Autentikasi Gambar Memanfaatkan Koefisien DCT dengan Algoritma ElGamal

Rika Dewi (13517147)[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13517147@std.steiitb.ac.id

***Abstrak*—Pada era digital, kebutuhan untuk melakukan autentikasi terhadap gambar digital menjadi penting agar dapat menjamin keaslian dan kepemilikan sebuah gambar. Beberapa metode autentikasi gambar menganggap segala jenis modifikasi menyebabkan gambar gagal terautentikasi. Padahal, terdapat beberapa jenis modifikasi pada gambar yang secara praktis dapat diterima seperti kompresi. Metode autentikasi yang diusulkan pada makalah ini memanfaatkan koefisien DCT yang dipertahankan pada saat kompresi JPEG. Dengan teknik autentikasi berbasis tanda tangan digital, metode ini menggunakan algoritma ElGamal untuk membuat kunci publik privat yang digunakan dalam skema pembuatan dan verifikasi tanda tangan digital. Metode autentikasi yang diajukan ini terbukti tahan terhadap serangan yang memodifikasi tanda tangan digital, kunci, maupun manipulasi gambar seperti mengubah warna, memotong, dan memutar gambar.**

***Keywords*—algoritma ElGamal, autentikasi, gambar digital, tanda tangan digital.**

I. Pendahuluan

Kemudahan dalam mendapatkan dan menyebarkan gambar pada media digital, membuat manipulasi terhadap data gambar menjadi mudah pula untuk dilakukan. Dengan banyaknya kakas-kakas canggih yang memudahkan manipulasi gambar, kini tidak cukup hanya mengandalkan mata manusia untuk memastikan kredibilitas suatu gambar. Pada bidang-bidang tertentu seperti militer, finansial, dan medis, manipulasi terhadap gambar dapat berakibat fatal. Oleh karena itu, metode untuk melakukan autentikasi pada suatu gambar menjadi penting dilakukan.

Terdapat dua metode yang dapat digunakan untuk melakukan autentikasi pada gambar digital yaitu dengan menggunakan tanda tangan digital atau dengan memasukkan kode ke dalam gambar yang biasa disebut watermark. Metode tanda tangan digital adalah metode yang berbasiskan enkripsi kunci publik privat [1]. Secara umum, skema autentikasi menggunakan tanda tangan digital adalah sebagai berikut. Kunci privat akan digunakan untuk mengenkripsi konten data. Hasil dari enkripsi ini akan disebut sebagai tanda tangan digital. Proses autentikasi kemudian akan dilakukan dengan memanfaatkan kunci publik untuk melakukan dekripsi tanda tangan digital. Hasil dekripsi ini kemudian akan dibandingkan dengan konten data. Jika hasilnya sama, maka data tersebut terautentikasi.

Metode kedua menggunakan watermark pada gambar [2]. Watermark bekerja dengan menyisipkan kode rahasia ke dalam gambar. Proses autentikasi gambar dilakukan dengan mengekstrak watermark dari gambar digital. Perbedaan terbesar dari kedua metode ini adalah metode watermark membuat perubahan pada gambar digital sedangkan tanda tangan digital tidak menyebabkan perubahan pada gambar.

Berbeda dari teknik autentikasi pada teks yang menganggap data sebagai aliran bit yang tidak memperbolehkan sedikitpun modifikasi, informasi pada gambar dapat dipertahankan meskipun telah mengalami modifikasi tertentu seperti kompresi. Hal ini menyebabkan verifikasi bit per bit seperti pada teks tidak cocok digunakan untuk mengautentikasi gambar. Studi terhadap autentikasi pada gambar berbasis relasi telah dilakukan oleh Lin dan Chang [3]. Untuk menghasilkan sistem autentikasi gambar yang mampu mentoleransi kompresi JPEG, Lin dan Chang melakukan eksplorasi terhadap operasi pada sistem kompresi berbasis JPEG. Alhasil, Lin dan Chang mengusulkan sistem autentikasi gambar menggunakan metode tanda tangan digital dengan mengenkripsi relasi kovariansi antara koefisien DCT. Lin dan Chang menemukan bahwa nilai kovariansi selalu dipertahankan sebelum dan sesudah proses kompresi JPEG.

Sistem autentikasi gambar yang diusulkan oleh Lin dan Chang menggunakan RSA sebagai algoritma enkripsi kunci publik privat. Siahaan dkk. melakukan studi komparatif antara RSA dan ElGamal sebagai algoritma kunci publik privat [4]. Hasil dari studi komparatif ini membuktikan algoritma RSA memiliki waktu enkripsi yang lebih cepat dibandingkan ElGamal, sedangkan ElGamal memiliki waktu dekripsi yang lebih cepat dibandingkan RSA. Pada metode autentikasi berbasis tanda tangan digital, umumnya proses dekripsi akan lebih sering dilakukan dibandingkan enkripsi. Hal ini karena untuk sebuah gambar digital, proses enkripsi hanya akan dilakukan satu kali untuk menghasilkan tanda tangan digital, sedangkan proses verifikasi dapat dilakukan berkali-kali untuk mengautentikasi gambar digital. Oleh karena itu, pada makalah ini akan dikembangkan sebuah metode autentikasi gambar berbasiskan tanda tangan digital dengan menggunakan algoritma ElGamal dan memanfaatkan koefisien DCT.

II. Dasar Teori

A. Kriptografi

Kriptografi adalah cabang ilmu yang mempelajari tentang cara mengubah sebuah pesan sehingga orang lain tidak dapat membaca pesan tersebut tanpa mengetahui algoritma dan kunci yang tepat. Kriptografi bertujuan menjaga keamanan pesan yang melingkupi beberapa aspek yaitu kerahasiaan, integritas data, autentikasi, dan non repudiation. Proses dalam kriptografi dapat dibagi menjadi dua proses yaitu enkripsi dan dekripsi. Enkripsi adalah proses mengubah pesan asli agar tidak dapat dibaca oleh pihak yang tidak mengetahui algoritma dan kunci. Pesan asli ini disebut juga sebagai plainteks, sedangkan plainteks yang sudah dienkripsi disebut sebagai cipherteks. Proses dekripsi adalah proses mengembalikan cipherteks menjadi plainteks [5].

B. Algoritma ElGamal

Algoritma ElGamal merupakan sebuah 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 [6].

Algoritma ElGamal merupakan salah satu algoritma blok cipher. Pada awalnya, blok-blok plainteks akan dienkripsi dan menghasilkan blok-blok cipherteks yang kemudian digabungkan lagi menghasilkan cipherteks secara utuh. Dalam proses dekripsi, cipherteks dipecah menjadi blok-blok cipherteks yang kemudian tiap bloknya akan didekripsi dan digabungkan menjadi plainteks semula.

C. Fungsi Hash SHA-256

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 yang telah diubah menjadi *message digest* tidak dapat diubah kembali menjadi pesan awal (*irreversible*) [7].

Secure Hash Algorithm (SHA) merupakan salah satu fungsi hash satu arah yang dihasilkan dari kompetensi yang diselenggarakan oleh *National Institute of Standards and Technology* (NIST). Salah satu jenis SHA adalah SHA-2. SHA-2 sendiri memiliki variasi 224, 256, 384, and 512 tergantung dari panjang bit *message digest* yang dihasilkan.

Seperti telah dijelaskan pada paragraf sebelumnya, SHA-256 adalah jenis SHA yang menghasilkan hasil hash sepanjang 256 bit dengan 128 bit sebagai pengaman terhadap *collision attack*. Skema fungsi SHA-256 adalah sebagai berikut [8].

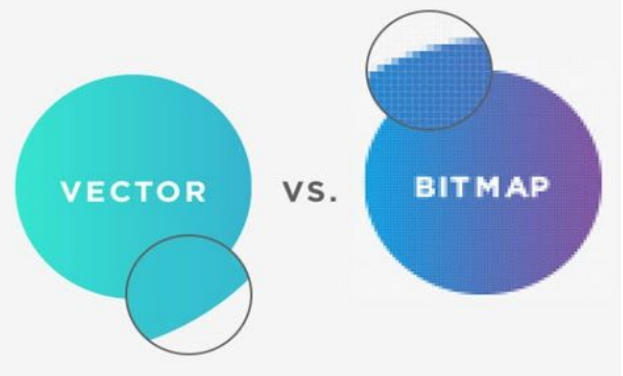
1. Pesan *m* yang akan dikenai fungsi hash akan diberi padding sehingga dihasilkan pesan yang memiliki panjang keliapatan 512 bit.
2. Pesan *m* kemudian dibagi dalam blok pesan berukuran 512 bit *M(1), M(2), ..., M(N)*
3. Setiap blok pesan 512 bit akan diproses secara sekuensial dengan formula sebagai berikut.

$$H(i) = H(i-1) + C_{M(i)}\,(H(i-1))$$

Dengan C adalah fungsi kompresi SHA-256.

E. Gambar Digital

Gambar digital adalah gambar yang terkomposisi atas elemen gambar, biasa disebut juga dengan piksel, masing-masing dengan kuantitas terbatas dan diskrit dari representasi numerik terhadap intensitas atau nilai keabuan yang merupakan keluaran dari fungsi dua dimensional dengan diberikan masukan berupa koordinat spasial, dilambangkan oleh x, y pada sumbu-x dan sumbu-y, secara berurutan [8]. Gambar digital memiliki dua jenis representasi yaitu gambar raster (bitmap) dan gambar vektor seperti ditunjukkan pada Gambar 1. Gambar raster direpresentasikan dalam nilai pada suatu titik, sedangkan gambar vektor direpresentasikan dalam fungsi dua dimensi. Pada umumnya dan untuk selanjutnya, istilah gambar digital mengacu kepada format gambar raster.



Gambar 1. Gambar vektor dan gambar bitmap

F. Koefisien DCT

Discrete Cosine Transform (DCT) adalah teknik yang digunakan untuk mengubah piksel-piksel pada gambar digital dari domain spasial menjadi domain frekuensi. Pada domain frekuensi, identifikasi redundansi pada gambar digital menjadi lebih mudah dilakukan. Pada kompresi JPEG, sebuah gambar digital akan dipetakan menjadi blok berukuran 8x8. Setiap blok ini kemudian akan dikenai fungsi DCT dengan formula sebagai berikut [9].

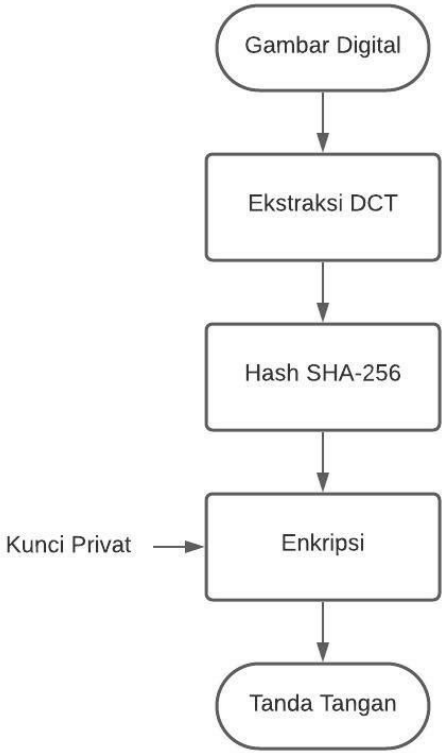
$$F(u,v) = \frac{1}{4}C(u)C(v)\sum_{i=0}^{7}\sum_{j=0}^{7} f(i,j)\cos((2i+1)u\pi/16)\cos((2j+1)v\pi/16)$$

III. Skema dan Implementasi Autentikasi Gambar

Metode autentikasi gambar digital yang diajukan akan memanfaatkan kovariansi koefisien DCT dari gambar digital original terhadap koefisien DCT dari gambar digital yang akan diuji kredibilitasnya. Dengan memanfaatkan algoritma enkripsi publik privat, metode autentikasi ini akan terdiri dari dua prosedur utama yaitu sebagai berikut pembuatan tanda tangan digital dan prosedur autentikasi gambar.

A. Prosedur Penandatanganan

Prosedur penandatangan gambar digital terdiri dari tiga proses utama yaitu ekstraksi koefisien DCT pada gambar digital, fungsi hash SHA-256, kemudian dilanjutkan dengan enkripsi yang menghasilkan tanda tangan digital. Secara umum, prosedur ini tergambar dalam Gambar 2. yang menunjukkan skema penandatanganan.



Gambar 2. Skema Penandatanganan

1). Ekstraksi DCT

Gambar digital yang akan ditandatangani akan diproses terlebih dahulu untuk mendapatkan koefisien DCT pada gambar tersebut. Pemilihan DCT koefisien didasarkan dari sifat kompresi JPEG. Teknik kompresi pada JPEG memanfaatkan kelemahan mata manusia yang tidak dapat melihat gambar dengan frekuensi tinggi, sehingga informasi berfrekuensi tinggi tersebut dapat dihilangkan.

Untuk mendapatkan nilai DCT dari sebuah gambar digital, pertama-tama dilakukan transformasi representasi ruang warna dari RGB (*Red Green Blue*) menjadi YCbCr yang terdiri atas tiga matriks yaitu Y merepresentasikan kecerahan, Cb merepresentasikan perbedaan warna biru relatif terhadap chroma, dan Cr merepresentasikan perbedaan warna merah relatif terhadap chroma. Setiap matriks YCbCr akan dipartisi menjadi blok berukuran 8x8. Setiap komponen blok kemudian akan dikenai fungsi 2-D DCT. Hasil dari ekstraksi DCT terhadap gambar digital adalah tiga buah matriks yang masing-masing merupakan nilai koefisien DCT dari YCbCr.

2). Fungsi Hash SHA-256

Sebelum dikenai fungsi hash SHA-256, hasil dari tiga buah matriks DCT akan digabungkan dengan urutan Y, Cb, dan Cr membentuk sebuah himpunan bit. Hal inilah yang menjadi input dalam fungsi hash SHA-256. Hasil dari fungsi ini akan menghasilkan *message digest* sepanjang 256 bit.

3). Enkripsi

Proses enkripsi dilakukan dengan menggunakan algoritma kunci publik privat ElGamal. Sebelum enkripsi, pertama-tama dilakukan proses pembangkitan kunci yang menghasilkan kunci publik dan kunci privat. Kunci privat ini akan digunakan pada proses enkripsi untuk menghasilkan tanda tangan digital, sedangkan kunci publik akan digunakan nanti pada proses verifikasi tanda tangan digital.

a). Pembangkitan Kunci

Pada proses pembangkitan kunci, pertama-tama dipilih sebuah bilangan p, di mana nilai p harus prima. Lalu, dipilih sebuah bilangan g yang nilainya $1 \leq g < 1 - p$ dan x yang nilainya $1 \leq x < p - 2$. Terakhir, dihitung nilai dari y sehingga dipenuhi persamaan

$$y \equiv g^x \bmod p$$

Pasangan kunci publik yang dihasilkan adalah (p, g, y), sementara pasangan kunci privat adalah (p, g, x).

b). Pembuatan Tanda Tangan

Misal $H(m)$ adalah *message digest* yang dihasilkan dari fungsi hash SHA-256 yang dilakukan pada langkah sebelumnya, maka untuk melakukan pembuatan tanda tangan, dibutuhkan pasangan kunci privat (p, g, x). Langkah untuk membuat tanda tangan digital adalah sebagai berikut.

1. Nilai k dipilih sedemikian rupa sehingga memenuhi persamaan berikut.

   $$GCD(k, p - 1) = 1$$

   Dengan kata lain, k merupakan akar primitif dari p.
2. Nilai r dihitung dengan formula berikut.

   $$r \equiv d^k \bmod p$$

3. Nilai s dihitung dengan formula berikut.

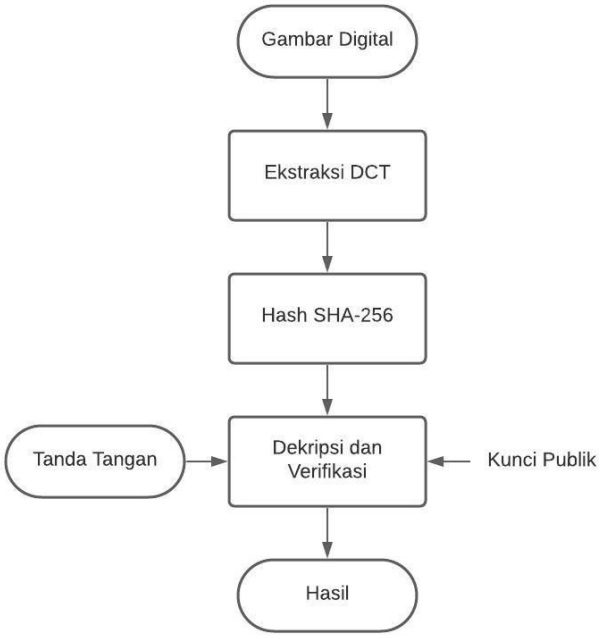
   $$s \equiv k^{-1}(H(m) - zr)$$

4. Tanda tangan yang dihasilkan adalah pasangan dari (r,s).

Dengan demikian, hasil akhir dari prosedur penandatangan yang digambarkan melalui skema Gambar 2. adalah sebuah tanda tangan digital, pasangan kunci privat, dan pasangan kunci publik. Kunci privat ini akan bersifat rahasia, sedangkan kunci publik tidak bersifat rahasia sehingga dapat diberikan kepada pihak-pihak yang akan melakukan verifikasi terhadap gambar.

B. Prosedur Autentikasi

Prosedur autentikasi sebuah gambar digital dilakukan dalam tiga buah tahap yaitu ekstraksi DCT, fungsi hash SHA-256, dan dekripsi serta verifikasi. Secara umum, prosedur autentikasi dapat dilihat pada Gambar 3. tentang skema autentikasi.



Gambar 3. Skema Autentikasi

Proses ekstraksi DCT dan fungsi hash SHA-256 yang dilakukan pada prosedur autentikasi ini sama dengan proses yang dilakukan pada prosedur penandatanganan. Oleh karena itu, penjelasan akan ditekankan pada proses dekripsi dan verifikasi.

1). Dekripsi dan Verifikasi Tanda Tangan

Misal *H(m)* adalah *message digest* dari gambar digital yang ingin diverifikasi dan dihasilkan dari fungsi hash SHA-256 yang dilakukan pada langkah sebelumnya. Untuk melakukan verifikasi tanda tangan dibutuhkan pasangan kunci publik *(p, g, y)*. Langkah untuk melakukan verifikasi tanda tangan terhadap *H(m)* adalah sebagai berikut.

1. Nilai *v1* dihitung dengan formula berikut

$$v1 \equiv y^r r^s$$

2. Nilai *v2* dihitung dengan formula berikut

$$v2 \equiv g^{H(m)}$$

3. Jika *v1* dan *v2* tidak sama, maka tanda tangan tersebut tidak valid. Begitu pula sebaliknya, Jika v1 dan v2 sama, maka tanda tangan tersebut valid.

IV. Hasil Pengujian dan Analisis

Bagian ini berisi pengujian terhadap keamanan dari skema autentikasi yang diajukan, ketahanan terhadap beberapa jenis manipulasi gambar, dan ketahanan terhadap dilakukannya kompresi.

Eksperimen 1: Uji Autentikasi Gambar Asli

Pengujian dilakukan dengan menggunakan langit.jpg seperti terlihat pada Gambar 4. Pengujian dilakukan dengan membuat tanda tangan digital menggunakan langit.jpg. Autentikasi kemudian dilakukan dengan menggunakan tanda tangan digital tersebut menggunakan gambar original yang sama.

Gambar 4. Gambar original "langit.jpg"

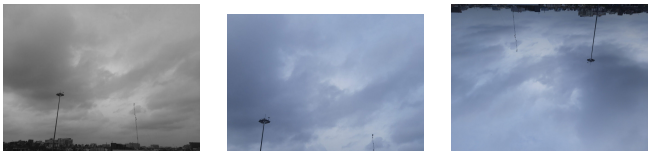
Tabel I. Hasil Pengujian Eksperimen 1

Kunci publik *(p, g, y)*	(57143, 28931, 9210)
Kunci privat *(p,g,x)*	(57143, 28931, 4227)
Tanda tangan *(r,s)*	(22044, 27358)
Hasil	terautentikasi

Dari hasil eksperimen 1 yang terlihat pada Tabel I. didapatkan bahwa metode autentikasi gambar yang diajukan berhasil mengautentikasi gambar yang original yang tidak dimanipulasi.

Eksperimen 2: Uji Manipulasi Gambar

Eksperimen kedua dilakukan dengan melakukan beberapa manipulasi terhadap gambar original langit.jpg dengan mengubah warna, memotong, dan memutar gambar original seperti terlihat pada Gambar 5.



(a) (b) (c)

Gambar 5. Manipulasi terhadap gambar "langit.jpg": (a) mengubah warna menjadi grayscale, (b) memotong tepi gambar, (c) melakukan rotasi 180^o

Tabel II. Hasil Pengujian Eksperimen 2

Gambar 5. (a) Grayscale	
Kunci publik *(p, g, y)*	(38747, 32603, 9839)
Kunci privat *(p,g,x)*	(38747, 32603, 13832)
Tanda tangan *(r,s)*	(28961, 29678)
Hasil	tidak terautentikasi
Gambar 5. (b) Memotong tepi gambar	
Kunci publik *(p, g, y)*	(43223, 8384, 31573)
Kunci privat *(p,g,x)*	(43223, 8384, 37202)
Tanda tangan *(r,s)*	(42103, 14908)
Hasil	tidak terautentikasi
Gambar 5. (c) Rotasi	
Kunci publik *(p, g, y)*	(34583, 1900, 3664)
Kunci privat *(p,g,x)*	(34583, 1900, 12217)
Tanda tangan *(r,s)*	(26918, 32446)
Hasil	tidak terautentikasi

Dari hasil eksperimen kedua yang terlihat pada Tabel II., terlihat bahwa metode autentikasi yang diusulkan berhasil menghasilkan hasil tidak terverifikasi untuk semua gambar yang telah termanipulasi. Hal ini membuktikan bahwa metode autentikasi gambar yang diajukan dapat membuktikan keaslian gambar sehingga menjamin integritas data.

Eksperimen 3: Uji Kompresi Gambar

Eksperimen ketiga dilakukan untuk menguji ketahanan metode autentikasi terhadap kompresi yang dilakukan pada gambar digital. Pada pengujian ini, kompresi dilakukan secara *lossy* dan *lossless*.

(a)

(b)

Gambar 6. Kompresi terhadap gambar "langit.jpg": (a) secara *lossy*, (b) secara *lossless*

Tabel III. Hasil Pengujian Eksperimen 3

Gambar 6. (a) Lossy	
Kunci publik *(p, g, y)*	(61343, 16955, 12683)
Kunci privat *(p,g,x)*	(61343, 16955, 45649)
Tanda tangan *(r,s)*	(1809, 35403)
Hasil	tidak terautentikasi
Gambar 6. (b) Lossless	
Kunci publik *(p, g, y)*	(56039, 35661, 37220)
Kunci privat *(p,g,x)*	(56039, 35661, 14080)
Tanda tangan *(r,s)*	(21239, 35556)
Hasil	terautentikasi

Pada Tabel III. terlihat variasi hasil pada eksperimen ketiga. Hasil ini menunjukkan bahwa metode autentikasi yang diusulkan memiliki ketahanan terhadap kompresi jenis *lossless* namun tidak tahan terhadap kompresi jenis *lossy*. Hal ini disebabkan karena nilai koefisien DCT tidak dipertahankan pada kompresi secara *lossy*.

Eksperimen 4: Uji Perubahan Tanda Tangan Digital

Pengujian dilakukan dengan melakukan sedikit perubahan pada tanda tangan digital dengan mengubah 1 digit nilai tanda tangan digital. Eksperimen ini dilakukan untuk menguji ketahanan metode autentikasi yang diusulkan terhadap serangan yang ditujukan pada tanda tangan digital.

Tabel IV. Hasil Pengujian Eksperimen 4

Kunci publik *(p, g, y)*	(45707, 10971, 4585)
Kunci privat *(p,g,x)*	(45707, 10971, 10710)
Tanda tangan *(r,s)*	(22951, 10792)
Tanda tangan modifikasi *(r,s)*	(22950, 10792)
Hasil	tidak terautentikasi

Hasil pengujian eksperimen keempat dapat dilihat pada Tabel IV. Terlihat bahwa perubahan sedikit pada tanda tangan digital menyebabkan hasilnya tidak terautentikasi. Hal ini membuktikan metode autentikasi yang dihasilkan tahan terhadap serangan yang memodifikasi tanda tangan digital.

Eksperimen 5: Uji Kunci Tidak Sepadan

Pengujian ini dilakukan dengan melakukan modifikasi 1 digit dari kunci publik sehingga kunci publik yang digunakan untuk dekripsi dan verifikasi tidak sepadan terhadap kunci privat yang digunakan untuk enkripsi. Eksperimen kelima ini dilakukan untuk menguji ketahanan metode autentikasi yang diusulkan terhadap serangan yang memodifikasi kunci algoritma.

Tabel V. Hasil Pengujian Eksperimen 5

Kunci publik *(p, g, y)*	(51047, 17371, 26113)
Kunci publik modifikasi *(p, g, y)*	(51047, 17372, 26113)
Kunci privat *(p,g,x)*	(51047, 17371, 7665)
Tanda tangan *(r,s)*	(24007, 50287)
Hasil	tidak terautentikasi

Hasil pengujian dari eksperimen kelima dapat dilihat pada Tabel V. Terlihat bahwa sedikit perubahan pada kunci publik membuat hasilnya menjadi tidak terautentikasi. Hal ini membuktikan metode autentikasi yang diajukan memiliki ketahanan terhadap serangan yang melakukan modifikasi terhadap kunci sehingga kunci publik privat menjadi tidak sepadan.

V. Kesimpulan

Dari hasil eksperimen terbukti bahwa metode autentikasi berbasis tanda tangan digital yang diusulkan dapat digunakan untuk menjamin keaslian gambar digital dan membuktikan kepemilikan sebuah gambar digital. Dari segi keamanan, metode autentikasi yang diusulkan memiliki ketahanan terhadap serangan yang memodifikasi baik tanda tangan digital maupun memodifikasi kunci publik privat. Manipulasi terhadap gambar digital seperti mengubah warna, memotong, ataupun memutar gambar, menyebabkan integritas data tidak dapat terjamin sehingga tidak terautentikasi menggunakan metode ini. Terlebih, metode autentikasi ini tahan terhadap kompresi secara *lossless*, namun tidak dapat mengautentikasi gambar yang terkompresi secara *lossy*. Oleh karena itu, pengembangan selanjutnya terhadap metode ini dapat dilakukan untuk menangani kompresi secara *lossy*.

VII. Ucapan Terima Kasih

Pertama-tama, penulis berterima kasih kepada Tuhan Yang Maha Esa atas berkat dan rahmatnya makalah tentang autentikasi gambar ini dapat diselesaikan. Terima kasih juga kepada Pak Rinaldi Munir selaku pengajar kriptografi yang telah memberikan pengetahuan yang menjadi dasar ilmu pengembangan skema autentikasi gambar digital yang ada di makalah ini. Penulis juga ingin mengucapkan terima kasih kepada seluruh pihak lain yang telah membantu pengerjaan makalah ini.

Referensi

[1] W. Diffle and M. E. Hellman, "New directions in cryptography," IEEE Trans. Inform. Theory, vol. IT-22, pp. 644–654, Nov. 1976.

[2] "A watermark-based robust image authentication method using wavelets," Columbia Univ., New York, ADVENT Project Rep., Apr. 1998.

[3] C.-Y. Lin and S.-F. Chang, "A robust image authentication method distinguishing JPEG compression from malicious manipulation," IEEE Trans. Circuits Syst. Video Technol., vol. 11, pp. 153–168, Feb. 2001

[4] Siahaan, Andysah Putera Utama, dkk. 2018. "Comparative Analysis of RSA and ElGamal Cryptographic Public-key Algorithms," Universitas Sumatra Utara. DOI: 10.4108/eai.23-4-2018.2277584.

[5] Easttom, Chuck. 2015. Modern Cryptography: Applied Mathematics for Encryption and Information Security. NY: McGraw-Hill. ISBN: 978-1-25-958809-9.

[6] "Digital Signatures: ElGamal Signature Scheme and Digital Signature Algorithm (and Birthday Attacks)" Internet: https://www.commonlounge.com/discussion/35a1c2baa00b447f9275e8f71b02ef29 [20 Desember 2020]

[7] Munir, Rinaldi. 2019. Slide Kuliah IF4020 Kriptografi: Fungsi Hash.

[8] Gonzalez, Rafael. (2018). Digital image processing, 4e. New York, NY: Pearson. ISBN 978-0-13-335672-4. OCLC 966609831.

[9] Furht, Borko. 2006. *Discrete Cosine Transform (DCT)*. MA: Springer US. DOI: https://doi.org/10.1007/0-387-30038-4_61

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 2020

Rika Dewi (13517147)