JT : Jurnal Teknik
P-ISSN: 2302-8734
E-ISSN: 2581-0006

Vol. 11 No. 01 Th. 2022
Halaman : 62 - 72
Published 27 Juni 2022

IMPLEMENTASI STEGANOGRAFI FILE CITRA DIGITAL MENGGUNAKAN METODE LEAST SIGNIFICANT BIT

IMPLEMENTATION OF DIGITAL IMAGE FILE STEGANOGRAPHY USING THE LEAST SIGNIFICANT BIT METHOD

[1]Angga Aditya Permana, [2]Habib Amna
[1] Program Studi Informatika, Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara
Jl. Boulevard, Gading Serpong, Kel. Curug Sangereng, Kec. Kelapa Dua, Kab. Tangerang – Banten
[2]Program Studi Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Syarif Hidayatullah Jakarta
Jl. Ir H. Juanda No.95, Cemp. Putih, Kec. Ciputat Tim., Kota Tangerang Selatan, Banten 15412

e-mail: angga.permana@umn.ac.id

Receive: 16 April 2022 Accepted: 27 Juni 2022

Abstract

The use of steganography aims to disguise confidential data so that it is difficult to detect, by inserting a secret message into the image. The simplest method used to hide secret messages in this application is to insert messages into low bits (LSB - Least Significant Bit) by replacing each pixel bit in the inserted image file. The number of characters of the secret message that can be accommodated depends on the size of the image file as a placeholder. Python is a programming language that is widely used by developers, Python can also be used for computing and visualization, by using an interface design commonly known as a GUI (Graphical User Interface). on digital images of png image files using Python and hiding the existence of a hidden message or information and producing an image file that has a quality that is not much different from the original digital image file.
Keywords*: Steganografy, Image, Python, LSB*

Abstrak

Penggunaan steganografi bertujuan untuk menyamarkan data rahasia sehingga sulit untuk dideteksi, dengan menyisipkan pesan rahasia kedalam citra. Metode paling sederhana yang digunakan untuk menyembunyikan pesan rahasia pada aplikasi ini adalah dengan cara menyisipkan pesan kedalam bit rendah (LSB - *Least Significant Bit*) yaitu dengan cara mengganti tiap-tiap bit pixel pada file citra yang disisipkan. Banyaknya karakter dari pesan rahasia yang dapat ditampung tergantung pada besar kecilnya ukuran dari file citra sebagai tempat penampung. Python adalah bahasa pemrograman yang banyak digunakan oleh developer , Python juga dapat digunakan untuk komputasi dan visualisasi, yaitu dengan menggunakan desain antar muka (*interface*) yang biasa dikenal dengan nama GUI (*Graphical User Interface*).Tujuan yang di harapkan antara lain membangun perangkat lunak steganografi pada citra digital file gambar png dengan menggunakan Python dan menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi dan menghasilkan file gambar yang mempunyai kualitas tidak jauh berbeda dengan citra digital file gambar aslinya.
Kata Kunci: Steganografi, citra digital, python, LSB

JT : Jurnal Teknik
P-ISSN: 2302-8734
E-ISSN: 2581-0006

JT
FT UMT

Vol. 11 No. 01 Th. 2022
Halaman : 62 - 72
Published 27 Juni 2022

PENDAHULUAN

Steganografi merupakan teknik penyembunyian informasi dengan cara penyisipan pada suatu media. Kata steganography (steganografi) berasal dari bahasa Yunani yaitu steganos yang berarti menyembunyikan dan graptos artinya tulisan sehingga arti secara keseluruhan ialah tulisan yang disembunyikan (Permana, 2018).

Perlu diketahui bahwa teknik steganografi berusaha merahasiakan komunikasi dengan cara menyembunyikan pesan ataupun mengkamuflase pesan. Maka sesungguhnya prinsip dasar dalam steganografi lebih dikonsentrasikan pada kerahasian komunikasinya (pesan atau informasi) bukan pada datanya. (Budianto, 2020)

Tujuan yang di harapkan antara lain membangun perangkat lunak steganografi pada citra digital file gambar (jpg) dengan menggunakan aplikasi matlab, dan menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi dan menghasilkan file gambar yang mempunyai kualitas tidak jauh berbeda dengan citra digital file gambar aslinya, sehingga pesan terlihat hanya seperti pesan biasa saja

Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan penerima tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Kata steganography (steganografi) berasal dari bahasa yunani yang artinya "menyembunyikan", dan graptos yaitu "tulisan" (Stellars, 1996). Steganografi merupakan seni penyembunyian pesan ke dalam pesan lainnya sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu di dalam pesan tersebut. (Djuwitaningrum, 2016)

Menurut Bachtiar (2016) dan wicaksana (2019) Metode yang digunakan untuk menyembunyikan pesan pada media digital tersebut berbeda-beda. Contohnya pada file image pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah atau bit yang paling kanan (lsb) pada data pixel yang menyusun file tersebut. Seperti kita ketahui untuk file bitmap 24 bit maka setiap pixel (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111.

Contoh 8 bit pixel :

1 pixel : (00 01 10 11)
white red green blue

Contoh 24 bit pixel :

Contohnya huruf A dapat kita sisipkan dalam 3 pixel, misalnya data raster original adalah sebagai berikut :

(00100111 11101001 11001000)
red blue green
(00100111 11001000 11101001)
red Green blue
(11001000 00100111 11101001)
green Red blue

JT : Jurnal Teknik
P-ISSN: 2302-8734
E-ISSN: 2581-0006

Vol. 11 No. 01 Th. 2022
Halaman : 62 - 72
Published 27 Juni 2022

Sedangkan representasi biner huruf A adalah 100000111. Dengan menyisipkan-nya pada data pixel diatas maka akan dihasilkan :

(00100111	11101000	11001000)
red	green	green
(00100110	11001000	11101000)
white	Green	green
(11001001	00100111	11101001)
blue	Red	blue

Terlihat hanya empat bit rendah yang berubah, untuk mata manusia maka tidak akan tampak perubahannya. Secara rata-rata dengan metode ini hanya setengah dari data bit rendah yang berubah, sehingga bila dibutuhkan dapat digunakan bit rendah kedua bahkan ketiga. (Munir, 2004)

Media penyisipan pesan rahasia yang digunakan dalam teknik Steganografi digital antara lain adalah :

1. Teks

   Dalam algoritma Steganography yang menggunakan teks sebagai media penyisipannya biasanya digunakan teknik NLP sehingga teks yang telah disisipi pesan rahasia tidak akan mencurigakan untuk orang yang melihatnya. Contoh format teks : teks file, html, pdf, dll.
2. Audio

   Format ini pun sering dipilih karena biasanya berkas dengan format ini berukuran relatif besar. Sehingga dapat menampung pesan rahasia dalam jumlah yang besar pula. Contoh format audio : wav, voc, mp3, dll.
3. Citra

   Format pun paling sering digunakan, karena format ini merupakan salah satu format file yang sering dipertukarkan dalam dunia internet. Alasan lainnya adalah banyaknya tersedia algoritma Steganografi untuk media penampung yang berupa citra.

   Contoh format citra : bitmap (bmp), gif, pcx, jpeg, dll.
4. Video

   Format ini memang merupakan format dengan ukuran file yang relatif sangat besar namun jarang digunakan karena ukurannya yang terlalu besar sehingga mengurangi kepraktisannya dan juga kurangnya algor itma yang mendukung format ini. Contoh format video : mpeg, avi dll.

PENILAIAN STEGANOGRAPHY YANG BAIK

Menurut Iswahyudi (2012) Penilaian sebuah algoritma steganografi yang baik dapat dinilai dari beberapa faktor yaitu:

Fidelity. Mutu citra penampung tidak jauh berubah. Setelah penambahan data rahasia, citra hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui jika di dalam citra tersebut terdapat data rahasia.

JT : Jurnal Teknik
P-ISSN: 2302-8734
E-ISSN: 2581-0006

Vol. 11 No. 01 Th. 2022
Halaman : 62 - 72
Published 27 Juni 2022

1. **Robustness**. Data yang disembunyikan harus tahan (robust) terhadap berbagai operasi menipulasi yang dilakukan pada citra penampung, seperti pengubahan kontras, penajaman, pemampatan, rotasi, pembesaran gambar, pemotongan (cropping), enkripsi, dan sebagainya. Bila pada citra penampung dilakukan operasi- operasi pengolahan citra tersebut, maka data yang disembunyikan seharusnya tidak rusak.
2. **Recovery**. Data yang disembunyikan harus diungkapkan kembali (Reveal). Karena tujuan dari steganografi adalah penyembunyian data, maka sewaktu- waktu data rahasia di dalam citra penampung harus dapat diambil kembali untuk dapat digunakan lebih lanjut.

TEKNIK PENGUNGKAPAN DATA

Data yang desembunyikan di dalam citra dapat dibaca kembali dengan cara pengungkapan (Reveal atau Extraction). Posisi byte yang menyimpan bit data dapat diketahui dari bilangan acak yang dibangkitkan. Karena algoritma kriptografi yang digunakan menggunakan kunci pada proses enkripsi, maka kunci yang sama digunakan untuk membangkitkan bilangan acak. Bilangan acak yang dihasilkan sama dengan bilangan acak yang dipakai pada saat penyembunyian data. Dengan demikian, bit- bit data rahasia yang bertaburan di dalam citra dapat dikumpulkan kembali. Berikut contoh langkah-langkah teknik pengungkapan data.

Tabel 1 Keterangan Teknik Pengungkapan Data

Pixel	Gambar Stego (RGB)	Raster data	Bit rendah	Bit Biner	Hasil
[1,1]	46	00101110	0	**01101000**	h
[2,1]	39	00100111	1		
[3,1]	37	00100101	1		
[4,1]	28	00011100	0		
[5,1]	21	00010101	1		
[6,1]	30	00011110	0		
[7,1]	46	00101110	0		
[8,1]	46	00101110	0		

Setelah pixel dari citra steganografi diubah menjadi raster data agar memperoleh bit rendah. Bit-bit tersebut dikumpulkan hingga terbentuk bit biner. Arah bacanya adalah atas ke bawah dan kiri ke kanan. Setiap 8 bit biner merepresentasikan sebuah karakter. Setelah semua bit biner diubah menjadi karakter, akan diperoleh pesan yang tersembunyi.

METODE PENELITIAN

Sistem steganografi yang dibahas akan di fokuskan kepada bagaimana cara membangun suatu sistem steganografi pada citra digital file gambar yang efisien dan untuk mengeksploitasi keterbatasan sistem penglihatan manusia dengan cara menurunkan kualitas warna pada file gambar yang belum disisipi pesan rahasia. Sehingga dengan keterbatasan tersebut manusia sulit menemukan gradasi penurunan kualitas warna file gambar yang telah disisipi pesan rahasia. Sistem ini terdiri dari dua buah sub sistem yaitu: sistem penyisipan dan sistem pengekstrakkan.

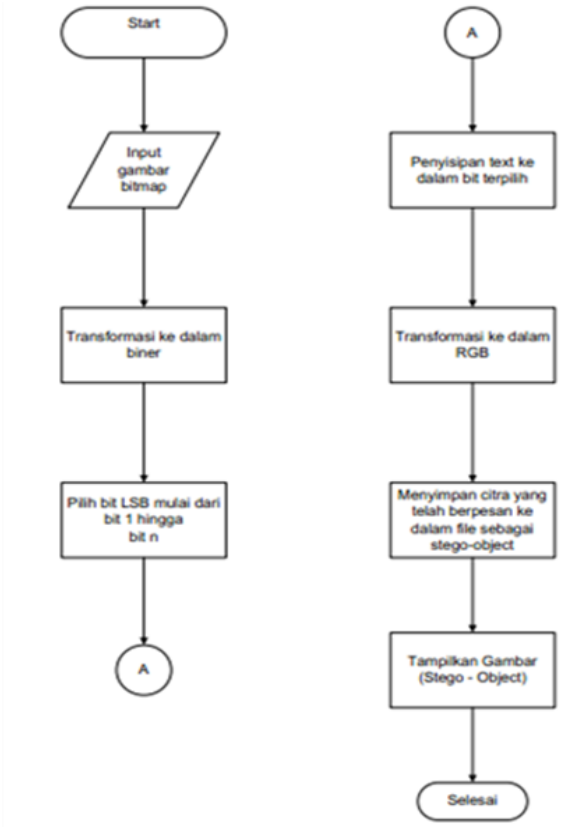
Sistem penyisipan berfungsi untuk melakukan proses penyembunyian pesan ke file

JT : Jurnal Teknik
P-ISSN: 2302-8734
E-ISSN: 2581-0006

Vol. 11 No. 01 Th. 2022
Halaman : 62 - 72
Published 27 Juni 2022

citra digital gambar. Komponen dari sistem penyisipan ini yaitu terdapat komponen untuk menuliskan pesan yang dipakai untuk menempatkan penulisan pesan rahasia.

Sistem pengekstrakkan berfungsi untuk melakukan pengekstrakkan file untuk memperoleh pesan yang telah disisipkan ke dalam file gambar tersebut. Komponen pada sistem pengekstrakkan ini terdapat komponen untuk membaca baca pesan yang digunakan untuk menempatkan pesan rahasia yang akan dibaca, sehingga keluarannya akan memulai proses pemisahan pesan rahasia dari file gambar.



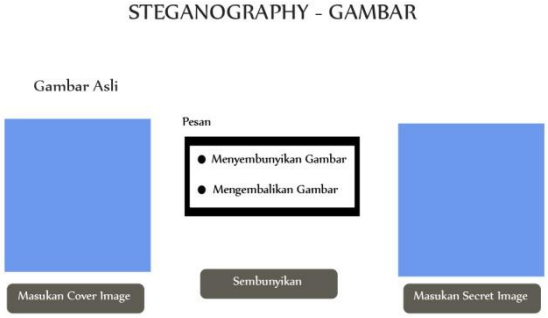
Gambar 1 - Diagram alir proses penyisipan pesan

JT : Jurnal Teknik
P-ISSN: 2302-8734
E-ISSN: 2581-0006

Vol. 11 No. 01 Th. 2022
Halaman : 62 - 72
Published 27 Juni 2022

Gambar 2 - Diagram alir proses ekstrasi pesan

Berikut merupakan rancangan interface aplikasi steganografi:



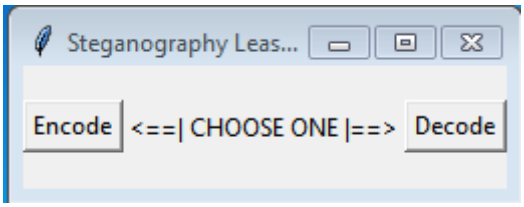
Gambar 3 Rancangan interface aplikasi steganografi

HASIL DAN PEMBAHASAN

Adapun tampilan input dari program yang di buat adalah:

1. Menu Utama

Pada tampilan menu utama, fungsinya untuk memilih encode atau decode

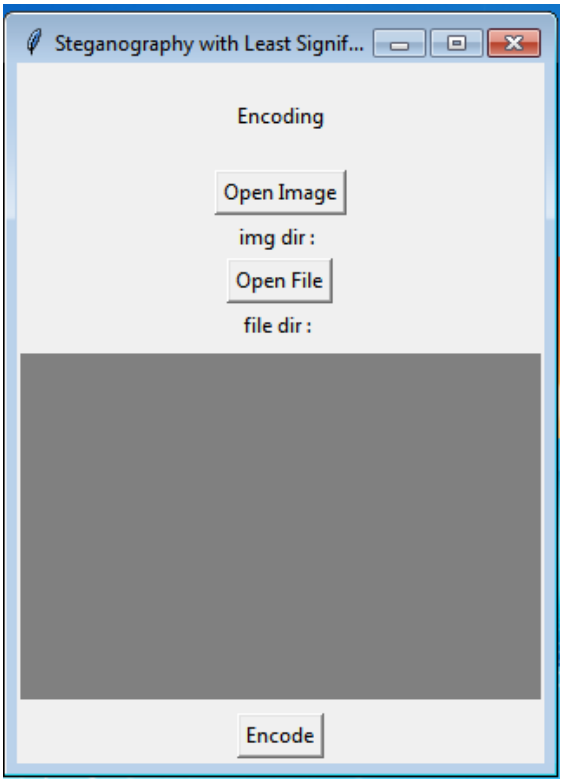


Gambar .4. Menu Utama

JT : Jurnal Teknik
P-ISSN: 2302-8734
E-ISSN: 2581-0006

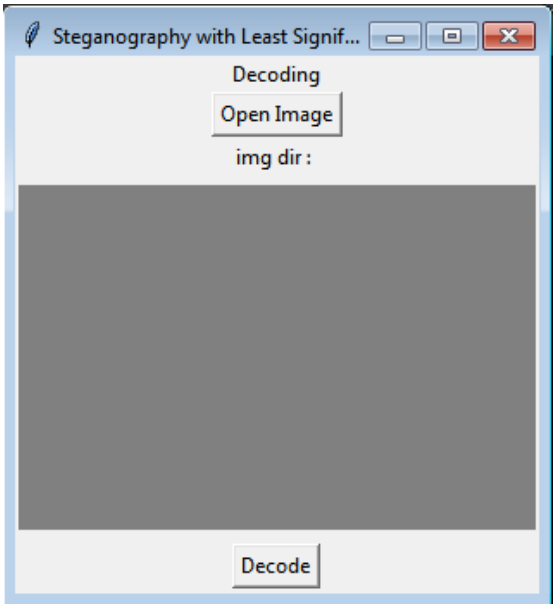
Vol. 11 No. 01 Th. 2022
Halaman : 62 - 72
Published 27 Juni 2022

2. Menu Encoding
Tampilan menu encoding untuk melakukan pengamanan gambar ke gambar.



Gambar 5. Menu Enodingi

3. Menu Dekoding
Tampilan menu decode file yang telah di sembunyikan dalam stego object.



Gambar 6. Menu Decoding

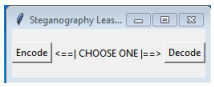
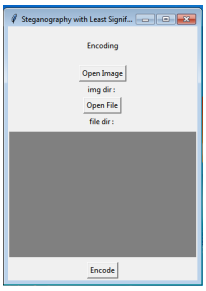
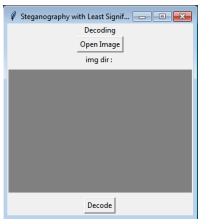
JT : Jurnal Teknik
P-ISSN: 2302-8734
E-ISSN: 2581-0006

Vol. 11 No. 01 Th. 2022
Halaman : 62 - 72
Published 27 Juni 2022

TABLE PENGUJIAN BLACK BOX

A. Menu Utama

Tabel 2. *Blackbox Testing*

NO	Skenario Pengujian	Hasil Yang Diharapkan	Kesimpulan
1	Klik Opsi Encode Test case : 	Sistem akan masuk menampilkan page encoding 	Valid
2	Klik Opsi Decode	Sistem masuk ke page decoding 	Valid

B. Menu Encode

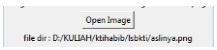
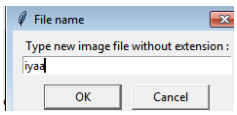
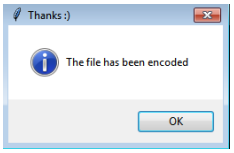
Tabel 3. Encode

No	Skenario Pengujian	Hasil Yang Diharapkan	Kesimpulan
1	Masuk Di Bagian Encoding , klik opsi Open Stego Object	 Berhasil menampilkan gambar	VALID

JT : Jurnal Teknik
P-ISSN: 2302-8734
E-ISSN: 2581-0006

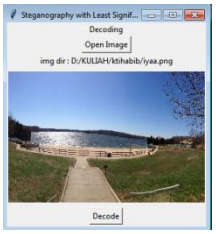
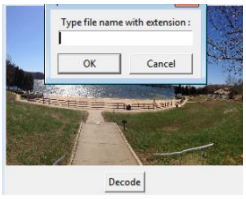
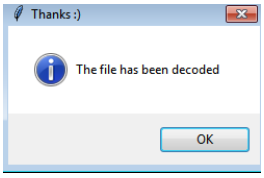
JT FT UMT

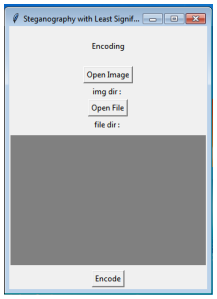
Vol. 11 No. 01 Th. 2022
Halaman : 62 - 72
Published 27 Juni 2022

2	Klik Opsi Open Image untuk gambar yang disembunyikan	 Membuka gambar yang akan disembunyikan	VALID
3	Klik Encode Pada Menu Encoding	 Muncul verifikasi untuk memberi nama file	VALID
4	Test case : Setelah Encoding selesai maka muncul notifikasi	 File has been encoded	VALID

C. Menu Decoding

Tabel 3. Decoding

No	Skenario Pengujian	Hasil Yang Diharapkan	Kesimpulan
1	Masuk Menu Decode dan pilih opsi Open Image Stego Object	 Menampilkan Gambar stego object	VALID
2	Klik Opsi Decode	 Setelah Proses Decode Maka Muncul Notifkasi verifikasi nama file dengan ekstensi .png	VALID
3	Test case : Setelah proses selesai makamuncul notifikasi	 The fle has been decoded	VALID

4	Test case: Aplikasi Tidak bisa Kembali ke menu awal		TIDAK VALID

UCAPAN TERIMA KASIH

Penelitian ini dapat dilaksanakan dengan baik berkat bantuan dari berbagai pihak, untuk itu peneliti mengucapkan terima kasih kepada Universitas Multimedia Nusantara atas dukungan dan bantuan yang telah diberikan selama proses penulisan artikel ini.

SIMPULAN DAN SARAN

A. Kesimpulan

Dari hasil-hasil analisis tersebut, maka di dapatkan kesimpulan:

1. Dengan menggunakan metode Least Significant Bit (LSB) yaitu suatu metode penyembunyian pesan rahasia melalui media digital file image, maka aplikasi steganografi tersebut dapat di bangun yaitu dengan cara mengganti bit ke-8, 16, dan 24 pada representasi biner file image bmp 24-bit dengan representasi biner pesan rahasia yang akan disembunyikan.
2. Efisiensi yang didapatkan antara lain tidak mengubah ukuran citra file gambar tersebut dan tidak mudah untuk mengetahui dan membedakan dengan menggunakan indera penglihatan manusia antara citra file gambar yang asli dengan citra file gambar yang sudah disisipkan pesan rahasia.
3. Kualitas yang di hasilkan mempunyai kualitas yang tidak 3. Kualitas yang di hasilkan mempunyai kualitas yang tidak jauh berbeda dengan citra digital file gambar aslinya.

B. Saran

1. Untuk pengembangan aplikasi ini dapat ditambahkan fitur – fitur tambahan semisal button untuk melakukan perintah back
2. Untuk penambahan fungsi pada aplikasi, perlu dikembangkan algoritma baru bisa dengan musik file dan lainnya

DAFTAR PUSTAKA

Bachtiar, Adam R. Fakhrul, Firman N. 2018. Pemrograman Berorientasi Objek Menggunakan Java. Bandung: Informatika.

Budianto, C. D, Wicaksana, A, dan Hansun, S, 2020 "Elliptic Curve Cryptography and LSB Steganography for Securing Identity Data," in ACIT 2019: Applied Computing and Information Technology, Springer, vol. 847, 2020, pp. 111–127, doi: 10.1007/978-3-030-25217-5 9.

Djuwitaningrum, E.R. dan Apriyani, M. 2016. Teknik Steganografi Pesan Teks Menggunakan Metode Least Significant Bit dan Algoritma Linear Congruential Generator. Jurnal Informatika, 4(2): 79-85.

Iswahyudi, C., Setyaningsih, E., 2012. Pengamanan Kunci Enkripsi Citra Pada AlgoritmaSuper Enkripsi Menggunakan Metode End Of File. Jurnal Prosiding NasionalAplikasi Sains & Teknologi (SNAST) Periode III.

Munir, Rinaldi. 2004. Pengolahan Citra Digital dengan Pendekatan Algoritmik. Bandung: Informatika.

Permana, A A, 2018, APLIKASI PENYISIPAN TEKS PADA GAMBAR DENGANALGORITMA BLOWFISH DAN LEAST SIGNIFICANT BIT, JurnalInformatika Vol 1 No 1 ISSN : 2549 : 0710

Wicaksana, A, dan Maria I P. 2019 "Digital Watermarking for Color Image Using DHWT and LSB." 2019 5th International Conference on New Media Studies (CONMEDIA). IEEE, 2019.