ISSN : 2962 – 5688
Website : jurnal.umj.ac.id/index.php/TripleA
Email : triplea@umj.ac.id

TRIPLE A
Jurnal Pendidikan Teknologi Informasi

IMAGE STEGANOGRAPHY DENGAN MENGGUNAKAN METODE LSB PADA PYTHON

Farhan Rizki Permana , Raihan Fadillah Setiyanto , Aditya Rafi Fauzi

Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta

Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta

Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta

aditya.rafifauzi.tik20@mhsw.pnj.ac.id,

farhan.rizkipermana.tik20@mhsw.pnj.ac.id,

3. *raihan.fadillahsetiyanto.tik20@mhsw.pnj.ac.id*

Abstract

Image Steganography adalah teknik menyembunyikan pesan rahasia di dalam gambar agar tidak terlihat oleh mata manusia. Metode Least Significant Bit (LSB) adalah salah satu metode yang umum digunakan dalam steganografi gambar. Metode ini memanfaatkan bit terakhir dari piksel gambar untuk menyimpan bit pesan. Dalam penelitian ini, kami mengimplementasikan metode LSB menggunakan bahasa pemrograman Python. Pertama, kami memuat gambar yang akan digunakan sebagai media steganografi. Kemudian, kami mengonversi pesan rahasia ke dalam format biner. Berdasarkan pesan biner tersebut, kami memilih piksel-piksel yang akan dimodifikasi dalam gambar. Kami mengubah bit terakhir pada setiap piksel tersebut sesuai dengan bit pesan rahasia. Proses ini dilakukan secara berurutan, dari piksel pertama hingga piksel terakhir. Setelah semua bit pesan telah disisipkan, gambar hasil steganografi dapat disimpan dalam format baru atau dapat langsung ditampilkan. Untuk mengambil pesan rahasia dari gambar steganografi, kami mengikuti proses yang sebaliknya. Kami membaca bit terakhir dari setiap piksel gambar dan menggabungkannya menjadi pesan biner. Pesan biner tersebut kemudian diubah kembali menjadi bentuk pesan asli.

Keywords— Image Steganography, LSB, penyisipan pesan, ekstraksi pesan, Python

PENDAHULUAN

Dalam era digital yang semakin maju, keamanan dan privasi data menjadi isu yang kian penting. Dalam konteks ini, steganografi gambar telah menjadi salah satu teknik yang digunakan untuk menjaga kerahasiaan dan keutuhan informasi. Steganografi gambar adalah cabang ilmu yang mempelajari cara menyembunyikan data rahasia dalam gambar digital tanpa menimbulkan kecurigaan pada penerima pesan.

Salah satu metode yang umum digunakan dalam steganografi gambar adalah Least Significant Bit (LSB). Metode ini memanfaatkan fakta bahwa perubahan kecil pada bit terakhir piksel gambar tidak secara signifikan mempengaruhi penampilan visual gambar tersebut. Dengan menggunakan metode LSB, bit-bit pesan dapat disembunyikan pada bit-bit yang kurang signifikan dalam piksel gambar.

Keamanan sistem informasi dan metode autentikasi yang handal. Kami juga akan menguraikan konsep dasar *One Time Password* (*OTP*) dan algoritma *RSA* sebagai metode autentikasi yang efektif. Selain itu, kami akan memaparkan pentingnya penggunaan bahasa pemrograman *Python* dalam implementasi sistem otentikasi ini, yang memberikan fleksibilitas dan kemudahan dalam pengembangan aplikasi.

One Time Password (OTP)

One Time Password (OTP) merupakan sebuah kode yang digunakan hanya sekali untuk otentiasi pengguna dalam sebuah sesi. Kode ini dihasilkan secara unik Python, sebagai bahasa pemrograman yang populer dan memiliki dukungan pustaka yang luas, menyediakan berbagai alat dan pustaka yang memungkinkan implementasi steganografi gambar dengan metode LSB secara efisien. Melalui penggunaan Python, implementasi metode LSB menjadi lebih mudah dan dapat diakses oleh para peneliti, pengembang, dan praktisi.

Dalam konteks ini, jurnal ini bertujuan untuk menyajikan sebuah implementasi praktis dari metode LSB untuk steganografi gambar menggunakan bahasa pemrograman Python. Melalui jurnal ini, pembaca akan mempelajari langkah-langkah implementasi metode LSB secara terperinci dan memahami cara menggunakannya untuk menyembunyikan data rahasia dalam gambar digital.

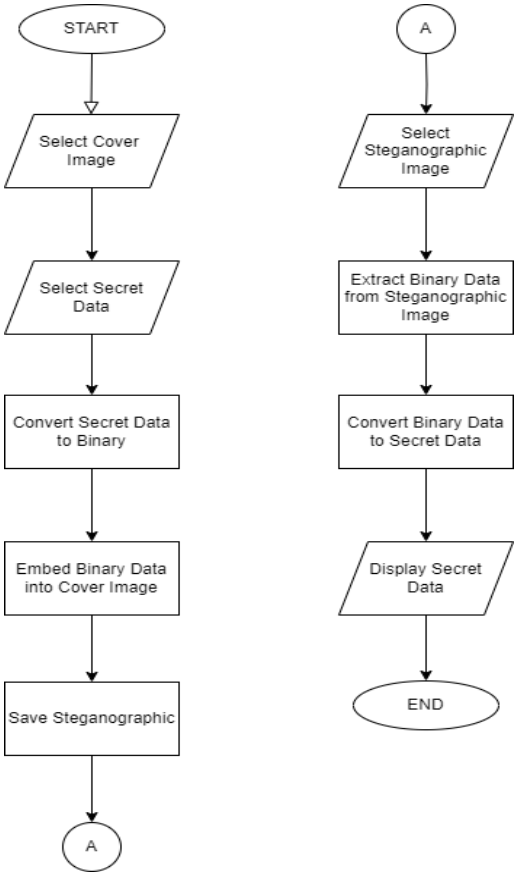
Selain itu, jurnal ini juga akan melakukan evaluasi terhadap kinerja metode LSB dalam hal kapasitas penyembunyian data dan ketahanannya terhadap serangan. Evaluasi ini penting untuk menentukan keandalan dan efektivitas metode LSB dalam menjaga kerahasiaan data yang disembunyikan.

Dengan adanya jurnal ini, diharapkan peneliti, pengembang, dan praktisi di bidang keamanan informasi dapat memperoleh pemahaman yang lebih baik tentang steganografi gambar dengan metode LSB dan mampu mengimplementasikannya menggunakan bahasa pemrograman Python. Di samping itu, jurnal ini juga diharapkan dapat memberikan kontribusi dalam pengembangan teknik steganografi gambar untuk memperkuat privasi dan keamanan data di era digital yang semakin kompleks ini.

METODE PENELITIAN

Dalam hal metodologi penelitian steganografi menggunakan metode Least Significant Bit (LSB) hanya dikumpulkan berupa berkas berkas data saja yang

dibutuhkan seperti jurnal pendukung dan pengumpulan bahan-bahan data seperti di bawah ini :



Gambar 1. Flowchart Program

Tahapan analisis Studi Komparasi Image Steganography Dengan Menggunakan Metode Lsb Pada Python. Berikut adalah langkah-langkah dan penjelasannya:

Langkah 1 : Flowchart dimulai dengan "Start".

Langkah 2 : Pengguna diminta untuk memilih gambar yang akan digunakan sebagai gambar sampul melalui "Select Cover Image".

Langkah 3 : Pengguna kemudian diminta untuk memilih data rahasia yang akan disisipkan melalui "Select Secret Data".

Langkah 4 : Data rahasia tersebut kemudian dikonversi ke dalam format biner melalui "Convert Secret Data to Binary".

Langkah 5 : Data biner yang dihasilkan akan disisipkan ke dalam gambar sampul melalui "Embed Binary Data into Cover Image".

Langkah 6 : Gambar steganografi yang telah dihasilkan disimpan melalui "Save Steganographic Image".

Langkah 7 : Pengguna kemudian diminta untuk memilih gambar steganografi yang akan digunakan untuk ekstraksi data rahasia melalui "Select Steganographic Image".

Langkah 8 : Data biner yang tersembunyi dalam gambar steganografi diekstraksi melalui "Extract Binary Data from Steganographic Image".

Langkah 9 : Data biner yang diekstraksi kemudian dikonversi kembali menjadi data rahasia asli melalui "Convert Binary Data to Secret Data".

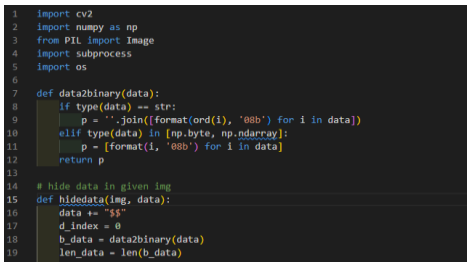
Langkah 10 : Data rahasia yang diekstraksi ditampilkan melalui "Display Secret Data".

Langkah 11 : Aliran program berakhir di "End".

HASIL DAN PEMBAHASAN

Analisis Kebutuhan

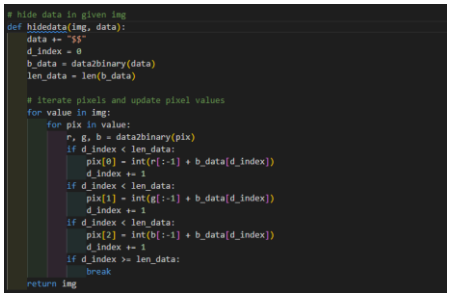
Berikut adalah syntax untuk mengenkripsi pesan didalam gambar menggunakan bahasa pemrograman python.



Gambar 3. Syntax Python.

Pada *Gambar 3.Syntax Python* melakukan *import*(menggunakan) pada beberapa *Library* yang dimiliki oleh python, diantaranya adalah

- ***Open cv*** atau ***cv2*** berfungsi untuk membaca dan menulis gambar serta melakukan operasi pada piksel-piksel gambar. cv2 biasanya digunakan untuk membaca, menulis, dan memanipulasi gambar dan video, mendeteksi objek, mengenali wajah, melakukan pelacakan gerakan, serta banyak aplikasi lain dalam bidang pengolahan citra dan visi komputer.
- ***Numpy*** berfungsi untuk melakukan manipulasi data numerik dan mengonversi data ke dalam representasi biner. NumPy menyediakan objek array yang efisien dan efektif dalam penggunaan memori untuk menyimpan dan memanipulasi data numerik dengan cara menyediakan berbagai fungsi dan operasi matematika untuk melakukan operasi pada array numerik yang effisien dan cepat.
- ***PIL(Python Image Library)*** berfungsi untuk membuka, menyimpan, dan memanipulasi gambar-gambar yang digunakan dalam proses steganografi. Dengan PIL, kita dapat melakukan operasi seperti resize, crop, rotasi, konversi format, penyesuaian kualitas, dan banyak masih lagi fungsi dari library PIL
- ***Subprocess*** berfungsi untuk menjalankan perintah shell yang membuka folder yang berisi file output hasil enkripsi. Subprocess memungkinkan kita untuk berkomunikasi dengan shell sistem operasi, menjalankan perintah-perintah sistem, mengontrol input dan output, serta melakukan pemrosesan paralel dari dalam skrip Python.
- ***Os*** berfungsi untuk mendapatkan jalur lengkap file output hasil enkripsi dan membuka folder yang berisi file output tersebut. Os memungkinkan kita untuk mengakses dan mengontrol berbagai fitur dan layanan sistem operasi seperti manajemen file dan folder, menjalankan perintah-perintah shell, mengelola variabel lingkungan, dll.



Gambar 4. Syntax Python (2)

Pada *Gambar 4. Syntax Python(2)* memilik Fungsi **hidedata(img, data)** yang diantaranya berfungsi untuk menyembunyikan data di dalam gambar yang diberikan lalu mengonversi data menjadi representasi biner. Setiap nilai piksel dalam gambar diperbarui dengan bit data yang disematkan lalu mengembalikan kembali gambar yang telah diubah.

Gambar 5. Syntax Python (3)

Pada *Gambar 5. Syntax Python(3)* Fungsi ini digunakan untuk mencari data yang disembunyikan dalam gambar. Bit data yang sudah disematkan lalu diambil kembali dari bit terakhir setiap nilai piksel kemudian nilai piksel dalam gambar diubah menjadi representasi biner. String biner yang sudah ditemukan diubah menjadi karakter menggunakan chr() hingga ditemukan penanda akhir "$$". Sehingga kemudian data yang sudah terbaca dikembalikan kembali.

```
def steganografi():
    x = 1
    while x != 0:
        print('''\n Image Steganography
1. encode
2. decode''')
        u_in = int(input("\n enter your choice: "))
        if u_in == 1:
            encode()
        else:
            ans = decode()
            print("\n your message: " + ans)
        x = int(input("\n enter 1 to continue or 0 to exit: "))

steganografi()
```

Gambar 6. Syntax Phyton (4)

Pada *Gambar 6. Syntax Python* Fungsi ini merupakan inti dari program dimana pengguna diberikan pilihan antara menkripsi atau mendekripsi pesan. Pilihan pengguna digunakan untuk memanggil fungsi encode() atau decode(). Setelah itu, pengguna diberi opsi untuk melanjutkan atau keluar dari program.

4. Implementasi dan Hasil

4.1 Lingkungan Pemrograman

Implementasi steganografi dengan menggunakan metode LSB pada Python dilakukan dengan memanfaatkan beberapa library dan modul yang tersedia. Lingkungan pemrograman yang digunakan dalam penelitian ini adalah sebagai berikut:

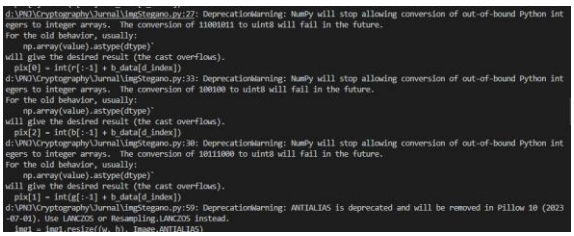
- Bahasa Pemrograman: Python
- Library/Modul: PIL (Python Imaging Library) atau OpenCV
- Sistem Operasi: Windows 10

4.2 Deskripsi Implementasi

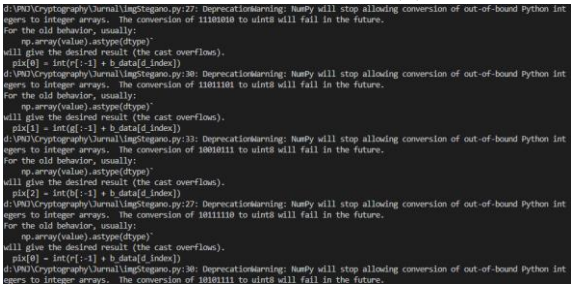
Implementasi steganografi gambar dengan metode LSB pada Python melibatkan langkah-langkah berikut:

- Pertama, memuat gambar yang akan digunakan sebagai media steganografi menggunakan library PIL atau modul OpenCV
- Kedua, mengonversi pesan rahasia ke dalam bentuk biner.
- Ketiga, memodifikasi bit terakhir dari piksel-piksel gambar sesuai dengan bit-bit pesan rahasia, seperti yang terlihat pada *Gambar 7 & 8 Konversi Bit ke Pixel.* Proses ini dilakukan dengan mengiterasi piksel-piksel gambar secara berurutan.

Keempat, menyimpan gambar hasil steganografi dalam format baru atau menampilkannya secara langsung menggunakan library PIL atau modul OpenCV.



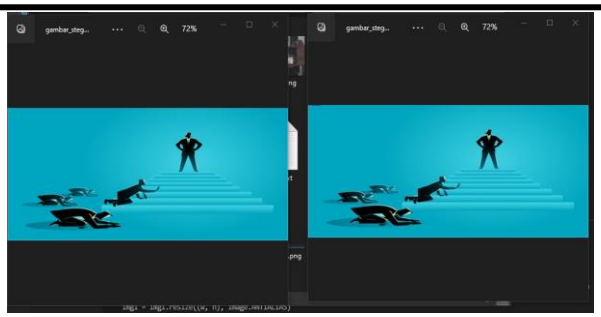
Gambar 7. Konversi Bit ke Pixel (1)



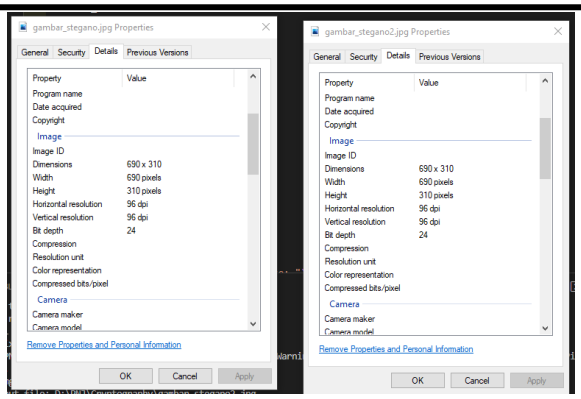
Gambar 8. Konversi Bit ke Pixel (2)

Dibawah ini adalah gambar hasil dari steganografi sebelum dan sesudah di inject oleh pesan teks. Terlihat sekilas tidak ada perbedaan pada kedua gambar dibawah ini.

TRIPLE A: Jurnal Pendidikan Teknologi Informasi. Vol. 2 (1), pp: 1 - 7



Gambar 9. Hasil Sebelum dan Sesudah di Inject Pesan Teks



Gambar 10. Sebelum dan Sesudah Inject tidak ada Perubahan Pada Pixel

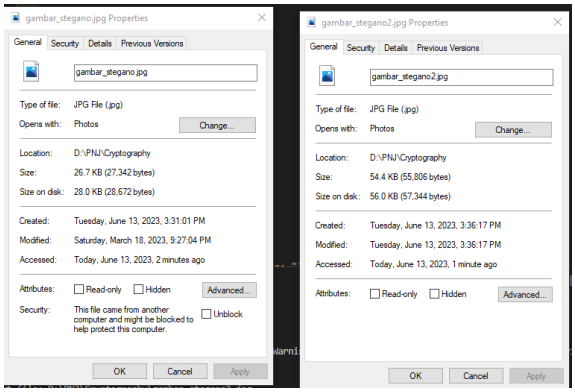
Hasil Eksperimen

Eksperimen yang dilakukan menggunakan berbagai gambar dan pesan rahasia dengan panjang yang berbeda. Hasil eksperimen ini menunjukkan efektivitas metode LSB dalam menyembunyikan pesan rahasia dalam gambar tanpa mengganggu tampilan visual gambar asli secara signifikan. Gambar hasil steganografi dapat dibandingkan dengan gambar asli untuk memverifikasi keberhasilan penyisipan pesan. Selain itu, ekstraksi pesan rahasia dari gambar steganografi juga dilakukan untuk memastikan keberhasilan metode LSB dalam mengambil pesan yang disembunyikan.

Hasil eksperimen ini akan ditampilkan dalam bentuk visualisasi gambar dan pesan yang berhasil disembunyikan serta perbandingan antara gambar asli dan gambar hasil steganografi. Analisis lebih lanjut terhadap hasil eksperimen juga akan dilakukan untuk mengevaluasi kekuatan dan kelemahan metode LSB pada steganografi gambar dengan menggunakan Python.

Berikut ini adalah hasil perbandingan foto sebelum di inject oleh pesan teks dan setelah di inject pesan teks tidak ada perubahan pixels yang menandakan gambar tetap mirip walaupun didalamnya sudah ditambahkan pesan teks.

Berikut ini adalah hasil perbandingan bobot foto sebelum di inject oleh pesan teks dan setelah di inject pesan teks. Bisa dilihat pada gambar sebelum di inject teks bobot yang tertera digambar adalah 26.7KB dan gambar setelah di inject oleh pesan teks bobotnya menjadi 54.4KB



Gambar 11. Hasil Foto sebelum dan sesudah inject Terdapat Perubahan Pada Ukuran FIle

SIMPULAN

1. Kesimpulannya, metode LSB dalam steganografi gambar yang diimplementasikan menggunakan Python berhasil menyembunyikan pesan rahasia dengan baik. Penggunaan bahasa pemrograman Python mempermudah proses pengolahan gambar dan manipulasi piksel-piksel. Dalam pengembangan selanjutnya, penelitian ini dapat diekspansi dengan mengimplementasikan teknik

steganografi lainnya dan membandingkan performa dengan metode LSB.

DAFTAR PUSTAKA

Anita Putri Ratnasaria, Felix Andika Dwiyanto. "Metode steganografi citra digital". Sains, Aplikasi, Komputasi dan Teknologi Informasi. Vol 2, No 2, April 2020, pp. 52-56.

Marija Mojsilović, Selver Pepić, Goran Miodragović. "Implementation of embedded messages using steganography in the PHP software package". Technics and Informatics in Education – TIE 2022.

Malese, L. (2021). Penyembunyian Pesan Rahasia Pada Citra Digital dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (LSB). Jurnal Ilmiah Wahana Pendidikan, 7(5), 343-354.

Muhammad Kailani Ridwan, William Frado Pattipeilohy, Sanwani. "Aplikasi Keamanan Document Digital Menggunakan Algoritma Steganografi Discrete Cosine Transform (DCT) pada Perusahan Alat Berat". J.I.T.K (Jurnal Ilmu Pengetahuan dan Teknologi Komputer).Vol.5 No. 2, 2020.

Muh. Basri, Muhammad Fadhlil Gushari. "PENERAPAN STEGANOGRAFI GAMBAR BERWARNA PADA DELAPAN IMAGE COVER MENGGUNAKAN METODE LSB". JURNAL SINTAKS LOGIKAVol. 1 No. 3, Oktober-2021.

M. R. Islam, T. R. Tanni, S. Parvin, M. J. Sultana & A. Siddiqa (2021) A modified LSB image steganography method using filtering algorithm and stream of password, Information Security Journal: A Global Perspective, 30:6, 359-370

Penda Sudarto Hasugian, Agustina Simangunsong. "Implementation of Least Significant Bit (LSB) Algorithm dor Data Security in Digital Imagery". Jurnal Info Sains: Informatikan dan Sains, Volume 10, No 02 September 2020.

Sabyasachi Pramanik, S. Suresh Raja. "A Secured Image Steganograpy Using Genetic Algorithm". Advances in Mathematics: Scientific Journal 9 (2020), no.7, 4533–4541.

Syaifullah Abdurrahman, Aditya Prapanca. "Pengamanan File Dokumen Ujian Dengan Image Steganography Metode Lsb" JINACS (Journal of Informatics and Computer Science). Vol. 03 No. 02, 2021.

Wijaya, B. A., Manalu, A. J.., Tarigan, B. A. and Silitonga, L. S. (2021) "Steganography Text Message Using LSB and DCT Methods", Jurnal Mantik, 5(3), pp. 1825-1832.