Sistem Penandatanganan Berkas Citra Menggunakan Steganografi dan ECDSA

Ahmad Rizqee Nurhani - 13517058
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13517058@std.stei.itb.ac.id

***Abstract*—Steganografi adalah sebuah teknik yang dapat digunakan oleh seseorang untuk menyembunyikan sebuah pesan atau berkas dalam media lain. Steganografi citra adalah penyembunyian pada media gambar. Tanda tangan digital adalah sebuah tanda tangan elektronik yang dapat digunakan untuk membuktikan keaslian identitas pemilik sebuah berkas. Dengan menggunakan teknik steganografi diharapkan sebuah tanda tangan digital dapat disisipkan kedalam sebuah media citra agar keaslian media tersebut dapat dibuktikan.**

***Keywords*—ECDSA, LSB, penyisipan, tanda tangan, citra, Keccak.**

I. PENDAHULUAN

Pada jaman sekarang teknologi telah berkembang dengan pesat. Penyebaran informasi terjadi degan sangat cepat dan hanya dengan membuka sebuah aplikasi *browser* dan melakukan pencarian pada *search bar* seseorang dapat dengan mudah mendapatkan informasi yang diinginkan oleh orang tersebut. Penyebaran informasi dalam bentuk digital menjadi cara utama dalam penyampaian informasi dikarenakan media internet yang dapat diakses oleh hampir semua orang dan dapat menyebarkan banyak informasi dengan cepat.

Dengan berkembangnya internet, penyebaran media citra seperti gambar, ilustrasi, foto, atau media citra lainnya banyak dilakukan oleh manusia. [1] Berdasarkan statistik instagram, hampir 95 juta foto di unggah pada platform tersebut. Dapat dikatakan bahwa pengungahan media citra dilakukan oleh banyak orang. Informasi yang disebarkan melalui media citra dapat mengandung informasi penting sehingga keaslian dari sebuah media citra harus dapat dipastikan.

Selain sebagai saran informasi, sebuah media citra berupa ilustrasi dapat digunakan sebagai sarana nafkah. Ilustrasi dapat dijual oleh ilustrator dengan harga yang cukup tinggi. Karena media citra ini merupakan sarana nafkah dari ilustrator, keaslian media diperlukan agar pembeli ilustrasi dapat menjamin keaslian dari ilustrasi yang telah dibeli.

Menentukan keaslian sebuah media citra dapat dilakukan dengan berbagai cara. Pemilik media citra dapat memberikan *watermark* atau penanda pada media tersebut untuk menyatakan bahwa media tersebut memiliki pemilik. Tentu saja teknik ini memiliki kekurangan yaitu, jika *watermark* diletakkan dalam media citra, maka *watermark* tersebut dapat merusak media. Jika *watermark* diletakkan di luar ata di *border* media citra maka *watermark* tersebut akan mudah dihilangkan. Oleh sebab itu dibutuhkan sebuah cara untuk menandai sebuah media citra tanpa merusak media.

Cara yang dapat dilakukan untuk menjamin keaslian sebuah citra adalah dengan menyisipkan sebuah tanda tangan digital dalam citra. Penyisipan ini dapat dilakukan dengan menggunakan teknik steganografi. Dengan melakukan penyisipan, sebuah isi dari sebuah citra tidak akan terlihat rusak dan informasi yang disampaikan oleh citra dapat dipastikan asli dengan melakukan pencocokan tanda tangan digital.

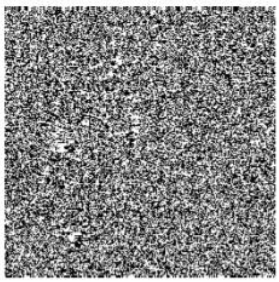
Dalam makalah ini, penulis akan menggunakan sebuah teknik steganografi citra yang bernama LSB sekuensial dalam menyisipkan tanda tangan dan ECDSA dalam pembangkitan tanda tangan. Teknik tersebut dipakai karena ECDSA dan LSB merupakan salah satu teknik paling umum yang dapat digunakan dalam penandatanganan digital dan steganografi. Dalam algoritma ECDSA fungsi *hash* yang akan dipakai penulis adalah fungsi Keccak.

II. DASAR TEORI

A. Steganografi Citra

Steganografi adalah sebuah ilmu atau seni menyembunyikan sebuah pesan rahasia sedemikian sehingga tidak seorangpun yang mengetahui keberadaan pesan tersebut. Tujuan dari steganografi adalah agar sebuah pesan tidak terdeteksi keberadaannya. Steganografi berbeda dengan kriptografi dimana steganografi bertujuan menghilangkan keberadaan sebuah informasi sehingga pihak ketiga tidak akan sadar terhadap keberadaan pesan tersembunyi pada sebuah pesan steganografi. Sedangkan pada kriptografi pihak ketiga akan dapat dengan mudah melihat bahwa terdapat pesan tersembunyi pada pesan kriptografi. Dalam pengaplikasian steganografi pada media digital, penyembunyian pesan rahasia dapat dilakukan dengan cara mengubah LSB berkas yang digunakan sebagai media berkas rahasia.

LSB atau least significant bit adalah bit pada sebuah byte yang kurang berarti. Bit ini jika dirubah tidak akan merusak informasi yang ingin disampaikan oleh sebuah berkas. Pada sebuah citra, bit LSB akan menggambarkan sebuah bitplane acak seperti gambar dibawah.



Gambar 1. bitplane LSB sebuah berkas citra

bitplane tersebut merupakan sebuah bagian redundan pada sebuah berkas citra, sehingga perubahan pada LSB tidak akan mengubah persepsi sebuah citra kepada mata seseorang pengamat.

Steganografi citra adalah pengaplikasian steganografi pada media citra. Pada pengaplikasian steganografi ini LSB yang diubah merupakan LSB pada pixel-pixel citra. Pada dasarnya sebuah citra tersusun dari sejumlah pixel. Pixel-pixel ini memiliki ukuran tertentu. Sebagai contoh sebuah citra yang memiliki warna mempunyai pixel dengan ukuran 24 bit. Bit pixel tersebut tersusun dari komponen merah, hijau dan biru (RGB). Sebagai contoh pada bit pixel

10010011100101001000101010

8 bit pertama dari pixel menentukan warna merah, 8 bit kedua dari pixel tersebut menentukan warna hijau, dan 8 bit terakhir menentukan warna biru. Pada steganografi citra LSB dari byte merah, hijau dan biru pad pixel akan digunakan untuk menyimpan informasi mengenai berkas yang ingin disembunyikan.

B. Tanda Tangan Digital

Tanda tangan digital adalah sebuah metode otentikasi menggunakan prinsip kriptografi yang dapat digunakan oleh penerima sebuah pesan untuk memastikan kebenaran pesan yang diterima. Tanda tangan digital memenuhi tiga prinsip kriptografi. Prinsip-prinsip tersebut adalah:

1. Otentikasi
   Tanda tangan digital dapat digunakan dalam menentukan apakah pengirim pesan merupakan pengirim sebenarnya atau bukan.
2. Keaslian pesan
   Tanda tangan digital dapat digunakan untuk menentukan apakah sebuah pesan atau berkas telah dibuah atau tidak.
3. Anti-penyangkalan
   Tanda tangan digital dapat digunakan untuk mencegah pengirim pesan atau berkas dari menyangkal bahwa mereka telah mengirim pesa atau berkas tersebut.

C. ECDSA

ECDSA atau Elliptic Curve Digital Signiture Algorithm sebuah metode pembangkitan tanda tangan digital menggunakan algoritma matematis kurva eliptik (ECC). Penggunaan ECC pada penandatanganan dapat memenuhi tiga prinsip kriptografi yang dimiliki oleh sebuah tanda tangan digital. Hal ini dikarenakan ECC merupakan sebuah algoritma kunci publik sehingga pengkonfirmasian tanda tangan dapat dilakukan oleh penerima pesan tersebut menggunakan kunci publik yang dimiliki oleh penerima pesan. Selain itu ECC dibandingkan dengan kunci publik lain seperti RSA dan ElGamal memiliki panjang kunci yang lebih pendek sehingga komputasi yang diperlukan untuk menentukan keaslian tanda tangan tidak sebesar algoritma RSA dan ElGamal.

Dalam pembangunan sebuah algoritma ECDSA diperlukan sebuah parameter domain kurva eliptik berupa *D = {a,b,G,p,n}*. Nilai-nilai pada domain kurva tersebut dapat diisi menggunakan standar domain kurva seperti *secp256k1*. Untuk mengembangkan ECDSA terdapat 3 hal yang harus diimplementasi. Hal-hal tersebut adalah:

1. Pembangunan kunci
   Pada tahap ini dilakukan pembangkitan sebuah kunci publik dan kunci privat untuk pembuatan tanda tangan. Kunci publik adalah sebuah bilangan bulat acak yang akan digunakan untuk membangun tanda tangan. Kunci privat adalah sebuah koordinat (x,y) yang akan digunakan untuk memverifikasi tanda tangan tersebut.
   Tahap-tahap pada proses pengembangan kunci adalah sebagai berikut:
   a. Memilih sebuah bilangan random d_a yang memiliki nilai diantara [1,n-1] sebagai kunci privat.
   b. Menghitung Q_a dengan cara
      $$Q_a = d_a.G = (x_1, y_1)$$
      Q_a adalah kunci publik.
2. Penandatanganan
   Sebuah pesan akan diubah menjadi bentuk yang lebih ringkas menggunakan sebuah fungsi hash. Pesan yang telah diubah ini tidak dapat diubah menjadi bentuk semula walaupun menggunakan kunci dan algoritma yang sama. Pesan ini akan dienkripsi menggunakan kunci privat milik pengirim untuk menghasilkan tanda tangan digital. Biasanya tanda tangan ini nanti akan ditambahkan kedalam sebuah pesan yang akan dikirim.
   Tahap-tahap pada proses penandatanganan adalah sebagai berikut:
   a. Memilih sebuah bilangan random k yang memiliki nilai diantara [1,n-1]
   b. Menghitung Q_a dengan cara
      $$Q_a = k.G = (x_1, y_1)$$
      Menghitung nilai r yaitu,
      $$r = x_1 \bmod n$$
   c. Menghitung
      $$d_a^{-1} \bmod n$$
   d. Menghitung hash dari massage awal, e, dengan cara
      $$e = Hash(m)$$
   e. Menghitung nilai s yaitu,
      $$s = d_a^{-1}(e + d_a.r) \bmod n$$
   f. Tanda tangan digital adalah (r,s)
3. Verifikasi tanda tangan
   Tanda tangan akan diverifikasikan dengan cara melakukan dekripsi pada tanda tangan dengan menggunakan kunci publik. Hasil dekripsi tersebut merupakan sebuah bilangan bulat yang seharusnya merupakan hasil *hashing* dari pesan yang ingin dikirimkan. Verifikasi dilakukan dengan mencocokan nilai hash dari dekripsi dengan nilai hash pesan. Jika hasil sama maka dapat dikatakan bahwa isi pesan tidak diubah.
   Tahap-tahap pada proses verifikasi adalah sebagai berikut:
   a. Memverifikasi bahwa r dan s adalah bilangan bulat yang antara [1,n-1]

b. Menghitung hash dari massage, e, dengan cara
$$e = Hash(m)$$

c. Menghitung nilai
$$w = s^{-1} \, mod \, n$$

d. Menghitung u_1 dan u_2 dengan cara
$$u_1 = e.w \, mod \, n$$
$$u_2 = r.w \, mod \, n$$

e. Menghitung
$$u_1.G + u_2.Q_A = (x_1, y_1)$$

f. Menghitung
$$v = x_1 \, mod \, n$$

g. Jika nilai v sama dengan nilai r maka tanda tangan valid

Penjelasan mengenai implementasi ECDSA akan dijelaskan pada subbab implementasi.

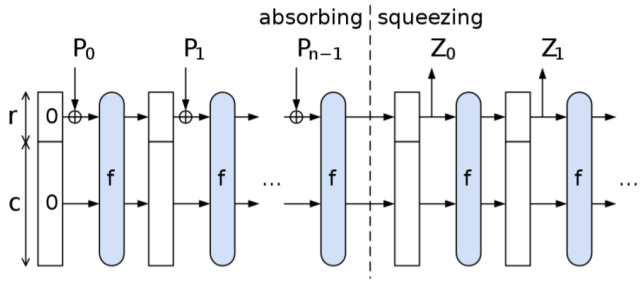
D. Fungsi Hash Keccak

Fungsi hash merupakan sebuah fungsi yang dapat digunakan untuk mengubah ukuran sebuah pesan agar menjadi lebih ringkas. Fungsi hash merupakan sebuah fungsi satu arah dimana pesan yang masuk setelah diubah oleh sebuah fungsi hash tidak dapat dikembalikan kebentuk semula.

Fungsi hash keccak atau yang biasa disebut dengan SHA3 merupakan sebuah fungsi hash yang dihasilkan oleh kompetisi pembuatan fungsi hash yang diselenggarakan NIST pada tahun 2007. Fungsi ini dibuat oleh Guido Breton, Joan Daemen, Michael Peeters, dan Gilles Van Assche. Fungsi ini didesain dengan konstruksi spons dimana penyerapan dan pemerasan digest dilakukan. Fungsi hash memiliki 3 fase. Fase itu adalah

1. Preproses
   - Misalkan panjang sebuah digest yang diinginkan adalah d bit
   - Pertama pesan M ditambah dengan bit-bit pengganjal menjadi sebuah string P shingga panjang P tersebut akan habis dibagi dengan sebuah nilai r, dimana r adalah *bitrate*
   - Selanjutnya P akan dipotong-potong menjadi balok-balok P_i berukuran r-bit
   - Kemudian b-bit dari dari sebuah peubah status S diinisialisasikan menjadi nol. Nilai b didapatkan dari menjumlahkan nilai r dengan sebuah konstanta kapasitas yang bernama c.
   - Setelah langkah diatas dilaksanakan langkah berikutnya dilakukan pada fase penyerapan.
2. Penyerapan
   - Untuk setiap blok masukan P_i berukuran r-bit, XOR-kan dengan r-bit pertama dari status S, lalu hasilnya dimasukkan kedalam fungsi permutasi f untuk menghasilkan status baru S.
   - Lakukan langkah diatas menggunakan status S sampai seluruh blok P_i selesai diproses.
   - Setelah semua blok masukan diproses, proses berlanjut ke fase pemerasan.
3. Pemerasan
   - Inisialisasi sebuah string kosong bernama Z.
   - Append r-bit pertama dari status S kedalam string Z.
   - Jika panjang string Z masih belum sama dengan nilai d masukkan string Z ke fungsi permutasi f untuk menghasilkan status S baru.

Gambar dibawah merupakan ilustrasi sebuah fungsi hash keccak.

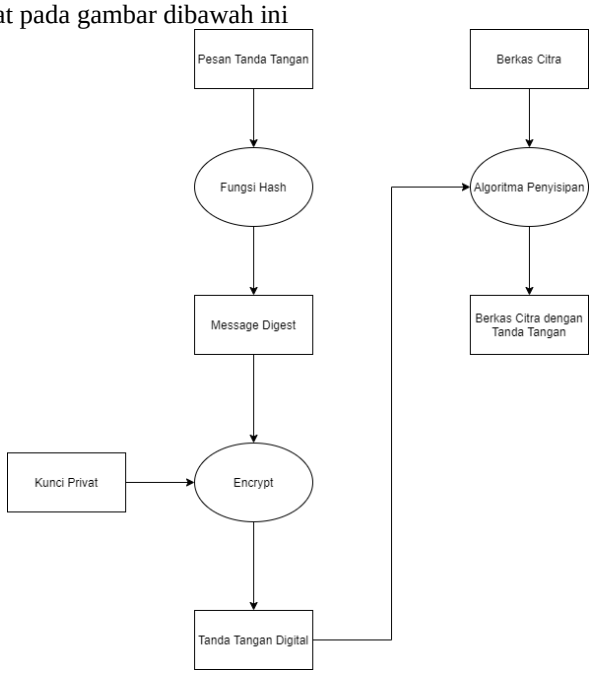


Gambar 2. Ilustrasi fungsi keccak

III. IMPLEMENTASI

A. Rancangan Sistem

Penandatanganan berkas citra terdiri dari dua tahap yaitu, pembangkitan tanda tangan dan penyisipan tanda tangan. Pada pembangkitan tanda tangan, algortima yang akan dipakai adalah algoritma ECDSA dengan fungsi hash berupa fungsi keccak. Pada penyisipan tanda tangan dalam sebuah berkars citra, teknik steganografi yang akan dipakai adalah penyisipan pada LSB secara sequensial. Ilustrasi proses penandatanganan dapat dilihat pada gambar dibawah ini



Gambar 3. Diagram proses penandatanganan

Dalam pengimplementasian fungsi hash Keccak, konstanta yang dipakai merupakan standar SHA3-256 yang memiliki parameter:

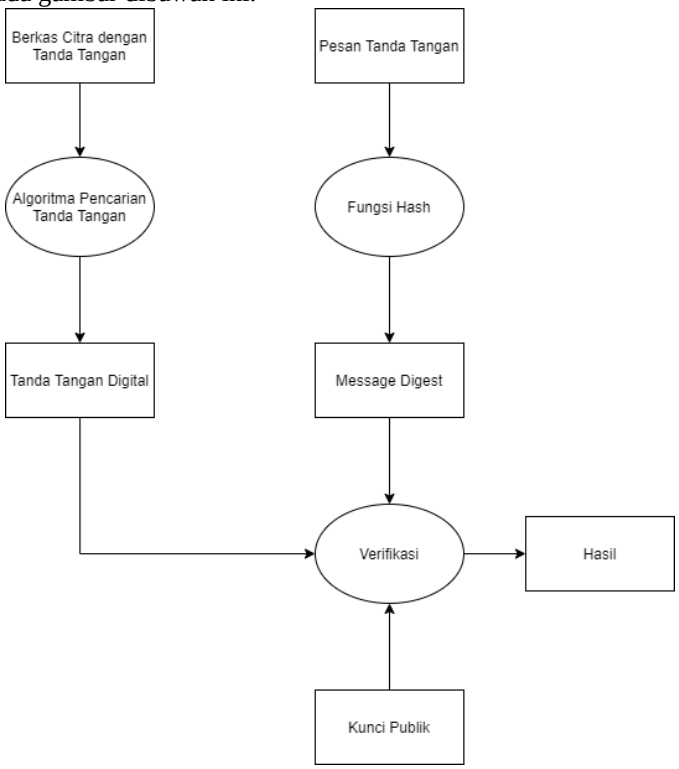
1. r = 1088
2. c = 512
3. Output = 256 bits
4. d = 0x06
5. Fungsi permutasi adalah *Round Constants*. Fungsi ini menggunakan round function yang sama dengan

spesifikasi asli pada algoritma Keccak menggunakan 3 buah intermediary variables, fungsi XOR, dan fungsi cyclic left shift. Round function ini akan dilakukan sebanyak 24 kali mengikuti standar untuk r + c = 1600.

Dalam pengimplementasian algoritma ECDSA, domain kurva eliptik yang digunakan adalah *secp256k1* dengan parameter sebagai berikut:

a	0x0000000000000000000000000000000000000000000000000000000000000000
b	0x0000000000000000000000000000000000000000000000000000000000000007
p	0xfffffffffffffffffffffffffffffffffffffffffffffffffffffffefffffc2f
n	0xfffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd0364141
G	(0x79be667ef9dcbbac55a06295ce870b07029bfcdb2dce28d959f2815b16f81798, 0x483ada7726a3c4655da4fbfc0e1108a8fd17b448a68554199c47d08ffb10d4b8)

Untuk memverifikasi tanda tangan, tanda tangan yang tersembunyi dalam citra harus dicari dan diverifikasikan melalui proses verifikasi ECDSA. Ilustrasi proses verifikasi dapat dilihat pada gambar dibawah ini.



Gambar 4. Diagram proses verifikasi

Agar pelaksanaan verifikasi oleh pihak penerima dapat dilakukan, selain kunci publik pihak penerima harus memiliki domain kurva eliptik dan pesan tanda tangan.

B. Eksperimen

Berikut ini merupakan hasil eksperimen yang akan dilakukan untuk membuktikan tiga prinsip kriptografi yaitu otentikasi, integritas data dan anti-penyangkalan. Selain prinsip kriptografi tersebut, eksperimen juga dilakukan untuk membuktikan prinsip steganografi yaitu penghilangan keberadaan pesan rahasia.

1. Eksperimen steganografi

   Pada eksperimen berikut ini sebuah pesan tanda tangan akan disembunyikan didalam citra. Tanda tangan tersebut adalah

   100720180370813893182858784931901595034676659563581576981427655942580973678088873924146860634041105856540983964474351504007355906291424028150000889949705

   Hasil eksperimen ini terdapat pada gambar dibawah ini.

Gambar 5. Gambar original

Gambar 6. Gambar yang telah disisipkan tanda tagan

Jika dilihat dengan mata biasa kedua gambar terlihat sama. Tetapi jika gambar 6 diekstraksi menggunakan algoritma pencarian tanda tangan akan menghasilkan sebuah pesan berisi.

100720180370813893182858784931901595034676659563581576981427655942580973678088873924146860634041105856540983964474351504007355906291424028150000889949705

Pesan tersembunyi yang ditemukan oleh algoritma pencarian pesan rahasia menghasilkan sebuah pesan tanda tangan yang bernilai sama dengan tanda tangan sebenarnya.

2. Eksperimen otentikasi

   Dengan menggunakan tanda tangan digital ini, identitas dari pengirim dapat ditentukan. Hal ini karena pesan yang disampaikan dapat berupa nama pengirim citra. Dan pesan tersebut jika dilakukan hash menggunakan algoritma keccak dan verifikasi dengan metode verifikasi ECDSA akan menghasilkan sebuah nilai yang sama dengan nilai r kunci publik yang ada.

Isi Pesan: Ahmad Rizqee Nurhani
Kunci privat:

110189382171281758274484122160216886207103030503632056342186031874542814127859

Tanda Tangan:

(776185826444111782781227735949693713612095533927386826238357404406688034977 94,
156139100102004415072559232279304645776270320416270498545247818159901526376 04)

Kunci publik:

(104082288048177433477682931733758474122518967927777591955411026692389776037 52,
270366974307379744600736447717393279347633142252608312619803418962243550992 2)

Hasil Verifikasi:

776185826444111782781227735949693713612095533927386826238357404406688034977 94

Hasil verifikasi sama dengan kunci publik sehingga pesan tersembunyi pada citra berisi nama dari pengirim citra. Sehingga dengan menggunakan ECDSA ini otentikasi pengirim dapat dilakukan.

3. Eksperimen integritas data
   Karena informasi mengenai isi file disimpan pada pixel citra, maka jika terjadi perubahan signifikan pada citra informasi mengenai tanda tangan akan hilang dari citra tersebut.

Gambar 8. Gambar 7 yang telah diedit

   Saat gambar dimasukkan kedalam algoritma pencarian pesan rahasia, algoritma tidak menemukan pesan rahasia pada gambar tersebut. Hal ini membuktikan bahwa dengan sistem ini integritas dari berkas dapat disimpan.
4. Eksperimen anti penyangkalan
   Karena ECDSA memiliki sistem verifikasi dan penerima sebuah pesan dapat melakukan verifikasi sendiri selama mereka memiliki kunci publik, maka pengirim pesan tidak dapat menyangkal bahwa mereka bukanlah pengirim pesan tersebut. Eksperimen berikut akan menunjukan bahwa dengan mengganti sedikit saja pesan, hasil verifikasi akan berubah drastis.

Pesan: Ahmad Rizqee Nurhani
Kunci privat:
110189382171281758274484122160216886207103030503632056342186031874542814127859

Tanda tangan digital:
(840217448102170816719307475432138093224892534993343087576291984105495659012 0,
887606111559291494080245305269647149522488643910425596395116340522158013211 00)

Kunci publik;
(104082288048177433477682931733758474122518967927777591955411026692389776037 52,
270366974307379744600736447717393279347633142252608312619803418962243550992 2)

Pesan salah: Ahmad Rizqee Narhani

Hasil Verifikasi:
755622835943275838670778837486282899435667262446028816171363466047081709864 02

Dari hasil eksperimen diatas dapat dilihat bahwa nilai yang dihasilkan pada verifikasi berbeda dengan nilai r pada kunci privat. Hal ini membuktikan bahwa pengirim pesan tidak dapat menyangkal kalo dialah pengirim pesan karena penerima dapat melakukan verifikasi terhadap tanda tangan.

C. Analisis Hasil Uji Coba

Hasil eksperimen membuktikan bahwa penyisipan sebuah tanda tangan digital pada sebuah citra dapat menyelesaikan seluruh prinsip yang diinginkan. Tanda tangan yang diselipkan kedalam citra akan aman meskipun dilakukan duplikasi citra karena informasi mengenai tanda tangan tersimpan pada pixel citra. Mengenai kamanan tanda tangan dapat dilihat bahwa perubahan sedikitpun pada pesan dapat menghasilkan nilai verifikasi yang sangat berbeda dengan nilai r pada kunci publik sehingga hampir tidak mungkin terjadi salah verifikasi. Dalam menjaga integritas data dapat dilihat bahwa perubahan pada citra yang akan merusak pixel-pixel pada citra dapat merusak informasi yang tersimpan dalam citra sehingga jika informasi tersebut tidak dapat diekstraksi maka penerima dapat menkonklusikan bahwa citra telah dirubah. Selain itu karena pesan dapat berupa nama dari pengirim, tanda tangan digital dapat dipakai sebagai identifikasi pengirim pesan.

IV. KESIMPULAN

Penggunaan teknik steganografi dalam menyembunyikan sebuah tanda tangan digital pada citra dapat menjamin keaslian citra tersebut. Selain karena sulit dideteksi kecuali oleh yang sudah mengetahui bahwa citra mengandung pesan rahasia, tanda tangan digital ini sulit untuk dipalsukan karena membutuhkan kunci privat untuk membangunnya. Oleh sebab itu sistem ini

dapat digunakan untuk menjaga keaslian citra. Selain itu identitas pengirim citra juga dapat dijamin.

V. Ucapan Terima Kasih

Saya ingin mengucapkan terima kasih kepada Allah SWT., karena atas berkat dan rahmatnya makalah ini dapat diselesaikan pada waktunya. Saya ingin mengucapkan terima kasih kepada kedua orang tua saya karena dengan dukungan kedua orang tua, saya dapat melanjutkan masa perkuliahan ini. Saya tidak lupa mengucapkan terima kasih kepada Bapak Dr. Ir. Rinaldi Munir, MT selaku dosen mata kuliah IF4020 Kriptografi yang telah membagikan ilmunya kepada saya. Selain itu saya juga ingin berterima kasih kepada teman-teman seperkuliahan mata kuliah IF4020 Kriptografi yang telah berjuang bersama dengan penulis dalam menjalani perkuliahan ini.

Referensi

[1] 99Firm. *Instagram Marketing Statistics*. Dikutip pada 19 Desember 2020 dari: https://99firms.com/blog/instagram-marketing-statistics/#gref
[2] Munir, Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi: Elliptic Curve Cryptography (ECC).
[3] Munir, Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi: Fungsi hash
[4] Munir, Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi: Steganografi
[5] Munir, Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi: Fungsi hash SHA-3 (Keccak)
[6] Munir, Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi: Tanda-tangan digital (digital signature)
[7] Triwinarko, Andy. 2004. Elliptic Curve Digital Signature Algorithm (ECDSA). Departemen Teknik Informatika ITB

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, 19 Desember 2020

Ahmad Rizqee Nurhani
13517058