PENGAMANAN DAN PENYEMBUNYIAN PESAN PADA AREA TEPI DARI CITRA DIGITAL MENGGUNAKAN METODE LEAST SIGNIFICANT BIT DAN ALGORITMA BLOWFISH

Diajukan Sebagai Syarat untuk Menyelesaikan
Pendidikan Program Strata-1 pada
Jurusan Teknik Informatika

Oleh:

Arviansyah Nur
NIM : 09021281722033

Jurusan Teknik Informatika
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2023

LEMBAR PENGESAHAN SKRIPSI

PENGAMANAN DAN PENYEMBUNYIAN PESAN PADA AREA TEPI DARI CITRA DIGITAL MENGGUNAKAN METODE LEAST SIGNIFICANT BIT DAN ALGORITMA BLOWFISH

Oleh:

Arviansyah Nur
NIM: 09021281722033

Palembang, 3 Agustus 2023

Pembimbing I

Julian Supardi, M.T., Ph.D.
NIP. 197207102010121001

Pembimbing II,

M. Naufal Rachmatullah, S.Kom., M.T.
NIP. 199212012022031008

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

TANDA LULUS UJIAN SIDANG SKRIPSI

Pada hari Jum'at, 28 Juli 2023 telah dilaksanakan ujian sidang skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Arviansyah Nur

NIM : 09021281722033

Judul : Pengamanan dan Penyembunyian Pesan Pada Area Tepi Dari Citra Digital Menggunakan Metode Least Significant Bit dan Algoritma Blowfish

dan dinyatakan lulus

1. Ketua Penguji
Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003 .....

2. Penguji I
Syamsuryadi, M.Kom., Ph.D.
NIP. 197102041997021003 .....

3. Pembimbing I
Julian Supardi, M.T., Ph.D.
NIP. 197207102010121001 .....

4. Pembimbing II
M. Naufal Rachmatullah, S.Kom., M.T.
NIP. 199212012022031008 .....

Mengetahui
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

HALAMAN PERNYATAAN

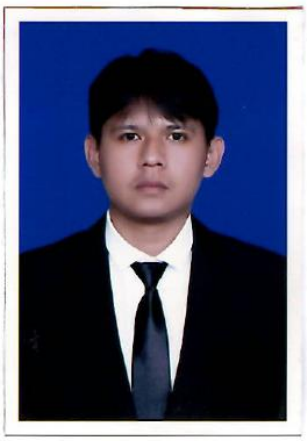
Yang bertanda tangan di bawah ini:

Nama	: Arviansyah Nur
NIM	: 09021281722033
Program Studi	: Teknik Informatika
Judul	: Pengamanan dan Penyembunyian Pesan Pada Area Tepi Dari Citra Digital Menggunakan Metode Least Significant Bit dan Algoritma Blowfish

Hasil pengecekan software ithenticate/Turnitin : 19%

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

Demikian pernyataan ini saya buat dengan sebenar-benarnya dan tidak ada paksaan dari pihak manapun.



Palembang, Agustus 2023

Arviansyah Nur
NIM. 09021281722033

MOTO DAN PERSEMBAHAN

"*Demi kemuliaan*"

Kupersembahkan karya tulisan ini kepada:

- Kedua orang tuaku
- Saudaraku
- Sahabatku
- Almamamterku

PENGAMANAN DAN PENYEMBUNYIAN PESAN PADA AREA TEPI DARI CITRA DIGITAL MENGGUNAKAN METODE LEAST SIGNIFICANT BIT DAN ALGORITMA BLOWFISH

Oleh:

Arviansyah Nur (09021281722033)

Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email: arviansyahnur3@gmail.com

ABSTRAK

Proses kriptografi menghasilkan tulisan acak yang dapat mengaburkan pesan sehingga sulit dibaca oleh orang lain. Akan tetapi, kriptografi sendiri masih terlalu lemah untuk mengamankan pesan sehingga diperlukan steganografi untuk menyamarkan keberadaan pesan tersebut agar tidak terlihat oleh mata manusia. Selain menyembunyikan pesan, tujuan lainnya adalah mengetahui dampak dari penyisipan pesan. Pada proses enkripsi dan dekripsi pesan menggunakan algoritma *blowfish,* proses penyisipan menggunakan steganografi *Least Significant Bit*, dan proses pendeteksian tepi menggunakan algoritma *canny*. Dari penelitian yang dilakukan dengan kombinasi kriptografi dan steganografi, diperoleh citra yang sangat baik dengan nilai PSNR sebesar 76.6932 dan MSE sebesar 0.0013 untuk panjang pesan sebesar 64 *bytes*. Sedangkan untuk tampilan secara kasat mata menunjukkan hasil yang relatif mirip antara *host image* dan *stego image*.

Kata kunci: kriptografi, Blowfish, edge detection, Canny, steganografi, Least Significant Bit (LSB),

SECURING AND HIDING MESSAGES IN THE EDGE AREA OF DIGITAL IMAGES USING THE LEAST SIGNIFICANT BIT METHOD AND BLOWFISH ALGORITHM

By:

Arviansyah Nur (09021281722033)

Informatics Engineering, Faculty of Computer Science, Sriwijaya University

Email: arviansyahnur3@gmail.com

ABSTRACT

The process of cryptography produces random text that can obscure a message, making it difficult for others to read. However, cryptography itself is still not strong enough to secure the message, so steganography is needed to conceal the existence of the message from the human eye. Besides hiding the message, another objective is to assess the impact of message embedding. In the process of encrypting and decrypting the message, the Blowfish algorithm is used, while message embedding utilizes the Least Significant Bit steganography, and edge detection is performed using the Canny algorithm. Through research conducted with the combination of cryptography and steganography, an excellent image is obtained with a PSNR value of 76.6932 and MSE of 0.0013 for a message length of 64 bytes. Meanwhile, visually, the results show a relatively similar appearance between the host image and the stego image.

Keywords: cryptography, Blowfish, edge detection, Canny, steganography, Least Significant Bit (LSB)

KATA PENGANTAR

Pujian syukur kepada Allah SWT atas berkat dan rahmat-Nya yang telah diberikan kepada Penulis sehingga dapat menyelesaikan Tugas Akhir ini dengan baik. Tugas Akhir ini disusun untuk memenuhi salah satu syarat guna menyelesaikan pendidikan program Strata-1 pada Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Dalam menyelesaikan Tugas Akhir ini banyak pihak yang telah memberikan bantuan dan dukungan baik secara langsung maupun secara tidak langsung. Penulis ingin menyampaikan rasa terima kasih ini kepada:

1. Kedua orang tua saya yang telah setia dan sabar menunggu saya dalam menyelesaikan studi ini.
2. Ibu Alvi Syahrini Utami, M.Kom. Selaku ketua jurusan Teknik Informatika yang telah memberi kesempatan saya untuk mendapatkan tambahan waktu dalam mengerjakan penelitian ini.
3. Bapak Julian Supardi, M.T., Ph.D. dan Bapak M. Naufal Rachmatullah, S.Kom., M.T. yang telah membimbing saya dalam mengerjakan penelitian ini.
4. Bapak M. Qurhanul Rizqie, M.T., Ph.D. yang telah membimbing saya dari awal perkuliahan hingga saat ini.
5. Seluruh Bapak dan Ibu Dosen Teknik Informatika Universitas Sriwijaya.
6. Sahabat-sahabat saya yang senantiasa direpotkan dalam membantu penelitian ini.

7. Teman-teman kelas dan angkatan yang selalu berjuang bersama-sama dalam menuntut ilmu di perkuliahan.

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 2023

Arviansyah Nur

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

BAB I

PENDAHULUAN

1.1 Pendahuluan

Pada bab ini dibahas mengenai latar belakang, rumusan masalah, dan tujuan peneltian. Bab ini memberikan penjelasan umum mengenai keseluruhan penelitian.

1.2 Latar Belakang

Keamanan data merupakan suatu hal yang penting dan dibutuhkan oleh kebanyakan orang terutama untuk pesan yang bersifat *privacy.* Sampai saat ini kebutuhan akan internet telah menjadi bagian dari kebutuhan primer bagi beberapa orang. Berkomunikasi dan mengirimkan pesan melalui media sosial merupakan salah satu dari penggunaan internet itu sendiri. Banyaknya pengguna internet yang melakukan pertukaran informasi baik itu informasi biasa ataupun penting mengakibatkan tak sedikitnya pihak luar yang menginginkan informasi tersebut, sehingga membuat informasi tersebut rentan akan serangan-serangan oleh pihak luar. Oleh karena itu, dibutuhkan suatu mekanisme sistem keamanan yang dapat menangani kerahasiaan sebuah data.

Pada saat ini teknik pengamanan data dengan kriptografi masih dirasa kurang dikarenakan masih menimbulkan kecurigaan karena pesan yang disamarkan dapat dengan mudah dikenali (Hariady *et al.,* 2016). Adapun cara yang dapat dilakukan untuk meningkatkan keamanan suatu data setelah proses enkripsi dengan steganografi, yaitu menyembunyikan data tersebut ke dalam

suatu data yang lain sehingga tidak menimbulkan kecurigaan pada pihak-pihak yang tidak berkepentingan.

Dalam penelitian ini, teknik yang digunakan didasarkan pada penelitian yang menjadi referensi utama dan terbukti efektif, yaitu melakukan proses enkripsi menggunakan algoritma *One Time Pad* (OTP) pada pesan yang disisipkan pada area tepi dari citra menggunakan metode *Least Significant Bit* (LSB). Analisis histogram bekerja dengan baik dan dengan dilakukannya pengkonversian pesan ke bentuk biner sebelum dilakukan pengenkripsian pesan dapat meminimalisir pihak yang tidak berwenang dalam mencuri pesan (Irawan *et al.,* 2017). Namun di sisi lain penelitian, pengenkripsian pesan menggunakan algoritma *One Time Pad* (OTP) menyebutkan bahwa pembangkitan kunci acak membutuhkan kerja berat pada sistem, membutuhkan *resource memory* yang lumayan banyak jika pesan yang dimiliki terlalu panjang, dan juga memiliki hasil pendeskripsian yang pecah atau melebur jika pesan yang dimiliki terlalu panjang (Harahap dan Khairina, 2017).

Penelitian tersebut menjadi dasar dari penelitian ini dimana digunakan algoritma *Blowfish* yang hanya membutuhkan *resource memory* sedikit pada data yang berukuran kecil maupun besar. *Edge detection* menggunakan algoritma *canny* dan dilanjutkan dengan menyisipkan *ciphertext* ke dalam tepi citra menggunakan *Least Significant Bit* (LSB).

1.3 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka penelitian yang dilakukan berupa enkripsi pesan menggunakan algoritma *blowfish,* pencarian tepi citra menggunakan algoritma *canny,* dan dilanjutkan dengan penanaman *ciphertext* pada area tepi dari citra menggunakan metode *Least Significant Bit* (LSB). Adapun rumusan masalah yang dibahas pada penelitian ini yaitu:

1. Bagaimana kualitas citra *stego* yang dihasilkan berdasarkan nilai *Mean Square Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR)?
2. Bagaimana pengaruh nilai *Mean Square Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR) pada variasi panjang pesan yang disisipkan ke dalam tepi citra *host image*?

1.4 Tujuan Penelitian

Tujuan pada penelitian ini adalah sebagai berikut:

1. Mengetahui kualitas citra *stego* yang dihasilkan berdasarkan nilai *Mean Square Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR).
2. Mengetahui pengaruh nilai *Mean Square Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR) pada variasi panjang pesan yang disisipkan ke dalam tepi *host image.*
3. Mengembangkan perangkat lunak untuk melakukan pengujian hasil dari penelitian.

1.5 Manfaat Penelitian

Manfaat pada penelitian ini sebagai berikut:

1. Memperoleh informasi mengenai kualitas citra *stego* yang dihasilkan dari perangkat lunak enkripsi dan dekripsi berdasarkan nilai *Mean Square Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR).
2. Memperoleh informasi mengenai pengaruh nilai *Mean Square Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR) pada variasi panjang pesan yang disisipkan ke dalam tepi *host image.*
3. Mempersulit individu yang tidak bertanggung jawab dalam mencuri informasi saat proses pengiriman pesan dari pengirim ke penerima, dengan menerapkan metode *Least Significant Bit* dan algoritma *Blowfish*.

1.6 Batasan Masalah

Batasan masalah yang diberikan dalam penelitian ini meliputi:

1. Data yang disisipkan dalam bentuk masukan teks*;*
2. Pesan yang disisipkan ke dalam citra di antaranya berukuran 64, 128, 256, 512, 1024 *bytes*;
3. *Host image* yang digunakan berupa citra berwarna dengan ukuran 512 x 512 piksel dengan format *.jpg;*
4. Panjang kunci enkripsi maksimal 56 karakter, dikarenakan *blowfish* hanya dapat menerima masukan kunci sebesar 448 bit*;*

1.7 Sistematika Penulisan

Sistematika penulisan tugas akhir ini mengikuti format penulisan standar yang telah ditetapkan oleh Fakultas Ilmu Komputer Universitas Sriwijaya, yang dapat dijelaskan sebagai berikut:

BAB I. PENDAHULUAN

Pada bab ini diuraikan mengenai latar belakang, perumusan masalah, tujuan dan manfaat penelitian, batasan masalah dan sistematika penulisan.

BAB II. KAJIAN LITERATUR

Pada bab ini membahas seluruh dasar-dasar teori yang digunakan mulai dari definisi sistem, informasi mengenai domain, dan semua yang digunakan pada tahapan analisis, perancangan, dan implementasi.

BAB III. METODELOGI PENELITIAN

Pada bab ini membahas mengenai tahap-tahap yang diterapkan pada penelitian. Setiap rencana dari tahapan penelitian dideskripsikan secara rinci berdasarkan kerangka kerja. Dilanjutkan dengan perancangan manajemen proyek dalam pelaksanaan penelitian.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Pada bab ini akan membahas mengenai analisis serta perancangan perangkat lunak. Dimulai dengan pengumpulan dan analisa kebutuhan, rancangan serta konstruksi perangkat lunak agar sesuai dengan kebutuhan dalam pengembangan perangkat lunak.

BAB V. PENGEMBANGAN PERANGKAT LUNAK

Pada bab ini menyajikan hasil pengujian berdasarkan rancangan sebelumnya beserta tabel hasil pengujian yang sudah dianalisis dan diuaraikan.

BAB VI. PENGEMBANGAN PERANGKAT LUNAK

Pada bab ini berisi kesimpulan dan saran dari penulis berdasarkan hasil yang telah diteliti.

1.8 Kesimpulan

Dari pendahuluan ini, telah dijelaskan secara umum mengenai penelitian yang dilakukan, meliputi latar belakang, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah serta sistematika penulisan.

DAFTAR PUSTAKA

Abdullah, D., & Saputro, D. N. (2016). Implementasi Algoritma Blowfish Dan Metode Least Significant Bit Insertion Pada Video Mp4. *Pseudocode*, *3*(2), 137-145.

ADRIAN, Aldo; BINTORO, Ketut Bayu Yogha. PENERAPAN KONSEP SOMATIC HYPERMUTATION DALAM ALGORITMA ENKRIPSI ONE-TIME PAD. Jurnal Ilmu Komputer, [S.l.], v. 11, n. 1, p. 1-8, may 2018. ISSN 2622-321X. Available at: <https://ojs.unud.ac.id/index.php/jik/article/view/39724>. Date accessed: 20 dec. 2022. doi: https://doi.org/10.24843/jik.2018.v11.i01.p01.

C. Irawan, D. R. I. M. Setiadi, C. A. Sari and E. H. Rachmawanto, "Hiding and securing message on edge areas of image using LSB steganography and OTP encryption," 2017 1st International Conference on Informatics and Computational Sciences (ICICoS), 2017, pp. 1-6, doi: 10.1109/ICICOS.2017.8276328.

Dhaief, Zahraa & Ali, Raniah & Maryoosh, Amal. (2020). Hiding Encrypted Text in Image using Least Significant Bit image Steganography Technique. International Journal of Engineering Research and Advanced Technology. 06. 10.31695/IJERAT.2020.3642.

Djuwitaningrum, Endang R., and Melisa Apriyani. "Teknik Steganografi Pesan Teks Menggunakan Metode Least Significant Bit Dan Algoritma Linear

Congruential Generator." Juita, vol. IV, no. 2, Nov. 2016, pp. 79-85, doi:10.30595/juita.v0i0.1333.

E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed and E. Mohamed, "A secure image steganography algorithm based on least significant bit and integer wavelet transform," in Journal of Systems Engineering and Electronics, vol. 29, no. 3, pp. 639-649, June 2018, doi: 10.21629/JSEE.2018.03.21.

Febryan, A. & Purboyo, Tito & Saputra, Randy. (2017). Steganography methods on text, audio, image and video: A survey. International Journal of Applied Engineering Research. 12. 10485-10490.

Harahap, M. K., & Khairina, N. (2017). Analisis Algoritma One Time Pad Dengan Algoritma Cipher Transposisi Sebagai Pengamanan Pesan Teks. *Sinkron : Jurnal Dan Penelitian Teknik Informatika*, *1*(2), 58-62. https://doi.org/10.33395/sinkron.v1i2.42.

Hariady, M. M., Suyatno, A., & Astuti, I. F. (2017). Keamanan Dan Penyisipan Pesan Rahasia Pada Gambar Dengan Enkripsi Blowfish Dan Steganografi End Of File.

Jain, A. (2020). A Secured Steganography Technique for Hiding Multiple Images in an Image Using Least Significant Bit Algorithm and Arnold Transformation. In: Hemanth, D., Shakya, S., Baig, Z. (eds) Intelligent Data Communication Technologies and Internet of Things. ICICI 2019. Lecture Notes on Data Engineering and Communications Technologies, vol 38. Springer, Cham. https://doi.org/10.1007/978-3-030-34080-3_42.

Lasarus Pelipus Malese. (2021). Penyembunyian Pesan Rahasia Pada Citra Digital dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (LSB). https://doi.org/10.5281/zenodo.5563416.

Lilyani, D. (2014). Implementasi Steganografi Pada Citra Digital Dengan Menggunakan Metode Dynamic Cell Spreading. *Pelita Informatika Budidarma*, *4*(1).

Mazurczyk, W., & Caviglione, L. (2014). Steganography in modern smartphones and mitigation techniques. *IEEE Communications Surveys & Tutorials*, *17*(1), 334-357.

Munir, R. 2019. Kriptografi. *2*. Informatika Bandung, hal.645.

PERANGIN-ANGIN, Resianta et al. Analisa Alokasi Memori dan Kecepatan Kriptograpi Simetris Dalam Enkripsi dan Dekripsi. Journal Information System Development (ISD), [S.l.], v. 4, n. 1, jan. 2019. ISSN 2528-5114. Available at: <https://ejournal-medan.uph.edu/index.php/isd/article/view/222>.

P. P. Bandekar and G. C. Suguna, "LSB Based Text and Image Steganography Using AES Algorithm," 2018 3rd International Conference on Communication and Electronics Systems (ICCES), 2018, pp. 782-788, doi: 10.1109/CESYS.2018.8724069.

Sejati, A. (2010). Studi dan perbandingan steganografi metode EOF (End of File) dengan DCS (Dynamic Cell Spreading). *Bandung: Institut Teknologi Bandung*.

Setiadi, De Rosal Ignatius Moses & Rachmawanto, Eko. (2017). Secure Image Steganography Algorithm Based on DCT with OTP Encryption. Journal of Applied Intelligent System. 2. 1-11. 10.33633/jais.v2i1.1330.

Yusnaini, Riyan & Susanto, Agus. (2019). Peningkatan Deteksi Steganografi Algoritma Least Significant Bit pada Citra Grayscale. 3.