Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.201854727
Vol. 5, No. 4, September 2018, hlm. 389-394 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 51/E/KPT/2017 e-ISSN: 2528-6579

KOMBINASI GIFSHUFFLE, ENKRIPSI AES DAN KOMPRESI DATA HUFFMAN UNTUK MENINGKATKAN KEAMANAN DATA

Dedi Darwis[1], Rizky Prabowo[2] , Nurul Hotimah[3]

[1, 3]Fakultas Teknik dan Ilmu Komputer, Universitas Teknokrat Indonesia
[2]Jurusan Ilmu Komputer, Universitas Lampung
Email: [1]darwisdedi@teknokrat.ac.id, [2]rizkydevelop@gmail.com, [3]shines.close@gmail.com

(Naskah masuk: 29 Maret 2018, diterima untuk diterbitkan: 28 Agustus 2018)

Abstrak

Informasi merupakan hal yang sangat berharga. Saat informasi atau data jatuh ke tangan yang tidak bertanggung jawab, maka akan menjadi bencana bagi pemiliknya. Berbagai macam cara dilakukan untuk melindungi data atau informasi. Teknik pengamanan data atau informasi telah berkembang dengan sangat pesat. Proses pengamanan pesan yang banyak beredar diataranya dengan menggunakan kriptografi dan steganografi. Dua teknik ini merupakan teknik yang berbeda maksud dan tujuannya. Kriptografi bertujuan untuk mengacak pesan supaya sulit dibaca oleh pihak yang tidak berkepentingan. Sedangakan steganografi bertujuan untuk menyembunyikan pesan.
Pada penelitian ini akan menggabungkan teknik kriptografi metode AES dengan teknik steganografi metode *gifsuffle*. Teknik kriptografi metode AES akan digunakan untuk merubah data atau informasi yang berbentuk *plain-text* menjadi *cipher-text*. Selanjutnya *cipher-text* tesebut akan disembunyikan ke dalam gambar berformat gif dengan metode steganografi *gifsuffle*. Metode *gifsuffle* akan dikombinasikan dengan algoritma huffman untuk memperbanyak pesan yang dikirimkan.
Penelitian ini berhasil menggabungkan metode kriptografi AES dengan metode steganografi *gifsuffle*. Hasil pengujian *imperceptibility* menunjukkan 85% responden tidak dapat membedakan gambar asli dengan gambar yang telah disisipi pesan. Pemisahan gambar dengan pesan dapat dilakukan dengan akurasi 100% dan proses dekripsi pesan cipher-text menjadi plain-text juga dapat dilakukan dengan sempurna.

Kata kunci: *AES, gifsuffle, huffman,kriptografi,steganografi*

COMBINATION OF GIFSHUFFLE, AES ENCRYPTION AND HUFFMAN COMPRESSION DATA AS EFFORT FOR IMPROVING DATA SECURITY

Abstract

Information is a very valuable thing. When information or data falls into irresponsible hands, it will be disastrous for the owner. A variety of ways are done to protect data or information. Data security techniques have grown very rapidly. The process of securing a message that many circulated diataranya by using cryptography and steganography. These two techniques are different techniques of purpose and purpose. Cryptography aims to randomize messages to be difficult to read by unauthorized parties. While steganografi aims to hide the message. In this research combine AES cryptographic method and with gifsuffle steganography method. AES method will be used to convert data or information in the plain-text form into cipher-text form. Furthermore, the cipher-text will be hidden into gif-format images with gifsuffle steganography method. The gifsuffle method will be combined with the huffman algorithm to multiply the transmitted data.
This research successfully combined AES cryptography method with gifsuffle steganography method. Imperceptibility test results show 85% of respondents can not distinguish original images with images that have been inserted data. Separation of images with data can be well done and the accuration reach 100%. Process of decrypting cipher-text into plain-text can also be done perfectly.

Keywords: *AES, cryptography, gifsuffle, huffman, steganography*

1. PENDAHULUAN

Pentingnya nilai informasi pada setiap aspek dapat memungkinkan adanya usaha pemindah alihan atau pencurian informasi ataupun data oleh pihak yang tidak berwenang. Media penyimpanan dan penyebaran data atau informasi yang digunakan menjadi salah satu alasan rentannya data atau informasi mudah diambil oleh pihak yang kurang bertanggung jawab. Hal ini disebabkan oleh sistem keamanan yang kurang efisien dalam memproteksi kerahasiaan data maupun informasi. Upaya yang dapat dilakukan untuk menjaga keamanan dan kerahasiaan data atau informasi, salah satu teknik yang digunakan untuk pengamanan data tersebut adalah menggunakan steganografi. Steganografi adalah teknik yang digunakan untuk menyembunyikan atau menyamarkan pesan atau informasi kedalam media penampung yang dapat berupa audio, gambar, video atau media digital lainnya(Sadikin, 2012). Teknik ini digunakan dengan tujuan agar data atau informasi rahasia yang hanya boleh diakses oleh pihak tertentu, tidak dapat diakses oleh pihak yang tidak berwenang. Salah satu teknik steganografi yang dapat digunakan yitu menggunakan metode *GifShuffle*, dimana metode ini memanfaatkan media citra berformat GIF(*Graphics Interchange Format*) yang berukuran relatif kecil dan bersifat lossless yang berarti bahwa citra tidak mengalami kehilangan kualitas ketika dikompresi atau disisipi data(Darwis & Everhard, 2015). Namun berdasarkan pengujian yang dilakukan, algoritma ini hanya menyediakan ruang penyimpanan pesan yang sangat terbatas pada skema *colourmapencoding* yakni sebesar 1683 bit(Kwan, 2010).

Keterbatasan tersebut dapat di atasi dengan metode kompresi data Huffman, dimana algoritma ini bersifat *loseless* yang berarti bahwa tidak ada informasi yang hilang setelah proses pemampatan terjadi(Sharma, 2010). Steganografi dapat dianalisis atau dideteksi berdasarkan spatial *domain steganographic schemes* dan *frequencydomain* menggunakan metode *ConvolutionalNeuralNetwork* (Salomon, et al., 2017). Karena bermunculan metode-metode yang dapat menyerang steganografi, maka diperlukan teknik untuk mengamankan pesan ataupun data yang terdapat dalam *stegoimage*. Metode kriptografi yang digunakan ialah AES, dimana pesan atau data asli diubah menjadi suatu bentuk kode yang tidak dapat dikenali lagi(Kristoforus & Aditya, 2012). Penelitian yang dilakukan bertujuan untuk merancang dan menerapkan teknik keamanan data steganografi dengan metode *gifshuffle* dan menambahkan metode kompresi data Huffman, agar jumlah data atau pesan yang dapat disisipkan lebih banyak. Serta mengkombinasikannya dengan kriptografi AES agar data atau informasi lebih terjamin keamanannya.

2. PENELITIAN TERDAHULU

Beberapa penelitian yang telah dilakukan sebelumnya diantaranya dilakukan oleh(Sharma, 2010)melakukan analisa algoritma Huffman terhadap format JPEG dan membandingkannya dengan teknik kompresi lainnya seperti aritmatika, LZW dan *RunLengthEncoding*. Perbandingan algoritma Huffman dengan Aritmatika, LZW dan *RunLengthEncoding*, dimana pada algoritma Huffman menghasilkan *loseless* pada hasil gambar yang terkompresi, penerapan yang relatif mudah dan menghasilkan kode yang optimal dibanding algoritma aritmatika dan *RunLengthEncoding*.

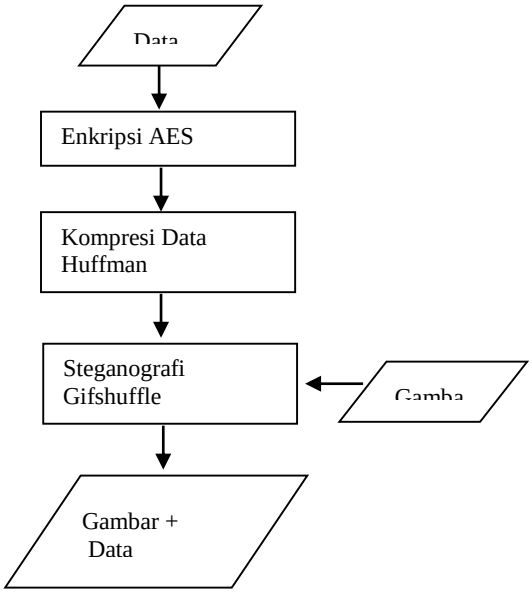
Penelitian lain dilakukan oleh (Mohd & Sharma, 2014)menganalisa sebuah teknik steganografi baru yang diusulkan yaitu teknik yang didasarkan pada perbedaan skema saluran RGB dan teks menggunakan analisis histogram. Teknik ini merupakan teknik domain spasial yang meningkatkan kualitas parameter *PeakSignalNoise* Ratio (PSNR) dan *MeanSquareError* (MSE).

(Kwan, 2010) mencetuskan algoritma gifshuffle yang merupakan progam untuk menyembunyikan pesan ke dalam gambar gif dengan cara menyusun ulang *colourmap* sesuai dengan *sourcecode* teks yang ingin di-*embed*. Proses *shuffle* gambar yang dilakukan nampak tidak dapat dibedakan dengan gambar aslinya.

(Darwis & Everhard, 2015) meneliti bagaimana mengamankan data laporan keuangan koperasi dari pihak yang tidak berkompeten. Teknik keamanan yang dilakukan meliputi teknik steganografi menggunakan metode*gifshuffle* sebagai media penampung data laporan keuangan. Selain itu (Omotosho, et al., 2014) meneliti mengenai cara mengamankan data resep dokter yang akan dikirim dari rumah sakit ke apotik, dimana perlindungan ini bertujuan untuk menjaga kerahasiaan resep dokter untuk pasien dari pihak yang tidak berwenang. Teknik pengamanan yang digunakan dalam penelitian ini yakni menggunakan steganografi dengan metode LSB untuk menyisipkan resep rahasia. Serta teknik kriptografi dengan metode AES untuk merubah resep rahasia menjadi sekumpulan kode yang sulit dipecahkan.

3. METODE

Proses pengamanan data dapat dilihat pada gambar 1.



Gambar 1. Proses pengamanan data

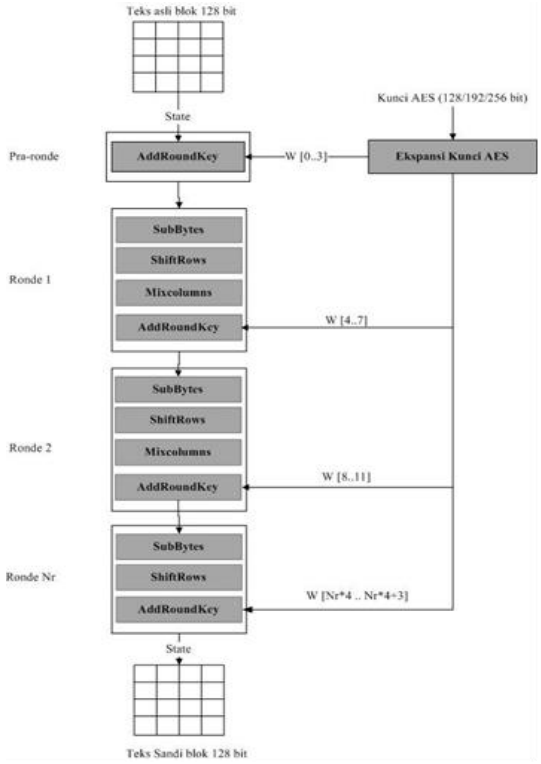
3.1. Kriptografi

Teknik penulisan pesan rahasia ini digunakan oleh bangsa mesir sekitar 3000 tahun sebelum masehi. Penulisan rahasia ini disebut *hieroglyphcs* dimana mereka (bangsa mesir kuno) menyembunyikan tulisan supaya tidak dapat diketahui oleh pihak yang tidak diharapkan. Kriptografi tidak hanya mengenai penyembunyian pesan atau tulisan tetapi lebih pada sekumpulan teknik matematika untuk keamanan informasi yang bersifat kerahasiaan.

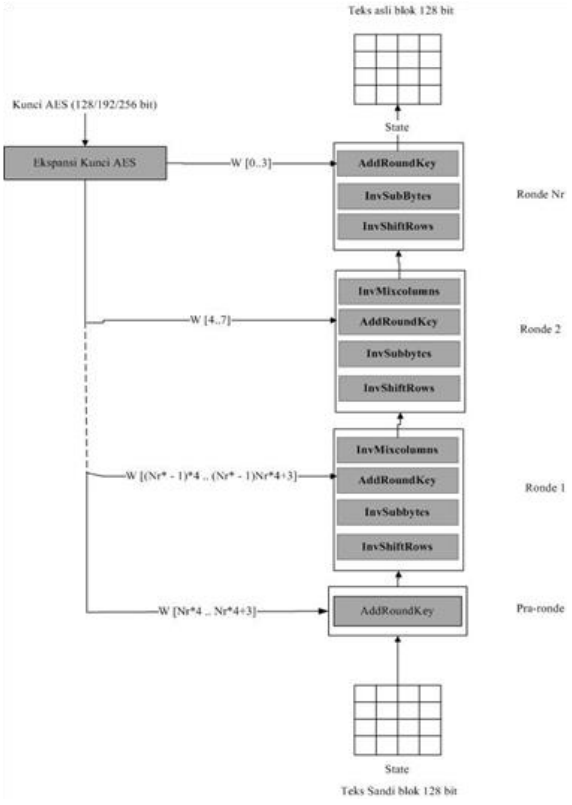
Berdasarkan pada penggunaan kunci, kriptogrfi terdiri dari dua jenis yaitu*simmetricencryption*dan *assimmetricEncryption*(Stallings & Brown, 2012).Kriptografi kunci *simmetric* menggunakan sebuah kunci (*single-key*) yang sama yang digunakan untuk melakukan proses enkripsi dan dekripsi. Sedangkan kriptografi kunci *assimmetric*menggunakan kunci yang berbeda pada saat melakukan proses enkripsi dan dekripsi.

3.2. *Advance Encryption Standard* (AES)

AES merupakan sistem penyandian blok yang bersifat *non-feistel* yang menggunakan teknik subtitusi, permutasi dan sejumlah putaran pada setiap blok yang akan dienkripsi (Setyaningsih, 2015).Secara garis besar proses enkripsi AES terdiri dari 4 jenis transformasi, yaitu *SubBytes*, *ShiftRows*, *MixColumns* dan *AddRoundKey*, sedangkan pada ronde terahir tidak dilakukan transformasi *Mixcolumns*. Skema enkripsi AES dapat dilihat pada Gambar 2. Proses dekripsi AES menggunakan transformasi *invers* yaitu, *InvSubBytes*, *InvShiftiRows*, *InvsMixColumns*. *AddRoundKey* merupakan transformasi yang bersifat *self-invers* dengan syarat menggunakan kunci yang sama. Skema dekripsi dapat dilihat pada Gambar 2.



Gambar 2. Enkripsi *Advance Encryption Standard*

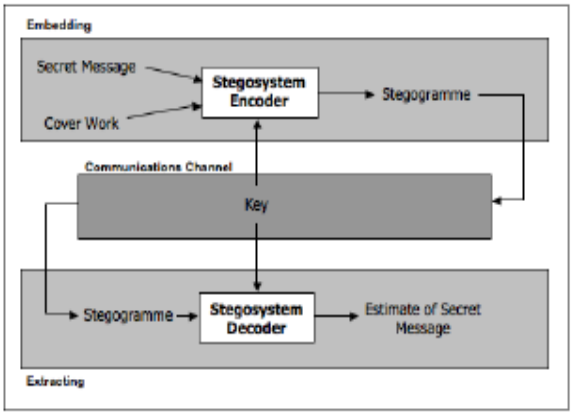


Gambar 3. Dekripsi *Advance Encryption Standard*

3.3. Steganografi

Steganografi pertama kali digunakan untuk mengirim pesan pada masa kerajaan yunani kuno. Teknik ini dilakukan dengan mencukur kepala

seorang budak kemudian dituliskan sebuah pesan rahasia, jika rambut budak tersebut telah tumbuh kembali, maka budak tersebut diutus untuk menyampaikan pesan rahasia tersebut(Cox, et al., 2008). Pada era modern steganografi diimplementasikan secara komputasi dimana *file* text, gambar, *file* audio dan *file* video dapat ter-embed kedalam *coverwork* steganografi (Bateman, 2008). Steganografi terdiri dari dua tahapan yaitu *embedding*dan *extacting*. *Embedding* adalah proses penyembunyian pesan kedalam *cover work*, hal ini harus dilakukan secara hati-hati agar *stego cover* yang dihasilkan tidak menimbulkan kecurigaan pihak ketiga, sedangkan *extracting* adalah proses yang lebih sederhana karena hanya mengembalikkan pesan rahasia yang berada didalam *cover work.*



Gambar 4. *Embedding* dan *Extracting*

Gambar 4. menjelaskan bagaimana proses steganografi berjalan. Terdapat dua *input* yang dibutuhkan dalam proses *embedding* :

1. *Secret Message* : biasanya berupa teks*file* yang memuat pesan yang ingin disisipkan.
2. *Cover Work* : digunakan untuk mengkonsep *stegogramme* yang memuat pesan rahasia.

3.4. *Gifshuffle*

Algoritma *gifshuffle*bekerja dengan cara menyembunyikan pesan kedalam gambar *gif* dengan cara melakukan *shufflecolourmap.Gifshuffle* bekerja disemua gambar *gif*, termasuk transparasi dan animasi *gif*. Algoritma *gifshuffle* pada intinya memanfaatkan *headerfilegif* yang menyimpan palet warna sebagai media penyisipan pesan. Gambar *gif* berisi *colourmap* sampai 256 entri dan menghasilkan kapasitas penyimpanan maksimum 1683 bit.

3.5. Pengujian

Pengujian steganografi terdiri dari tiga tahap yang akan dilakukan terhadap data yang telah terenkripsi, terkompresi dan tersisipkan kedalam media steganografi. Tiga tahap tersebut meliputi *fidelity*, *imperceptibility* dan *recovery*.

4. Hasil

Hasil pengujian terhadap pesan yang di enkripsi dan dekripsi dapat dilihat pada Tabel 1.

Tabel 1. Kecepatan Enkripsi dan Dekripsi

No.	*Plain text* (Hexa)	Enkripsi (*seconds*)	Dekripsi (*seconds*)
1	4e 55 52 55 4C 48 4F 54 49 4D 41 48 55 4C 55 4C	0.322144	0.210373
2	4B 41 4B 4B 44 45 44 49 62 61 69 6B 48 41 54 49	0.132969	0.124793
3	50 41 4B 4E 47 41 44 69 52 61 4E 42 50 4B 4B 55	0.120812	0.153897
4	6E 75 72 75 6C 4C 41 47 49 62 65 6C 61 6A 61 72	0.123331	0.139135
5	6D 41 54 45 6D 61 74 69 6B 41 41 53 49 4B 6C 6F	0.115934	0.135554
6	41 6c 6c 48 6B 75 4D 41 48 41 62 65 73 40 52	0.150456	0.160964
7	4D 41 4D 41 4B 42 41 50 41 4B 53 45 68 61 74 7A	0.120771	0.144201
8	6D 61 73 48 34 31 32 69 4D 33 34 4B 79 75 6E 7c	0.117455	0.146964

Tabel 1. Menunjukan kecepatan keberhasilan proses enkripsi dan dekripsi sebuah *plain-text* menjadi *chyper-text* dan sebaliknya.

Pengujian Kompresi dan dekompresi algoritma Huffman dilakukan untuk mengetahui apakah ada data yang hilang ketika proses pemampatan dilakukan terhadap data (*loseless*). Pengujian dilakukan dengan simulasi menggunakan *projectopensource* paranoia yang mana didalam *project* tersebut sudah tersedia kompresi dengan menggunakan Huffman yang langsung terintegrasi dengan kriptografi dan steganografi. Hasil perhitungan menunjukan bahwa rasio kompresi yang didapat sebesar 78% yaitu sebesar 16 bit dari ukuran data asli sebesar 72 bit.

Pengujian *imperceptibility* dilakukan berdasarkan indera penglihatan manusia, apakah terdapat perbedaan antara stego image dengan *cover image.*Pesan yang disisipkan kedalam *cover image* berukuran 1.157 bytes dan besarnya *cover image* adalah 19.081 bytes dengan dimensi 512 x 512 *pixel*. Hasil pengujian ini dapat dilihat pada Table 2.

Tabel 2. Hasil Pengujian *Imperceptibility*

Stego Key	Jumlah		
	Berbeda	TidakBerbeda	SedikitBerbeda
?.<;{}@#$56hjkl%	0	11	2

Stego Key	Jumlah		
	Berbeda	TidakBerbeda	SedikitBerbeda
La-Tahzan3901092	0	9	3
4E5552554C484F54494d4148554C554C	0	7	5
KAMPUS TEKNOKRAT	0	8	3
321@-=;">	0	10	2

Dari Tabel 2 terlihat bahwa 85% responden sulit membedakan antara gambar yang sudah disisipkan pesan dengan gambar asli. Ini menunjukkan bahwa pengujian *imperceptibility*mendapatkan hasil yang baik.

Pengujian *Fidelity* adalah pengujian yang dilakukan untuk mengetahui mutu atau kualitas yang dihasilkan stego *image* berdasarkan nilai MSE (*Meant Square Error*) dan nilai PSNR (*Peak Signal to Noise Ratio*). Adapun rumus untuk mendapatkan nilai MSE dan PSNR adalah sebagai berikut:

$$MSE = \frac{1}{\mathrm{M}\,.\,\mathrm{N}} \sum_{x=1}^{M} \sum_{y=1}^{N} (Sxy - Cxy) \qquad (1)$$

Sedangkan untuk mencari nilai PSNR didapat dari rumus sebagai berikut

$$PSNR = 10\ \log_{10}\left(\frac{C2max}{MSE}\right) \qquad (2)$$

Keteranagan
Cmax : nilai pixel terbesar dari keseluruhan citra
X dan Y : koordinat suatu titik pada citra
M dan N : dimensi dari citra
S : citra tersisipi
C : citra asli

Pada pengujian ini telah didapat nilai MSE dan PSNR berdasarkan besar *file* dan besar *cover image*. Adapun pengujian PSNR dan MSE yang dilakukan dengan menambah metode *poison noise*. Untuk lebih detailnya dapat dilihat pada Tabel 3.

Tabel 3. Hasil pengujian MSE dan PSNR

Cover Image	*File*Pesan	Stego Image	MSE (db)	PSNR (db)
Sastryy.gif (20.1 KB)	UJI1.txt	Sastryy.gif (20.2 KB)	106.29827	+27.75537
Lenaa.gif (236 KB)	UJI2.txt	Lenaa.gif (237 KB)	65.84445	+29.97961
HflameSurf_still.gif (18.6 KB)	UJI3.txt	HflameSurf_still.gif (20.7 KB)	21.23128	+34.89504
HflameVort_still.gif (28.3 KB)	UJI4.txt	HflameVort_still.gif (29.1 KB)	45.75332	+31.56057
hydrogen_vorticity.gif (2.8 MB)	UJI5.txt	hydrogen_vorticity.gif (24.4 KB)	83.29923	+28.95839

Pada Tabel 3 dapat dilihat bahwa hasil PSNR adalah berkisar 27 – 34 db dan nilai MSE lebih dari 100 db. Hal ini menunjukan terdapat kesalahan dalam melakukan pengujian *fidelity*, sebab dengan menambahkan *noise* didalamnya kualitas citra justru tampak kurang baik. Untuk itu sebaiknya penambahan *noise* kedalam citra hasil *stegoimage* tidak perlu dilakukan.

Pengujian ini dilakukan terhadap *stego image*, apakah data yang telah disipkan didalamnya dapat dikembalikan atau dipisahkan dari media penampung. Adapun pengujian dapat dilihat berdasarkan keutuhan pesan yang diekstrasi, pada tahap ini pengujian dapat dilihat pada Gambar 5 mengenai proses ekstrasi.

Gambar 5. Proses ekstraksi

Pada Gambar 5 terlihat mengenai hasil *encoding* atau proses pengembalian pesan. Proses yang harus dilakukan untuk memisahkan pesan dari gambar adalah dengan memilih gambar *stego image* yang akan diekstrak, kemudian *input* kunci atau key yang sama yang digunakan untuk meng-*embed* pesan kedalam gambar. Setelah gambar dan kunci telah dipilih maka selanjutnya pilih menu tools dan pilih lagi sub menu *decode*. Proses tersebut mengeluarkan pesan yang sama dengan pesan yang disisipkan kedalam gambar.

5. Simpulan

Hasil simulasi yang dilakukan, didapatkan bahwa proses pengamanan data menggunakan steganografi, kriptografi dan kompresi data berhasil diintegrasikan dan diterapkan dengan hasil yang baik. Algoritma kriptografi AES yang digunakan dapat melindungi data asli apabila citra *stego image* berhasil diekstrasi oleh *steganalyst*.HasilPSNR pada *stego image* yang dilakukan untuk saat ini bernilai 30 db, nilai ini didapat karena dilakukan penambahan metode *poison noisy*. 85% responden berpendapat bahwa tidak dapat membedakan antara stego image dengan *cover image*. Kompresi data yang digunakan menggunakan metode Huffman dapat meningkatkan banyaknya pesan yang disisipkan kedalam gambar.

DAFTAR PUSTAKA

BATEMAN, P., 2008. *Image Steganography and Steganalysis,* United Kingdom: Department of Computing Faculty of Engineering and Physical Sciences University of Surrey.

COX, J. et al., 2008. *Digital Watermarking and Steganography.* Second penyunt. USA: Morgan Kauffman.

DARWIS, D. & EVERHARD, Y., 2015. *Penerapan Steganografi, Kriptografi Dan Kompresi Data Sebagai Upaya Peningkatan Keamanan Laporan Keuangan Koperasi KJKS BMT.* s.l., Seminar Teknologi Informasi dan Komunikasi.

KRISTOFORUS, K. & ADITYA, S., 2012. *Implementasi Algoritma Rijndael Untuk Enkripsi Dan Dekripsi Pada Citra Digital.* s.l., Seminar Nasional Aplikasi dan Teknologi Informasi.

KWAN, M., 2010. *Darkside Technologies.* [Online] Available at: http ://www.darside.com.au/gifshuffle [Diakses 04 06 2016].

MOHD, N. & SHARMA, M. K., 2014. A New Steganography Technique Based on Difference Scheme of RGB Channels and Text Using Histogram Analysis. *International Journal of Engineering Research and Aplication*, 4(5), pp. 64-69.

OMOTOSHO, A., ADEGBOLA, O., MIKAIL, O. O. & EMUOYIBOFARHE, J., 2014. A Secure Electronic Prescription System Using Steganography with Encryption Key Implementation. *International Journal of Computer and Information Technology*, 03(5), pp. 980-986.

SADIKIN, R., 2012. *Kriptografi Untuk Keamanan Jaringan.* Yogyakarta: Andi.

SALOMON, M. et al., 2017. ConsultationSteganalysis via a convolutional neuralnetwork using large convolution filters forembedding process with same stego key: Adeep learning approach for telemedicine. *European Research in Telemedicine / La Recherche Européenne en Télémédecine*, 6(2), pp. 79-92.

SETYANINGSIH, E., 2015. *Kriptografi & Implementasinya Menggunakan MATLAB.* Yogyakarta: Andi.

SHARMA, M., 2010. Compression Using Huffman Coding. *International Journal of Computer Science and Network Security*, 10(5), pp. 133-140.

STALLINGS, W. & BROWN, L., 2012. *Computer Security Principles and Pactice.* Second penyunt. United States: Prentice Hall.