

**RANCANG BANGUN SISTEM PENGAMANAN DOKUMEN
PENGAJUAN HAK PATEN DENGAN MENGGUNAKAN METODE
STEGANOGRAFI LINE SHIFTING**

LAPORAN TUGAS AKHIR

Laporan ini Disusun Guna Memenuhi Salah Satu Syarat Memperoleh Gelar Sarjana Strata (S1) pada Program Studi Teknik Informatika Fakultas Teknologi Industri Universitas Islam Sultan Agung Semarang



DISUSUN OLEH

AHMAD SAIFURROHMAN

NIM 32601800003

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM SULTAN AGUNG
SEMARANG**

2022

FINAL PROJECT

**DESIGN A SYSTEM PATENT DOCUMENT SECURITY USING THE LINE
SHIFTING STEGANOGRAPHY METHOD**

*Proposed to complete the requirement to obtain a bachelor's degree (S1) at
Informatics Engineering Departement of Industrial Technology Faculty Sultan
Agung Islamic University*



**MAJORING OF INFORMATICS ENGINEERING
INDUSTRIAL TECHNOLOGY FACULTY
SULTAN AGUNG ISLAMIC UNIVERSITY
SEMARANG**

2022

LEMBAR PENGESAHAN PEMBIMBING

Laporan Tugas Akhir dengan judul “RANCANG BANGUN SISTEM PENGAMANAN DOKUMEN PENGAJUAN HAK PATEN DENGAN MENGGUNAKAN METODE STEGANOGRAFI LINE SHIFTING” ini disusun oleh

:

Nama : AHMAD SAIFURROHMAN

NIM : 32601800003

Program Studi : Teknik Informatika

Telah disahkan oleh dosen pembimbing pada :

Hari :

Tanggal :

Mengesahkan,

Pembimbing I



Bagus Satrio Waluyo Poetro, S.Kom, M.Cs
NIDN. 1027118801

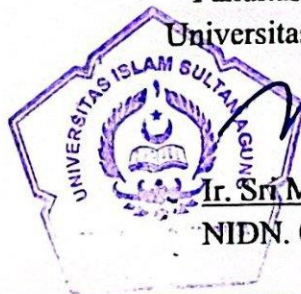
Pembimbing II

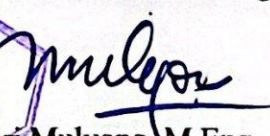


M. Taufik, ST., MIT
NIDN. 0622037502

Mengetahui,

Ketua Program Studi Teknik Informatika
Fakultas Teknologi Industri
Universitas Islam Sultan Agung




Ir. Sri Mulyono, M.Eng
NIDN. 0626066601

LEMBAR PENGESAHAN PENGUJI

Laporan tugas akhir dengan judul “RANCANG BANGUN SISTEM PENGAMANAN DOKUMEN PENGAJUAN HAK PATEN DENGAN MENGGUNAKAN METODE STEGANOGRAFI LINE SHIFTING” ini telah dipertahankan di depan dosen penguji

Tugas Akhir pada :

Hari :


Tanggal :

Penguji I


Dedy Kurniadi, ST., M.Kom
NIDN. 0622058802

TIM PENGUJI

Penguji II


Badie'ah, ST., M.Kom
NIDN. 0619018701

SURAT PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan dibawah ini :

Nama : Ahmad Saifurrohman

NIM : 32601800003

Judul Tugas Akhir : RANCANG BANGUN SISTEM PENGAMANAN DOKUMEN PENGAJUAN HAK PATEN DENGAN MENGGUNAKAN METODE STEGANOGRAFI LINE SHIFTING

Dengan bahwa ini saya menyatakan bsahwa judul dan isi Tugas Akhir yang saya buat dalam rangka menyelesaikan Pendidikan Strata Satu (S1) Teknik Informatika tersebut adalah asli dan belum pernah diangkat, ditulis ataupun dipublikasikan oleh siapapun baik keseluruhan maupun sebagian, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka, dan apabila di kemudian hari ternyata terbukti bahwa judul Tugas Akhir tersebut pernah diangkat, ditulis ataupun dipublikasikan, maka saya bersedia dikenakan sanksi akademis. Demikian surat pernyataan ini saya buat dengan sadar dan penuh tanggung jawab.

Semarang, 28 Februari 2023

Yang Menyatakan,



Ahmad Saifurrohman

KATA PENGANTAR

Dengan mengucapkan syukur alhamdulillah atas kehadiran Allah SWT yang telah memberikan rahmat dan karunianya kepada penulis, sehingga dapat menyelesaikan Tugas Akhir dengan judul “Rancang Bangun Sistem Pengamanan Dokumen Pengajuan Hak Paten Dengan Menggunakan Metode Steganografi Line Shifting” ini untuk memenuhi salah satu syarat menyelesaikan studi serta dalam rangka memperoleh gelar sarjana (S-1) pada Program Studi Teknik Informatika Fakultas Teknologi Industri Universitas Islam Sultan Agung Semarang.

Tugas Akhir ini disusun dan dibuat dengan adanya bantuan dari berbagai pihak, materi maupun teknis, oleh karena itu saya selaku penulis mengucapkan terima kasih kepada:

1. Rektor UNISSULA Bapak Prof. Dr. H. Gunarto, SH., M.Hum yang mengizinkan penulis menimba ilmu di kampus ini.
2. Dekan Fakultas Teknologi Industri Ibu Dr. Novi Marlyana, ST., MT.
3. Dosen pembimbing I penulis Bagus Satrio Waluyo Poetro, S.Kom., M.Cs yang telah meluangkan waktu dan memberi ilmu.
4. Dosen pembimbing II penulis M.Taufik, ST., MIT yang telah memberikan banyak nasehat dan saran.
5. Orang tua penulis yang telah mengizinkan untuk menyelesaikan laporan ini.
6. Dan kepada semua pihak yang tidak dapat saya sebutkan satu persatu.

Dengan segala kerendahan hati, penulis menyadari masih banyak terdapat banyak kekurangan-kekurangan dari segi kualitas atau kuantitas maupun dari ilmu pengetahuan dalam penyusunan laporan, sehingga penulis mengharapkan adanya saran dan kritikan yang bersifat membangun demi kesempurnaan laporan ini.

Semarang, 30 Desember 2022

Ahmad Saifurrohman

DAFTAR ISI

COVER	i
LEMBAR PENGESAHAN PEMBIMBING	iii
LEMBAR PENGESAHAN PENGUJI.....	iv
SURAT PERNYATAAN KEASLIAN TUGAS AKHIR.....	v
PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	x
DAFTAR TABEL	xi
ABSTRAK	xii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah.....	2
1.3 Pembatasan Masalah	2
1.4 Tujuan.....	2
1.5 Manfaat.....	3
1.6 Sistematika Penulisan.....	3
BAB II TINJAUAN PUSTAKA DAN DASAR TEORI	5
2.1 Tinjauan Pustaka	5
2.2 Dasar Teori.....	7
2.2.1 Steganografi.....	7
2.2.2 Line Shifting	9
2.2.3 Encode	9
2.2.4 Decode.....	9
2.2.5 Python.....	10
2.2.6 PyPDF.....	10
2.2.7 Reportlab	11
2.2.8 Flask	11
2.2.9 HTML.....	12

2.2.10	Profil LPPM UNISSULA.....	12
BAB III METODE PENELITIAN		13
3.1	Metode Pengumpulan Data	13
3.1.1	Studi Literatur.....	13
3.1.2	Dokumentasi.....	13
3.1.3	Observasi	13
3.2	Metodologi Perancangan Alur Sistem.....	13
3.2.1	Analisis Kebutuhan	13
3.2.2	Analisis Alur Sistem.....	14
3.2.3	Use Case Diagram.....	18
3.2.4	Activity Diagram.....	18
3.3	Perancangan Antar Muka	20
BAB IV HASIL DAN ANALISIS PENELITIAN		23
4.1	Cara Kerja Sistem.....	23
4.2	Implementasi User Interface.....	26
4.3	Pengujian Sistem	28
4.4	Hasil dan Analisa.....	30
BAB V KESIMPULAN DAN SARAN		31
5.1	Kesimpulan.....	31
5.2	Saran.....	31
DAFTAR PUSTAKA		
LAMPIRAN		

DAFTAR GAMBAR

Gambar 3. 1 Proses Enkripsi.....	15
Gambar 3. 2 Proses Dekripsi.....	16
Gambar 3. 3 Alur Sistem.....	17
Gambar 3. 4 Use Case Diagram.....	18
Gambar 3. 5 Activity Encode.....	19
Gambar 3. 6 Activity Decode	20
Gambar 3. 7 Mockup Halaman Encode.....	21
Gambar 3. 8 Mockup Halaman Decode.....	22
Gambar 4. 1 Tampilan Encode	27
Gambar 4. 2 Tampilan Decode	28



DAFTAR TABEL

Tabel 4. 1 Pengujian Sistem.....	29
----------------------------------	----



ABSTRAK

Dokumen digital merupakan salah satu jenis data yang mudah dikirim dan diduplikasi melalui internet, sehingga rawan terkena serangan. Kemudahan ini bisa dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab untuk melakukan tindakan yang dapat merugikan hak cipta dokumen tersebut. Oleh karena itu, dibutuhkan teknik yang dapat menyembunyikan data dalam media sebagai watermark tanpa mengurangi atau merubah informasi yang adapada dokumen tersebut, teknik ini disebut steganografi. Dengan steganografi, data tersebut tidak terlihat oleh pihak yang tidak berwenang dan tidak menimbulkan kecurigaan terkait dengan keberadaan data tersebut. Saat melakukan uji sistem menggunakan white box, program ini tidak memiliki error saat dijalankan. Dengan percobaan pada lima kasus uji, hanya satu percobaan yang mengalami kegagalan saat di deocde ulang. Yaitu pengujian terhadap dokumen pdf hanya memiliki satu halaman dan pesan disisipkan sebanyak 35 karakter. Dalam penerapan steganografi line shifting untuk dokumen, masih ada karakter yang bukan merupakan karakter pesan yang ikut tercetak pada saat proses decode.

Kata Kunci: Dokumen digital, Steganografi, Line Shifting.

ABSTRACT

Digital documents are one type of data that is easily sent and duplicated through the internet, making it vulnerable to attacks. This convenience can also be exploited by irresponsible parties to infringe on the copyright of the document. Therefore, a technique is needed to hide data in media as a watermark without reducing or changing the information in the document, this technique is called steganography. With steganography, the data is not visible to unauthorized parties and does not raise suspicion about the existence of the data. When testing the system using white box, the program has no errors when run. With testing on five cases, only one test experienced failure during decoding. This is a test on a pdf document with only one page and a message embedded with 35 characters. In the implementation of line shifting steganography for documents, there are still characters that are not message characters that are printed during the decoding process.

Keywords: Digital Document, Steganography, Line Shifting.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan data merupakan hal yang sangat penting untuk menjamin keamanan data digital, perlu ada tindakan preventif yang diambil terhadap kemungkinan pencurian, penyadapan, perusakan, dan pemalsuan oleh pihak-pihak yang tidak berwenang. Dokumen digital merupakan salah satu jenis data yang rawan terkena serangan, karena mudah dikirim dan diduplikasi melalui internet serta mudah disimpan untuk digunakan kembali. Namun, kemudahan tersebut juga dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melakukan tindakan yang merugikan hak cipta dokumen tersebut. Oleh karena itu, dibutuhkan teknik yang dapat mengamankan dokumen teks digital dari serangan yang dapat merusak atau mengambil dokumen tersebut, salah satunya adalah dengan menggunakan teknik steganografi.

Steganografi merupakan teknik yang digunakan untuk menyisipkan data ke dalam media cover, seperti gambar atau citra image, tanpa mengurangi informasi yang ada di dalamnya. Hal ini memungkinkan data tersebut tidak terlihat oleh pihak yang tidak berwenang dan tidak menimbulkan kecurigaan terkait dengan keberadaan data tersebut (Ratama & Munawaroh, 2022).

Line Shifting adalah salah satu metode yang dapat digunakan dalam steganografi untuk menyisipkan pesan atau data ke dalam media digital, terutama dokumen. Dengan menggunakan metode ini, kita dapat mencegah ancaman yang mungkin terjadi dengan menyembunyikan data dalam media tersebut.

Ancaman terhadap integritas data merupakan masalah yang sering terjadi. Untuk mencegah hal ini, maka perlu adanya data atau dokumen sebagai pesan sekaligus watermarking yang disisipkan ke dalam dokumen cover sehingga dokumen pesan tidak dapat terlihat oleh orang lain tanpa adanya bantuan sistem tertentu. Proses dekripsi hanya dapat dilakukan dengan memasukkan kunci yang sama yang digunakan dalam proses enkripsi. Selain itu, metode ini juga dapat digunakan sebagai proses autentikasi untuk memastikan bahwa data tersebut milik

orang yang benar-benar membuatnya, karena kunci harus dimasukkan terlebih dahulu sebelum proses dekripsi dapat dilakukan.

Berdasarkan paparan diatas steganografi dibutuhkan dalam Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) UNISSULA bidang Hak Kekayaan Intelektual dan Komersialisasi khususnya dalam mengamankan dokumen Pengajuan Paten dari orang yang tidak bertanggung jawab. Dengan bantuan steganografi, LPPM UNISSULA dapat mengamankan dokumen tersebut. Berdasarkan latar belakang ini, penulis mengambil judul "Rancang Bangun Sistem Pengamanan Dokumen Pengajuan Hak Paten Dengan Menggunakan Metode Steganografi Line Shifting".

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah dari perancangan sistem adalah bagaimana cara mengamankan dokumen pengajuan hak paten menggunakan metode Steganografi Line Shifting sebagai solusinya ?

1.3 Pembatasan Masalah

Adapun batasan masalah dalam penelitian ini adalah sebagai berikut :

1. Media yang digunakan untuk penelitian merupakan dokumen dengan ekstensi pdf.
2. Aplikasi masih bersifat prototype dengan media dokumen pdf sebagai bahan pengujian.
3. Sistem keamanan yang dibangun hanya untuk mengamankan dokumen di tingkat internal UNISSULA.

1.4 Tujuan

Tujuan dari tugas akhir ini adalah menerapkan teknik steganografi dengan metode Line Shifting untuk mengamankan dokumen pengajuan hak paten yang dimiliki oleh LPPM UNISSULA di bidang Hak Kekayaan Intelektual dan Komersialisasi yang berbasis web. Dengan demikian, diharapkan bahwa dokumen tersebut akan lebih aman dan mudah dienkrpsi demi menjamin keamanannya.

1.5 Manfaat

Manfaat yang diharapkan dari pembuatan sistem ini adalah untuk mengamankan dokumen hak paten yang masih dalam proses pengajuan.

1.6 Sistematika Penulisan

Adapun sistematika penulisan yang digunakan dalam penyusunan laporan tugas akhir adalah sebagai berikut:

BAB 1 : PENDAHULUAN

Bab ini membahas mengenai latar belakang pemilihan judul penelitian, rumusan masalah yang menjadi fokus penelitian, batasan masalah yang digunakan dalam penelitian, tujuan penelitian yang ingin dicapai, metodologi penelitian yang digunakan dalam penelitian tersebut, serta sistematika penulisan yang digunakan dalam penyusunan laporan penelitian.

BAB 2 : TINJAUAN PUSTAKA DAN DASAR TEORI

Bab ini berisi tentang studi literatur yang mencakup penelitian-penelitian sebelumnya yang berkaitan dengan topik tersebut dan landasan teori yang berisi tentang prinsip-prinsip dasar dan konsep teknis yang relevan untuk pengembangan sistem keamanan berbasis web sehingga relevan untuk memahami konsep kerja dari sistem keamanan berbasis web dengan menggunakan bahasa pemrograman dan metode yang telah dipilih.

BAB 3 : METODE PENELITIAN

Bab ini menjelaskan urutan langkah-langkah dalam penelitian yang dimulai dengan perancangan sistem, penjelasan tentang alur kerja sistem, desain aplikasi, dan pengujian aplikasi.

BAB 4 : HASIL DAN ANALISIS PENELITIAN

Pada bab ini, penulis menjabarkan hasil penelitian terkait uji coba encode dan decode dari sistem steganografi.

BAB 5 : KESIMPULAN DAN SARAN

Pada bab ini, penulis menyajikan kesimpulan dari seluruh proses penelitian yang telah dilakukan, serta memberikan saran-saran untuk pengembangan lebih lanjut.



BAB II

TINJAUAN PUSTAKA DAN DASAR TEORI

2.1 Tinjauan Pustaka

Adapun beberapa penelitian sebelumnya yang menjadi bahan pertimbangan dan sumber referensi yang berhubungan dengan judul penelitian ini adalah sebagai berikut:

Penelitian yang berjudul Implementasi Pengamanan Dokumen Menggunakan Metode Steganografi Line-Shifting, dalam penelitian tersebut, telah dilakukan implementasi aplikasi steganografi menggunakan metode Line-Shift Coding yang telah dibangun menggunakan bahasa Java. Aplikasi tersebut berbasis desktop dan dapat digunakan untuk mengamankan file dengan format PDF dan DOCX. Pada proses enkripsi, karakter pesan diubah ke dalam bentuk ASCII dalam kode huruf dan simbol. Kemudian, pesan diubah ke bit biner. Pada tahap ekstraksi, dokumen yang telah di ubah menjadi bentuk enkripsi diubah lagi ke dalam bentuk byte stream, dan kemudian diubah menjadi baris-baris byte. Pencarian jarak yang berbeda di setiap baris dilakukan pada seluruh baris file dokumen. Apabila jarak yang berbeda ditemukan pada baris genap, maka diinterpretasikan sebagai bit 0, dan ketika perbedaan jarak ditemukan di baris ganjil, maka diinterpretasikan sebagai bit 1. Dengan demikian, aplikasi ini dapat digunakan untuk mengamankan dokumen dengan cara menyisipkan pesan rahasia secara tersembunyi pada file dokumen yang tidak terlihat oleh orang lain (Riansyah dkk., 2022).

Penelitian berikutnya yaitu Implementasi Steganografi Pada Media Teks Dengan Metode *Line-Shift Coding* Dan Metode Centroid. Pada saat diuji dengan variasi sudut kemiringan gambar, metode *Line-Shift Coding* menunjukkan hasil yang tidak memuaskan, menandakan bahwa metode tersebut tidak dapat menangani perbedaan sudut kemiringan gambar hal ini disebabkan oleh perubahan arah pergeseran baris pada dokumen steganografi yang disebabkan oleh perubahan hasil perbandingan jarak antar centroid, akibat dari perubahan sudut kemiringan gambar. Karena perbandingan jarak antar centroid berubah, arah pergeseran baris juga dapat mengalami penyimpangan. Pada pengujian operasi pemotongan gambar terhadap

metode *Line-Shift Coding*, dapat diambil kesimpulan bahwa metode ini tidak tahan terhadap pengujian tersebut. Hal ini dikarenakan bahwa pesan terletak di bagian awal dari dokumen dan diperpanjang sesuai bit pesan. Jika terjadi pemotongan terhadap gambar, beberapa bagian gambar yang di isi pesan akan hilang, sehingga keseluruhan pesan tidak dapat dikembalikan. Namun, pada pengujian operasi *resizing* gambar, dapat diambil kesimpulan bahwa metode ini tidak tahan terhadap pengujian tersebut sampai dengan ukuran yang melebihi atau sama dengan 700963 piksel. Penyebabnya adalah ketika ukuran gambar semakin kecil, maka spasi antar baris juga semakin kecil. Gambar yang memiliki ukuran 650894 piksel, terdapat kelompok baris genap yang memiliki jumlah baris lebih sedikit daripada jumlah yang semestinya, karena dua baris dihitung sebagai satu baris. Hal ini mengakibatkan pesan yang tersembunyi dalam gambar tidak dapat dikembalikan. Namun, ketika ukuran gambar yang lebih besar dari ukuran asli, pesan yang tersembunyi di dalamnya dapat berhasil dikembalikan. Hal ini disebabkan karena perbandingan jarak antar centroid memiliki hasil yang sama pada dokumen stego, sehingga tidak mempengaruhi arah pergeseran pesan (Adiniarti, 2009).

Penelitian yang berjudul Implementasi Algoritma Caesar Cipher Dan Steganografi Least Significant Bit Untuk File Dokumen. Berdasarkan hasil penelitian dalam pembangunan perangkat lunak untuk mengamankan dan merahasiakan dokumen rahasia, dapat disimpulkan bahwa file yang bersifat rahasia atau penting dan hanya ingin diketahui oleh pihak tertentu dapat diamankan dengan menggunakan perangkat lunak yang dibangun menggunakan bahasa pemrograman Java dan menerapkan algoritma Caesar Cipher dan Least Significant Bit (LSB). Dokumen yang dienkripsi oleh algoritma Caesar Cipher akan menggeser huruf dalam dokumen sebanyak jumlah yang ditentukan oleh kunci yang dimasukkan. Sedangkan dokumen yang disisipkan dalam gambar menggunakan algoritma LSB dengan mengubah bit paling kanan atau paling belakang pada gambar dengan bit dokumen yang ingin disisipkan. Dalam proses enkripsi, semua jenis file dokumen dapat dienkripsi, namun hanya 2 dari total 5 file dokumen yang dapat disisipkan menggunakan proses embedding. Ukuran file penampung dalam perangkat lunak ini hanya 250x250 pixel sehingga dokumen yang akan disisipkan hanya dapat

memiliki maksimal 31 karakter. Seluruh file dokumen yang dienkripsi dari total 5 file dapat didekripsi dengan baik. Berdasarkan pengujian, perangkat lunak ini hanya dapat menyisipkan 2 file dokumen, dan kedua file tersebut dapat dikembalikan saat diekstraksi (Yusup dkk., 2020).

Penelitian yang berjudul Pengamanan File Dokumen Ujian dengan Image Steganography Metode Lsb dalam penelitian ini, peneliti berhasil mengimplementasikan program steganografi serta menggunakannya dalam mengenkripsi file dokumen ujian sekolah ke dalam gambar. Ukuran gambar yang telah di steganografi tidak terlalu berbeda dengan gambar aslinya dan tampilannya mirip seperti gambar aslinya. Selanjutnya, peneliti membuat pengujian dengan implementasikan serangan MITM untuk mendeteksi file yang ditransfer dari komputer ke komputer lain melalui file *sharing*. Topologi yang digunakan adalah topologi star yang dibuat secara virtual pada aplikasi GNS3. Setelah topologi star terbentuk, peneliti mentransfer file dokumen ujian melalui file sharing dan bertindak sebagai MITM untuk mendeteksi file yang ditransfer. Dari hasil pengujian tersebut, dapat ditarik kesimpulan bahwa ketika file dokumen ujian dikirim secara langsung tanpa menggunakan proses steganografi, nama dan format filenya dapat terlihat jelas oleh MITM yang sedang memantau lalu lintas data. Oleh karena itu, dapat disimpulkan bahwa penggunaan steganografi memang sangat penting untuk menjaga kerahasiaan data yang dikirimkan. Namun, jika dokumen ujian dikemas dalam gambar steganografi sebelum ditransfer, maka MITM akan menganggapnya hanya sebagai gambar biasa dan data akan aman dari serangan (Abdurrahman & Prapanca, 2021).

2.2 Dasar Teori

2.2.1 Steganografi

Steganografi (*steganography*) adalah teknik untuk menyembunyikan informasi atau data rahasia pada media digital sehingga keberadaan informasi atau data rahasia tersebut tidak dapat diketahui oleh orang lain. Media digital yang digunakan dalam steganografi digital meliputi teks, gambar, video serta suara (audio). Proses menyisipkan pesan pada media penutup (cover) disebut encoding,

sedangkan proses mengambil pesan dari media stego (stegotext) disebut decoding. Untuk melakukan encoding dan decoding, diperlukan kunci rahasia (stegokey) agar pesan yang disisipkan atau diekstrak hanya dapat diakses oleh pihak yang berhak (Nirmala, 2020).

Terdapat beberapa istilah terkait erat dengan steganografi, yaitu (Gunawan, 2018) :

1. Pesan tersembunyi atau *embedded message*, juga dikenal sebagai *hidden text*.
2. Pesan yang digunakan untuk menyembunyikan pesan tersembunyi, disebut *covertext* atau *cover-object*.
3. Pesan yang sudah mengandung pesan tersembunyi, dikenal sebagai *stegotext* atau *stego-object*.

Terdapat beberapa teknik untuk menyisipkan pesan pada media digital, di antaranya adalah (Buha Johannes, 2021) :

1. *Injection*, yaitu menanamkan pesan secara langsung ke media. Namun, teknik ini memiliki masalah yaitu ukuran media menjadi lebih besar dan mudah terdeteksi. Teknik ini juga disebut *embedding*.
2. *Substitusi*, yaitu mengganti data normal dengan data rahasia. Teknik ini biasanya tidak mengubah ukuran data asli, tetapi tergantung pada file media dan data yang akan disembunyikan. Teknik ini bisa menurunkan kualitas media yang ditumpangi.
3. *Transformasi Domain*, teknik ini sangat efektif dan menyembunyikan data pada *transform space*.
4. *Spread Spectrum*, merupakan teknik pentransmisi yang menggunakan kode *pseudo-noise* independen terhadap data informasi untuk menyebarkan energi sinyal dalam jalur komunikasi yang lebih besar. Oleh penerima, sinyal dikumpulkan kembali menggunakan replika kode *pseudo-noise* tersinkronisasi.
5. *Statistical Method*, teknik ini disebut juga skema *steganographic* 1 bit. Skema tersebut menanamkan satu bit informasi pada media tumpangan dan mengubah statistik walaupun hanya 1 bit. Sistem ini bekerja berdasarkan kemampuan penerima dalam membedakan antara informasi yang dimodifikasi dan yang belum.

6. *Distortion*, metode ini menciptakan perubahan pada objek yang ditumpangi oleh data rahasia.

2.2.2 Line Shifting

Line-shifting adalah teknik steganografi yang mengubah dokumen dengan cara memindahkan baris secara vertikal pada teks sesuai dengan bit yang ingin disisipkan. Dokumen teks dibagi menjadi dua kelompok, yaitu kelompok genap dan ganjil. Kelompok genap terdiri dari baris-baris genap yang dapat digunakan untuk menyisipkan pesan, yaitu baris-genap yang diapit oleh kelompok ganjil dalam paragraf yang sama. Kelompok ganjil berisi baris-baris ganjil yang berdekatan dengan kelompok genap. Setiap baris pada kelompok genap digeser, sementara kelompok ganjil, yang disebut sebagai kelompok kontrol, tetap pada posisi semula. Kelompok kontrol digunakan untuk memperkirakan dan mengkompensasi distorsi untuk setiap proyeksi profil horizontal (Riansyah dkk., 2022).

2.2.3 Encode

Dalam steganografi, encoding digunakan untuk menyembunyikan pesan atau informasi dalam suatu media yang tidak dicurigai seperti gambar, audio, atau video. Proses ini disebut steganografi. Dalam proses encoding steganografi, pesan atau informasi diencode dalam bentuk kode atau simbol yang kemudian disisipkan dalam media yang digunakan sebagai cover. Proses ini dilakukan dengan mengubah atau menambahkan beberapa bit dari media cover yang digunakan sebagai media penyimpan pesan. Sehingga pesan tersebut tidak akan terlihat oleh pihak yang tidak dikehendaki.

2.2.4 Decode

Decoding adalah proses mengubah informasi yang diencode kembali ke format atau kode asli. Ini dapat dilakukan dengan menggunakan kunci atau algoritma yang sesuai. Decoding digunakan dalam berbagai bidang, seperti komunikasi, komputer, dan pengolahan sinyal. Dalam komunikasi, decoding digunakan untuk mengubah sinyal elektronik menjadi pesan yang dapat diterima

oleh penerima. Dalam komputer, decoding digunakan untuk mengubah data dari format yang tidak dapat dibaca menjadi format yang dapat dibaca.

Dalam steganografi, proses decoding dilakukan dengan mengambil pesan yang disisipkan dari media cover. Proses ini dilakukan dengan mengambil beberapa bit dari media yang digunakan sebagai media penyimpan pesan. Kemudian pesan tersebut didecode kembali menjadi pesan asli dengan menggunakan kunci atau algoritma yang sesuai.

2.2.5 Python

Python adalah sebuah bahasa pemrograman tinggi yang menggunakan metode *Object Oriented Programming* dan semantik dinamis untuk menjalankan instruksi multi guna secara langsung dengan cara interpretatif. Keunggulan dari Python sebagai bahasa pemrograman tinggi adalah keterbacaan syntax yang baik dan mudah dipelajari karena dilengkapi dengan manajemen memori otomatis.

Python adalah bahasa pemrograman yang dinamis dan mudah dipahami yang cocok digunakan untuk berbagai jenis pengembangan perangkat lunak. Dilengkapi dengan pustaka standar yang dapat diperluas, Python bisa dipelajari hanya dalam beberapa hari. Salah satu kerangka kerja Python yang terkenal adalah Flask. Flask merupakan micro-framework yang tidak memerlukan banyak perangkat dan pustaka. Namun, framework ini dapat meningkatkan efisiensi pengembangan. Flask cocok digunakan pada program yang berkapasitas energi kecil dan memerlukan sedikit sumber daya memori. Meskipun ringan, Flask tetap berfungsi sesuai kebutuhan. Kerangka kerja Flask terdiri dari dua komponen penting, yaitu Werkzeug dan Jinja2. Werkzeug digunakan untuk menyediakan routing, debugging, dan Web Server Gateway Interface (WSGI), sedangkan Jinja2 digunakan sebagai template engine (Ngantung & Pakereng, 2021).

2.2.6 PyPDF

PyPDF adalah sebuah modul pustaka yang disediakan untuk bahasa pemrograman Python yang digunakan untuk memanipulasi dokumen PDF.

Fungsinya mencakup pembuatan, pembacaan, dan pengubahan dokumen PDF (Wiandana, 2020).

PyPDF2 adalah sebuah modul Python yang dapat digunakan untuk memproses file PDF. Modul ini dapat digunakan untuk mengambil informasi dari file PDF, menggabungkan beberapa file PDF menjadi satu, memisahkan halaman dari file PDF, menambahkan komentar atau teks ke file PDF, dan masih banyak lagi.

2.2.7 Reportlab

Reportlab merupakan Modul perangkat lunak yang dapat membuat dokumen secara langsung dalam Adobe Portable Document Format (PDF) menggunakan bahasa pemrograman Python. Modul ReportLab secara langsung membuat PDF berdasarkan perintah grafik. Sehingga dapat menghasilkan laporan dengan sangat cepat - terkadang lipat lebih cepat daripada alat penulisan laporan tradisional. Pendekatan ini digunakan bersama oleh beberapa modul lain - PDFlib untuk C, iText untuk Java, iTextSharp untuk .NET, dan lainnya. Namun, modul ReportLab berbeda karena dapat bekerja di tingkat yang jauh lebih tinggi, dengan mesin berfitur lengkap untuk menyusun dokumen lengkap dengan tabel dan bagan.

2.2.8 Flask

Flask merupakan suatu framework web yang digunakan untuk membangun aplikasi web dan ditulis dengan menggunakan bahasa pemrograman Python. Flask termasuk dalam kategori microframework yang memiliki fitur yang minimalis dan dapat diintegrasikan dengan berbagai macam library dan pustaka lainnya. Dengan menggunakan Flask dan bahasa pemrograman Python, pengembang dapat membuat aplikasi web yang terstruktur dengan mudah dan juga dapat mengatur perilaku atau behaviour dari aplikasi web tersebut secara lebih fleksibel.

Flask adalah sebuah microframework yang dikembangkan oleh Armin Ronacher. Tujuan utama dari Flask adalah untuk menyederhanakan inti framework-nya sedemikian rupa sehingga menjadi sangat ringan dan cepat. Dengan menggunakan tagline "web development, one drop at a time", Flask memungkinkan

pengguna untuk membuat situs web dengan cepat dengan menggunakan library yang sederhana (Gilvy Langgawan Putra dkk., 2019).

Selain itu, meskipun Flask disebut sebagai microframework, Flask tidak kekurangan fungsionalitas. Istilah microframework di sini mengacu pada tujuan Flask untuk menjaga core aplikasi semudah mungkin namun mudah ditambahkan fitur. Dengan demikian, fleksibilitas dan skalabilitas Flask relatif tinggi dibandingkan dengan framework lain.

2.2.9 HTML

HTML adalah bahasa pemrograman standar yang digunakan untuk menampilkan konten pada halaman web. Dengan HTML, pengguna dapat mengatur tampilan dan desain konten pada halaman web, membuat tabel, mempublikasikan halaman web secara online, membuat formulir input untuk registrasi dan transaksi melalui web, serta menampilkan gambar pada browser. (Mariko, 2019).

2.2.10 Profil LPPM UNISSULA

Lembaga Penelitian dan Pengabdian Kepada Masyarakat (LPPM) Unissula adalah unsur pelaksana akademik yang melaksanakan sebagian tugas pokok dan fungsi Unissula di bidang Penelitian dan Pengabdian Kepada Masyarakat. Mempunyai visi “Menjadi lembaga terkemuka di bidang penelitian dan pengabdian masyarakat dalam rangka pengembangan dan pemanfaatan ilmu pengetahuan dan teknologi atas dasar nilai-nilai Islam dan membangun peradaban Islam menuju masyarakat sejahtera yang dirahmati Allah SWT dalam kerangka rahmatan lil ‘alamiin”.

BAB III

METODE PENELITIAN

3.1 Metode Pengumpulan Data

Adapun tahapan dari pengumpulan data untuk menyelesaikan penelitian ini adalah :

3.1.1 Studi Literatur

Dalam studi literatur penulis mempelajari teori mengenai PHP, Python, dan metode Line Shifting serta code program untuk menjalankan perintah yang diinginkan melalui berbagai sumber informasi seperti buku, website, jurnal, dan video tutorial di youtube.

3.1.2 Dokumentasi

Penulis telah mempelajari tentang modul, bahasa pemrograman, dan tools yang dibutuhkan untuk sistem yang akan dibuat dengan membaca dokumentasi yang disediakan oleh situs resmi dari modul, bahasa pemrograman, dan tools tersebut.

3.1.3 Observasi

Penulis telah mengumpulkan data yang diperlukan melalui observasi dan pengamatan terhadap cara implementasi program. Data yang digunakan merupakan data dokumen hak kekayaan intelektual yang diperoleh dari LPPM UNISSULA.

3.2 Metodologi Perancangan Alur Sistem

3.2.1 Analisis Kebutuhan

Pada tahap analisis kebutuhan adalah tahap di mana sistem di analisa untuk menentukan apa saja yang dibutuhkan serta dapat dilakukan oleh sistem dalam proses input hingga output yang sesuai. Sistem harus memiliki beberapa proses atau fungsi, di antaranya :

A. Upload File PDF

Upload file PDF merupakan hal pertama yang harus bisa dilakukan oleh sistem. File PDF yang diupload akan menjadi media carrier atau pembawa pesan yang nantinya akan disisipi dengan sebuah pesan teks. Proses upload dapat dilakukan dengan memilih file dari media penyimpanan lokal user.

B. Menuliskan Pesan

Fungsi kedua yang harus dimiliki oleh sistem adalah menuliskan pesan di halaman encode. Fungsi ini digunakan untuk menuliskan pesan teks yang akan disisipkan ke dalam dokumen PDF yang di upload.

C. Menyisipkan Pesan (Encode)

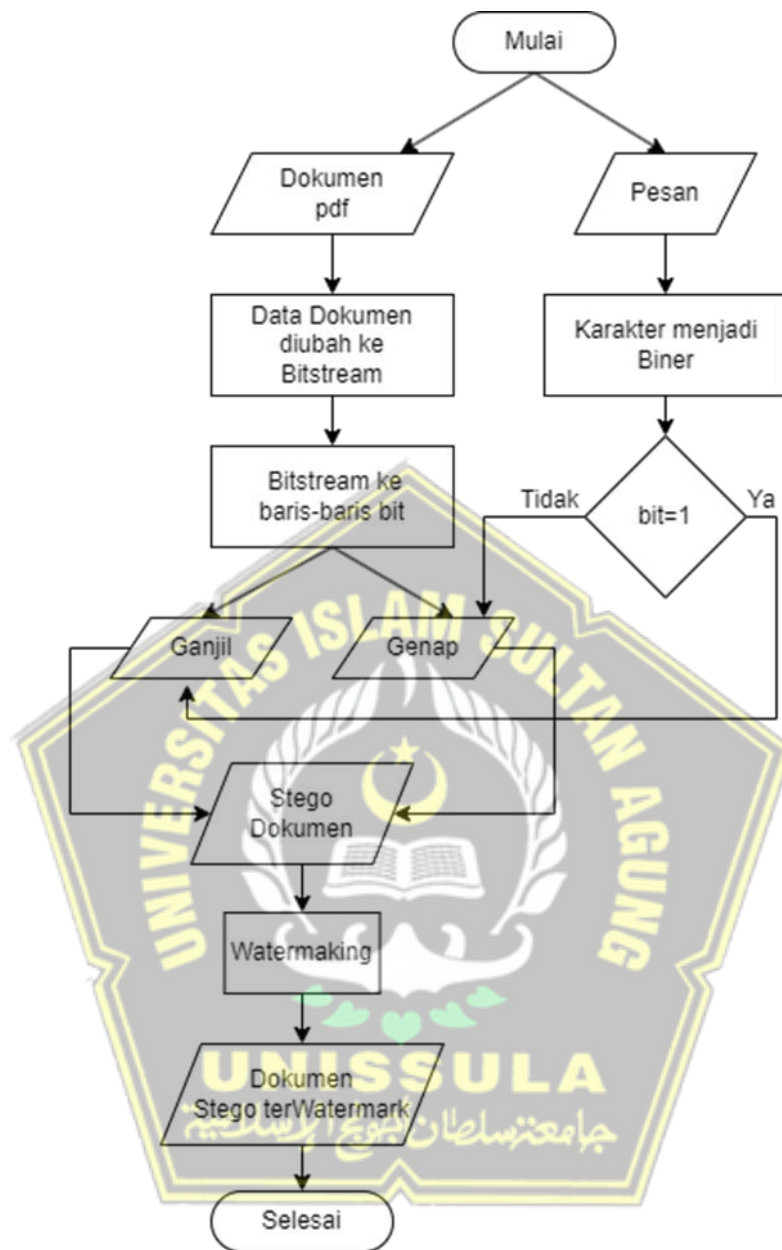
Pada fungsi ini sistem bertugas untuk melakukan penyisipan pesan teks ke dalam PDF yang telah di inputkan oleh user. Sistem ini akan memasukkan pesan ke dalam PDF dengan menggeser baris baris bit teks yang ada pada PDF, apabila bit bernilai 1 maka akan dimasukkan dalam baris bit ganjil, jika bit bernilai 0 maka akan dimasukkan dalam baris bit genap. Setelah dokumen PDF tersisip oleh pesan sistem mengeluarkan dokumen PDF baru.

D. Mengekstraksi Pesan (Decode)

Di fungsi ini merupakan kebalikan dari fungsi decode, sistem bertugas mengekstrak pesan teks yang ada di dalam PDF baru yang telah di inputkan oleh user. Dokumen PDF baru di ubah kembali ke dalam bentuk bitstream yang kemudian dibagi menjadi dua group bit genap dan ganjil. Di ekstraksi kedalam bit 1 dan bit 0 setelah itu dikonversikan kembali ke dalam bentuk karakter. Kemudian sistem mencetak pesan ke layar.

3.2.2 Analisis Alur Sistem

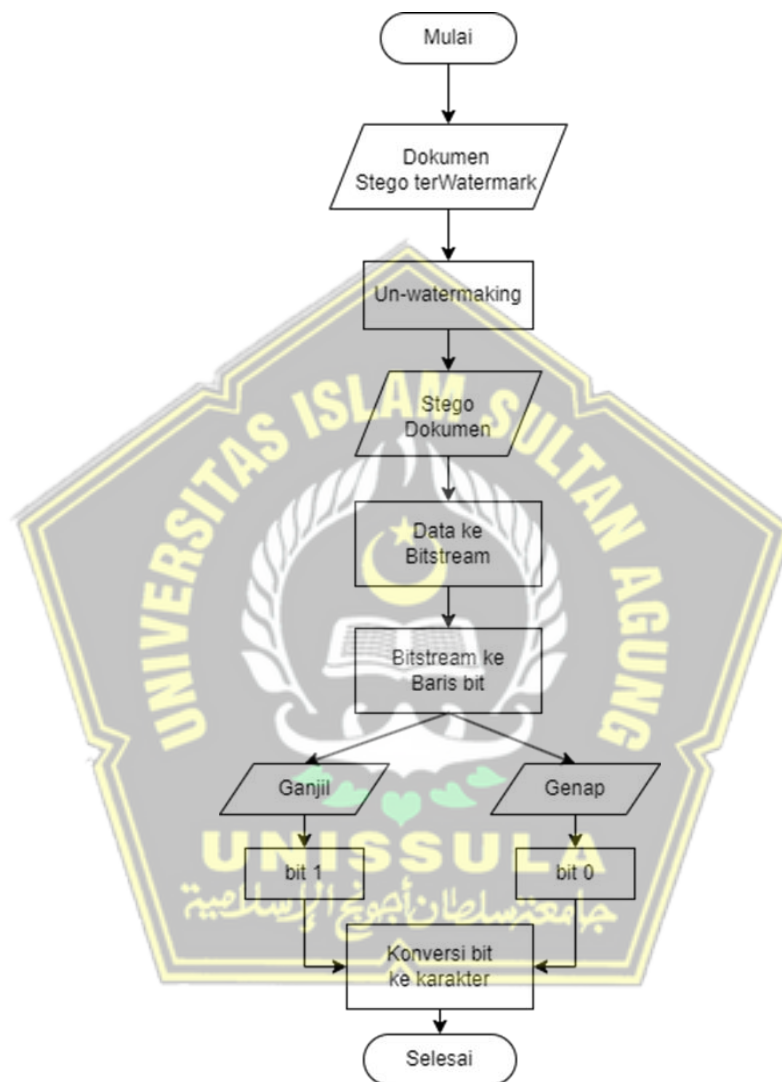
Pada Analisis alur sistem, akan dibuat sebuah flowchart yang menunjukkan alur perancangan dan sekaligus alur kerja dari sistem ini.



Gambar 3. 1 Proses Enkripsi

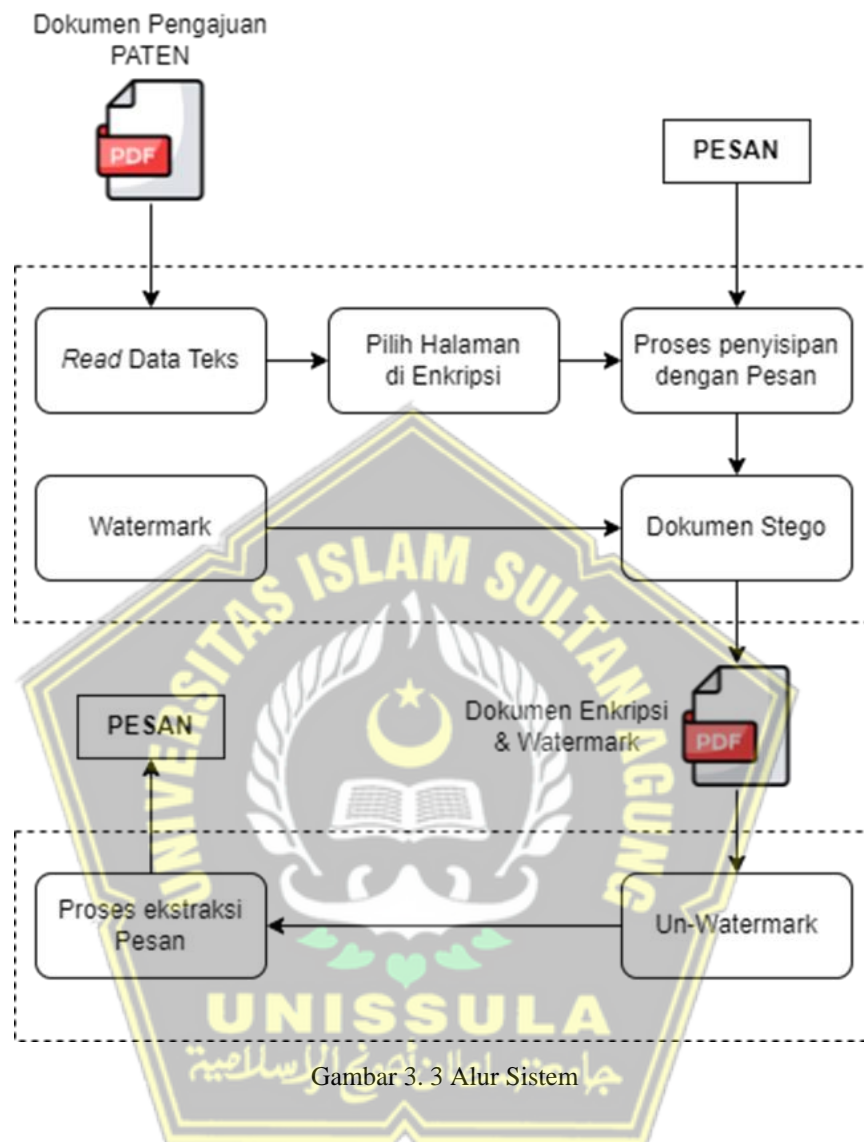
Ketika user memilih enkripsi maka user memasukkan dokumen pengajuan paten dan pesan. Isi dokumen pengajuan paten diubah ke dalam bitstream yang kemudian akan dibagi kedalam baris bit genap dan ganjil. Sedangkan karakter pada pesan akan diubah dalam kode ASCII yang kemudian diubah menjadi biner. Biner akan diubah ke dalam bentuk bit, apabila bit bernilai 1 maka akan dimasukkan dalam baris bit ganjil, jika bit bernilai 0 maka akan dimasukkan dalam baris bit

genap yang ada pada dokumen pengajuan paten. Setelah itu menghasilkan dokumen baru tersteganografi yang kemudian akan di watermarking. Untuk flowchart dapat dilihat pada gambar 3.1.



Gambar 3. 2 Proses Dekripsi

Pada proses dekripsi user memasukkan dokumen enkripsi lalu pada prosesnya watermark di hilangkan setelah itu isi dari dokumen steganografi di ubah kembali ke dalam bentuk bitstream yang kemudian dibagi menjadi dua group bit genap dan ganjil. Di ekstraksi kedalam bit 1 dan bit 0 setelah itu dikonversikan kembali ke dalam bentuk karakter. Untuk flowchart dapat dilihat pada gambar 3.2.

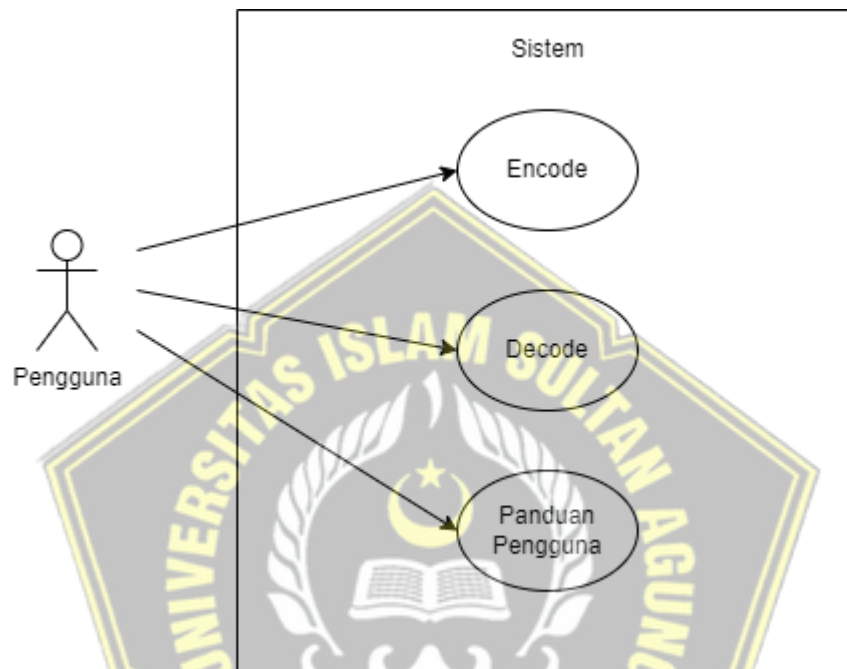


Gambar 3. 3 Alur Sistem

Sebagai gambaran alur proses sistem dapat di lihat pada gambar 3.3. Pada gambar menunjukkan user di awal memasukkan dokumen pengajuan paten yang di dalamnya terdapat abstrak, deskripsi, klaim, dan gambar. Isi dari dokumen pengajuan di baca oleh sistem, pada halaman ke dua dari dokumen sampai terakhir yang berisikan deskripsi, klaim, dan gambar akan di enkripsi dengan menyisipi sebuah pesan dan menghasilkan dokumen baru yang kemudian diberi watermark.

3.2.3 Use Case Diagram

Pada perancangan sistem steganografi line shifting ini terdiri dari dua proses utama yang dilakukan oleh pengguna yaitu, proses menyisipkan pesan (encode) dan proses ekstraksi pesan (decode). Use Case sistem yang akan dibangun dapat dilihat pada gambar 3.4



Gambar 3. 4 Use Case Diagram

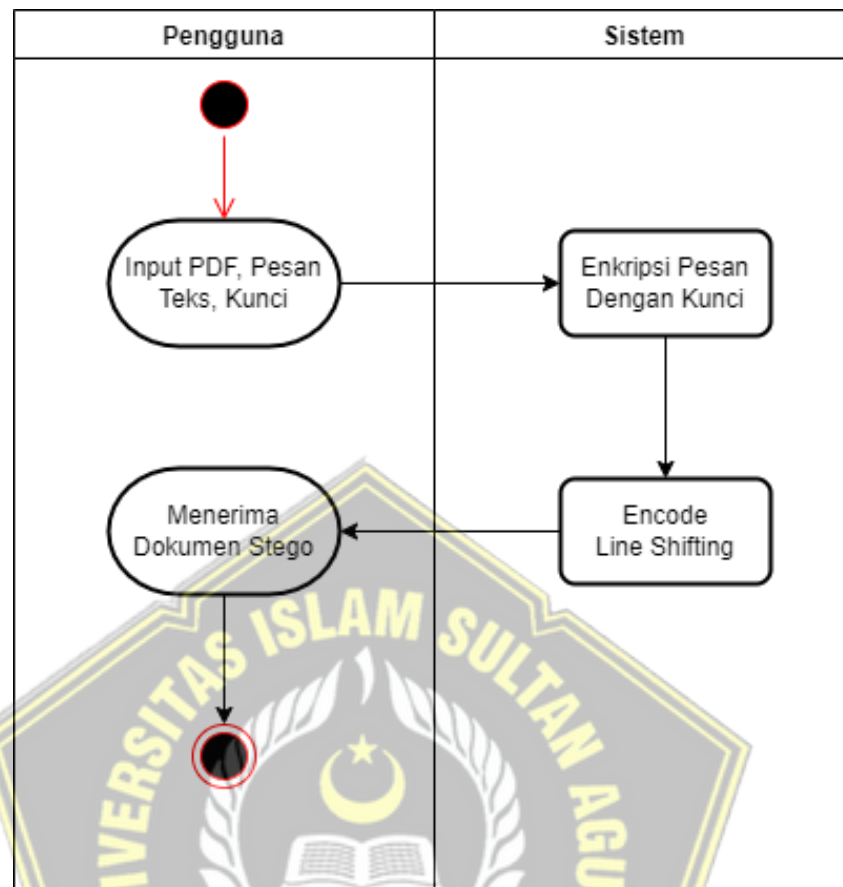
Pada gambar 3.4 Dapat dilihat pada sistem yang dibangun terdiri dari 1 aktor dan 3 case, Encode, Decode dan Panduan Pengguna.

3.2.4 Activity Diagram

Adapun activity diagram pada sistem yang dikembangkan memiliki dua activity yaitu, Activity Encode dan Activity Decode

A. Activity Encode

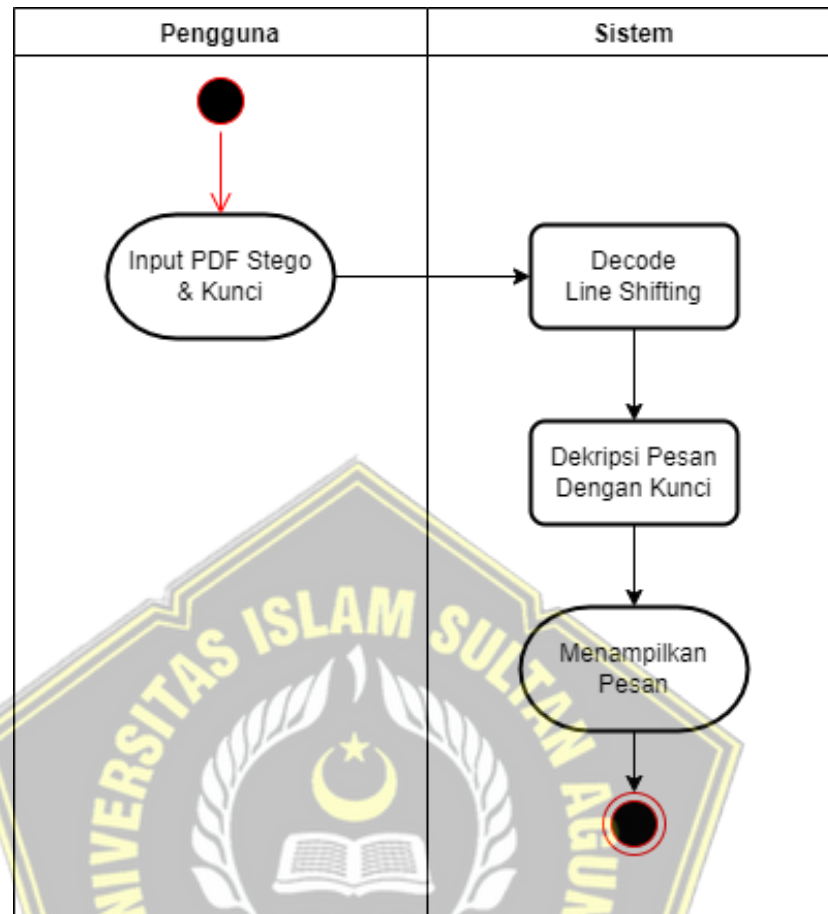
Pada activity encode terdapat pengguna dan sistem. Pengguna menginputkan dokumen pdf yang akan di steganografi, pesan teks, dan juga kunci. Sistem akan mengenkripsi pesan dengan kunci dilanjutkan proses steganografi line shifting dan menghasilkan dokumen baru yang tersteganografi. Desain activity encode dapat dilihat pada gambar 3.5



Gambar 3. 5 Activity Encode

B. Activity Decode

Pada activity decode pengguna menginputkan dokumen pdf hasil steganografi dan kunci selanjutnya pada sistem akan mengekstraksi pesan yang tersisip kemudian mendekripsi pesan dengan kunci dan sistem menampilkan pesan tersebut. Desain activity decode dapat dilihat pada gambar 3.6



Gambar 3. 6 Activity Decode

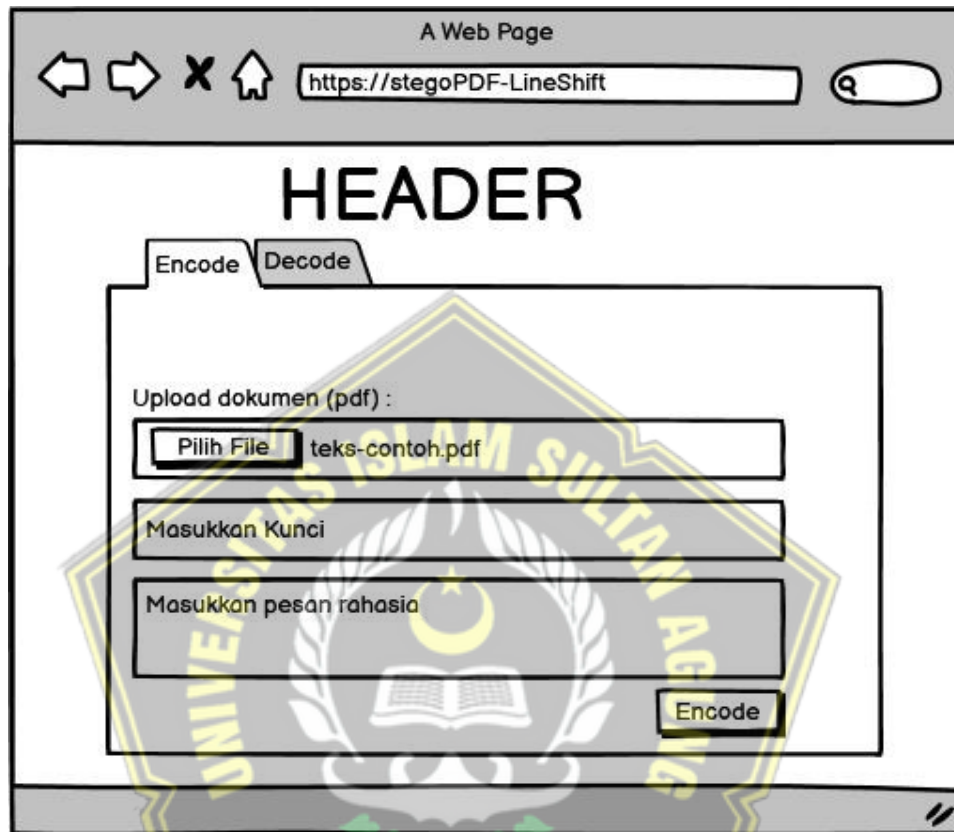
3.3 Perancangan Antar Muka

Pada tahap perancangan antarmuka adalah desain mockup yang akan diaplikasikan ke dalam sistem. Berikut adalah rancangan antarmuka dari Sistem Pengamanan Dokumen Pengajuan Hak Paten Dengan Menggunakan Metode Steganografi Line Shifting.

1. Halaman Encode

Halaman encode adalah halaman awal dari sistem ini, karena penulis berfokus membuat sebuah sistem yang sederhana dan mudah digunakan, maka halaman awal dari sistem ini adalah halaman ketika pengguna langsung bisa menyisipkan pesannya seperti terlihat pada gambar 3.7.

Pengguna akan mengupload sebuah dokumen PDF dan menuliskan pesan berupa teks. Proses upload dapat dilakukan dengan memilih file dari media penyimpanan lokal oleh user.



Gambar 3. 7 Mockup Halaman Encode

2. Halaman Decode

Halaman decode adalah halaman yang akan digunakan pengguna untuk mengupload dokumen PDF tersteganografi, kemudian sistem mengekstrak dan menampilkan pesan yang tersisip dalam dokumen PDF tersteganografi tersebut.

A Web Page

https://stegoPDF-LineShift

HEADER

Encode Decode

Upload dokumen steganografi (pdf) :

Pilih File file-contoh-terstegano.pdf

Masukkan Kunci

Decode

Pesan Rahasia :

Gambar 3. 8 Mockup Halaman Decode

BAB IV

HASIL DAN ANALISIS PENELITIAN

4.1 Cara Kerja Sistem

Sistem ini memiliki dua proses utama, yaitu enkripsi dan dekripsi. Proses encode akan menyisipkan pesan yang ditentukan oleh pengguna ke dalam file PDF dengan menggeser baris-baris yang merupakan baris genap atau ganjil. Proses dekripsi akan mengekstrak pesan yang tersimpan dalam file PDF dengan menggeser baris-baris yang merupakan baris genap atau ganjil kembali ke posisi semula. Berikut penjabaran alur proses utama dari sistem yang telah dibangun.

A. Proses Encode

Program Encode ini dibuat dengan bahasa pemrograman Python yang digunakan untuk menyisipkan pesan ke dalam sebuah file PDF dengan metode steganografi lineshifting yang menggeser baris-baris teks dalam file sesuai dengan kunci encode yang telah ditentukan.

Proses yang dilakukan oleh fungsi encrypt adalah sebagai berikut :

1. Pertama, kode menggunakan decorator `@app.route('/encrypt', methods=['POST'])` untuk menentukan URL yang akan digunakan oleh aplikasi untuk mengeksekusi fungsi encode ini.
2. Kemudian, fungsi `encrypt()` akan dijalankan ketika ada request POST diterima pada URL tersebut. Dalam fungsi ini, file PDF, pesan, dan kunci yang diterima dari form input akan dibaca dan disimpan dalam variabel `pdf_file`, `pesan`, dan `kunci`.
3. Selanjutnya, pesan yang ingin disimpan akan diencode dengan menggunakan kunci encode yang telah ditentukan. Encode dilakukan dengan XOR tiap karakter dari pesan dengan karakter dari kunci yang diambil dengan index yang sama modulo panjang dari kunci. Hasil encode disimpan dalam variabel `pesan_enkripsi`.
4. Kemudian, file PDF dibaca menggunakan `PyPDF2` dan objek `pdf_reader` dibuat. Selain itu, objek `pdf_writer` juga dibuat untuk digunakan dalam proses menyimpan perubahan pada file PDF.

5. Selanjutnya, setiap halaman dalam file PDF akan diiterasi. Pada setiap halaman, teks dari halaman tersebut akan dibaca dengan menggunakan method `extract_text()` dari objek `pdf_reader`.
6. Selanjutnya, baris-baris dari teks halaman akan di-shift sesuai dengan kunci encode yang telah ditentukan. Baris yang merupakan baris genap atau ganjil akan diganti dengan pesan yang telah diencode.
7. Selanjutnya, Membuat File PDF baru dengan menggunakan canvas dari `reportlab`. Selanjutnya, file PDF baru yang telah dibuat akan dibaca sebagai halaman baru.
8. Setelah itu, ditambahkan watermark dengan menggunakan canvas dari `reportlab`
9. Selanjutnya, halaman baru yang telah disisipi pesan akan digabungkan dengan halaman asli menggunakan method `merge_page()` dari objek `pdf_reader`. Selanjutnya, halaman yang telah disisipi pesan akan ditambahkan ke dalam objek `pdf_writer` dengan menggunakan perintah `pdf_writer.add_page(halaman_baru)`. Halaman yang telah disisipi pesan ini akan menjadi halaman baru yang akan ditambahkan ke dalam file pdf hasil encode.
10. Setelah semua halaman dalam file pdf asli telah disisipi pesan dan ditambahkan ke dalam objek `pdf_writer`, perubahan yang telah dilakukan pada file pdf tersebut akan disimpan dengan menggunakan perintah `pdf_writer.write(pdf_output)`. File pdf hasil encode akan disimpan dalam objek `pdf_output` yang merupakan sebuah objek `io.BytesIO`.
11. Setelah file pdf hasil encode disimpan, pointer dari objek `pdf_output` akan diatur ke awal dengan perintah `pdf_output.seek(0)`. Ini dilakukan agar browser dapat membaca file pdf hasil encode yang telah disimpan dalam objek `pdf_output`.
12. File pdf hasil encode akan dikirim ke browser dengan menggunakan perintah `response = app.make_response(pdf_output.read())`. Perintah ini akan mengirimkan isi dari objek `pdf_output` ke browser sebagai file pdf hasil encode.

13. Terakhir, tipe file yang dikirim dan nama file yang digunakan akan ditentukan dengan perintah `response.headers['Content-Type'] = 'application/pdf'` dan `response.headers['Content-Disposition'] = 'inline; filename=hasil.pdf'`. File pdf hasil encode akan ditampilkan di browser dengan nama "hasil.pdf" dan ditampilkan sebagai file pdf.

B. Proses Decode

Pada program decode yang merupakan kebalikan dari encode, yaitu digunakan untuk membuka pesan yang telah disisipkan ke dalam file PDF menggunakan metode steganografi lineshifting. Caranya adalah dengan menggeser baris-baris yang merupakan baris genap atau ganjil kembali ke posisi semula sesuai dengan kunci encode yang telah ditentukan sebelumnya.

Proses yang dilakukan oleh program decode adalah sebagai berikut :

1. Pertama, program akan membaca file pdf dan kunci yang diterima dari form input dengan menggunakan perintah `"pdf_file = request.files.get('file_pdf').read()"` dan `"kunci = request.form.get('kunci')"`.
2. Selanjutnya, program akan membuat objek pdf_reader dan pdf_writer dengan menggunakan `PyPDF2.PdfReader(io.BytesIO(pdf_file))` dan `PyPDF2.PdfWriter()`.
3. Kemudian, program akan melakukan decode pesan yang disisipkan dengan menggunakan kunci encode yang telah ditentukan dengan menggunakan perintah `"pesan = ""`
4. Selanjutnya, program akan melakukan iterasi setiap halaman dalam file PDF dengan perintah `"for halaman in range(len(pdf_reader.pages))"`
5. Dalam iterasi tersebut, program akan membaca halaman yang sedang diterjemahkan dengan perintah `"teks = pdf_reader.pages[halaman].extract_text()"` dan `"halaman_pdf = pdf_reader.pages[halaman]"`
6. Kemudian program akan menggeser baris-baris yang merupakan baris genap atau ganjil kembali ke posisi semula sesuai dengan kunci encode yang telah ditentukan dengan perintah `"for i, baris in enumerate(teks.splitlines())"`

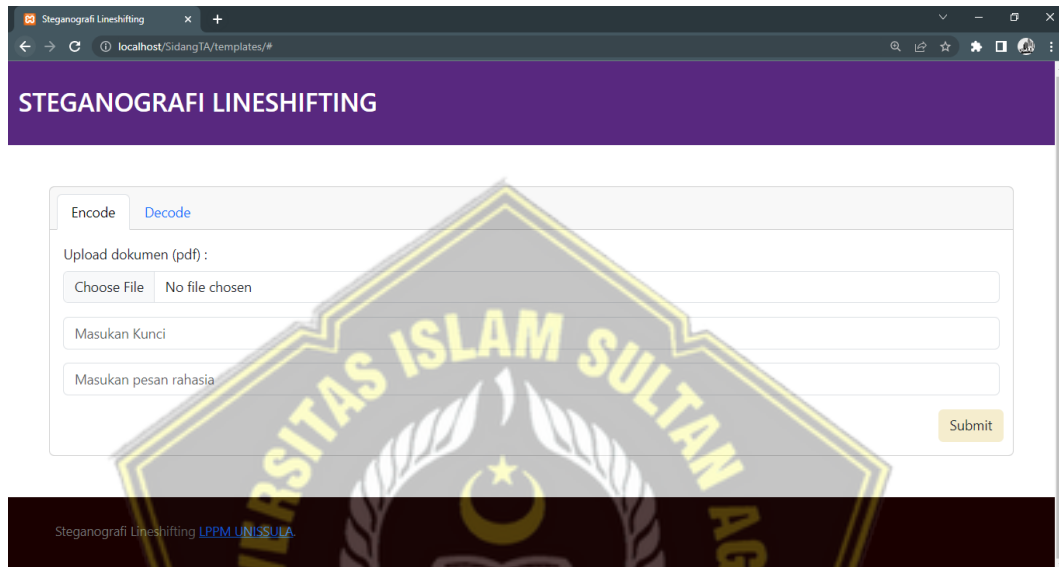
7. Selanjutnya, program akan melakukan decode pesan yang telah dibuka dengan perintah "for i, c in enumerate(pesan):"
8. Selanjutnya, kode program akan membuat sebuah perulangan untuk setiap halaman dalam file PDF yang diterima dari form input. Dalam setiap iterasi perulangan, kode program akan mengekstrak teks dari halaman tersebut menggunakan perintah `pdf_reader.pages[halaman].extract_text()`
9. Setelah teks dari halaman tersebut diekstrak, kode program akan membuat sebuah perulangan untuk setiap baris dari teks tersebut. Dalam setiap iterasi perulangan, kode program akan mengecek apakah baris tersebut merupakan baris genap atau ganjil. Jika baris tersebut merupakan baris genap, maka baris tersebut akan ditambahkan ke dalam variabel pesan.
10. Setelah seluruh halaman dalam file PDF diterjemahkan dan pesan yang disisipkan dibuka kembali, kode program akan mengaplikasikan kunci encode yang telah ditentukan untuk mendecode pesan tersebut. Hal ini dilakukan dengan cara menggunakan operator XOR (^) pada setiap karakter dari pesan tersebut dengan karakter dari kunci encode yang sesuai dengan posisinya.
11. Setelah pesan tersebut selesai didecode, kode program akan menyimpan pesan tersebut ke dalam session dan mengarahkan kembali ke halaman utama dengan perintah `return redirect('/')`.

4.2 Implementasi User Interface

Implementasi merupakan tahap setelah rancangan selesai dibuat, pada sistem ini sudah dibuat rancangan tampilan user interface untuk web. Untuk hasil dari implementasi user interface pada real device dapat ditunjukkan pada beberapa hasil berikut :

A. Halaman Encode

Pada halaman ini, pengguna akan langsung di arahkan ke tab encode, di tab encode ini akan ada beberapa field yang tersedia bagi pengguna untuk memasukkan dokumen, kunci, dan pesan yang akan di proses dengan steganografi line shifting.



Gambar 4. 1 Tampilan Encode

Seperti yang terlihat pada gambar 4.1 merupakan tampilan untuk fungsi encode. Untuk melakukan proses encoding pengguna harus memasukkan beberapa field yaitu, dokumen pdf yang digunakan sebagai carrier atau pembawa pesan, kunci yang digunakan untuk mengencode pesan yang akan disimpan, pesan rahasia yang akan disisipkan ke dalam pdf.

B. Halaman Decode

Pada halaman decode ini akan ada beberapa field yang tersedia bagi pengguna untuk memasukkan dokumen stego dan kunci.

Gambar 4. 2 Tampilan Decode

Pada gambar 4.2 merupakan tampilan untuk fungsi decode. Untuk melakukan proses decoding atau ekstrak pesan, pengguna harus memasukkan beberapa field yaitu, dokumen pdf hasil steganografi proses encode dan kunci yang digunakan untuk mendecode pesan yang ada pada pdf stego. Setelah melalui proses decoding pesan akan ditampilkan pada Pesan Rahasia.

4.3 Pengujian Sistem

Pada tahap ini akan dilakukan pengujian sistem, dimana metode yang akan dipakai adalah *Black box testing* adalah metode pengujian yang melihat suatu sistem atau aplikasi sebagai "kotak hitam" tanpa memperhatikan bagaimana sistem tersebut bekerja secara internal. Dalam *black box testing*, tester hanya mengkonsentrasikan diri pada input dan output dari sistem, bukan pada bagaimana sistem itu bekerja.

Tujuan dari black box testing adalah untuk menentukan apakah sistem memenuhi spesifikasi dan harapan dari pengguna dan memproduksi output yang

benar berdasarkan input yang diterimanya. Ini termasuk menguji validitas, konsistensi, dan kualitas data yang diterima oleh sistem dan output yang dihasilkan.

Black box testing dilakukan dengan menentukan serangkaian uji coba yang dapat memvalidasi spesifikasi sistem dan memastikan bahwa sistem memproduksi output yang diharapkan. Tester menentukan jenis *input* yang diterima oleh sistem dan memverifikasi *output* yang dihasilkan untuk memastikan bahwa output sesuai dengan harapan. Tester juga menguji sistem untuk menentukan apakah sistem memiliki kapasitas untuk menangani berbagai jenis input dan menghasilkan output yang benar. Dalam studi kasus ini, saya akan menggunakan teknik uji fungsional yang digunakan untuk menguji apakah sistem memenuhi spesifikasi dan harapan pengguna dengan memasukkan input dan memverifikasi output yang dihasilkan.

Tabel 4. 1 Pengujian *Encode*

Skenario Pengujian	Kasus Pengujian	Hasil Pengujian diharapkan	Hasil Uji Coba	Kesimpulan
Menyisipkan pesan ke pdf (1 halaman)	Menyisipkan 10 karakter pesan	Pesan dapat disisipkan	Sesuai	Berhasil
Menyisipkan pesan ke pdf (1 halaman)	Menyisipkan 35 karakter pesan	Pesan dapat disisipkan	Sesuai	Berhasil
Menyisipkan pesan ke pdf (5 halaman)	Menyisipkan 10 karakter pesan	Pesan dapat disisipkan	Sesuai	Berhasil
Menyisipkan pesan ke pdf (5 halaman)	Menyisipkan 35 karakter pesan	Pesan dapat disisipkan	Sesuai	Berhasil
Menyisipkan pesan ke pdf (15 halaman)	Menyisipkan 10 karakter pesan	Pesan dapat disisipkan	Sesuai	Berhasil
Menyisipkan pesan ke pdf (>15 halaman)	Menyisipkan 35 karakter pesan	Pesan dapat disisipkan	Sesuai	Berhasil

Tabel 4. 2 Pengujian *Decode*

Skenario Pengujian	Kasus Pengujian	Hasil Pengujian diharapkan	Hasil Uji Coba	Kesimpulan
Mengekstrak pesan ke pdf (1 halaman)	Mengekstrak 10 karakter pesan	Pesan dapat ditampilkan	Sesuai	Berhasil
Mengekstrak pesan ke pdf (1 halaman)	Mengekstrak 35 karakter pesan	Pesan dapat ditampilkan	Tidak Sesuai	Tidak dapat menampilkan pesan yang disisipkan
Mengekstrak pesan ke pdf (5 halaman)	Mengekstrak 10 karakter pesan	Pesan dapat ditampilkan	Sesuai	Berhasil
Mengekstrak pesan ke pdf (5 halaman)	Mengekstrak 35 karakter pesan	Pesan dapat ditampilkan	Sesuai	Berhasil
Mengekstrak pesan ke pdf (15 halaman)	Mengekstrak 10 karakter pesan	Pesan dapat ditampilkan	Sesuai	Berhasil
Mengekstrak pesan ke pdf (>15 halaman)	Mengekstrak 35 karakter pesan	Pesan dapat ditampilkan	Sesuai	Berhasil

4.4 Hasil dan Analisa

Dari tahapan pengujian yang dilakukan dapat dilihat bahwa sistem steganografi untuk menyisipkan pesan menggunakan bahasa pemrograman python dan microframework Flask dapat berjalan dengan baik.

Dan dari lima kasus uji dengan black box testing, pada proses decode terdapat satu kasus uji yang mengalami kegagalan dalam proses ekstraksi pesan dimana testing tersebut untuk menguji panjang pesan yang berbeda. Panjang karakter dibuat 35 karakter dan di sisipkan di PDF yang hanya memiliki 1 halaman, hasil encode dari kasus uji tersebut yaitu pesan tidak dapat terbaca sama sekali. Lain halnya jika panjang pesan tersebut disisipkan di PDF yang memiliki 4 halaman, ketika di encode menghasilkan pesan yang masih bisa terbaca.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari hasil penelitian yang telah dilakukan penulis, dapat ditarik kesimpulan bahwa sistem pengamanan dokumen dengan steganografi line shifting yang dibangun menggunakan bahasa python dapat di tarik beberapa poin kesimpulan yang penulis dapat selama penelitian ini :

- a. Line Shifting dapat di implementasikan untuk melakukan proses pesnyisipan pesan berupa teks ke dalam pdf.
- b. Dalam penelitian ada 1 kasus uji yang mengalami kegagalan saat proses decode pesan yaitu jika sebuah dokumen pdf yang hanya memiliki 1 halaman kemudian disisipi pesan sebanyak 35 karakter.
- c. Masih adanya karakter yang bukan merupakan karakter pesan yang ikut tercetak pada saat proses decode

5.2 Saran

Berdasarkan penelitian yang sudah ada, untuk penelitian yang akan datang penulis menyarankan :

- a. Karena masih ada karakter bukan pesan yang tercetak saat proses encode, diharapkan untuk penelitian selanjutnya dapat menangani hal tersebut.
- b. Mengkaji lebih lanjut mengenai Steganografi Lineshifting untuk dapat digunakan pada file selain PDF.

DAFTAR PUSTAKA

- Abdurrahman, S., & Prapanca, A. (2021). Pengamanan File Dokumen Ujian Dengan Image Steganography Metode Lsb. *Journal of Informatics and Computer Science*, 03.
- Adiniarti, I. (2009). *Implementasi Steganografi Pada Media Teks Dengan Metode Line-Shift Coding dan Metode Centroid*.
- Buha Johannes, S. (2021). Steganografi Penyisipan Pesan Pada File Citra Menggunakan Metode LSB (Least Significant Bit). *SP Nusantara*. <http://download.garuda.kemdikbud.go.id/article.php?article=1929454&val=13467&title=Steganografi%20Penyisipan%20Pesan%20Pada%20File%20Citra%20Dengan%20Menggunakan%20Metode%20LSB%20Least%20Significant%20Bit>
- Gunawan, I. (2018). Penggunaan Algoritma Kriptografi Steganografi Least Significant Bit Untuk Pengamanan Pesan Teks dan Data Video. *J-SAKTI (Jurnal Sains Komputer Dan Informatika)*, 2(1), 57. <https://doi.org/10.30645/j-sakti.v2i1.48>
- Mariko, S. (2019). APLIKASI WEBSITE BERBASIS HTML DAN JAVASCRIPT UNTUK MENYELESAIKAN FUNGSI INTEGRAL PADA MATA KULIAH KALKULUS. *Jurnal Inovasi Teknologi Pendidikan*, 6(1), 80–91. <https://doi.org/10.21831/jitp.v6i1.22280>
- Ngantung, R. K., & Pakereng, M. A. I. (2021). Model Pengembangan Sistem Informasi Akademik Berbasis User Centered Design Menerapkan Framework Flask Python. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, 5(3), 1052. <https://doi.org/10.30865/mib.v5i3.3054>
- Nirmala, E. (2020). Penerapan Steganografi File Gambar Menggunakan Metode Least Significant Bit (LSB) dan Algoritma Kriptografi Advanced Encryption Standard (AES) Berbasis Android. *Jurnal Informatika Universitas Pamulang*, 5(1), 36. <https://doi.org/10.32493/informatika.v5i1.4646>
- Ratama, N., & Munawaroh. (2022). Implementasi Metode Kriptografi dengan Menggunakan Algoritma RC4 dan Steganografi Least Significant Bit Dalam

Mengamankan Data Berbasis Android. *Jurnal Media Informatika Budidarma*, 6(2), 1272–1281. <https://doi.org/10.30865/mib.v6i2.3902>

Riansyah, D., Wijaya, A., Suroyo, H., Universitas, M., Darma, B., Universitas, D., Darma, B., Bina, U., & Palembang, D. (2022). Implementasi Pengamanan Dokumen Menggunakan Metode Steganografi Line-. *Eprints.Binadarma.ac.id*, 1–8. http://eprints.binadarma.ac.id/10610/1/if025_penelitian_s1.pdf

Wiandana, I. G. A. (2020). *Rancang Bangun Sistem Pelacakan Dokumen Memanfaatkan FUSE dan Samba File-System: Studi Kasus PT. Aneka Tuna Indonesia*. <https://repository.its.ac.id/82040/>

Yusup, I. M., Carudin, & Purnamasari, I. (2020). Implementasi Algoritma Caesar Cipher Dan Steganografi Least Significant Bit Untuk File Dokumen. *Jurnal Teknik Informatika Dan Sistem Informasi*, 6(3). <https://doi.org/10.28932/jutisi.v6i3.2817>

