APLIKASI PENGAMANAN DOKUMEN DIGITAL MENGGUNAKAN ALGORITMA KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (AES-128), KOMPRESI HUFFMAN DAN STEGANOGRAFI END OF FILE (EOF) BERBASIS DESKTOP PADA CV. KARYA PERDANA

Wawan Budianto[1*], **Safrina Amini**[1], **Pipin Farida Ariyani**[2]
[12] Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
[*]Email: safrina.amini@budiluhur.ac.id

Abstrak

CV. Karya Perdana adalah perusahaan penyuplai berbagai macam peralatan komputer atau kebutuhan lain untuk perusahaan yang sudah menjadi rekanan. CV. Karya Perdana memiliki beberapa dokumen dalam bentuk digital yang harus dijaga kerahasiaannya seperti surat yang digunakan untuk transaksi dalam proses penyuplaian barang yang dibutuhkan. Untuk itu diperlukan suatu aplikasi yang bisa menjaga keamanan dalam penyimpanan dan pengiriman dokumen digital tersebut, salah satu cara yang digunakan yaitu dengan menggunakan teknik kriptografi, kompresi dan steganogafi. Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikan isi pesan menjadi suatu kode-kode yang tidak dimengerti sehingga tidak dibaca oleh pihak lain yang tidak berhak, kompresi adalah pemapatan data sehingga data yang dihasilkan menjadi lebih kecil dan steganografi adalah ilmu penyembunyian pesan atau informasi pada suatu media sehingga keberadaannya tidak terdeteksi oleh pihak yang tidak mempunyai akses atas isi pesan atau informasi tersebut. Algoritma kriptografi yang digunakan adalah Advanced Encryption Standard (AES-128), algoritma kompresi Huffman dan algoritma steganografi End of File (EOF). Algoritma AES merupakan standar enkripsi dengan kunci-simetris yang diumumkan oleh National Institute of Standard and Technology (NIST). Algortima kompresi Huffman merupakan kompresi yang bersifat losseless, dimana metode ini harus mendekompresi berkas agar dapat direkontruksikan menjadi berkas semula tanpa kehilangan informasi. Algoritma EOF menggunakan cara menambahkan file data pada akhir file gambar sehingga tidak mempengaruhi gambar dimana file data yang disisipkan ukurannya dapat melebihi file gambar. Dengan menggabungkan teknik kriptografi, kompresi dan steganografi maka aplikasi ini dapat menghasilkan ukuran file enkripsi lebih kecil sehingga proses penyisipan lebih cepat dan memberikan keamanan dokumen digital yang ada pada perusahaan.

***Kata kunci**: AES-128, EOF, huffman, kompresi, pengamanan*

1. PENDAHULUAN

1.1. Latar Belakang

Teknologi membuat pekerjaan dapat dikerjakan dengan cepat, akurat dan efisien sehingga banyak dokumen yang penting disimpan dalam bentuk digital. CV. Karya Perdana mempunyai dokumen digital yang sangat penting seperti surat yang digunakan dalam transaksi sebagai penyuplai untuk perusahaan lain. Keamanan dokumen digital tersebut harus dijaga baik dalam penyimpanan maupun dalam pengiriman, sehingga tidak bisa disalahgunakan oleh pihak lain yang tidak berhak atas dokumen tersebut yang akan menyebabkan kerugian pada CV. Karya Perdana dan perusahaan lain sebagai rekanan.

1.2. Permasalahan

Berdasarkan latar belakang masalah, maka dapat dirumuskan permasalahan sebagai berikut:

(1) Bagaimana cara membuat aplikasi untuk menjaga keamanan dokumen digital menggunakan algoritma *Advanced Encryption Standard* (AES-128), kompresi Huffman dan steganografi *End of File* (EOF).
(2) Bagaimana mengembalikan dokumen digital yang sudah dilakukan enkripsi, kompresi serta penyisipan ke bentuk *file* asli tanpa mengalami perubahan sedikitpun.

(3) Bagaimana mengurangi ukuran *file* hasil enkripsi sehingga dalam proses penyisipan ke dalam gambar tidak membutuhkan waktu yang lama.

1.3. Tujuan Penulisan

Berdasarkan permasalahan yang didapat sebelumnya, maka tujuan dari penulisan ini adalah sebagai berikut:

(1) Membuat aplikasi pengamanan dokumen digital menggunakan *Advanced Encryption Standard* (AES-128), algoritma kompresi Huffman dan algoritma steganografi *End of File* (EOF).
(2) Menghasilkan aplikasi yang mampu mengamankan dokumen digital dan mengembalikan ke bentuk aslinya.
(3) Menghasilkan aplikasi yang mampu melakukan proses penyisipan ke dalam gambar lebih cepat dengan dilakukan proses kompresi pada *file* hasil enkripsi.

1.4. Batasan Masalah

Agar pembuatan aplikasi terfokus dan tidak keluar dari materi pembahasan, maka diberikan beberapa batasan masalah sebagai berikut:

(1) Algoritma Kriptografi yang digunakan adalah *Advanced Encryption Standard* (AES-128).
(2) Algoritma Kompresi yang digunakan adalah Kompresi Huffman.
(3) Algoritma Steganografi yang digunakan adalah End of File (EOF).
(4) Bahasa pemograman yang digunakan adalah Java dan berbasis desktop.
(5) File dokumen yang dienkripsi, kompresi dan sisipkan dibatasi dengan ekstensi .doc dan .docx dan cover dibatasi dengan ekstensi .jpg dan .png.

2. METODOLOGI

Ada pun metode perancangan yang dilakukan adalah sebagai berikut:

(1) Metode Pustaka
Metode ini dilakukan untuk mengumpulkan data atau informasi dengan mencari referensi berupa jurnal, artikel dan situs internet mengenai metode yang akan digunakan dalam pembuatan aplikasi dan penulisan tugas akhir ini.
(2) Metode Analisis
Data atau informasi yang diperoleh kemudian di analisis dan dipelajari untuk merancang aplikasi.
(3) Perancangan Aplikasi
Merancang aplikasi dengan metode algoritma kriptografi *Advanced Encryption Standard* (AES-128), kompresi Huffman dan algoritma steganografi *End of File* (EOF).
(4) Pengkodean
Pada tahap ini data yang telah dianalisis untuk perancangan aplikasi dibuat dengan menggunakan bahasa pemrograman java.
(5) Pengujian
Pengujian dilakukan terhadap aplikasi yang telah dibuat dan mencari beberapa kesalahan hingga aplikasi yang dibuat sesuai dengan yang dirancang.

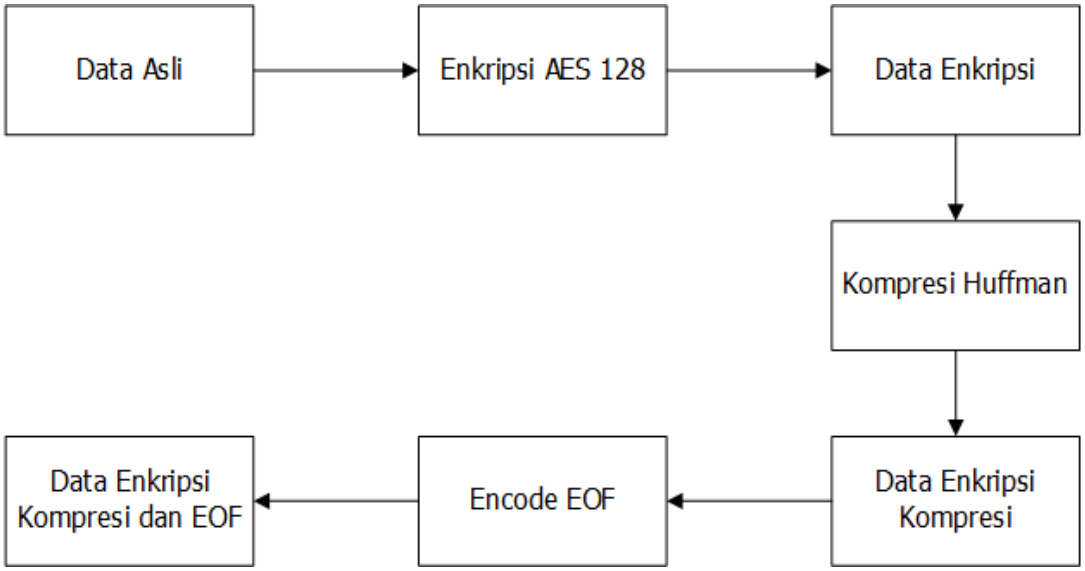
3. HASIL DAN PEMBAHASAN

3.1. Rancangan Program

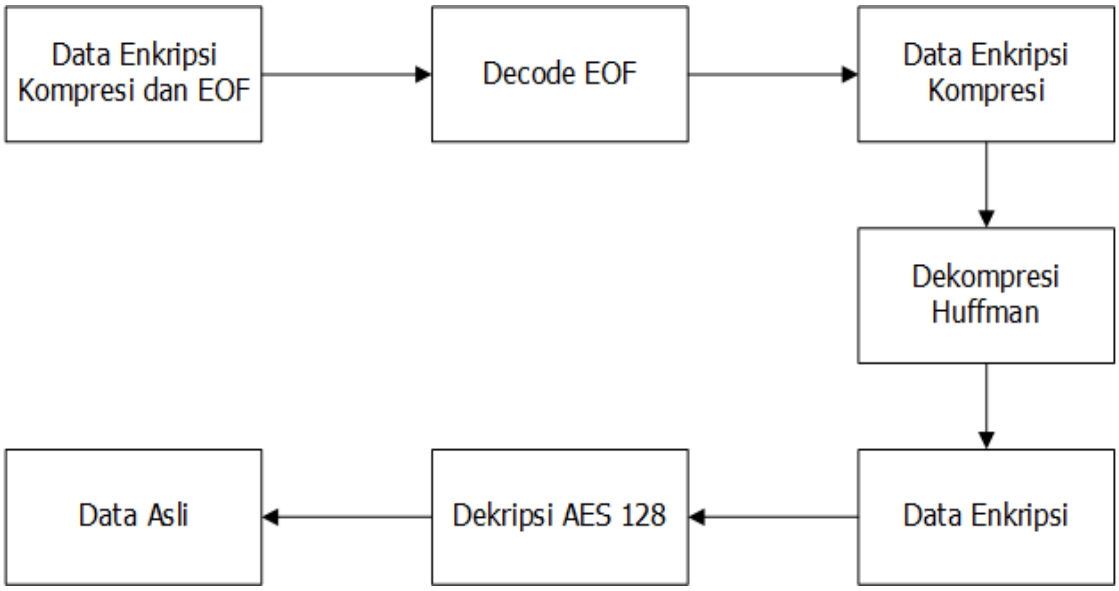
Program yang dibuat terdiri dari 5 buah *form layout*, yaitu *form* Menu, *form Encode, form Decode, form Log* Data, *form Help,* dan *form About.* Pada *form Menu* didalamnya terdapat 5 tombol utama yaitu tombol *Encode, Decode, Log, Help,* dan *About.*

Proses *encode* pada aplikasi ini dimulai dengan proses enkripsi *file* asli dengan menggunakan algoritma enkripsi AES 128 selanjutnya *file* hasil enkripsi dikompresi dengan menggunakan algoritma kompresi Huffman kemudian dilakukan proses *encode* atau penyisipan hasil enkripsi dan kompresi dengan menggunakan algoritma steganografi EOF. Pada proses *decode file,* dilakukan proses *decode* terlebih dahulu dengan menggunakan algoritma steganografi EOF, kemudian dilakukan proses dekompresi dengan menggunakan algoritma kompresi Huffman selanjutnya *file*

hasil *decode* dan dekompresi didekripsi dengan menggunakan algoritma kriptografi AES 128. Alur program ditunjukan pada gambar di bawah ini:



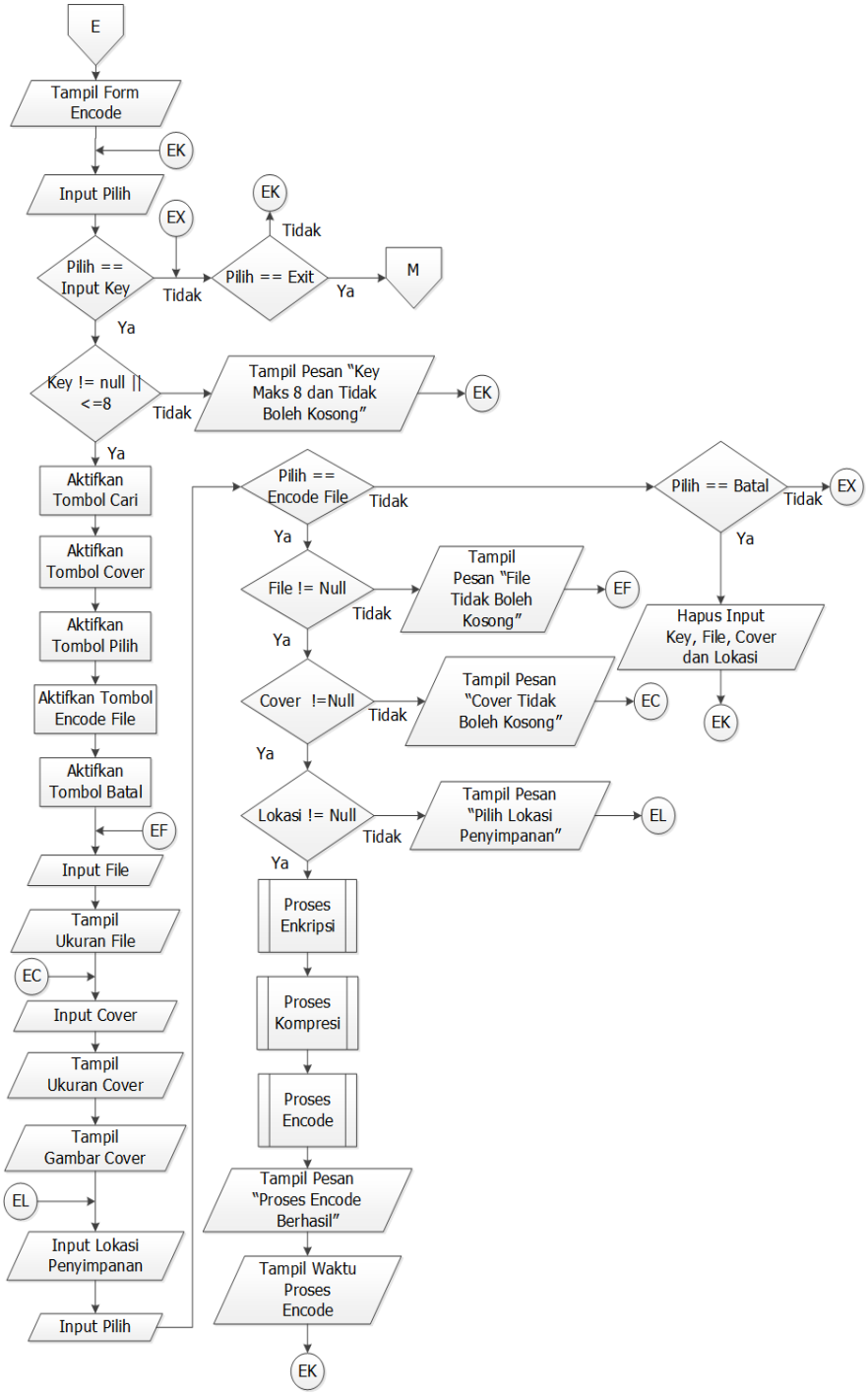
Gambar 1. Alur program encode aplikasi



Gambar 2. Alur program decode aplikasi

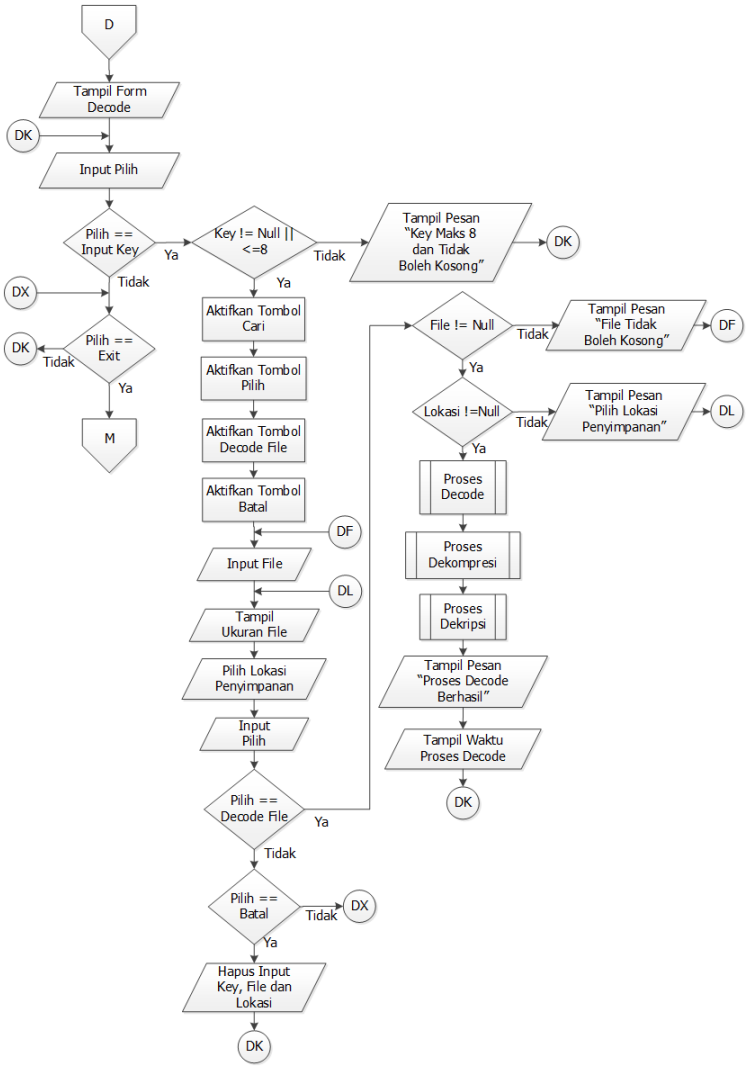
3.2. Flowchart

Flowchart form Encode menggambarkan alur proses yang ada pada *form Encode.* Pengguna memasukan *key* yang diinginkan minimal 1 karakter dan tidak boleh lebih dari 8 karakter. Selanjutnya pengguna memilih *file*, *cover* dan lokasi penyimpanan *file* hasil dari proses *encode*.



Gambar 3. Flowchart form encode

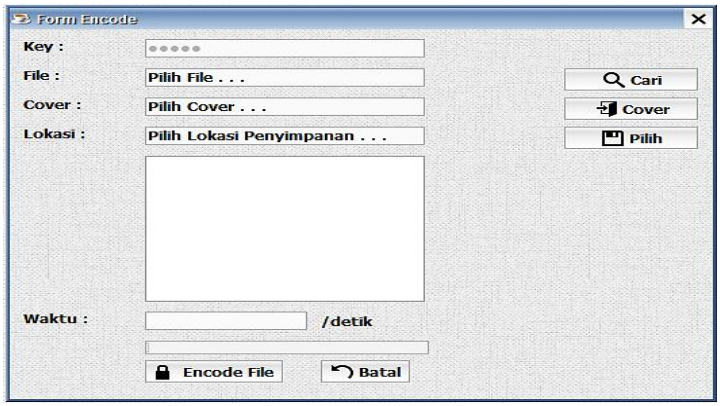
Flowchart form Decode menggambarkan alur proses yang ada pada *form Decode.* Pengguna memasukan *key* yang sesuai dengan kunci *encode.* Selanjutnya pengguna memilih *file* yang akan di *decode* dan lokasi penyimpanan *file* hasil *decode*



Gambar 4. Flowchart form decode

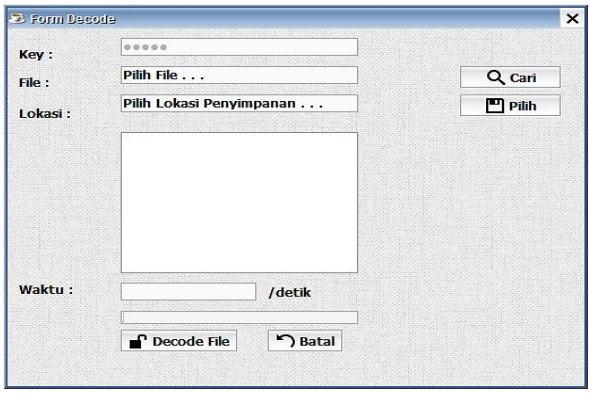
3.3. Tampilan Layar Program

Berikut ini adalah tampilan layar *form encode* yang digunakan untuk melakukan proses enkripsi, kompresi dan penyisipan ke dalam gambar.



Gambar 5. Tampilan layar form encode

Tampilan layar *form decode* ini digunakan untuk melakukan proses pengembalian dokumen digital yang sudah dilakukan proses pengamanan ke bentuk aslinya.



Gambar 6. Tampilan layar form decode

3.4. Hasil Tabel Pengujian

Untuk mengetahui hasil yang telah dicapai dari aplikasi keamanan yang dibuat dalam penelitian ini perlu dilakukan proses pengujian aplikasi. Berikut ini adalah tabel pengujian yang dilakukan pada proses *encode* dan *decode*.

Tabel 1. Uji coba proses encode

Nama *file*	Ukuran *file*	Nama *cover*	Ukuran *cover*	Ukuran *output*	Waktu (detik)
Surat Penawaran.docx	13 KB	UBL Logo.png	373 KB	392 KB	1.856
Surat Perintah Kerja.doc	46 KB	KP Logo.png	105 KB	168 KB	18.565

Tabel 2. Uji coba proses decode

Nama file	Ukuran input	Ukuran output	Waktu (detik)
Encode_UBL Logo.png	391 KB	14 KB	1.545
Encode_KP Logo.png	167 KB	46 KB	9.017

3.5. Evaluasi Program

3.5.1 Kelebihan Program

(1) Keamanan aplikasi terjaga karena menggunakan proses *login* untuk satu admin pada saat awal menggunakan aplikasi sehingga hanya admin yang bisa mengakses aplikasi.
(2) Terjaganya keamanan file asli karena pada proses encode akan menghasilkan file baru.
(3) Terdapat validasi pada saat memilih file yang akan diamankan dan gambar yang digunakan sebagai cover yaitu dibatasi file dengan ekstensi .docx, .doc dan cover dengan ekstensi .jpg dan .png.
(4) Terdapat validasi untuk file yang sudah dilakukan proses encode dan decode sehingga tidak terjadi proses encode dan decode berulang kali pada file yang sama.
(5) Apabila kunci yang dimasukan salah pada proses decode maka muncul peringatan sehingga pengguna tidak menunggu lama dan file *decode* rusak.

3.5.2 Kekurangan Program

(1) Aplikasi hanya bisa melakukan proses *encode file* dengan ekstensi .docx dan .doc dan *cover* dengan ekstensi .png dan .jpg.
(2) Apabila ukuran *file* lebih besar maka waktu proses *encode* yang dibutuhkan semakin lama.
(3) Fitur dalam aplikasi ini masih banyak yang dapat dikembangkan seperti dapat ditambahkan proses pendaftaran untuk *user* jika ingin mengakses aplikasi, admin bisa menghapus *user* yang sudah tidak digunakan dan admin bisa melihat aktifitas *user* seperti dokumen apa saja yang diamankan oleh *user*.

4. KESIMPULAN

Berdasarkan permasalahan, analisis program, dan uji coba yang telah dilakukan maka didapat kesimpulan sebagai berikut:

(1) Algoritma kriptografi AES-128, kompresi Huffman dan steganaografi EOF dapat digunakan dengan baik pada aplikasi pengamanan dokumen digital.
(2) Proses pengembalian dokumen digital yang sudah dilakukan pengamanan dilakukan dengan baik ke bentuk *file* aslinya.
(3) Dengan dilakukan kompresi setelah melakukan enkripsi waktu proses yang dibutuhkan untuk melakukan penyisipan kedalam gambar menjadi lebih sedikit.
(4) Waktu proses pengamanan dan pengembalian dokumen digital sesuai dengan ukuran *file* dokumen digital tersebut, dengan ukuran yang lebih kecil maka waktu yang dibutuhkan menjadi lebih sedikit.

Untuk pengembangan lebih lanjut mengenai aplikasi pengamanan dokumen digital adapun saran yang diberikan antara lain:

(1) Aplikasi pengamanan ini diharapkan dapat melakukan proses enkripsi, kompresi dan *encode* dengan format dokumen digital lebih banyak lagi seperti (*.ppt, *.xlsx, *.pdf, dll) dan *cover* (*.gif, *.mp3, *.mp4, dll).
(2) Waktu proses pengamanan dan pengembalian dokumen digital dengan rata-rata berukuran besar dapat berjalan lebih cepat dengan *hardware* yang lebih baik.
(3) Diharapkan *file* hasil enkripsi menjadi lebih kecil dengan menerapkan algoritma kompresi tambahan supaya proses *encode* menjadi lebih cepat

UCAPAN TERIMA KASIH

Penulis juga berterima kasih kepada Universitas Budi Luhur yang telah memberikan dukungannya selama ini baik berupa dukungan materil maupun dukungan moril sehingga makalah ini dapat diselesaikan dengan baik. Tidak lupa pula penulis berterima kasih kepada Universitas Muria Kudus yang telah memberi kesempatan kepada penulis untuk dapat berpartisipasi dalam Seminar Nasional Teknologi dan Informatika (SNATIF) tahun 2017 ini. Semoga Universitas Budi Luhur dan Universitas Muria Kudus dapat terus menjadi perguruan tinggi yang unggul di bidangnya.

DAFTAR PUSTAKA

Anggraini, Y. & Sakti, D.V.S., (2014) Penerapan Steganografi Metode End Of File (EOF) Dan Enkripsi Metode Data Encryption Standard (DES) Pada Aplikasi Pengamanan Data Gambar Berbasis Java Programming. *konferensi Nasional Sistem Informasi 2014*, Hal. 1743–1753. ISSN: 2355-1941.

Ariyus, D., (2008), *Pengantar Ilmu Kriptografi*, Yogyakarta: ANDI.

Martono & Irawan, (2013), Penggunaan Steganografi dengan Metode End of File (Eof) pada Digital Watermarking. *Jurnal TICOM*, 2(1), Hal. 229–235. ISSN: 2302-3252.

Musril, H.A., (2012), Studi Komparasi Metode Arithmetic Coding Dan Huffman Coding Dalam Algoritma Entropy Untuk Kompresi Citra Digital. *Jurnal Teknologi Informasi & Pendidikan*, 5(2), Hal. 133–156. ISSN: 2086-4981.

Ophie, E., (2014), Optimasi Enkripsi Teks Menggunakan AES dengan Algoritma Kompresi Huffman. *Makalah IF3020 Kriftografi - Sem. II.*

Winarno, A., Cahyanto, E.T.B. & Mulyadi, (2012), Polynomial Functions Dan Implementasinya Dalam Algoritma Advanced Encryption Standard Pada Database Accounting. *PROSIDING*, (November), Hal. 32–44. ISBN: 987-979-16353-8-7.