tiga aspek dalam pengamanan data yaitu otentikasi, keaslian dan kerahasiaan data. Otentikasi menjamin identitas dari pengirim. Penjaminan dilakukan dengan menggunakan kunci privat yang hanya dimiliki pengirim tertentu untuk mengenkripsi pesan pada *E-Mail*. Keaslian data menjamin tidak adanya manipulasi terhadap pesan yang dikirimkan. Penjaminan dapat dicek dari kecocokan antara pesan dengan tanda tangan digital-nya. Kerahasiaan data diterapkan dengan teknik steganografi. Dengan teknik ini, orang lain tidak akan menyadari keberadaan dari tanda tangan digital itu sendiri.

DAFTAR REFERENSI

[1] Adha, Ripandy. 2010. Message Digest dalam bentuk *QR Code* Sebagai Tanda Tangan Digital. Bandung

[2] Munir, Rinaldi. 2004. Bahan Kuliah IF5054 Kriptografi, Departemen Teknik Informatika. Bandung

[3] ITB, 2004. Widhiyasa, Arief. 2008. Kombinasi Algoritma Tanda Tangan Digital dengan Steganografi untuk Autentikasi File Media. Bandung

[4] http://en.wikipedia.org/wiki/Digital_signature. Waktu Akses: 8 Mei 2011

[5] http://id.wikipedia.org/wiki/Steganografi. Waktu Akses: 8 Mei 2011

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, 9 Mei 2011

Filman Ferdian (13507091)