JURNAL SINTAKS LOGIKA Vol. 2 No. 1 , Januari - 2022
https://jurnal.umpar.ac.id/index.php/sylog

E-ISSN : 2775-412X

APLIKASI STEGANOGRAPHY PDF TO IMAGE DENGAN METODE SPREAD SPECTRUM

Marlina[1*], Nurrahmi Wahyuni[2]

[1,2]Program Studi Teknik Informatika, Universitas Muhammadiyah Parepare, Indonesia
marlinairvan85@gmail.com, nurrahmiw@gmail.com

Informasi Artikel

Riwayat Artikel:

Dikirim *Author* : 9-11-2021
Diterima Redaksi : 10-12-2021
Revisi *Reviewer*: 12-12-2021
Diterbitkan *online*: 18-01-2022

Keywords:

Steganography; PDF; JPG; Spread Spectrum

ABSTRACT

Data/information sent via the internet is still vulnerable to theft and eavesdropping. Therefore we need a way to secure the data / information to be sent. Steganography is a technique that can be used to secure data/information. Steganography is a technique used to hide messages in a medium such as images, audio and video. Based on these problems, the authors make a steganography application that can be used to hide PDF files into image media (cover image), and can be used to retrieve PDF from images that have been inserted (Stegano Image). The image media used as input (cover image) is in JPG format. The algorithm used to hide and retrieve PDFs and from images is Spread Spectrum. As for testing the system, the results are in accordance with what has been targeted, the results show that encryption and decryption are carried out by testing the table 5 times.

Kata kunci:

Steganografi; PDF; JPG; Spread Spectrum

ABSTRAK

Data/informasi yang dikirim melalui *internet* masih rawan terhadap pencurian dan penyadapan. Oleh karena itu dibutuhkan cara untuk mengamankan data/informasi yang akan dikirim. Steganografi merupakan salah satu teknik yang dapat digunakan untuk mengamankan data/informasi. Steganografi adalah teknik yang digunakan untuk menyembunyikan pesan ke dalam suatu media seperti gambar, *audio* dan *video*. Berdasarkan permasalahan tersebut maka penulis membuat Aplikasi steganografi yang dapat digunakan menyembunyikan *file PDF* ke dalam media gambar (*image cover*), dan dapat digunakan untuk mengambil kembali *PDF* dari gambar yang telah disisipi (*Stegano Image*). Media gambar yang digunakan sebagai *input* (*cover image*) berformat JPG. Algoritma yang digunakan untuk menyembunyikan dan pengambilan *PDF* dan dari gambar adalah *Spread Spectrum*. Adapun pengujian sistemnya mendapatkan hasil yang sesuai dengan apa yang telah ditargetkan, hasil penelitian menunjukkan bahwa enkripsi dan dekripsi dilakukan dengan pengujian tabel sebanyak 5 kali.

Penulis Korespondensi:

Marlina,
Program Studi Teknik Informatika,
Universitas Muhammadiyah Parepare,
Jl. Jenderal Ahmad Yani KM 6, Parepare
Email: marlinairvan85@gmail.com

I. PENDAHULUAN

Teknologi informasi (dan komunikasi) saat ini adalah bagian penting dalam manajemen informasi. Salah satu pekerjaan manusia yang akan sangat terbantu dengan hadirnya teknologi informasi, dengan keuntungan yang ditawarkan yaitu pekerjaan manusia dalam menyembunyikan data atau pesan [2]. Untuk melakukan proses pengiriman pesan biasanya dibutuhkan suatu cara dalam menjaga keamanan pesan tersebut, agar pesan tidak mudah diketahui oleh orang lain [1].

Perkembangan dan kemajuan teknologi komunikasi digital yang pesat, terdapat banyak kemungkinan tindak kejahatan digital yang terus bertambah dan berkembang. Tindak kejahatan digital berupa pencurian maupun penyadapan informasi adalah beberapa isu ancaman keamanan yang harus diamati dan diperhatikan untuk diminimalisir [7]. Pada steganografi

ada 3 hal penting yang perlu diperhatikan yaitu : *imperceptibility, fidelity, recovery* [9]. Kata steganografi (*steganography*) berasal dari bahasa Yunani yang terdiri dari kata *steganos* yang artinya tersembunyi dan *graphein* yang artinya menulis, sehingga bisa diartikan sebagai tulisan yang tersembunyi [1].

Teknik *Steganography* ini mempunyai beberapa metode yang digunakan untuk mengamankan suatu data atau pesan salah satunya adalah metode *spread spectrum*. Metode *Spread Spectrum* mentransmisikan sebuah sinyal pita informasi yang sempit kedalam sebuah kanal pita lebar dengan penyebaran frekuensi. *Spread spectrum image steganography* adalah metode yang menempatkan informasi di dalam derau semua keseluruhan *cover image*. Penggunaan *file image* sebagai salah satu media *steganography* merupakan langkah yang baik. Lalu lintas pertukaran *file image* di internet merupakan hal biasa, sehingga *steganography* menggunakan *file image* adalah teknik yang baik untuk mengamankan pesan rahasia melalui media internet. Semakin sering file itu atau semakin terlihat file itu maka akan semakin kecil kecurigaan bahwa terdapat pesan tersembunyi dalam file tersebut [2].

Adapun hasil dari penelitian sebelumnya adalah sebagai berikut :

Penelitian ini ditulis oleh Aditya Aziz Fikhri, Hendrawaty pada tahun 2018 dengan judul "Implementasi Steganografi *Text To Image* menggunakan metode *One Bit Least Significant Bit* Berbasis *Android*". Penelitian ini membahas tentang implementasi steganografi pada *smartphone Android* yang dapat digunakan menyembunyikan pesan teks ke dalam media gambar RGB 24 bit *(cover image)*, dan dapat juga digunakan untuk mengambil kembali pesan teks dari gambar RGB 24 bit yang telah disisipi (*Stego image*). Media Gambar yang digunakan sebagai *input (cover image)* berformat JPEG/PNG. Algoritma yang digunakan untuk penyembunyian dan pengambilan pesan teks ke dan dari gambar adalah *One bit Least Significant Bit* [3]. Penelitian ini ditulis oleh Pujianto pada tahun 2017 dengan judul "Model Keamanan Pesan pada Video menggunakan metode *One's Complement Cryptography dan Track Free Atom Steganography* 1". Penelitian ini membahas tentang penyisipan pesan pada video mp4 menggunaan algoritma track free atom berhasil dilakukan dengan baik, bahkan tanpa mempengaruhi kualitas audio dan gambar yang ada didalamnya dikarenakan atom yang digunakan untuk menyimpan sample audio dan gambar tidak dirubah.

Penelitian ini ditulis oleh Dian Hafidh Zulfikar pada tahun 2018 dengan judul "Keamanan Pesan Rahasia Menggunakan Steganografi DCT (*Discrete Cosine Transform*) pada Citra JPEG". Penelitian ini membahas tentang penerapan proses steganografi pada kawasan dct juga akan dilakukan pengujian. Pengujian tersebut meliputi pengujian terhadap kualitas citra apakah setelah disisipkan pesan mengalami penurunan kualitas atau tidak dan ketahanan citra stego untuk melihat apakah pesan yang disisipkan masih dapat diekstrak meskipun gambar mengalami beberapa perubahan [10].

Berdasarkan uraian dan permasalahan diatas, penulis bertujuan untuk membuat aplikasi steganografi dengan metode *Spread Spectrum* yang dapat menyisipkan pesan *file* berformat *PDF* ke dalam *file image* menggunakan bahasa pemrograman *PHP* sehingga pesan tersebut dapat terjaga kerahasiaannya.

II. METODOLOGI PENELITIAN

A. Tempat dan Waktu Penelitian

Tempat penelitian dilakukan di Universitas Muhammadiyah Parepare. Waktu yang dibutuhkan dalam pelaksanaan penelitian ini adalah ± 4 bulan.

B. Jenis Penelitian

Jenis penelitian yang dilakukan merupakan penelitian eksperimental, yaitu penelitian yang pengumpulan datanya melalui pencatatan secara langsung dari hasil percobaan yang dilakukan.

C. Pengumpulan Data

1) Secara tidak langsung (*Studi Literatur*)
   Metode tidak langsung ini maksud ialah mengumpulkan data-data tentang *Steganography* maupun informasi yang terkait seperti artikel yang berasal dari media internet.
2) Secara Langsung (*Observasi*)
   Metode secara langsung yaitu mengumpulkan data-data atau informasi yang terkait dengan perancangan program aplikasi *Steganography.*

D. Alat dan Bahan Penelitian

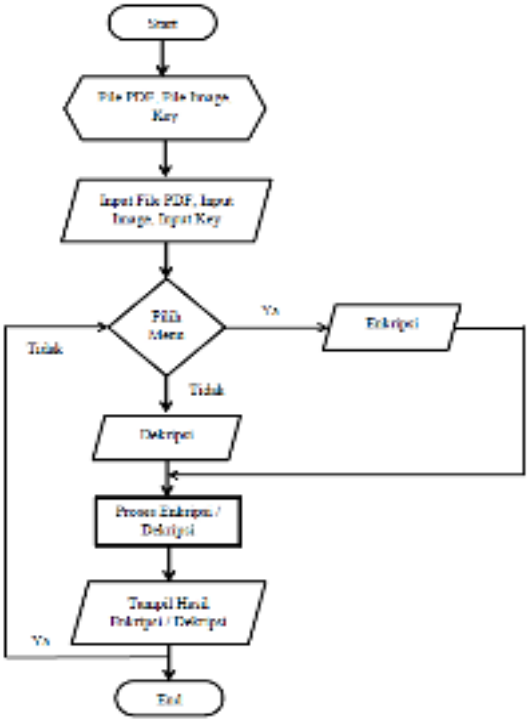
Untuk melakukan proses penelitian dalam pembuatan aplikasi, maka diperlukan perangkat keras dan perangkat lunak guna mendukung kegiatan penelitian tersebut. Berikut ini merupakan penjelasan dari *hardware* dan *software* yang

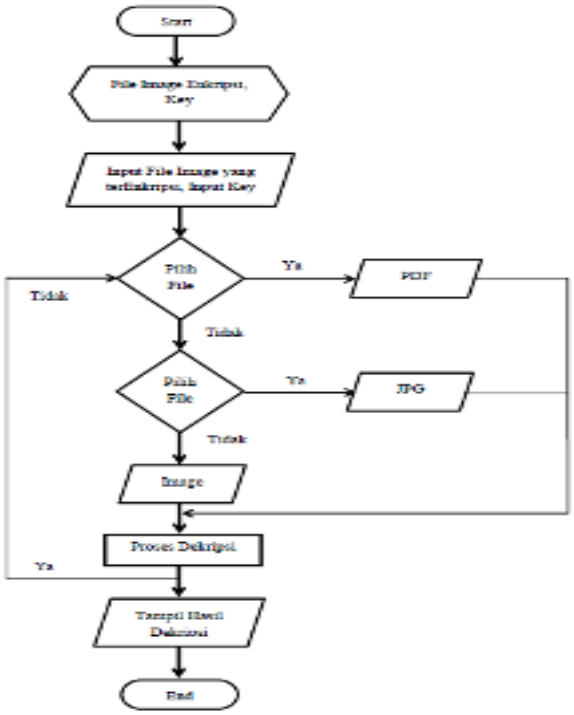
digunakan dalam pembuatan aplikasi *Steganography* ini.

Tabel 1. Hardware dan Software

Perangkat Keras (*Hardware*)	
Laptop	Acer Aspire E14
Processor	*Intel®Core™ i5-4210U @ 1.70GHz 2.40 GHz*
RAM	*4 GB*
Harddisk	*500 GB*
OS	*Windows 10 64-bit*
Perangkat Lunak (*Software*)	
Xampp	
Sublime Text 3	
Browser Google Chrome	

E. Rancangan Penelitian





Gambar 1. Flowchart Aplikasi

Perancangan model *UML* (*Unified Modelling Language*) Sistem yang penulis rancang adalah sistem berupa enkripsi dan dekripsi *file pdf* dan *image.* Adapun dalam melakukan perancangan sistem adalah dengan memanfaatkan *Diagram UML* berupa *Usecase diagram, Activity diagram,* dan *Sequence diagram*.

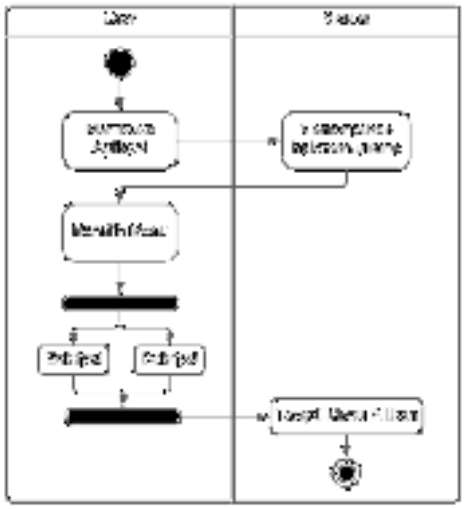
1) *Use case diagram*

   Use Case diagram berfungsi untuk menjelaskan alur sistem jika dilihat menurut pandangan orang yang berada diluar sistem.

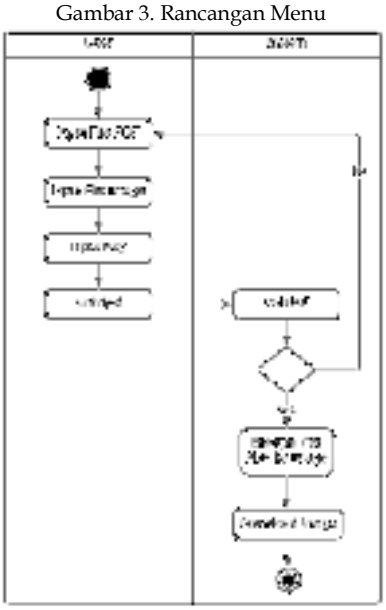
Gambar 2. Rancangan *Usecase Diagram*

2) *Activity diagram*

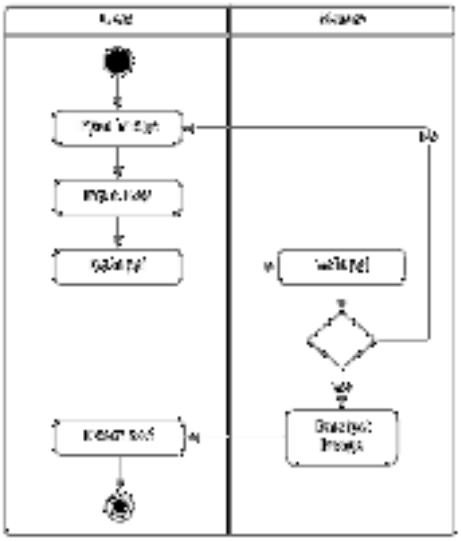
Activity diagram memodelkan alur kerja (*workflow*) sebuah proses dan urutan dalam suatu proses. *Activity diagram* pada sistem yang penulis rancang antara lain :



Gambar 3. Rancangan Menu



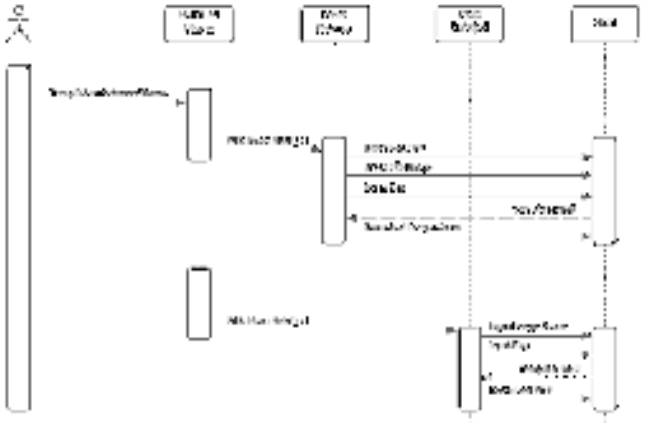
Gambar 4. Rancangan Menu Enkripsi



Gambar 5. Rancangan Menu Dekripsi

3) *Sequence diagram*

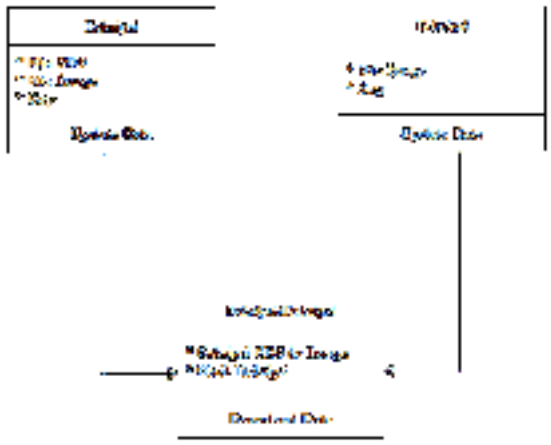
Sequence diagram adalah suatu diagram yang menggambarkan interaksi antara objek dan mengkondisikan komunikasi antara objek-objek tersebut. Berikut *sequence diagram* aplikasi yang akan dibangun.



Gambar 6. Rancangan Aplikasi yang Dibangun

4) *Class diagram*

Class diagram adalah jenis diagram struktur statis yang menggambarkan struktur sistem dengan menunjukkan system *class,* atribut, metode, dan hubungan antar objek. Berikut *Class Diagram* yang dirancang :



Gambar 7. *Class Diagram*

III. HASIL DAN PEMBAHASAN

A. *Rancangan Aplikasi*

1) *Halaman Utama*

Gambar 8. Halaman Utama

Halaman Utama atau yang lebih dikenal sebagai *user interface* adalah media yang menghubungkan manusia dengan komputer agar dapat saling berinteraksi

2) *Halaman Menu Enkripsi*

Gambar 9. Halaman Menu Enkripsi

Pada halaman menu enkripsi ini digunakan untuk mengenkripsi *file pdf* ke *file image*. Langkah pertama yang harus dilakukan adalah dengan meng*input* atau *upload file pdf* dan *file image*, lalu meng*input key* atau *password*. Setelah itu, enkripsi dengan menekan tombol Enkripsi.

3) *Halaman Menu Hasil Enkripsi*

Gambar 10. Halaman Menu Hasil Enkripsi

Pada halaman ini digunakan untuk menampilkan hasil dari *file pdf* yang sudah di enkripsi ke dalam *image*. Maka *spectrum* gambar sebelum dan sesudah di enkripsi akan mengalami perubahan dikarenakan gambar awal telah disisipkan file pdf, dan perubahannya tergantung dari hasil *spread spectrum*-nya.

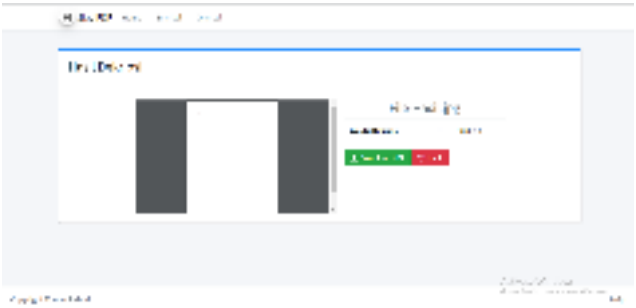
4) *Halaman Menu Dekripsi*

Gambar 11. Halaman Menu Dekripsi

Pada halaman menu dekripsi ini digunakan untuk mendekripsi *file cover image*. Langkah pertama yang dilakukan *input cover image* yang sudah terenkripsi,

lalu meng*input key* atau *password* sesuai dengan *key* yang telah terenkripsi ke dalam *cover image*, lalu menekan tombol dekripsi untuk memulai proses Dekripsi.

5) *Halaman Menu Hasil Dekripsi*



Gambar 12. Halaman Menu Hasil Dekripsi

Pada halaman ini digunakan untuk menampilkan hasil dari *file cover image* yang sudah di dekripsi.

B. *Pengujian Sistem*

Pengujian aplikasi dilakukan dengan menggunakan metode pengujian yaitu pengujian *blackbox, whitebox* dan tabel hasil pengujian.

1) *Pengujian Blackbox*

Pengujian *Blackbox* (*blackbox testing*) adalah salah satu metode pengujian yang berfungsi pada sisi fungsionalitas yang ada dalam sistem. Kemudian membandingkan hasil keluaran sistem dengan hasil yang diharapkan. Bila hasil yang diharapkan sesuai dengan hasil pengujian, artinya aplikasi sesuai dengan desain yang telah ditentukan sebelumnya. Jika belum sesuai maka perlu dilakukan pengecekan lebih lanjut dan perbaikan.

Gambar 13. Berhasil Terenkripsi

Gambar 14. Bukan *File PDF* yang Diinput

Gambar 15. Bukan *File JPG* yang Diinput

Gambar 16. Gagal Terenkripsi

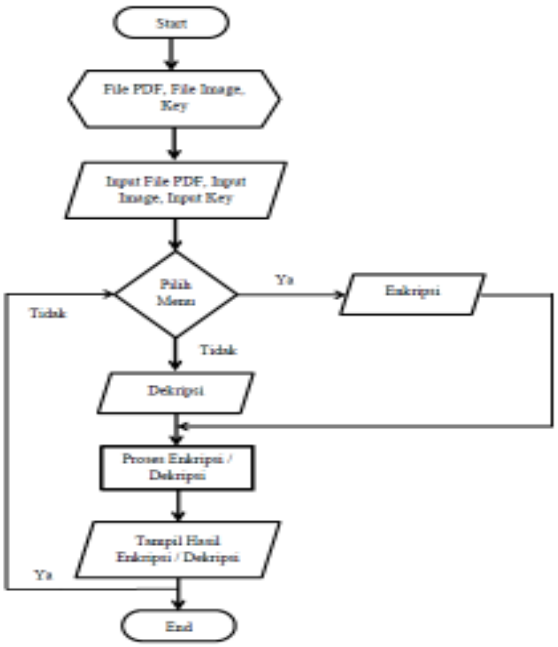
Gambar 17. Berhasil Terdekripsi

Gambar 18. Bukan *Cover Image JPG*

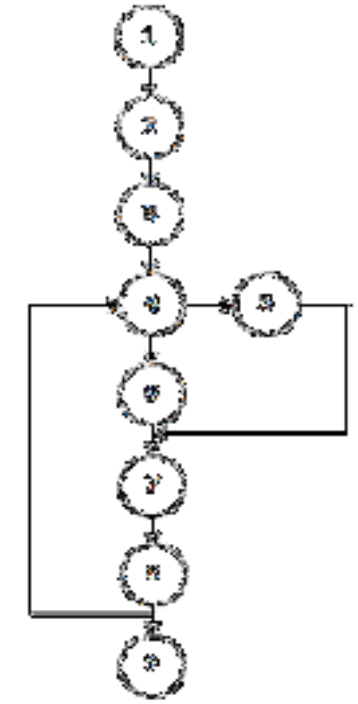
Gambar 19. *Password/Key* Salah

2) *Pengujian Whitebox*

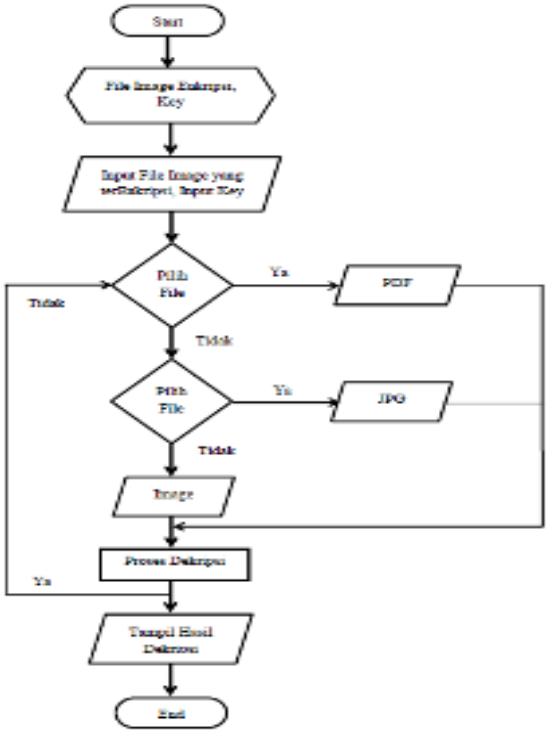
Pada tahap pengujian *White Box,* dilakukan pengujian terhadap pengecekan kode program yang digunakan pada aplikasi ini. Pengujian *White Box* dilakukan untuk memastikan bahwa aplikasi dapat berjalan dengan lancar dan tidak terdapat kesalahan dalam logika pemrograman.



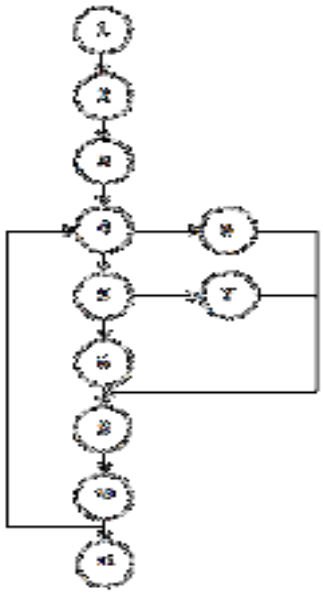
Gambar 20. *Flowchart* Enkripsi



Gambar 21. *Flowgraph* Enkripsi



Gambar 22. *Flowchart* Dekripsi



Gambar 23. *Flowgraph* Dekripsi

3) Pengujian Akurasi

Adapun proses pengujian akurasi yang telah dilakukan sebanyak 5 kali percobaan pada aplikasi, untuk mengetahui persentase kesalahan dengan rumus sebagai berikut :

Presentasi Kesalahan *:* $\frac{\text{Jumlah bilangan yang sesuai}}{\text{Jumlah bilangan yang dicoba}}$ X 100%

Tabel 2. Hasil Pengujian Enkripsi

Sebelum Enkripsi	Sesudah Enkripsi	Ukuran PDF	UG Awal - Akhir	Berhasil atau Gagal
		2.72 kb	7.39 kb – 147 kb	Berhasil
		4.46 kb	12.5 kb – 147.2 kb	Berhasil
		233 kb	124 kb – 124 kb	Gagal
		278 kb	54.9 kb – 54.9 kb	Gagal

Tabel 3. Hasil Pengujian Dekripsi

File Cover	Ukuran File Cover	Waktu Eksekusi
	147 kb	1 detik
	147,2 kb	1 detik
	124 kb	0 detik
	54.9 kb	0 detik

IV. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan oleh penulis maka dapat ditarik kesimpulan yaitu : Pembuatan aplikasi steganografi ini menggunakan Metode *spread spectrum* dalam mengenkripsi/dekripsi sebuah pesan rahasia ke dalam gambar berformat *jpg*, media yang digunakan yaitu *file* pdf, sistem ini dibangun menggunakan aplikasi *Sublime Text 3* sebagai rancangan aplikasinya, dan untuk tampilan nya menggunakan *web browser*. Adapun pengujian sistemnya mendapatkan hasil yang sesuai dengan apa yang telah ditargetkan. Aplikasi ini dibuat dengan tujuan dapat membantu penggunanya untuk mengirimkan sebuah data-data yang bersifat rahasia, agar pesan dapat sampai ke tangan penerima tanpa menimbulkan kecurigaan pada pihak lain. Hasil penelitian menunjukkan bahwa enkripsi dan dekripsi dilakukan dengan pengujian tabel sebanyak 4 kali, diperoleh kesimpulan pada saat enkripsi yaitu 100% yang dimana resolusi dari *cover image*

harus lebih besar dari *file pdf* yang ingin disisipkan, apabila resolusi *cover* lebih kecil maka akan gagal ketika di enkripsi.

REFERENSI

[1] Anshori, Yusuf, AY Erwin Dodu, and Megawati Purwaningsih. "Aplikasi Steganografi pada Media Citra Digital Menggunakan Metode Least Significant Bit (LSB)." *Sains dan Teknologi Informasi.,* vol.5. No.1, hlm.1-10, Juni 2019.(https://doi.org/10.33372/stn.v5i1.435).

[2] K. Donavan, E. Ekojono, and I. F. Rozi, "Aplikasi Steganography untuk Enkripsi Image to Image dengan Metode Spread Spectrum", *JIP*, vol. 1, no. 3, hlm. 29, Mar. 2017.. (https://doi.org/10.33795/jip.v1i3.110).

[3] Fikhri, Aditya Aziz, and Hendrawaty Hendrawaty. "Implementasi Steganografi Text To Image Menggunakan Metode One Bit Least Significant Bit Berbasis Android." *Jurnal Infomedia: Teknik Informatika, Multimedia & Jaringan* .,Vol.3.No.1 hlm.10-17,2018. (https://dx.doi.org/10.30811/jim.v3i1.623).

[4] N. F. Hasan, C. N. Dengen, and D. Ariyus, "Analisis Histogram Steganografi Least Significant Bit Pada Citra Grayscale", *Digitalzone*, vol. 11, no. 1, hlm. 20-29, May 2020. (https://doi.org/10.31849/digitalzone.v11i1.3413).

[5] L. Malese, "Penyembunyian Pesan Rahasia Pada Citra Digital dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (LSB)", *jiwp*, vol. 7, no. 5, hlm. 343-354, Sep. 2021.(https://doi.org/10.5281/zenodo.5563416).

[6] Mardiansyah, Arief, and Yusfrizal Yusfrizal. "APLIKASI PENYISIPAN PESAN PADA GAMBAR MENGGUNAKAN SPREAD SPECTRUM DAN GOST BERBASIS ANDROID." *IT (INFORMATIC TECHNIQUE) JOURNAL* Vol. 8 No.1 hlm.81-92. April 2020.(http://dx.doi.org/10.22303/it.8.1.2020.81-92).

[7] Saidah, Sofia, Nur Ibrahim, and Mochammad Haldi Widianto. "Pengamanan Pesan pada Steganografi Citra dengan Teknik Penyisipan Spread Spectrum." *ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika* Vol.7.No.3 hlm. 544. 2019(http://dx.doi.org/10.26760/elkomika.v7i3.544).

[8] Sianturi, Tri Nusanti, and Rinaldo Gomgom Hutagaol. "Penyisipan Pesan Rahasia Kedalam Audio Menggunakan Algoritma F5." *Seminar Nasional Teknologi Komputer & Sains (SAINTEKS)*. Vol. 1. No. 1. hlm.890-893. Januari 2019. (http://dx.doi.org/10.30700/.v1i1.788)

[9] S. Reno, "Algoritma Steganografi dengan Metode Spread Spectrum Berbasis PCMK", *JURNAL MULTIMEDIA NETWORKING INFORMATICS*, vol. 3, no. 2, hlm. 32–37, Nov. 2017. (https://doi.org/10.32722/multinetics.v3i2.1125).

[10] Zulfikar, Dian Hafidh. "Keamanan Pesan Rahasia Menggunakan Steganografi DCT (Discrete Cosine Transform) pada Citra JPEG." *Jurnal Informatika Global* Vol.9 No.2, hlm.118-123 Desember 2019. (http://dx.doi.org/10.36982/jiig.v9i2.585).