

PENGAMANAN CITRA DIGITAL DENGAN STEGANOGRAFI MENGUNAKAN METODE (RPP) RANDOM PIXEL POSITIONING

Fery Kurniadi*¹, R. Fanry Siahaan²

Jl. Iskandar Muda No. 1, Medan Baru, Sumatera Utara 20222, telp 0821 6844 7508

^{1,2}Program Studi Teknik Informatika, STMIK Pelita Nusantara, Sumatera Utara

e-mail: * ferykurniadi04@gmail.com, rfanry@gmail.com

Abstrak

Seiring perkembangan teknologi, kerahasiaan suatu informasi sangat penting sebab dapat menyebabkan kerugian materil maupun non materil dan saat ini banyak teknik pengamanan data yang sudah dimanfaatkan, salah satu diantaranya adalah teknik steganografi yang menyembunyikan data rahasia ke dalam wadah (media) digital berupa gambar sehingga keberadaan data rahasia tersebut tidak diketahui oleh orang lain. Penelitian ini bertujuan untuk membangun aplikasi steganografi yang menjadikan alternative dalam pengamanan data agar tidak terjadi manipulasi data pengalokasian dana desa di dinas PMD kabupaten Deli Serdang dengan mengimplementasikan metode Random Pixel Positioning. Hasil penelitian dapat disimpulkan bahwa Penyisipan pesan atau dokumen dengan metode random pixel positioning dalam media gambar dapat dilakukan dengan baik.

Kata kunci : Steganography, Data Security, PMD, Random Pixel Positioning

Abstract

Along with technological developments, the confidentiality of information is very important because it can cause material and non-material losses and currently there are many data security techniques that have been used, one of which is the steganography technique that hides confidential data into digital (media) containers in the form of images so that the existence of confidential data is not known by others. This study aims to build a steganography application that makes an alternative in securing data so that there is no manipulation of data on the allocation of village funds at the PMD department of Deli Serdang district by implementing the Random Pixel Positioning method. The results of the study can be concluded that the insertion of messages or documents with the random pixel positioning method in the image media can be done well.

Keywords— Steganography, Data Security, PMD, Random Pixel Positioning

1. PENDAHULUAN

Kerahasiaan dari suatu informasi sangat penting sebab dapat menyebabkan kerugian materil maupun non materil.

Saat ini banyak teknik pengamanan data yang sudah dimanfaatkan salah satu diantaranya adalah steganografi. Steganografi merupakan sebuah teknik keamanan data dengan cara melindunginya dari pihak lain dengan cara menyembunyikannya ke dalam media yang lain

(Aldo & Hakim, 2018). Steganografi menyembunyikan informasi atau pesan didalam media lain, seperti citra digital, teks, suara, atau video, agar tidak menimbulkan kecurigaan orang lain. Dinas Pemberdayaan Masyarakat dan Desa (DPMD) Kabupaten Deli Serdang yang mengelola penyaluran Dana Desa yang diterima oleh setiap Desa yang ada di 24 Kecamatan di Kabupaten Deli Serdang. Data dana tersebut supaya tidak di dapat dimanipulasi oleh pihak yang tidak berkepentingan maka sangat diperlukan sebuah

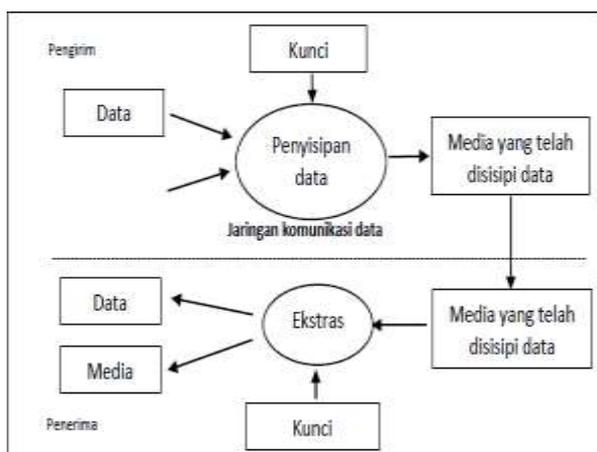
sistem untuk mengamankan data-data dana desa dimaksud. Salah satu metode untuk mengamankan data dana desa namun tidak menimbulkan kecurigaan dari pihak lain adalah steganografi.

Metode *Random Pixel Positioning (RPP)* merupakan salah satu metode yang dapat digunakan untuk pembuatan steganografi. Caranya adalah dengan mengubah file gambar maupun file sisipan kedalam bentuk bit dan memasukkan bit-bit pada file yang disisipkan ke dalam bit-bit pada file gambar.

Berdasarkan uraian pada latar diatas penulis mengangkat judul skripsi “Penerapan Steganografi Pada Citra Digital Menggunakan Metode Random Pixel Positioning (RPP) Untuk Keamanan Data” agar data yang bersifat rahasia aman dan tidak mudah dilihat oleh pihak ketiga.

2. METODE PENELITIAN

Steganografi memiliki 2 langkah utama yaitu embedding/penyisipan dan ekstraksi (pengungkapan) seperti terlihat pada gambar 2.1. Proses penyisipan adalah proses menyisipkan objek tersembunyi atau informasi pesan yang akan disisipkan, dalam objek penutup atau dalam wadah media, untuk menghasilkan file baru yang telah disisipkan pesan. proses extracting adalah proses mengembalikan seluruh hidden object setelah dimasukkan ke cover object (Rohmanu, 2017).



Sumber: (Rohmanu, 2017)

Beberapa Kriteria-kriteria yang harus dipenuhi dalam pembuatan steganografi. Kriteria - kriteria tersebut ialah (Morkel et al., 2005):

1. *Imperceptibility* ialah keberadaan pesan tidak dapat dipersepsi oleh indrawi. Jika pesan

disisipkan ke dalam sebuah citra, citra yang telah disisipi pesan harus tidak dapat dibedakan dengan citra asli oleh mata. Begitu pula dengan suara, telinga harus mendapati perbedaan antara suara asli dan suara yang telah disisipi pesan.

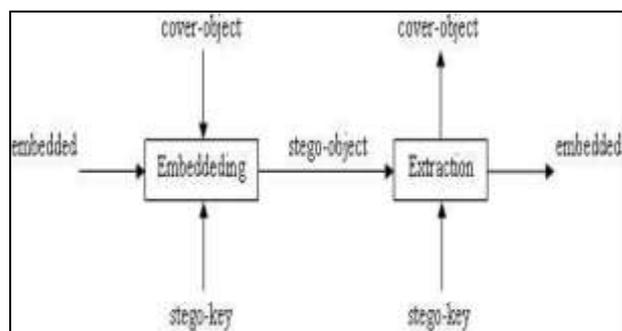
2. *Fidelity* ialah kualitas media penampung tidak berubah banyak akibat penyisipan. Perubahan yang terjadi harus tidak dapat dipersepsi oleh indra.
3. *Recovery* ialah pesan yang disembunyikan harus dapat diungkap kembali. Tujuan steganografi adalah menyembunyikan informasi, maka sewaktu-waktu informasi yang disembunyikan harus dapat diambil kembali untuk dapat digunakan lebih lanjut sesuai keperluan.

2.1 Konsep dan Terminologi Steganografi

Ada beberapa istilah yang terkait dengan steganografi (Kurniawan dan Agustini, 2018), yaitu:

1. Hidden text atau pesan yang disematkan: pesan tersembunyi.
2. Cover-object: Pesan yang digunakan untuk menyembunyikan pesan yang disematkan.
3. Stego-object: pesan yang sudah berisi pesan yang disematkan.

Dalam steganografi digital, pesan yang disematkan dan cover-objek dapat berupa teks, gambar, audio, atau video. Penyisipan pesan ke dalam media cover-objek disebut encoding, sedangkan ekstraksi pesan dari objek stego disebut decoding. Kedua proses ini mungkin memerlukan kunci rahasia (stegokey) sehingga hanya pihak yang berwenang yang dapat melakukan penyisipan dan ekstraksi pesan, sehingga meningkatkan tingkat keamanan data. Proses umum penyisipan dan ekstraksi pesan ditunjukkan pada Gambar 2.2.



Gambar 2.2 Proses Umum Penyisipan dan Ekstraksi

Pesan

2.2 Random Pixel Positioning (RPP) Steganografi

Random Pixel Positioning merupakan salah satu metode yang dapat digunakan dalam steganografi. Metode ini beroperasi pada domain spasial citra. Berdasarkan analisis sistem penglihatan manusia yang menyatakan bahwa mata manusia tidak sensitif terhadap perubahan piksel yang memiliki kontras tinggi melainkan sensitif terhadap perubahan piksel yang memiliki kontras rendah. Berkat properti ini, dimungkinkan untuk memasukkan lebih banyak bit data rahasia dalam piksel dengan nilai kontras tinggi dan lebih sedikit bit dalam piksel kontras rendah dengan proses penyisipan acak. Inilah logika metode *Random Pixel Positioning* (RPP) dalam steganografi.

Pesan dapat disisipkan dengan mengambil sebanyak t bit dari pesan yang akan disisipkan. Kemudian nilai penempatan acak baru dihitung untuk penyisipan ke dalam gambar menggunakan Persamaan 2.4.

$$d'i=li+b..... (2.4)$$

Dimana:

b : Nilai desimal dari jumlah bit disisipkan.

d_i : Nilai terkecil dari *range* selisih perbandingan dua *pixel*.

Untuk menyisipkan pesan ada beberapa aturan yang harus dipenuhi yaitu :

1. Jika $P_i \geq P_{i+1}$ dan $d'i > d_i$, maka $(P_i + [m/2], P_{i+1} - [m/2])$
2. Jika $P_i < P_{i+1}$ dan $d'i > d_i$, maka $(P_i - [m/2], P_{i+1} + [m/2])$
3. Jika $P_i \geq P_{i+1}$ dan $d'i \leq d_i$, maka $(P_i - [m/2], P_{i+1} + [m/2])$
4. Jika $P_i < P_{i+1}$ dan $d'i \leq d_i$, maka $(P_i + [m/2], P_{i+1} - [m/2])$

Dimana m didapat dari selisih $d'i$ dengan d_i menggunakan persamaan 2.5.

$$M = |d'i - d_i|.....2.5)$$

Proses ini berlanjut sampai semua bit pesan dimasukkan ke dalam gambar. Pesan dari citra stego menggunakan metode ini diawali dengan menghitung nilai positioning random (d_i) antara dua piksel secara acak. Nilai positioning random

digunakan untuk menentukan nilai *continuous ranges* (R).

Berdasarkan informasi tersebut, dimungkinkan untuk mengetahui ukuran data rahasia yang dimasukkan ke dalam piksel, untuk mengambil pesan rahasia yang dimasukkan, proses ekstraksi ini dilakukan sampai semua data rahasia yang telah disisipkan didapatkan kembali.

2.2.1 Proses Penyisipan

Prosedur dalam penyisipan pesan yang digunakan dalam penyisipan pesan menggunakan metode RPP ini mirip dengan prosedur penyisipan pesan di LSB. Prosedur penyisipan pesan dapat dijelaskan dalam persamaan berikut:

$$I_s(i, j) = \begin{cases} I(i, j) - 1, & LSB(I(i, j)) = 1 \text{ and } m = 0 \\ I(i, j), & LSB(I(i, j)) = m \\ I(i, j) + 1, & LSB(I(i, j)) \neq 0 \text{ and } m = 1 \end{cases}$$

Dimana:

$I_s(i, j)$: Stego Object

$I(i, j)$: Media penampung

LSB ($I(i, j)$) : Least Significanti Bit

m : Pesan rahasia

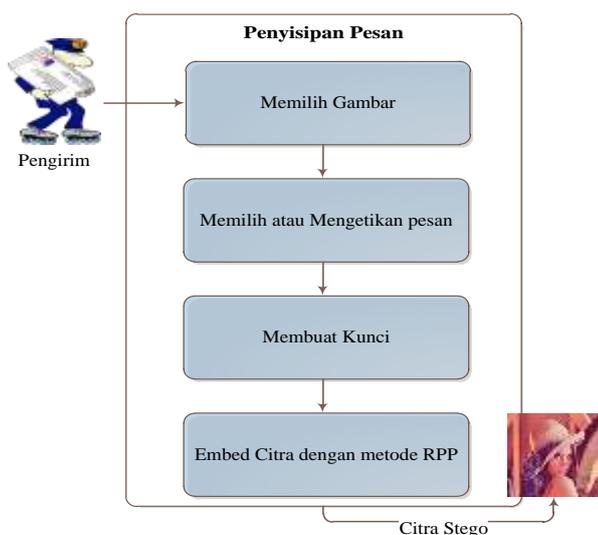
Berikut adalah algoritma penyisipan

Input : media penampung, pesan, kunci

Output : StegoObject

- 1 picture \leftarrow read()
- 2 *inframe* \leftarrow *picture_to_bit*(stego)
- 3 *messages* \leftarrow read()
- 4 *ascii* \leftarrow *text_to_ascii*(*messages*)
- 5 *binary* \leftarrow *ascii_to_binary*(*ascii*)
- 6 *key* \leftarrow read()
- 7 *random_number* \leftarrow *generate_random*()
- 8 **foreach** *inframe*
- 9 *frame* \leftarrow *insertion*()
- 10 *stego_object* \leftarrow *to_object*(*frame*)
- 11 *output*(*stego_object*)

Proses penyisipan digambarkan dalam gambar 4.1 berikut.



Gambar 4.1 Proses Penyisipan Pesan

Berikut adalah algoritma untuk ekstraksi:

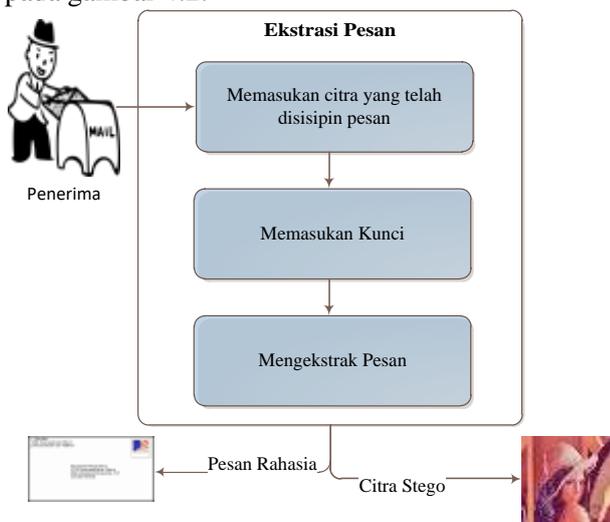
input : *stego, key*

output : *text*

```

1  stego ← read()
2  inframe ← picture_to_bit(stego)
3  key ← read()
4  random ← generate_random_number()
5  for each inframe
6    binary ← extract()
7    output(binary)
8    ascii ← binary_to_ascii(binary)
9    text ← ascii_to_text(ascii)
10 output(text)
    
```

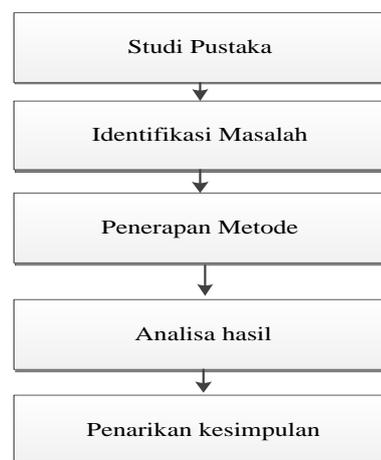
Tahapan-tahapan proses ekstraksi pesan aplikasi steganografi secara umum dapat dilihat pada gambar 4.2.



Gambar 4.2 Proses Ekstraksi Pesan

2.3 Kerangka Kerja Penelitian

Kerang kerja Penelitian ini dilakukan secara sistematis agar tercapai suatu alur kerja yang baik sebagai pedoman bagi peneliti dalam melaksanakan penelitian agar hasil yang diperoleh tidak menyimpang dari tujuan yang diinginkan dan dapat dilaksanakan dengan benar dan sesuai dengan tujuan yang telah ditetapkan. Kerangka Penelitian ditunjukkan pada Gambar 3.1



Gambar 3.1 Kerangka penelitian

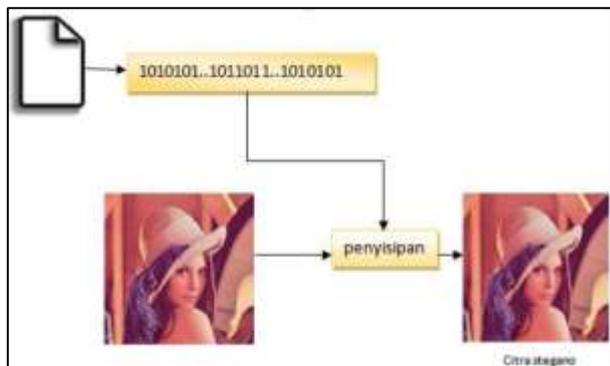
2.4 Analisa Perancangan

Penelitian ini dilakukan secara mandiri dan tidak memerlukan tempat lokasi penelitian sebab pada penelitian ini hanya mengacu pada penerapan metode *random pixel positioning* dalam steganografi. Yang menjadi permasalahan terkait dengan aplikasi steganografi dalam penyisipan pesan yaitu, menyisipkan pesan dalam teks, gambar, suara, dan video. Adapun untuk menyisipkan pesan teks pada mediaum atau file berformat gambar (jpg, png, bmp, dan gift), pada file suara dalam format (mp3, wav, dan wma), serta pada file video dalam format 3gp. Dalam hal pengumpulan data aplikasi ini menggunakan cara studi pustaka, yaitu dengan mengumpulkan data dan informasi terkait pembuatan aplikasi steganografi dari buku teks dan internet.

1. Analisis Proses Penyisipan/ *Embedding*

Proses penyisipan adalah proses menyembunyikan informasi pada media penampung, dalam hal ini media penyisipan adalah citra digital. Proses ini akan menghasilkan citra yang telah

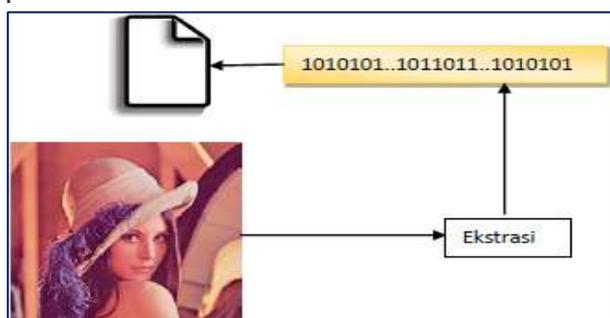
disisipkan pesan (stego-object) yang mirip dengan citra sebelumnya yang disisipkan pesan. Proses penyisipan menggunakan metode Random Pixel Positioning (RPP) yang ditunjukkan pada Gambar 4.1.



Gambar Proses penyisipan

2. Analisis Proses Ekstraksi

Proses ekstraksi adalah proses mengambil informasi yang tersembunyi dalam citra digital. Proses ini akan menghasilkan file informasi yang tersembunyi, dengan input berupa gambar stegoobject. Proses ekstraksi pada metode penempatan piksel acak ditunjukkan pada Gambar 4.8



Gambar Proses Ekstraksi

3. HASIL DAN PEMBAHASAN

Halaman pembuka merupakan tampilan *splash screen* sebelum masuk ke halaman utama. Tampilan ini hanya menyediakan tombol OK untuk memasuki halaman utama.



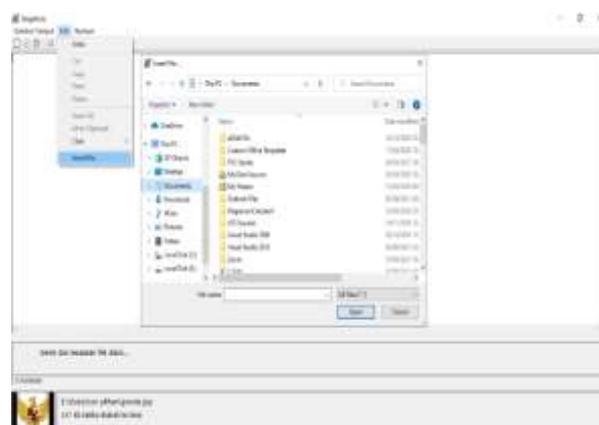
Gambar 5.1 Splash screen

Halaman utama merupakan tampilan yang menyediakan seluruh menu atau perintah yang akan dilakukan dalam mengamankan data dengan steganografi. Menu utama yang tersedia dalam halaman ini adalah menu Gambar/ Sampul, Edit dan Bantuan. Berikut adalah tampilan dari halaman utama.



Gambar 5.2 Halaman Utama

Dokumen atau file yang akan di sisipkan ke dalam media penampung dapat berformat microsoft office, *.pdf atau format dokumen yang lainnya.



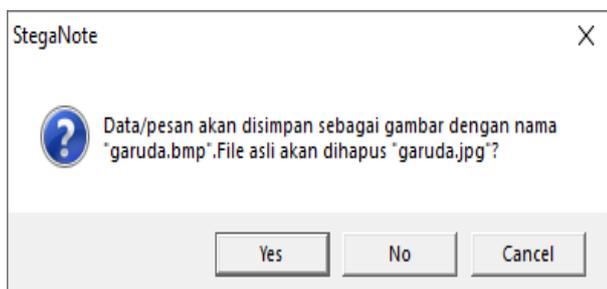
Gambar 5.3 pemilihan dokumen yang akan disisipkan

Penyisipan pesan (*Sosialisasi Kebijakan Dana Desa TA 2021_share.pdf*) merupakan salah satu perintah yang dapat dilakukan dalam metode steganografi yang bertujuan untuk menyisipkan pesan ke dalam media penampung (*garuda.jpg*). Jika dokumen atau file yang akan disisipkan dan media penampung sudah tersedia, maka Langkah berikutnya adalah mengklik ikon yang ber lambang *w* (*write data to image*) untuk melakukan proses penyisipan. Maka sistem akan menyuguhkan tampilan untuk memasukan *password* penyisipan pesan.

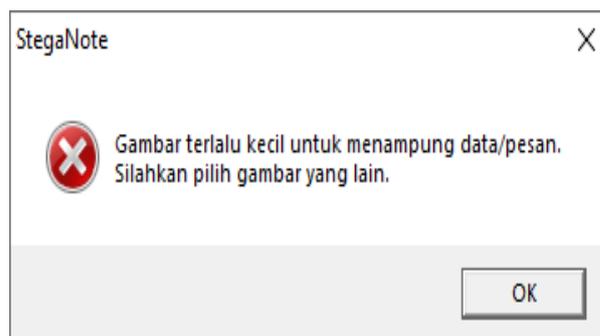


Gambar 5.4 Proses pemasukan *password* dalam penyisipan pesan

Jika tombol Sisipkan di tekan, maka akan muncul pesan dialog yang meminta konfirmasi bahwa media penyimpanan dengan format *.jpg akan diubah ke format *.bmp serta konfirmasi penghapusan media penyimpanan yang asli seperti pada gambar 5.6 berikut.



Gambar 5.5 Konfirmasi proses penyisipan pesan
Jika ukuran media penampung lebih kecil dari media yang akan disimpan maka sistem akan menampilkan pesan sebagai berikut.



Gambar 5.6 Pesan jika ukuran media penampung lebih kecil dari dokumen

Jika media penampung dan file yang akan disisipkan sudah diganti dan ukurannya sudah lebih besar dari media yang akan disisipkan maka akan dilakukan proses penyisipan seperti pada gambar berikut.



Gambar 5.7 Proses penyisipan dokumen ke dalam media penampung

Sama halnya seperti melakukan penyisipan pesan, Ketika media penampung yang telah tersisipi dengan pesan, maka dapat dilakukan dengan pengestrakan dengan cara menekan tombol *R* (*read data from image*), jika media penampung tersebut mengandung pesan yang telah disipin maka sistem akan menampilkan *form* dialog untuk memasukan *password* ekstraksi.



Gambar 5.8 Pemasukan password ekstraksi pesan dari media penampung.

Jika password ekstraksi yang dimasukkan benar maka sistem akan melakukan proses pegekstrakan pesan, seperti yang ditampilkan pada gambar berikut.



Gambar 5.9 Proses ekstraksi pesan dari media penampung

4. KESIMPULAN

Berdasarkan hasil penelitian yang penulis lakukan dengan judul Penerapan Steganografi Pada Citra Digital Menggunakan Metode *Random Pixel Positioning* (RPP) Untuk Keamanan Data memiliki kesimpulan sebagai berikut:

1. Penyisipan pesan dengan metode *random pixel positioning* dalam steganografi mampu menyembunyikan data dengan baik.
2. Ukuran media penampung menjadi besar sebab format media penampung berubah menjadi *.bmp.
3. Rancangan dan tampilan penyisipan pesan dengan steganografi mudah dipahami dan dioperasikan.

5. SARAN

1. Dalam pengembangan berikutnya, penulis menyarankan agar pengembangan sistem dilakukan dengan bebas online. Sehingga dapat dilakukan darimanapun dan kapanpun.
2. Agar ukuran media penampung tidak membesar setelah proses penyisipan perlu dilakukan pemilihan metode yang lain namun dokumen tetap mamu disisipkan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Bapak R. Fanry Siahaan, S.Kom., M.kom., Selaku Dosen Pembimbing saya yang telah banyak membantu, meluangkan waktu dan pikirannya serta banyak memberi nasihat untuk mengarahkan, mendorong, dan membimbing untuk menyelesaikan skripsi ini. Dalam Penyusunan skripsi ini, penulis menyadari adanya kekurangan atau kesalahan yang tidak penulis ketahui, penulis memohon maaf sebesar – besarnya semoga akan ada perbaikan dikemudian hari. Penulis juga menyadari bahwa skripsi ini sangat jauh dari kesempurnaan, hal ini tidak lepas dari keterbatasan waktu dan ketidaksempurnaan yang penulis miliki. Untuk itu penulis mengharapkan saran dan perbaikan dari penerus selanjutnya, sehigga skripsi ini dapat bermanfaat bagi kita semua.

DAFTAR PUSTAKA

- [1] Amri, U., Wijaya, I. G. P. S., & Bimantoro, F. (2018). Steganografi Menggunakan Metode Pencocokan LSB dan Karakter Non-Breaking Space Sebagai Penanda Pesan. *Journal of Computer Science and Informatics Engineering (J-Cosine)*. <https://doi.org/10.29303/jcosine.v1i1.18>
- [2] Darwis, D. (2017). Teknik Steganografi untuk Penyembunyian Pesan Teks Menggunakan Algoritma GIFSHUFFLE. *Jurnal Teknoinfo*. <https://doi.org/10.33365/jti.v1i1.6>.
- [3] Jannah, L. M., Santoso, I., & Christyono, Y. (2018). KINERJA STEGANOGRAFI METODE END OF FILE PADA DATA CITRA DIGITAL. *TRANSIENT*.

<https://doi.org/10.14710/transient.7.1.34-39>

- [4] L. M. Marvel, C. G. Boncelet, and C. T. Retter, "Spread spectrum image steganography," *IEEE Trans. Image Process.*, 1999, doi: 10.1109/83.777088.
- [5] Kurniawan, M., & Agustini, S. (2018). Algoritma Steganografi untuk Pengamanan Data Teks ke dalam Citra Digital Menggunakan XOR Sederhana. *INTEGER: Journal of Information Technology*. <https://doi.org/10.31284/j.integer.2018.v3i2.416>
- [6] Michael, K. (2012). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. *Computers & Security*. <https://doi.org/10.1016/j.cose.2012.03.005>
- [7] Morkel, T., Olivier, M. S., & Eloff, J. H. . (2005). an Overview of Image Steganography. *Africa*.
- [7] Munir, R. (2013). Pengantar Pengolahan Citra. *Pengolahan Citra Digital*.
- [8] Rohmanu, A. (2017). Implementasi Kriptografi dan Steganografi Dengan Metode Algoritma Des dan Metode End Of File. *Jurnal Informatika SIMANTIK*.
- [9] Rosa & Salahuddin, 2013. (2013). UML, Use Case Diagram, Activity Diagram, Class Diagram. In *Rekayasa Perangkat Lunak Terstruktur*.
- [10] Y. Huang, C. Liu, S. Tang, and S. Bai, "Steganography integration into a low-bit rate speech codec," *IEEE Trans. Inf. Forensics Secur.*, 2012, doi: 10.1109/TIFS.2012.2218599.
- [11] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on lsb matching revisited," *IEEE Trans. Inf. Forensics Secur.*, 2010, doi: 10.1109/TIFS.2010.2041812.