Universitas Maritim Raja Ali Haji
SOJ
Student Online Journal

TEKNIK PENYEMBUNYIAN DATA MENGGUNAKAN METODE KOMPRESI LEMPEL ZIV WELCH (LZW), END OF FILE (EOF) DAN ADVANCED ENCRYPTION STANDARD (AES) KEDALAM MEDIA GAMBAR FORMAT BMP

Chandra Zulfika, Muhamad Radzi Rathomi, Nurul Hayaty
150155201020@student.umrah.ac.id
Program Studi Teknik Informatika, Fakultas Teknik, Universitas Maritim Raja Ali Haji

Abstract

The more sophisticated the technology, people can send or exchange messages to convey or send important information easily. Messages that are confidential or not will be sent to the recipient of the message, but messages made using the TXT can be replaced and damaged by irresponsible parties. There is a lot of knowledge in securing files that are used at this time including compression, cryptography, and steganography. The cryptographic algorithm used is Advanced Encryption Standard (AES-128), Ziv Welch Lemp compression algorithm (LZW) and End of File (EOF) steganography algorithm. In the research that will be carried out LZW Algorithm will do the txt data compression process. After that the compression results will be encrypted using the AES method and the last is to insert the encryption results into the bmp image using the EOF method. The results of testing in this study LZW, AES and EOF methods were successfully implemented when tested one by one, but could not be implemented properly when all of these methods were combined when tested. Where the data from the seven test data used are only two data that were successfully tested.

Keywords: Lempel Ziv Welch, Advanced Encryption Standard, End Of File

I. Pendahuluan

Semakin canggihnya teknologi, orang bisa berkirim atau bertukar pesan untuk menyampaikan atau mengirim informasi penting dengan mudah. Pesan yang bersifat rahasia maupun tidak akan dikirim ke penerima pesan, tetapi pesan yang dibuat menggunakan TXT itu dapat diganti dan dirusak oleh pihak – pihak yang tidak bertanggungjawab. Sehingga penggunaan pesan dalam format TXT tidaklah aman. Oleh karena itu, untuk mengirim pesan yang sangat privasi membutuhkan keamanan akan informasi yang akan dikirimkan ke penerima.

Salah satu ilmu dalam mengamankan file yang digunakan pada saat ini yaitu kriptografi. Dimana kriptograpi digunakan untuk menjaga keamanan dari pihak yang tidak memiliki hak akses terhadap suatu data baik data berupa e-mail, dokumen, maupun berkas pribadi. Ada banyak macam Teknik krtiptografi yang bisa digunakan salah satunya yaitu *Advanced Encryption Standard* (AES). Algoritma AES merupakan algoritma chipper yang aman untuk melindungi data atau informasi yang bersifat rahasia. AES dipublikasikan oleh NIST (*National Institute of Standard and Technology*) pada tahun 2001 yang digunakan untuk menggantikan algoritma DES yang sudah dianggap kuno dan mudah dibobol (Bhaudhayana dan Widiartha 2015).

Namun jika hanya menggunakan kriptografi sebagai pengaman informasi akan menimbulkan kecurigaan karena data akan nampak seperti dienkripsi. Oleh sebab itu, perlu menyembunyikan data yang sudah dienkripsi ke dalam gambar supaya pihak yang tidak berkepentingan tidak merasa curiga dalam melihat gambar tersebut. dan teknik penyembunyian data ke dalam gambar disebut dengan teknik steganografi.

Steganografi digunakan sebagai seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Salah satu algoritma yang digunakan dalam steganografi yaitu *End of File* (EOF). Keunggulan dari metode *End of File* (EOF) file yang disisipkan tidak akan mengganggu kualitasnya, keunggulan lainnya metode EOF mempunyai kelebihan dapat menyisipkan pesan dalam jumlah yang tidak terbatas(Kusumawati dan Anisah 2015).

Akan tetapi metode EOF memiliki kelemahan karena ukuran data yang akan disisipkan ditambah dengan ukuran dari citra yang menjadi media penampung. Kelemahan tersebut membuat citra yang disisipkan akan terlihat disisipkan file/data. Sehingga untuk menutupi kelemahan yang dimiliki EOF file txt yang akan disisipkan akan dikompresi untuk mengurangi ukuran size dari citra tersebut. Metode kompresi yang akan digunakan pada penelitian yaitu *Lempel Ziv Welch (*LZW*)*.Oleh karena itu penelitian akan menggunakan Metode Kompresi *Lempel Ziv Welch* (LZW), *End Of File* (EOF) Dan *Advanced Encryption Standard* (AES) dalam mengamankan teks dokumen TXT ke dalam citra gambar format bmp.

II. Metode Penelitian

2.1 Kriptografi

Kriptografi adalah ilmu dan seni yang digunakan untuk menjaga keamanan pesan (*Chriptography is the art an science of keeping message secure*). Definisi lain, 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 . Dalam perkembangannya, ada 2 jenis algoritma kriptografi yakni algoritma enkripsi kunci simetris dan algoritma enkripsi kunci publik. Rijndael termasuk dalam jenis algoritma kriptografi yang sifatnya simetri dan cipher block. Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu (Indriyono, 2017)

2.2 Kompresi

Kompresi data sebenarnya adalah proses meminimalkan ukuran data atau berkas dengan mengurangi data yang berulang, karena umumnya pada sebuah data sering terjadi pengulangan. Data yang telah dikompres agar bisa digunakan kembali harus dikembalikan lagi seperti semula. Proses pengembalian sebuah data yang terkompresi menjadi seperti data aslinya disebut dengan dekompresi (Utari, 2016).

2.3 Steganografi

Steganografi merupakan seni atau ilmu yang digunakan untuk menyembunyikan pesan rahasia sehingga selain orang yang dituju, orang lain tidakakan menyadari keberadaan dari pesan rahasia tersebut. Steganografi membutuhkan dua bagian yang sangat penting yaitu berkas atau media penampung dan data rahasia yang akandisembunyikan. Steganografi berfungsi untuk menyamarkan keberadaan data rahasia sehingga sulit dideteksi, dan juga dapat melindungi hak cipta dari suatu produk. Data rahasia yang disembunyikan dapat diungkapkan kembali sama seperti aslinya tanpa merusak media file dan pesannya (Anggraini & Sakti, 2014).

2.4 *Advanced Encryption Standard* (AES)

Advanced Encryption Standard (AES) adalah algoritma kriptografi yang menjadi standar algoritma enkripsi kunci simetris pada saat ini. *Advanced Encryption Standard* (AES) dipublikasikan oleh NIST (*National Institute of Standard and Technology*) pada tahun 2001. AES merupakan blok kode simetris untuk menggantikan DES (*Data Encryption Standard*)(Rachman 2018).Input dan output dari algoritma AES terdiri dari urutan data sebesar 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau plaintext yang nantinya akan dienkripsi menjadi ciphertext. *Cipher key* dari AES terdiri dari key dengan panjang 128 bit, 192 bit, atau 256 bit. Perbedaan panjang kunci akan mempengaruhi jumlah round yang akan diimplementasikan pada algoritma AES ini(Prasetyo 2016).

2.5 *End Of File* (EOF)

Metode ini merupakan metode pengembangan LSB. Dalam metode ini pesan disisipkan diakhir berkas. Pesan yang disisipkan dengan metode ini jumlahnya tidak terbatas. Akan tetapi efek sampingnya adalah ukuran berkas menjadi lebih besar dari ukuran semula. Ukuran berkas yang terlalu besar dari yang seharusnya, tentu akan menimbulkan kecurigaan bagi yang mengetahuinya. Teknik EOF atau *End Of File* merupakan salah satu teknik yang digunakan dalam steganografi. Teknik ini menggunakan cara dengan menyisipkan data pada akhir file. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sesuai dengan kebutuhan. Ukuran file yang telah disisipkan data sama dengan ukuran file sebelum disisipkan data ditambah dengan ukuran data yang disisipkan ke dalam file tersebut (Muslih dan Rachmawanto 2016). Pada metode EOF ukuran pesan yang akan disisipi bisa lebih besar dari ukuran citranya. Metode EOF, kualitas citra setelah disisipi pesan tidak berubah, tetapi akan mengubah ukuran citranya (Pandapotan dan Zebua, 2016).

Tahapan proses embedding atau penyisipan pesan menggunakan metode End of File adalah sebagai berikut :

a. Inputkan cipherteks yang akan disisipkan.
b. Inputkan citra yang akan menjadi media penyisipan cipherteks.
c. Baca nilai setiap pixel citra.
d. Tambahkan cipherteks sebagai nilai akhir pixel citra dengan diberi karakter penanda sebagai penanda akhir cipherteks.
e. Petakan menjadi citra baru.

2.6 *Lempel-Ziv-Welch* (LZW)

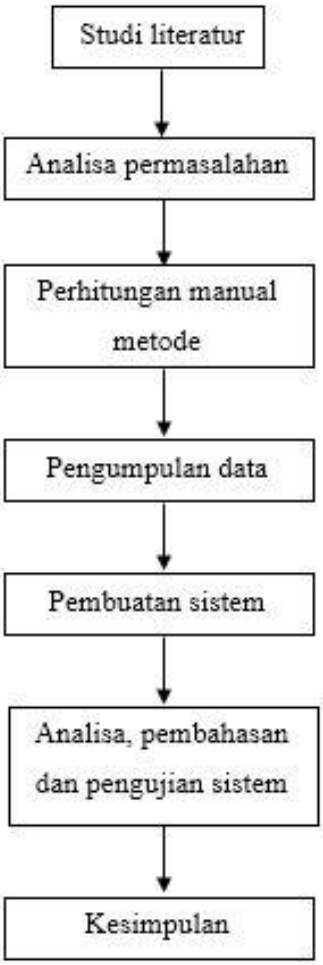
LZW merupakan kependekan kata dari *Lempel-Ziv-Welch*. *Abraham Lempel, Jacob Ziv, dan Terry Welch* adalah pencipta algoritma kompres lossless universal ini. Kelebihan algoritma ini yaitu cepat dalam implementasi dan kekurangannya kurang optimal karena hanya melakukan analisis terbatas pada data. Algoritma ini melakukan kompresi dengan menggunakan kamus, dimana fragmen-fragmen teks digantikan dengan indeks yang diperoleh dari sebuah "kamus" (Satyapratama et al., 2015). Pendekatan ini bersifat adaptif dan efektif karena banyak karakter dapat dikodekan dengan mengacu pada string yang telah muncul sebelumnya dalam teks.

2.7 Bahan atau Materi Penelitian

Data yang digunakan yaitu berupa data yang diambil dari internet atau data pribadi dalam format txt dan Bmp yang digunakan dalam proses implementasi ketiga metode dalam penelitian.

2.8 Kerangka Pikir Penelitian

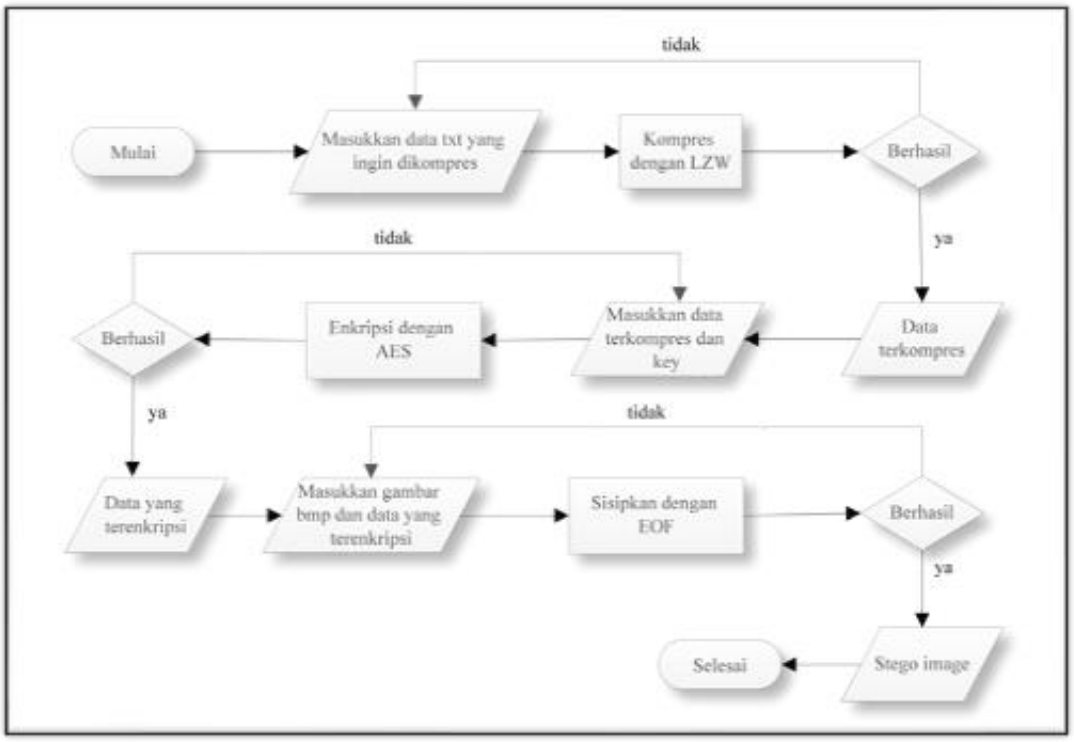
Adapun Kerangka Pikir Penelitian yang dilakukan pada implementasi Metode AES, LZW dan EOF seperti terlihat pada Gambar 1.



Gambar 1. Kerangka pikir penelitian

Kerangka pikir penelitian diawali dengan melakukan studi literatur tentang Kriptografi, Kompresi dan Steganography dan contoh implementasinya sehingga didapatkan 3 metode yang dipakai untuk penelitian. Selanjutnya melakukan analisis permasalahan tentang keamanan data agar sesuai dengan studi literatur yang telah dilakukan sebelumnya. Selanjutnya perhitungan manual metode dilakukan supaya sesuai dengan sistem yang dibuat. Selanjutnya mengumpulkan data dengan mengambil data dari internet, artikel dan data buatan pribadi sendiri lalu sumber lainnya untuk diimplementasikan kedalam 3 metode. Pembuatan sistem dilakukan setelah selesai perhitungan manual dan pengumpulan data. Pembuatan sistem mengacu kepada studi literatur, analisis masalah dan perhitungan manual agar sesuai dengan sistem. Setelah sistem selesai dibuat, dilakukan Analisa, pembahasan dan pengujian sistem untuk mengimplementasikan metode yang dipakai kedalam sistem dan mendapatkan kesimpulan tentang implementasi metode yang dipakai setelah melakukan pengujian.

2.9 Flowchart Alur Kerja Sistem



Gambar 2. Flowchart Alur Kerja Sistem

Pada Gambar 2.ditunjukkan proses perancangan sistem. Proses pertama *flowchart* dimulai dengan memasukkan data txt yang ingin dikompres dan melakukan proses kompresi dengan metode LZW. Selanjutnya setelah berhasil, hasil dari kompresi akan dienkripsi dengan AES dengan memasukkan hasil kompresi dan kuncinya dan Proses ketiga menyisipkan data yang telah terenkirpsi ke citra dengan EOF dengan memasukkan hasil enkripsi dengan citra gambar bmp. Di pengujian nanti, metode akan diuji satu persatu dulu untuk melihat apakah metode tersebut berhasil diimplementasikan atau tidak.

III. Hasil dan Pembahasan

3.1 Hasil Penelitian

Data yang akan digunakan pada penelitian adalah beberapa data berjenis teks bertipe txt dan citra bertipe bmp sebagai media penampung. Data akan diuji per metode, gabungan dua metode dan ketiga metode.

3.2 Pengujian dan Analisa LZW

Pengujian dilakukan untuk mengetahui apakah metode LZW bisa diimplementasikan. Data yang digunakan yaitu tujuh data txt.

Tabel **1.** Pengujian Metode LZW

No	Ukuran Sebelum dikompres	Ukuran setelah dikompres	Rasio Kompresi	Persentase Penghematan	Berhasil di extract (Ya/ Tidak)
1	16 bytes	32 bytes	2	-100	Ya
2	2.93 KB	2.52 KB	0.86	13.99	Ya
3	9.89 KB	6.62 KB	0.66	33.06	Ya

Tabel **1.** Pengujian Metode LZW (Lanjutan)

No	Ukuran Sebelum dikompres	Ukuran setelah dikompres	Rasio Kompresi	Persentase Penghematan	Berhasil di extract (Ya/ Tidak)
4	13.7 KB	8.42 KB	0.61	38.54	Ya
5	11 bytes	22 bytes	2	-100	Ya
6	16 bytes	26 bytes	1	-62	Ya
7	5 byte	10 bytes	2	-100	Ya

3.3 Pengujian dan Analisa AES

Pengujian dilakukan untuk mengetahui apakah metode AES bisa diimplementasikan. Data yang digunakan yaitu tujuh data txt.

Tabel **2.** Pengujian Metode AES

No	Ukuran	Kunci	Rasio Kompresi	Berhasil Enkripsi dan Dekripsi (Ya/Tidak)
1	16 bytes	informatikaumrah	32 bytes	Ya
2	3,010 bytes	rezekianaksolehh	3,024 bytes	Ya
3	10,131 bytes	makankuaci10buah	10,144 bytes	Ya
4	14,042 bytes	Chandrazulfika15	14,048 bytes	Ya
5	11 bytes	chandrazulfika15	16 bytes	Ya
6	16 bytes	uhuyyyyyyyyyyyyy	32 bytes	Ya
7	5 bytes	mainmainmianmain	16 bytes	Ya

3.4 Pengujian dan Analisa EOF

Pengujian dilakukan untuk mengetahui apakah metode EOF bisa diimplementasikan. Data yang digunakan yaitu tujuh data txt dan empat data bmp.

Tabel **3.** Pengujian Metode EOF

No	Ukuran Data	Ukuran Gambar	Ukuran Stego	Berhasil di extract (Ya/ Tidak)
1	16 bytes	594 KB (608,538 bytes)	594 KB (608,566 bytes)	Ya
2	2.93 KB	1.84 MB (1,935,498 bytes)	1.84 MB (1,938,513 bytes)	Ya
3	9.89 KB	874 KB (895,578 bytes)	884 KB (905,637 bytes)	Ya
4	13.7 KB	2.66 MB (2,798,802 bytes)	2.68 MB (2,812,801 bytes)	Ya
5	11 bytes	594 KB (608,538 bytes)	594 KB (608,561 bytes)	Ya
6	16 bytes	1.84 MB (1,935,498 bytes)	1.84 MB (1,935,526 bytes)	Ya
7	5 byte	874 KB (895,578 bytes)	874 KB (895,595 bytes)	Ya

3.5 Pengujian dan Analisa LZW dan AES

Pengujian dilakukan untuk mengetahui apakah gabungan dua metode LZW ke AES bisa diimplementasikan. Data yang digunakan yaitu tujuh data txt dan kunci yang sama sebelumnya.

Tabel **4.** Pengujian Metode LZW dan AES

No	Ukuran Sebelum dikompres	Ukuran setelah dikompres	Ukuran setelah Enkripsi	Ukuran setelah Dekripsi	Berhasil dekompres?
1	16 bytes	32 bytes	48 bytes	32 bytes	Ya
2	2.93 KB	2.52 KB	2.53 KB	2.52 KB	Ya
3	9.89 KB	6.62 KB	6.64 KB	6.62 KB	Ya
4	13.7 KB	8.42 KB	8.43 KB	8.42 KB	Ya
5	11 bytes	22 bytes	32 bytes	22 bytes	Ya
6	16 bytes	26 bytes	32 bytes	26 bytes	Ya
7	5 byte	10 bytes	16 bytes	10 bytes	Ya

3.6 Pengujian dan Analisa AES dan LZW

Pengujian dilakukan untuk mengetahui apakah gabungan dua metode AES ke LZW bisa diimplementasikan. Data yang digunakan yaitu tujuh data txt dan kunci yang sama sebelumnya.

Tabel **5.** Pengujian Metode AES dan LZW

No	Ukuran Data	Ukuran setelah Enkripsi	Ukuran setelah Kompres	Ukuran setelah Dekompres	Berhasil dekompres?
1	16 bytes	32 bytes	50 bytes	61 bytes	Tidak
2	2.93 KB	2.95 KB	3.57 KB	5.13 KB	Tidak
3	9.89 KB	9.90 KB	10.8 KB	18.0 KB	Tidak
4	13.7 KB	13.7 KB	14.7 KB	25.2 KB	Tidak
5	11 bytes	16 bytes	30 bytes	31 bytes	Tidak
6	16 bytes	32 bytes	54 bytes	57 bytes	Tidak
7	5 byte	16 bytes	26 bytes	29 bytes	Tidak

3.7 Perbandingan LZW ke AES dan AES ke LZW

Membandingkan gabungan metode mana yang baik dalam mengecilkan ukuran data ketika proses dilakukan berbeda yaitu enkripsi dan kompresi atau kompresi dan enkripsi. Data yang akan dipakai untuk pengujian adalah data yang telah dipakai pada pengujian sebelumnya.

Tabel **6.** Perbandingan enkripsi ke kompresi dan kompresi ke enkripsi

No	Ukuran Data	Proses	Hasil Proses	Data Berhasil Dikembalikan Utuh?
1	2.93 KB	LZW ke AES	2.53 KB	Ya
2	2.93 KB	AES ke LZW	3.57 KB	Tidak
3	9.89 KB	LZW ke AES	6.64 KB	Ya
4	9.89 KB	AES ke LZW	10.8 KB	Tidak

Dari Tabel 6. perbandingan enkripsi ke kompresi dan kompresi ke enkripsi yang berhasil mengecilkan data dan berhasil mengembalikan data yaitu proses dari LZW ke AES. Akan tetapi pada proses AES ke LZW tidak berhasil mengecilkan data dan tidak dapat mengembalikan data seperti semula.

3.8 Pengujian dan Analisa AES dan EOF

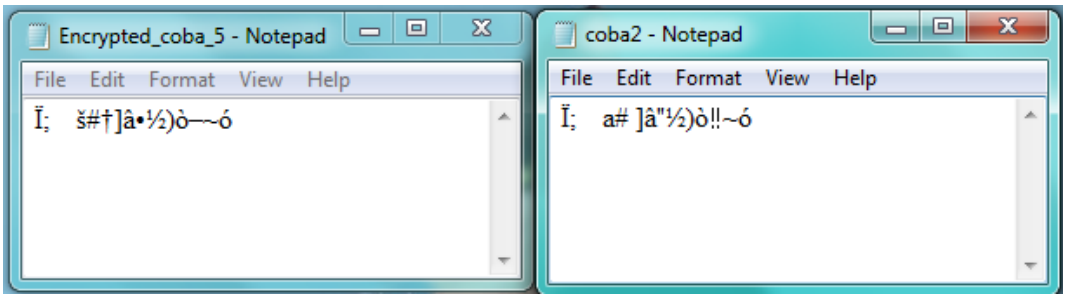
Pengujian dilakukan untuk mengetahui apakah gabungan dua metode AES ke EOF bisa diimplementasikan. Data yang digunakan yaitu tujuh data txt , empat data bmp dan kunci yang sama pada pengujian sebelumnya.

Tabel **7.** Pengujian Metode AES dan EOF

No	Ukuran Data	Ukuran Gambar	Ukuran setelah Disisipkan	Berhasil dikembalikan ke data awal?
1	16 bytes	594 KB (608,566 bytes)	594 KB (608,602 bytes)	Tidak
2	2.93 KB (3,010 bytes)	1.84 MB (1,938,513 bytes)	1.85 MB (1,941,035 bytes)	Tidak
3	9.89 KB (10,131 bytes)	884 KB (905,637 bytes)	892 KB (913,878 bytes)	Tidak
4	13.7 KB (14,042 bytes)	2.68 MB (2,812,801 bytes)	2.69 MB (2,824,257 bytes)	Tidak
5	11 bytes	594 KB (608,538 bytes)	594 KB (608,578 bytes)	Tidak
6	16 bytes	1.84 MB (1,935,498 bytes)	1.84 MB (1,935,558 bytes)	Ya
7	5 bytes	874 KB (895,578 bytes)	874 KB (895,614 bytes)	Ya

3.9 Analisa Pengujian AES dan EOF

Dari pengujian LZW dan EOF yang telah dilakukan, akan dianalisa kenapa terdapat data ekstrak dari citra tidak dapat kembali seperti semula. Pengujian kali ini menggunakan sample data coba_5 dengan kunci "chandrazufika15" dan gambar yang digunakan untuk menyisipkan Gb_1. Dapat dilihat karakter berganti pada data AES yang diektrak pada Gambar 3.



Gambar 3. Karakter data setelah enkripsi (kiri) dan setelah ekstrak (kanan)

Dari Gambar 3, terlihat bahwa data setelah enkripsi dan ekstrak dari citra tidak lagi sama. Perubahan karakter dapat dilihat pada Tabel 8.

Tabel **8.** Perubahan karakter

No	Data Enkripsi	Data Setelah Ektrak	Berubah/Tidak Berubah/hilang
1	Ï	Ï	Tidak Berubah
2	;	;	Tidak Berubah
3	š	a	Berubah
4	#	#	Tidak Berubah
5	†		Hilang

Tabel **8.** Perubahan karakter (Lanjutan)

No	Data Enkripsi	Data Setelah Ektrak	Berubah/Tidak Berubah/hilang
6	]	]	Tidak Berubah
7	â	â	Tidak Berubah
8	•	"	Berubah
9	½	½	Tidak Berubah
10	)	)	Tidak Berubah
11	ò	ò	Tidak Berubah
12	–	!!	Berubah
13	~	~	Tidak Berubah
14	ó	ó	Tidak Berubah

Selanjutnya dilakukan pengujian pada data AES yang terenkripsi untuk mengetahui apakah data enkripsi bisa disalin dan dipindahkan ke file txt baru. Pengujian dilakukan karena pada saat proses AES ke EOF , isi dari data setelah enkripsi akan dipindahkan untuk disisipkan kedalam citra. Data yang akan digunakan data coba_2 dan data coba_6. Hasil dapat dilihat pada Tabel 9.

Tabel **9.** Analisis Kompresi AES dan salinan Kompresi AES

No	Ukuran data setelah Enkripsi (hasil Enkripsi/hasil Salinan Enkripsi)	Ukuran data setelah Dekripsi (hasil dekripsi/hasil salinan dekrispi)	Data Kembali seperti semula ? (hasil kompresi / hasil salinan kompresi)
1	2.95 KB / 2.95 KB	2.93 KB / 2.93 KB	Ya / Tidak
2	32 bytes / 32 bytes	16 bytes / 16 bytes	Ya / Ya

Dari semua pengujian yang dilakukan dapat dijelaskan hasil dari analisa yaitu:

a. Ukuran data dari hasil enkripsi dan salinan enkripsi tetap sama.
b. Hasil enkripsi berhasil mengembalikan data dengan baik dan hasil salinan enkripsi tidak bisa mengembalikan data seperti semula pada data yang panjang, tetapi pada data yang ukuran kecil bisa dikembalikan.
c. Jadi data hasil enkripsi bisa disalin / dipindahkan ke file lain pada data yang kecil akan tetapi pada data yang ukuran lebih besar tidak bisa dikembalikan.
d. Metode EOF tidak bisa mengenali beberapa karakter dari hasil enkripsi AES.
e. Jadi hasil enkripsi bisa disisipkan dengan data yang karakter dikenali oleh EOF dan data berukuran kecil.

3.10 Pengujian dan Analisa LZW, AES, dan EOF

Pengujian terakhir adalah menguji apakah gabungan ketiga metode dapat diimplementasikan. Data yang digunakan adalah data sebelumnya.

Tabel **10.** Pengujian Metode LZW, AES dan EOF

No	Ukuran Data	Ukuran Gambar	Ukuran setelah Disisipkan	Berhasil dikembalikan ke data awal?
1	16 bytes	594 KB (608,566 bytes)	594 KB (608,627 bytes)	Tidak
2	3,010 bytes	1.84 MB (1,938,513 bytes)	1.84 MB (1,940,244 bytes)	Tidak
3	10,131 bytes	884 KB (905,637 bytes)	886 KB (907,808 bytes)	Tidak
4	14,042 bytes	2.68 MB (2,812,801 bytes)	2.68 MB (2,814,572 bytes)	Tidak

Tabel **10.** Pengujian Metode LZW, AES dan EOF (Lanjutan)

No	Ukuran Data	Ukuran Gambar	Ukuran setelah Disisipkan	Berhasil dikembalikan ke data awal?
5	11 bytes	594 KB (608,538 bytes)	594 KB (608,596 bytes)	Tidak
6	16 bytes	1.84 MB (1,935,498 bytes)	1.84 MB (1,935,557 bytes)	Ya
7	5 bytes	874 KB (895,578 bytes)	874 KB (895,612 bytes)	Ya

3.11 Pembahasan

Dari pengujian dan analisa yang telah dilakukan sebelumnya, terdapat beberapa pembahasan yaitu :

a. Metode AES berhasil diimplementasikan kedalam aplikasi. Hasil pengujian dari Tabel 2, yang didapatkan data yang diienkripsi dapat dikembalikan seperti semula. Data yang dikompres oleh LZW juga dapat dienkripsi dan dekripsi oleh metode AES.
b. Metode LZW berhasil diimplementasikan kedalam aplikasi. Hasil yang di dapatkan pada Tabel 1, yaitu pada saat mengkompresi data yang isinya karakter minim perulangan sehingga nilai rasio dan persentase penghematannya sangat buruk karena metode ini melakukan kompresi berdasarkan perulangan karakter. Akan tetapi walaupun hasilnya tidak terkompres dengan baik, data yang isinya minim karakter perulangan ini berhasil dikembalikan ke seperti semula ketika melalui proses kompresi dan dekompresi di metode LZW.
c. Metode EOF berhasil diimplementasikan kedalam aplikasi. Hasil yang didapat pada pengujian Tabel 3, saat mensisipkan data dan mengektraknya dapat berjalan dengan baik data yang dikembalikan utuh seperti semula. Kualitas citra tidak berubah, namun citra yang telah disisipkan ukurannya bertambah besar dari citra asli yang belum disisipkan.
d. Metode LZW-AES berhasil diimplementasikan pada penggabungan kedua metode ini. Dimana pada pengujian Tabel 4, data hasil kompresi bisa dienkripsi dan didekripsi oleh AES dikembalikan dengan utuh. Sehingga LZW bisa mengeluarkan kembali data yang terkompresi.
e. Metode AES-LZW tidak berhasil diimplementasikan pada penggabungan kedua metode ini. Dimana pada pengujian Tabel 5, LZW tidak bisa menampung/membaca file txt dari AES. Sehingga gabungan kedua metode ini tidak bisa digunakan.
f. Metode AES-EOF tidak berhasil diimplementasikan dengan baik. Dikarenakan pada pengujian Tabel 7, EOF bisa mensisipi dan mengektrak data yang karakternya hanya dikenalinya. Sehingga pada data yang karakter yang tidak dikenalinya akan hilang atau berubah karakternya.
g. Pada Pengujian **Error! Reference source not found.**abel 10, yang terakhir ketiga metode disatukan yaitu LZW-AES-EOF bisa diimplementasi tetapi tidak semua data yang bisa digunakan. Dimana ditemukan bahwa metode EOF tidak bisa mengembalikan data dari enkripsi AES yang tidak dikenali oleh EOF, sehingga hasil ektrak EOF hanya terbatas pada karakter yang dikenalinya.

IV. Kesimpulan

Dari pengujian dan analisa yang telah dilakukan sebelumnya, terdapat beberapa kesimpulan, yaitu :

a. Pada setiap metode dapat diimplemetasikan dan digunakan untuk mengamankan dokumen txt.
b. Pada gabungan dua metode yang berhasil diimplementasikan yaitu LZW ke AES. Semua data uji berhasil dimana bisa dikompres dan enkripsi kemudian didekripsi dan dekompres. Sedangkan pada tiga metode yang digabungkan LZW-AES-EOF tidak berhasil diimplementasi dengan baik karena dari tujuh data uji hanya dua data yang berhasil diimplementasikan dengan ketiga metode.

V. Daftar Pustaka

Anggraini, Y., & Sakti, D. V. S. Y. 2014. Penerapan Steganografi Metode End of File (Eof) Dan Enkripsi Metode Data Encryption Standard (Des) Pada Aplikasi Pengamanan Data Gambar Berbasis Java. *Konferensi Nasional Sistem Informasi, STMIK Dipanegara Makassar, September 2016*, 1743–1753.

Bhaudhayana, G. W., & Widiartha, I. M. 2015. Implementasi algoritma kriptografi aes 256 dan metode steganografi lsb pada gambar bitmap. *Jurnal Ilmu Komputer Universitas Udayana*, *8*(2), 15–25.

Indriyono, B. V. 2017. Implementasi Sistem Keamanan File dengan Metode Steganografi EOF dan Enkripsi Caesar Cipher. *Sisfo*, *06*(01), 1–16.

Kusumawati, T. I. jaya, & Anisah, D. 2015. Analisa dan Implementasi Steganografi untuk Pelaporan Internal Perusahaan Menggunakan Algoritma Data Encryption Standard (DES) dan Metode End Of File (EOF) Berbasis Java Programming. In *Telematika MKOM* (Vol. 7, Issue 2, pp. 177–186).

Muslih, & Rachmawanto, E. H. 2016. Pengamanan File Multimedia Dengan Metode Steganografi End of File Untuk Menjaga Kerahasiaan Pesan. *Techno.COM*, *15*(1), 1–6, ISSN:2356-2579.

Pandapotan, S. T., & Zebua, T. 2016. Analisa Perbandingan Least Significant Bit dan End Of File Untuk Steganografi Citra Digital Menggunakan Matlab. *Seminar Nasional Inovasi Dan Teknologi (SNITI)*, *3*, 604–608.

Prasetyo, R. 2016. *Aplikasi Pengamanan Data dengan Teknik Algoritma Kriptografi AES dan Fungsi Hash SHA-1 Berbasis Desktop*. *05*(September), 61–65.

Rachman, A. 2018. *Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES)*. *3*(2), 112–115.

Satyapratama, A., Widjianto, & Yunus, M. 2015. Analisis Perbandingan ALgoritma LZW dan Huffman pada Kompresi File Gambar BMP dan PNG. *Jurnal Teknologi Informasi*, *Volume 6*, 69–81.

Utari, C. T. 2016. Implementasi Algoritma Run Length Encoding Untuk Perancangan Aplikasi Kompresi Dan Dekompresi File Citra. *Jurnal TIMES*, *V*(2), 24–31.