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

Ahmad Saifurrohman, Bagus Satrio Waluyo Poetro, Moch Taufik
Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Sultan Agung Semarang

email: ahmadsaifurrohman3@std.unissula.ac.id, bagusswp@unissula.ac.id, mtaufik@unissula.ac.id

Abstract
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 tercetak pada saat proses decode.

Keyword: Dokumen digital, Steganografi, Line Shifting.

1. PENDAHULUAN

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 [1].

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 watermaking yang disisipkan ke dalam dokumen *cover* sehingga dokumen pesan tidak dapat terlihat oleh orang lain tanpa adanya bantuan sistem tertentu. Proses decode hanya dapat dilakukan dengan memasukkan kunci yang sama yang digunakan dalam proses encode. 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 decode 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 "Sistem Pengamanan Dokumen Pengajuan Hak Paten Dengan Menggunakan Metode Steganografi *Line Shifting*".

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 [2].

Peneletian 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 melebih 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 [3].

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 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 [4].

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 [5].

1.1 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 [6].

1.2 *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 [7].

1.3 Flask

Flask merupakan sebuah *microframework* yang dikembangkan oleh Armin Ronacher. Tujuan inti dari Flask adalah untuk menyederhanakan framework 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 [8].

1.4 LPPM UNISSULA

Lembaga penelitian dan pengabdian masyarakat (LPPM) merupakan lembaga yang dibawah naungan Universitas Islam Sultan Agung Semarang yang diberikan tanggung jawab untuk penyelenggaraan dan pelaksanaan penelitian dan pengabdian kepada masyarakat. Di dalam LPPM sendiri terdapat beberapa bidang salah satunya yaitu bidang Hak Kekayaan Intelektual (HKI). HKI sendiri terdiri dari dua yaitu hak cipta dan hak kekayaan industri. Menurut ketentuan yang berlaku dalam peraturan perundang-undangan yang relevan, hak cipta adalah hak eksklusif dari pemegang hak untuk memulai, mempertahankan, atau meningkatkan ciptaannya, atau memberi izin untuk itu. Sedangkan kekayaan industri terdiri dari 6 hak yaitu :

- Paten
- Desain industri
- Varietas tanaman
- Merek
- Desain tata letak sirkuit terpadu
- Rahasia dagang

2. METODE PENELITIAN

2.1 Pengumpulan Data

Adapun tahapan dari pengumpulan data untuk menyelsaikan penilitian ini adalah :

1. Studi Literatur

Dalam studi literatur penulis mempelajari teori mengenai 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.

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. 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.

2.2 Perancangan Sistem

2.2.1 Analisis Kebutuhan Sistem

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 :

1. Menyisipkan pesan (encode)

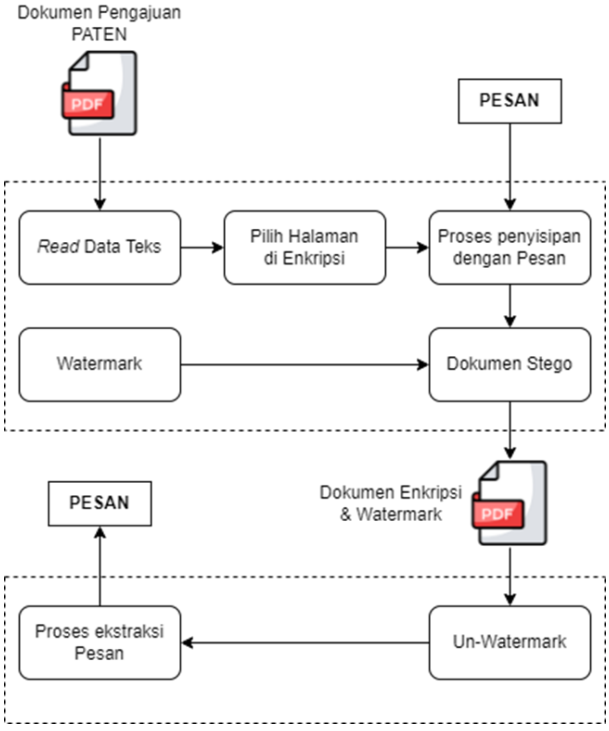
Pada fungsi ini sistem bertugas untuk melakukan penyisipan pesan teks ke dalam PDF yang telah di inputkan oleh *user*. Sistem ini akan memasukkan pesan ke dalam PDF dengan menggeser baris baris bit teks yang ada pada PDF, apabila bit bernilai 1 maka akan dimasukkan dalam baris bit ganjil, jika bit bernilai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

2. 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 ektraksi kedalam bit 1 dan bit 0 setelah itu dikonversikan kembali ke dalam bentuk karakter. Kemudian sistem mencetak pesan ke layar.

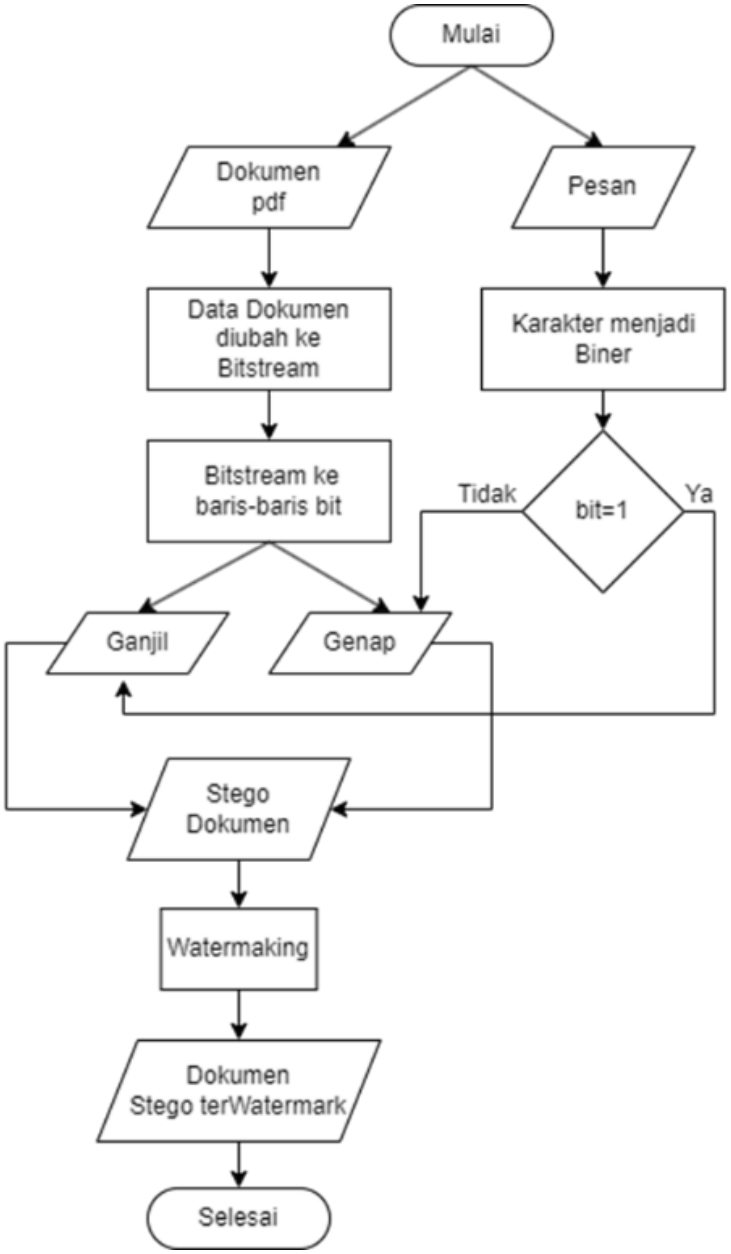
2.2.2 Analisis Alur Sistem

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



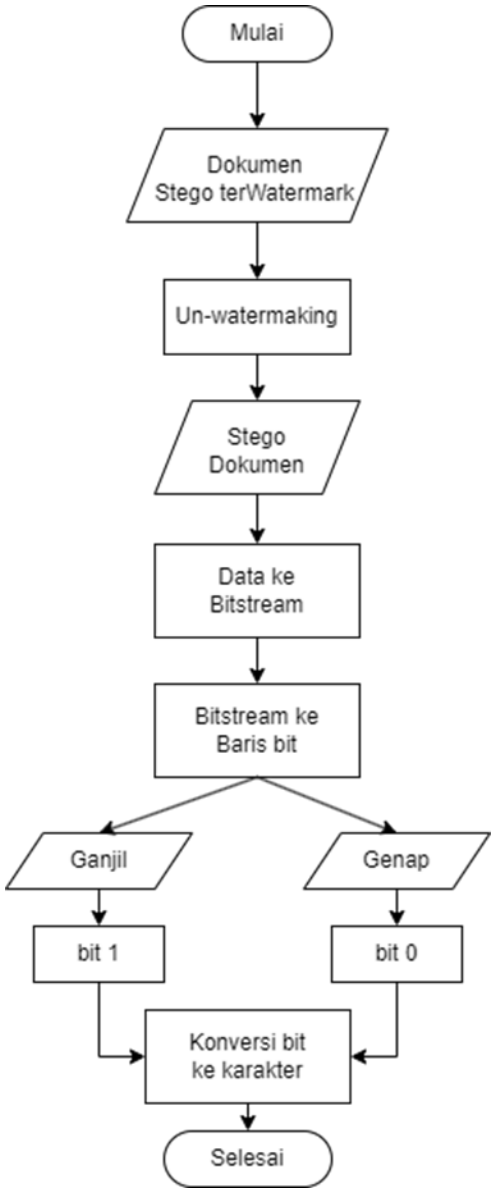
Gambar 1. Alur Sistem

Sebagai gambaran alur proses sistem dapat di lihat pada gambar 1. 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 enskripsi dengan menyisipi sebuah pesan dan menghasilkan dokumen baru yang kemudian diberi *watermark*.



Gambar 2. Proses Encode

Pada menu encode 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 *watermaking*. Untuk *flowchart* dapat dilihat pada gambar 2.



Gambar 3. Proses Decode

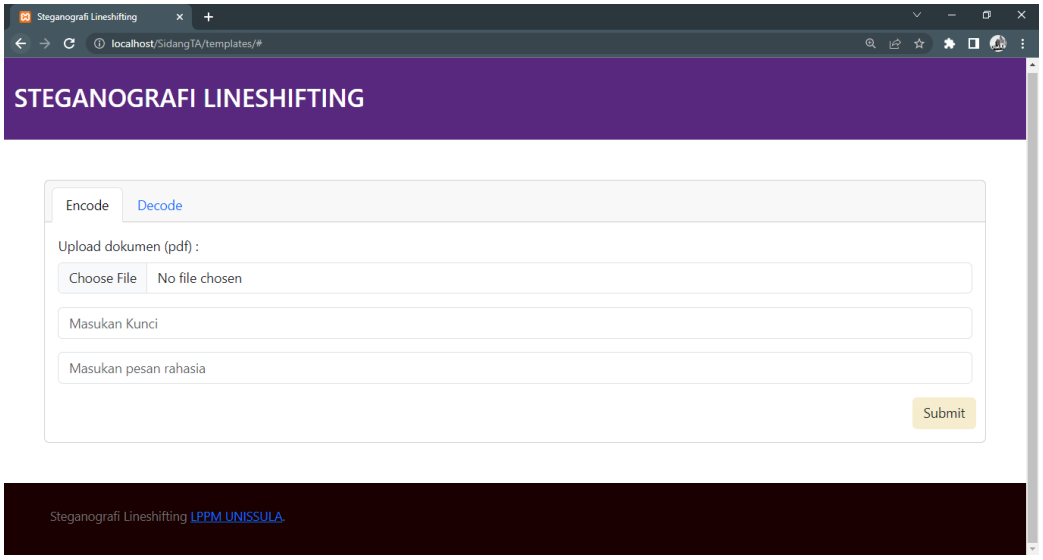
Pada proses decode user memasukkan dokumen encode lalu pada prosesnya *watermark* di hilangkan setelah itu isi dari dokumen steganografi di ubah kembali ke dalam bentuk bitstream yang kemudian dibagi menjadi dua group bit genap dan ganjil. Di ektraksi kedalam bit 1 dan bit 0 setelah itu dikonversikan kembali ke dalam bentuk karakter. Untuk flowchart dapat dilihat pada gambar 3.

3. HASIL DAN ANALISA

Sistem ini memiliki dua proses utama, yaitu encode dan decode. Proses encode akan menyisipkan pesan yang ditentukan oleh pengguna ke dalam file PDF dengan menggeser baris-baris yang merupakan baris genap atau ganjil. Proses decode akan mengekstrak pesan yang tersimpan dalam file PDF dengan mengeser baris-baris yang merupakan baris genap atau ganjil kembali ke posisi semula.

3.1. User Interface

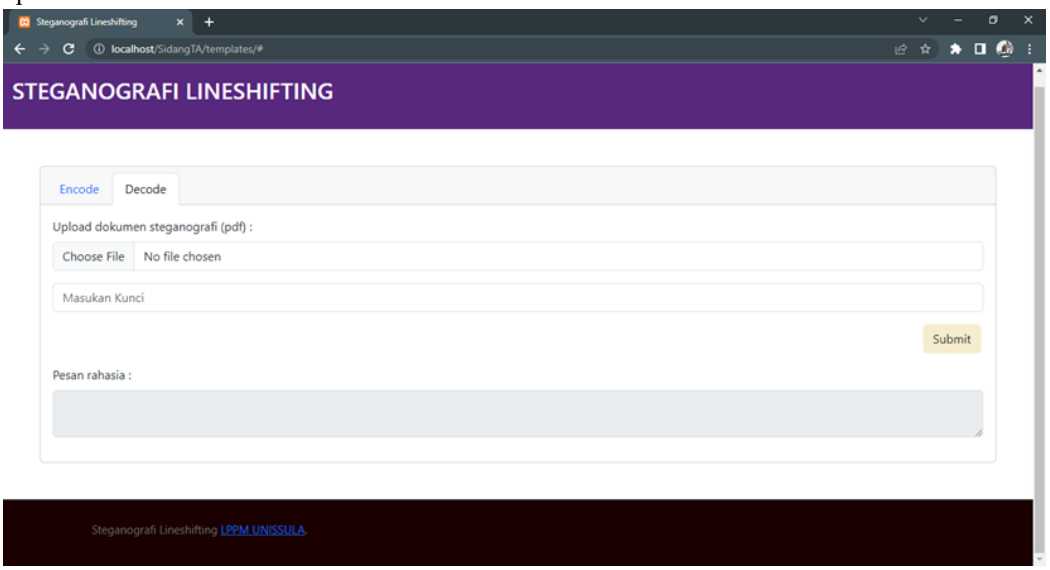
1. Tampilan Encode



Gambar 4. Tampilan Menu Encode

Pada gambar 4. merupakan tampilan untuk fungsi encode. Pada menu 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.

2. Tampilan Decode



Gambar 5. Tampilan Menu 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.

3.2. Pengujian Sistem

Tabel 1. Tabel Pengujian

Skenario Pengujian	Kasus Pengujian	Hasil Pengujian	Kesimpulan
Menyisipkan pesan ke dalam file PDF	Upload PDF 1 halaman, Kunci dan Pesan	Sesuai	Tidak ada error
Menyisipkan pesan ke dalam file PDF dengan jumlah halaman yang berbeda.	Upload PDF 4 halaman, Kunci dan Pesan	Sesuai	Tidak ada error
Menyisipkan pesan ke dalam file PDF dengan jumlah halaman yang berbeda.	Upload PDF 1 halaman, Kunci dan Pesan 34 Karakter	Sesuai	Tidak ada error
Menyisipkan pesan ke dalam file PDF dengan panjang pesan yang berbeda	Upload PDF 1 halaman, Kunci dan Pesan 35 Karakter	Ekstraksi Pesan tidak sesuai	Tidak ada error
Menyisipkan pesan ke dalam file PDF dengan panjang pesan yang berbeda	Upload PDF 4 halaman, Kunci dan Pesan	Sesuai	Tidak ada error

Dari tahapan pengujian yang dilakukan dapat dilihat bahwa sistem penyisipan pesan menggunakan bahasa pemrograman python dapat digunakan untuk steganografi *Line Shifting*. Dimana ada lima kasus uji untuk melakukan testing.

Ada satu kasus uji yang mengalami kegagalan saat encode 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.

4. 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 implementasikan untuk melakukan proses pesnyisipan pesan berupa teks ke dalam pdf. 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. Masih adanya karakter yang bukan merupakan karakter pesan yang ikut tercetak pada saat proses decode

DAFTAR PUSTAKA

[1] N. Ratama dan Munawaroh, "Implementasi Metode Kriptografi dengan Menggunakan Algoritma RC4 dan Steganografi Least Significant Bit Dalam Mengamankan Data Berbasis Android," *Jurnal Media Informatika Budidarma*, vol. 6, no. 2, hlm. 1272–1281, 2022, doi: 10.30865/mib.v6i2.3902.

[2] D. Riansyah, A. Wijaya, S. Kom, H. Suroyo, S. Si, dan M. Kom, "IMPLEMENTASI PENGAMANAN DOKUMEN MENGGUNAKAN METODE STEGANOGRAFI LINE-SHIFTING."

[3] I. Adiniarti, "Implementasi Steganografi Pada Media Teks Dengan Metode Line-Shift Coding dan Metode Centroid," 2009.

[4] I. M. Yusup, Carudin, dan I. Purnamasari, "Implementasi Algoritma Caesar Cipher Dan Steganografi Least Significant Bit Untuk File Dokumen," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 6, no. 3, Des 2020, doi: 10.28932/jutisi.v6i3.2817.

[5] S. Abdurrahman dan A. Prapanca, "Pengamanan File Dokumen Ujian Dengan Image Steganography Metode Lsb," *Journal of Informatics and Computer Science*, vol. 03, 2021.

[6] E. Nirmala, "Penerapan Steganografi File Gambar Menggunakan Metode Least Significant Bit (LSB) dan Algoritma Kriptografi Advanced Encryption Standard (AES) Berbasis Android," *Jurnal Informatika Universitas Pamulang*, vol. 5, no. 1, hlm. 36, 2020, doi: 10.32493/informatika.v5i1.4646.

[7] D. Riansyah *dkk.*, "Implementasi Pengamanan Dokumen Menggunakan Metode Steganografi Line-," *eprints.binadarma.ac.id*, hlm. 1–8, 2022, [Daring]. Available: http://eprints.binadarma.ac.id/10610/1/if025_penelitian_s1.pdf

[8] M. Gilvy Langgawan Putra, M. Ihsan Alfani Putera, P. Studi Informatika, dan J. Matematika dan Teknologi Informasi Institut Teknologi Kalimantan, "ANALISIS PERBANDINGAN METODE SOAP DAN REST YANG DIGUNAKAN PADA FRAMEWORK FLASK UNTUK MEMBANGUN WEB SERVICE," 2019. Diakses: Des 29, 2022. [Daring]. Available: http://www.ejournal.upnjatim.ac.id/index.php/scan/article/view/1480/1213