INFORMATICS AND DIGITAL EXPERT (INDEX) - VOL. 4 NO. 1 (2022) 1-9
Terbit *online* pada laman web jurnal : https://e-journal.unper.ac.id/index.php/informatics
| ISSN (Print) 2775-2208 | ISSN (Online) 2715-0453 |

Pengamanan Citra Medis Berbasis Steganografi dan Kriptografi Dengan Menggunakan Metode *End Of File* Dan *Advanced Encryption Standard*

Grace Christian M. Purba [1], Asep Id Hadiana [2] Irma Santikarama [3]

[1,2,3]*Jurusan Informatika, Fakultas Sains dan Informatika, Universitas Jendral Achmad Yani, Cimahi, Indonesia*
e-mail: gchrist230899@gmail.com[*1], asep.hadiana@lecture.unjani.ac.id [2], @gmail.com [3]

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Redaksi : 28 Januari 2022
Revisi Akhir : 13 Juni 2022
Diterbitkan *Online* : 01 Juli 2022

Kata Kunci :
Steganografi**,** Kriptografi**,** Keamanan Data**,** Kesehatan**,** Citra Medis

Korespondensi :
Telepon / Hp : +62 851 55433588
E-mail : **gchrist230899@gmail.com**

A B S T R A K

Perkembangan teknologi pada saat ini telah mengalami perubahan yang sangat pesat khususnya pada bidang keamanan data. Dalam bidang keamanan data terdapat teknik-teknik yang dapat digunakan untuk mengamankan suatu data, contoh teknik yang dapat digunakan ialah steganografi dan kriptografi. Steganografi merupakan suatu teknik penyembunyian data dengan menyembunyikan data ke dalam suatu *file* media, sedangkan kriptografi adalah teknik penyembunyian pesan dengan menggunakan teknik enkripsi. Steganografi memanfaatkan kelemahan indra manusia seperti mata dan telinga, sehingga steganografi ini bisa diterapkan dalam berbagai media digital. Citra medis yang bersifat elektronik merupakan kelengkapan dari catatan kesehatan pribadi pasien, sehingga data tersebut harus diamankan agar tidak terjadi penyalahgunaan oleh pihak yang tidak berkaitan. Untuk mengetahui seberapa aman hasil stego, dilakukan beberapa pengujian seperti MSE, PSNR, *Robustness*, dan *cyberattack*. Hasil dari pengujian MSE mendapatkan 1,656 dan PSNR 46,026 dB sehingga dapat dikatakan baik. Adapun hasil dari pengujian *robustness* dan *cyberattack* pesan yang disisipkan dan di enkripsi tidak dapat terungkap.

1. PENDAHULUAN

Citra medis merupakan salah satu citra digital pada bidang kesehatan yang sangat sensitif dan perlu untuk diamankan [1], supaya kerahasiaannya terjaga sesuai kode etik citra medis [2]. Citra medis perlu untuk diamankan agar datanya tidak dapat diakses oleh pihak yang tidak berkepentingan sehingga tidak terjadi manipulasi, pencurian data berharga atau informasi yang penting [2][3]. Pada tahun 2018 sebuah institusi kesehatan SingHealth Singapura mengalami kebocoran data pribadi, tercatat sekitar 1.5 juta data rekam medis warga singapura tersebar luas [4][5]. Mengamankan data citra medis perlu dilakukan agar data citra medis tidak disalah gunakan oleh pihak yang tidak berwenang seperti tertulis pada Undang-Undang Republik Indonesia Nomor 29 Tahun 2004 tentang Praktik Kedokteran yang menyatakan bahwa data rekam medis harus dijaga kerahasiaannya [6]. Selain itu juga sebagaimana diatur pada pasal 28G ayat (1) Undang-Undang Dasar Republik Indonesia Tahun 1945 (UUD RI 1945) yang menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi [7].

Dalam menjaga kerahasiaan data medis diperlukan teknik yang mampu mengamankan data. Di dalam *security sistem* terdapat dua teknik keamanan yaitu kriptografi, dan *information hiding*. Kriptografi adalah ilmu atau seni yang digunakan untuk menjaga keamanan pesan [8]. Dalam *information hiding* terdapat metode steganografi. Steganografi merupakan ilmu atau teknik menyembunyikan pesan/data kedalam sebuah wadah seperti citra, audio, video [9][10]. Atau dalam kata lain steganografi adalah teknik untuk menulis tulisan yang terselubung [9]. Steganografi pertama kali diperkenalkan oleh seorang sejarawan Yunani bernama Hiteus pada abad 5 sebelum masehi dengan menulis pesan rahasia berupa gambar pada kulit kepala seorang budak [11]. Seiring berjalannya waktu teknik steganografi semakin berkembang hingga saat ini.

Pentingnya mengamankan data citra medis adalah untuk menciptakan rasa aman pada masyarakat sebagaimana tercatat bahwa sekitar 70% orang khawatir jika informasi mengenai kesehatan mereka mengalami kebocoran [12]. Seperti berita yang sempat ramai akhir-akhir ini mengenai penjualan data penanganan kasus pandemi COVID 19 di Indonesia melalui forum online ‘Raid Forums’, data yang bocor merupakan data yang cukup lengkap seperti nama, umur, nomor telepon, alamat rumah, Nomor Identitas Kependudukan (NIK), hasil rapid test, hasil Polymerase Chain Reaction (PCR), hingga status terkait COVID-19 [13]. Pentingnya *cyber security* digunakan untuk menciptakan rasa aman pada pasien dan untuk mengurangi kasus penyalahgunaan data. Seperti sebelumnya diterapkan pada data rekam medis menggunakan teknik AES dan Vigenere Cipher, hasil eksperimen didapat adalah sistem kriptografi dengan

Super Enkripsi Vigenere Cipher dan AES-128-CBC memiliki keunggulan dari nilai korelasi dan entropi, namun masih memiliki waktu proses yang lebih lama dari pada menggunakan 1 algoritma [14].

Di dalam kriptografi terdapat tiga teknik yaitu *symmetric encryption*, *asymmetric encryption* dan *hash functions*. *Symmetric encryption* (SE) merupakan teknik yang cukup unggul karena waktu proses enkripsi dan dekripsi relatif cepat. Algoritma yang paling populer dalam teknik SE adalah Advanced Encryption Standard (AES). Meskipun teknik SE cukup populer SE memiliki kelemahan distribusi kunci tidak aman [8]**.** Maka dari itu untuk mengatasi kelemahan tersebut penulis menggunakan penggabungan dua teknik *security system* yaitu dengan teknik Kriptografi Advanced Encryption Standard (AES) 128 Bit Dan Steganografi Metode End Of File (EOF).

Penelitian ini bertujuan untuk menjaga dan mengamankan data citra medis sehingga menimbulkan rasa aman bagi pasien. Harapan dari penelitian ini yaitu untuk menjaga keamanan data medis pasien dengan cara menyisipkan sebuah data medis tersebut ke dalam sebuah citra dan enkripsi data yang sudah disisipkan, dengan bantuan sebuah sistem yang dapat melakukan penyisipan pesan tersebut sehingga dapat membantu meningkatkan keamanan data tersebut dari pihak yang tidak bertanggung jawab.

2. METODE PENELITIAN

2.1. Citra Medis

Citra medis adalah citra yang diciptakan dalam rangka mendiagnosis atau mendeteksi suatu penyakit. Citra medis banyak membantu para dokter dan dan para radiologi dalam mendiagnosa suatu penyakit. Jenis citra yang digunakan untuk mendiagnosa penyakit ini adalah jenis citra khusus yang dihasilkan dari peralatan medis seperti X-ray, USG (Ultrasonography), CT (Computed Tomography) Scanner, MRI (Magnetic Resonance Imaging) dan PET (Positron emission Tomography) [15].

Dalam penjelasan Undang-Undang Republik Indonesia No. 29 Tahun 2004 Tentang Praktik Kedokteran pada Pasal 47 ayat 2, yang menegaskan "Rekam medis sebagaimana dimaksud pada ayat (1) harus disimpan dan dijaga kerahasiaannya oleh dokter atau dokter gigi dan pimpinan sarana pelayanan kesehatan" [6]. Dan juga pada Peraturan Menteri Kesehatan Republik Indonesia No.269/ Menkes/Per/III/2008 tentang Rekam Medik/ Medical Records. Pasal 10 ayat 1, yang menegaskan "Informasi Tentang Identitas, Diagnosis, Riwayat Penyakit, Riwayat Pemeriksaan dan Riwayat Pengobatan Pasien Harus Dijaga Kerahasiaannya oleh Dokter, Dokter Gigi, Tenaga Kesehatan Tertentu, Petugas Pengelola dan Pimpinan Sarana Pelayanan Kesehatan" [16].

Karena citra medis memiliki sifat sensitif dari informasi yang disimpan dalam catatan kesehatan elektronik, beberapa perlindungan keamanan telah diperkenalkan melalui Health Insurance Portability and Accountability Act (HIPAA) dan Health Information Technology for Economic and Clinical Health (HITECH) [17].

2.2. Steganografi

Istilah steganografi berasal dari kata Yunani yaitu s*teganos* yang berarti tertutup dan *graphia* yang berarti menulis. Penggunaan steganografi ini bertujuan untuk menyamarkan sebuah keberadaan informasi penting sehingga sulit dideteksi dan melindungi sebuah data. Pada penelitian sebelumnya dijelaskan steganografi merupakan seni komunikasi rahasia dengan menyembunyikan atau menyisipkan pesan kedalam sebuah media atau object yang tampaknya tidak berbahaya [18]. Steganografi membutuhkan 2 file properti yaitu file penampung dan data penting [19]. Media penampung juga bisa berupa teks, gambar, audio, dan video, untuk pesan penting juga bisa berupa file dokumen, gambar, dan pesan lainnya.

2.3. End Of File

End Of File merupakan salah satu teknik yang menyisipkan pesan pada akhir file [20]. Metode ini pun adalah lanjutan dari metode LSB (*Least Significant Bit*). Pesan yang disisipkan dalam metode ini tidak memiliki batas akan tetapi memiliki efek samping yaitu mempengaruhi ukuran media penampung tersebut.

Adapun kriteria yang harus diperhatikan dalam penyisipan dan penyembunyian data adalah [10][21] :

1. *Impercebility*

   Keberadaan data tidak dapat diketahui dengan indera manusia. Jika pesan disisipi kedalam sebuah *image* atau media penampung maka seharusnya tidak dapat dibedakan dengan citra yang asli saat dilihat dengan mata.
2. *Fidelity*

   Media penampung seharusnya tidak jauh berubah agar tidak menimbulkan kecurigaan, sehingga pengamat tidak mengetahui bahwa di dalam media penampung atau *image* tersebut ada data informasi yang telah disisipkan.
3. *Robustness*

   Data yang sudah disisipkan harus bertahan terhadap berbagai operasi manipulasi yang dilakukan pada citra penampung.
4. *Recovery*

   Data yang berisi informasi yang telah disembunyikan harus dapat kembali seperti waktu memasukan informasi pertama kali.

2.4. Kriptografi

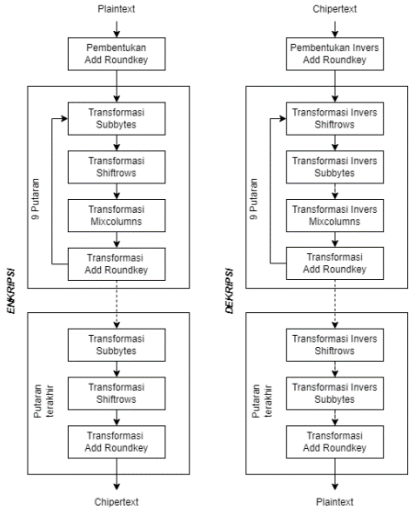
Kriptografi berasal dari Bahasa Yunani yang artinya kriptos dan grapho, yang mempunyai arti "tulisan tersembunyi" [22]. Pada penelitian sebelumnya

dijelaskan bahwa kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan data dan informasi seperti keabsahan data, integritas data, serta autentifikasi data[23].

Sehingga teknik kriptografi ini memiliki aspek yang sangat penting dalam menjaga kerahasian data yang diamankan, dikarenakan aspek autentikasi dan integritas data terpenuhi dengan metode ini. Aspek-aspek tersebut ini berguna bagi orang yang menginginkan keamanan bagi informasi atau data penting yang ingin diamankan.

2.5. Advanced Encryption Standard

Advanced Encryption Standard (AES) merupakan algoritma kriptografi yang dapat digunakan untuk mengamankan data. Algoritma AES ini menggunakan kunci simetris yang dimana kunci simetris ini menggunakan kunci yang sama pada proses enkripsi dan dekripsi. Berikut proses pada AES bisa dilihat pada gambar



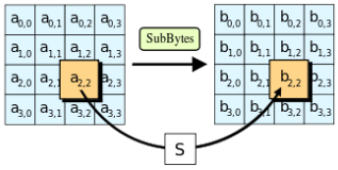
Gambar 1. Proses Algoritma AES

Block cipher AES dapat diimplementasikan dengan banyak ukuran bit (128, 192 dan 256 bit) masing-masing 128 bit dibagi menjadi empat blok operasi yang diterapkan pada matriks (4 * 4) dengan jumlah putaran berbeda menurut jumlah bit (10 putaran untuk 128 bit, 12 putaran untuk 192 bit dan 14 putaran untuk 256 bit) masing-masing terdiri dari empat transformasi dasar [24][25][26]:

1. Transformation Subbytes
   S-Box digunakan untuk operasi substitusi, byte ini akan diganti dengan yang lain dengan menggunakan tabel s-box [25].

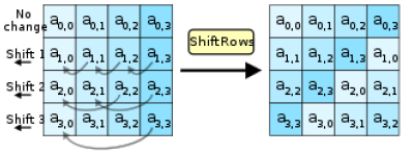
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	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 2. Tabel S-Box



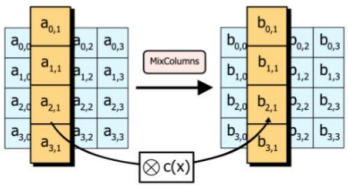
Gambar 3. Transformasi Subbytes

2. Transformasi Shiftrows
   Shiftrows adalah transposisi byte, dengan menerapkan operasi pergeseran untuk 3 baris terakhir [25].



Gambar 4. Transformasi Shiftrows

3. Transformasi Mixcolumn
   Kolom-kolom vektor selalu dikalikan dengan nilai matriks tetap, byte pada langkah ini diperlakukan sebagai persamaan polinomial [25].



Gambar 5. Transformasi Mixcolumn

Transformasi ini dinyatakan sebagai perkalian matriks:

$$s'(x) = a(x) \otimes s(x) \qquad (1)$$

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \qquad (2)$$

$$s'_{0,c} = (\{02\} \bullet s_{0,c}) \oplus (\{03\} \bullet s_{1,c}) \oplus s_{2,c} \oplus s_{2,c} \quad (3)$$

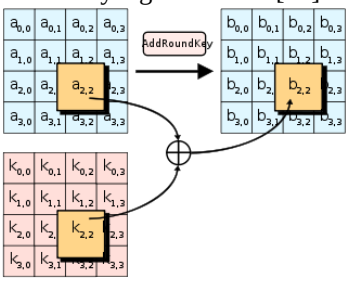
$$s'_{1,c} = s_{0,c} \oplus (\{02\} \bullet s_{1,c}) \oplus (\{03\} \bullet s_{2,c}) \oplus s_{3,c} \quad (4)$$

$$s'_{2,c} = s_{0,c} \oplus s_{1,c} \oplus (\{02\} \bullet s_{2,c}) \oplus (\{03\} \bullet s_{3,c}) \quad (5)$$

$$s'_{3,c} = (\{03\} \bullet s_{0,c}) \oplus s_{1,c} \oplus s_{2,c} \oplus (\{02\} \bullet s_{3,c}) \quad (6)$$

4. Transformasi Add Round Key

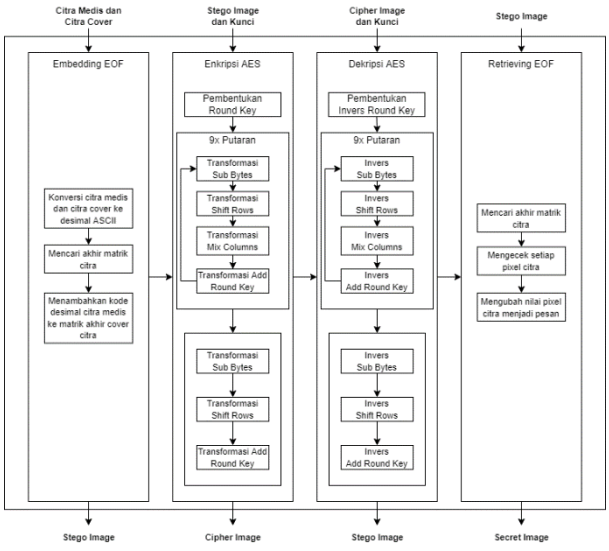
   Add round key adalah operasi XOR antara kunci dan status yang dihasilkan [25].



Gambar 6. Transformasi Add Roundkey

3. PERANCANGAN SISTEM

Perancangan sistem ini membahas bagian isi dari tahapan yang dilakukan. Gambaran perancangan sistem bisa dilihat pada gambar dibawah ini :



Gambar 7. Perancangan Sistem Pengamanan Citra Medis

3.1. Perolehan Data

Perolehan data dilakukan melalui observasi pada situs Kaggle yang berisi banyak data set. Data yang digunakan berupa data citra medis dengan berbagai hasil laboratorium seperti CT-Scan, MRI, USG, X-Ray dan Mammography. Pengambilan data dilakukan dengan melakukan pencarian terhadap berbagai jenis citra medis tersebut pada situs Kaggle.

3.2. End Of File (EOF)

Data masukan pada proses ini menggunakan citra cover dan citra medis sebagai pesan. Dimana citra cover dan citra medis sebagai pesan akan dikonversi kedalam bentuk desimal ASCII. Setelah dilakukan konversi kedalam desimal ASCII, nilai desimal ASCII dari pesan akan disisipkan ke baris akhir dari matrik citra cover. Misalnya pada sebuah citra cover dengan ukuran 5x6 pixel disisipkan pesan berupa citra medis :

Kode ASCII dari citra medis (CT-Scan) adalah :

0	1	2	3	4	5
6	7	8	9	10	11
12	13	14	15	16	17
18	19	20	21	22	23
24	25	26	27	28	29

Misalkan matriks dari citra cover sebagai berikut :

0	1	2	3	4	5
6	7	8	9	10	11
6	12	13	14	15	0
16	6	17	18	6	16
1	19	20	21	1	0

Baris akhir matriks yang kosong pada matriks citra cover akan disisipi nilai desimal ASCII yang dimiliki citra medis (pesan) tersebut. Sehingga matriks yang telah disisipi akan menjadi seperti :

0	1	2	3	4	5
6	7	8	9	10	11
6	12	13	14	15	0
16	6	17	18	6	16
1	19	20	21	1	0
0	1	2	3	4	5
6	7	8	9	10	11
12	13	14	15	16	17
18	19	20	21	22	23
24	25	26	27	28	29

Hasil diatas merupakan matriks dari citra stego, dimana telah dilakakukannya proses penyisipan pesan berupa citra medis ke dalam citram cover sebagai media penampung.

3.3. Advanced Encryption Standard (AES)

Berikut merupakan beberapa tahapan dalam metode AES.

Pembentukan Roundkey

Contoh data yang akan diamankan yakni sebuah plaintext pada tabel ASCII yang diubah ke dalam hexadesimal. Berikut merupakan contoh rangkaian karakter ASCII yang diasumsikan untuk diamankan.

Contoh plaintext yang akan diamankan :

32	88	31	E0
43	5A	31	37
F6	30	98	07
A8	8D	A2	34

Contoh plainkey yang akan diamankan :

2B	28	AB	09
7E	AE	F7	CF
15	D2	15	4F
16	A6	88	3C

Cipherkey dalam hexadesimal : 2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C . Lalu dilakukan proses pembagian setiap nilai hexa ke dalam masing masing word atau w[i] yang masing masing word berisi 4 byte data seperti *w*[0] = (2B,7E,15,16), *w*[1] = (28,AE,D2,A6), *w*[2] = (AB,F7,15,88), *w*[3] = (09,CF,4F,3C).
Setelah itu dilakukan pergeseran terhadap *w*[3] satu *byte* ke kiri secara sirkuler : *w*[3] = (CF,4F,3C,09). Lalu lakukan proses substitusi hasil pergeseran tersebut dengan *S-box*: (8A,84,EB,01). Lalu XOR kan hasil substitusi hasil pergeseran dengan *S-box* tersebut dengan tabel *Rcon*[1] = (01,00,00,00), menghasilkan (8B,84,EB,01).

Lalu dilanjutkan dengan mencari w[4] hingga w[n] dengan melakukan operasi XOR dan mengkonversi hasil operasinya ke dalam hexadesimal.
Mencari *w*[4], *w*[5], *w*[6], *w*[7] sebagai berikut :

1. *w*[4] = *w*[0] ⊕ (*w*[3])
   w[4] = (2B,7E,15,16) ⊕ (8B,84,EB,01) = (A0,FA,FE,17)
2. *w*[5] = *w*[4] ⊕ *w*[1] = (88,54,2C,B1)
3. *w*[6] = *w*[5] ⊕ *w*[2] = (23,A3,39,39)
4. *w*[7] = *w*[6] ⊕ *w*[3] = (2A,6C,76,05)

Jadi hasil dari proses pembentukan roundkey :
Roundkey 1 : A0 FA FE 17 88 54 2C B1 23 A3 39 39 2A 6C 76 05
Proses pembentukan roundkey ini dilakukan sebanyak sepuluh kali putaran.

Roundkey 0 : 2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C
Roundkey 1 : A0 FA FE 17 88 54 2C B1 23 A3 39 39 2A 6C 76 05
Roundkey 2 : F2 C2 95 F2 7A 96 B9 43 23 A3 39 39 73 59 F6 7F
….
Roundkey 10 : D0 14 F9 A8 C9 EE 25 89 E1 3F 0C C8 B6 63 0C A6

Proses Enkripsi

Proses enkripsi dilakukan dengan mengubah setiap karakter *plaintext* yang akan dienkripsi menjadi sebuah *state* yang bernilai hexadecimal. Berikut merupakan tahapan dalam enkripsi pada algoritma AES.

1) Transformasi Subbytes

Transformasi *SubBytes* memetakan setiap byte dari array *state* dengan menggunakan tabel substitusi *S-box.* Cara pensubstitusiannya adalah sebagai berikut : untuk setiap byte pada *array state*, misalkan *S*[r,c] = *xy*, yang dimana hal ini *xy* adalah digit heksadesimal dari nilai *S*[r,c], maka nilai substitusinya, dinyatakan dengan *S'*[r,c], adalah elemen di dalam *S-box* yang merupakan perpotongan baris *x* dengan kolom *y*.

$$\begin{bmatrix} 19 & A0 & 9A & E9 \\ 3D & F4 & C6 & F8 \\ E3 & E2 & 8D & 48 \\ BE & 2B & 2A & 08 \end{bmatrix} = \begin{bmatrix} D4 & E0 & B8 & 1E \\ 27 & BF & B4 & 41 \\ 11 & 98 & 5D & 52 \\ AE & F1 & E5 & 30 \end{bmatrix}$$

2) Transformasi Shiftrows

Transformasi *ShiftRows* melakukan pergeseran secara *wrapping* (siklik) pada 3 baris terakhir dari array state. Jumlah pergeseran bergantung pada nilai baris (r). Baris *r* = 0 tidak digeser, baris *r* = 1 digeser sejauh 1 *byte*, baris *r* = 2 digeser sejauh 2 *byte*, baris *r* = 3 digeser sejauh 3 *byte.*

$$\begin{bmatrix} D4 & E0 & B8 & 1E \\ BF & B4 & 41 & 27 \\ 5D & 52 & 11 & 98 \\ 30 & AE & F1 & E5 \end{bmatrix}$$

3) Transformasi Mixcolumns

Transformasi *MixColumns* mengalikan matriks *state* dengan sebuah matriks tertentu.

$$\begin{bmatrix} D4 & E0 & B8 & 1E \\ BF & B4 & 41 & 27 \\ 5D & 52 & 11 & 98 \\ 30 & AE & F1 & E5 \end{bmatrix} \bullet \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} = \begin{bmatrix} 04 & E0 & 48 & 28 \\ 66 & CB & F8 & 06 \\ 81 & 19 & D3 & 26 \\ E5 & 9A & 7A & 4C \end{bmatrix}$$

Contoh proses perhitungan untuk mencari isi matriks 04 dengan cara melakukan operasi baris dikalikan dengan kolom lalu dilakukan operasi XOR.

({02} • D4) ⊕ ({03} • BF) ⊕ ({01} • 5D) ⊕ ({01} • 30)

a. (02 • D4) = (02 • 1101 0100) => 1010 1000 ⊕ 0001 1011 = 1011 0011
b. (03 • BF) = (02 • BF) ⊕ (01 • BF) => 0110 0101 ⊕ 1011 1111= 1101 1010
c. (01 • 5D) = 5D => 0101 1101
d. (01 • 30) = 30 => 0011 0000

Maka hasil dari ({02} • D4) ⊕ ({03} • BF) ⊕ ({01} • 5D) ⊕ ({01} • 30)
= 1011 0011 ⊕ 1101 1010 ⊕ 0101 1101 ⊕ 0011 0000 => 0000 0100 = 04
Sehingga didapatkan hasil dari transformasi mixcolumns : 04 66 81 E5 E0 CB 19 9A 48F8 D3 7A 28 06 26 4C.

4) Transformasi Add Roundkey

Transformasi add roundkey adalah melakukan operasi XOR terhadap sebuah roundkey dengan array state dan hasilnya disimpan di *array state* yang baru.

$$\begin{bmatrix} 04 & E0 & 48 & 28 \\ 66 & CB & F8 & 06 \\ 81 & 19 & D3 & 26 \\ E5 & 9A & 7A & 4C \end{bmatrix} \oplus \begin{bmatrix} A0 & 88 & 23 & 2A \\ FA & 54 & A3 & 6C \\ FE & 2C & 39 & 76 \\ 17 & B1 & 39 & 05 \end{bmatrix} = \begin{bmatrix} A4 & 68 & 6B & 02 \\ 9C & 9F & 5B & 6A \\ 7F & 35 & EA & 50 \\ F2 & 2B & 43 & 49 \end{bmatrix}$$

Sehingga didapatkan hasil round 1 : A4 9C 7F F2 68 9F 35 2B 6B 5B EA 43 02 6A 50 49. Proses dilakukan hingga putaran kesepuluh dengan cara yang sama, pada putaran kesepuluh hanya melakukan transformasi subbytes, transformasi shiftrows dan transformasi add roundkey. Sehingga chipertext yang dihasilkan yakni 39 25 84 1D 02 DC 09 FB DC 11 85 97 19 6A 0B 32.

Proses Dekripsi

Proses dekripsi algoritma AES dilakukan dengan melakukan invers pada proses yang sudah dilakukan pada proses enkripsi. Seperti tahapan pembentukan invers roundkey, invers subbytes, invers shiftrows, invers mix columns.

1) **Invers SubBytes**

Invers subbytes merupakan transformasi yang berkebalikan dengan transformasi subbytes. Pada proses ini setiap elemen pada state dipetakan dengan menggunakan tabel invers S-Box

2) **Invers Shiftrows**

Invers shiftrows merupakan transformasi yang berkebalikan dengan transformasi shiftrows. Pada transformasi ini dilakukan pergeseran bit ke kanan berkebalikan dengan transformasi shiftrows yang melakukan pergeseran bit ke kiri 2).

3) **Invers Mixcolumns**

Pada transformasi ini setiap kolom state dikalikan dengan matriks, blok ciphertext disimpan di dalam matriks yang bernama state berukuran 4x4.

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$$

Transformasi invers mixcolumns mengalikan setiap kolom dari larik state seperti pada tabel matriks diatas. Proses invers mixcolumns serupa dengan transformasi mixcolumns, namun dengan perbedaan konstanta matriks yang digunakan sebagai pengali dengan state.

4. HASIL DAN PEMBAHASAN

4.1. Pengujian Steganografi End Of File (EOF)

Pengujian ini melakukan dua skenario yang dimana skenario pertama melakukan pengujian tanpa serangan dan yang kedua pengujian melakukan serangan. Untuk skenario pertama melakukan pengujian kualitas citra pada masing-masing citra setelah dilakukannya penyisipan (*fidelity*). Dan untuk skenario kedua pengujian melakukan pengujian serangan yang dimana citra stego akan dilakukan perputaran dan pemotongan (*robustness*).

Pengujian pertama ini dilakukan untuk melihat kualitas dari media penampung atau citra cover yang tidak mengalami banyak perubahan akibat penyisipan. Pada pengujian *fidelity* ini akan dilakukan pengujian sebagai berikut :

1. Pengujian pertama akan dilakukan dengan menggunakan 5 citra cover dengan ukuran yang berbeda antara 55 – 325 kb dengan pesan berupa citra medis yang disisipkan dengan ukuran yang berbeda antara 55 – 415 kb.
2. Pengujian kedua akan dilakukan perhitungan MSE dan PSNR untuk melihat hasil kualitas citra cover sesudah dan sebelum disisipkan citra medis sebagai pesan.

Tabel 1. Hasil Pengujian Fidelity 1

Citra Cover	Ukuran Citra (kb, bytes)	Citra Medis (Pesan)	Ukuran Pesan (kb, bytes)	Ukuran Stego (kb, bytes)
	176, 0 kb 180,102 bytes		414 kb 424,263 bytes	590 kb 604,377 bytes
	324,0 kb 332,781 bytes		101 kb 103,713 bytes	426 kb 436,506 bytes
	55,8 kb 57,146 bytes		227 kb 232,684 bytes	283 kb 289,842 bytes
	247, 0 kb 253,383 bytes		249 kb 255,762 bytes	497 kb 509,157 bytes
	93,2 kb 95,454 bytes		54, 2 kb 55,573 bytes	147 kb 151,039 bytes

Pada tabel diatas pengujian terhadap 5 citra yang berbeda dengan pesan berupa citra medis. Sehingga memperoleh hasil yang dapat disimpulkan bahwa pesan yang disisipkan hanya menambah ukuran dari citra cover tersebut tanpa merubah intensitas warna dari pesan yang disisipkan.

Pengujian MSE dan PSNR digunakan untuk mengukur kualitas citra yang dihasilkan. MSE adalah nilai error kuadrat rata-rata antara cinta asli dengan citra yang telah disisipi pesan. Sedangkan PSNR adalah perbandingan nilai piksel citra cover dengan citra stego yang dihasilkan.

Berikut rumus untuk menghitung *Mean Square Error* (MSE).

$$MSE_{AVG} = \frac{MSE_R + MSE_G + MSE_B}{X.Y} \quad (7)$$

Keterangan :
MSE = Nilai Mean Square Error dari citra
XY = Merupakan dimensi dari citra

Berikut ini adalah rumus yang digunakan untuk menghitung PSNR.

$$PSNR = 20 \log 10 \left(\frac{255}{\sqrt{MSE}}\right) \quad (8)$$

Keterangan: :
PSNR = Nilai PSNR citra (dalam dB)
MSE = Nilai MSE

Tabel 2. Hasil Pengujian MSE Dan PSNR

Citra Cover	Citra Medis (Pesan)	Ukuran Citra (kb, bytes)	Ukuran Stego (kb, bytes)	MSE	PSNR
		176, 0 kb 180,102 bytes	590 kb 604,377 bytes	1,60	46,11
		324,0 kb 332,781 bytes	426 kb 436,506 bytes	1,55	46,27
		55,8 kb 57,146 bytes	283 kb 289,842 bytes	1,77	45,85
		247, 0 kb 253,383 bytes	497 kb 509,157 bytes	1,57	46,29
		93,2 kb 95,454 bytes	147 kb 151,039 bytes	1,79	45,61

Setelah dilakukan perhitungan MSE dan PSNR. Hasil yang didapat dari kedua pengujian tersebut mendapatkan hasil yang baik, yang dimana MSE mendapatkan nilai rata-rata 1,656 dan PSNR 46,026 dB. Semakin rendah nilai MSE menandakan semakin baik kualitas penyisipan, semakin tinggi nilai PSNR menandakan semakin baik kualitas citra.

Pengujian kedua ini dilakukan untuk melihat citra stego dapat diungkap kembali menjadi pesan rahasia yang akan disampaikan, citra stego tersebut akan dilakukan perputaran dan pemotongan.

Tabel 3. Hasil Pengujian Robustness

Citra Stego	Ukuran Citra Stego (kb, bytes)	Ukuran Citra Putar (kb, bytes)	Ukuran Citra Potong (kb, bytes)	*Recovery*
	590 kb 604,377 bytes	351 kb 359,493 bytes	-	Gagal
	426 kb 436,506 bytes	291 kb 297,212 bytes	-	Gagal
	283 kb 289,842 bytes	134 kb 136,542 bytes	-	Gagal
	497 kb 509,157 bytes	236 kb 241,996 bytes	-	Gagal
	147 kb 151,039 bytes	115 kb 117,234 bytes	-	Gagal
	590 kb 604,377 bytes	-	136 kb 140,178 bytes	Gagal
	426 kb 436,506 bytes	-	121 kb 124,441 bytes	Gagal
	283 kb 289,842 bytes	-	43,5 kb 44,597 bytes	Gagal
	497 kb 509,157 bytes	-	131 kb 134,230 bytes	Gagal
	147 kb 151,039 bytes	-	51,5 kb 52,760 bytes	Gagal

Setelah melakukan serangan dengan melakukan perputaran dan pemotongan terhadap citra stego, mendapatkan hasil yang baik, citra stego tidak dapat di ungkapkan kembali.

4.2 Pengujian Kriptografi Advanced Encryption Standard (AES)

Penetrasi testing adalah sebuah metode yang dilakukan untuk mengevaluasi keamanan dari sebuah sistem dan jaringan komputer. Pengujian ini dilakukan untuk menguji seberapa amankah kunci yang digunakan pada proses enkripsi gambar yang terenkripsi oleh metode AES.

Untuk pengujian kunci AES, penulis membuat kunci mulai dari angka, huruf, simbol dan mengkombinasi angka, huruf dan simbol. Pengujian ini berfungsi untuk mengetahui seberapa amankah kunci dari serangan brute force.

Tabel 4. Hasil Pengujian Kunci AES

No	Nama File	Kunci	Hasil Penetrasi Kunci
1	Gambar 1	1234423520123456	2 hari
2	Gambar 2	abcdefghijklmnop	34.00 tahun

3	Gambar 3	Abcd,./123ef45;’	2.000.000.000.000 tahun
4	Gambar 4	Abcdefgh12345678	37.000.000.000 tahun
5	Gambar 5	12345678!@#$%^&*	18.000 tahun

Dari hasil diatas bisa kita lihat bahwa dengan menggunakan metode AES cukup aman karena menggunakan kunci 128bit dengan panjang 16 karakter, hasil dari kunci diatas bisa kita lihat paling cepat memerlukan waktu 2 hari dan paling lama 2 triliun tahun untuk membukanya. Jadi kesimpulannya dengan menggunakan kombinasi dari huruf, angka dan simbol akan menghasilkan kunci yang akan sulit dibuka.

Pengujian penetrasi file merupakan tahap uji kedua yang akan dilakukan untuk mengetahui apakah file yang sudah dienkripsi dengan menggunakan metode AES bisa di dekripsi dengan menggunakan aplikasi pihak ketiga. Pengujian ini akan dilakukan dengan menggunakan *cyber attack*. Yang dimana *cyber attack* ini merupakan serangan untuk mendapatkan akses tidak sah ke komputer, sistem komputasi, atau jaringan computer dengan tujuan untuk memanipulasi atau mencuri data yang tersimpan dalam sistem.

Pada pengujian ini salah satu aplikasi *cyber attack* yang digunakan ialah *openssl* dimana aplikasi ini digunakan untuk mendekripsi file yang telah terenkripsi. Dimana openssl merupakan tools untuk melakukan enkripsi dan dekripsi yang disediakan untuk keperluan keamanan sistem dan *openssl* ini memiliki banyak algoritma kriptografi untuk mengamankan data.

```
D:\Tes>openssl enc -AES-128-cbc -d -a -salt -in Encrypt.jpg -out hasil.jpg
enter AES-128-CBC decryption password:
error reading input file
```

Gambar 8. Hasil Pengujian Penetrasi File

Bisa kita lihat gambar diatas dimana hasilnya adalah “error reading input file“, yang dimana gambar tersebut tidak dapat terbaca dengan aplikasi pihak ketiga. Ini membuktikan bahwa gambar yang terenkripsi dengan menggunakan metode AES cukup baik dan tidak mudah untuk ditembus.

5. KESIMPULAN

Penelitian ini telah menghasilkan sebuah sistem pengamanan citra medis dengan menerapkan teknik steganografi dan kriptografi yang menggunakan metode End Of File (EOF) dan Advanced Encryption Standard (AES). Berdasarkan hasil pengujian *fidelity* dan *robustness* pada file citra medis yang disisipkan kedalam citra cover menggunakan EOF hasil dari pengujian *fidelity* ini memperoleh nilai rata-rata MSE 1,656 yang dimana pengujian ini mendapatkan hasil yang baik dikarenakan semakin rendah nilai MSE semakin baik penyisipan yang dilakukan. Sedangkan pengujian PSNR memperoleh nilai rata-rata 46,026 dB yang dimana pengujian ini mendapatkan hasil yang baik dikarenakan semakin tinggi nilai PSNR semakin baik kualitas citra tersebut. Untuk pengujian *robustness* pada citra stego jika diputar dan dilakukan pemotongan mendapatkan hasil yang baik, dikarenakan tidak dapat terungkapnya pesan yang disisipkan. Untuk pengujian pada file yang terenkripsi dengan menggunakan metode *cyber attack* mendapatkan hasil yang baik dikarenakan file yang sudah terenkripsi tidak dapat dipulihkan kembali.

DAFTAR PUSTAKA

[1] H. Sajedi and S. Rahbar Yaghobi, “Information hiding methods for E-Healthcare,” *Smart Heal.*, vol. 15, no. January 2017, p. 100104, 2020, doi: 10.1016/j.smhl.2019.100104.

[2] D. C. Lou, M. C. Hu, and J. L. Liu, “Multiple layer data hiding scheme for medical images,” *Comput. Stand. Interfaces*, 2009, doi: 10.1016/j.csi.2008.05.009.

[3] B. Santoso, “Color-based microscopic image steganography for telemedicine applications using pixel value differencing algorithm,” *J. Phys. Conf. Ser.*, vol. 1175, no. 1, pp. 1–7, 2019, doi: 10.1088/1742-6596/1175/1/012057.

[4] P. M. Herlambang *et al.*, “Model Perilaku Keamanan Siber Pada Pengguna Sistem Informasi Kesehatan Pada Masa Pandemi Covid-19 Cyber Security Behavior Model on Health Information System Users During Covid-19 Pandemic,” *Cyber Secur. dan Forensik Digit.*, vol. 3, no. 2, pp. 28–33, 2020.

[5] D. P. BSSN, “2020 Buku Putih Keamanan Siber Sektor Kesehatan,” pp. 33–42, 2020.

[6] 29 UU RI Nomor, “UU No. 29 Tahun 2004 Tentang Praktik Kedokteran,” *Aturan Prakt. Kedokt.*, pp. 157–180, 2004.

[7] “PERUBAHAN KEDUA UNDANG-UNDANG DASAR NEGARA REPUBLIK INDONESIA TAHUN 1945,” vol. 105, no. 3, pp. 129–133, 1945, [Online]. Available: https://webcache.googleusercontent.com/search?q=cache:BDsuQOHoCi4J:https://media.neliti.com/media/publications/9138-ID-perlindungan-hukum-terhadap-anak-dari-konten-berbahaya-dalam-media-cetak-dan-ele.pdf+&cd=3&hl=id&ct=clnk&gl=id.

[8] Basri, “Kriptografi Simetris Dan Asimetris Dalam Perspektif Keamanan Data Dan Kompleksitas Komputasi,” *J. Ilm. Ilmu Komput.*, vol. 2, no. 2, pp. 17–23, 2016, [Online]. Available: http://ejournal.fikom-unasman.ac.id.

[9] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Digital image steganography: Survey and analysis of current methods,” *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010, doi: 10.1016/j.sigpro.2009.08.010.

[10] Edisuryana Mukharrom, Isnanto R Riza, and Somantri Maman, “Aplikasi Steganografi Pada Citra Berformat Bitmap Dengan Menggunakan Metode End of File,” *Transien*, 2013.

[11] Irfan, "Penyembunyian Informasi (steganography) Gambar Menggunakan Metode LSB (Least Significant Bit)," *Rekayasa Teknol.*, 2013.

[12] A. M. Ningtyas and I. K. Lubis, "LITERATUR REVIEW PERMASALAHAN PRIVASI PADA REKAM MEDIS ELEKTRONIK," *J. Pseudocode*, vol. 5, no. September, pp. 12–17, 2018.

[13] K. Hendriyanto, "Juridical Analysis of Illegal Information Access: Case Study on Sales of Data Patients Covid-19," *Soepra*, vol. 7, no. 1, p. 27, 2021, doi: 10.24167/shk.v7i1.2689.

[14] F. Nuraeni, Y. Purnama Putra, I. Hendriyani, P. Studi Teknik Informatika, and S. Tasikmalaya, "Implementasi Kriptografi Superenkripsi Vigenere Cipher Dan Advanced Encrytion Standard (Aes) Pada Pengamanan Data Riwayat Pasien Rumah Sakit," *Ejurnal.Dipanegara.Ac.Id*, 2019, [Online]. Available: https://ejurnal.dipanegara.ac.id/index.php/sensitif/article/view/560.

[15] B. Sugandi, "Teknologi Citra untuk Peningkatan Kualitas Hidup yang Lebih Baik," *J. Integr.*, vol. 10, no. 1, pp. 21–27, 2018.

[16] MenKes, "Kesehatan Ri," no. 269, 2008.

[17] C. S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand, "Security Techniques for the Electronic Health Records," *J. Med. Syst.*, vol. 41, no. 8, 2017, doi: 10.1007/s10916-017-0778-4.

[18] J. V. Purba, M. Situmorang, and D. Arisandi, "Implementasi Steganografi Pesan Text Ke Dalam File Sound (.Wav) dengan Modifikasi Jarak Byte Pada Algoritma Least Significant Bit (LSB)," *J. Dunia Teknoogi Inf.*, 2012.

[19] M. Iksal, "PENGAMANAN DATA RIWAYAT PENYAKIT PADA PASIEN MENGGUNAKAN STEGANOGRAFI MOST SIGNIFICANT BIT (MSB)," vol. 21, no. 1, pp. 1–9, 2020.

[20] Sembiring Sandro, "Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan Teks Pada Gambar Dengan Metode End of File," *Pelita Inform. Budi Darma*, 2013.

[21] R. Munir, "Citra Biner," *Pengolah. Citra Digit. Dengan Pendekatan Algoritm.*, 2005.

[22] L. Benny, "Analisis Dan Perancangan Aplikasi Kriptografi Keamanan File Berbasis Teks Dengan Menggunakan Metode Rsa," *Ris. dan E-Jurnal Manaj. Inform. Komput.*, vol. 1, no. April P-ISSN : 2541-1322, pp. 15–23, 2017, [Online]. Available: http://jurnal.polgan.ac.id/index.php/remik/article/view/10116.

[23] A. R. Tulloh, Y. Permanasari, and E. Harahap, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen," *J. Mat. UNISBA*, 2016.

[24] N. Fips, "197: Announcing the advanced encryption standard (AES)," *... Technol. Lab. Natl. Inst. Stand. ...*, 2001, doi: 10.1016/S1353-4858(10)70006-4.

[25] M. Azure, "Medical Image Encryption using DNA-Planes," vol. 1, no. 1, 2020, doi: 10.21275/ART20176928.

[26] J. J. Amador and R. W. Green, "Symmetric-key block cipher for image and text cryptography," *Int. J. Imaging Syst. Technol.*, 2005, doi: 10.1002/ima.20050.