Implementasi *Digital Signature* dan *Watermarking* pada Citra dengan Metode LSB, ElGamal dan Hash Function

Ivan Fadillah
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
13516128@std.stei.itb.ac.id

Abstrak— *Digital Signature* atau Tanda tangan digital adalah otentikasi elektronik yang di enkripsi pada dokumen digital. Sementara itu, *watermarking* adalah teknik yang digunakan untuk menyisipkan informasi tertentu ke dalam data digital seperti musik, citra, video dan lain-lain. Pada makalah ini, akan dilakukan penggabungan metode tanda tangan digital dan *watermarking* digital untuk otentikasi sebuah citra. Pembentukan tanda tangan digital pada citra menggunakan algoritma Elgamal dan fungsi hash SHA512. Fungsi hash ini dapat mengubah pesan dengan ukuran sembarang menjadi pesan ringkas dengan ukuran tetap. Setelah citra ditandatangani proses selanjutnya adalah melakukan penyisipan watermarking dengan metode LSB. Implementasi tanda tangan digital dan penyisipan watermark ini diharapkan dapat meningkatkan kepercayaan informasi yang terdapat persebaran citra melalui Internet.

Keywords— tanda tangan digital, watermarking, algoritma elgamal, fungsi hash.

I. PENDAHULUAN

Sekarang ini, di era wabah virus covid-19, penggunaan internet di Indonesia berkembang dengan pesat, terutama pada penggunaan media sosial. Kegiatan berbagi file digital seperti gambar, video, dokumen dan file lainnya seringkali terjadi dilakukan secara online. Hal ini seperti ini terkadang bisa menimbulkan masalah besar terhadap file tersebut. Salah satunya yang sering terjadi adalah memanipulasi gambar atau foto untuk membuat berita hoax, pencurian hak cipta gambar dan lain sebagainya. Hal seperti ini seharusnya tidak boleh dilakukan karena selain melanggar UU Informasi Transaksi dan Elektronik (ITE), hal ini juga dapat menimbulkan citra buruk terhadap pemilik hak cipta. Oleh karena itu pada makalah ini akan diusulkan sebuah solusi otentikasi yang dapat menjaga keaslian gambar atau citra yang di unggah oleh seseorang di internet. Solusi yang diusulkan menggunakan tanda tangan digital dan *watermarking.*

Penggunaan tanda tangan digital digunakan untuk mencegah modifikasi *single bit* data pada gambar. Sementara proses *watermarking* digunakan untuk menyembunyikan informasi gambar *watermark* yang diselipkan pada gambar asli. Penggunaan *watermark* ini harapannya dapat mendeteksi daerah konten citra yang diubah oleh seseorang.

Pada Makalah ini akan dibahas implementasi Penggunaan Tanda Tangan Digital dengan algoritma kunci publik yaitu ElGamal dan Fungsi Hash SHA512 pada citra, kemudian dilakukan proses penyisipan gambar watermark dengan metode LSB (Least Significant Bit).

II. DASAR TEORI

A. Tanda Tangan Digital (*Digital Signature*)

Tanda tangan digital adalah tanda tangan elektronik yang digunakan untuk membuktikan keaslian identitas pengirim pesan. Tanda tangan mengonfirmasi bahwa informasi berasal dari penanda tangan dan belum diubah. Tanda tangan digital digunakan untuk memastikan isi file yang dikirim tanpa ada perubahan setelah dikirim. Tanda tangan digital adalah nilai kriptografis yang bergantung pada isi pesan dan kunci.

Tanda tangan digital selalu berbeda-beda antara satu file dengan file lain. Terdapat dua cara dalam menandatangani pesan, yaitu melakukan enkripsi pesan dan menggunakan kombinasi fungsi hash dan kriptografi kunci-publik. Penandatangan pesan dengan cara mengenkripsinya memberikan dua fungsi yaitu kerahasiaan dan otentikasi pesan. Sedangkan penandatanganan pesan dengan kombinasi fungsi hash dan kunci publik hanya untuk keotentikan pesan saja. Untuk memeriksa integritas data yang telah diberi tanda tangan digital, digunakan publik key dari pihak yang memberi tanda tangan digital. Apabila hasil data yang diperoleh sama maka data tersebut tidak terjadi perubahan, namun jika hasil data yang diperoleh berbeda maka data yang telah diberi tanda

tangan digital telah terjadi perubahan dan/atau pihak yang memberi tanda tangan berbeda dengan pemilik kunci publik.

B. Digital Watermarking

Digital watermarking adalah penyisipan informasi (watermark) yang mengacu pada pemilik berkas atau dokumen digital untuk tujuan melindungi kepemilikan, copyright atau menjaga keaslian konten. Berkas atau dokumen digital dapat berupa video, audio, citra, dokumen teks dan sebagainya. Tujuan dari digital watermarking yaitu untuk perlindungan copyright, fingerprinting, pembuktian kepemilikan dan sebagainya.

Proses digital watermarking diawali dengan tahap embedding. Pada tahap ini, informasi digital yang asli akan disisipkan sinyal watermark di dalamnya. Setelah disisipkan, maka informasi digital tersebut dapat disebarluaskan. Setelah disebarluaskan, informasi digital kemungkinan mendapatkan beberapa 'serangan' untuk merusak sinyal watermark yang telah disisipkan. Serangan dapat berupa manipulasi informasi atau dengan menyisipkan noise-noise tertentu. Tujuannya adalah agar sinyal watermark tidak dapat diekstrak kembali seperti semula dan tidak dapat dibuktikan.

Syarat watermarking :

- Watermark melekat di dalam citra
- Penyisipan watermark tidak merusak kualitas citra
- Watermark dapat dideteksi/ekstraksi kembali sebagai bukti kepemilikan/copyright atau bukti adanya modifikasi

Tahap yang terakhir adalah ekstraksi sinyal watermark dari informasi digital yang telah disisipi sebelumnya. Jika hasil ekstraksi yang dihasilkan adalah sama dengan sinyal watermark semula, maka informasi digital tersebut terbukti kepemilikan dan keasliannya

C. Algoritma ElGamal

Algoritma ElGamal merupakan salah satu algoritma kunci publik yang dikemukakan oleh Taher Elgamal pada tahun 1985. Algoritma Elgamal menggunakan permasalahan logaritma diskrit. Algoritma ini terdiri dari tiga proses, yaitu proses pembangkitan kunci, proses enkripsi, dan proses dekripsi. Algoritma ElGamal merupakan salah satu algoritma block cipher, dimana melakukan enkripsi pada block-block plaintext yang menghasilkan block-block ciphertext yang kemudian digabungkan lagi menghasilkan ciphertext. Dalam proses dekripsi ciphertext dipecah menjadi block-block ciphertext yang kemudian di setiap block di deskripsi dan digabungkan menjadi plaintext semula.

D. Fungsi Hash SHA3-512

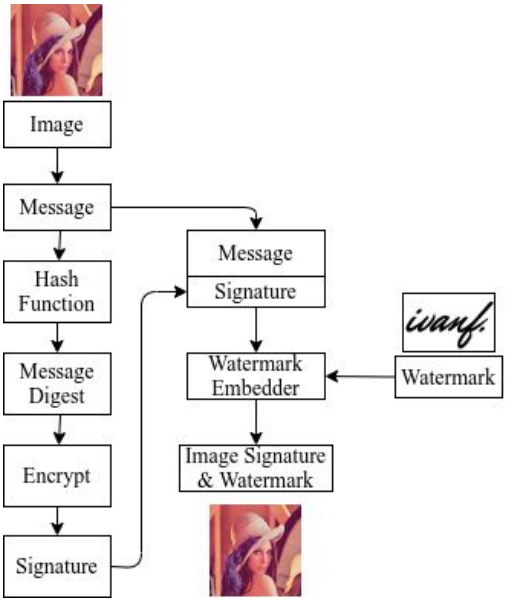
Fungsi hash merupakan fungsi yang mengubah suatu pesan dengan ukuran sembarang menjadi suatu pesan ringkas yang panjangnya selalu tetap meskipun panjang pesan aslinya berbeda-beda. Fungsi hash memiliki sifat satu arah, yang berarti setelah pesan diubah menjadi message digest, pesan tidak dapat diubah kembali menjadi pesan awal (irreversible).

SHA3 merupakan fungsi hash satu arah yang dihasilkan oleh kompetensi yang diselenggarakan oleh NIST. Proses dari algoritma SHA3 adalah sebagai berikut:

- Praproses pesan masukan (P), yaitu menambahkan padding pada pesan masukan. Panjang pesan akhir harus merupakan kelipatan r, dimana r = bitrate.
- Pemecahan pesan masukan menjadi P0, P1, …, Pi, dimana i = jumlah kelipatan panjang bitrate untuk panjang pesan masukan.
- Absorbing pada semua pesan masukan
- Squeezing sebanyak j, dimana j = kelipatan panjang keluaran r/w, r = bitrte dan w panjang lane
- keluaran merupakan gabungan dari keluaran Squeezing pada rentang bitrate tertentu

III. PEMBAHASAN

A. Arsitektur Umum



Gambar 1. Arsitektur umum *Sigature* dan *Watermarking Image*

B. Pembangkitan Tanda Tangan Digital

Proses tanda tangan digital yang memanfaatkan fungsi hash dan algoritma ElGamal terdiri dari beberapa tahap yaitu tahap penandatanganan dan tahap verifikasi. Pada tahap penandatangan terjadi proses seperti pada gambar 2, yaitu:

1. Menghitung message digest dari pesan menggunakan algoritma SHA512
2. Melakukan enkripsi pada message digest oleh algoritma ElGamal menghasilkan tanda tangan digital Pada tahap ini enkripsi dilakukan dengan

menggunakan kunci private si pengirim yang telah dibangkitkan sebelumnya.

3. Menempelkan atau menyisipkan tanda tangan digital pada file citra

C. Penyisipan dan Deteksi Watermarking Citra

Proses penyisipan watermark dilakukan pada ranah spasial yaitu dengan menyisipkan langsung pada nilai byte dari pixel citra.

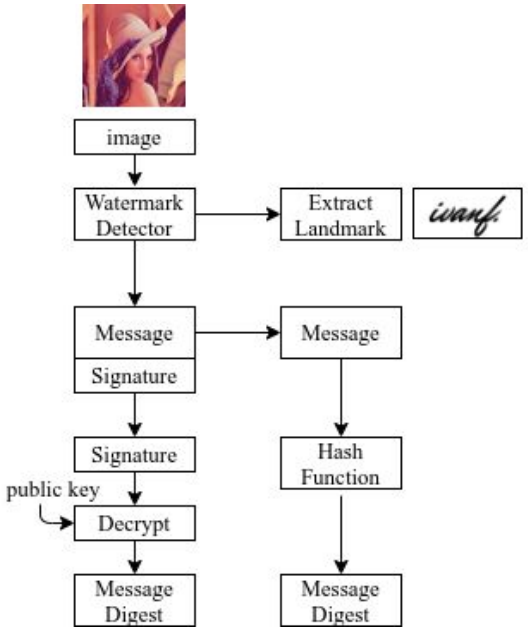
Tahapan yang dilalui adalah sebagai berikut:

1. Konversi watermark ke format binernya
2. Inisialisasi gambar output sama dengan gambar input
3. Iterasi setiap piksel pada gambar dan dengan melakukan hal berikut:
   a. Mengubah nilai piksel menjadi biner
   b. Melakukan operasi XOR bit watermark dan LSB bit pixel pada citra
   c. Selanjutnya memperbarui pixel citra
   d. Terakhir, cetak hasil input beserta gambar output.

D. Verifikasi Citra

Pada tahap verifikasi terjadi proses seperti pada gambar 3 yaitu:

1. Memisahkan citra dengan watermark
2. Memisahkan citra hasil point 1 dengan tanda tangan digital
3. Melakukan dekripsi tanda tangan digital dengan algoritma ElGamal menjadi message digest. Pada tahap ini dekripsi dilakukan dengan menggunakan kunci publik pengirim.
4. Menghitung nilai hash pesan yang diterima menggunakan algoritma SHA512
5. Membandingkan nilai yang diperoleh pada point 2 dan 3.



Gambar 2. Verifikasi *Sigature* dan *Watermarking Image*

Jika pada tahap verifikasi point 5 hasil perbandingan sama maka diketahui bahwa pengirim pesan terotentikasi dan data yang dikirim tidak terjadi perubahan. Namun jika perbandingan nilainya berbeda maka kemungkinan terjadi perubahan pada pesan saat dikirim dan /atau pengirim pesan ternyata orang yang berbeda.

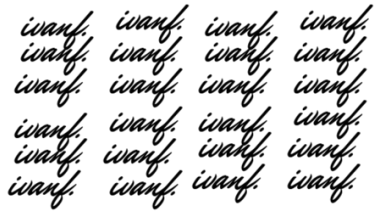
Pengolahan data citra pada enkripsi dilakukan dengan mengambil nilai byte dari citra, nilai byte tersebut yang akan diubah jadi message digest, kemudian message digest yang telah dilakukan enkripsi akan disisipkan setelah byte terakhir pesan. Pengolahan data citra pada dekripsi dilakukan dengan mengambil nilai beberapa byte terakhir pada citra. Message digest yang dihasilkan oleh algoritma SHA512 memiliki ukuran panjang yang sama untuk setiap ukuran pesan yang berbeda sehingga dapat ditentukan banyak nilai byte yang diambil yang merupakan tanda tangan digital yang telah disisipkan pada citra

IV. EKSPERIMEN DAN PEMBAHASAN

Eksperimen dari tanda tangan digital dan watermarking pada file citra akan dilakukan dengan menggunakan citra yang memiliki ukuran dan background yang berbeda, seperti yang ditunjukan pada gambar

Gambar 3. Pengujian Citra 1

Gambar 4. Pengujian Citra 2



Gambar 5. Watermark Pengujian Citra

Pada proses tanda tangan digital kunci publik dan kunci privat yang digunakan adalah sebagai sebagai berikut:

Public key (p, g, y): [17, 3, 15]
Private key (x): 6

1. Pengujian Citra 1

Dengan menggunakan fungsi hash SHA512 didapat nilai hash sebagai berikut:

bbbe80e9d4792c5934fff680ccacddcefc19f84e38052
6a42a8aed0e322719ebf0f1d08e1ddff53a96b91b137
a8dffc55c63796f11dc88576c7aefc172a74f82

Selanjutnya nilai hash tersebut di enkripsi dengan Elgamal menggunakan kunci privat menghasilkan *signature*:

01010 01010 01010 01001 01000 00000 01001 01101
00100 00100 00011 01101 01010 01111 01001 01101
01111 00100 01110 01110 01110 01110 01000 00000
01111 01111 00101 01111 00100 00100 01111 01001
01110 01111 00101 01101 01110 01000 00100 01001
01111 01000 00000 01001 01010 01110 00101 00100
01010 00101 01000 00101 01001 00100 00000 01001
01111 01010 01010 00011 00101 01101 01001 01010
01110 00000 01110 00101 00100 00000 01000 01001
00101 00100 00100 01110 01110 01001 01111 00101
01101 01110 01010 01101 00101 01010 00101 01111
00011 00101 01000 00100 01110 01110 01111 01001
01001 01111 01110 01111 00011 01101 01110 01110
00101 00101 00100 01111 01000 01000 01001 00011
01110 01111 00011 00101 01001 01110 01111 00101
00011 01010 00101 00011 00100 01110 01000 01010

Kemudian tanda tangan tersebut disisipkan di bawah gambar, dan hasilnya dapat dilihat pada gambar 6.

Gambar 6. Hasil penyisipan tanda tangan pada data uji 1

Selanjutnya, Citra ini dilakukan penyisipan watermarking dengan metode LSB. Hasilnya dapat dilihat pada gambar 7. Pada gambar tampak sedikit garis pada bagian langit.

Gambar 7. Hasil penyisipan *watermark* pada data uji 1

PSNR (Peak signal-to-noise ratio) = **30.26**

2. Pengujian Citra 2

Dengan menggunakan fungsi hash SHA512 didapat nilai hash sebagai berikut:

76821c36ab09adb2a408ebec72d75bbb18f274cd390
1bfd91f2211c06d969311a048f0b92e614dc8d201c3b
c288c2b6be503be51897adf759ea85adcc4879da6

Selanjutnya nilai hash tersebut di enkripsi dengan Elgamal menggunakan kunci privat menghasilkan *signature*:

01011 00110 00000 00010 01101 00111 00111
00110 01101 00010 01000 00101 01101 01100
00010 00010 01101 01100 01000 00000 00001
00010 00001 00111 01011 00010 01100 01011
00001 00010 00010 00010 01101 00000 00110
00010 01011 01100 00111 01100 00111 00101
01000 01101 00010 00110 01100 00101 01101
00110 00010 00010 01101 01101 00111 01000
00110 01100 00101 00110 00101 00111 01101
01101 01101 01000 01100 00000 00110 01000
00010 00101 00010 00001 00110 01101 01100
01100 00111 00000 01100 00010 01000 01101
00111 00111 00010 00111 00010 00000 00000

00111 00010 00010 00110 00010 00001 00001
01000 00111 00010 00001 00001 01101 00000
00101 01011 01101 01100 00110 01011 00001
00101 00001 01101 00000 00001 01101 01100
00111 00111 01100 00000 01011 00101 01100
01101 00110

Kemudian tanda tangan tersebut disisipkan di bawah gambar, dan hasilnya dapat dilihat pada gambar 8.

Gambar 8. Hasil penyisipan tanda tangan pada data uji 2

Selanjutnya, Citra ini dilakukan penyisipan watermarking dengan metode LSB. Hasilnya dapat dilihat pada gambar 9. Pada gambar tampak sedikit garis pada bagian atas.

Gambar 9. Hasil penyisipan *watermark* pada data uji 1

PSNR (Peak signal-to-noise ratio) = **45.81**

C. Analisis Kasus

1. Adanya perubahan pada Citra dan Kunci Publik

Perubahan satu byte pada citra akan mengubah nilai fungsi hash sehingga hasil ini akan mengakibatkan perbedaan hasil deskripsi dari tanda tangan digital yang disisipkan pada bagian bawah citra dengan nilai message digest citra tersebut. Selain itu perubahan byte pada citra juga akan menyebabkan watermark menjadi rusak. Sehingga kita dapat menyimpulkan bahwa terdapat modifikasi citra pada citra aslinya.

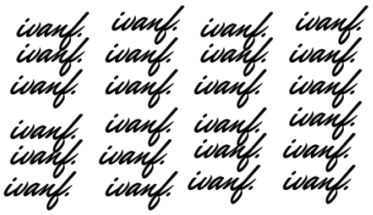
Watermark : Rusak

Verifikasi : Tidak Valid

2. Tidak terjadi perubahan pada Citra dan kunci publik

Ketika tidak terjadi perubahan pada citra dan kunci publik valid, maka watermark akan terekstraksi dengan benar dan hasil fungsi hash pada citra akan sama dengan hasil deskripsi citra tersebut.

Watermark : Tidak berubah



Verifikasi : Valid

IV. KESIMPULAN DAN SARAN PENGEMBANGAN

Penggunaan tanda tangan digital dan watermarking pada citra dapat meningkatkan dan keamanan keaslian citra tersebut. Berdasarkan hasil eksperimen bahwa penggunaan metode tanda tangan digital ini hasil yang didapatkan tidak merusak citra aslinya karena nilai PSNR masih dapat ditoleransi oleh penglihatan.

Dengan adanya makalah ini harapannya dapat dikembangkan lebih lanjut pada berbagai file digital lainnya seperti video, musik dan lain-lain. Selain itu juga penggunaan metode ini harapannya dapat dikembangkan dan diaplikasikan pada berbagai media sosial. Pengembangan metode pada makalah ini masih memiliki kekurangan sehingga penulis berharap penggunaan tanda tangan digital dapat dan watermarking ini dikembangkan lebih dalam lagi.

REFERENSI

[1] Munir, Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi: Algoritma ElGamal.

[2] Munir, Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi: Fungsi Hash.

[3] Munir, Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi: SHA-3:Kompetensi Fungsi Hash oleh NIST

[4] Munir, Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi: Tanda-tangan Digital .

PERNYATAAN

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

Bandung, 10 Juni 2020

Ivan Fadillah
13516128