Implementasi Gabungan Tanda Tangan Digital RSA dan Steganografi pada Citra Untuk Melindungi Citra yang Mengandung Hak Cipta

Radhinansyah Hemsa Ghaida - 13518087
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
13518087@std.stei.itb.ac.id

***Abstract*—Penyalahgunaan hak cipta terutama hak cipta untuk citra sudah sering terjadi seiring dengan percepatan alur informasi akibat perkembangan teknologi. Hal ini tentunya sangat merugikan para pembuat citra orisinil yang karyanya diambil oleh orang-orang yang tidak bertanggung jawab. Pengaplikasian tanda tangan digital sudah terbukti dapat menjadi bukti absah terkait kepemilikan dokumen. Tanda tangan digital juga bisa diaplikasikan pada citra yang memiliki hak cipta sehingga bukti kepemilikannya bisa didapatkan dengan jelas. Steganografi juga dapat dikombinasikan dengan tanda tangan digital sehingga tanda tangan digital tersebut dapat disisipkan pada citra yang memiliki hak cipta.**

Keywords—Tanda tangan digital, steganografi, LSB, citra, RSA, hash.

I. PENDAHULUAN

Dewasa ini, citra-citra semakin banyak beredar di dunia maya. Citra-citra tersebut mudah sekali diambil dan dipakai oleh orang-orang yang tidak bertanggung jawab untuk kepentingan masing-masing. Hal ini tentu sangat merugikan pembuat citra tersebut karena citra yang seharusnya menjadi hak ciptanya dapat diambil oleh orang yang tidak bertanggung jawab serta dipakai untuk kepentingannya pribadi.

Pengambilan citra secara illegal merupakan hal yang sangat merugikan apabila orang yang mengambil citra tersebut memakainya untuk kepentingan komersial. Banyak orang yang dapat dirugikan dari hal ini terutama para pembuat citra orisinil seperti pelukis dan fotografer.

Salah satu cara untuk menjamin keaslian sebuah dokumen maupun citra adalah dengan penyematan tanda tangan digital pada citra orisinil yang dibuat. Tanda tangan digital tersebut dapat disisipkan pada citra yang ingin dilindungi sehingga keaslian citra tersebut dapat dipertanggung jawabkan. Namun, implementasi tanda tangan digital saja tidak cukup. Hal tersebut perlu dikombinasikan dengan steganografi untuk menyembunyikan bit-bit hasil tanda tangan digital tersebut pada citra sehingga citra yang diberikan tanda tangan digital tersebut tidak rusak.

Oleh Karena itu, pada makalah ini, penulis akan membahas terkait implementasi gabungan tanda tangan digital RSA dan steganografi sebagai metode penyisipan tanda tangan digital tersebut pada citra untuk melindungi hak cipta dari citra tersebut. Dengan menggunakan gabungan tanda tangan digital dan steganografi, keabsahan dan verifikasi dari kepemilikan citra dapat dijamin dan ditelusuri.

II. DASAR TEORI

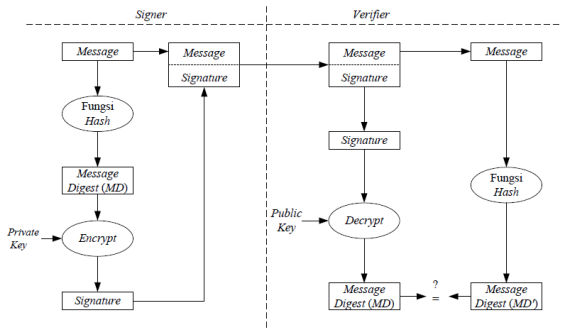
A. *Tanda Tangan Digital*

Tanda tangan digital (*Digital Signature*) merupakan tanda tangan yang diberikan untuk data digital. Tanda tangan digital adalah nilai kriptografis yang bergantung pada isi pesan dan kunci. Tanda tangal digital selalu berbeda-beda antara satu isi dokumen dengan dokumen lain. Tanda tangan digital dan tanda tangan secara umum memiliki beberapa karakteristik, yaitu:

1. Tanda tangan adalah bukti yang otentik.
2. Tanda tangan tidak dapat dilupakan
3. Tanda tangan tidak dapat dipindah untuk digunakan ulang
4. Dokumen yang telah ditandatangani tidak dapat diubah
5. Tanda tangan tidak dapat disangkal

Tanda tangan digital menyelesaikan beberapa masalah keamanan yang disediakan oleh kriptografi yaitu Otentikasi (*authentication*), keaslian pesan (*data integrity*), dan anti-penyangkalan (nonrepudiation).

Salah satu metode penandatanganan digital adalah dengan menggunakan kriptografi kunci-publik dan fungsi hash. Berikut merupakan alur metode penandatanganan digital dengan menggunakan kriptografi kunci-publik dan fungsi hash:



Gambar 1. Alur Tanda-tangan Digital

B. Algoritma Kunci Publik RSA

RSA merupakan algoritma kunci publik yang ditemukan oleh tiga peneliti dari MIT (*Massachussets Institute of Technology*), yaitu Ronald Rivest, Adi Shamit, dan Led Adleman, pada tahun 1976. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan bulat yang besar menjadi faktor-faktor prima. Algoritma RSA memiliki beberapa properti utama sebagai berikut:

1. p dan q bilangan prima (rahasia)
2. n = p . q (tidak rahasia)
3. ..(n) = (p - 1)(q - 1) (rahasia)
4. e adalah kunci enkripsi dengan syarat PBB(e, …(n)) = 1 dan relative prima terhadap ..(n) (tidak rahasia)
5. d adalah kunci dekripsi dimana dihitung dari d kongruen e^{-1} mod (…(n)) (rahasia)
6. m adalah plainteks (rahasia)
7. c adalah cipherteks (tidak rahasia)

Algoritma RSA memiliki persamaan enkripsi dan dekripsi sebagai berikut:

$$Enkripsi: E_e(m) = c = m^e \bmod n \quad (1)$$

$$Dekripsi: D_d(c) = m = c^d \bmod n \quad (2)$$

Algoritma RSA memerlukan sepasang kunci yaitu kunci publik (*e, n*) dan kunci privat (*d, n*). Pembangkitan sepasang kunci tersebut memiliki prosedur pembangkitan sebagai berikut:

1. Pilih dua bilangan prima, p dan q
2. Hitung n = pq
3. Hitung ..(n) = (p - 1)(q - 1)
4. Pilih sebuah bilangan bulat *e* sebagai kunci publik dimana *e* harus relatif prima terhadap ..(n).
5. Hitung kunci dekripsi, d, dengan persamaan ed kongruen 1 (mod ..(n)) atau d kongruen e^{-1} mod (..(n))

C. Fungsi Hash SHA-3

Fungsi *hash* SHA-3 yang dikenal juga dengan nama Kecak merupakan fungsi *hash* yang dibuat oleh Guido Breton, Joan Daemen, Michael Peeters, dan Gilles Van Assche. SHA-3 menggunakan fungsi non-kompresi untuk menyerap dan kemudian mengambil *digest.* Fungsi ini didesain dengan konstruksi spons dimana penyerapan dan pemerasan digest dilakukan. Fungsi *hash* SHA3 ini memiliki 3 fase, yaitu:

1. Preproses

   Pertama, pesan M ditambah dengan bit-bit pengganjal (*padding)* menjadi string P sehingga habis dibadi dengan *r* atau *n* = length (P)/*r*. Selanjutnya, *P* dipotong menjadi blok-blok P_i berukuran r-bit. Kemudian, b-bit dari peubah status S diinisialisasi menjadi nol dan konstruksi spons berlangsung dalam dua fase yaitu fase penyerapan dan fase pemerasan.

2. Penyerapan (*absorbing)*

   Untuk setiap blok masukan P_i berukuran r-bit, XOR-kan dengan r-bit pertama dari *state* S, lalu hasilnya dimasukkan ke dalam fungsi permutasi *f* untuk menghasilkan *state* baru *S*. Bila semua blok masukan selesai diproses, konstruksi spons beralih ke fase pemerasan.

3. Pemerasan (*squeezing*)

   Pada fase pemerasan, *message digest* akan disimpan di dalam Z. Inisialisasi Z dengan string kosong (*null string*). Kemudian, selagi Panjang Z belum sama dengan d, r-bit pertama dari *state* S disamungkan ke Z. Jika Panjang Z masih belum sama dengan *d*, masukkan ke dalam fungsi permutasi *f* menghasilkan *state* baru S.

D. Steganografi

Steganografi adalah ilmu dan seni menyembunyikan pesan rahasian dengan suatu cara sedemikan sehingga tidak seorang pun yang mengetahui keberadaan pesan tersebut. Tujuan dari steganografi adalah agar pesan tidak terdeteksi keberadaannya.

Steganografi digital merupakan penyembunyian pesan digital di dalam dokumen digital lainnya. Dokumen digital yang digunakan sebagai media untuk penyembunyian pesan dapat berupa teks, gambar, audio, dan video. Terdapat beberapa terminologi steganografi digital, yaitu:

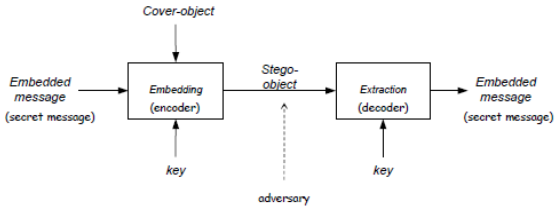
1. *Embedded message* atau *secret* message merupakan pesan yang disembunyikan.
2. *Cover-object* merupakan media digital yang diguanakan untuk menyembunyikan *embedded message*.
3. *Stego-object* yaitu media yang sudah berisi pesan *embedded message.*
4. *Stego-key* yaitu kunci yang digunakan untuk menyisipkan pesan dan mengekstraksi pesan dari stego-object.

Kriteria Steganografi yang baik, yaitu:

1. *Imperceptible*: Keberadaan pesan rahasia tidak dapat dipersepsi secara visual atau secara audial

2. *Fidelity*: Kualitas cover-object tidak jauh berubah akibat penyisipan pesan rahasia
3. *Recovery*: Pesan yang disembunyikan harus dapat diekstraksi kembali
4. *Capacity*: Ukuran pesan yang disembunyikan dapat sebesar mungkin

Berikut merupakan diagram alur proses steganografi:



Gambar 2. Alur Steganografi

Salah satu metode penyisipan pesan pada *cover-obejct* yang paling sering dipakai adalah metode *Least Significany Byte (LSB)*. LSB adalah bit pada sebuah *byte* yang memiliki nilai yang kurang berarti untuk seluruh *byte* tersebut. Jika bit ini dirubah, informasi pada citra tidak akan rusak. Bitplane LSB, yaitu bitplane 0, terlihat seperti citra acak. Bitplane LSB merupakan bagian yang redundan pada citra yang berarti perubahan nilai bit ini tidak mengubah persepsi citra secara keseluruhan. Maka dari itu, metode LSB ini adalah metode yang mengganti bit LSB dari *pixel* dengan bit-bit pesan. Pada citra *true color*, terdapat 24 bit dalam sebuah pixel yang terdiri dari komponen RGB (Red-Green-Blue). Satu pixel dalam citra *true color* memiliki bentuk 8 bit Red, diikuti dengan 8 bit Green, dan diikuti dengan 8 bit Blue, sehingga setiap *pixel* berukuran 3 *byte*. Metode LSB pada citra *true color* adalah dengan mengubah bit LSB pada setiap *byte* RGB dalam sebuah *pixel*. Untuk mengekstraksi pesan dari *stego-image* kita hanya perlu membaca *byte-byte* di dalam citra, mengambil bit-bit LSBnya, dan merangkainya kembali menjadi bit-bit pesan.

III. Rancangan Solusi dan Implementasi

Pada bagian ini, akan dibahas terkait rancangan solusi yang akan dibuat dan implementasi dari rancangan solusi.

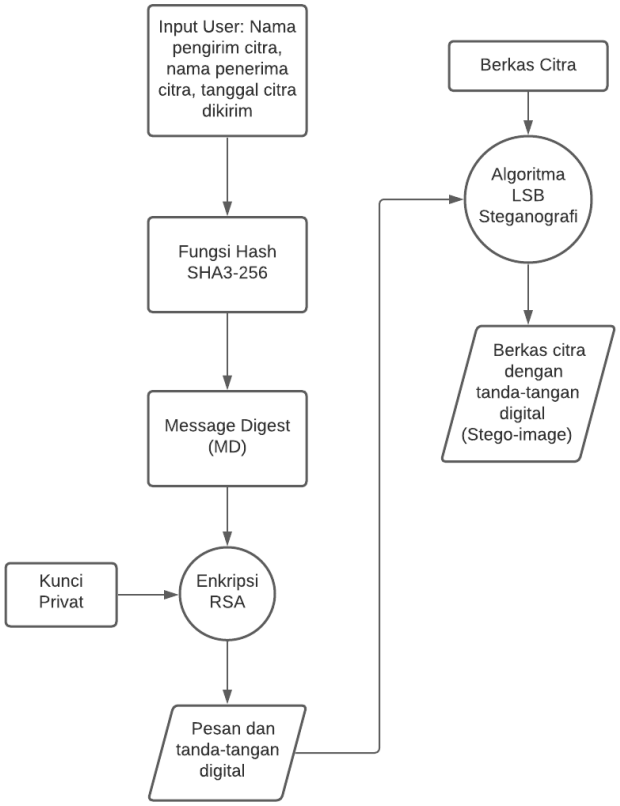
A. Rancangan Solusi

Pembangkitan berkas digital terdiri dari empat tahap yaitu pembentukan tanda tangan digital, penyisipan tanda tangan digital pada citra menggunakan steganografi, pengambilan tanda tangan digital dari citra menggunakan steganografi, dan verifikasi tanda tangan digital.

Pembangkitan kunci yang dilakukan menggunakan algoritma kunci publik RSA dengan jumlah bit yaitu 4096. Dari tahap ini akan dihasilkan kunci publik dan kunci privat yang telah terenkripsi.

Selanjutnya, pada tahap pembentukan tanda tangan digital, akan dihasilkan sebuah tanda tangan digital dengan format hex. Pada tahap ini, user akan diminta data yaitu nama pengirim gambar, nama penerima gambar, dan tanggal gambar dikirim. Hal ini bertujuan untuk menjadi bukti keabsahan dari penerima gambar yang memiliki hak untuk memakai gambar tersebut. Ketiga bukti keabsahan tersebut yang akan dijadikan pesan yang ditanda tangani secara digital. Penyematan tanda tangan digital ini menggunakan algoritma RSA serta SHA3-256.

Setelah itu, pada tahap penyisipan tanda tangan digital pada citra menggunakan steganografi, dilakukan penyisipan dari pesan dan tanda tangan digital pada tahap sebelumnya Penyisipan tanda tangan digital ini menggunakan metode *least significat byte*. Dari tahap ini akan dihasilkan sebuah stego-image yaitu gambar yang telah dilakukan penyisipan pesan dan tanda tangan digital, serta panjang dari pesan dan tanda tangan digital tersebut. Berikut merupakan *flow* dari pembentukan tanda tangan digital dan penyisipan tanda tangan digital pada citra:

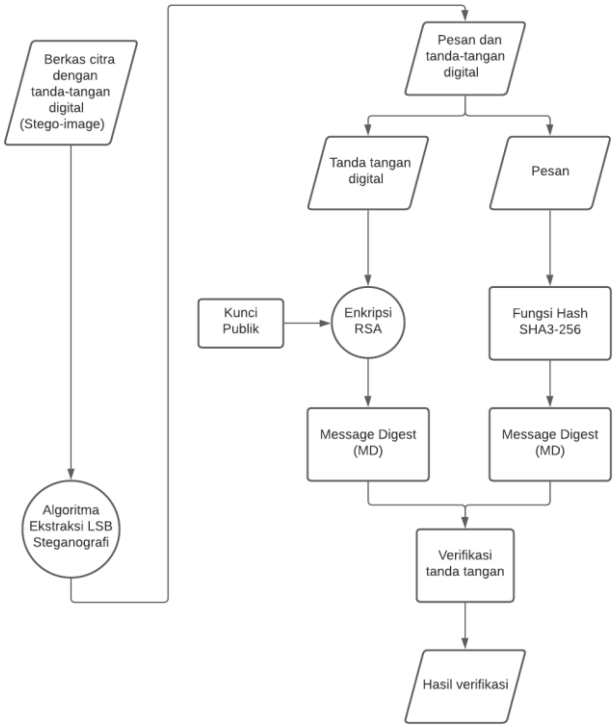


Gambar 3. Alur rancangan solusi pembentukan dan penyisipan tanda tangan digital

Kemudian, pada tahap pengambilan tanda tangan digital dari citra menggunakan steganografi, dilakukan ekstraksi pesan dari stego-image yang ada. Pengambilan pesan dan tanda tangan digital tersebut dilakukan dengan mengambil bit-bit terakhir pada stego-image sepanjang 8 kali panjang pesan dan tanda tangan digital yang disematkan. Dari tahap ini, akan dihasilkan pesan serta tanda tangan digital.

Terakhir, pada tahap verifikasi tanda tangan digital, akan dilakukan verifikasi keabsahan terkait pesan dan tanda tangan digital yang telah diekstraksi sebelumnya. Pada tahap ini akan

dilakukan pemisahan terhadap pesan dan tanda tanda digital. Dilakukan hashing terhadap pesan menggunakan algoritma SHA3-256 lalu akan dilakukan pembandingan angtara hasil hashing pesan tersebut dengan tanda tangan digital yang ada. Dari tahap ini akan dihasilkan 2 hal yaitu pesan dan tanda tangan digital yang disematkan serta verifikasi apakah pesan dan tanda tangan digital tersebut sudah diubah atau belum. Berikut merupakan *flow* dari pengambilan pesan dan tanda tangan digital dari citra dan verifikasi tanda tangan digital:



Gambar 4. Alur rancangan solusi pengambilan dan verifikasi tanda tangan digital

B. Implementasi

Rancangan solusi yang telah dijabarkan pada bagian sebelumnya akan diimplementasikan menjadi sebuah program menggunakan bahasa *Python*. Secara keseluruhan, program ini menggunakan *library* PyCryptodrome yang sudah memiliki algoritma pembangkitan kunci publik RSA, hashing menggunakan SHA3-256 serta penyematan tanda tangan digital menggunakan algoritma RSA dan verifikasi tanda tangan digital menggunakan algoritma RSA. Program ini mengimplementasikan lima tahap yang telah dijabarkan sebelumnya pada bagian rancangan solusi.

Pembangkitan berkas digital terdiri dari empat tahap yaitu pembentukan tanda tangan digital, penyisipan tanda tangan digital pada citra menggunakan steganografi, pengambilan tanda tangan digital dari citra menggunakan steganografi, dan verifikasi tanda tangan digital. Pada tahap pembangkitan kunci, program akan melihat apakah pengguna telah memiliki file berisi kunci publik dan kunci privat atau belum. Jika sudah, maka tidak dilakukan pembangkitan kunci. Namun, jika belum ada, maka akan dilakukan pembangkitan kunci dan dihasilkan dua buah file baru yaitu “privkey.pem” yang berisi kunci privat yang telah dienkripsi dan “pubkey.pem” yang berisi kunci publik yang telah dienkripsi.

Selanjutnya, pengguna akan diminta untuk memasukkan berkas citra yang ingin diberikan tanda tangan. Lalu, pengguna juga akan diminta keterangan terkait nama pengirim, nama penerima, serta tanggal citra dikirimkan ke penerima. Ketiga keterangan tersebut dijadikan sebuah string. String tersebut yang menjadi pesan pada tanda tangan digital. Selanjutnya, dilakukan pembentukan tanda tangan digital menggunakan library PKCS1_v1_5 dan library SHA256. Dari bagian ini, program akan menghasilkan sebuah string pesan dan tanda tangan digital yang berbentuk hex dimana tanda tangan digital tersebut dipisahkan oleh tanda ‘<ds>’ dari pesan.

Selanjutnya, tahap penyisipan tanda tangan digital pada citra menggunakan steganografi, digunakan library cv2 untuk mengakses berkas citra. Berkas citra yang dapat diakses yaitu berkas citra dengan format ‘.png’. Pesan terlebih dahulu akan diubah ke bentuk binary lalu disematkan pada *least significant byte* sebanyak panjang pesan dari citra. Dari tahap ini akan dihasilkan sebuah stego-image dengan nama “stegano.png”.

Pada tahap pengambilan tanda tangan digital dari citra menggunakan steganografi, pengguna akan diminta memasukan stego-image yang telah disematkan tanda tangan serta panjang dari pesan dan tanda tangan digital yang akan diesktraksi. Pada tahap ini, akan dihasilkan ekstraksi pesan berbentuk string berisi pesan dan tanda tangan digital dari *lsb stego-image* sepanjang 8 kali panjang pesan dan tanda tangan digital.

Pada tahap terakhir yaitu, tahap verifikasi tanda tangan digital, tanda tangan digital yang telah diambil akan diverifikasi menggunakan kunci publik yang sebelumnya telah dibentuk. Jika tanda tangan digital berhasil diverifikasi, maka akan keluar ouput “Signature is Valid!”. Namun, jika tanda tangan gagal diverifikasi, maka akan keluar output “No, the message was signed with the wrong private key or has been modified”.

IV. PENGUJIAN DAN PEMBAHASAN

Pada bagian ini, akan dibahas terkait pengujian dan pembahasan dari program yang telah dibuat. Pada pengujian ini diceritakan bahwa seorang pembuat citra bernama radhin akan mengirimkan lukisannya kepada seorang pelanggan bernama gita yang telah membayar uang untuk citra tersebut. Citra tersebut akan dikirimkan pada tanggal 20 Desember 2021. Pengujian terdiri dilakukan sebanyak 3 kali yaitu sebuah pengujian valid, sebuah pengujian yang gagal akibat citra diubah (disunting), dan pengujian yang gagal akibat tanda tangan digital yang diganti. Pada pengujian ini, terdapat beberapa variabel yang digunakan yaitu sebagai berikut:

Variabel	**Nilai**
Kunci Publik hasil pembangkitan	-----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDViab/Bk80g6t9w19rpKkUQOsJ

	xQw5B3KuY0spmjO2lP3ezxF8vy6CUZc8AvhGZsDwdZcIBfvF8PBwvHuZ1tgl62sn+e6VoIkK3moz69sDCrjMmenZAl3r1iQpNg5dnoOsIjCiJKLp01KqajwpZeO84GuODSlbAw1ZhDhfnKm8hwIDAQAB -----END PUBLIC KEY-----
Kunci Privat hasil pembangkitan	-----BEGIN RSA PRIVATE KEY----- MIICXAIBAAKBgQDViab/Bk80g6t9w19rpKkUQOsJxQw5B3KuY0spmjO2lP3ezxF8 vy6CUZc8AvhGZsDwdZcIBfvF8PBwvHuZ1tgl62sn+e6VoIkK3moz69sDCrjMmenZAl3r1iQpNg5dnoOsIjCiJKLp01KqajwpZeO84GuODSlbAw1ZhDhfnKm8hwIDAQAB AoGAWvVDmSYK3wenKO7r2mJNUz9D3ul8h15Qz0+kWJhCpudYLGxvun+FRCWVEg8B yptCXCr6poRF9s7m3F6tF56Yeub10MYauZv92g6dvkbwrNmbspfe31lPg4is85KD 9Nkc33D4cXqwE+4KXW1Jo/YsKkF2zfuq/8ePAQmepPlH0UECQQDbrPw4aUppfpfp nOR4Lcv5Em2CuftM7V4ri/aWpmIS1dAZ4XnIOgWyrykf82BlCSIt6rXOqWFiHvc0 +NS3WLuPAkEA+NjXPhh2Zp8jD0mwZQzh36Xkiq75eZX/Vy0or9gDfuXwvZcRS9oj trfePoSjS+cunmRijBvgXkrHeKodecJTiQJBAMgwBQ03TluCxNdcZYvrWCUbmPZ3 m74H1jhi7Q1uhJNbi6/6HOvNjGHAY/684ExSnXYwnQu+qYMsauU4GUkYMJsCQHaT 9XUceQcLm8xEI+7zBYrp5Q6EtFJQvJzQ4wtv1rKYZXAiVVacutntodSOpbWckuVdFmyHOBIWdhi0j1ke1WkCQBWrdIdFAvrZ862ISH0bpHlxY42W/z2EgGDAgcDoN4Iv jD9HWBpPrUHZNd5aA31Hp56PTEJCzYr8zQtmk0s6O7A= -----END RSA PRIVATE KEY-----
Nama pengirim	radhin
Nama penerima	gita
Tanggal pengiriman gambar	20-12-2021

Pengujian ini memakai sebuah citra “image.png” dengan bentuk sebagai berikut:

Gambar 5. Citra “image.png” yang akan disisipkan pesan dan tanda tangan digital

A. Pengujian Umum

Pada tahap pengujian ini dilakukan pengujian yang berhasil terhadap verifikasi tanda-tangan digital. Penyematan tanda tangan digital dilakukan dengan melakukan tanda-tangan terhadap pesan:

radhin
gita
20-12-2021

Setelah dilakukan tanda tangan, didapatkan tanda-tangan digital sebagai berikut:

56cf10b0947ff139c4060d8a2a2f8e1769bec12489602687aae
159a7984fc181b82e4edd798b88a349b1287a9efed4b3a1e221
e1e0415e3fab54cf3588a987ab55a6ae2cf234cf81b44aeeed9b
068ab28792beb01c79720f005fcdba54d9cb48f6a06d6bcf6e8
8446b854274cfa8ba3f1c97013f42367a443c026fc5b3f1cd58

Setelah itu, didapatkan pesan dan tanda tangan digital yang akan disembunyikan pada stego-object yaitu sebagai berikut:

radhin
gita
20-12-2021
<ds>56cf10b0947ff139c4060d8a2a2f8e1769bec124896026
87aae159a7984fc181b82e4edd798b88a349b1287a9efed4b3
a1e221e1e0415e3fab54cf3588a987ab55a6ae2cf234cf81b44
aeeed9b068ab28792beb01c79720f005fcdba54d9cb48f6a06
d6bcf6e88446b854274cfa8ba3f1c97013f42367a443c026fc5
b3f1cd58</ds>

Dari penyematan tanda-tangan digital dan pesan tersebut, didapatkan sebuah stego-image dengan nama “stegano.png” sebagai berikut:

Gambar 6. Citra “stegano.png” hasil penyipisan pesan dan tanda tangan digital

Dapat dilihat bahwa penyematan tanda-tangan digital dan pesan pada citra tidak merubah bentuk visual yang dapat dikenali oleh mata manusia secara umum dari citra tersebut.

B. Pengujian Valid

Pada pengujian ini dilakukan ekstraksi terhadap pesan dan tanda tangan digital dari stego-image “stegano.png”. Dari hasil ekstraksi pesan dan tanda tangan digital dengan panjang pesan yaitu 288, didapatkan hasil sebagai berikut:

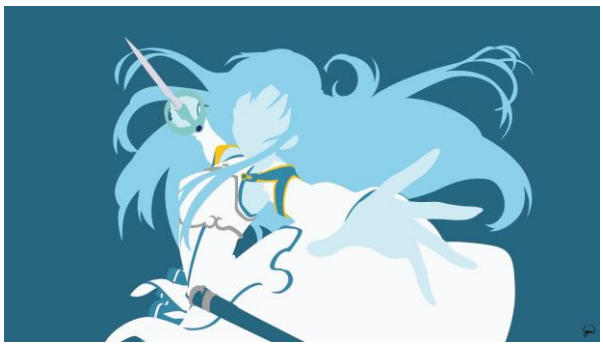
```
radhin
gita
20-12-2021
<ds>56cf10b0947ff139c4060d8a2a2f8e1769bec124896026
87aae159a7984fc181b82e4edd798b88a349b1287a9efed4b3
a1e221e1e0415e3fab54cf3588a987ab55a6ae2cf234cf81b44
aeeed9b068ab28792beb01c79720f005fcdba54d9cb48f6a06
d6bcf6e88446b854274cfa8ba3f1c97013f42367a443c026fc5
b3f1cd58</ds>
```

Tanda tangan digital tersebut kemudian dipisahkan dari pesannya berdasarkan tanda ‘<ds>’. Kemudian dilakukan verifikasi terhadap tanda tangan digital dan pesan dan didapatkan hasil dari program sebagai berikut:

```
Signature is Valid!
```

C. Pengujian Gagal Akibat Citra Disunting

Pada pengujian ini dilakukan ekstraksi terhadap pesan dan tanda tangan digital dari stego-image “stegano1.png”, dimana citra tersebut merupakan citra “stegano.png” yang dilakukan perubahan warna. Citra tersebut memiliki bentuk sebagai berikut:



Gambar 6. Citra “stegano.png” yang dilakukan perubahan warna

Dari hasil ekstraksi pesan dan tanda tangan digital dengan panjang pesan yaitu 288, tidak didapatkan apapun karena dengan dilakukannya perubahan terhadap warna, maka pesan didalamnya juga berubah. Program kemudian memberikan output sebagai berikut

```
There is no digital signature or your image has been changed
```

D. Pengujian Gagal Akibat Tanda-tangan Digital Diubah

Pada pengujian ini dilakukan ekstraksi terhadap pesan dan tanda tangan digital dari stego-image “stegano.png”. Dari hasil ekstraksi pesan dan tanda tangan digital dengan panjang pesan yaitu 288, didapatkan hasil sebagai berikut:

```
radhin
gita
20-12-2021
<ds>56cf10b0947ff139c4060d8a2a2f8e1769bec124896026
87aae159a7984fc181b82e4edd798b88a349b1287a9efed4b3
a1e221e1e0415e3fab54cf3588a987ab55a6ae2cf234cf81b44
aeeed9b068ab28792beb01c79720f005fcdba54d9cb48f6a06
d6bcf6e88446b854274cfa8ba3f1c97013f42367a443c026fc5
b3f1cd57</ds>
```

Tanda tangan digital tersebut kemudian dipisahkan dari pesannya berdasarkan tanda ‘<ds>’. Kemudian dilakukan verifikasi terhadap tanda tangan digital dan pesan dan didapatkan hasil dari program sebagai berikut:

```
No, the message was signed with the wrong private key or has been modified!
```

E. Pembahasan

Dari hasil pengujian yang dilakukan, didapatkan beberapa hasil dengan pambahasan sebagai berikut:

1. Pengujian Valid

   Dari pengujian ini didapatkan hasil “Signature is Valid!” dimana program berhasil memberikan

kesimpulan bahwa citra tersebut dapat dibuktikan validitas dan autentikasinya karena bersumber dari pengirim gambar secara langsung.

2. Pengujian Gagal Akibar Citra Disunting

   Dari pengujian ini, didapatkan hasil yaitu “There is no digital signature or your image has been changed”. Hal tersebut diakibatkan oleh perubahan pada citra sehingga byte-byte RGB pada citra berubah. Dengan begitu, ekstraksi dari pesan dan tanda tangan digital gagal. Hal ini akan sangat bermanfaat bagi para penjual maupun pengedar citra secara *online* karena banyak karya-karya mereka yang sering diubah oleh orang-orang yang tidak bertanggung jawab dan tidak terlacak.

3. Pengujian Gagal Akibat Tanda-tangan Digital Diubah

   Dari pengujian ini, didaptkan hasil yaitu “No, the message was signed with the wrong private key or has been modified!”. Hal tersebut diakibatkan oleh tanda tangan digital yang diekstraksi pada stego-image telah diubah.

V. KESIMPULAN DAN SARAN

Implementasi gabungan tanda-tangan digital menggunakan kunci publik RSA serta steganografi terbukti dapat dilakukan untuk membuktikan keabsahan terkait kepemilikan citra. Hal tersebut sangat bermanfaat di era *modern* ini dimana banyak sekali pencurian citra dengan maupun tanpa hak cipta sehingga sangat merugikan bagi para pembuat citra original. Para pencuri citra tersebut dapat melakukan penyuntingan terhadap citra yang bukan mereka miliki dan mengklaim kepemilikan citra tersebut. Dengan adanya program ini, diharapkan para pembuat citra original dapat dengan lebih aman melakukan pengiriman citranya kepada orang-orang yang memiliki hak untuk mengakses citra tersebut dan dapat membuktikan kepemilkan citra-citra miliknya yang beredar di internet secara bebas.

Program yang penulis bangun merupakan program yang sangat sederhana sehingga penulis memiliki saran pengembangan untuk kedepannya, program ini dapat diintegrasikan kepada *website* jual beli citra secara *online* baik yang dimiliki oleh organisasi maupun perseorangan, sehingga dapat bermanfaat secara luas terutama bagi para pembuat citra orisinil.

UCAPAN TERIMAKASIH

Ucapan terimakasih penulis nyatakan kepada Allah SWT, karena berkat rahmat serta karunia-Nya penulis bisa diberikan kekuatan dan ilmu untuk menyelesaikan makalah ini.

Penulis juga mengucapkan terimakasih kepada Bapak Dr. Ir. Rinaldi Munir, MT selaku dosen mata kuliah IF4020 Kriptografi yang telah memberikan ilmu yang sangat bermanfaat kepada penulis dan rekan-rekan penulis selama keberlangsungan mata kuliah ini. Tidak lupa, penulis juga mengucapkan terimakasih kepada rekan-rekan mata kuliah IF4020 yang sudah berjuang bersama-sama dengan penulis untuk menimba ilmu dan menyelesaikan mata kuliah ini.

REFERENCES

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

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

[3] Munir, Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi: SHA-3 (Kecak)

[4] Munir, Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi: Steganografi (Bagian 1)

[5] Munir, Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi: Steganografi (Bagian 2).

[6] 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 saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 20 Desember 2021

Radhinansyah Hemsa Ghaida
13518087