Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)

journal homepage: http://journal.lembagakita.org/index.php/jtik

Teknik *Steganography* untuk Menyisipkan Pesan pada Sebuah Citra Menggunakan Metode *Least Significant Bit* (LSB)

Ahmad Khuzaifi [1*], Fauziah [2], Iskandar Fitri [3]

[1,2,3] *Program Studi Teknik Informatika, Fakultas Teknologi Komunikasi dan Informatika, Universitas Nasional.*

a r t i c l e i n f o

Article history:
Received 13 August 2021
Received in revised form
3 September 2021
Accepted 2 October 2021
Available *online* July 2022

DOI:
https://doi.org/10.35870/jtik.v6i3.461

Keywords:
Copyright; Steganography; MATLAB.

a b s t r a c t

Copyright is a direct right granted to the creator of a work in any form that is real and recognized in accordance with the provisions of the legislation in force in the area. Copyright infringement is very detrimental to the creators of works who have tried hard in creating a work. The steganography technique can be a solution to insert hidden messages into digital data. In writing this scientific research journal, an application was made to give a hidden message sign to an image. The goal is to protect copyrighted works from being easily recognized by irresponsible parties. Making this simple application using MATLAB R2021a software. By using the Least Significant Bit [LSB] method, what happens is that the data bits will be inserted into the digital image bit by changing the last bit. The result is that the image inserted with the message does not experience significant changes, but when the image undergoes an extraction process, the inserted message will appear. The results of the Least Significant Bit [LSB] method in this study are successful in inserting a .txt file into the hidden original image so that it does not change the visualization of the image but only changes the image size from 56.9KB to 732KB.

Kata Kunci:
Hak Cipta; Steganography; MATLAB.

a b s t r a k

Hak cipta merupakan hak langsung yang diberikan kepada pembuat suatu karya dalam bentuk apapun yang nyata dan diakui sesuai dengan ketentuan peraturan perundang-undangan yang berlaku di wilayah tersebut. Pelanggaran hak cipta sangat merugikan para pencipta karya yang sudah berusaha keras dalam menciptakan suatu karya. Teknik Steganography dapat menjadi solusi untuk menyisipkan pesan tersembunyi ke dalam data digital. Pada penulisan jurnal penilitian ilmiah ini, dibuatlah aplikasi untuk memberikan tanda pesan tersembunyi pada sebuah citra. Tujuannya untuk melindungi karya cipta agar tidak mudah diakui oleh pihak yang tidak bertanggungjawab. Pembuatan aplikasi sederhana ini menggunakan software MATLAB R2021a. Dengan menggunakan metode Least Significant Bit[LSB], maka yang terjadi adalah bit-bit data akan disisipkan ke dalam bit citra digital dengan mengubah bit terakhirnya. Hasilnya adalah citra yang disisipkan pesan tidak mengalami perubahan yang signifikan, namun ketika citra mengalami proses ekstrak maka pesan yang disisipkan akan muncul. Hasil dari metode Least Significant Bit [LSB] pada penelitian ini adalah berhasil melakukan penyisipan file .txt ke dalam citra asli yang tersembunyi sehingga tidak merubah visualisasi citra namun hanya mengubah ukuran citra dari 56,9KB menjadi 732KB.

Corresponding author. Email: ahmadkhuzaifi20.ak@gmail.com [1].

1. Latar Belakang

Pada era digital seperti saat ini, kemudahan mengakses *internet* untuk mencari beragam informasi sangatlah mudah. Namun di satu sisi juga dapat menimbulkan kerugian. Misalnya ketika mengupload sebuah gambar di *internet*, maka semua orang bebas untuk mengunduhnya ke perangkat masing-masing tanpa harus meminta izin kepada pemilik gambar tersebut. Etika dalam memakai atau mengutip karya orang lain pun sering kali dilupakan. Karena itu, untuk melindungi hak cipta dalam berkarya dibutuhkan sistem keamanan yang menjamin kepemilikannya. Termasuk dalam *file* citra atau gambar yang banyak tersebar di *internet*.

Steganography pada citra digital dapat dijadikan solusi untuk menyimpan data rahasia ke dalam wadah citra digital. *Steganography* dapat digunakan juga untuk menyisipkan pesan yang bersifat rahasia, karena dengan teknik *Steganography* sulit dideteksi keberadaannya [1]. Pesan yang disisipkan berupa *file* berformat .txt yang telah dibuat sebelumnya untuk kemudian dimasukkan ke dalam citra digital. *Steganography* berasal dari bahasa Yunani, yang berarti tulisan yang tertutup/tersamar ("*covered letter*")[2]. Sesuai pengertiannya, citra digital yang disisipkan tidak mengalami perubahan secara tampilan. Namun perubahan terlihat pada ukuran gambar dalam satuan Kilo*Byte* (KB). Terlihat pada contoh awal citra asli berukuran 56,9 KB, namun setelah melalui proses Steganotraphy hasil output citra berukuran 732 KB. Terjadi demikian karena citra asli telah di enkripsi sebelumnya dengan pesan berformat .txt. Enkripsi adalah sebuah proses penyandian yang melakukan perubahan sebuah kode atau pesan dari plainteks, menjadi cipherteks [3]. Dengan mengubah bit bit data ke dalam bit citra digital menggunakan metode *Least Significant Bit* [LSB].

Metode *Least Significant Bit* [LSB] pada penelitian ini menggunakan teknik *Steganography*. Berbeda dengan penelitian yang dilakukan oleh Ika Febriana dan Ganjar Aji yaitu menerapkan teknik kriptografi ke dalam sistem keamanan SMS Android dan berhasil dengan baik [4], teknik *Steganography* dengan metode *Least Significant Bit* [LSB] ini tidak memiliki efek yang tampak jelas pada citra. Karena bit piksel metode LSB memiliki kontribusi yang kecil terhadap penampakan piksel citra tersebut. *Watermarking* atau tanda air bisa diartikan sebagai suatu teknik penyembunyian data atau informasi rahasia ke dalam suatu data lainnya dengan cara menumpangi (kadang disebut host data), tanpa orang lain menyadarinya adanya data tambahan pada data host-nya (Rinaldi Munir, 2004: Pengolahan Citra Digital) [5]. *Watermarking* dapat dikategorikan sebagai penanda bahwa citra tersebut sudah memiliki label kepemilikan data digital. Sejarah *watermarking* sudah ada sejak 700 tahun yang lalu. Pada akhir abad ke-13, pabrik kertas di Fabriano, Italia, membuat kertas yang diberi *watermark* dengan cara menekan bentuk cetakan gambar atau tulisan pada kertas yang baru setengah jadi [6]. *Watermarking* merupakan salah satu dari bentuk *Steganography* yaitu mengenai ilmu menyisipkan pesan rahasia ke dalam suatu data.

2. Metode Penelitian

Dalam metodologi penelitian ini menggunakan tahapan sebagai berikut:

Pemahaman Sistem dan Literatur

Pada tahap ini akan dijelaskan mengenai apa yang diperlukan oleh sistem dan literatur terhadap teknik *Steganography* dan metode yang digunakan yaitu *Least Significant Bit* (LSB). Penelitian yang dilakukan oleh I Gede Wiryawan, Sariyasa dan I Gede Aris Gunadi dalam *Steganography* berdasarkan metode LSB pada citra digital, mereka membuat tampilan data citra raw (mentah) lalu dilakukan teknik kompresi dan hanya sedikit informasi yang ada dalam citra asli yang hilang [7]. Meskipun hanya sedikit perbedaan yang timbul setelah citra dikompresi, tetap saja terdapat perbedaan di dalamnya. Pada metode *Least Significant Bit* (LSB), bit terkecil pada pesan rahasia akan mengubah bit bit pada citra digital asli, untuk kemudian disisipkan menggunakan teknik *Steganography*.

Analisis dan Perancangan Sistem

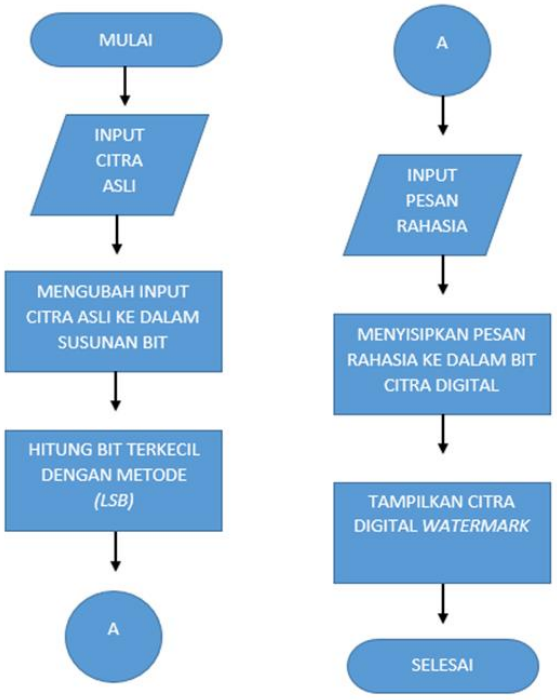
Tahap ini meliputi analisis dan perancangan sistem menggunakan studi literatur dan mempelajari sistem dan software yang ada pada penelitian ini [8]. Adapun analisis terdiri dari analisis kebutuhan fungsional dan non-fungsional, juga dalam perancangannya disertai dengan diagram alir atau *flowchart*.

a. Analisis Kebutuhan Fungsional

Kebutuhan fungsional merupakan proses-proses yang nantinya akan dilakukan oleh sistem dalam penerapan

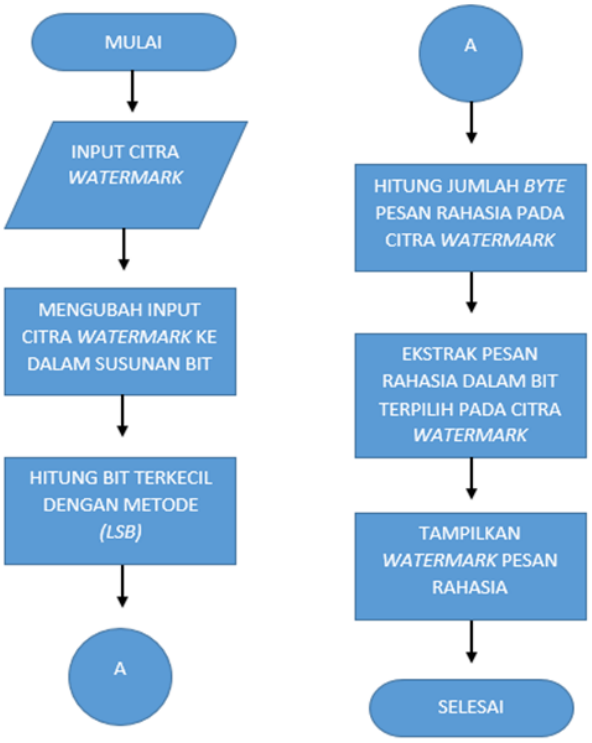
aplikasinya, berikut adalah analisisnya:

1) Tahap Enkripsi
   a. User masuk ke dalam tampilan awal aplikasi.
   b. Memilih data citra asli pada *database* komputer.
   c. Sistem melakukan proses mengubah citra asli ke dalam susunan bit.
   d. Sistem melakukan perhitungan bit terkecil dengan metodes LSB.
   e. User menginput pesan rahasia yang sudah disiapkan berformat *file* .txt.
   f. Sistem menyisipkan bit pesan rahasia ke dalam bit bit citra digital.
   g. Sistem menampilkan tampilan citra digital yang sudah disisipkan pesan rahasia.



Gambar 1. *Flowchart* Proses Enkripsi

2) Tahap Dekripsi
   a. User masuk ke halaman awal aplikasi.
   b. Memilih data citra *watermark* yang telah dienkripsi sebelumnya.
   c. Sistem mengubah input citra *watermark* ke dalam susunan bit.
   d. Sistem menghitung bit terkecil dan mengembalikannya pada nilai asli dari pesan yang disisipkan.
   e. Sistem menghitung jumlah *byte* pesan rahasia pada citra *watermark*.
   f. Sistem melakukan ekstrak pesan rahasia yang ada di dalam citra *watermark*.
   g. Sistem menampilkan *watermark* pesan rahasia.



Gambar 2. *Flowchart* Proses Dekripsi

b. Analisis Kebutuhan Non-fungsional

Kebutuhan non-fungsional dilakukan untuk mengetahui spesifikasi apa saja yang dibutuhkan dalam menjalankan sistem, berikut adalah hasil analisinya:

1) Spesifikasi Perangkat Keras (Hardware) :
   a. Prosesor : Intel Core i5-5200U @2.20GHz.
   b. RAM : 8 GB.
   c. Hard Disk : 500 GB
   d. VGA : Nvidia GeForce 920M
2) Spesifikasi Perangkat Lunak (Software) :
   a. OS/Operating System Windows 10 64-bit.
   b. Software MATLAB R2021a.

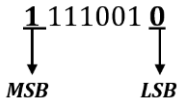
c. Teknik *Steganography*

Dalam sistem keamanan komputer, teknik *Steganography* digunakan untuk menyembunyikan data rahasia saat melakukan proses enkripsi. Jika enkripsi berhasil dipecahkan (*decipher*) pesan / data rahasia tetap tidak terlihat karena disembunyikan oleh sistem [9]. Proses *Steganography* bekerja dengan cara menyisipkan pada media tertentu seperti citra, *audio*,

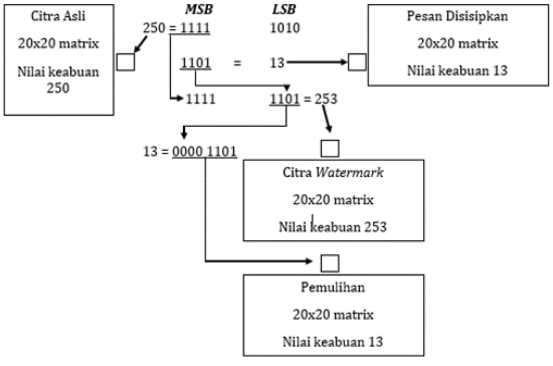
video dan lainnya. Metode yang dilakukan pada penelitian kali ini adalah dengan *Least Significant Bit* (LSB) dengan mengganti bit terkecil yang berada paling kanan pada barisan bit. Terdapat bit yang terbesar bernama *Most Significant Bit* (MSB) yang berada paling kiri pada barisan bit. Alasan penelitian ini dipilih metode *Least Significant Bit* (LSB) adalah karena jika mengganti bit terendah, maka perubahan pada citra digital tidak terlalu terlihat. Misalnya pada citra asli *byte* tersebut menyatakan warna hijau, maka perubahan satu bit tidak merubah tampilan visual citra karena penglihatan mata manusia juga terbatas dalam melihat hal-hal yang kecil seperti *byte*.

d. Metode *Least Significant Bit* (LSB)

Metode ini merupakan proses perubahan bit terakhir yang memiliki nilai tidak berarti atau terkecil. Karena dalam sebuah *byte* (terdiri dari 8 bit) terdapat 2 jenis bit yaitu *Most Significant Bit* (MSB) dan *Least Significant Bit* (LSB). Berikut contoh penyusunan bit dalam sebuah *byte*:



Metode *Least Significant Bit* (LSB) merupakan proses merubah bit terendah yang ada pada citra digital asli. Dipilihnya metode ini karena dengan mengubah bit terakhir maka perubahan yang dihasilkan tidak terlalu berdampak pada tampilan citra [10]. Mekanisme LSB dapat dilihat dengan mengambil contoh pada gambar 8 bit dengan membagi 4 bit MSB dan 4 bit LSB.



Gambar 3. Mekanisme *Least Significant Bit* (LSB)

Gambar 3 menunjukkan bahwa pada bagian LSB lah yang diubah menjadi sebuah nilai dari pesan yang akan disisipkan. Setelah itu seluruh pixel yang ada dikumpulkan kembali menjadi citra utuh seperti semula karena yang mengalami perubahan hanya bit yang terkecil dan tidak memiliki arti. Itulah salah satu keuntungan yang dimiliki oleh metode *Least Significant Bit* (LSB).

e. Histogram

Histogram digunakan untuk mengetahui informasi yang penting dalam isi citra digital yaitu dengan menampilkan grafik yang menggambarkan penyebaran nilai-nilai pixel pada citra. Histogram juga dapat memperlihatkan kecerahan dan kontras dari sebuah gambar, sehingga dapat dikatakan histogram merupakan salah satu alat bantu yang penting dalam pengolahan citra secara kualitatif dan kuantitatif.

3. Hasil dan Pembahasan

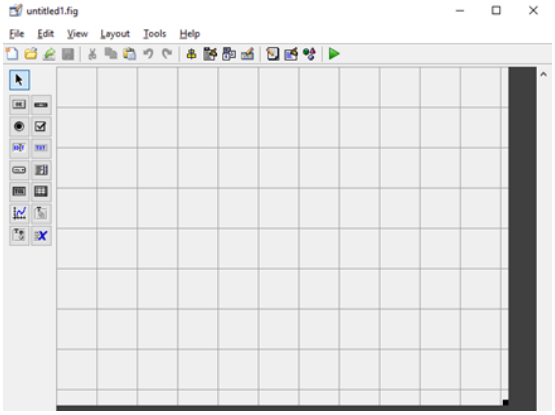
Pada tahap ini akan dijelaskan perancangan dan pemrograman aplikasi dengan menggunakan software MATLAB R2021a. Fitur GUI (*Graphical User Interface*) pada MATLAB sangat memudahkan dalam pembuatan tampilan aplikasi. *File* yang dihasilkan oleh MATLAB berekstensi .m untuk proses pemrograman dan .fig untuk aplikasi GUI berjalan.

Implementasi Aplikasi

Implementasi aplikasi adalah tahap penerapan dan pengujian terhadap aplikasi sehingga siap dioperasikan. Pada tahap ini akan terlihat kekurangan dan kelebihan yang dimiliki oleh aplikasi tersebut. Berikut adalah implementasi aplikasi dalam penelitian ini :

1) Tampilan Blank GUI

Merupakan tampilan awal pada MATLAB saat menggunakan fitur GUI dengan menginput perintah ”GUIDE” pada command window, lalu muncul tampilan Blank GUI.



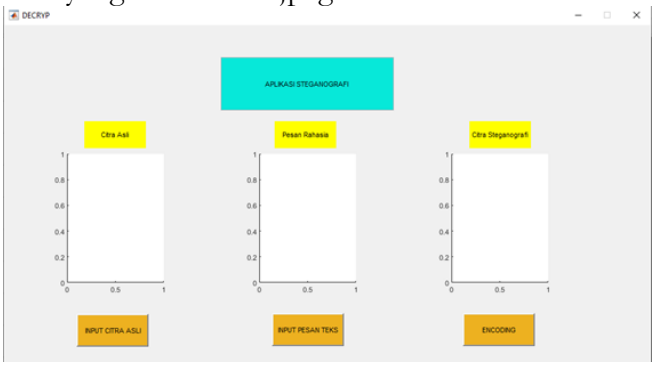
Gambar 4. Tampilan Blank GUI

2) Tampilan Desain Halaman Aplikasi

Menggunakan tools yang ada pada fitur GUI untuk mendesain tampilan aplikasi, seperti : Axes, Push Button, Edit Text dan sebagainya. *File* GUI yang disimpan berformat .fig. Ketika program dijalankan maka akan diarahkan ke bagian pemrograman, dan format *file* tersebut adalah .m.

a. Halaman Proses *Encoding*

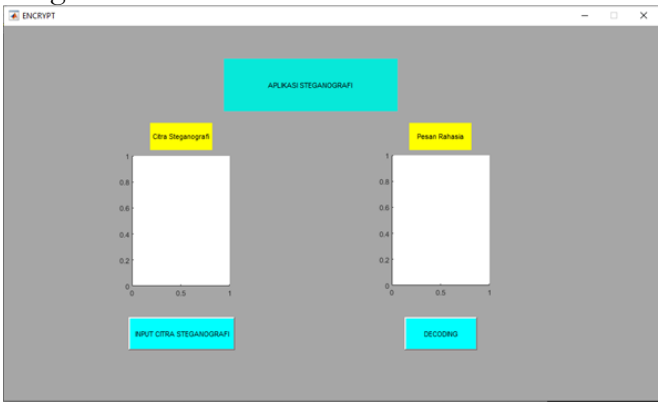
Implementasi yang dilakukan user pada halaman ini bertujuan untuk menyisipkan pesan rahasia ke dalam citra digital asli. Pesan yang dimasukkan berformat .txt yang akan dimasukkan ke dalam data yang berformat .jpeg.



Gambar 5. Tampilan *Encoding*

b. Halaman Proses *Decoding*

Implementasi pada halaman ini adalah sebagai pembuktian bahwa citra digital yang telah disisipkan pesan rahasia tersebut benar disisipkan. Caranya adalah dengan mengekstrak citra yang telah disisipkan pesan rahasia, jika memang disisipkan maka data *watermark* akan muncul dengan format .txt.



Gambar 6. Tampilan *Decoding*

Pengujian Aplikasi

Proses hasil uji coba aplikasi dapat dibagi dalam 2 fase, yaitu Proses *Encryption* adalah proses untuk mengenkripsi citra asli dengan *watermark* sehingga menghasilkan keluaran citra *watermark* yang dapat dilihat pada Tabel 1. Proses Kedua adalah Proses *Decryption* yaitu suatu proses mengekstrak citra *watermark* untuk melihat isi dari pesan rahasia yang terdapat di dalamnya yang dapat dilihat pada Tabel 2.

Tabel 1. Hasil Uji Coba Proses *Encryption*

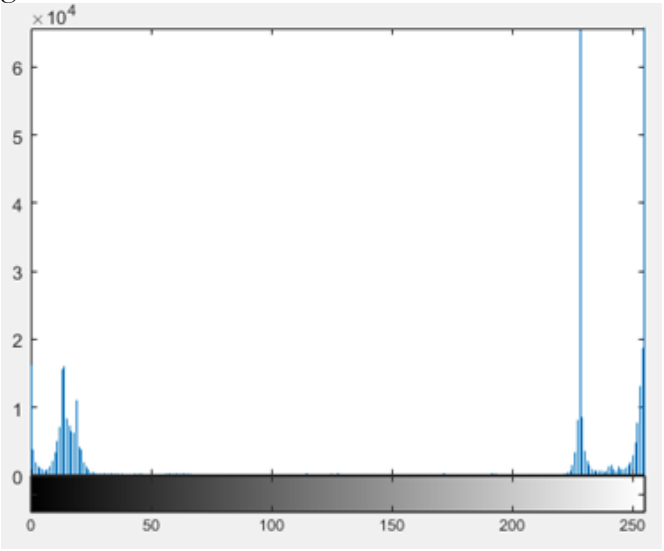
No.	**Citra Asli**	***Watermark***	**Citra *Watermark***
1.	 asli.jpeg 56,9 *KB* (500x500)	 rahasia.txt 32 *bytes*	 encrypted_Image. jpeg 732 *KB* (500x500)

Tabel 2. Hasil Uji Coba Proses *Decryption*

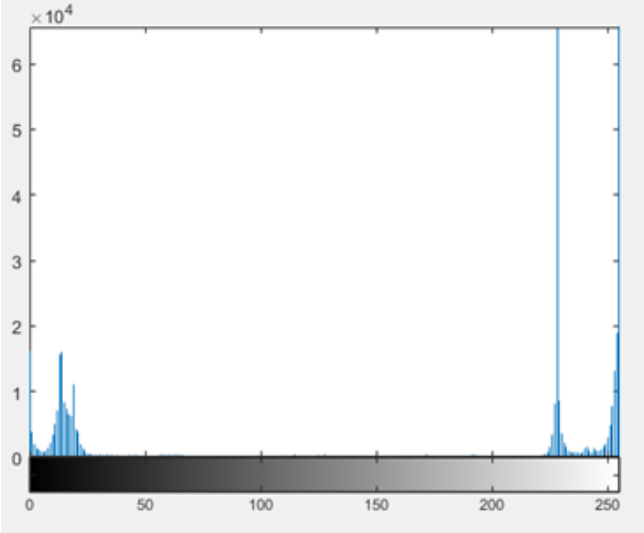
No.	Citra *Watermark*	*Watermark*
1.	 encrypted_Image.jpeg 732 *KB* (500x500)	 rahasia.txt 32 *bytes*

Proses Histogram

Pada pengujian gambar citra asli dan citra *watermark* mengalami perbedaan grafik namun tidak terlalu signifikan, perbedaan tersebut dapat dilihat pada gambar 5 dan 6.



Gambar 7. Histogram Citra Asli



Gambar 8. Histogram Citra *Watermark*

Pembahasan

Metode *Least Significant Bit* (LSB) yang digunakan pada proses uji coba tersebut memberikan efek pada besaran size ukuran citra yang telah disisipkan. Terlihat bahwa citra awal berukuran 56,9 KB namun saat disisipkan *watermark* berupa *file* .txt sebesar 32 *byte*s maka ukuran citra *watermark* menjadi 732 KB. Namun pada tampilan visual citra dan ukuran dimensi citra keduanya sama antara citra asli dengan citra yang telah disisipkan pesan, itu berarti Metode *Least Significant Bit* (LSB) pada penelitian ini berhasil dilakukan.

File watermark merupakan *file* .txt yang berisi kalimat "Gambar Ini Milik Kasih Nama Kopi" yang jika dihitung perkarakter berjumlah 32 *byte*s. Berikut adalah penjabaran bit dari *file watermark* tersebut.

Teks ASCII:
Gambar Ini Milik Kasih Nama Kopi

Biner:

```
01000111  01100001  01101101  01100010
01100001  01110010  00100000  01001001
01101110  01101001  00100000  01001101
01101001  01101100  01101001  01101011
00100000  01001011  01100001  01110011
01101001  01101000  00100000  01001110
01100001  01101101  01100001  00100000
01001011  01101111  01110000  01101001
```

Pada metode *Least Significant Bit* (LSB) akan mengganti bit terkecil dari citra digital asli dalam rentang 0 sampai 255. Cara mendapatkan nilai bit terkecil adalah:

1. Mendapatkan nilai piksel pada citra digital asli pada baris 1, kolom 1.
2. Nilai piksel yang didapat (misal bernilai 199) diubah menjadi biner 8 bit.
3. Nilai yang didapatkan adalah 1111 1111.
4. Bit terkecil yang akan disubstitusi adalah nilai bit terakhir yang terletak dipaling kanan bit biner yaitu 1.

4. Kesimpulan

Berdasarkan penelitian pembuatan aplikasi dengan software MATLAB R2021a dengan teknik *Steganography* menggunakan metode *Least Significant Bit* (LSB) tersebut, maka didapatkan kesimpulan sebagai berikut:

1) Citra asli tidak mengalami perubahan secara visual ketika disisipkan pesan rahasia berupa *file* .txt.
2) Besar ukuran citra asli dengan citra *watermark* dalam satuan KB mengalami perubahan setelah disisipkan pesan rahasia yaitu dari awalnya sebesar 56,9 KB menjadi 732 KB.
3) Ukuran dimensi citra asli dengan citra *watermark* tidak mengalami perubahan yaitu tetap 500x500.
2) Hasil dari enkripsi citra menggunakan metode *Least Significant Bit* (LSB) ini berhasil mengubah bit yang ada dalam citra dan menggantinya dengan bit pesan rahasia yang disisipkan berjumlah 32 *byte*s. Pada proses dekripsi citra juga berhasil mengekstrak pesan rahasia yang ada di dalam citra *watermark*.

5. Daftar Pustaka

[1] Aliy Hafiz, "Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode *Least Significant Bit* (LSB)", Jurnal Cendikia Vol. XVII Cendikia 2019.

[2] Krisnawati, "Metode *Least Significant Bit* (LSB) dan End Of *File* (EOF) Untuk Menyisipkan Teks Ke Dalam Citra Grayscale", Seminar Nasional Informatika 2008 (semnasIF 2008).

[3] Buyung Solihin Hasugian, "Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil dan Menengah", Juli 2017.

[4] Ika Febriana, Ganjar Aji, "Penerapan Teknik Kriptografi Pada Keamanan SMS Android", JOEICT (Jurnal of Education and Information Communication Technology), Volume 1, Nomor 1, Tahun 2017: 29 – 36.

[5] Ichsan Aulia, "Implementasi Teknik *Watermarking* Pada Citra Digital Dengan Menggunakan Metode Fractal dan Discrete Cosine Transform", Majalah Ilmiah INTI, Volume 6, Nomor 2, Februari 2019.

[6] Irfan, Nazori AZ, "Prototipe Teknik Penyisipan Dokumen Citra Digital Menggunakan *Watermarking* dengan Metode DCT (Discrete Cosine Transform)", Jurnal TICOM Vol.2 No.1 September, 2013.

[7] I Gede Wiryawan, Sariyasa, I Gede Aris Gunadi, "Steganografi Berdasarkan Metode *Least Significant Bit* (LSB) Pada Citra Digital Dengan Teknik Kompresi Lossless", Jurnal Ilmu Komputer Indonesia (JIKI) Vol : 4, No. 1, Februari 2019.

[8] Burham Isnanto, Ari Amir, "Kristografi Des dan Steganografi Pada Dokumen dan Citra Digital Menggunakan Metode LSB", Jurnal Teknologi Informatika dan Komputer Atma Luhur Vol 1. September 2014.

[9] Darmayanti, Awang Harsa.K, "Sistem Steganografi Pada Citra Digital Menggunakan *Least Significant Bit*", Prosiding Seminar Sains dan Teknologi FMIPA Unmul, Vol. 1 No. 1 Juli 2016.

[10] Dedi Darwis, "Implementasi Teknik Steganografi *Least Significant Bit* (LSB) dan Kompresi Untuk Pengamanan Data Pengiriman Surat Elektronik", Jurnal TEKNOINFO, Vol. 10, No. 2, 2016.