Penerapan Algoritma AES pada Dokumen Penting yang Disisipkan Dalam Citra Berbasis Algoritma LSB dan Sobel

Yunita Dwi Setiyaningrum[1], Wijanarto[2], Asih Rohmani[3]
Fakultas Ilmu Komputer Universitas Dian Nuswantoro
Jl.Imam Bonjol No. 207 Semarang, Telp. (024) 3575916
email : [1]yunitadwisetiyaningrum@gmail.com, [2]wijanarto@dsn.dinus.ac.id,

Diterima: 21 Oktober 2019; Direvisi: 22 Nopember 2019; Disetujui: 25 Nopember 2019

Abstrak

Kemajuan teknologi berimbas pada kegiatan sehari-hari, misalnya sekarang ini masyarakat mudah mengirim dan menerima dokumen melalui e-mail tanpa terbatas oleh waktu dan jarak. Perkembangan teknologi ini juga berimbas pada peningkatan dampak negatif yang merugikan, seperti munculnya cybercrime, pishing, trojan, hackers. Penelitian ini bertujuan untuk meningkatkan pengamanan data pada dokumen penting yang tersimpan di server maupun sistem lain yang terdapat di PT Nasmoco Majapahit sebagai obyek penelitian. Metode yang dipakai adalah dengan menerapkan teknik kriptografi Advanced Encryption Standard (AES) pada dokumen yang akan disisipkan dalam citra dengan algoritma Least Significant Bit (LSB) dengan deteksi tepi Sobel. Teknik ini diharapkan mampu merahasiakan atau mengamankan dokumen penting milik perusahaan yang disisipkan dalam gambar, sedemikian sehingga gambar asli dengan gambar yang telah disisipi oleh dokumen penting tersebut menjadi sulit dibedakan oleh mata normal manusia pada umumnya. Hasil yang diperoleh dari penelitian ini menunjukkan bahwa algoritma AES dapat melakukan proses enkripsi dengan cukup cepat, yaitu rata-rata durasi sebesar 37,0976 detik. Pada deteksi tepi dalam proses penyisipan pesan bergantung pada objek dalam citra bukan hanya ukuran piksel saja semakin objek rumit maka semakin banyak koordinat yang digunakan untuk menyisipkan teks. Dan hasil kualitas citra stego setelah dilakukan pengujian menggunakan PSNR dan MSE hasil rata-ratanya juga cukup tinggi yaitu MSE sebesar 0,0425 dan PSNR sebesar 62,9392.

Kata kunci: *kriptografi, dokumen, steganografi, citra*

Abstract

Advances in technology have an impact on daily activities, for example now people can easily send and receive documents via email without being limited by time and distance. The development of this technology also has an impact on the increase of adverse negatives, such as preventing cybercrime, pishing, trojans, hackers. This research is aimed at increasing the security of data on important documents stored on servers or other systems in PT Nasmoco Majapahit as research objects. The method used is to apply cryptographic techniques Advanced Encryption Standard (AES) on documents that will be distributed in the image with the Least Significant Bit (LSB) algorithm with Sobel edge detection. This technique is expected to produce better or make important company documents that are inserted in the image, arranging the original image with an image that has been inserted by this important document becomes difficult to distinguish by the eyes of normal humans in general. The results obtained from this study indicate that AES can perform the encryption process quite quickly, namely an average duration of 37.0976 seconds. On edge detection in the process of inserting the message required on the object in the picture not only the size of the image. The more complicated objects, the more coordinates are used to insert text. And the results of the stego image quality after testing

using PSNR and MSE, the results of the assessment are also quite high, namely MSE of 0.0425 and PSNR of 62.9392.

***Keywords**: cryptography, documents, steganography, image*

1. PENDAHULUAN

Berdasar hasil survei, pada periode 2000-2017 pertumbuhan jumlah pengguna internet di dunia mencapai 97.64%. Dari prosentase pertumbuhan pengguna internet tersebut, Asia memperoleh predikat sebagai pengguna internet terbanyak di dunia dengan angka 49,7% dan negara Indonesia mencapai 50,4% [1]. Berdasarkan hasil survei diatas, adanya perkembangan teknologi yang serba canggih ini menyebabkan semakin bertambah pula *cybercrime,* salah satunya adalah *pishing* [2]. Masyarakat Indonesia harus dapat bertindak lebih cerdas dan selalu waspada dalam menyikapi munculnya teknologi yang semakin berkembang ini. Selain itu, keamanan data terutama dokumen rahasia juga menjadi hal utama yang harus di prioritaskan supaya bisa menghindari adanya kerentanan pencurian data rahasia. Di Indonesia, salah satu bentuk sasaran para pelaku *cybercrime* adalah *pishing*. Hal ini dibuktikan dengan hasil survei yang tercantum di Data dan Statistik Kementerian Komunikasi dan Informatika RI pada tahun 2014 mencapai 3,6% [3]. *Pishing* bukan hanya terjadi di Indonesia saja, menurut thehackernews.com, maraknya *pishing* justru dengan mengatasnamakan orang yang dikenal oleh korban, agar mudah untuk melakukan penyusupan dokumen yang dikirim. Pada PT. Nasmoco, belum terdapat sistem untuk pengamanan saat mengirim dokumen penting melalui e-mail. Oleh karena itu, dokumen yang bersifat rahasia ini harus dijaga keamanannya agar terhindar dari ancaman pihak luar.

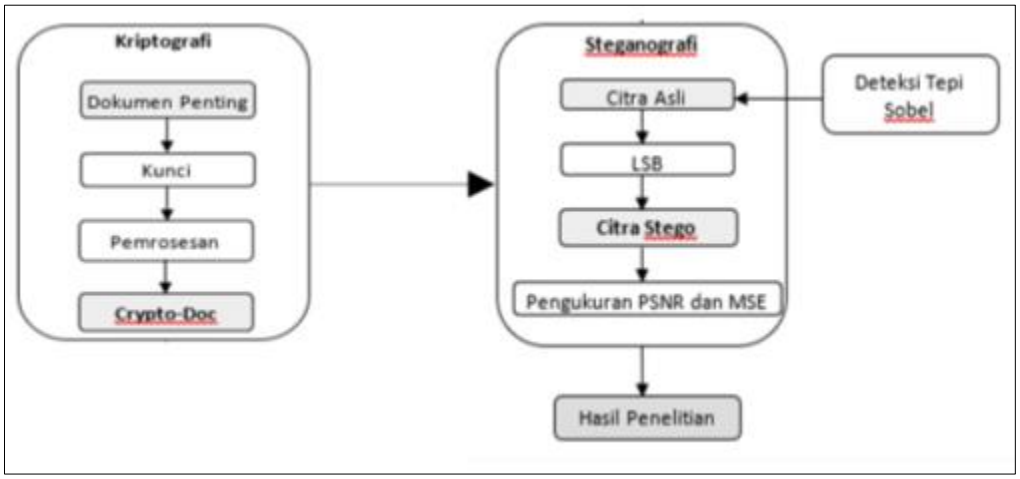
Menurut Pasal 1 ayat (2) UU No.8 Tahun 1997 yang dimaksud dari dokumen penting perusahaan yaitu catatan, data, atau keterangan yang dibuat maupun diterima oleh perusahaan untuk pelaksanaan kegiatan diperusahaan tersebut, baik tertulis maupun dengan media apapun[4]. Beberapa penelitian terkait sudah dilakukan, di bidang enkripsi data dengan teknik kriptografi perbandingan kecepatan algoritma *Advanced Encryption Standard* (AES) dan *Data Encryption Standard (*DES), menghasilkan kesimpulan bahwa AES lebih cepat performanya yaitu 8,105 (windows) dan 7,11 (MAC) dibanding DES dari waktu eksekusi pada windows dan MAC [5].

Analisa performa algoritma LSB, DCT, dan DWT untuk aplikasi *Digital Watermarking* dengan *Steganography*, menghasilkan kesimpulan bahwa DCT mempunyai PSNR yang paling tinggi, sedangkan DWT mempunyai MSE yang lebih tinggi [6]. Sementara penelitian untuk meningkatkan nilai *imperceptibility* dari penampung teks dalam [7] menghasilkan penelitian untuk membandingkan lima algoritma deteksi tepi ini (Robert, Laplace, Prewitt, Sobel, Canny), bahwa deteksi tepi Canny mempunyai kualitas yang paling tinggi dengan nilai PSNR yang paling rendah dan nilai MSE yang paling tinggi. Namun, deteksi tepi sobel merupakan metode yang bisa dikatakan seimbang, dimana kapasitasnya tinggi namun nilai PSNR dan MSE tidak terlalu rendah dibanding deteksi tepi yang lain.

Sementara dalam [8] mencoba menganalisis kualitas dari citra stego (citra setelah disisipkan) dengan LSB dan AES dan hasilnya mengalami perubahan. Ini terbukti melalui hasil analisis histogram warna mulai dari citra asli ke citra hasil stego. Perubahan kualitas ini bergantung dari ukuran pesan yang disisipkan. Selain itu, citra berubah setelah proses penyisipan pesan. Dengan ketiga algoritma tersebut maka orang awam sulit membedakan gambar asli dengan gambar yang telah disisipi oleh pesan rahasia. Pada penelitian ini citra cover menggunakan format bitmap (*.bmp) yaitu salah satu jenis format file penyimpanan yang masih asli belum melalui proses kompresi yang berfungsi sebagai penyimpanan dari citra biner sampai citra berwarna. Terakhir, implementasi kriptografi CBC dan steganografi LSB menggunakan deteksi tepi Sobel yang dilakukan dalam [9] , pada citra stego yaitu dengan melihat dari hasil PSNR yang tinggi dan nilai MSE yang rendah maka kualitas citra tersebut semakin bagus .

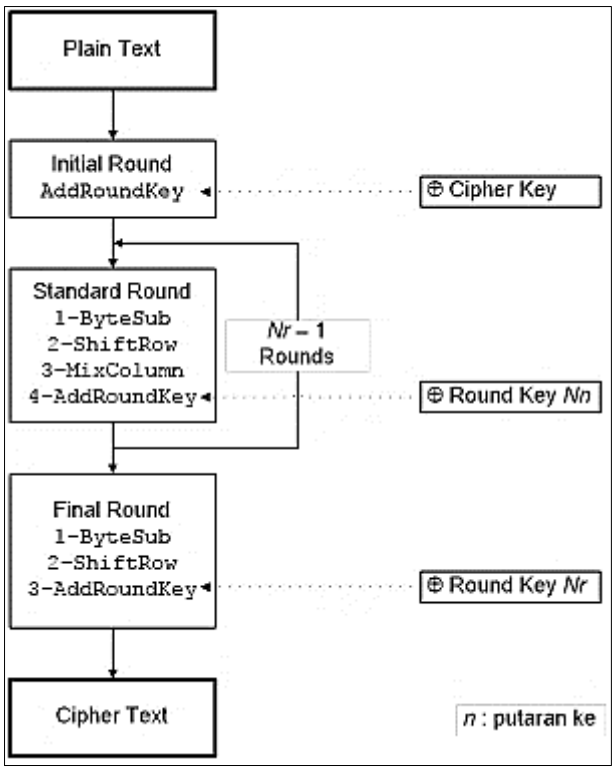
2. METODE PENELITIAN

Data yang digunakan pada penelitian adalah file dokumen berformat *.docx yang disisipkan pada citra berformat *.bmp. Gambar 1 menjelaskan skema penelitian, yang dimulai dari proses mengumpulkan dokumen berformat *.docx dengan besar file maksimal 50 Kb.



Gambar 1. Skema Penelitian

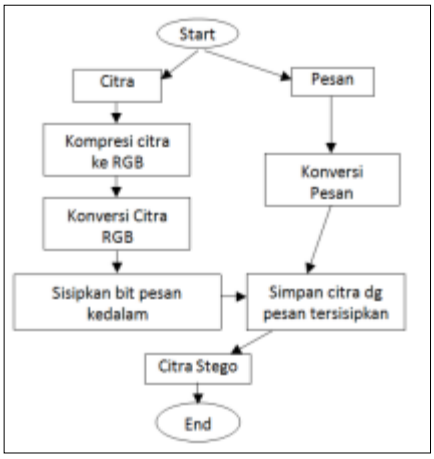
Setelah itu disiapkan pula citra yang sudah ditentukan sebagai media untuk penyisipan dari dokumen tersebut, dengan kompresi bmp pada dimensi 256 x 256, 512 x 512, dan 1024 x 1024 piksel. Langkah selanjutnya adalah melakukan proses enkripsi dan dekripsi dari sample dokumen secara manual, sehingga menghasilkan kripto dokumen (dokumen yang sudah terenkripsi isinya), dengan langkah-langkah seperti dijelaskan pada gambar 2.



Gambar 2. Skema Algoritma AES

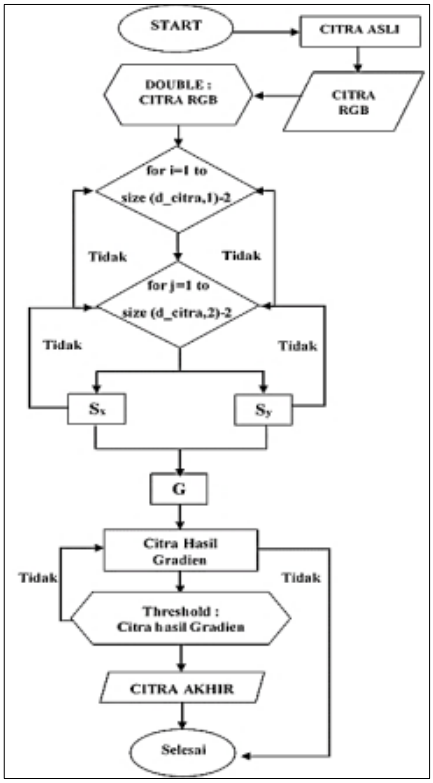
Dari dokumen terenkripsi akan dilakukan *initial round* dengan menambahkan *chiper key* sehingga akan menghasilkan data untuk dilakukan *standard round* sebanyak N putaran, mulai dari membagi *byte* (*byte sub*), operasi menggeser baris (*shift row*), mencampur kolom (*mix coloumn*) dan menambahkan *round key* yang diproduksi dengan operasi *XOR Round Key* setiap putarannya. Setelah itu finalisasi putaran dengan melakukan proses terhadap *byte sub*, *shift row* dan menambah ulang *round key* ke-N dan hasil akhirnya berupa *chipertext*.

Langkah berikutnya, dilakukan penyisipan data kripto dokumen tersebut ke dalam citra (dengan kompresi citra yang digunakan berformat *.bmp dengan ukuran 1024 x 1024 piksel) dengan menggunakan metode LSB hingga mendapatkan hasil citra stego, seperti pada skema gambar 3 dibawah ini [10]



Gambar 3. Skema Algoritma LSB (Encoding)

Setelah itu akan dilakukan pengambilan data citra stego (citra yang sudah tersisipi) kemudian melakukan proses deteksi tepi sobel sebagai pengamanan citra. Gambar 4 dibawah ini merupakan flowchart algoritma deteksi tepi sobel[10]:



Gambar 4. Skema Algoritma Sobel

3. HASIL DAN PEMBAHASAN

Citra yang digunakan dalam penelitian ini adalah 9 buah citra 8-bit dengan format *.bmp. Citra cover bertipe warna RGB. Citra cover dipilih dari jumlah *keypoint* yang lebih banyak daripada jumlah bit biner pada pesan agar semua bit biner pesan dapat disisipkan kedalam citra cover.

Enkripsi teks dengan AES

Berdasarkan algoritma pada gambar 1 diatas, proses pengenkripan teks dengan tulisan "Nomor : 031/IT/V" dan kunci "insistem" diproses menggunakan AES, *plaintext* yang berisi teks dan kunci dilakukan enkripsi untuk mendapatkan simbol *ciphertext* seperti disajikan dalam tabel 1 dibawah ini :

Tabel 1. Enkripsi Plainteks dan Kunci Menjadi *Ciphertext*

No	Plainteks			Kunci			Chiperteks		
	Simbol	ASCII	Biner	Simbol	ASCII	Biner	ASCII	Biner	Simbol
1	N	4E	0100 1110	i	69	0110 1001	93	1001 0011	ô
2	o	6F	0110 1111	n	6E	0110 1001	97	1001 0111	ù
3	m	6D	0110 1101	s	73	0111 0011	AF	1010 1111	>>
4	o	6F	0110 1111	i	69	0110 1001	DB	1101 1011	■
5	r	72	0111 0010	s	73	0111 0011	AC	1010 1100	¼
6	(spasi)	20	0010 0000	t	74	0111 0100	EB	1110 1011	Ù
7	:	3A	0011 1010	e	65	0110 1001	16	0001 1001	DLE
8	(spasi)	20	0010 0000	m	6D	0110 1001	D3	1101 0011	Ë
9	0	30	0011 0000			0000 0000	56	0101 0110	V
10	3	33	0011 0011			0000 0000	20	0010 0000	DC4
11	1	31	0011 0001			0000 0000	C2	1100 0010	_
12	/	2F	0010 1111			0000 0000	8A	1000 1010	ė
13	I	49	0100 1001			0000 0000	47	0100 0111	G
14	T	54	0101 0100			0000 0000	82	1000 0010	ê
15	/	2F	0010 1111			0000 0000	6D	0110 1110	M
16	V	56	0101 0110			0000 0000	17	0001 0111	DC1

Selanjutnya berdasarkan teknik seperti diatas telah dilakukan eksperimen terhadap 6 file dokumen dengan pasangan kuncinya seperti disajikan tabel 2 berikut :

Tabel 2. Data Eksperimen Enkripsi Dokumen

Dokumen Asli	UkuranDokumen	Kunci
dok_1.docx	12,2 KB	infomemo
dok_2.docx	13KB	inacara
dok_3.docx	12KB	inperbaik
dok_4.docx	14,4KB	inkonsum
dok_5.docx	12,7KB	Insistem

dok_6.docx	11,6KB	Infomemo

Hasil dari eksperimen terhadap dokumen pada tabel 2, disajikan pada tabel 3 berikut dibawah ini, dalam bentuk waktu proses dan hasil ***entropy*** (semakin mendekati uint8 maka tingkat keacakannya semakin rumit) :

Tabel 3. Durasi Proses Enkripsi dan Entropi Hasil Eksperimen

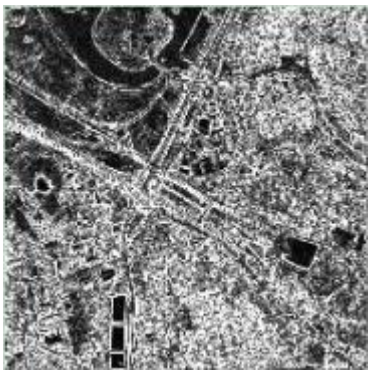
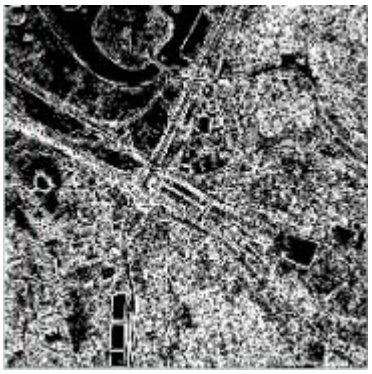
DokumenAsli	Durasi (sec)	Entropy
dok_1.docx	38,073088	7,8418
dok_2.docx	38,669243	7,8598
dok_3.docx	36,826473	7,8282
dok_4.docx	42,757815	7,8838
dok_5.docx	33,649265	7,8527
dok_6.docx	32,61005	7,8286
Σ Rata − rata	37,09765583	7,8491

Didapatkan rata-rata proses enkripsi tiap dokumen sebesar 37.1 detik dengan entropi sebesar 7.8, artinya semakin besar nilai entropi yang mendekati nilai 8 bit integer semakin rumit dan tinggi nilai acaknya.

Penentuan Koordinat dengan Deteksi Tepi Sobel

Sementara citra yang akan disisipi dokumen akan ditentukan koordinatnya dengan deteksi sobel, citra tersebut dari RGB diubah menjadi *grayscale* terlebih dahulu, karena deteksi tepi ini mengambil nilai kontras warna *background* dan *foreground.* Setelah itu citra *grayscale* tersebut dideteksi tepinya dengan *tresholding* sebesar 80 agar tepi lebih jelas. Kemudian hasil dari deteksi yang berupa koordinat tepi yang berfungsi untuk menyisipan teks didalam citra.

Gambar 5 dibawah ini merupakan contoh output dari hasil deteksi tepi sobel dengan hasil deteksi tepi sobel ditambah dengan nilai *tresholding* :

Citra Asli	**Citra Sobel**	**Citra Threshold**
		
a. citra_3.bmp	b. Citra Sobel	c. Citra Threshold

Gambar 5. Citra Deteksi Sobel

Koordinat pada hasil citra deteksi tepi sobel dengan nilai treshold = 80 disimpan sebagai koordinat untuk penampung dalam proses penyisipan teks dokumen. Pada tabel 4 berikut ini merupakan koordinat dari "**citra_3.bmp**" untuk penampung teks :

Tabel 4 : Koordinat dari Citra Sobel Untuk Penampung Teks

Iterasi	X	Y	Iterasi	X	Y
1	2	393	11	2	405
2	2	394	12	2	406
3	2	395	13	2	409
4	2	396	14	2	410
5	2	397	15	2	411
6	2	398	16	2	414
7	2	399	17	2	415
8	2	400	18	2	416
9	2	401	...	...	...
10	2	402	47.364	511	511

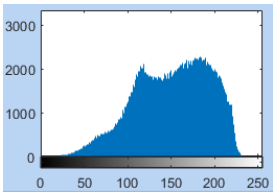
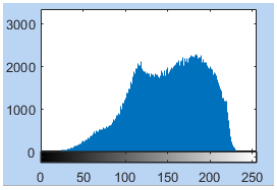
Setelah itu dilakukan proses LSB, dengan menggunakan koordinat dari hasil proses deteksi tepi sobel diatas. Setelah mendapatkan koordinatnya kemudian proses LSB ini melakukan penyisipan *ciphertext* dari hasil proses pengenkripan dengan metode AES diatas. Berikut ini merupakan langkah – langkah dalam penyisipan teks ke dalam citra, berdasarkan koordinat dari citra hasil deteksi sobel dan *ciphertext* hasil dari proses AES yang akan disisipkan dalam citra, kemudian dilakukan proses steganografi dengan menggunakan algoritma LSB, dan akan menghasilkan citra stego, untuk mengetahui perbandingan antara citra asli dan citra stego bisa dilihat dari nilai MSE dan PSNR, selain itu juga bisa dilihat melalui histogram. Sehingga citra berubah menjadi seperti tabel 5 dibawah ini.

Tabel 5 : Hasil Proses Steganografi

Iterasi	X	Y	RGB	Citra Cover	Pesan	Citra Stego
1	2	5	3	159	1	159
2	2	10	3	159	0	159
3	2	11	3	181	0	181
4	2	24	3	161	1	161
5	2	25	3	181	0	181
6	2	26	3	194	0	194
7	2	27	3	203	1	203
8	2	32	3	165	1	165
9	2	33	3	185	1	185
			...			
128	2	454	3	189	1	189

Berikut histogram antara citra cover dan citra stego, seperti tabel 6 berikut dibawah ini:

Tabel 6. Perbandingan Citra Cover dan Stego

Citra Cover	**Histogram Citra Cover**	**Citra Stego**	**Histogram Citra Stego**
 citra_3.bmp		 stego_3.bmp	

Terlihat histogram hasil perbandingan citra cover sebelum dan sesudah di stego tidak berubah banyak, hal ini menunjukkan bahwa algoritma berhasil melakukan stego tanpa mengalami degradasi yang besar berdasarkan pengamatan visual mata manusia normal, seperti secara jelas disajikan dalam tabel 7 dibawah ini.

Tabel 7 : Hasil Perbandingan Histogram Citra Cover dan Citra Stego

Gradasi Warna	FrekuensiGradasi Warna Citra Cover	FrekuensiGradasi Warna Citra Stego	Hasil SelisihFrekuensi GradiasiWarna
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
		...	
221	899	900	1
222	885	880	4
223	886	890	5
		...	
254	0	0	0
255	0	0	0
256	0	0	0

Tabel 7 hanya menampilkan hasil proses yang mengalami perubahan besar antara citra cover dan stego yaitu pada warna 221, 222 dan 223 dimana terdapat perbedaan 1, 4 dan 5 yang artinya hanya kecil sekali perubahan yang diakibatkan penyisipan pada citra cover ke citra stego. Selain itu juga disajikan pada tabel 8 dan 9, Selain hasil selisih frekuensi gradian warna, ada beberapa range yang dapat diperoleh dari perbandingan pada histogram citra cover dan citra stegodiantaranya merupakan hasil perbandingan histogram dari citra cover dan citra stego pada layer ***Blue***:

Tabel 8. Perbandingan Histogram pada layer Blue

Range	Citra Cover	Citra Stego
Gradian Warna	0 - 255	0 - 255
Mean	181,72	181,72
Median	183	183
StandarDeviasi	24,53	24,54
Pixels	262144	262144
Percent	100	100

Terlihat bahwa terdapat perbedaan nilai standar deviasi dengan selisih sangat kecil yaitu 0.01, dimananilaibias ini memastikan sangat kecil perbedaan yang ditemukan, sehingga dapat dikatakan bahwa tidak terjadi perubahan yang signifikan antara citra cover dan stego. Juga pada tabel 8, merupakan waktu dalam pemrosesan penyisipan teks dokumen dengan menggunakan LSB :

Tabel 9. Durasi Proses Penyisipan Teks Dengan LSB

Citra Cover	Durasi LSB (sec)
citra_1.bmp	Gagal
citra_2.bmp	Gagal
citra_3.bmp	0,352543
citra_4.bmp	0,542407
citra_5.bmp	0,379739
citra_6.bmp	0,335288
Σ Rata– rata	**0,4024943**

Terdapat 2 kegagalan pengukuran disebabkan tingginya nilai randon dan putaran yang dilakukan algoritma, namun rata-rata durasi berada pada kisaran 0.4 detik, yang dinilai cukup cepat dalam mengerjakan data tersebut. Dan terakhir hasil evaluasi algoritma dengan mengukur PSNR dan MSE pada model terpilih disajikan pada tabel 10 berikut dibawah ini.

Tabel 10. Evaluasi MSE dan PSNR Pada Model

Citra Asli	Citra Stego	MSE	PNSR
 citra_1.bmp (256 x 256)	Error. Karena byte citralebih kecildibanding byte dokumennya	ERROR	ERROR

 citra_2.bmp (256 x 256)	Error. Karena byte citralebih kecildibanding byte dokumennya	ERROR	ERROR
 citra_3.bmp (512 x 512)	 stego_3.bmp	0,0628	60,1498
 citra_4.bmp (512 x 512)	 stego_4.bmp	0,0753	59,3649
 citra_5.bmp (1024 x 1024)	 stego_5.bmp	0,0167	65,9160
 citra_6.bmp (1024 x 1024)	 stego_6.bmp	0,0152	66,3259
Σ Rata– rata		0,0425	62,9392

Dari tabel 10 dapat dilihat bahwa hasil penyisipan teks ke citra mendapatkan rata-rata MSE sebesar 0,03835 dan rata-rata hasil PSNR sebesar 63,2871. Dan untuk pada “citra _1.bmp”

dan "citra_2.bmp" tidak dapat melakukan proses penyisipan dikarenakan besar bit pada citra lebih kecil dibanding besar bit dokumennya.

4. KESIMPULAN

Berdasarkan hasil penelitian maka dalam disimpulkan sementara, bahwa hasil rata-rata durasi sebesar 37,0976 detik pada pemrosesan algoritma AES sehingga dapat disimpulkan bahwa kinerja algoritma AES bekerja dengan cukup cepat saat melakukan enkripsi pada teks dokumen penting. Dan dari hasil pemrosesan AES pada size dokumen 14,4 KB memerlukan durasi cukup besar hingga mencapai 42,7578 detik dibanding dokumen lainnya, hal ini disimpulkan bahwa ukuran dokumen sangat mempengerahui kecepatan dalam proses enkripsi.

Hasil durasi saat proses LSB untuk penyisipan teks dalam citra mencapai rata-rata sebesar 0,4024943 detik, selain dengan menggunakan koordinat pada citra hasil deteksi tepi sobel hasilnya bukan hanya bergantung besar kecilnya dimensi namun juga dilihat dari kompleksitas pada objek dalam citra. Dan pada dimensi 256 x 256 tidak bisa melakukan proses LSB, dikarenakan besar byte pada dokumen lebih besar dibanding besar byte pada citra. Hasil kualitas citra stego dalam proses penyisipan teks dokumen setelah dilakukan pengujian terhadap nilai PSNR dan MSE hasil rata-ratanya cukup tinggi yaitu MSE sebesar 0,0425 dan PSNR sebesar 62,9392.

Kompleksitas pada citra juga mempengaruhi hasil MSE dan PSNR, semakin rumit hasil deteksi tepi sobel maka nilai MSE dan PSNR juga semakin besar. Hasil histogram antara citra cover dengan citra stego juga tidak terlihat perubahan yang signifikan, dapat dibuktikan dengan hasil selisih frekuensi gradian warna pada tabel 4.12, gradian warna 221 selisih 1, 222 selisih 5, dan 223 selisih 4. Selain itu, standar deviasi layer blue pada citra cover dan citra stego selisih 0,01.

5. SARAN

Kedepan disarankan untuk menerapkan citra dengan dimensi lebih besar dan kedalaman bit yang lebih dalam dengan harapan dapat mengetahui perbandingan pada hasil proses LSB. Memberi parameter *tresholding* dengan nilai lebih dari 80 hal ini bertujuan untuk mengetahui pengaruh dari perbandingan hasil MSE dan PSNR.

6. DAFTAR PUSTAKA

[1] WIC, "Report on World Internet Development 2017," p. 35, 2017.

[2] M. Kumar, "Don ' t Fall For This Dangerously Convincing Ongoing Phishing Attack," pp. 0–2, 2017.

[3] D. Kominfo, "LaporanTahunan KOMINFO 2016," Jakarta.

[4] Undang-Undang Republik Indonesia Nomor 8 Tahun 1997 Tentang Dokumen Perusahaan , [online] http://www.anri.go.id/assets/download/23UU-Nomor-8-Tahun-1997-Tentang-Dokumen-Perusahaan.pdf [diakses tanggal 06 Juni 2019]

[5] Ahmed Khalid and S. D. Rihan, "A Performance Comparison of Encryption A Performance Comparison of Encryption Algorithms AES and DES," *Int. J. Eng. Res. Technol.*, vol. 4, no. November, pp. 151–154, 2017.

[6] S. Chandran and K. Bhattacharyya, "Performance analysis of LSB, DCT, and DWT for digital watermarking application using steganography," *Int. Conf. Electr. Electron. Signals, Commun. Optim. EESCO 2015*, no. September, 2015.

[7] S. Sarkar, "Comparison of various Edge Detection Techniques for maximum data hiding using LSB Algorithm," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 3, pp. 4722–4727, 2014.

[8] Nurhayati and S. S. Ahmad, "Steganography for inserting message on digital image using least significant bit and AES cryptographic algorithm," *Proc. 2016 4th Int. Conf. Cyber IT Serv. Manag. CITSM 2016*, 2016.

[9] T. A. Wijaya, "DokumenKaryaIlmiah | Skripsi | Prodi Teknik Informatika - S1 | FIK | UDINUS | 2016," *Fik*, vol. 1, no. 1, pp. 1–2, 2016.

[10] N. Jain, S. Meshram, and S. Dubey, "Image Steganography Using LSB and Edge – Detection Technique," *Int. J. Soft Comput. Eng.*, vol. 2, no. 3, pp. 217–222, 2012.