METODE PENGAMANAN HAK CIPTA DENGAN KRIPTOGRAFI KLASIK DAN KOMBINASI TEKNIK DIGITAL WATERMARKING MENGGUNAKAN METODE LEAST SIGNIFICANT BIT (LSB)

METHODS OF SAFEGUARDING COPYRIGHT WITH CLASSICAL CRYPTOGRAPHY AND COMBINATION OF USING DIGITAL WATERMARKING TECHNIQUES LEAST SIGNIFICANT BIT METHOD (LSB)

Ahmad Kurniadi[1)], Dony Ariyus[2)]
[1, 2,)]Magister Teknik Informatika Universitas AMIKOM Yogyakarta
e-mail: ahmad.kurniadi@students.amikom.ac.id[1)], dony.a@amikom.ac.id[2)]

Abstract: *With the rapid development of the internet, the exchange of information and digital data is increasingly being used, but from the various data it should not be able to be modified or distributed freely or without permission because changing the shape of the original image results in losses to the victims concerned. This violation is common in internet media but not all internet users are aware of it. So, a digital content that will be published must have rules in the use and protection that are widely recognized, so that the intellectual property rights of the creator are maintained. The way to protect intellectual property rights over a digital work is by licensing the content. In this final project, a Creative Commons License is used. Digital watermarking is a technique used to insert information that shows ownership of digital data and information. Based on these problems, we conduct research to implement the implementation of cryptographic implementation in image media message text by combining cryptographic and steganographic methods using an edge detection algorithm based on python programming. Based on this background we designed a security system through the image watermarking method which we then integrated with the steganography method. This system is designed and tested with Image data types of various sizes, as well as testing the results of the watermarking process and the Scanning watermark process. The test results show that the application is better used for files with image data types .jpg and also png*
Keywords: Criptografi, Watermarking, *Least Significant Bit* (LSB)

Abstrak: Dengan berkembangnya internet yang pesat menjadikan pertukaran informasi dan data digital semakin banyak digunakan namun dari berbagai data tersebut seharusnya tidak dapat dimodifikasi atau didistribusikan secara bebas atau tanpa izin karena pengubahan bentuk gambar asli berakibat kerugian pada korban yang bersangkutan. Pelanggaran ini yang sering terjadi di media internet namun tidak semua pengguna internet menyadarinya. Maka, sebuah konten digital yang akan dipublikasikan haruslah memiliki aturan dalam pemanfaatan dan perlindungan yang diakui secara luas, agar supaya hak kekayaan intelektual penciptanya tetap terjaga. Cara untuk melindungi hak kekayaan intelektual atas suatu karya digital adalah dengan memberikan lisensi pada konten tersebut. Digital watermarking adalah teknik yang digunakan untuk menyisipkan informasi yang menunjukan kepemilikan atas sebuah data dan informasi digital. Berdasarkan permasalahan tersebut maka kami mengadakan penelitian untuk melakukan penerapan implementasi kriptografi pada teks pesan media gambar dengan melakukan kombinasi pada metode kriptografi dan steganografi menggunakan algoritma edge detection. Berdasarkan latar belakang tersebut kami merancang sistem security melalui metode watermarking gambar yang kemudian kami integrasikan dengan metode steganografi. Sistem ini dirancang dan diuji dengan Tipe data Gambar dengan berbagai ukuran, serta menguji hasil dari Proses watermarking dan proses Scanning watermark. Hasil pengujian menunjukkan bahwa aplikasi lebih baik digunakan terhadap file dengan tipe data gambar .jpg dan juga png
Kata Kunci: Kriptografi, watermarking, *Least Significant Bit* (LSB)

PENDAHULUAN

Perkembangan teknologi semakin mempermudah orang berkomunikasi. Salah satu hal terpenting dalam komunikasi menggunakan komputer dan jaringan komputer adalah untuk menjamin keamanan pesan, data,ataupun informasi dalam proses pertukaran data, Salah satu bentuk komunikasi yang sering digunakan adalah mengirim dan menerima pesan. Seiring berkembangnya teknologi, semakin berkembang juga kejahatan terhadap keamanan pesan yang dikirim terutama pesan pada media gambar. Salah satu bentuk kejahatan

terhadap suatu pesan media gambar adalah pengubahan media gambar dengan maksud pencemaran nama baik terhadap seseorang terutama pada public figure. Bentuk pengubahan pesan gambar tersebut biasanya dengan memodifikasi pesan tersebut. Salah satu cara untuk mencegah hal tersebut adalah dengan cara membentuk sistem security pada media gambar tersebut.

Bentuk penelitian yang sedang kami lakukan adalah dengan pembuatan perangkat lunak dengan sistem security pada media gambar dengan melakukan kombinasi watermarking pada gambar dengan mengintegrasikan teknik kriptografi dan steganografi sehingga membentuk algoritma baru sehingga tidak dapat mengubah pesan rahasia media gambar menjadi pesan acak *(ciphertext)* yang tidak memiliki makna sehingga pesan rahasia hanya dapat terbaca oleh pihak yang berhak.

Watermarking merupakan suatu bentuk dari Steganography (teknik untuk menyembunyikan suatu informasi pada suatu media tanpa perubahan yang berarti pada media tersebut). Penelitian ini dimulai pada proses watermarking menggunakan metode edge detection kemudian mengintegrasikan kombinasi teknik kriptografi dengan dua tahap yaitu enkripsi dan deskripsi. Enkripsi dilakukan dengan cara mengubah data asli menjadi data rahasia, sedangkan dekripsi dilakukan dengan cara mengubah data rahasia menjadi data asli, setelah itu dilakukan kombinasi sehingga membentuk algoritma baru.

Salah satu metode yang dapat dilakukan adalah metode Vigenere Cipher. Metode Vigenere Cipher menyembunyikan pesan berupa teks melalui teknik substitusi dengan mengubah setiap huruf menjadi huruf lain berdasarkan kunci yang digunakan. Metode ini dapat mengubah pesan menggunakan kombinasi beberapa huruf alfabet dan memerlukan waktu cukup lama untuk memecahkan algoritma tersebut, sehingga keamanan pesan media gambar dapat terjaga. Berdasarkan uraian diatas, maka dilakukan penerapan implementasi dengan merancang suatu perangkat lunak dengan pembelajaran metode Vigenere cipher pada sistem. Perancangan sistem kriptografi vigenere cipher dengan bentuk enkripsi gambar dan dekripsi text yang dapat diprogram dengan menggunakan bahasa pemprograman visual C++. Hasil penelitian ini adalah sebuah implementasi kombinasi sistem kriptografi dan steganografi pada media gambar dengan format jpg atau png.

KAJIAN TEORI

2.1 Kriptografi

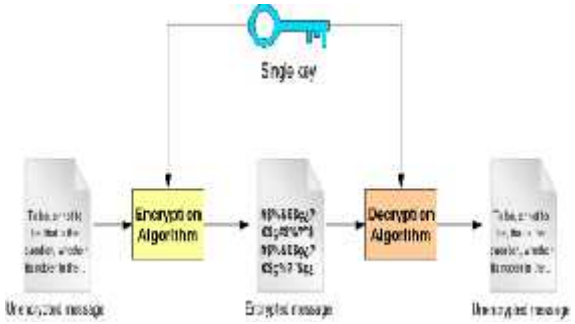
Kata kriptografi berasal dari bahasa Yunani yang terdiri dari dua buah kata yaitu *cryptos* dan *graphia*. Kata *crypto* berarti rahasia sedangkan *graphia* berarti tulisan yang secara umum memiliki makna tulisan rahasia. Menurut Dony Ariyus pada bukunya yang berjudul *Pengantar Ilmu Kriptografi: teori, analisis, dan implementasi* tahun 2008 menjelaskan bahwa kriptografi adalah ilmu yang mempelajari tentang bagaimana menjaga kerahasiaan suatu pesan, agar isi pesan yang ditampilkan tersebut aman sampai ke penerima pesan (Ariyus, 2008b).

Kriptografi adalah ilmu yang mempelajari bagaimana melakukan enkripsi dan dekripsi, dengan memanfaatkan model matematika tertentu. Kriptografi diilhami dengan teknik enkripsi atau teknik penyandian yang mengubah sebuah pesan yang dapat dibaca *(plaintext)* menjadi sebuah pesan yang acak dan sulit diartikan. Untuk dapat membaca pesan yang terenkripsi diperlukan proses terbalik dari enkripsi yang disebut dekripsi (Kurniawan, 2008)

2.2 Algoritma Kriptografi

Kriptografi Algoritma Simetris

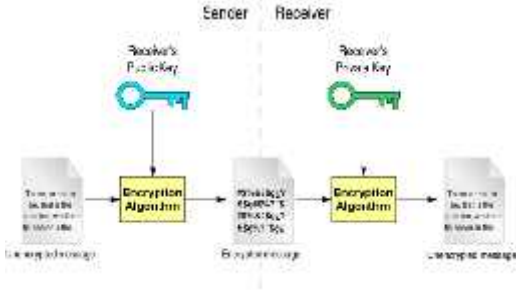
Algoritma kriptografi simetris menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Skema enkripsi akan disebut *symmetric-key* apabila pasangan kunci untuk proses enkripsi dan dekripsinya sama. Algoritma kriptografi simetris dibagi menjadi dua kategori yaitu algoritma aliran *(stream cipher)* dan algoritma blok *(block cipher)* (Ariyus, 2008b)Contoh skema algoritma kunci simetris



Gambar 1. Skema Algoritma Kunci Simetris (Schneier, 1996)

Kriptografi Algoritma Asimetris

Algoritma asimetris adalah pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan yang satu lagi untuk dekripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsi suatu pesan, sedangkan hanya satu orang saja yang memiliki kunci rahasia untuk melakukan pembongkaran terhadap kode yang dikirim untuknya (Ariyus, 2008a). Contoh skema algoritma kunci asimetris



Gambar 2. Skema Algoritma Kunci Asimetris (Schneier, 1996)

2.3 Algoritma Vigenere Cipher

Vigenère cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau kira-kira pada tahun 1986. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu *Blaise de Vigenère*, namun sebenarnya algoritma ini telah digambarkan sebelumnya pada buku La Cifra del Sig. Giovan Batista Belaso, sebuah buku yang ditulis oleh Giovan Batista Belaso, pada tahun 1553. (Basuki Rakhmat; Muhammad Fairuzabadi, 2010)

2.4.Edge Detection

Perbedaan yang signifikan sebuah image brightness sangat menarik untuk beberapa alasan. Alasan yang pertama adalah sebuah tepian dari objek biasanya memiliki perbedaan intensitas cahaya (image yang terang bisa terdapat di latar belakang yang gelap atau sebaliknya image yang gelap bisa berada di latar belakang yang terang).dan alasan yang kedua adalah perbedaan tersebut dapat pula muncul akibat dari pola yang terbentuk dari perbedaan intensitas cahaya (zebra memiliki garis tubuh, macan tutul memiliki bintik-bintik pada tubuhnya atau garis-garis yang terbentuk karena bayangan). Obyek yang berada dalam bidang citra dan tidak bersinggungan dengan batas bidang citra, berarti obyek tersebut dikelilingi daerah yang bukan obyek yaitu latar belakang. Pertemuan antara bagian obyek dan bagian latar belakang disebut tepi obyek (dapat juga disebut tepi latar belakang, tetapi kita tidak tertarik pada latar belakang). Tepi merupakan salah satu fitur citra yang penting karena dapat mewakili informasi yang penting dari obyek dalam pemandangan. Poin-poin dimana sebuah image memiliki perbedaan intensitas cahaya yang tajam itulah yang sering disebut edges atau edge points (Astawa & Imawati, 2013).

Operator Canny didesain untuk menjadi sebuah pendeteksi tepi yang optimal(berdasarkan kriteria tertentu). Canny menggunakan sebuah gambar grayscale, dan menghasilkan sebuah gambar yang menampilkan posisi dari intensitas dan akhir yang telah ditemukan. Operator Canny bekerja dalam sebuah proses bertingkat. Pertama gambar akan diperhalus dengan menggunakan konvolusi Gaussian. Kemudian sebuah operator turunan

pertama dari 2-D digunakan untuk menghaluskan gambar pada daerah yang telah ditandai dengan sebagian turunan pertama yang tinggi. Tepi ini diberikan kenaikan menjadi lipatan dalam ukuran gradien gambar. Kemudian algoritma tersebut mencari puncak dari lipatan ini dan memberi nilai nol pada semua piksel yang bukan merupakan puncak lipatan yang menghasilkan garis tipis pada gambar keluaran, sebuah proses yang dikenal dengan non-maximal suppression.

Proses pencarian ini menampilkan hysteresis yang dikendalikan oleh dua thresholds: T1 dan T2 dengan T1 > T2. Pencarian hanya dapat dimulai pada titik dimana nilai lipatan lebih tinggi dari T1. Pencarian kemudian berlanjut dalam dua arah keluar dari titik tersebut hingga tinggi dari lipatan tersebut bernilai kurang dari T2. Hysteresis ini membantu untuk meyakinkan bahwa tepi yang memiliki noise tidak rusak menjadi banyak bagian tepi

(a) (b) (c)

Gambar 3. (a) citra koin asli (b) deteksi tepi dengan operator sobel (c) deteksi tepi dengan operator canny

2.5.Digital Watermarking

Watermarking merupakan cara untuk menyisipkan *watermark* atau proses penambahan kode secara permanen ke dalam citra digital yang ingin dilindungi hak ciptanya dengan tidak merusak citra aslinya dan tahan terhadap serangan (Munir, 2019). Pada dasarnya, teknik *watermark* (tanda air) secara hirarkis berakar pada ilmu steganografi. Pada tugas akhir ini digital *watermark* digunakan untuk memberikan informasi identifikasi sebuah citra digital atas informasi sumber daya penciptanya. *Watemarking* dapat juga dikategorikan sebagai *visible watermarking* (*watermark* terlihat oleh indra manusia) dan *invisible watermarking* (*watermark* yang tidak tampak) (Munir, 2019).

METODOLOGI PENELITIAN

Cara kerja dari *Vigenère cipher* ini mirip dengan Caesar cipher, yaitu mengenkripsi plainteks pada pesan dengan cara menggeser huruf pada pesan tersebut sejauh nilai kunci pada deret alphabet. *Vigenère cipher* adalah salah satu algoritma kriptografi klasik yang menggunakan metode substitusi abjad majemuk. Substitusi abjad-majemuk mengenkripsi setiap huruf yang ada menggunakan kunci yang berbeda, tidak seperti *Caesar cipher* yang menerapkan metode substitusi abjad-tunggal yang semua huruf disuatu pesan dienkripsi menggunakan kunci yang sama.

3.1 Proses Enkripsi Caesar Chiper

Proses penyandian (enkripsi) dapat secara matematis menggunakan operasi modulus dengan mengubah huruf-huruf menjadi angka, A = 0, B = 1,…, Z = 25. dengan geseran secara matematis dengan contoh pergeseran 3 dituliskan sebagai berikut:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Menjadi :

D	E	F	G	H	I	J	K	L	M	N	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12

Q	R	S	T	U	V	W	X	Y	Z	A	B	C
13	14	15	16	17	18	19	20	21	22	23	24	25

Rumus Enkripsi untuk Caesar Cipher:
E(x) = (x+key) mod 25 dimana x merupakan index sebagai contoh menggunakan kata kunci 4 maka hasilnya akan sebagai berikut::

Plaintext	:	P	U	R	W	O	R	E	J	O
Indek	:	15	20	17	22	14	17	4	9	18
Index + key (4) mod 25	:	19	24	22	26	18	21	8	13	22
Ciphertext	:	T	Y	V	A	S	Y	I	N	S

Sedangkan untuk rumus Dekripsinya adalah sebagai berikut :
D(x) = (x-key) mod 25

Plaintext	:	T	Y	V	A	S	Y	I	N	S
Indek	:	19	24	22	26	18	21	8	13	22
Index + key (4) mod 25	:	15	20	17	22	14	17	4	9	18
Ciphertext	:	P	U	R	W	O	R	E	J	O

Untuk Enkripsi Caesar Cipher menggunakan operasi mod 25 karena dimulai dari 0-25.

3.2 Proses Enkripsi Vigenere Cipher

Proses ini sama halnya dengan proses Caesar Cipher yaitu menggunakan rumus modulus dengan menggubah huruf – huruf menjadi angka. Proses Vigenere Cipher menggunakan rumus sebagai berikut:
Rumus enkripsi Vigenere cipher : Pi=(Ci+Ki)mod 26
Rumus Dekripsi Vigenere Cipher : Pi = (Ci - Ki) mod 26
Dimana:
Ci = nilai desimal karakter ciphertext ke-i, Pi = nilai desimal karakter plaintext ke-I, Ki = nilai desimal karakter kunci ke-i

Contoh untuk *plaintext* menggunakan *key* ada adalah sebagai berikut:

Plaintext	:	I	N	F	O	R	M	A	S	I
Indek	:	8	13	5	14	17	12	0	18	8
Key	:	A	D	A	A	D	A	A	D	A
Indek	:	0	3	0	0	3	0	0	3	0
Pi = (Ci + Ki) mod 26	:	8	16	5	14	20	12	0	21	8
Ciphertext	:	I	Q	F	O	U	M	A	V	I

Untuk Dekripsinya adalah sebagai berikut:

Plaintext	:	I	Q	F	O	U	M	A	V	I
Indek	:	8	16	5	14	20	12	0	21	8
Key	:	A	D	A	A	D	A	A	D	A
Indek	:	0	3	0	0	3	0	0	3	0
Pi = (Ci + Ki) mod 26	:	8	13	5	14	17	12	0	18	8
Ciphertext	:	I	N	F	O	R	M	A	S	I

Huruf pada kunci akan dikonversi menjadi sebuah nilai, misalnya A = 0, B = 1, sampai dengan Z = 25. Setelah itu prosesnya sama seperti pada Caesar cipher dimana setiap huruf pada plainteks akan digeser sejauh nilai kunci yang posisinya bersesuaian. Pergeseran huruf-huruf ini bisa dipetakan dalam bentuk tabel 26x26 yang memetakan antara huruf pada plainteks dengan huruf pada kunci seperti yang diperlihatkan pada table 1.

Tabel 1. Pemetaan *Vigenere Cipher*

Selain menggunakan Algoritma *Vigenere Cipher* bujur sangkar *Vigenere* untuk melakukan algoritma ini dapat dilakukan dengan menjumlahkan *plaintext* dengan kunci kemudian di modulo 26. Dengan Asumsi a = 0, b = 1, c = 2, ……, z = 25

3.3 Proses Metode Edge Detection

Proses ini merupakan metode pendeteksian tepi pada gambar untuk menginputkan algoritma kombinasi kriptografi dan steganografi. Metode edge detection pada media gambar ini menggunakan bahasa pemrogaman C++ Visual Studio dengan beberapa input syntac algoritma seperti dibawah ini,

```
ProgressBar1.Value = 0
Dim gambar As New Bitmap(PictureBox1.Image)
PictureBox2.Image = gambar

Dim baris, kolom As Integer
Dim merah, hijau, biru, abu2 As Integer
Dim batas As Integer

batas = HScrollBar1.Value
For baris = 0 To gambar.Width - 1
    For kolom = 0 To gambar.Height - 1
        merah = gambar.GetPixel(baris, kolom).R
        hijau = gambar.GetPixel(baris, kolom).G
        biru = gambar.GetPixel(baris, kolom).B

        abu2 = Int((merah + hijau + biru) / 3)

        If abu2 <= batas Then
            gambar.SetPixel(baris, kolom, Color.FromArgb(255, 255, 255))
        Else
            gambar.SetPixel(baris, kolom, Color.FromArgb(0, 0, 0))
        End If
    Next
    ProgressBar1.Increment(1)
```

Gambar 4. Code Inisialisasi Image Processing

Setelah melakukan input code c++ diatas kemudian dilakukan input kombinasi algoritma baru yang dibentuk dari metode kriptografi dan steganografi.

3.4 Proses Metode Least Significant Bit (LSB)

Bit atau binary digit adalah unit dasar penyimpanan data di dalam komputer, nilai bit suatu data adalah 0 (nol) atau 1 (satu). Semua data yang ada pada komputer disimpan ke dalam satuan bit ini, termasuk gambar, suara, ataupun video hanya saja penerjemahan representasi bit pada masing-masing media yang tentunya akan berbeda.

Seperti penjelasan pada bagian sebelumnya bahwa format pewarnaan pada media gambar juga menggunakan satuan bit dalam penyimpanannya. Sebagai contoh pewarnaan *monochrome* menggunakan 1 bit untuk merepresentasikan warna hitam atau putih, pewarnaan *grayscale* menggunakan 8 bit untuk merepresentasikan tingkat keabuan dan pada pewarnaan RGB menggunakan 24 bit (8 bit untuk *Red,* 8 bit untuk *Green*, 8 bit untuk *Blue*).

Least Significant Bit (LSB) adalah bagian dari barisan data biner yang mempunyai nilai paling tidak berarti atau paling kecil. Bit LSB letaknya di paling kanan pada barisan biner, karena nilai 1 bit LSB pada barisan biner hanya merepresentasikan nilai 1 desimal, maka bit

ini dianggap tidak berarti. Sehingga jika terjadi perubahan pada nilai bit LSB maka tidak akan terjadi perubahan secara signifikan (Hasan et al., 2020).

Pada citra 24 bit, setiap piksel terdiri dari 3 *byte* yang merepresentasikan warna RGB. Sebagai contoh satu piksel berukuran 3 *byte* dapat disispkan pesan sebanyak 3 bit. Jika dalam 1 piksel dapat di sisipkan pesan sebanyak 3 bit maka untuk citra dengan ukuran 600 x 500 dapat disisipkan pesan sebanyak 600 x 500 x 3 = 900000 bit atau 11 900000 / 8 = 112500 *byte*. Gambar 5. di bawah ini adalah contoh gambar yang akan disisipi informasi. Gambar ini menggunakan format pewarnaan *grayscale*, artinya tiap pixel dari gambar ini direpresentasikan dengan nilai sepanjang 8 bit.

Gambar 5. Bananas.jpg

Dimisalkan data berupa teks "secret" akan disisipkan kedalam gambar tersebut. Jika direpresentasikan ke dalam *binary* kata "secret" menjadi.

Tabel 2. Konversi ASCII teks "secret"

Char	*ASCII*	*Hexa*	*Binary*
s	115	73	01110011
e	101	65	01100101
c	99	63	01100011
r	114	72	01110010
e	99	63	01100011
t	116	74	01110100

Dimisalkan nilai *binary* dari gambar bananas.jpg seperti berikut.

Tabel 3. Nilai biner bananas.jpg

00000000	00000000	00000001	00000001	00000001	00000001	00000001	00000001
00000000	00000000	00000001	00000001	00000001	00000001	00000001	00000001
00000000	00000000	00000001	00000001	00000001	00000001	00000001	00000001
00000001	00000001	00000010	00000010	00000010	00000011	00000011	00000011
00000001	00000001	00000010	00000010	00000010	00000011	00000011	00000011
00000001	00000001	00000010	00000010	00000010	00000011	00000011	00000011

Maka dalam penerapannya nilai bit pada kata "secret" akan disisipkan atau mengganti nilai bit ke-8 pada binary bananas.jpg.

Tabel 4. Nilai biner teks "secret"

0	1	1	1	0	0	1	1
0	1	1	0	0	1	0	1
0	1	1	0	0	0	1	1
0	1	1	1	0	0	1	0
0	1	1	0	0	0	1	1
0	1	1	1	0	1	0	0

Hasil akhir (citra-stego):

Tabel 5. Nilai biner bananas.jpg setelah disisipkan pesan

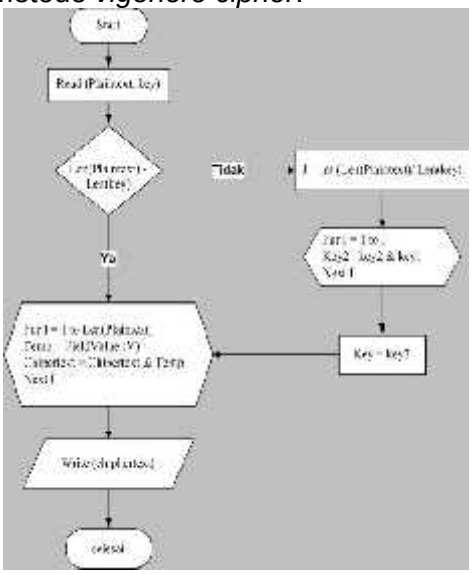
00000000	00000001	00000001	00000001	00000000	00000000	00000001	00000001
00000000	00000001	00000001	00000000	00000000	00000001	00000000	00000001
00000000	00000001	00000001	00000000	00000000	00000000	00000001	00000001
00000000	00000001	00000011	00000011	00000010	00000010	00000011	00000010
00000000	00000001	00000011	00000010	00000010	00000010	00000011	00000011
00000000	00000001	00000011	00000011	00000010	00000011	00000010	00000010

Setelah dikonstruksi ulang menjadi sebuah gambar digital, gambar bananas yang telah disisipkan informasi berupa kata "secret" akan memiliki persepsi sama terhadap gambar

bananas yang asli, karena perbedaan 1 bit pada warna RGB tidak dapat dideteksi oleh mata manusia.

3.5 Flowchart

Bagan alir *(Flowchart)* adalah bagan yang menggambarkan urutan instruksi proses dan hubungan satu proses dengan proses yang lainnya menggunakan simbol-simbol tertentu (Ridlo, 2017). Dalam pengoperasian komputer terutama dalam prosess pengolahan data terdapat beberapa simbol yang disebut *Flowchart.* Berikut ini adalah gambar 6. *flowchart* enkripsi dan dekripsi dari metode *vigenere cipher*.

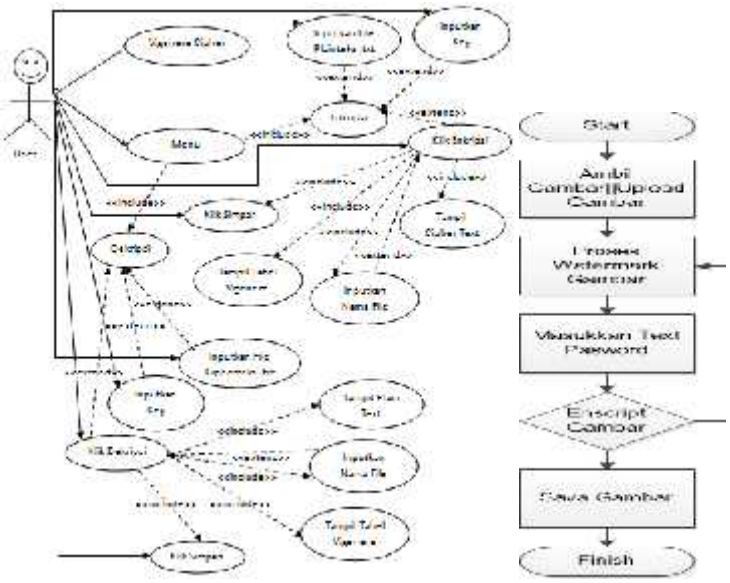


Gambar 6. Flowchart Enkripsi dan Dekripsi Vigenere Cipher

3.6 Use Case Program

Use case diagram menggambarkan fungsionalitas yang diharapkan dari sebuah sistem. Pada diagram ini menekankan "apa" yang diperbuat sistem, dan bukan "bagaimana" membuat sistem. Sebuah *use case* merepresentasikan sebuah interaksi antara aktor dengan sistem. Pada gambar memodelkan interaksi antara user dengan sistem kriptografi *vigenere cipher*.

Pada sistem aplikasi yang kami buat ini hanya terdapat seorang aktor yang dinamakan *user*. Hanya ada 1 (satu) *user* yang bisa mengoperasikan aplikasi. Terdapat 3 (tiga) menu data yang dapat dilakukan oleh *user*, dengan terlebih dahulu *user* harus memilih menu enkripsi ke aplikasi. Agar dapat memasukkan file *plainteks* yang bertipe .txt serta *key*-nya sehingga di dapatkan pesan *cipherteks*-nya. Kemudian pesan *cipherteks* dapat disimpan sebagai file yang bertipe .txt di komputer. Begitu juga dengan dekripsi dari file *cipherteks*-nya. Cara yang dilakukan sama seperti memasukkan file *plainteks* yang bertipe .txt.



Gambar 7. *Use case Diagram*

Selain itu terdapat metode penggunakan sistem program ini yaitu dengan upload gambar kemudian melakukan metode watermarking yang diinginkan lalu memasukkan text pasword sesuai dengan metode use case plaintext dan chipertext yang telah dijelaskan diatas yang kemudian dilanjutkan dengan enskripsi data lalu menyimpan data gambar yang telah dienskripsi tersebut.

PEMBAHASAN

4.1 Dashboard Rancangan Halaman Utama

Gambar 8. Dashboard Program

Halaman ini merupakan halaman dashboard utama yang digunakan sebagai *outer frame* untuk mengeksekusi program. Fitur dashboard program terdiri dari menu upload gambar, RGB (Red Grreen Blue) Watermarking Threshold dan Inverting Gambar. Selain itu juga terdapat fitur enskripsi gambar melalui metode kombinasi kriptografi dan steganographi dengan modifikasi teks *vigenere cipher* yang di implementasikan pada sistem pasword. Dari seluruh fitur yang dapat digunakan diaplikasi ini telah melalui pengujian. Beberapa pengujian yang telah kami lakukan antara lain :

4.2 Pengujian Watermarking

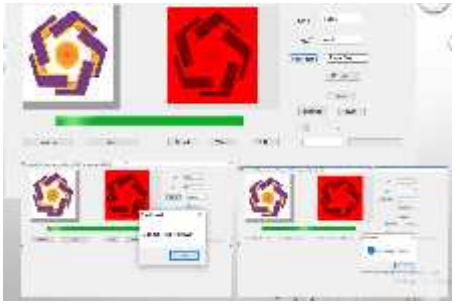
Gambar 9. Pengujian Watermarking

Pengujian Watermarking dilakukan dengan cara merubah ganbar citra asli yang kemudian di konversi pada citra RGB (Red Green Blue). Selain itu gambar citra asli juga dapat di Threshold dan Invertion untuk kemudian dilakukan enskripsi terhadap gambar tersebut dengan integrasi metode kriptografi dan steganografi sebagai implementasi dari sistem security

4.3 Pengujian Pengambilan dan Penyimpanan Gambar

Metode pertama dari sistem pengujian adalah sistem upload atau mengambil gambar dari file yang telah tersedia pada laman komputer. Jenis file gambar yang dapat diupload adalah tipe JPG dan PNG. Ukuran gambar yang dapat di upload maksimal adalah 10 mb. Setelah memilih metode watermarking baik dengan RGB, Threshold dan Invertion untuk menyimpan gambar dapat menekan tombol save dan menentukan lokasi penyimpanan gambar.

4.4 Pengujian Enskripsi Gambar



Gambar 10. Proses Enskripsi Gambar

Metode enskripsi data dilakukan untuk melindungi gambar dengan aman. Metode ini dilakukan dengan konsep kombinasi kriptografi dan steganografi yang diimplementasikan dalam bentuk logika penyusunan pasword dan kata kunci dengan output berupa chiper text dan melakukan eksekusi enskripsi. Apabila enskripsi berhasil dilakukan maka akan muncul pemberitahuan "Gambar Telah tersimpan" dan jika mengalami gagal enskripsi maka akan muncul pemberitahuan " Pasword Anda Salah", jika hal ini terjadi maka dapat dilakukan proses dari awal.

4.5 Data Pengujian secara kesuluruhan

No	Hasil Cover Image	Nama File Awal (.jpg)	Ukuran Awal(Kb)	Nama File Akhir (.jpg)	Ukuran Akhir (File)	Jumlah Karakter	Deskripsi Stego (Info Pasword)	Proses Encrypsi
1		Logo_Amikom	8.01	Amikom_Red	12.3	41854	messi,ronaldo, soccer goal	Berhasil
2		Logo_Amikom	8.01	Amikom_Green	10.9	31768	modric,kaka,madrid goal	Berhasil
3		Logo_Amikom	8.01	Amikom_Blue	11.8	38901	xavi,suarez,barcawin	Berhasil
4		Logo_Amikom	8.01	Amikom_Invert	14.1	58342	zidane,henry,pranciswin	Berhasil

Gambar 11. Daftar Pengujian Program Secara Keseluruhan

Metode pengujian secara keseluruhan dapat dilihat dari tabel diatas. Pengujian dilakukan pada file awal yang sama dengan berbagai macam jenis watermarking mulai RGB watermarking serta threshold watermarking. Kesimpulan dari pengujian sistem dengan file gambar yang diuji sama adalah ukuran file setelah dienskripsi menjadi lebih besar dari ukuran semula, selain itu juga terdapat penambahan jumlah karakter.

KESIMPULAN

Berdasarkan keseluruhan proses yang dilakukan untuk melakukan watermarking media gambar dengan implementasi kombinasi Kriptografi dan Steganografi pada Teks Pesan menggunakan Algoritma Vigenere Cipher ini dapat disimpulkan bahwa implementasi jurnal ini dilakukan untuk melakukan penerapan watermarking dengan implementasi kriptografi dan steganografi pada pesan gambar dengan menggunakan metode vigenere cipher. Sistem ini dirancang dengan melakukan perancangan sistem prangkat lunak dengan luaran bentuk enkripsi dan dekripsi text yang dapat diprogram dengan menggunakan bahasa pemprograman C++ Visual Studio. Hasil luaran penelitian ini adalah sebuah implementasi program sistem watermarking menggunakan kombinasi kriptografi dan steganografi yang terinterasi algoritma vigenere cipher berbasis pemrogaman C++ Visual Studio.

DAFTAR PUSTAKA

Ariyus, D. (2008a). Komunikasi Data. In *Andi*. https://doi.org/10.1186/s13104-016-1915-8

Ariyus, D. (2008b). Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi. In *Journal of Chemical Information and Modeling*. https://doi.org/10.1017/CBO9781107415324.004

Astawa, I. P. P., & Imawati, I. A. P. F. (2013). Identifikasi Lokasi Iris Mata Berbasis Transformasi Hough dan Deteksi Tepi Canny. *Eksplora Informatika*.

Basuki Rakhmat; Muhammad Fairuzabadi. (2010). Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vigenère Dan Rc4. *Zhurnal Eksperimental'noi i Teoreticheskoi Fiziki*.

Hasan, N. F., Dengen, C. N., & Ariyus, D. (2020). Analisis Histogram Steganografi Least Significant Bit Pada Citra Grayscale. *Digital Zone: Jurnal Teknologi Informasi Dan Komunikasi*. https://doi.org/10.31849/digitalzone.v11i1.3413

Munir, R. (2019). Kriptografi. In *2*.

Ridlo, I. A. (2017). Panduan pembuatan flowchart. *Fakultas Kesehatan Masyarakat*.

Schneier, B. (1996). Applied Cryptography. *Electrical Engineering*. https://doi.org/10.1.1.99.2838s