JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER

VOL. 5. NO. 2 FEBRUARI 2020
P-ISSN: 2685-8223 | E-ISSN: 2527-4864

APLIKASI KEAMANAN DOCUMENT DIGITAL MENGGUNAKAN ALGORITMA STEGANOGRAFI DISCRETE COSINE TRANSFORM (DCT) PADA PERUSAHAN ALAT BERAT

Muhammad Kailani Ridwan[1]; William Frado Pattipeilohy[2]; Sanwani[3*]
[*]Corespondent Author

Sistem Informasi [1,2]
Universitas Budi Luhur [1,2]
www.budiluhur.ac.id [1,2]
kheys.ridwan@gmail.com[1], william_frado@budiluhur.ac.id[2]

Sistem Informasi [3]
STMIK Nusa Mandiri [3]
www.nusamandiri.ac.id [3]
sanwani.swq@nusamandiri.ac.id[3]

Abstract— *Electronic documents are information that is permitted or stored in a way that is requested by a computer or other electronic device to be installed, assigned or processed. These documents consist of text, graphics or spreadsheets. For the current technological developments that improve progress, security is very important in companies that are difficult to avoid the follow-up of information by parties who are not responsible. One method that can be used to obtain digital documents is using Steganography and Cryptography technology by using Discrete Cosine Transform (DCT) technology and Advanced Desktop Encryption Standard (AES-192) algorithm based on Java Desktop. The purpose of this application is to prepare data or files to be hidden on the cover image of the file. Before inserting with the closing image file, the file is encrypted with a symmetrical key using the AES-192 algorithm. The benefits obtained in this application, the confidentiality of information or data on this heavy equipment company can be difficult with good and safe. With this application it is expected to help the confidentiality of information or data on heavy equipment companies. .*

Keywords*: Steganografi, Discrete Cosine Transform, DCT, Kriptografi, AES-192, Advanced Encryption Standard.*

Intisari—*Dokumen elektronik adalah informasi yang direkam atau disimpan dengan cara yang memerlukan perangkat komputer atau perangkat elektronik lain untuk menampilkan ,menafsirkan atau memprosesnya. Dokumen-dokumen tersebut berupa teks, grafik atau spreadsheet. Seiring perkembangan teknologi saat ini yang semakin maju, keamanan menjadi sangat penting pada perusahaan alat berat untuk menghindari terjadinya tindak pencurian informasi oleh pihak-pihak yang tidak bertanggung jawab. Salah satu cara yang dapat digunakan untuk mengamankan dokumen digital adalah memanfaatkan teknologi Steganografi dan Kriptografi dengan menggunakan algoritma Discrete Cosine Transform (DCT) dan algoritma Advanced Encryption Standard (AES-192) berbasis Java Dekstop. Tujuan aplikasi ini mengamankan sebuah data atau file yang akan disembunyikan pada file image cover. Sebelum disisipkan dengan file image cover, file tersebut dilakukan proses enkripsi pesan text terlebih dahulu dengan kunci simetris menggunakan algoritma AES-192. Manfaat yang didapatkan dalam aplikasi ini, kerahasiaan informasi atau data pada perusahfaan alat berat tersebut bisa terjaga dengan baik dan aman. Dengan aplikasi ini diharapkan dapat membantu menjaga kerahasiaan informasi atau data pada perusahaan alat berat.*

Kata Kunci*: Steganografi, Discrete Cosine Transform, DCT, Kriptografi, AES-192, Advanced Encryption Standard.*

PENDAHULUAN

Dalam era globalisasi perkembangan teknologi yang semakin pesat telah mempengaruhi segala bidang untuk terus berusaha membuat sistem informasi yang lebih baik. Salah satu kunci keberhasilan untuk menghadapi persaingan global adalah dengan terus meningkatkan pengetahuan yang dimiliki oleh setiap pribadi dalam menciptakan suatu sistem yang dapat berguna sesuai dengan keperluan masing–masing individu(Latif & Pratama, 2015). Sehingga dapat menghantarkan dan mendapatkan informasi lebih cepat dibandingkan dengan teknologi yang

digunakan sebelumnya, karena banyak pekerjaan dapat diselesaikan dengan cepat, akurat, dan efisien(Yuniati, Indriyanta, & Rachmat C., 2011) .

Salah satu dampak negative dalam perkembangan teknologi adalah adanya pencurian data, yang merupakan salah satu masalah serius dan ditakuti oleh para pengguna jaringan komunikasi di Alat Berat(Nurdin Bagenda & Mulyana, 2016). Dengan adanya pencurian data maka aspek keamanan dalam pertukaran informasi serta penyimpanan data dianggap penting(Hasugian, 2013) pada perusahan alat berat, karena suatu komunikasi data jarak jauh, belum tentu memiliki jalur transmisi yang aman dari penyadapan, serta penyimpanan data belum tentu aman dari pencurian(Nurdin, 2017), sehingga keamanan informasi menjadi bagian penting dalam dunia informasi itu sendiri. Salah satunya untuk mengamankan suatu informasi tersebut dengan menggunakan metode steganografi dan kriptografi(Anggraini & Sakti, 2014).

Metode Algoritma steganografi yang digunakan yaitu Algoritma Discrete Cosine Transform (DCT) dan metode kriptografi yang digunakan adalah Algoritma Advanced Encryption Standard (AES-192). Media Steganografi sebagai cover object adalah *file* berupa citra digital image (*.jpg,*.jpeg,*.bmp,*.png). Menyembunyikan pesan file document (*.docx,*.doc, *xls, *.xlsx dan pdf) ukuran *file* hanya dibatasi 1 MB dan tidak melebihi ukuran *file* Cover Image. Mekanisme penentuan *file* yang ingin di-*encode* dan di-*decode* hanya berdasarkan exstensi *file* (format *file*).

Dengan penggunaan aplikasi ini akan memperkuat system keamanan document sehingga perusahaan memiliki rasa ketenangan di bidang keamanan data dan mampu menjalankan bisnis nya dengan baik serta mampu mengembangkan bisnis dibidang yang lain.

BAHAN DAN METODE

Metode yang digunakan dalam penelitian ini adalah dengan melakukan metode penelitian kepustakaan, wawancara dan observasi di perusahaan alat berat. Pada metode pengembangan sistem yang digunakan adalah dengan tahap antara lain analisis, desain, implementasi dan perawatan.

Steganografi merupakan suatu ilmu atau seni dalam menyembunyikan informasi dengan memasukkan informasi tersebut ke dalam pesan lain(Niswati, 2012). Dengan demikian keberadaan informasi tersebut tidak diketahui oleh orang lain. Tujuan dari steganografi adalah untuk menyembunyikan pesan dalam pesan berbahaya lainnya dengan cara yang tidak memungkinkan musuh apapun bahkan untuk mendeteksi bahwa ada pesan kedua. Secara umum, teknik steganografi yang baik harus memiliki visual/imperceptibility statistik yang baik dan payload yang cukup(Alatas, 2009). Steganografi membutuhkan dua aspek yaitu media penyimpan dan informasi rahasia yang akan disembunyikan. Metode steganografi sangat berguna jika digunakan pada steganografi komputer karena banyak format file digital yang dapat dijadikan media untuk menyembunyikan pesan. Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya teks, citra, suara, dan video. Data rahasia yang disembunyikan juga dapat berupa teks, citra, suara, atau video.

Discrete Cosine Transform (DCT) adalah digunakan untuk mengubah sebuah sinyal menjadi komponen frekuensi dasarnya. Discrete Cosine Transform(DCT) termasuk metode steganography pada Algorithms and Transformation yang menyembunyikan data dalam fungsi matematika(Obukhov & Kharlamov, 2008). DCT mempunyai dua sifat utama untuk kompresi citra dan video yaitu Mengkonsentrasikan energi citra ke dalam sejumlah kecil koefisien (energi compaction). Meminimalkan saling ketergantungan diantara koefisien-koefisien (decorrelation).

Standar enkripsi dengan kunci-simetris yang diadopsi oleh pemerintah Amerika Serikat terdiri atas 3 blok cipher, yaitu AES-128, AES-192 dan AES-256, yang diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai Rijndael. Masing-masing cipher memiliki ukuran 128-bit, dengan ukuran kunci masing-masing 128, 192, dan 256 bit. AES telah dianalisis secara luas dan sekarang digunakan di seluruh dunia, seperti halnya dengan pendahulunya, Data Encryption Standard (DES)(Rahman, Miah, & Azad, 2014).
Setiap 3 blok chiper pada AES-128, AES-192 dan AES-256 mempunyai perbedaan pada jumlah key dan jumlah putaran keterangan pada tabel 2.

Tabel 1 : Perbandingan Jumlah Round dan Key pada Tipe AES

Tipe	Jumlah Key (NK)	Ukuran Blok (Nb)	Jumlah Putaran (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

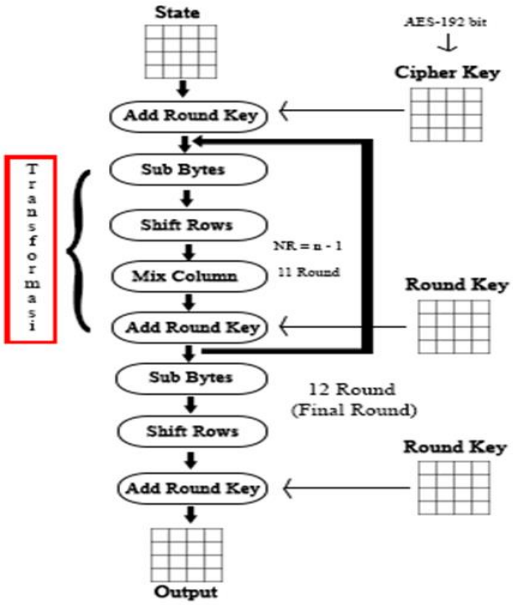
Sumber : (Bouillaguet et al., 2012)

Pada dasarnya, operasi Advanced Encryption Standard (AES) dilakukan terhadap *Array Of Byte*

Terakreditasi Sinta Peringkat 3 (Sinta 3) berdasarkan SK Dirjen Penguatan RisBang Kemenristekdikti
Nomor 28/E/KPT/2019, Tanggal 26 September 2019

VOL. 5. NO. 2 FEBRUARI 2020
P-ISSN: 2685-8223 | E-ISSN: 2527-4864

dua dimensi yang disebut *State*. *State* mempunyai ukuran NROWS x NCOLS. Pada awal enkripsi, data masukan yang berupa in0, in2, in4 ,in5, in6, in7, in8, in9, in10, in11, in12, in13, in14, in15 disalin ke dalam *Array State*.

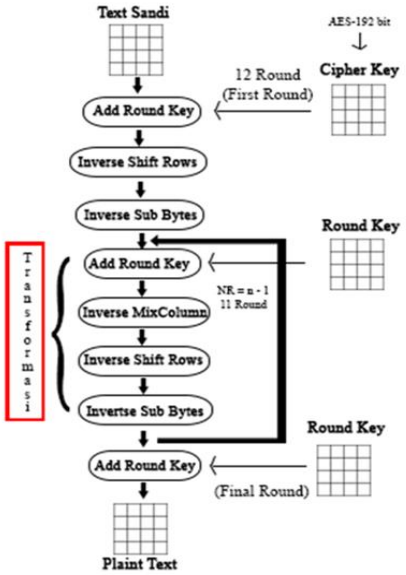


Sumber : (Primartha, 2013)

Gambar 1. Proses Enkripsi AES - 192

Proses Enkripsi pada gambar 1 dimulai dari AddRoundKey. AddRoundKey yaitu mengkobinasikan sebuah Chiperkey dan State dengan menggunakan operator XOR(Saputra & Kusumaningsih, 2018). Yang kedua Sub Bytes adalah menukar isi matriks dengan baris dan kolom pada tabel S-Box. Di bawah ini adalah contoh tabel S-Box. Yang ke tiga Shift Rows adalah sebuah proses melakukan pergeseran pada setiap elemen blok/tabel yang dilakukan per barisnya. baris pertama tidak dilakukan pergeseran, baris kedua dilakukan pergeseran 1 byte, baris ketiga dilakukan pergeseran 2 byte dan baris ke-empat dilakukan pergeseran 3 bytes. Berikutnya Mix Column adalah mengalikan tiap elemen dari Blok Chiper dengan matriks yang sudah ditentukan. Pengalian dilakukan seperti perkalian matriks biasa yaitu menggunakan Dot Product lalu perkalian keduanya dimasukkan ke dalam sebuah Blok Chiper baru. Bila sudah dikalikan semua dengan matriks yang sudah ditentukan. Maka terbentuk hasil Polynomial dengan bentuk biner dan hasil itu di gabungkan dengan rumus perkalian Mix Column pada setiap tahap perkalian matriks.

Dan yang terakhir Add Round Key adalah mengkombinasikan Chiperteks yang sudah ada dengan Chiperkey dihubungkan pada operator XOR(Hakim, Khairil, & Utami, 2014).



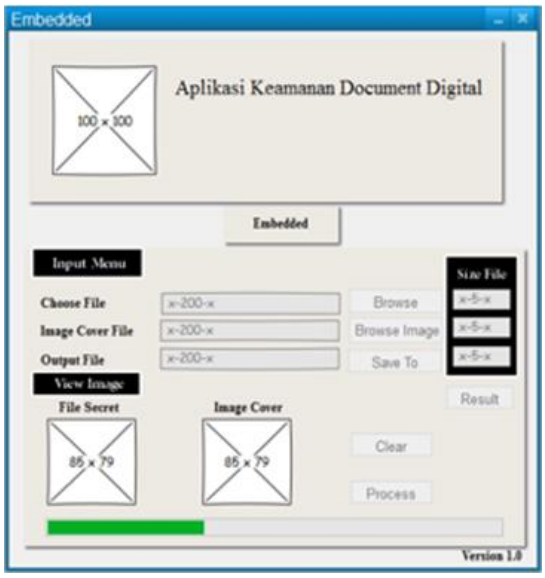
Sumber : (Primartha, 2013)

Gambar 2. Proses Deskrip AES – 192

Proses Deskrip pada gambar 2 dimulai dari InvMixColumns yaitu Setiap kolom dalam state dikalikan dengan matrik yang sudah ditentukan pada perkalian dalam AES-192, berikutnya InvShiftRows adalah transformasi byte yang berkebalikan dengan transformasi ShiftRows. Pada transformasi InvShiftRows, dilakukan pergeseran bit ke kanan sedangkan pada ShiftRows dilakukan pergeseran bit ke kiri. Yang ketiga InvSubBytes juga merupakan transformasi bytes yang berkebalikan dengan transformasi SubBytes. Pada InvSubBytes, tiap elemen pada state dipetakan dengan menggunakan tabel Inverse S-Box dan yang terakhir AddRoundKey adalah mengkombinasikan chiperteks yang sudah ada dengan chiperkey dihubungkan pada operator XOR.

HASIL DAN PEMBAHASAN

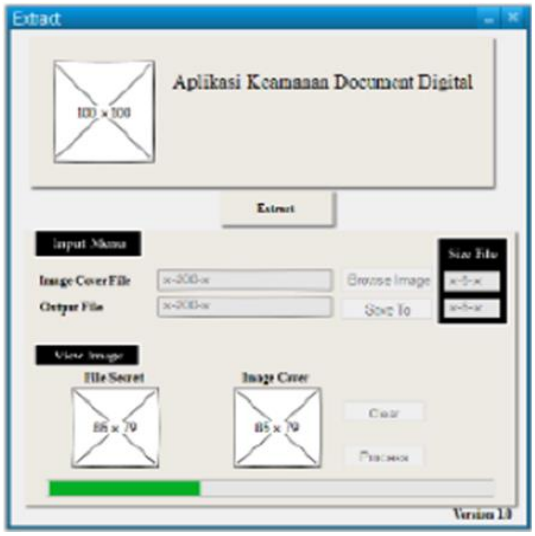
Perancangan akan dibuat dua tampilan ata desain yaitu tampilan layar Embed dan tampilan layar Extract. Pada rancangan *embedded* gambar 3 dibawah dijelaskan tentang bagaimana *user* melakukan sebuah penyisipan pada *file rahasia* dengan *file cover* sehingga dapat menghasil *stego image* atau *output* gambar. Saat melakukan proses *user* diminta untuk memasukan *password* sepanjang 8 *character* dan akan dilakukan sebuah proses enkripsi yaitu AES-192. setelah selesai melakukan proses enkripsi akan disisipkan dengan menggunakan Discrete Cosine Transform.



Sumber : (Sukarno, 2013)

Gambar 3. Rancangan Layar Embed

Setelah penjelasan dari rancangan layar porses *embedded*. Gambar 4 adalah gambar dari rancangan layar *extract*.



Sumber : (Sukarno, 2013)

Gambar 4. Rancangan Layar Extract

Pada rancangan layar *form extract* hampir sama dengan racangan layar *embedded* hanya saja ada beberapa perbedaan seperti tidak adanya choose *file secret* dikarenakan hanya mengeluarkan *file* asli dari *stego image*.
implementasi dan uji coba dari sistem yang akan dibuat. Bab ini akan menjelaskan tentang hasil dari proses *embed* dan *extract* berdasarkan uji yang telah disiapkan dengan berbagai uji coba *file Cover* dengan *file document* pada algoritma kripstografi AES-192 dan algoritma steganografi Discrete Cosine Transform (DCT). Pada bab ini juga akan membuat suatu evaluasi dari pengujian program tersebut. Evaluasi tersebut bertujuan agar selanjutnya progam ini akan dikembangkan kembali menjadi lebih baik lagi dan lebih berguna bagi yang menggunakan atau *user.* Tabel 2 menunjukani proses pengujian dari sample gambar atau *file Cover*.

Tabel 2 : Sample File Cover

NO	Gambar Cover	Nama File	Ukuran Pixel	Ukuran Gambar
1		Sample 1.JPEG	1920 x 1200	180 KB
2		Sample 2.JPG	2880 x 1800	699 KB
3		Sample 3.JPG	640 x 640	128 KB
4		Sample 4.JPG	640 x 640	104 KB

Sumber : (Ridwan, 2019)

Pada sampel tabel 2 menggunakan 4 sampel *file cover* dengan masing-masing ukuran pixel tinggi dan lebar yang berbeda-beda berekstensi tipe *file* jpg. Kemudian sampel *file cover* diatas akan dilakukan uji coba untuk melakukan penyisipan pada *file* dokumen *pdf, xlsx* dan *docx* dengan *file cover* sebagai media penampung. Dalam pengujian kali ini akan dibahas antara proses *embed* dan *extract* antara *file document.* Tabel 3 adalah hasil uji coba pada percobaan *file* dokumen pada *file cover*.

Tabel 3: Pengujian Embed file docx,xlsx dan pdf

No	File Secret		File Gambar		Waktu Embed (Sec.)
	Nama File	Ukuran	Nama File	Ukuran	
1	smo 1-30 des.docx	28 KB	Sample 1.jpeg	179 KB	199.09
2	smo 1-30 des.docx	28 KB	Sample 2.jpg	699 KB	245.23
3	smo 1-30 des.docx	28 KB	Sample 3.jpg	128 KB	155.33
4	smo 1-30 des.docx	28 KB	Sample 4.jpg	104 KB	156.09
5	Master 1-30 TARAKAN SEPT 2015.xlsx	22 KB	Sample 1.jpeg	179 KB	136.91
6	Master 1-30 TARAKAN SEPT	22 KB	Sample 2.jpg	699 KB	198.58

Terakreditasi Sinta Peringkat 3 (Sinta 3) berdasarkan SK Dirjen Penguatan RisBang Kemenristekdikti
Nomor 28/E/KPT/2019, Tanggal 26 September 2019

	2015.xlsx				
7	Master 1-30 TARAKAN SEPT 2015.xlsx	22 KB	Sample 3.jpg	128 KB	96.65
8	Master 1-30 TARAKAN SEPT 2015.xlsx	22 KB	Sample 4.jpg	104 KB	95.14
9	CORPORATE SECRETARY.pdf	17 KB	Sample 1.jpeg	179 KB	34.51
10	CORPORATE SECRETARY.pdf	17 KB	Sample 2.jpg	699 KB	77.22
11	CORPORATE SECRETARY.pdf	17 KB	Sample 3.jpg	128 KB	11.70
12	CORPORATE SECRETARY.pdf	17 KB	Sample 4.jpg	104 KB	12.28

Sumber : (Ridwan, 2019)

Pada hasil pengujian *embed* dapat dilihat pada tabel 4 menggunakan sebuah PSNR dan MSE.

Tabel 4 : Hasil Pengujian *Embed*

NO	Format	Stego File		PSNR (db)	MSE (db)
		Nama File	Ukuran		
1.	Doc	Stego Gambar 1.Jpeg	1.33 MB	50.3366	0.6018
2	Doc	Stego Gambar 2.JPG	7.57 MB	53.3827	0.2984
3	Doc	Stego Gambar 3.JPG	885 KB	43.7495	2.7424
4	Doc	Stego Gambar 4.JPG	813 KB	43.1658	3.1369
5	Xlsx	Stego Gambar 1.Jpeg	1.31 MB	51.0571	0.5098
6	Xlsx	Stego Gambar 2.JPG	7.56 MB	53.8033	0.2709
7	Xlsx	Stego Gambar 3.JPG	878 KB	44.6986	2.2041
8	Xlsx	Stego Gambar 4.JPG	803 KB	44.1296	2.5126
9	Pdf	Stego Gambar 1.Jpeg	1.29 MB	51.8329	0.4264
10	Pdf	Stego Gambar 2.JPG	7.55 MB	54.2310	0.2455
11	Pdf	Stego Gambar 3.JPG	874 KB	45.7243	1.7404
12	Pdf	Stego Gambar 4.JPG	794 KB	45.1793	1.9731
TOTAL				**581.290**	**16.662**

Sumber : (Ridwan, 2019)

Hasil pengujian dari tabel 4 pada saat selesai melakukan *embed* dapat ditarik kesimpulan bahwa rata-rata PSNR $\frac{581.2907}{12} = 48.4409db$ dan MSE $\frac{16.6623}{12} = 1.3885db$ kualitas citra yang dilakukan penyisipan adalah **baik** dengan rata-rata **> 40db** dari 12 sample dari tipe *file* dokumen yang berbeda-beda.

Tabel 5 : Hasil Pengujian Extract

No	Stego File		Hasil Extract	Ukuran	Waktu (Seconds)
	Nama File	Ukuran			
1	Stego Gambar 1.Jpeg	1.33 MB	smo 1-30 des.docx	28 KB	44.25
2	Stego Gambar 2.JPG	7.57 MB	smo 1-30 des.docx	28 KB	94.91
3	Stego Gambar 3.JPG	885 KB	smo 1-30 des.docx	28 KB	16.08
4	Stego Gambar 4.JPG	813 KB	smo 1-30 des.docx	28 KB	15.40
5	Stego Gambar 1.Jpeg	1.31 MB	Master 1-30 TARAKAN SEPT 2015.xlsx	22 KB	34.51
6	Stego Gambar 2.JPG	7.56 MB	Master 1-30 TARAKAN SEPT 2015.xlsx	22 KB	77.22
7	Stego Gambar 3.JPG	878 KB	Master 1-30 TARAKAN SEPT 2015.xlsx	22 KB	11.70
8	Stego Gambar 4.JPG	803 KB	Master 1-30 TARAKAN SEPT 2015.xlsx	22 KB	12.28
9	Stego Gambar 1.Jpeg	1.29 MB	CORPORATE SECRETARY.pdf	17 KB	27.0
10	Stego Gambar 2.JPG	7.55 MB	CORPORATE SECRETARY.pdf	17 KB	50.88
11	Stego Gambar 3.JPG	874 KB	CORPORATE SECRETARY.pdf	17 KB	7.77
12	Stego Gambar 4.JPG	794 KB	CORPORATE SECRETARY.pdf	17 KB	8.61

Sumber : (Ridwan, 2019)

Hasil pengujian diatas pada saat selesai melakukan *extract.* Dapat ditraik kesimpulan bahwa tidak terjadi perubahan *size file* yang di*extract*. Sehingga *file* tersebut sama seperti aslinya.

KESIMPULAN

Sesuai dengan pembahasan mengenai aplikasi keamanan document digital menggunakan algoritma steganografi discrete cosine transform (DCT) dan algoritma kriptografi advanced encryption standard (AES-192), maka kesimpulan yang dapat diambil antara lain yaitu yang pertama waktu yang digunakan untuk melakukan proses embed dan extract berbanding lurus dengan ukuran file yang diproses. Semakin besar ukuran file yang diproses maka semakin lama proses embed dan extract, semakin kecil ukuran file yang diproses, semakin cepat porses embed dan extract dilakukan. Kedua dengan adanya aplikasi steganografi dan kriptografi, proses penyimpan

informasi menjadi lebih aman dan yang terakhir Proses extract dengan password yang asli akan mengembalikan file menjadi file semula tanpa mengalami perubahan sedikitpun. Penelitian ini masih jauh dari sempurna dan masih perlu banyak perbaikan dan pengembangan supaya menjadi lebih baik lagi. Adapun saran untuk pengembangan dari penelitian ini antara lain waktu proses embed dan extract file yang rata-rata berukuran besar diharapkan dapat berjalan lebih cepat pada hardware yang lebih baik, dikembangkan menggunakan algoritma steganograi yang lebih baik, agar ukuran file hasil embed diharapkan dapat menjadi lebih kecil lagi dan aplikasi ini diharapkan dapat ditingkatkan kinerjanya sehingga file cover tidak hanya file gambar png, jpg dan bmp saja, namun file cover lainnya serta dapat Juga file video dan audio.

REFERENSI

Alatas, P. (2009). Implementasi teknik steganografi dengan metode lsb pada citra digital. *Universitas Gunadarma*.

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*.

Bouillaguet, C., Derbez, P., Dunkelman, O., Fouque, P. A., Keller, N., & Rijmen, V. (2012). Low-data complexity attacks on AES. *IEEE Transactions on Information Theory*. https://doi.org/10.1109/TIT.2012.2207880

Hakim, E. L., Khairil, & Utami, F. H. (2014). Aplikasi Enkripsi Dan Deskripsi Data Menggunakan Algoritma Rc4 Dengan Menggunakan Bahasa Pemrograman Php. *Jurnal Media Infotama*.

Hasugian, A. H. (2013). Implementasi Algoritma Hill Cipher Dalam Penyandian Data. *Pelita Informatika Budi Darma*.

Latif, F., & Pratama, A. W. (2015). Perancangan Sistem Informasi Manajemen Arsip Elektronik (E-Arsip) Berbasis Microsoft Access Pada PT.HI-TEST. *Jurnal Akuntansi, Ekonomi Dan Manajemen Bisnis*. https://doi.org/10.24843/LKJITI.6.3.16972

Niswati, Z. (2012). STEGANOGRAFI BERBASIS LEAST SIGNIFICANT BIT (LSB) UNTUK MENYISIPKAN GAMBAR KE DALAM CITRA GAMBAR. *Jurnal Lppm Unindra*, *5*. https://doi.org/http://dx.doi.org/10.30998/faktorexacta.v5i2.194

Nurdin, A. P. N. (2017). Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia. *Jesik*.

Nurdin Bagenda, D., & Mulyana, I. (2016). PERANCANGAN SISTEM KEAMANAN BRANKAS MENGGUNAKAN KARTU RFID BERBASIS ARDUINO. *JURNAL LPKIA*.

Obukhov, A., & Kharlamov, A. (2008). Discrete Cosine Transform for 8x8 Blocks with CUDA. *October*.

Primartha, R. (2013). Penerapan Enkripsi dan Dekripsi File menggunakan Algoritma Advanced Encryption Standard (AES). *Journal of Research in Computer Science and Applications*.

Rahman, A. U., Miah, S. U., & Azad, S. (2014). Advanced encryption standard. In *Practical Cryptography: Algorithms and Implementations Using C++*. https://doi.org/10.1201/b17707

Ridwan, M. (2019). *APLIKASI KEAMANAN DOCUMENT DIGITAL MENGGUNAKAN ALGORITMA STEGANOGRAFI DISCRETE COSINE TRANSFORM (DCT) PADA PERUSAHAN ALAT BERAT*. Jakarta.

Saputra, D., & Kusumaningsih, D. (2018). Implementasi Keamanan Database Menggunakan Algoritma Aes-192 Pada Pt Gurita Lintas Samudera Berbasis Android. *Jurnal Skanika*, *1*(`Vol 1 No 3 (2018): Jurnal SKANIKA Juli 2018), 884–888. Retrieved from http://jom.fti.budiluhur.ac.id/index.php/SKANIKA/article/view/2501

Sukarno, A. S. (2013). Pengembangan Aplikasi Pengamanan Dokumen Digital Memanfaatkan Algoritma Advance Encryption Standard, RSA Digital Signature dan Invisible Watermarking. *Prosiding Seminar Nasional Aplikasi Teknologi Informasi (SNATI) 2013*.

Yuniati, V., Indriyanta, G., & Rachmat C., A. (2011). ENKRIPSI DAN DEKRIPSI DENGAN ALGORITMA AES 256 UNTUK SEMUA JENIS FILE. *Jurnal Informatika*. https://doi.org/10.21460/inf.2009.51.69