Jurnal Elektronik Ilmu Komputer Udayana
Volume 13 No. 3, February 2025

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Penyisipan Pesan Tersembunyi Dalam Citra Menggunakan Metode Spread Spectrum dan Least Significant Bit (LSB)

Muhammad Caesar Gilang Indrawan[a1], I Gusti Agung Gede Arya Kadyanan[a2], I Wayan Supriana[a3], I Made Widiartha[a4]

[a]Informatics Departement, Faculty of Mathematics and Natural Science, Udayana University
Jl. Raya Kampus Unud, Jimbaran, South Kuta, Badung, Bali, Indonesia

[1]caesargilang50@gmail.com
[2]gungde@unud.ac.id
[3]wayan.supriana@unud.ac.id
[4]madewidiartha@unud.ac.id

Abstract

The advancement of information technology has facilitated data transmission but also increased cybersecurity threats. To protect data security, steganography is used to hide messages within images, ensuring only the intended recipient can read them. This research uses two steganography methods: Spread Spectrum and Least Significant Bit (LSB). The advantage of the Spread Spectrum method is that it produces images with low PSNR and MSE values, making the steganographic images similar to the original ones. However, the embedding and extraction processes are slow. To overcome this weakness, the LSB method is used, allowing for quick message embedding and extraction while maintaining the resolution and size of the images before and after message embedding. In this study, Spread Spectrum is used to determine the location of message embedding, while LSB is used for the message embedding process.

Keywords: *Steganography, cybersecurity threats, images, Spread Spectrum, Least Significant Bit (LSB)*

1. Pendahuluan

Perkembangan teknologi saat ini telah memberikan banyak kemudahan bagi manusia untuk melakukan berbagai aktivitas. Contohnya adalah pengiriman data dan informasi. Saat ini, pengiriman data dan informasi menjadi lebih mudah dan cepat. Namun, seiring dengan perkembangan teknologi tersebut, tentunya semakin berkembang pula berbagai bentuk kejahatannya. Oleh karena itu, pada saat ini telah dilakukan berbagai upaya untuk menjaga keamanan data dan informasi tersebut. Salah satu upaya untuk mejaga keamanan data dan informasi tersebut adalah dengan menerapkan Steganografi.

Steganografi adalah ilmu yang mempelajari cara menyembunyikan pesan atau data dalam media lain tanpa menarik perhatian dari pihak yang tidak berwenang. Tujuan dari steganografi adalah untuk memastikan bahwa pesan yang dikirimkan hanya dapat dibaca oleh penerima yang dituju dan tidak dapat terdeteksi oleh orang lain. Dalam era digital, steganografi telah menjadi semakin penting dengan munculnya internet dan teknologi komunikasi digital lainnya. Dalam konteks ini, steganografi dapat digunakan untuk menyembunyikan informasi dalam file gambar, audio, dan video.

Steganografi memiliki banyak metode. Namun metode yang akan digunakan dalam penelitian ini adalah metode Spread Spectrum dan Least Significant Bit (LSB). Metode Spread Spectrum memiliki kelebihan dibandingkan metode lainnya yaitu hasil citra yang telah diolah memiliki nilai PSNR dan MSE yang kecil, sehingga citra hasil steganografi mampu menyerupai citra aslinya, performa robustness pada citra baik karena hanya memiliki perubahan pixel sangat kecil, dan peluang terdeteksinya pesan rendah. Namun metode ini juga memiliki kelemahan yaitu kurang tahan terhadap serangan berupa noise, cropping, dan proses kompresi serta memiliki proses embedding dan ekstraksi yang lama.[1] Maka dari itu untuk mengatasi kelemahan dari metode Spread Spectrum perlu ditambahkan metode lain yaitu Least Significant Bit (LSB). Metode Least Significant Bit (LSB) memiliki kelebihan yang tidak dimiliki oleh metode Spread Spectrum yaitu proses penyisipan dan ekstraksi pesan cepat, citra sebelum dan sesudah disisipkan pesan memiliki resolusi yang sama, dan ukuran dari citra sebelum dan sesudah disisipkan pesan memiliki ukuran yang sama. Dalam implementasinya, metode spread spectrum akan

digunakan dalam menentukan letak pesan akan disisipkan dan metode Least Significant Bit (LSB) akan digunakan dalam proses menyisipkan pesannya.

2. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian eksperimental. Metode penelitian eksperimental adalah suatu tindakan dan pengamatan yang dilakukan untuk mengecek hipotesis atau mengenali hubungan sebab akibat antara gejala. Dalam penelitian eksperimental, penyebab dari semua gejala akan diuji untuk mengetahui sebab atau variabel bebas itu akan mempengaruhi akibat atau variabel terikat.

2.1 Data Penelitian

Pada penelitian ini, Data yang digunakan oleh peneliti adalah citra yang digunakan sebagai *cover* untuk melindungi pesan di dalamnya. Data citra ini diperoleh dari website https://www.kaggle.com/datasets/dansbecker/urban-and-rural photos yang berjumlah 92 citra.

2.2 Variabel Penelitian

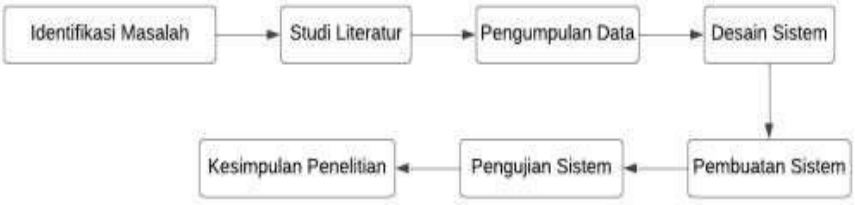
Dalam penelitian ini terdapat dua variabel, yaitu variabel bebas dan variabel terikat.

1. Variabel Bebas (Independen)
   Variabel ini merupakan variabel yang akan dilihat pengaruhnya terhadap variabel terikat dan variabel ini akan dimanipulasi oleh peneliti untuk menentukan hubungannya dengan suatu data yang diobservasi sesuai dengan kebutuhannya. Dalam penelitian ini, variabel bebasnya adalah pesan yang akan disisipkan ke dalam citra dan juga file citra itu sendiri dengan format **.jpg, *.png, *.jpeg.*

2. Variabel Terikat (Dependen)
   Variabel ini merupakan variabel hasil dari variabel bebas. Variabel ini umumnya menjadi tujuan penelitian dari sumber masalah yang ingin ditingkatkan kualitasnya. Pada penelitian ini, variabel terikatnya adalah hasil dari proses steganografi yang berupa file citra dengan format **.png.*

2.3 Diagram Alur Penelitian

Alur penelitian yang dilakukan dimulai dari tahap identifikasi masalah yang ingin diangkat. Lalu dilanjutkan dengan studi literatur. Pada tahap studi literatur dilakukan dengan mencaru sumber bacaan atau refrensi lainnya terkait permasalahan yang ingin diangkat. Setelah itu dilanjutkan dengan pengumpulan data berupa file gambar. Selanjutnya, melakukan desain dan implementasi sistem. Setelah sistem selesai dibangun, maka sistem akan dilakukan pengujian untuk mengambil kesimpulan penelitian.



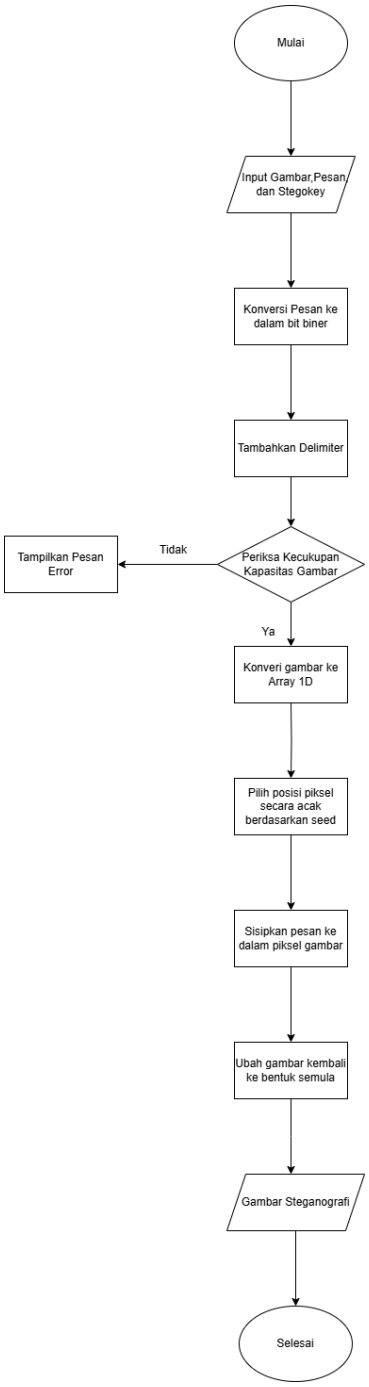
Gambar 1. Skema Penelitian

Dapat dilihat pada gambar 1, Penelitian ini dimulai dengan melakukan identifikasi masalah untuk mengetahui masalah apa yang ada dalam lingkunan sekitar. Kemudian dilanjutkan dengan studi literatur untuk mengetahui cara penyelesaian masalahnya, lalu dilanjutkan dengan pengumpulan data. Pada tahap ini, data-data yang menunjang penelitan akan dikumpulkan. Pada tahap desain sistem, mulai dirancang sistem yang akan dibangun dan dilanjutkan dengan pembuatan sistem. Setelah itu sistem akan diuji dalam tahap pengujian sistem dan diakhiri dengan membuat kesimpulan penelitian.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

2.4 Desain Sistem

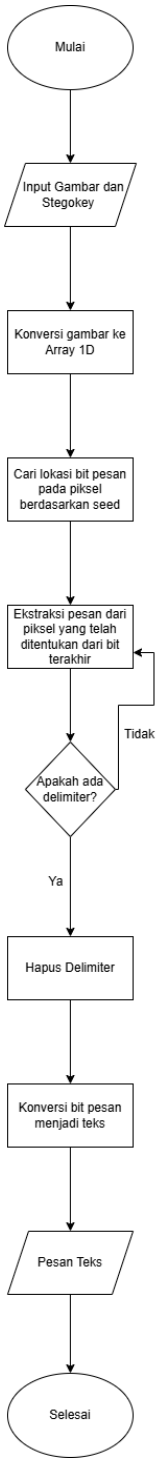
Berikut ini adalah alur kerja sistem secara keseluruhan:



Gambar 2. Flowchart Sistem Encode

Dapat dilihat pada gambar 2 di atas, proses encode dimulai dengan user memasukkan gambar, pesan, dan keywordnya. Setelah itu, program akan mengubah pesannya teks ke dalam bentuk biner dan di akhir pesan ditambahkan sebuah delimiter sebagai penanda akhir pesan. Lalu, program akan mengecek apakah kapasitas gambar ckuup untu menampung pesan apabila tidak akan muncul pesan error. Namun jika cukup maka program akan melanjutkan dengan mengonversi gambar ke dalam bentuk array 1 dimensi. Setelah itu program akan menghasilkan angka acak sebagai posisi

dimana pesan akan diletakkan. Lalu pesan akan disispkan sesuai lokasi yang telah ditetapkan sebelumnya. Lalu gambar akan diubah ke dalam bentuk semula dan gambar bsa diunduh oleh user.



Gambar 3. Flowchart Sistem Decode

Dapat dilihat pada gambar 3 di atas, proses decode dimulai dengan user memasukkan gambar dan keywordnya. Setelah itu, program akan mengonversi gambar ke dalam bentuk array 1 dimensi. Lalu, program akan mencari posisi dimana pesan yang diletakkan sebelumnya sesuai dengan

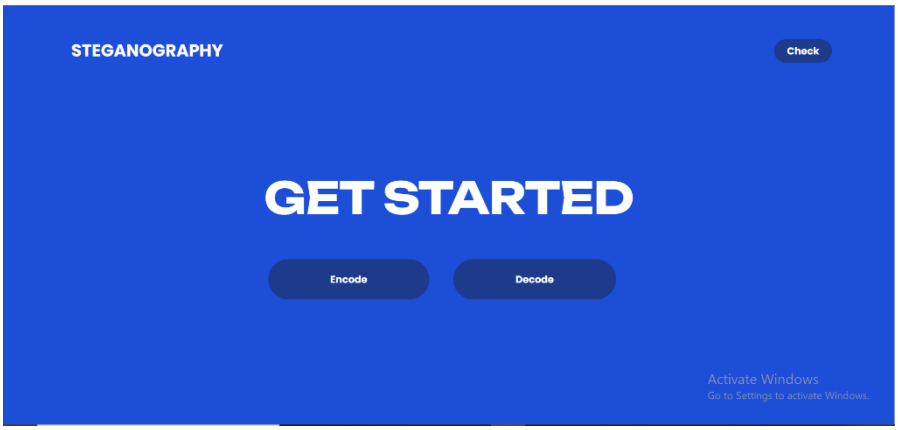
p-ISSN: 2301-5373
e-ISSN: 2654-5101

keywordnya. Lalu program akan mengekstraksi pesan dari bit terarkhir pesan. Lalu program akan mengecek apakah ada deilmiter jika ada maka program akan berhenti mengekstrasi dan delimiter dihapus. Namun jika tidak ada, maka program akan melanjutkan mengekstraksi pesan. Setelah itu program akan mengonversi bit-bit pesan yang telah dikumpulkan sebelumnya ke dalam bentuk semula dan dapat diunduh oleh user.

3. Hasil dan Pembahasan

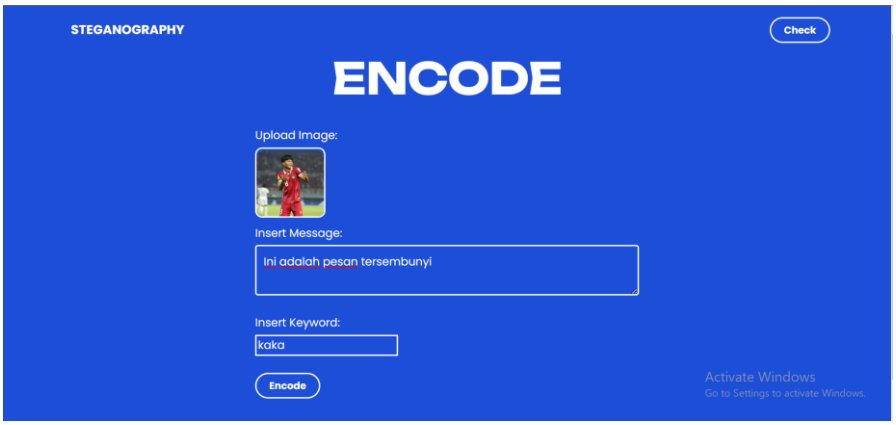
3.1. Implementasi

Berikut merupakan tampilan website steganografi.



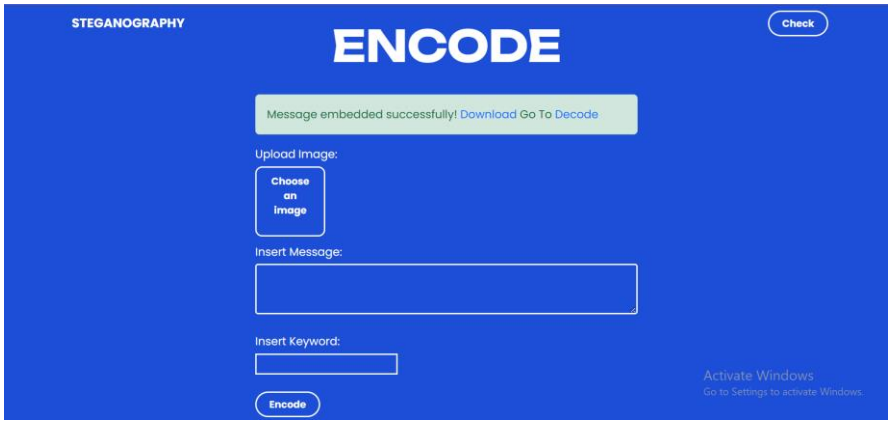
Gambar 4. Tampilan Awal Website

Pada tampilan awal website user akan menemukan sebuah kalimat “GET STARTED” dan terdapat beberapa tombol yaitu “Encode”, “Decode”, dan “Check”. Tombol-tombol ini akan mengarahkan user ke beberapa menu yang berada dalam website ini.



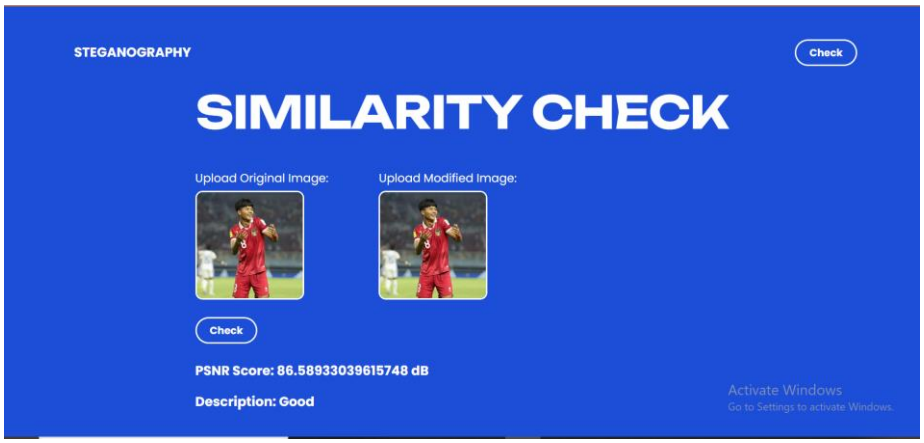
Gambar 5. Tampilan Form Encode

Untuk percobaan proses penyisipan, digunakan file gambar sebuah foto yang diambil di internet untuk percobaan penelitian ini dan pesan yang disisipkan berupa pesan teks “Ini adalah pesan tersembunyi”.



Gambar 6. Tampilan Hasil Encode

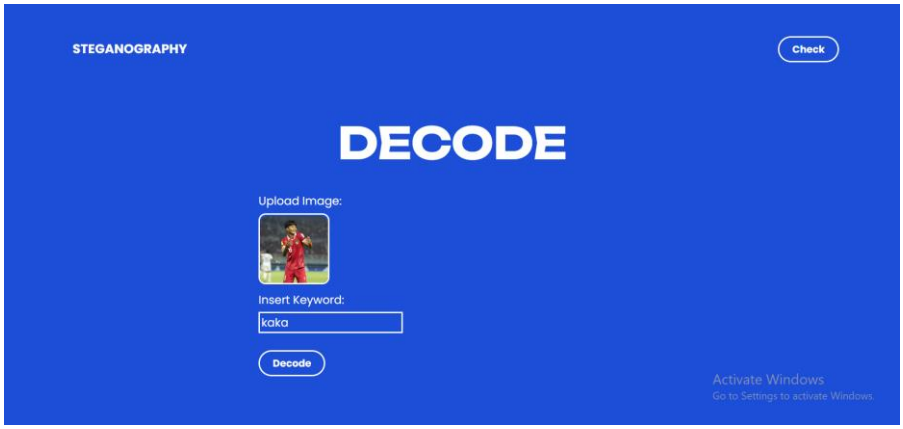
Jika proses encode berjalan lancar, maka akan tampil pesan “Message embedded successfully!”. Lalu user bisa menenkan tulisan “Download” untuk mengunduh gambar hasil dari proses encode tersebut. Kemudian jika user ingin melanjutkan untuk mengekstraksi pesan dari gambar, user bisa menekan tulisan “Decode”. Jika user ingin melakukan pengujian kemiripan citra antara citra asli dan citra steganografi, user bisa menekan tombol “Check” di pojok kanan atas website.



Gambar 7. Tampilan Hasil Halaman Check

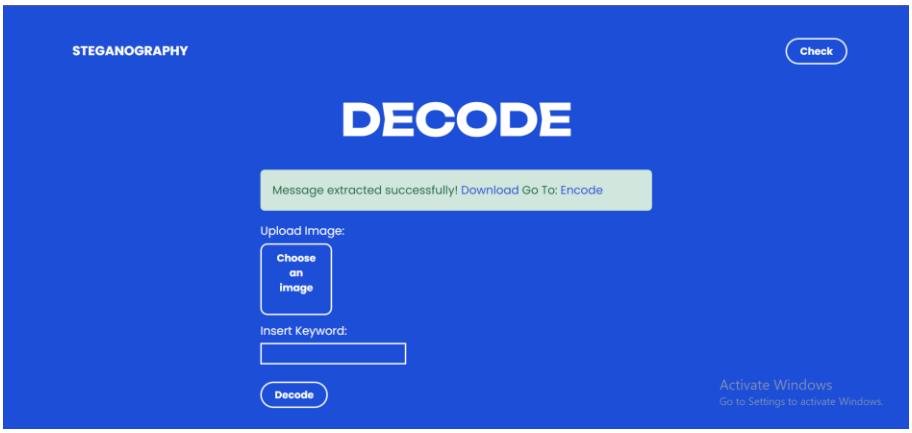
Berdasarkan gambar di atas, dapat dilihat bahwa nilai PSNR dari citra adalah 86.58933039615748 dB dan deskripsinya adalah “Good”. Deskripsi good ini didapat karena nilai PSNR dari citra melebihi 40 dB yang mana kualitas citra steganografi yang baik adalah minimal mencapai nilai PSNR 40 dB. Jadi dapat disimpulkan bahwa kualitas citra steganografi ini baik dan kemiripan citra steganografi dengan citra aslinya mirip.

p-ISSN: 2301-5373
e-ISSN: 2654-5101



Gambar 8. Tampilan Halaman Decode

Untuk percobaan digunakan file stego image yang merupakan hasil penyisipan yang dilakukan pada proses sebelumnya dan dibutuhkan juga keyword yang sebelumnya digunakan.



Gambar 9. Tampilan Hasil Halaman Decode

Kemudian user dapat menekan tombol decode dan akan dilakukan proses decode. Jika proses decode berhasil dilakukan maka akan muncul pesan “Message extracted successfully!”. Setelah itu user bisa mengunduh pesan yang telah diekstraksi dengan menekan tulisan “Download” dan jika user ingin ke halaman encode, user bisa menekan tulisan “Encode” di bawah.

3.2. Hasil

Untuk hasil uji kualitas atau PSNRnya dapat dilihat pada tabel dibawah berikut :

Tabel 1. Hasil Uji PSNR

No	Citra Asli	Citra Steganografi	PSNR (dB)
1			80.45

2			79.77
3			79.81
4			80.07
5			79.73
6			79.94

p-ISSN: 2301-5373
e-ISSN: 2654-5101

7			80.03
8			79.85
9			79.77
10			79.65

Rata-rata dari kesepuluh kali percobaan PSNR :

Rata-rata = (Total seluruh PSNR) / Jumlah percobaan PSNR

= (80.45 + 79.77 + 79.81 + 80.07 + 79.73 + 79.94 + 80.03 + 79.85 + 79.77 + 79.65)

= 799.07 / 10

= 79.90

Berdasarkan 10 kali pengujian yang dilakukan dalam tabel 1 di atas, didapatkan nilai rata-rata PSNR masih berada diatas 40dB[2] yang berarti hasil pengujian untuk pesan dan kata kunci tersebut dengan gambar-gambar di atas dapat disimpulkan bahwa kualitas citra steganografi yang dihasilkan oleh program ini termasuk baik.

4. Kesimpulan

Kesimpulan yang dapat diambil dari penelitian ini adalah sebagai berikut :

1. Metode steganografi Spread Spectrum dan Least Significant Bit (LSB) yang dibangun pada program ini berhasil menyisipkan pesan ke dalam citra dengan format *.jpg, *.png, dan *.jpe dan dapat menyimpan citra steganografi. Selain itu program ini berhasil mengekstraksi pesan dari citra steganografi dan mengunduhnya.
2. Dari 10 kali pengujian kemiripan gambar dengan metode PSNR didapatkan bahwa rata-rata PSNR yang dihasilkan adalah 68.67 dB. Penggunaan metode Spread Spectrum dan LSB termasuk baik karena rata-rata nilai PSNR yang dihasilkan masih diatas standar kategori baik yaitu diatas 40dB[3].
3. Dari 5 kali pengujian citra yang sama namun dengan ukuran yang berbeda untuk mengetahui pengaruh ukuran citra terhadap nilai PSNR, didapatkan bahwa rata-rata nilai kenaikan nilai PSNR dalam setiap tahapannya adalah 6.23%.
4. Dari 5 kali pengujian citra yang saman namun dengan ukuran yang berbeda untuk mengetahui pengaruh ukuran citra terhadap runtime program, didapatkan bahwa rata-rata kenaikan nilai runtime pada setiap tahapannya adalah 0.0025 detik untuk encode dan 0,625 detik untuk decode.

References

Aprilia, I., Ariyanti, D. and Izzuddin, A. (2019) ‘Analisa Pengukuran Kualitas Citra Hasil Steganografi’, pp. 116–121.

Aryani, L. *et al.* (2020) ‘Prediksi Jumlah Siswa Baru Dengan Menggunakan Metode Exponential Smoothing (Studi Kasus : Smk Ethika Palembang)’, *Bina Darma Conference on Computer Science*, 2(Vol 2 No 3 (2020): Bina Darma Conference on Computer Science (BDCCS)), pp. 237–244.

Assyahid, M. M., Rihartanto, R., & Utomo, D. S. B. (2018). *Implementasi Steganografi Pesan Text ke Dalam Audio Dengan Metode Spread Spectrum. Juristek*, *3(2), 27–34.*

Darwis, D., Junaidi, A. and Wamiliana (2019) ‘A New Approach of Steganography Using Center Sequential Technique’, *Journal of Physics: Conference Series*, 1338(1). Available at: https://doi.org/10.1088/1742- 6596/1338/1/012063.

Emmett Grames. (2020). *Implementasi Steganografi Menggunakan Metode Spread Spectrum Dalam Pengamanan Data Teks Pada Citra Digital.*

Jurnal, J. *et al.* (2023) ‘Implementasi Keamanan Aset Informasi Steganografi Menggunakan Metode Least Significant Bit (LSB)’, 3(1), pp. 40–46.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Mardiansyah Arief, & Yusfrizal. (2020). *Menggunakan Spread Spectrum Dan Gost Berbasis Android*. *82. IT Journal*, *Vol. 8, 81–92.*

Ratnasari, A. P., & Dwiyanto, F. A. (2020). Metode Steganografi Citra Digital. *Sains, Aplikasi, Komputasi Dan Teknologi Informasi*, *2*(2), 52. https://doi.org/10.30872/jsakti.v2i2.3300

Widianto, S. R. (2018). *Desain Algoritma Steganografi dengan Metode Spread Spectrum Berbasis PCMK (Permutasi Chaotic Multiputaran Mengecil dan Membesar) Yang Tahan Terhadap Gangguan. Prosiding Seminar Nasional Sains Dan Teknologi*, *1–8*.

Wiranata, A. D., & Aldisa, R. T. (2021). *Aplikasi Steganografi Menggunakan Least Significant Bit (LSB) dengan Enkripsi Caesar Chipper dan Rivest Code 4 (RC4) Menggunakan Bahasa Pemrograman JAVA*. *Jurnal JTIK (Jurnal Teknologi Informasi Dan Komunikasi)*, *5*(3), 277. https://doi.org/10.35870/jtik.v5i3.219

This page is intentionally left blank.