PENYEMBUNYIAN FILE TERENKRIPSI DENGAN KRIPTOGRAFI AES DI DALAM STEGANOGRAFI *END OF FILE*

Diajukan Untuk Menyusun Skripsi
di Jurusan Teknik Informatika Fakultas Ilmu Komputer UNSRI

Oleh:

Jessica Julia Paradina Siregar
NIM: 09021281722032

JURUSAN TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2021

LEMBAR PENGESAHAN TUGAS AKHIR

PENYEMBUNYIAN FILE TERENKRIPSI DENGAN KRIPTOGRAFI AES DI DALAM STEGANOGRAFI *END OF FILE*

Oleh :

Jessica Julia Paradina Siregar
NIM : 09021281722032

Palembang, 26 Agustus 2021

Pembimbing I	Pembimbing II
Julian Supardi, M.T.	Kanda Januar Miraswan, M.T.
NIP. 197207102010121001	NIP. 199001092019031012

Mengetahui,
Ketua Jurusan Teknik Informatika,

Alvi Syahrini Utami, M.Kom.
NIP 197812222006042003

TANDA LULUS UJIAN SIDANG TUGAS AKHIR

Pada hari Selasa tanggal 3 Agustus 2021 telah dilaksanakan ujian sidang tugas akhir oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama	:	Jessica Julia Paradina Siregar
NIM	:	09021281722032
Judul	:	Penyembunyian File Terenkripsi dengan Kriptografi AES di dalam Steganografi End of File

1 Pembimbing I

Julian Supardi, M.T.
NIP. 197207102010121001

2. Pembimbing II

Kanda Januar Miraswan, M.T.
NIP 199001092019031012

3. Penguji I

Dr. Abdiansah, S.Kom., M.Cs.
NIP 198410012009121005

4. Penguji II

Mastura Diana Marieska, M.T.
NIP. 198603212018032001

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	: Jessica Julia Paradina Siregar
NIM	: 09021281722032
Program Studi	: Teknik Informatika Bilingual
Judul Skripsi	: Penyembunyian File Terenkripsi dengan Kriptografi AES di dalam Steganografi *End of File*

Hasil Pengecekan Software *iThenticate/Turnitin* : **12%**

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan projek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, Agustus 2021

Jessica Julia Paradina Siregar
NIM. 09021381722142

MOTTO DAN PERSEMBAHAN

“God gives every bird its food, but does not throw it into the nest”

-Josiah G. Holland-

“I feel like that possibility of all those possibilities being possible is just another possibility that can possibly happen”

-Mark Lee-

Ku persembahkan karya tulis ini kepada:

- Kedua orangtua dan keluargaku
- Sahabat dan Teman Seperjuanganku
- Fakultas Ilmu Komputer
- Universitas Sriwijaya

Concealment of Encrypted Files with AES Cryptography using End of File Steganography

By :

Jessica Julia Paradina Siregar
NIM : 09021281722032

ABSTRACT

Sending data and messages through various media is a common activity. However, the leak and piracy of information can be a high risk. To protect the security of messages, this study uses the combination of AES cryptographic and End of File steganography methods. This study focuses on embedding a secret message in the form of text into an image in PNG format using End of File steganography method. Before embedding, the message is encrypted using AES cryptography method. In this study, 6 images with different resolutions are tested and in each image 15 words are embedded with ASCII characters encrypted. The quality of the embedded image is measured by PSNR and SSIM values. Based on the PSNR and SSIM values of the tested images, it can be concluded that the end of file steganography technique is considered suitable for embedding secret messages. Based on the time required for the embedding process, the average time is between 0.5 and 0.7 seconds and the average computation time resulting from the testing process is relatively stable at 0.59 seconds. Therefore, it can be concluded that the time required for embedding the message tends to be short and stable.

Keywords : Steganography, Cryptography, End of File, AES, PSNR, SSIM

Penyembunyian File Terenkripsi dengan Kriptografi AES di dalam Steganografi End of File

Oleh :

Jessica Julia Paradina Siregar
NIM : 09021281722032

ABSTRAK

Pengiriman data dan pesan melalui berbagai macam media merupakan hal yang lumrah dilakukan dan resiko terjadinya kebocoran informasi dan pembajakan sangat besar. Untuk itu, dilakukan penggabungan dari teknik kriptografi AES dan steganografi *End of File* untuk melindungi keamanan pesan pada penelitian ini. Penelitian ini berfokus pada penyisipan pesan rahasia berupa teks ke dalam citra dengan format PNG menggunakan metode steganografi *End of File*. Sebelum dilakukan penyisipan, pesan akan dienkripsi terlebih dahulu menggunakan metode kriptografi AES. Terdapat 6 citra dengan resolusi berbeda yang akan diujikan pada penelitian ini. Pada tiap citra dilakukan penyisipan berisi 15 kata dengan karakter ASCII yang telah dienkripsi. Kualitas pada citra hasil penyisipan diukur berdasarkan nilai PSNR dan nilai SSIM. Berdasarkan pengujian nilai PSNR dan nilai SSIM dari citra yang diujikan, dapat disimpulkan bahwa teknik steganografi *End of File* dinilai baik dalam penyisipan pesan rahasia. Berdasarkan pengujian waktu, rata-rata rentan waktu yang dibutuhkan dalam proses penyisipan yaitu antara 0.5 detik sampai 0.7 detik dan rata-rata waktu komputasi yang dihasilkan dari proses pengujian adalah 0.59 detik. Sehingga, dapat disimpulkan bahwa waktu yang dibutuhkan dalam penyisipan pesan cenderung singkat dan stabil.

Kata Kunci : Steganografi, Kriptografi, *End of File*, AES, PSNR, SSIM

KATA PENGANTAR

Penulis ucapkan puji syukur kepada Allah atas berkat dan rahmat-Nya yang telah diberikan kepada Penulis sehingga dapat menyelesaikan Tugas Akhir dengan judul "**Penyembunyian File Terenkripsi dengan Kriptografi AES di dalam Steganografi *End of File***" dengan baik untuk memenuhi salah satu syarat guna menyelesaikan pendidikan program Strata-1 pada Fakultas Ilmu Komputer Program Studi Teknik Informatika di Universitas Sriwijaya.

Pada kesempatan ini, penulis ingin mengucapkan terimakasih kepada pihak-pihak yang telah berperan memberikan bantuan dan dukungan baik secara langsung maupun secara tidak langsung dalam menyelesaikan tugas akhir ini.
Penulis ingin menyampaikan rasa terima kasih kepada:

1. Kedua orang tuaku, Panorangan Siregar dan Sumiati yang selalu mendokan serta memberikan dukungan baik moril maupun materil.
2. Bapak Jaidan Jauhari, M.T selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya beserta jajarannya. Ibu Alvi Syahrini Utami, M.Kom. selaku Ketua Jurusan Teknik Informatika beserta jajarannya, dan Ibu Mastura Diana Marieska, M.T. selaku Sekretaris Jurusan Teknik Informatika.
3. Bapak Julian Supardi, M.T. selaku dosen pembimbing I dan Bapak Kanda Januar Miraswan, M.T. selaku pembimbing II yang telah membimbing, mengarahkan, dan memberikan motivasi penulis dalam proses perkuliahan dan pengerjaan Tugas Akhir.
4. Bapak Drs. Megah Mulya, M.T. (Alm) selaku dosen pembimbing saya yang telah membimbing dan mengarahkan saya sehingga saya dapat mengawali tugas akhir saya dengan baik.
5. Bapak Samsuryadi, M.Kom, Ph.D. selaku dosen pembimbing akademik yang telah membimbing, mengarahkan dan memberikan motivasi penulis dalam proses perkuliahan.
6. Bapak Dr. Abdiansah, S.Kom., M.Cs. selaku dosen penguji I, dan Ibu Mastura Diana Marieska, M.T. selaku dosen penguji II yang telah memberikan saran dan masukan dalam pengerjaan Tugas Akhir saya sehingga dapat menjadi lebih baik.

7. Seluruh dosen Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
8. Mbak Wiwin, selaku staff administrasi Teknik Informatika Bilingual, dan seluruh staff Fakultas Ilmu Komputer Universitas Sriwijaya yang telah membantu dalam kelancaran proses administrasi dan akademik selama masa perkuliahan.
9. Suci Putri, Ridha Ayu, dan Ahmad Emir yang selalu memberikan support dari awal hingga akhir dan dalam keadaan apapun. Teman-teman jurusan Teknik Informatika yang telah membantu selama masa perkuliahan, maaf tidak dapat disebutkan satu persatu.
10. Abang Reza, Kak Chintya, dan Adik Andre yang selalu memberikan semangat, saran kiat-kiat mengerjakan skripsi, dan menghibur. Terutama untuk Andre si kecil yang sudah besar, *makasih* ya Andre dengan Andre yang tenang *gak ngapa-ngapain* itu *udah* bantu kakak *banget*!
11. Dreamies yang sudah menemani dari awal hingga akhir masa perkuliahan.
12. Seluruh pihak yang telah membantu dalam penyusunan dan penyempurnaan tugas akhir ini yang tidak dapat disebutkan satu persatu.

Penulis menyadari dalam penyusunan Tugas Akhir ini masih terdapat banyak kekurangan disebabkan keterbatasan pengetahuan dan pengalaman, oleh karena itu kritik dan saran yang membangun sangat diharapkan untuk kemajuan penelitian selanjutnya. Akhir kata semoga Tugas Akhir ini dapat berguna dan bermanfaat bagi kita semua.

Palembang, Agustus 2021

Jessica Julia Paradina Siregar

DAFTAR ISI

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

BAB I

PENDAHULUAN

1.1 Pendahuluan

Bab I menguraikan tentang latar belakang diangkatnya topik mengenai "Penyembunyian File Terenkripsi dengan Kriptografi AES di dalam Steganografi *End of File*" sebagai bahan penelitian. Pada bab ini juga tercakup tujuan penelitian, manfaat penelitian yang akan dilaksanakan, serta batasan masalah dari penelitian yang akan dilaksanakan.

1.2 Latar Belakang

Pada era digital ini pengiriman data dan pesan melalui berbagai macam media merupakan hal yang lumrah dilakukan. Namun, resiko terjadinya kebocoran informasi dan pembajakan oleh pihak yang tidak bertanggung jawab sangat besar. Oleh karena itu, untuk menjamin kerahasiaan dari informasi yang akan dikirimkan, informasi tersebut harus dilindungi. Salah satu cara untuk melindungi informasi tersebut adalah dengan menggunakan teknik kriptografi dan steganografi.

Kriptografi merupakan ilmu mengenai teknik pengamanan dalam komunikasi diantara dua pihak. Algoritma *Advanced Encryption Standard (*AES) adalah suatu algoritma *block cipher* dan mempunyai sifat simetri yang menggunakan kunci simetri pada waktu proses enkripsi dan dekripsi. Algoritma AES merupakan algoritma kriptografi yang dapat mengenkripsi dan dekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit.

Algoritma kriptografi AES merupakan salah satu algoritma kriptografi yang memiliki tingkat keamanan yang baik (Prameshwari & Sastra, 2018).

Perkembangan steganografi menjadi alternatif pengamanan dalam komunikasi data dalam jaringan internet. Berbeda dengan teknik kriptografi yang menyamarkan pesan dengan mengubah pesan tersebut menjadi tidak dapat dibaca, pada teknik steganografi pesan disamarkan dengan cara disembunyikan pada media penampung. Steganografi *End of File* adalah salah satu metode yang digunakan dalam penyembunyian pesan rahasia. Metode ini juga dikenal sebagai metode algortima injeksi dikarenakan metode steganografi ini melakukan penyisipan pesan pada bagian akhir dari media penampung. Media yang digunakan sebagai media penampung juga tidak mengalami perubahan kualitas sehingga pesan yang disembunyikan tidak akan diketahui (Jannah et al., 2018).

Berdasarkan penelitian yang telah dilakukan, Kriptografi AES dapat menjaga kerahasiaan pesan dan Steganografi metode EOF dapat mempertahankan kualitas dari media penampungnya. Pada penelitian ini akan dilakukan penggabungan kedua metode pada proses enkripsi dan dekripsi data *file* menggunakan algoritma kriptografi *Advanced Encryption Standard* (AES) dan penyisipan *file* yang telah terenkripsi menggunakan steganografi metode *End of File* (EOF) untuk menyisipkan *file* pada citra digital.

1.3 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, fokus permasalahan adalah sebagai berikut :

1. Bagaimana melakukan pengamanan pada pesan rahasia dengan menggunakan penggabungan dari metode kriptografi AES dan steganografi *End of File*.
2. Menganalisa kualitas dari citra setelah setelah disisipkan teks terenkripsi dengan citra asli.
3. Berapa lama waktu yang dibutuhkan oleh perangkat lunak pada setiap proses penyisipan pesan rahasia pada citra digital.

1.4 Tujuan Penelitian

Adapun tujuan penelitian adalah sebagai berikut :

1. Mengembangkan perangkat lunak menggunakan kombinasi metode Kriptografi AES dan metode Steganografi *End of File* (EOF) dalam mengamankan pesan rahasia.
2. Menghitung nilai kualitas citra dengan cara membandingan citra asli dari citra penampung yang digunakan dan citra stego yang akan dihasilkan berdasarkan dari perhitungan nilai *Peak Signal to Noise Ratio* (PSNR) dan nilai *Structural Similarity Index Metrics* (SSIM).
3. Melakukan pengukuran waktu komputasi yang dibutuhkan oleh perangkat lunak dalam melakukan proses penyisipan pesan rahasia ke dalam citra penampung.

1.5 Manfaat Penelitian

Penelitian yang dilakukan memiliki manfaat sebagai berikut :

1. Dihasilkannya perangkat lunak yang mampu mengimplementasikan penggabungan dari metode kriptografi AES dan steganografi *End of File*.
2. Mengetahui kualitas dari citra dan keamanan yang dihasilkan dari penggabungan antara algoritma kriptografi AES dan algoritma steganografi *End of File* dalam pengamanan pesan rahasia.
3. Dapat digunakan untuk menjaga kerahasiaan dari pesan yang ingin dikirimkan dengan menggunakan penggabungan metode kriptografi AES dan steganografi *End of File*.
4. Menjadi referensi dalam penelitian selanjutnya pada metode steganografi *End of File*.

1.6 Batasan Masalah

Beberapa poin dari batasan masalah yang ditetapkan pada penelitian ini adalah :

1. Pada metode kriptografi AES yang diterapkan, ukuran blok yang akan digunakan adalah ukuran 128 bit dan ukuran kunci yang akan digunakan adalah kunci dengan 24 karakter untuk *base64* dan 32 karakter untuk *hexadecimal*.
2. Masukan yang digunakan untuk penyisipan adalah pesan teks yang telah dienkripsi menggunakan algoritma kriptografi AES.

3. Citra yang digunakan sebagai citra penampung adalah citra digital berwarna dengan format PNG dan resolusi yang bervariasi, yaitu citra dengan resolusi 256 x 256, 512 x 512, 600 x 375, 480 x 361, 522 x 340, dan 700 x 467.

1.7 Sistematika Penulisan

Pada penelitian ini sistematika penulisan akan disusun menjadi beberapa bagian, yaitu :

BAB I. PENDAHULUAN

Pada bab 1 dijabarkan tentang latar belakang dari penulisan penelitian, rumusan masalah penelitian, tujuan penelitian, manfaat dari penelitian, dan sistematika penulisan dari penelitian.

BAB II. KAJIAN LITERATUR

Bab 2 akan menguraikan tentang landasan teori yang dijadikan acuan dalam penelitian yang dilakukan. Landasan teori ini meliputi penjelasan mengenai kriptografi AES, steganografi *End of File*, *Mean Square Error* (MSE), *Peak Signal to Noise Ratio* (PSNR), *Structural Similarity Index Metric* (SSIM), dan citra digital.

BAB III. METODOLOGI PENELITIAN

Bab 3 memaparkan tentang tahapan-tahapan yang akan dilaksanakan pada proses penelitian. Tahapan-tahapan perencanaan penelitian akan didetailkan menggunakan acuan kerangka kerja dan manajemen proyek penelitian akan dilampirkan pada bagian akhir dari bab.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Bab 4 menguraikan setiap tahapan yang akan dilakukan pada proses pengembangan lunak untuk melakukan pengamana pesan teks menggunakan metode kriptografi AES dan steganografi *End of File* berdasarkan metode *Rational Unified Process* (RUP).

BAB V. HASIL DAN ANALISIS PENELITIAN

Bab 5 memaparkan hasil dari pengujian dan menganalisis hasil dari pengujian yang telah dilakukan.

BAB VI. KESIMPULAN DAN SARAN

Bab 6 memaparkan tentang hasil kesimpulan dari penelitian yang telah dilakukan serta memberikan saran dengan tujuan untuk meningkatkan hasil pada penelitian selanjutnya dari penggunaan metode kriptografi AES dan steganografi *End of File*.

1.8 Kesimpulan

Permasalahan yang akan diselesaikan pada penelitian ini adalah melakukan pengembangan perangkat lunak dengan penggabungan metode kriptografi AES dan steganografi EOF, menganalisa kualitas dan performansi dari penggabungan teknik kriptografi AES dan steganografi EOF dalam pengamanan pesan rahasia dengan menghitung hasil nilai *Peak Noise to Ratio* (PSNR) dan *Structural Similarity Index Metrics* (SSIM) dari citra yang dihasilkan dan menghitung waktu yang digunakan dalam proses penyisipan pesan ke dalam citra penampung.

DAFTAR PUSTAKA

Aditya, S., & Jawa Bendi, K. (2012). Implementasi Algoritma Rijndael untuk Enkripsi dan Deskripsi Pada Citra Digital. *Seminar Nasional Aplikasi Teknologi Informasi 2012*, *2012*(Snati), 15–16.

Anwar, S., Komputer, M. I., & Luhur, U. B. (2017). *Implementasi Pengamanan Data Dan Informasi Dengan Metode Steganografi LSB dan Algoritma Kriptografi AES*. 37–42.

Bhaudhayana, G., & Widiartha, I. (2015). Implementasi Algoritma Kriptografi Aes 256 Dan Metode Steganografi Lsb Pada Gambar Bitmap. *Jurnal Ilmu Komputer*, *8*(2), 15–25.

Darwis, D., & Kisworo, K. (2017). Teknik Steganografi untuk Penyembunyian Pesan Teks Menggunakan Algoritma End Of File. *Explore: Jurnal Sistem Informasi Dan Telematika*, *8*(2). https://doi.org/10.36448/jsit.v8i2.950

Geta Putri, G., Styorini, W., & Dian Rahayani, R. (2015). Ethos (Jurnal Penelitian dan Pengabdian Masyarakat): 197-207 Analisis Kriptografi Simetris AES dan Kriptografi Asimetris RSA Pada Enkripsi Citra Digital. *Ethos (Jurnal Penelitian Dan Pengabdian Masyarakat)*, *3*(8), 197–207.

Horé, A., & Ziou, D. (2010). Image quality metrics: PSNR vs. SSIM. *Proceedings - International Conference on Pattern Recognition*, 2366–2369. https://doi.org/10.1109/ICPR.2010.579

Irawan, M. (2013). Penggunaan Steganografi dengan Metode End of File (EOF) pada Digital Watermarking. *Jurnal Teknologi Informasi Komputer*, *2*(1), 36–42.

Jannah, L. M., Santoso, I., & Christyono, Y. (2018). Kinerja Steganografi Metode End of File Pada Data Citra Digital. *Transient*, *7*(1), 34. https://doi.org/10.14710/transient.7.1.34-39

Kroll, P. & Kruchten, P. 2003. The Rational Unified Process Made Easy. Rational Unified Process Made Easy: A Practitioner's Guide to the RUP.

Lubis, A. A., Wong, N. P., Arfiandi, I., Damanik, V. I., & Maulana, A. (2015). Steganografi pada Citra dengan Metode MLSB dan Enkripsi Triple Transposition Vigenere Cipher. *Steganografi Pada Citra Dengan Metode MLSB Dan Enkripsi Triple Transposition Vigenere Cipher*, *16*(2), 125–134.

Minarni, M., & Fernando, A. G. (2020). IMPLEMENTASI ALGORITMA END OF FILE (EoF) PADA STEGANOGRAFI CITRA. *Jurnal TeknoIf*, *8*(1), 25. https://doi.org/10.21063/jtif.2020.v8.1.25-31

Muhamad Abdullah, A. (2017). *Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data Call for papers View project Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data View project Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt*. *June*. https://www.researchgate.net/publication/317615794

Munir, R. (2008). Pengantar Ilmu Kriptografi. *Penerbit Andi*, 1–16. http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Pengantar+Kriptografi#0

Novianto, D., & Setiawan, Y. (2018). Aplikasi Pengamanan Informasi Menggunakan Metode Least Significant Bit (Lsb) dan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Ilmiah Informatika Global*, *09*(2), 83–89.

Nurfitri, K., Suyanto, M., & . S. (2017). Penilaian Kualitas Pemampatan Citra Pada Aplikasi-Aplikasi Instant Messenger. *Multitek Indonesia*, *10*(2), 78. https://doi.org/10.24269/mtkind.v10i2.346

Prameshwari, A., & Sastra, N. P. (2018). Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen. *Eksplora Informatika*, *8*(1), 52. https://doi.org/10.30864/eksplora.v8i1.139

Sara, U., Akter, M., & Uddin, M. S. (2019). Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study. *Journal of Computer and Communications*, *07*(03), 8–18. https://doi.org/10.4236/jcc.2019.73002

Wang, Z., Bovik, A., & Sheikh, H. (2005). *Structural Similarity Based Image Quality Assessment*. *November 2017*, 225–241. https://doi.org/10.1201/9781420027822.ch7

Zebua, T. (2018). *Analisa Perbandingan Least Significant Bit dan End of File Untuk Steganografi Citra Digital Menggunakan Matlab*. *November 2016*. https://doi.org/10.31227/osf.io/dah2c