Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 3, No 3, June 2024
Hal 221-233
https://ejurnal.seminar-id.com/index.php/bulletinds

Pengamanan Pesan Teks Terenkripsi Algoritma AES yang Disembunyikan kedalam Citra Menggunakan Algoritma Gifhsuffle

Hary Octariza

Program Studi Teknik Informatika, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Budi Darma, Medan, Indonesia
Email: haryOza1525@gmail.com
Email Penulis Korespondensi: haryOza1525@gmail.com

Abstrak−Kemajuan sistem informasi di bidang ilmu komputer dan telekomunikasi sangatlah berkembang dan maju dengan pesat. Teknologi komputer sangat dibutuhkan untuk pekerjaan perkantoran ataupun personal menjadi lebih cepat, pertukaran data-data semakin mudah dilakukan. Data dapat berupa pesan dalam bentuk teks, gambar, audio maupun video. Data-data yang bersifat pribadi dan rahasia tidak dapat diketahui oleh umum atau dipublikasikan. Pengkombinasian teknik kriptografi dan teknik steganografi dapat meningkatkan keamanan pesan teks sehingga dapat memanimalisir terjadinya kerusakan pesan teks yang dapat dilakukan oleh pihak-pihak tdak bertanggung jawab dan merugikan pemilik pesan teks. Algoritma AES adalah algoritma yang dapat melakukan teknik kriptografi, sedangkan algoritma Gifhsuffle adalah algoritma yang dapat melakukan teknik steganografi. Penelitian ini mengggunakan algoritma AES untuk proses enkripsi dan dekripsi serta menggunakan algoritma Gifhsuffle untuk proses encoding (penyisipan) dan decoding. Sebuah file yang berisikan pesan akan di enkripsi menggunkan algoritma AES sehingga menghasilkan ciphertext yang dilanjutkan dengan penyembunyian ke dalam file citra yang berformat GIFmenggunakan proses encoding algoritma Gifhsuffle sehingga menghasilkan Stego Image. Proses ini dapat meningkatkan keamanan pesan dan mempresulit pihak-pihak yang tidak bertanggung jawab menemukan pesan tersebu.

Kata Kunci: Kriptografi, Steganografi, Algoritma AES, Algoritma Gifhsuffle, Citra, GIF

Abstract−The advancement of information systems in the field of computer science and telecommunications is growing and advancing rapidly. Computer technology is needed for office or personal work to be faster, data exchange is easier to do. Data can be in the form of messages in the form of text, images, audio or video. Data that is private and confidential cannot be known by the public or published. The combination of cryptographic techniques and steganographic techniques can increase the security of text messages so as to minimise the occurrence of text message damage that can be done by irresponsible parties and harm the owner of the text message. The AES algorithm is an algorithm that can perform cryptographic techniques, while the Gifhsuffle algorithm is an algorithm that can perform steganographic techniques. This research uses the AES algorithm for the encryption and decryption process and uses the Gifhsuffle algorithm for the encoding and decoding process. A file containing a message will be encrypted using the AES algorithm to produce a ciphertext followed by hiding it in a GIF-formatted image file using the Gifhsuffle algorithm encoding process to produce a Stego Image. This process can increase the security of the message and make it difficult for irresponsible parties to find the message.

Keywords: Cryptography, Steganography, AES Algorithm, Gifhsuffle Algorithm, Image, GIF

1. PENDAHULUAN

Kemajuan sistem informasi di bidang ilmu komputer dan telekomunikasi sangatlah berkembang dan maju dengan pesat. Teknologi komputer sangat dibutuhkan untuk pekerjaan perkantoran ataupun personal menjadi lebih cepat, pertukaran data-data semakin mudah dilakukan. Data dapat berupa pesan dalam bentuk teks, gambar, audio maupun video. Data-data yang bersifat pribadi dan rahasia tidak dapat diketahui oleh umum atau dipublikasikan. Data rahasia dalam bentuk pesan teks sangatlah rentan terhadap penyadapan oleh pihak-pihak yang dapat merugikan pemilik data. Dalam hal ini diperlukan adanya keamanan data untuk mengamankan data dari berbagai ancaman yang mungkin akan timbul. Salah satu cara yang dapat melakukan pengamanan data ataupun pesan adalah teknik penyandian data yang disebut dengan kriptografi dan teknik penyembunyian data yang disebut dengan steganografi.

Kriptografi merupakan teknik penyandian pesan dengan cara mengubahnya menjadi kode-kode dan simbol-simbol yang berguna untuk menjaga kerahasiaan pesan tersebut. Kriptografi bekerja dengan dua konsep yaitu enkripsi dan dekripsi. Enkripsi adalah proses penyandian pesan yang diubah menjadi bentuk yang hampir tidak dikenali sebagai pesan awal dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk penyandian tersebut menjadi pesan awal. Steganografi merupakan teknik penyembunyian pesan dengan cara menyisipkan pesan kedalam sebuah media. Dengan teknik steganografi, pesan yang ingin di sampaikan disembunyikan dalam suatu media, sehingga diharapkan tidak akan menimbulkan kecurigaan dari pihak lain yang tidak diinginkan untuk mengetahui pesan rahasia tersebut.

Algoritma Advanced Encryption Standard (AES) dan Gifhsuffle adalah salah satu algoritma yang dapat digunakan untuk mewujudkan teknik kriptograf. dan steganografi. Algoritma Advanced Encryption Standard (AES) adalah algoritma yang menggunakan sistem penyandian blok bersifat non-Feistel sebab menggunakan komponen yang selalu memiliki invers dengan panjang blok 128 blok. Algoritma AES memiliki panjang kunci 128,192 dan 256 bit dengan proses berulang yang disebut ronde [1]. Sedangkan algoritma Gifhsuffle adalah algoritma yang dapat menyembunyikan pesan ke dalam sebuah citra yang berformat GIF. Algoritma Gifhsuffle bekerja dengan 2 proses yaitu encoding dan decoding [2].

Berdasarkan masalah di atas, penelitian ini menguraikan proses pengamanaan pesan berupa teks yang akan dienkripsi dan dekripsi menggunakan algoritma kriptografi AES, kemudian hasil enkripsi berupa chipertext akan

Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 3, No 3, June 2024
Hal 221-233
https://ejurnal.seminar-id.com/index.php/bulletinds

disembunyikan kembali kedalam objek sebuah citra dengan format GIF berdasarkan algoritma Gifhsuffle, penyembunyian ini disebut dengan proses encoding. Sedangkan proses pengembalian pesan teks rahasia dilakukan dengan proses decoding berdasarkan algoritma Gifhsuffle. Hasil decoding merupakan data chipertext dari algoritma AES yang akan didekripsi kembali, sehingga pesan teks rahasia dapat dioptimalkan keamananya dengan dua teknik pengamanan yang berbeda.

2. METODOLOGI PENELITIAN

2.1 Kriptografi

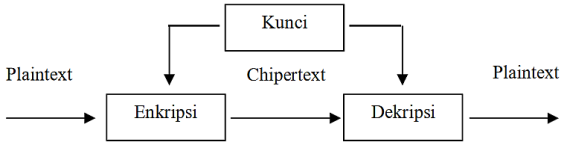
Kriptografi mempunyai peranan penting dalam dunia komputer. Hal ini disebabkan karena banyaknya informasi bersifat rahasia yang disimpan dan dikirimkan melaui media-media komputer. Informasi-informasi ini biasanya berisikan dokumen-dokumen penting dan data keuangan dari suatu instansi yang tidak ingin dibaca oleh pihak lain yang tidak berhak atas informasi tersebut. Oleh sebab itu ilmu kriptografi setiap saat terus dikembangkan oleh orang untuk dapat menjaga keamanan dan kerahasiaan informasi-informasi tersebut. Kriptografi berasal dari kata Yunani, yaitu Crypto yang berarti rahasia dan Grapho yang berarti menulis. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta authentikasi data. Secara umum kriptografi dapat diartikan sebagai ilmu dan seni penyandian yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu pesan. Kriptografi pada dasarnya sudah dikenal sejak lama. Menurut catatan sejarah, kriptografi sudah digunakan oleh bangsa Mesir sejak 4000 tahun yang lalu oleh raja-raja Mesir pada saat perang untuk mengirimkan pesan rahasia kepada panglima perangnya melalui kurir-kurinya [3]. Kriptografi adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi mendapatkan kembali data asli. Proses enkripsi dilakukan menggunakan suatu algoritma dengan beberapa parameter. Biasanya algoritma tidak dirahasiakan, bahkan enkripsi yang mengandalkan kerahasiaan algoritma dianggap sesuatu yang tidak baik. Rahasia terletak dibeberapa parameter yang digunakan, jadi kunci ditentukan oleh parameter. Parameter yang menentukan kunci dekripsi itulah yang harus dirahasiakan (parameter menjadi ekuivalen dengan kunci). Enkripsi adalah proses pengacakan naskah asli (plaintext) menjadi naskah acak (ciphertext) yang sulit untuk dibaca oleh seseorang yang tidak mempunyai kunci dekripsi. Sedangkan dekripsi adalah kebalikan dari enkripsi [3].

Berdasarkan uraian di atas, maka dapat disimpulkan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan menggunakan teknik enkripsi dan dekripsi, yaitu dengan cara melakukan proses pengacakan teks asli (plaintext) dengan menggunakan kunci (key) menjadi teks acak atau simbol-simbol tertentu (chipertext) sehingga makna dari teks asli tidak dapat diketahui oleh pihak yang tidak dikehendaki. Algoritma kriptografi adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi. Ada dua macam algoritma kriptografi, yaitu algoritma simetri (symmetric algorithms) dan algoritma asimetri (asymmetric algorithms).

a. Kriptografi Kunci Simetri

Kriptografi simetri disebut juga sebagai kriptografi konvensional. Kriptografi simetri adalah kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Kriptografi simetri sering disebut sebagai algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma satu kunci dan mengharuskan pengirim dan penerima menyetujui suatu kunci sebelum mereka dapat berkomunikasi dengan aman [3].

Berdasarkan uraian di atas, maka dapat disimpulkan bahwa kriptografi kunci simetri merupakan algoritma kunci tunggal atau algoritma satu kunci yang digunakan oleh dua orang atau dua golongan ketika ingin bertukar informasi, yang dalam hal ini disebut sebagai pengirim dan penerima untuk melakukan proses enkripsi dan dekripsi sehingga mereka dapat bertukar informasi atau berkomunikasi dengan aman. Berikut adalah gambar yang mengilustrasikan kinerja dari proses enkripsi dan dekripsi kunci simetri.



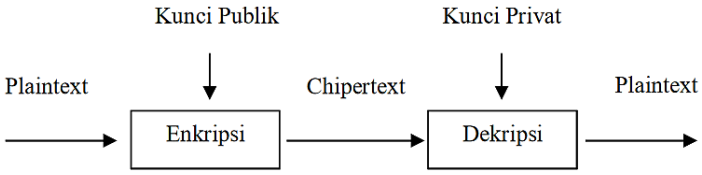
Gambar 1. Kriptografi Kunci Simetri

b. Kriptografi Kunci Asimetri

Kriptografi kunci asimetri yang sering disebut juga kriptografi kunci publik adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Algoritma asimetri ini disebut kunci publik karena kunci untuk enkripsi dapat dibuat publik yang berarti semua prang boleh mengetahuinya. Sembarang orang dapat menggunakan kunci enkripsi tersebut untuk mengenkrip pesan, namun hanya orang tertentu yaitu calon penerima pesan dan sekaligus pemilik kunci dekripsi yang merupakan pasangan kunci publik, yang dapat melakukan dekripsi terhadap pesan tersebut. Dalam sistem ini, kunci enkripsi disebut kunci publik, sementara kunci dekripsi disebut dengan kunci privat [3].

Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 3, No 3, June 2024
Hal 221-233
https://ejurnal.seminar-id.com/index.php/bulletinds

Berdasarkan uraian di atas, maka dapat disimpulkan bahwa kriptografi kunci asimetri merupakan algoritma yang menggunakan kunci yang berbeda untuk melakukan proses enkripsi dan dekripsi, kunci yang berbeda tersebut ialah kunci public dan kunci privat. Kunci public digunakan pada saat ingin melakukan proses enkripsi, sedangkan kunci privat digunakan untuk proses dekripsi. Berikut adalah gambar yang mengilustrasikan kinerja dari proses enkripsi dan dekripsi kunci asimetri.



Gambar 2. Kriptografi Kunci Asimetri

2.2 Algoritma AES

Advanced Encryption Standard (AES) merupakan sistem penyandian blok yang bersifat non-Feistel karena AES menggunakan komponen yang selalu memiliki invers dengan panjang blok 128 bit. Kunci AES dapat memiliki panjang kunci bit 128, 192 dan 256 bit, menggunakan proses yang berulang yang disebut ronde [1]. Adapun jumlah ronde yang digunakan tergantung dari panjang kunci AES seperti pada tabel 1 :

Tabel 1. Hubungan antara jumlah ronde dan panjang kunci

Panjang Kunci AES (bit)	Jumlah Ronde (Nr)
128	10
192	12
256	14

Proses di dalam AES merupakan tranformasi terhadap state. Enkripsi AES adalah tranformasi terhadap state secara berulang delam beberapa ronde [1].
Algoritma Rijndael mempunya 3 parameter yaitu :

1. Plaintext adalah array yang berukuran 16 byte, data masukan.
2. Chipertext adalah array yang berukuran 16 byte, yang berisi hasil enkripsi.
3. Key adalah array berukuran 16 byte, berisi kunci ciphering (chiper key).

Algoritma enkripsi AES menggunakan 4 jenis transformasi subtitusi yang disebut SubBytes, permutasi yang disebut dengan ShiftRows, pencampurannya disebut MixColoms, dan penambahan kunci disebut AddRoundKey.

2.2.1 Proses Enkripsi Algoritma Advanced Encryption Standard (AES)

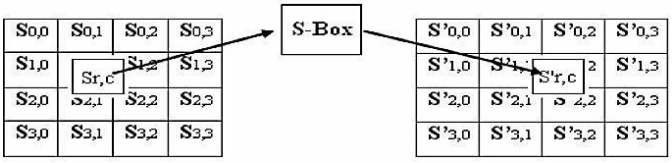
Proses enkripsi AES 128 bit adalah sebagai berikut [4] :

1. *AddRoundKey*
   Melakukan XOR antara state awal (*plaintext*) dengan *chiper key*.
2. Putaran sebanyak Nr-1 kali. Proses yang dilakukan pada setiap putaran adalah:
   a. *SubBytes*
   Proses subsitusi *byte* adalah operasi yang akan melakukan subsitusi tidak linier dengan cara mengganti setiap *byte state* dengan *byte* pada sebuah tabel yang dinamakan tabel S-Box. Sebuah tabel S-Box terdiri dari 16 x 16 baris dan kolom dengan masing-masing berukuran 1 *byte*. Tabel S-Box dan proses *SubBytes* akan diperlihatkan pada gambar 3 di bawah ini.

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Gambar 3. Tabel S-Box[5]

Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 3, No 3, June 2024
Hal 221-233
https://ejurnal.seminar-id.com/index.php/bulletinds

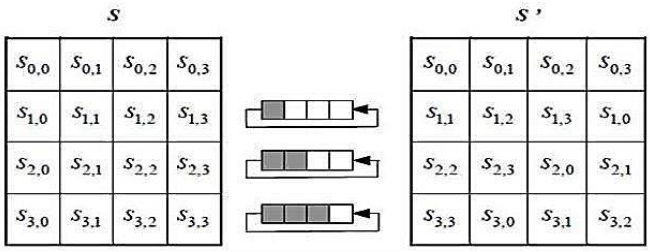


Gambar 4. Proses SubBytes

Dalam pensubstitusinya adalah setiap byte pada array state, misalkan S[r,c]=xy, yang mana dalam hal ini xy adalah digit heksadesimal dari nilai S[r,c], maka nilai subsitusinya, dinyatakan dengan S'[r,c], merupakan elemen dalam S – Box yaitu perpotongan baris x dan kolom y. Misalnya S[0,0]= 19, maka S'[0,0] = d4

b. ShiftRows

ShiftRows seperti namanya adalah sebuah proses yang melakukan shift atau pergeseran pada setiap elemen blok/tabel yang dilakukan per barisnya, yaitu baris pertama tidak dilakukan pergeseran, baris kedua dilakukan pergeseran 1 byte, baris ketiga dilakukan pergeseran 2 byte, dan baris keempat dilakukan pergeseran 3 byte. Pergeseran tersebut terlihat dalam sebuah blok adalah sebuah pergeseran tiap elemen ke kiri tergantung berapa byte tergesernya, tiap pergeseran 1 byte berarti bergeser ke kiri sebanyak satu kali.



Gambar 5. Proses SiftRows

c. MixColumn

MixColums adalah proses ketiga dalam satu ronde enkripsi AES, dalam penggabungan kolom ini, prosesnya akan beroperasi pada tiap kolom dari tabel state. Operasi ini menggabungkan 4 byte dari setiap kolom tabel state dan menggabungkan transformasi linier. Proses MixColumns memperlukan setiap kolom sebagai polynominal 4 suku dalam Glois field (GF) dan kemudian dikalikan dengan a(x) modulo (x4+1) adapun nilai polynominal dapat di lihat dalam tabel 2 berikut :

Tabel 2. Polynominal

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

Perkalian dalam matrik dapat dituliskan seperti gambar 2.5 di bawah ini :

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

Gambar 6. Perkalian Matrik MixColumn[6]

Sebagai hasil dari perkalian ini, empat byte dalam kolom digantikan oleh seperti gambar 7 yang berikut.

$$d_0 = 2 \bullet b_0 \oplus 3 \bullet b_1 \oplus 1 \bullet b_2 \oplus 1 \bullet b_3$$
$$d_1 = 1 \bullet b_0 \oplus 2 \bullet b_1 \oplus 3 \bullet b_2 \oplus 1 \bullet b_3$$
$$d_2 = 1 \bullet b_0 \oplus 1 \bullet b_1 \oplus 2 \bullet b_2 \oplus 3 \bullet b_3$$
$$d_3 = 3 \bullet b_0 \oplus 1 \bullet b_1 \oplus 1 \bullet b_2 \oplus 2 \bullet b_3$$

Gambar 7. Hasil Perkalian Matrik MixColumn

Setiap operasi penjumlahan dilakukan dengan operasi XOR, dan untuk perkalian dilakukan dalam Galois Field.

d. AddRoundKey.

Tahap ini, subkey digabungkan dengan state. Proses penggabungannya dilakukan menggunakan operasi XOR untuk setiap byte dari subkey dengan byte yang bersangkutan dari state. Setiap tahap, subkey dibangkitkan dari kunci utama dengan menggunakan proses key schedule. Setiap subkey berukuran sama dengan state yang bersangkutan, dan hasil dari operasi XOR akan disimpan di array state.

3. Final round
   Proses untuk putaran terkhir yang meliputi tiga proses operasi, yaitu : SubBytes, ShifRows, AddRoundKey.
4. Key Expension
   Ekspansi cipherkey di gunakan untuk membentuk roundkey yang akan di gunakan pada langkah-langkah enkripsi dan dekripsi

2.2.2 Proses Dekripsi Algoritma Advanced Encryption Standard (AES)

Proses dekripsi AES 128 bit adalah sebagai berikut [4] :

1. AddRoundKey
   Merupakan proses melakukan XOR antara state awal (cipherteks) dengan cipher key. Tahap ini disebut juga initial round.
2. Putaran sebanyak Nr-1 kali. Proses yang dilakukan pada setiap putaran yaitu :
   InvShiftRow, InvSubByte, AddRoundKey, InvMixColumn.
3. Finalround
   Proses untuk putaran terkhir yang meliputi tiga proses operasi, yaitu : InvShiftRow, InvSubByte, AddRoundKey

2.3 Steganografi

Steganografi (steganography) adalah ilmu dan seni menyembunyikan pesan rahasia (hiding message) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia. Kata steganografi berasal dari Bahasa Yunani yang berarti “tulisan tersembunyi” (covered writing). Steganografi terdapat konsep pesan yang akan disampaikan kepada orang lain, tentunya ada beberapa pesan yang penting sehingga hanya orang yang berhak saja yang dapat menerimanya, sehingga dalam bidang Steganografi ini pesan tersebut akan disembunyikan, artinya ini berhubungan dengan keamanan pesan. Jadi, terdapat dua hal yang penting disini yaitu penyampaian pesan dan keamanannya [7].

Berdasarkan uraian di atas, maka dapat disimpulkan bahwa Steganografi merupakan ilmu dan seni yang digunakan untuk menyembunyikan pesan atau data rahasia kedalam media seperti citra digital atau gambar, suara, dan video sehingga pesan atau data rahasia tersebut tidak terdeteksi oleh indra manusia.

2.4 Gifshuffle

Gifshuffle yang dikembangkan oleh Matthew Kwan adalah salah satu algoritma Steganografi yang menggunakan berkas citra dengan format GIF. Akan dibahas bagaimana proses encoding dan decoding pesan dalam citra dengan menggunakan gifshuffle. Algoritma ini melakukan penyisipan pesan dengan cara mengganti susunan palet warna yang ada dalam sebuah berkas citra dengan format GIF. Dalam algoritma ini tidak terjadi perubahan apapun dalam data berkas dengan format GIF. Sesuai dengan namanya gifshuffle akan melakukan Shuffle terhadap palet warna dari sebuah berkas gif. Shuffle jika diterjemahkan ke dalam bahasa Indonesia berari memutar. Sehingga dapat diartikan bahwa gifshuffle adalah algoritma yang memanfaatkan penukaran posisi ke 256 palet warna dalam berkas citra berformat GIF. Hal tersebut aman dilakukan karena dua buah berkas GIF dengan palet warna yang berbeda akan ditampilkan secara sama persis [2].

Berdasarkan uraian di atas, maka dapat disimpulkan bahwa gifshuffle adalah algoritma steganografi yang digunakan untuk menyembunyikan pesan atau data ke dalam media citra dengan format GIF. Algoritma gifshuffle memiliki dua macam aktifitas yang berbeda namun saling bersangkutan, yaitu :

1. Encoding
   Encoding merupakan proses penyisipan pesan atau data teks ke media, citra berformat GIF sebagai media untuk menyembunyikan pesan atau data teks tersebut. Hasil dari proses penyisipan pesan atau data disebut sebagai stego image.
2. Decoding
   Decoding merupakan proses pengekstrakan pesan atau data teks dari gambar, masukannya adalah citra berformat GIF tempat pesan atau data teks disembunyikan (stego image) dan keluarannya adalah pesan atau data teks. Proses ini dapat dikatakan sebagai proses pembalikan dari encoding.

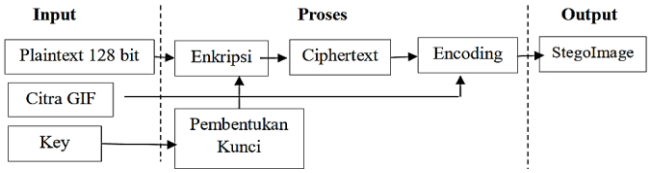
Algoritma gifshuffle pada intinya memanfaatkan header file GIF yang menyimpan palte warna sebagai media penyisipan pesan. Algoritma ini tidak terjadi perubahan apapun dalam data berkas dengan format GIF. Sehingga menambah aspek robustness dari algoritma ini. Sesuai dengan namanya Gifshuffle akan melakukan Shuffle terhadap palet warna dari sebuah berkas GIF. Shuffle jika diterjemahkan ke dalam bahasa Indonesia berarti memutar. Sehingga dapat diartikan bahwa gifshuffle adalah algoritma yang memanfaatkan penukaran posisi ke 256 palet warna dalam berkas citra berformat GIF. Hal tersebut aman dilakukan karena dua buah berkas GIF dengan palet warna yang berbeda akan ditampilkan secara sama persis.

Dengan dilakukannya penukaran posisi maka akan dapat diperoleh sebuah informasi berkaitan dengan perbedaan posisi dengan posisi awal. Sebagai contoh jika kita mempunyai 52 kartu remi maka kita akan dapat mengurutkan kartu-kartu tersebut dalam 52! cara. Dengan kata lain jika kita diberikan n buah kartu maka kita dapat menyimpan log2(n!) bit informasi berdasarkan pengurutannya [8]. Langkah-langkah Algoritma GifShuffle.

1. Dimulai dengan pesan yang akan disisipkan. Pesan tersebut akan diubah kedalam sebuah bentuk biner dengan representasi 1/0.
2. Anggap kumpulan representasi biner yang tadi diperoleh sebagai sebuah angka. Biasanya langkah ini akan menghasilkan sebuah bilangan yang sangat besar karena konversi dari biner yang besar . Namakan bilangan yang diperoleh ini sebagai M.
3. Hitung jumlah warna yang terkandung dalam berkas GIF yang ingin disisipkan. Namakan jumlah yang diperoleh ini sebagai N. Apabila M > N!-1 maka pesan yang ingin disisipkan berukuran terlalu besar sehingga proses penyisipan tidak dapat dilakukan.
4. Urutkan warna dalam palet warna sesuai dengan urutan yang natural. Setiap warna dengan format RGB dikonversikan ke bilangan integer dengan aturan (merah* 65536 + hijau * 256 + biru). Kemudian diurutkan berdasarkan besar bilangan interger yang mewakili warna tersebut.
5. Lakukan iterasi terhadap variabel I dengan nilai I dari 1 sampai N. Setiap warna dengan urutan N-i dipindahkan keposisi baru yaitu M mod i, kemudian M dibagi dengan i.
6. Kemudian palet warna yang baru hasil iterasi pada langkah 5 dimasukkan ke dalam palet warna berkas GIF. Apabila ada sebuah tempat yang diisi oleh 2 buah warna maka warna yang sebelumnya menempati tempat tersebut akan digeser satu tempat ke samping.
7. Berkas GIF dengan susunan yang baru akan menghasilkan ukuran gambar yang sama, tetapi sudah disisipi pesan. Berikut ini adalah hasil dari penyisipan gifshuffle

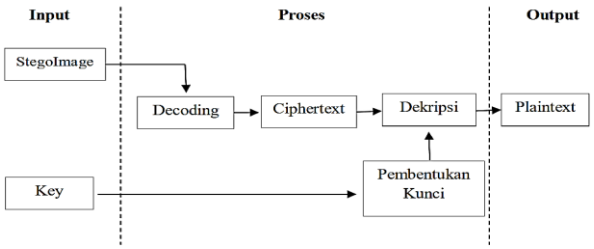
3. HASIL DAN PEMBAHASAN

Pada bab ini dilakukan pengumpulan informasi dan penguraian mengenai proses yang akan digunakan untuk membangun sistem peningkatan keamanan data teks terenkripsi algoritma AES menggunakan steganografi Gifshuffle. Dalam hal ini akan diuraikan tentang proses penyisipan data teks terenkripsi algoritma AES ke suatu media menggunakan steganografi dengan algoritma Gifshuffle. Sebelum dilakukannya proses penyisipan, terlebih dahulu dilakukan proses enkripsi pada pesan atau data teks menggunakan algoritma AES untuk menjaga keaslian dari pesan tersebut. Sehingga pesan atau data teks yang telah dienkripsi tersebut akan disisipkan ke suatu media citra GIF menggunakan steganografi Gifshuffle. Berkaitan dengan hal di atas, tahapan yang akan dilakukan adalah melakukan penginputan. Dalam hal penginputan, data yang akan dimasukkan yaitu Plaintext dengan panjang 128 bit, Citra GIF dengan ukuran sampel 10x13, dan key dengan panjang 128 bit. Berikutnya dilakukan proses pembentukan kunci, lalu plaintext dienkripsi dengan algoritma AES menggunakan key yang telah dibentuk. Ketika proses enkrpsi selesai dan menghasilkan ciphertext maka proses selanjutnya yaitu melakukan encoding atau penyisipan, sehingga setelah dilakukannya proses encoding maka keluaran atau output yang dihasilkan berupa StegoImage.Berikut ini adalah gambaran mengenai proses yang akan dilakukan:



Gambar 8. Gambar Tahapan Enkripsi dan Encoding

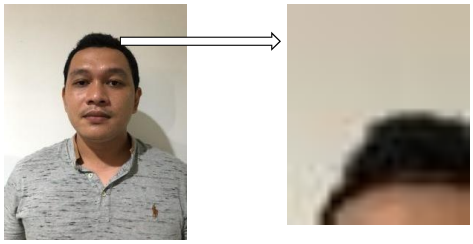
Tahapan decoding dan dekripsi merupakan kebalikan dari tahapan enkripsi dan encoding.Dalam tahapan ini juga mempunyai penginputan yaitu penginputan StegoImage, lalu dilakukan proses decoding atau pengekstrakan dengan menggunakan steganografi algoritma Gifshuffle. Setelah selesai melakukan proses pengekstrakan maka pesan yang disisipkan pada citra GIF akan muncul, dalam hal ini berupa ciphertext. Kemudian dilakukan proses dekripsi pada ciphertext dengan menggunakan kriptografi algoritma AES. Setelah selesai melakukan proses dekripsi maka keluaran atau outputyang dihasilkan yaitu plaintext atau teks asli. Berikut ini adalah gambaran mengenai proses tahapan yang akan dilakukan :



Gambar 9. Gambar Tahapan Decoding dan Dekripsi

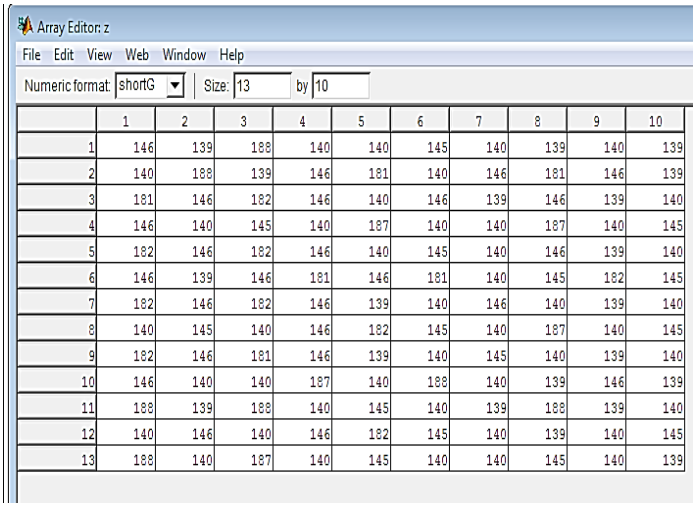
Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 3, No 3, June 2024
Hal 221-233
https://ejurnal.seminar-id.com/index.php/bulletinds

Adapun media yang digunakan untuk melakukan penyisipan adalah sebuah citra digital dengan format GIF resolusi 100 x 133pixel. Gambar berikut akan diambil 10 x 13pixel sebagai sampel dalam perhitungan manual. Pixel tersebut akan diambil nilai desimal palet warnanya.



Gambar 10. Sampel Gambar 10 x 13

Nilai desimal palet warna pada setiap pixel akan diekstraksi menggunakan software matlab. Perintah yang digunakan untuk menampilkan nilai palet warna didalam matlab adalah sebagai berikut :
G = imread (‘Tempat menyimpan file citra\File citra *GIF’);
Adapun hasil proses ekstraksi setiap pixel padasoftware matlab adalah sebagai berikut :


Array Editor: z

File Edit View Web Window Help

Numeric format: shortG Size: 13 by 10

	1	2	3	4	5	6	7	8	9	10
1	146	139	188	140	140	145	140	139	140	139
2	140	188	139	146	181	140	146	181	146	139
3	181	146	182	146	140	146	139	146	139	140
4	146	140	145	140	187	140	140	187	140	145
5	182	146	182	146	140	145	140	146	139	140
6	146	139	146	181	146	181	140	145	182	145
7	182	146	182	146	139	140	146	140	139	140
8	140	145	140	146	182	145	140	187	140	145
9	182	146	181	146	139	140	145	140	139	140
10	146	140	140	187	140	188	140	139	146	139
11	188	139	188	140	145	140	139	188	139	140
12	140	146	140	146	182	145	140	139	140	145
13	188	140	187	140	145	140	140	145	140	139

Gambar 11.Hasil Nilai Warna Setiap Pixel

Tampilan program merupakan tampilan dari aplikasi dengan penerapan algoritma AES pada enkripsi dan dekirpsi, dan algoritma Gifshuffle pada encoding dan decoding. Aplikasi ini dibuat dengan bebasis desktop. Aplikasi yang akan dijalankan dibangun dengan menggunakan software Microsoft Visual Studio 2008 dengan bahasa pemograman visual basic. Tampilan aplikasi program yang dibutuhkan diantaranya yaitu tampilan input dan tampilan output. Tampilan input tediri dari interface aplikasi, tampilan output terdiri dari hasil dari proses enkripsi dan dekripsi, serta encoding dan decoding.

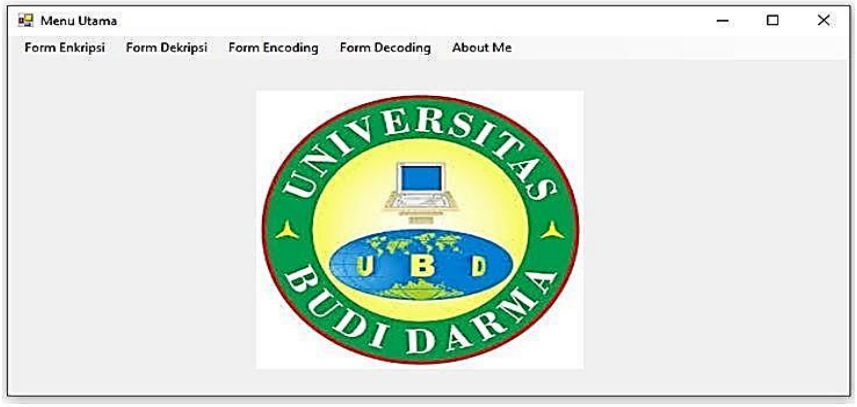
a. Tampilan Input

   Tampilan input merupakan tampilan yang akan menjelaskan berapa form aplikasi yang digunakan untuk kebutuhan program yang dibutuhkan diantaranya yaitu form menu utama, form enkripsi untuk menu enkripsi, form dekripsi untuk menu dekripsi, form encoding untuk menu encoding, form decoding untuk menu decoding,dan form about me tentang informasi profil penulis.

   1. Form Menu Utama

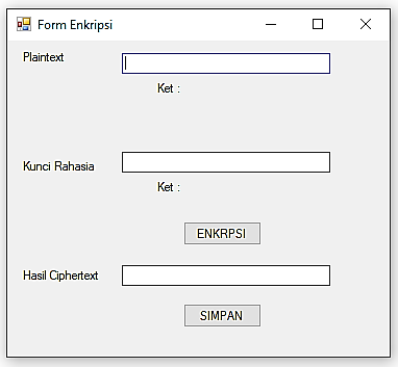
      Form menu utama merupakan form yang pertama kali muncul saat aplikasi dijalankan. Form menu utama memiliki beberapa sub menu diantaranya adalah menu form enkripsi, menu form dekripsi, menu form encoding, menu form decoding, dan menu form about me. Adapun tampilan halaman menu utama pada aplikasi dapat dilihat pada gambar di bawah ini.

Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 3, No 3, June 2024
Hal 221-233
https://ejurnal.seminar-id.com/index.php/bulletinds



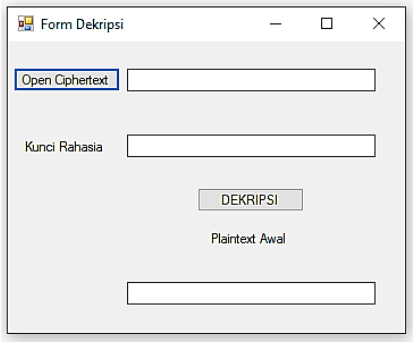
Gambar 12. Form Menu Utama

2. Form Enkripsi
   Form enkripsi merupakan form yang digunakan untuk melakukan proses enkripsi. Pada form ini disediakan interface untuk memasukkan plaintext, memasukkan kunci rahasia, label untuk menampilkan keterangan tentang panjang plaintext dan kunci rahasia, button enkripsi untuk melakukan proses enkripsi serta button simpan untuk menyimpan hasil ciphertext. Tampilan untuk form enkripsi dapat dilihat pada gambar berikut.



Gambar 14. Form Enkripsi

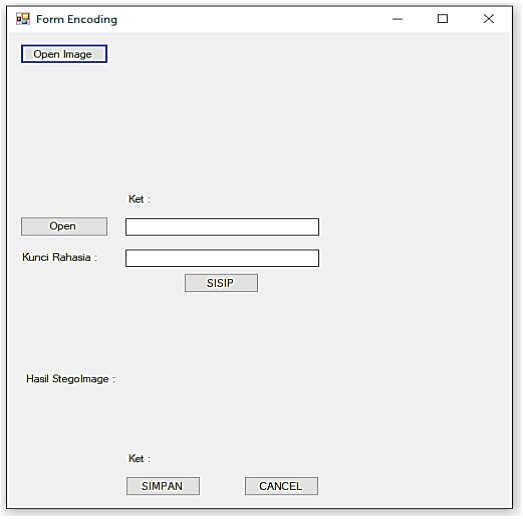
3. Form Dekripsi
   Form dekripsi merupakan form yang digunakan untuk melakukan proses dekripsi. Pada form ini disediakan interface diantaranya button untuk memilih file ciphertext yang akan didekripsi, textbox untuk menampilkan ciphertext yang akan didekripsi, textbox untuk memasukkan kunci rahasia yang sama pada saat melakukan enkripsi, button dekirpsi untuk mendekripsi ciphertext, dan textbox untuk menampilkan plaintext asli yang telah didekripsi. Tampilan untuk form dekripsi dapat dilihat pada gambar berikut.



Gambar 15. Form Dekripsi

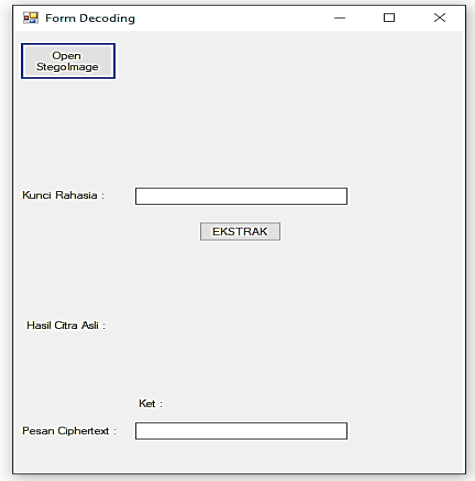
4. Form Encoding
   Form encoding merupakan form yang digunakan untuk melakukan proses encoding atau penyisipan. Pada form ini disediakan interface diantaranya adalah button open image untuk memilih objek gambar yang akan disisipkan, picturebox untuk menampilkan gambar yang telah dipilih, label untuk menampilkan keterangan pada gambar yang dipilih, button open ciphertext untuk memilih file ciphertext yang akan disisipkan ke dalam gambar, textbox untuk menampilkan ciphertext yang dipilih, textbox untuk memasukkan kunci, button untuk

melakukan proses penyisipan, picturebox untuk menampilkan hasil dari gambar yang telah disisipkan, label untuk menampilkan keterangan dari gambar yang telah disisipkan dan button untuk menyimpan file gambar. Tampilan untuk form encoding dapat dilihat pada gambar berikut.



Gambar 16. Form Encoding

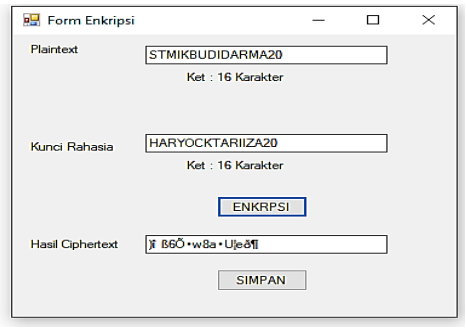
5. Form Decoding
   Form decoding merupakan form yang akan digunakan untuk melakukan proses decoding atau pengekstrakan. Pada form ini disediakan interface diantaranya adalah button untuk memilih file gambar yang telah disisipkan, picturebox untuk menampilkan file gambar yang telah dipilih, textbox untuk memasukkan kunci, button untuk melakukan proses pengekstrakan, picturebox untuk menampilkan hasil gambar asli, dan textbox untuk menampilkan ciphertext yang telah diekstrak. Tampilan form decoding dapat dilihat pada gambar berikut.



Gambar 17. Form Decoding

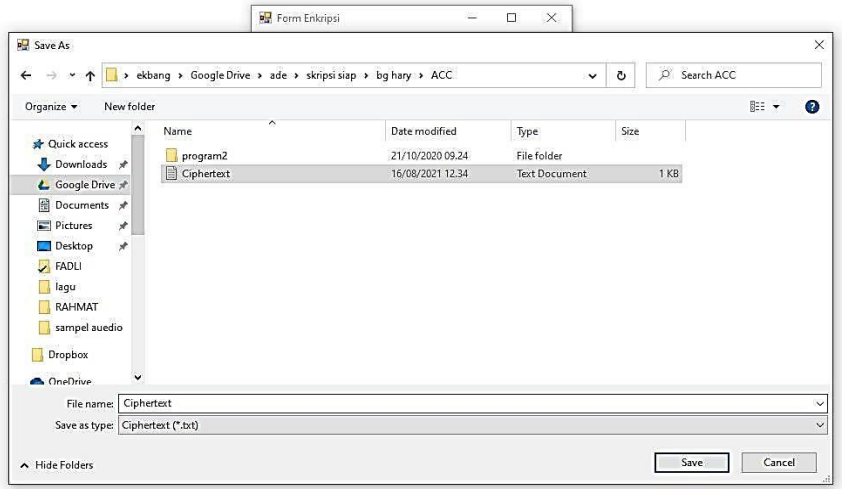
b. Tampilan Output
   Tampilan Output merupakan tampilan hasil dari proses enkripsi dan dekripsi serta hasil dari proses encoding dan decoding. Adapun proses tersebut dapat dilihat pada gambar di bawah ini :
   1. Tampilan Output Form Enkripsi
      Proses yang harus dilakukan ketika pengguna (user) melakukan enkripsi adalah dengan memasukkan plaintext dan kunci dengan panjang maksimal 128 bit, lalu memilih tombol enkripsi untukmelakukan pengenkripsian. Hasil dari proses output dapat dilihat pada gambar berikut.

Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 3, No 3, June 2024
Hal 221-233
https://ejurnal.seminar-id.com/index.php/bulletinds



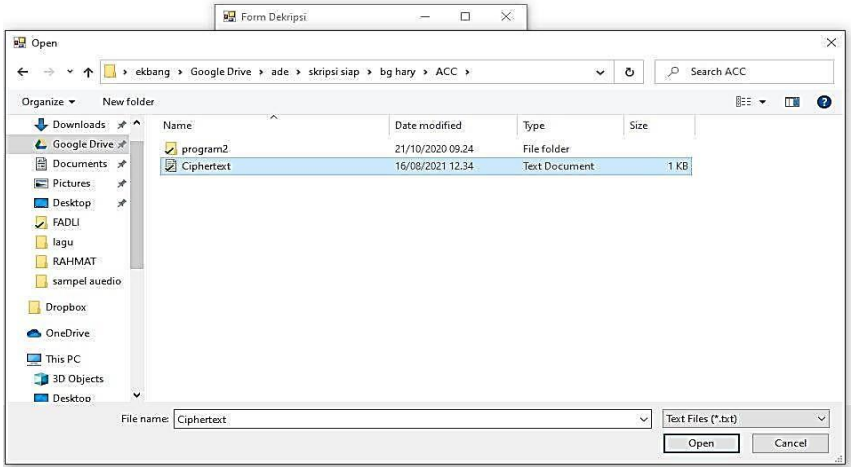
Gambar 18. Tampilan Output Form Enkripsi

Berdasarkan pada gambar 4.6, proses yang harus dilakukan ketika pengguna (user) ingin menyimpan hasil enkripsi adalah dengan memilih tombol simpan pada form menu enkripsi. Tampilan direktori komputer akan terbuka dan user yang dapat memilih tempat penyimpanan yang diinginkan, kemudian file tersebut akan disimpan dalam format *.txt. Tampilan dari proses penyimpanan file ciphertext dapat dilihat pada gambar berikut.



Gambar 19. Tampilan Penyimpanan File Ciphertext

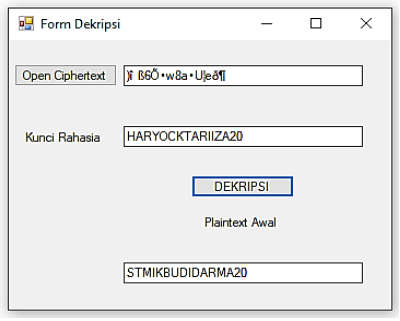
2. Tampilan Output Form Dekripsi
   Proses yang harus dilakukan ketika pengguna (user) melakukan dekripsi adalah dengan memilih tombol open ciphertext, hal ini dilakukan untuk memilih file ciphertext yang akan didekripsi. File yang telah dipilih maka akan ditampilkan pada textbox. Proses tersebut dapat dilihat pada gambar berikut.



Gambar 20. Tampilan Open Ciphertext

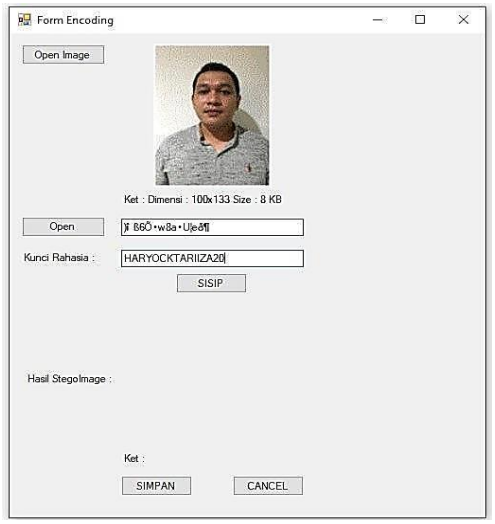
Berdasarkan gambar di atas untuk memulai proses dekirpsi dapat dilakukan dengan cara memasukkan kunci, kunci yang dimasukkan adalah kunci yang sama pada saat melakukan proses enkripsi. Kemudian pilih tombol dekripsi untuk melakukan proses pendekripsian. Tampilan tersebut dapat dilihat pada gambar berikut.

Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 3, No 3, June 2024
Hal 221-233
https://ejurnal.seminar-id.com/index.php/bulletinds



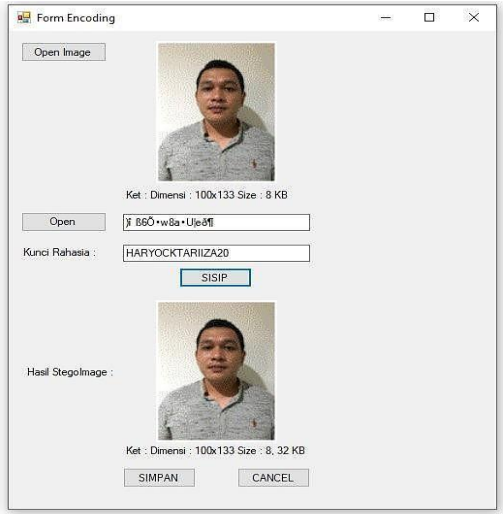
Gambar 21. Tampilan Output Form Dekripsi

3. Tampilan Output Form Encoding
   Proses yang harus dilakukan ketika pengguna (user) melakukan encoding atau penyisipan adalah dengan memilih tombol open image, lalu tampilan direktori akan terbuka untuk memilih gambar, picturebox akan menampilkan gambar yang telah dipilih, label akan menampilkan keterangan dimension dan size dari gambar yang dipilih. Kemudian pilih tombol open ciphertext, tampilan direktori akan terbuka untuk memilih file ciphertext yang akan disisipkan. Tampilan tersebut dapat dilihat pada gambar berikut.



Gambar 22. Tampilan Proses Penginputan Encoding

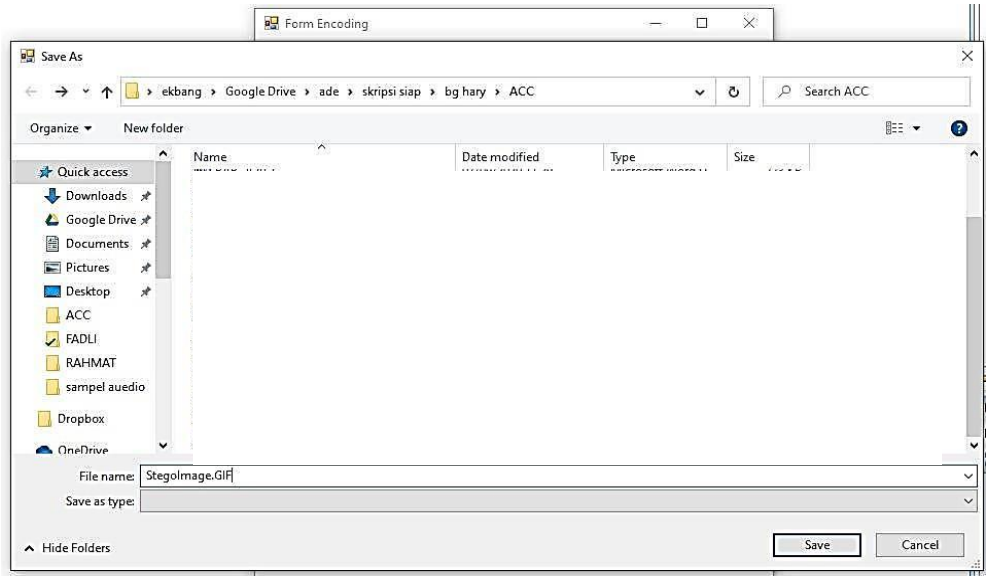
Berdasarkan gambar di atas untuk memulai proses penyisipan dapat dilakukan dengan memasukkan kunci, kemudian pilih tombol sisip. Hasil dari gambar yang telah disisipkan akan ditampilkan pada picturebox, dan label akan menampilkan keterangan pada gambar yang telah disisipkan. Tampilan tersebut dapat dilihat pada gambar berikut ini.



Gambar 23. Tampilan Output Encoding

Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 3, No 3, June 2024
Hal 221-233
https://ejurnal.seminar-id.com/index.php/bulletinds

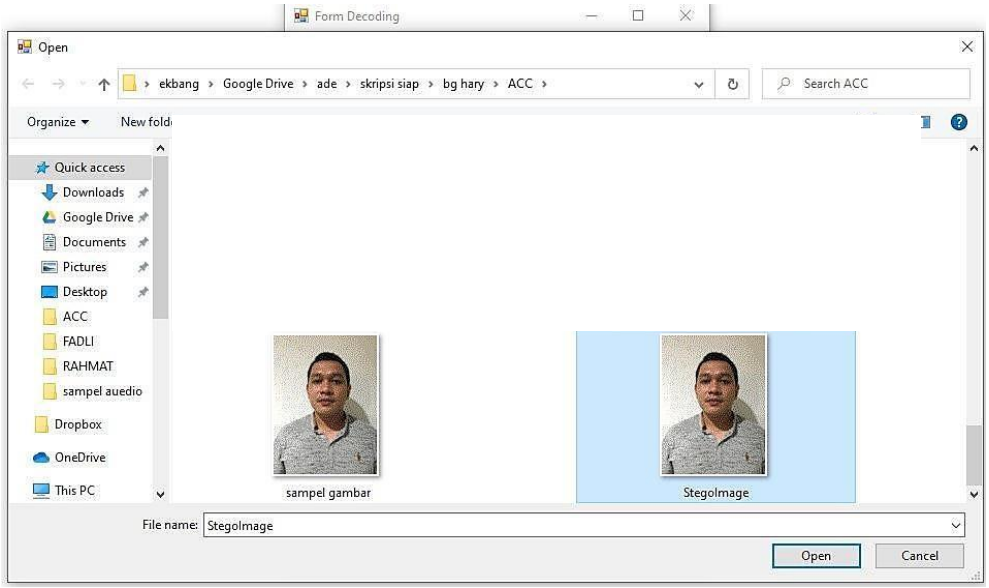
Berdasarkan pada gambar di atas, hasil dari penyisipan mengalami perubahan pada size gambar, namun tidak pada dimension gambar. Kemudian proses simpan dapat dilakukan ketika gambar sudah disisipkan dengan menekan tombol simpan. Tampilan direktori penyimpanan pada komputer akan tampil kemudian pengguna (user) dapat memilih tombol save. Tampilan tersebut dapat dilihat pada gambar di bawah ini.



Gambar 24. Tampilan Simpan StegoImage

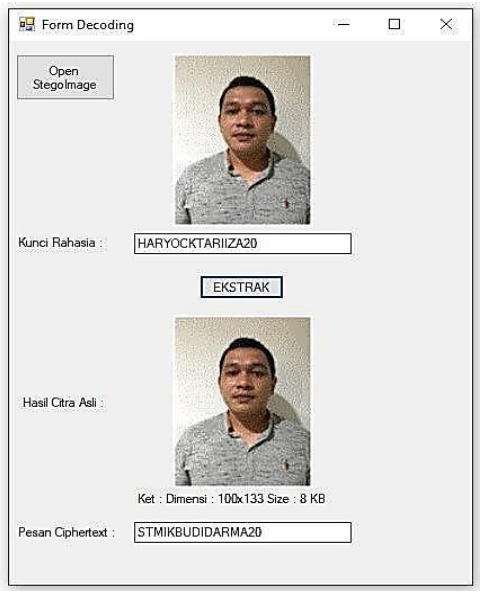
4. Tampilan Output Form Decoding

Proses decoding atau pengekstrakan adalah proses untuk mengekstrak file yang disisipkan pada gambar. Proses pengekstrakan dilakukan dengan cara memilih tombol open stegoimage untuk memilih gambar yang akan diekstrak. Tampilan direktori pada komputer akan terbuka dan user yang sidah memilih gambar dapat menekan tombol open. Kemudian masukkan kunci yang sama pada saat melakukan penyisipan. Tampilan pada proses tersebut dapat dilihat pada gambar berikut.



Gambar 25. Tampilan Proses Input StegoImage

Berdasarkan pada gambar di atas, proses yang harus dilakukan ketika pengguna (user) melakukan pengekstrakan adalah memilih tombol ekstrak pada form decoding. Picturebox akan menampilkan gambar asli hasil dari proses pengekstrakan dan pada textbox akan ditampilkan file ciphertext yang telah diekstrak. Tampilan tersebut dapat dilihat pada gambar berikut ini.



Gambar 26. Tampilan Output Form Decoding

8. KESIMPULAN

Dari hasil penelitian yang dilakukan terhadap peningkatan keamanan data teks terenkripsi algoritma AES yang disembunyikan ke dalam citra GIF menggunakan algoritma Gifshuffle, maka terdapat beberapa kesimpulan berdasarkan uraian yang telah tercantum pada bab-bab sebelumnya. Adapun kesimpulan dari hasil penelitian ini adalah Proses pengamanan citra digital dengan teknik kriptografi akan merubah nilai pixel citra digital tersebut sehingga citra digital akan sulit untuk dipahami. Data teks dengan format txt dapat diamankan dengan teknik kriptografi algoritma AES serta dapat disembunyikan ke dalam sebuah media berupa gambar berformat GIF dengan teknik steganografi. Sistem yang dirancang menggunakan Microsoft Visual Basic Net 2008 berdasarkan tahap-tahap proses enkripsi dan dekripsi algoritma AES serta tahap-tahap proses encoding dan decoding algoritma Giffshufle dapat mempermudah proses pengamanan dan penyembunyian data teks ke dalam citra GIF.

REFERENCES

[1] M. Winafil, S. Sinurat dan T. Zebua,” Implementasi Algoritma Advanced Encryption Standard Untuk MengamankanCitra Digital”, KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer), vol. 2, pp.450- 459, 2018
[2] D. Anggara dan A. S. Sembiring” Peningkatan Keamanan Data Teks Terenkripsi Algoritma Lucifer Menggunakan Steganografi Gifshuffle Pada Citra”, KOMIK (Konfersi Nasional Teknologi Informasi dan Komputer), Vol. 3, pp.439-445, 2019
[3] S. Kromodimoeljo, Teori dan Aplikasi Kriptografi, : SPK IT Consulting, 2009.
[4] A. Widarma, "Kombinasi Algoritma AES, RC4 dan Elmagal Dalam Skema Hybrid Untuk Keamanan Data", Journal of Computer Engineering System and Science, vol. 1, pp.1-8, 2016
[5] V. Yuniati, G. Indriyanta and A. Rachmat, "Enkripsi dan Dekripsi dengan Algoritma AES 256 Untuk Semua Jenis File", Informatika, vol. 5, pp.23-31, 2009
[6] Wikipedia, (2018,jan.12). Rijdael MixColumns [online]. Available: https://en.wikipedia.org/wiki/Rijndael_MixColumns
[7] D. Darwis, "Teknik Steganografi Untuk Penyembunyian Pesan Teks Menggunakan Algoritma Gifshuffle," Jurnal Teknoinfo, vol. 11, no. 1, pp. 1- 6, 2017.
[8] M. Khairani and S. Sembiring, "Analisis dan Implementasi Steganografi Pada Citra GIF Menggunakan Algoritma Gifshuffle," SNASTIKOM, pp. 9-14, 2013.
[9] S. Dharwiyanti and R. S. Wahono, "Pengantar Unified Modeling Language (UML)," IlmuKomputer.Com, 2003
[10] E. Shygan, "Daftar Simbol UML," 24 May 2013. [Online]. Available: https://id.scribd.com/document/143412967/Daftar-Simbol-Uml. [Accessed 08 May 2019].
[11] E. Sutanta, Pengantar Teknologi Informasi, Yogyakarta: Graha Ilmu. 2005.
[12] Hendrayudi, Dasar-Dasar Pemograman Microsoft Visual Basic 2008, Bandung: SatuNusa, 2011.