Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)

journal homepage: http://journal.lembagakita.org/index.php/jtik

Aplikasi Steganografi Menggunakan *Least Significant Bit* (LSB) dengan Enkripsi *Caesar Chipper* dan *Rivest Code* 4 (RC4) Menggunakan Bahasa Pemrograman JAVA

Ade Davy Wiranata [1], Rima Tamara Aldisa [2]

[1] *Fakultas Teknik, Universitas Muhammadiyah Prof Dr. Hamka.*

[2] *Fakultas Teknologi Komunikasi dan Informatika, Universitas Nasional.*

a r t i c l e i n f o

Article history:
Received 2 November 2020
Received in revised form
4 Desember 2020
Accepted 7 December 2020
Available *online* August 2021

DOI:
https://doi.org/10.35870/jtik.v5i3.219

Keywords:
Steganography, Least Significant Bit (LSB), Caesar Chiper and RC4.

Kata Kunci:
Steganografi, Least Significant Bit (LSB), Caesar Chipper dan RC4.

a b s t r a c t

The research objective is to hide messages through images using the LSB (Least Significant Bit) method and Caesar Chipper and Rivest Code 4 encryption. The LSB (Least Significant Bit) method is used as a message hiding technique in steganography where hiding hidden messages is done by changing a few bits in the segment. image with a secret message. The results of this study resulted in an implementation using the Least Significant Bit (LSB) to be applied to institutions with an interest in maintaining the confidentiality of encrypted image output, changing the image file size and sound (audio) file size.

a b s t r a k

Tujuan penelitian untuk menyembunyikan pesan melalui gambar menggunakan metode LSB (Least Significant Bit) dan enkripsi Caesar Chipper dan Rivest Code 4. Metode LSB (Least Significant Bit) digunakan sebagai teknik penyembunyian pesan dalam steganografi dimana menyembunyikan pesan yang tersembunyi dilakukan dengan mengubah sedikit bit di segmen gambar dengan pesan rahasia. Hasil Penelitian ini menghasilkan implementasi dengan menggunakan Least Significant Bit (LSB) untuk diterapkan pada institusi yang berkepentingan untuk menjaga kerahasiaan output gambar terenkripsi mengubah ukuran file gambar dan ukuran file suara (audio).

*Corresponding author. Email: rimatamaraa@gmail.com [1].
© E-ISSN: 2580-1643.

1. Latar Belakang

Teknik menjaga kerahasiaan pesan tidak hanya menggunakan kriptografi [1]. Teknik lain yang dapat digunakan adalah steganografi. Steganografi adalah seni dan ilmu menyembunyikan pesan rahasia dalam pesan lain sehingga pesan rahasia tersebut tidak dapat diketahui keberadaannya [2, 3]. Berbeda dengan kriptografi yang merahasiakan makna pesan tetapi keberadaan pesan tersebut tetap ada, steganografi merahasiakannya dengan cara menutupi atau menyembunyikan pesan tersebut [4, 5, 6].

Salah satu metode steganografi citra digital adalah *Least Significant Bit* (LSB), dengan teknik penyembunyian pesan pada lokasi bit terendah pada citra digital [7, 8]. Pesan diubah menjadi bit biner dan disembunyikan dalam gambar digital menggunakan metode LSB [9, 10]. Menerapkan metode LSB tanpa sistem keamanan memiliki peluang untuk dengan mudah dibongkar melalui analisis frekuensi dengan menyelesaikan bit terendah [11, 12]. Pada penelitian ini dibahas steganografi menggunakan metode LSB dan metode *Encrypting Caesar Chipper* dan *Rivest Code 4* (RC4).

2. Landasan Teori

Steganografi

Steganografi berasal dari bahasa Yunani "*steganos*" yang berarti "tersembunyi" dan "*graphein*" yang berarti "menulis" [13]. Steganografi dapat diartikan sebagai "tulisan sampul" [14]. Steganografi membutuhkan dua sifat: data rahasia yang akan disembunyikan. Steganografi digital menggunakan media digital sebagai wadah penyimpanannya, misalnya: suara, video, gambar dan teks. Data rahasia yang dapat disembunyikan juga dapat berupa suara, video, gambar dan teks [15].

B.LSB (Sedikit Significat Bit)

LSB (*Least Significant Bit*) adalah metode stegnografi yang paling sederhana dan termudah untuk diimplementasikan ke dalam aplikasi. Metode ini menggunakan gambar digital sebagai teks konversi. Dalam array bit dalam satu byte (1 byte = 8 bit), dan bit yang paling tidak berarti (bit paling signifikan atau LSB). (Rachmat, 2010) [16].

Metode RC4

Metode RC4 dirancang oleh Ron Rivest yang berasal dari RSA Security pada tahun 1987. RC4 sendiri memiliki singkatan resmi dari "*Rivest Code*". RC4 adalah kecepatan dan kesederhanaannya dalam menangani banyak aplikasi, membuatnya mudah untuk mengimplementasikan perangkat keras perangkat lunak [17, 18].

Caesar Chipper

Caesar Cipher adalah metodologi enkripsi pertama. Metode enkripsi ini merupakan jenis sandi pengganti, di mana setiap huruf dalam teks biasa diganti dengan huruf lain [19]. Misalnya dengan shift 3 langkah, A akan diganti dengan D, B akan menjadi E, dan seterusnya [20, 21].

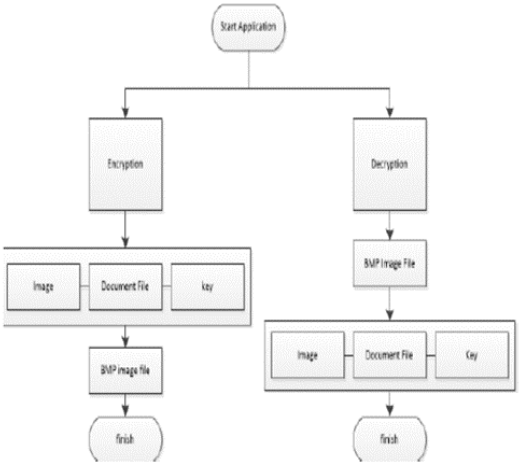
3. Metode Penelitian

Analisis

Merancang aplikasi untuk implementasi steganografi. Dua proses yang terjadi dalam implementasi steganografi adalah proses enkripsi dan dekripsi. Enkripsi adalah proses memasukkan dokumen ke dalam gambar dan dekripsi adalah proses ekstraksi untuk mengeluarkan dokumen atau pesan asli.

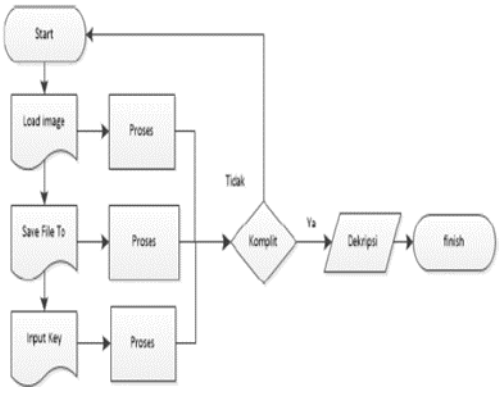
Desain Aplikasi

Aplikasi steganografi yang akan diusulkan adalah membuat aplikasi yang dapat digunakan untuk menyembunyikan dokumen / pesan rahasia dengan metode stegannografi LSB (*Least Significant Bit*) dan RC4 dan Caesar Chipper. Gambar alur desain aplikasi terlihat pada gambar 1 berikut.



Gambar 1. Alur desain aplikasi

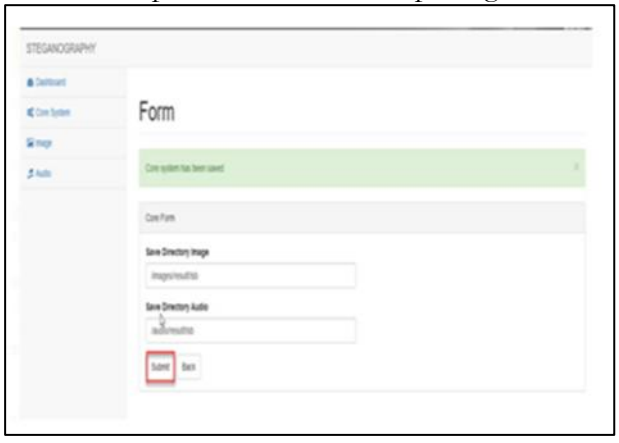
Dalam pembuatan aplikasi desain layar merupakan hal yang sangat penting. Desain layar harus mudah dipahami, sehingga dalam menggunakan aplikasi ini terasa nyaman dalam menggunakan aplikasi tersebut. Diagram alir untuk gambar dapat dilihat pada Gambar 2.



Gambar 2. Gambar Flowchart.

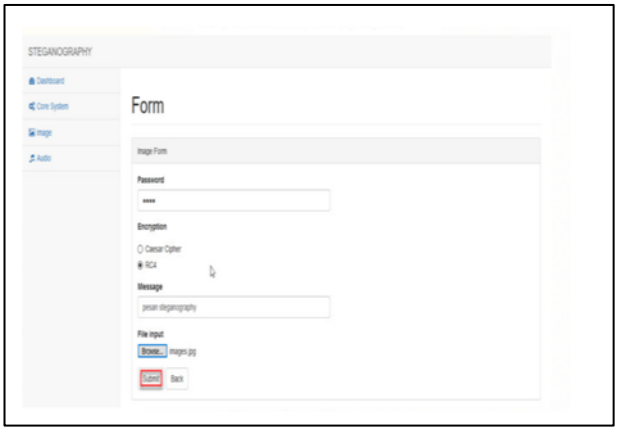
4. Hasil dan Pembahasan

Pada Gambar 3 merupakan tampilan layar berupa Image dan *Audio* yang berfungsi untuk menyisipkan dokumen / pesan rahasia terhadap image.



Gambar 3. Tampilan layar pemilihan gambar dan *audio*

RC 4 dan mengenkripsi Caesar Chiper terlihat pada Gambar 4 yang merupakan tampilan layar dari Formular seleksi terenkripsi untuk 2 metode RC 4 dan Caesar Chiper yang berfungsi untuk melakukan seleksi menggunakan metode yang diinginkan. Jadi peneliti menggunakan RC4.

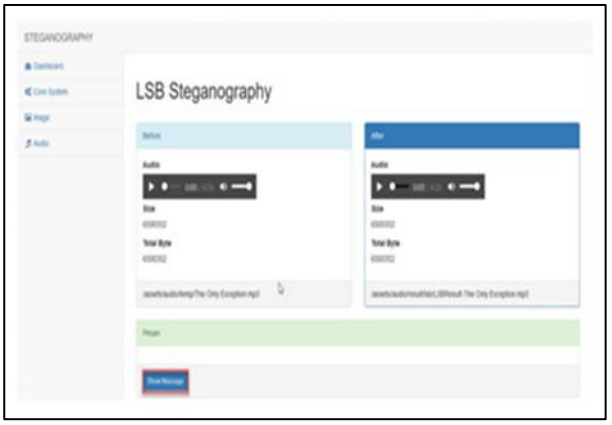


Gambar 4. Formulir seleksi enkripsi RC4 dan Caesar Cipher

Hasil Pengujian Aplikasi

1) Pengujian menggunakan format .mp3

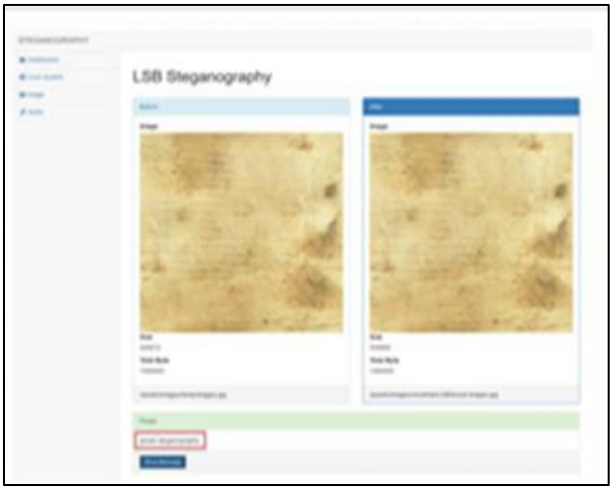
Setelah proses enkripsi, ukuran *audio* yang dihasilkan oleh *file* pesan yang diuji mengalami banyak perubahan dalam hal suara. Semakin besar *file* yang diujikan, semakin besar kualitas gambar suara yang berubah. Hasil perubahan *file audio* dapat dilihat pada Gambar 5.



Gambar 5. Pengujian Menggunakan format .mp3

2) Pengujian Menggunakan Format .jpg

Setelah proses enkripsi, ukuran citra yang dihasilkan oleh *file* pesan yang diuji mengalami banyak perubahan dari segi warna. Semakin besar *file* yang diuji, semakin tinggi kualitas gambar gambar yang berubah. Hasil perubahan tersebut dapat dilihat pada gambar 6.



Gambar 6. Pengujian Menggunakan format .jpg

5. Kesimpulan dan Saran

Berdasarkan analisis yang telah dilakukan, peneliti menemukan beberapa kesimpulan dan saran yang mungkin diperlukan untuk pengembangan aplikasi ke tahap selanjutnya.

1) Hasil aplikasi penyisipan pesan rahasia pada gambar berjalan dengan baik. Pesan atau dokumen yang disisipkan pada *file* gambar dan *file audio* dapat diambil kembali secara penuh.
2) Aplikasi steganografi yang telah dihasilkan dari implementasi dengan menggunakan LSB (*Least Significant Bit*) memberikan hal yang menarik untuk diterapkan pada institusi yang berkepentingan untuk menjaga kerahasiaan.
3) Dengan metode LSB (*Least Significant Bit*), citra yang disisipkan pada pesan atau dokumen tidak terlalu banyak menunjukkan perbedaan dengan citra berwarna.
4) Output gambar terenkripsi mengubah ukuran *file* gambar dan ukuran *file* suara (*audio*).

6. Daftar Pustaka

[1] Pabokory, F.N., Astuti, I.F. and Kridalaksana, A.H., 2016. Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer, 10(1), pp.20-31.

[2] Taburet, T., Bas, P., Sawaya, W. and Fridrich, J., 2020. Natural steganography in JPEG domain with a linear development pipeline. IEEE Transactions on Information Forensics and Security, 16, pp.173-186.

[3] Edisuryana, M., Isnanto, R.R. and Somantri, M., 2013. Aplikasi Steganografi Pada Citra Berformat Bitmap Dengan Menggunakan Metode End Of File. Transient: Jurnal Ilmiah Teknik Elektro, 2(3), pp.734-742.

[4] Zunaidi, M., 2013. Steganografi, Menyembunyikan Pesan atau File Dalam Gambar Menggunakan Command/DOS. Jurnal SAINTIKOM Vol, 12(1).

[5] Widianto, S.R., 2018. Desain dan Analisa Algoritma Steganografi dengan Metode Spread Spectrum Berbasis PCMK (Permutasi Chaotic Multiputaran Mengecil dan Membesar) Menggunakan Matlab. Jurnal Elektra, 3(1), pp.37-46.

[6] Yudha, D.P., Baihaqi, K.A. and Hasbi, B.I., 2019. Penyisipan Pesan Rahasia Pada Citra Gambar Dengan Teknik Steganografi Dan Algoritma Asimetris Enkripsi Rivest Shamir Adleman (RSA). Techno Xplore: Jurnal Ilmu Komputer dan Teknologi Informasi, 4(1), pp.15-19.

[7] Arya, A. and Soni, S., 2018. Performance Evaluation of Secrete Image Steganography Techniques Using Least Significant Bit (LSB) Method. vol, 6, pp.160-165.

[8] Bansal, K., Agrawal, A. and Bansal, N., 2020, June. A survey on steganography using least significant bit (lsb) embedding approach. In 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184) (pp. 64-69). IEEE.

[9] Setiadi, D.R.I.M., 2019. Payload Enhancement on Least Significant Bit Image Steganography Using Edge Area Dilation. International Journal of Electronics and Telecommunications, 65.

[10] Rahmansyah, E., 2019. Implementasi Algoritma Elgamal Dengan Pembangkit Bilangan Prima Lehmann Dan Algoritma Least Significant Bit (LSB) Dengan Cover Image Bitmap Untuk Keamanan Data Text. JURIKOM (Jurnal Riset Komputer), 6(1), pp.79-84.

[11] Sari, I.Y., Muttaqin, M., Jamaludin, J., Simarmata, J., Rahman, M.A., Iskandar, A., Pakpahan, A.F., Abdul Karim, S., Giap, Y.C., Hazriani, H. and Yendrianof, D., 2020. Keamanan Data dan Informasi. Yayasan Kita Menulis.

[12] Fathurrahmad, F., and Ester, E., 2020. Development And Implementation Of The Rijndael Algorithm And Base-64 Advanced Encryption Standard (AES) For Website Data Security. International Journal of Scientific & Technology Research, 9(11), pp.6-11.

[13] Hafiz, A., 2019. Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (LSB). Jurnal Cendikia, 17(1 April), pp.194-198.

[14] Fikhri, A.A. and Hendrawaty, H., 2019, January. Analisis Perbandingan Histogram dan Kualitas Citra Pada Image Steganografi Menggunakan Metode One Bit Least Significant Bit. In Prosiding Seminar Nasional Politeknik Negeri Lhokseumawe (Vol. 2, No. 1).

[15] Basim, Z. and Painem, P., 2020. Implementasi Kriptografi Algoritma RC4 Dan 3DES dan Steganografi Dengan Algoritma EOF Untuk Keamanan Data Berbasis Desktop Pada SMK As-Su'udiyyah. SKANIKA, 3(4), pp.45-52.

[16] Fata, R., 2018. Keamanan Pesan Rahasia Pada Streganografi Citra Menggunakan Kode Hamming (15, 11) (Doctoral dissertation, Institut Teknologi Sepuluh Nopember).

[17] Sumarno, S., 2018. Analisis Kinerja Kombinasi Algoritma Message-Digest Algortihm 5 (MD5), Rivest Shamir Adleman (RSA) dan Rivest Cipher 4 (RC4) Pada Keamanan E-Dokumen. Jurnal Sistem Informasi dan Ilmu Komputer Prima (JUSIKOM PRIMA), 2(1).

[18] Suhandinata, S., Rizal, R.A., Wijaya, D.O., Warren, P. and Srinjiwi, S., 2019. Analisis Performa Kriptografi Hybrid Algoritma Blowfish Dan AlgoritmA RSA. JURTEKSI (Jurnal Teknologi dan Sistem Informasi), 6(1), pp.1-10.

[19] Marisman, A.F. and Hidayati, A., 2015. Pembangunan Aplikasi Pembanding Kriptografi Dengan Caesar Cipher Dan Advance Encryption Standard (Aes) Untuk File Teks. Jurnal Penelitian Komunikasi dan Opini Publik, 19(3), p.123498.

[20] Latifah, R., Ambo, S.N. and Kurnia, S.I., 2017. Modifikasi Algoritma Caesar chiper dan rail fence untuk peningkatan keamanan teks alfanumerik dan karakter khusus. Prosiding Semnastek.

[21] Li, Q., Wang, X., Wang, X., Ma, B., Wang, C., Xian, Y. and Shi, Y., 2020. A Novel Grayscale Image Steganography Scheme Based on Chaos Encryption and Generative Adversarial Networks. IEEE Access, 8, pp.168166-168176.