JIKO (Jurnal Informatika dan Komputer) Ternate **p-ISSN : 2614 - 8897**
Vol. 02 No. 1, April 2018 **e-ISSN : 2656 - 2948**

PERBANDINGAN METODE STEGANOGRAFI LSB (*LEAST SIGNIFICANT BIT*) DAN MSB (*MOST SIGNIFICANT BIT*) UNTUK MENYEMBUNYIKAN INFORMASI RAHASIA KEDALAM CITRA DIGITAL

Salkin Lutfi[1], Rosihan[2]
Program Studi Teknik Informatika, Fakultas Teknik, Universitas Khairun
Jl.Jati Metro, Kota Ternate Selatan
E-mail : Salkin.lutfi@gmail.com[1], Rosihan.unkhair@outlook.com[2]

Abstract - Steganography is one of information hiding technique which is very much used for data security. Steganography is able to hide confidential information in digital media such as images / images. The purpose of the study is to design computer applications to compare the level of Robustness on MSB and LSB methods to hide confidential information into digital images. From the test results seen bits of raster images performed using the MSB method experienced a change of bits as much as 112 bits while the LSB changed as much as 109 so that the result of changes in bits from the original raster image relatife not much different between the two methods. Thus it is concluded that the MSB method produces images that are relatively significant changes in the original color of the image, while the LSB method produces images that have no visible visible color changes the image.

Keywords: MSB, LBS, Robustness, Steganography

***Abstrak* -- Steganografi merupakan salah satu teknik penyembunyian informasi yang sangat banyak dimanfaatkan untuk keamanan data. Steganografi mampu menyembunyikan informasi rahasia dalam media digital seperti citra/gambar. Tujuan dari penelitian yang adalah merancang aplikasi komputer untuk membandingkan tingkat *Robustness* pada metode MSB dan LSB untuk menyembunyikan informasi rahasia kedalam citra digital. Dari hasil pengujian terlihat bit dari raster gambar yang dilakukan menggunakan metode MSB mengalami perubahan bit sebanyak 112 bit sedangkan LSB mengalami perubahan sebanyak 109 sehingga hasil perubahan bit dari raster gambar original relatife tidak jauh berbeda antara kedua metode. Dengan demikian disimpulkan bahwa metode MSB menghasilkan gambar yang *relative* sangat signifikan perubahan warna asli gambar, sedangkan metode LSB menghasilkan gambar yang secara kasat mata tidak mengalami perubahan warna gambar.**

Kata Kunci: MSB, LBS , *Robustness* , *Steganografi*

I. PENDAHULUAN

Dengan semakin berkembangnya sistem informasi dan komunikasi, kebutuhan manusia dalam melakukan komunikasi data pun semakin meningkat. Hal ini ditandai dengan berkembang pesatnya teknologi yang terkait di dalamnya, yaitu teknologi dan media transmisi. Tidak hanya melalui kabel, data pun dapat juga dikirim melalui media non-kabel (*wireless*) yang menggunakan udara sebagai media merambatnya sinyal. Lewat sinyal yang merambat melalui udara, data dapat dikirimkan dari satu tempat ke tempat lain dengan mudah dan praktis.

Pada sistem jaringan komputer yang luas seperti internet, khususnya pengiriman pesan lewat *email* memungkinkan pesan dapat dibajak oleh orang yang tidak berwenang. Pada masalah keamanan pesan, terdapat dua permasalahan utama yang mesti diperhatikan oleh pengguna yaitu masalah privasi *(privacy)*. Privasi mengandung arti bahwa pesan yang dikirimkan hanya dapat baca informasinya oleh penerima yang sah. Keamanan dan kerahasiaan data pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang sehingga kemajuan bidang jaringan komputer dengan konsep open system akan memberi peluang untuk mengakses kawasan – kawasan vital tersebut. Sebab itu data, informasi perlu dilakukan pengamanan [3]. Selain itu hal yang menjadi permasalahan adalah hak cipta, sebuah karya cipta harus dilindungi supaya tidak ada penyalahgunaan atau pengakuan sebuah karya karena dapat merugikan pemiliknya [4].

Ada beberapa teknik dalam steganografi yakni Most Significant Bit (MSB) yakni penyisipan bit pesan terhadap bit yang paling berarti, misalkan pada bit 11010010 angka yang bergaris bawah merupakan bit yang berarti, bit tersebut membunyai nilai yang besar sehingga adanya perubahan nilai bit MSB yang besar akan memberikan efek perubahan warna pada citra y ang dapat dibedakan secara kasat mata [2].

Metode steganografi yang popular digunakan adalah metode LSB (Least Significant Bit) dan MSB (Most Significant Bit), metode MSB yaitu menyisipan pesan bit dengan mengganti bit awal dari sebuah citra sementara metode LSB yaitu menyisipkan pesan dengan mengganti bit akhir dari sebuah citra digital. Untuk mengetahui tingkat kesamaran dari kedua metode dapat dilihat dari *Robustness* (tingkat kerusakan citra) dari sebuah citra yang telah dilakukan steganografi.

Robustness adalah ukuran sejauh mana watermark bertahan setelah data mengalami bentuk-bentuk pemro sesan signal, perubahan geometris, ukuran dan sebagainya. Keamanan adalah ukuran suatu skema watermarking ber tahan terhadap segala usaha yang sengaja bertujuan mengha pus atau membuat watermark tidak terbaca. Imperceptibility menjamin agar perubahan pada data akibat watermarking tidak tertangkap atau dirasakan panca indra. Kapasitas data menyatakan ukuran seberapa besar watermarking bisa disisipkan [6].

Dari latar belakang tersebut sehingga penulis melakukan penelitian untuk mengimplementasikan algortima kriptografi Knapshack Markle-Hellman menjadi sebuah aplikasi yang dapat untuk keamanan data dan informasi dengan judul *"Perbandingan Metode Steganografi LSB (Least Signifivant Bit) dan MSB (Most Significant Bit) Untuk Menyembunyikan Informasi Rahasia Kedalam Citra Digital"*.

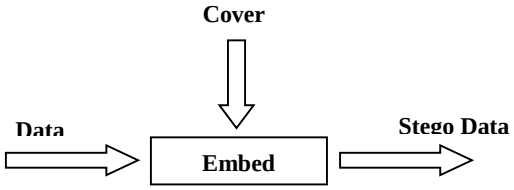
II. TINJAUAN PUSTAKA

2.1 Steganografi

Steganografi (*covered writing*) didefinisikan sebagai ilmu dan seni untuk menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia. Steganografi telah dikenal semenjak tahun 500 SM, dimana Herodotus (sejarawan Yunani) menuliskan pesan pada kepala budak dan menunggu sampai rambut kepalanya tumbuh kembali sehingga pesan tidak terlihat dan selanjutnya dia diutus untuk menyampaikan pesan tersebut tanpa menimbulkan kecurigaan oleh bangsa Persia [1].

Steganografi pada media digital file gambar digunakan untuk mengeksploitasi keterbatasan kekuatan sistem penglihatan manusia dengan cara menurunkan kualitas warna pada file gambar yang belum disisipi pesan rahasia. Sehingga dengan keterbatasan tersebut manusia sulit menemukan gradasi penurunan kualitas warna pada file gambar yang telah disisipi pesan rahasia.

Gambaran steganografi dapat ditunjukkan seperti pada gambar 1. berikut :



Gambar 1. Proses Steganografi

2.2 Metode Steganografi MSB (*Most Significant Bit*) dan Steganografi LSB (*Least Significant Bit*)

Metode steganografi yang banyak digunakan adalah metode modifikasi LSB (*Least Significant Bit*) dan metode MSB (*Most Significant Bit*). Metode MSB dan LSB tergolong metode yang menggunakan teknik substitusi. Kedua metode tersebut digunakan untuk steganografi berbasis media (*media-based steganography*) [5].

Pada file gambar BMP 24 bit setiap pixel pada gambar terdiri dari susunan tiga warna yaitu merah, hijau, biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (1 byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Sebagai contoh file gambar BMP 24 bit dengan warna merah murni dalam format biner akan terlihat sebagai berikut:

00000000 00000000 11111111
00000000 00000000 11111111

Sedangkan untuk warna hijau murni dalam format biner akan terlihat sebagai berikut :

00000000 11111111 00000000
00000000 11111111 00000000

Sedangkan untuk warna biru murni dalam format biner akan terlihat sebagai berikut :

11111111 00000000 00000000
11111111 00000000 00000000

Dari uraian di atas dapat dilihat bahwa informasi dari warna biru berada pada bit pertama sampai bit delapan, dan informasi warna hijau berada pada bit sembilan sampai dengan bit 16, sedangkan informasi warna merah berada pada bit 17 sampai dengan bit 24.

Metode penyisipan LSB (*Least Significant Bit*) ini adalah menyisipi pesan dengan cara mengganti bit ke 8, 16 dan 24, sedangkan MSB *(Most Significant Bit)* adalah menyisipkan pesan dengan cara menggantikan bit 1, 9, 17. Pada representasi biner file gambar dengan representasi biner pesan rahasia yang akan disembunyikan. Dengan demikian pada setiap pixel file gambar BMP 24 bit dapat disisipkan 3 bit pesan, misalnya terdapat data raster original file gambar adalah sebagai berikut:

00100111 11101001 11001000
00100111 11001000 11101001
11001000 00100111 11101001

Sedangkan representasi biner huruf A adalah 01000001, dengan menyisipkannya ke dalam pixel di atas maka dengan metode LSB akan dihasilkan :

00100111 11101001 11001000
00100111 11001000 11101000
11001000 00100111 11101001

Sedangkan dengan menggunakan metode MSB akan menghasilkan :

00100111 11101001 01001000
00100111 01001000 01101001
01001000 10100111 11101001

Dengan metode LSB terlihat pada bit 8, 16 dan 24 diganti dengan representasi biner huruf A (cetak tebal), dan hanya tiga bit rendah yang berubah (garis bawah), sedangkan dengan metode MSB terlihat pada bit 1, 9, dan 17 terdapat 6 bit yang berubah (garis bawah) sehingga untuk penglihatan mata manusia sangatlah

mustahil untuk dapat membedakan warna pada file gambar yang sudah diisi pesan rahasia jika dibandingkan dengan file gambar asli sebelum disisipi dengan pesan rahasia.

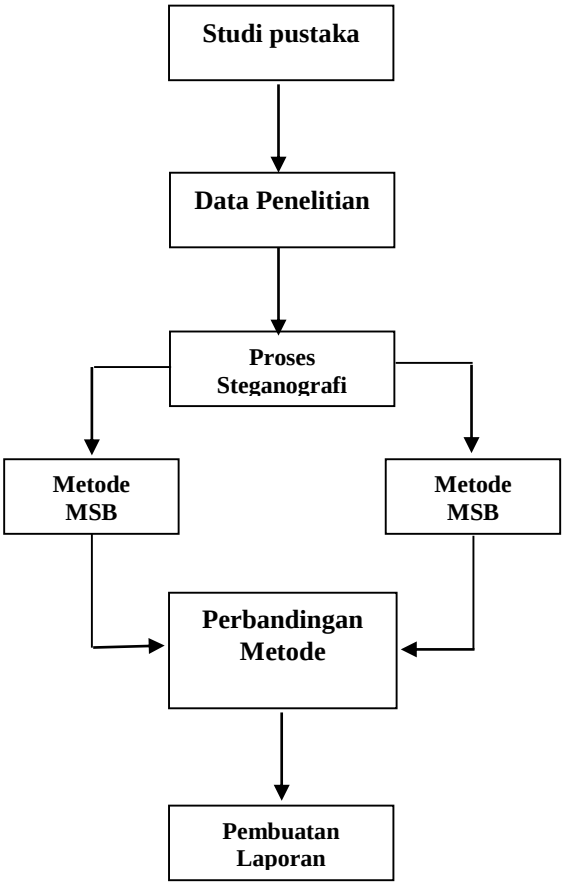
III. METODE PENELITIAN

3. 1 Metode Pengumpulan Data

Metode pengumpulan data yang penulis gunakan dalam penelitian ini adalah:

1. Studi pustaka
   Dalam pengumpulan data dengan studi pustaka penulis mempelajari literatur dan pustaka yang bersumber dari buku dan jurnal yang berhubungan dengan metode steganografi baik MSB maupu LSB
2. Observasi
   Observasi penulis gunakan untuk mengamati bit dari citra digital yang telah dilakukan proses penyisipan informasi untuk membandingkan *rebustness* dari hasil steganografi.

3.2. Tahapan Penelitian



Gambar 2. Tahapan Penelitian

Tahapan penelitian dimulai dengan tahapan studi literatur serta mengumpulkan data-data yang berkaitan dengan penelitian. Selanjutnya kemudian dilakukan tahapan proses steganografi dengan menyisipkan ke citra digital dengan menggunakan metode MSB maupun LSB. Selanjutnya yaitu dengan melakukan observasi hasil citra yang telah dilakukan proses steganografi. Tahapan yang terakhir yaitu pembuatan laporan penelitian.

3.3 Alat Penelitian

Untuk menunjang terlaksananya penelitian yang dikerjakan, tidak lepas dari kebutuhan perangkat keras (hardware) dan perangkat lunak (software). Bahan dan alat tersebut adalah:

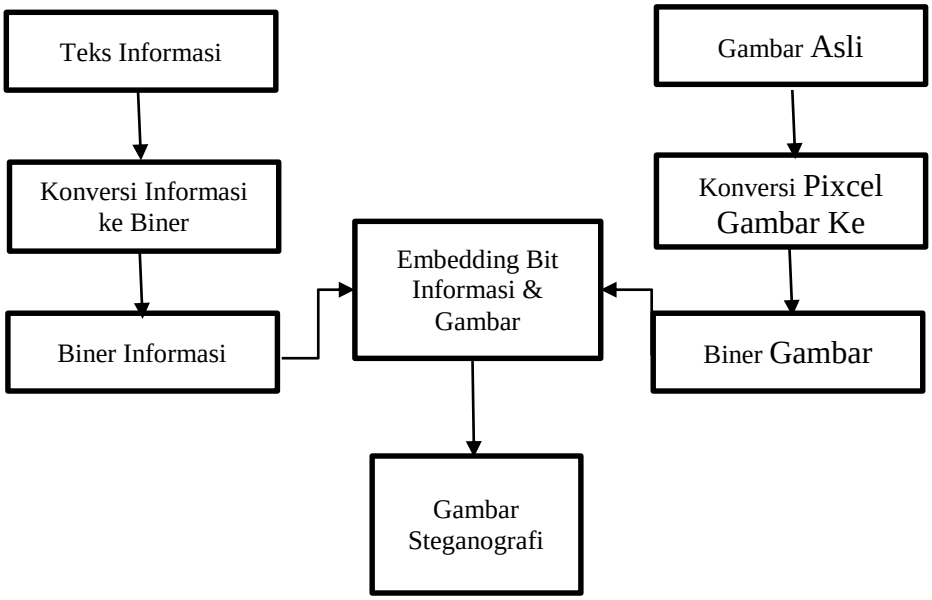
A. Perangkat Keras:
   - 1 unit laptop intel Dual Core,
   - Memori 1 Gb
   - 1 unit printer

B. Perangkat Lunak:
   - Sistem Operasi Windows 10
   - Photoshop CSS
   - Aplikasi Image Bitview

IV. HASIL PEMBAHASAN

4.1. Metode Steganografi *Most Significant Bit* (MSB) dan *Least Significant Bit*

Metode MSB dan LSB merupakan metode steganografi yang menggunakan penyisipan informasi kedalam media digital dalam hal ini penulis menggunakan media gambar, yaitu dengan menggantikan bit awal maupun akhir dari pixcel gambar. Berikut gambaran blok diagram penyisipan stegnografi



Gambar 3. Blok Diagram Metode MSB

Pada gambar 3. menggambarkan proses penyisipan informasi kedalam sebuah gambar digital, diamana proses ini dimulai dari mengekstrak pixcel gambar dan informasi yang disisip menjadi bilangan biner, lalu kemudian dialakukan tahap embedding/menyisipkan informasi kedalam gambar menggunakan baik menggunakan metode MSB maupun LSB dengan menggantikan bit awal maupun akhir dari gambar dengan bit-bit informasi satu persatu, lalu tahap akhir yaitu menyatukan kembali pixcel yang telah disisip menjadi gambar steganografi MSB yang telah disisip.

Dalam perbandingan ini penulis menggunakan sebuah gambar dan informasi yang sama dan melakukan proses embadding dengan metode MSB maupun LSB.

Gambar 4. Gambar asli

Gambar asli yang ini merupakan gambar yang nantinya akan disisipkan informasi yaitu "Universitas Khairun Ternate", sebelum melakukan penyisipan tentunya terlebih dahulu mengekstrak lalu mengkonvers pixcel gambar dan informasi menjadi bit biner dalam hal ini penulis menggunakan conversi biner 8 bit.

Berikut adalah raster original gambar yang telah ekstrak dan dikonversi dengan 8 bit.

10101111	11000000	11011111	10101111	11000000	11011111	10101111	11000000	11100000
10101111	11000000	11100000	10110000	11001111	11100000	10110000	11001111	11100000
10110000	11001111	11101111	10110000	11001111	11101111	10110000	11001111	11101111
10111111	11010000	11101111	10111111	11010000	11101111	10111111	11010000	11101111
10111111	11010000	11101111	10111111	11010000	11101111	10111111	11010000	11101111
10111111	11010000	11101111	10111111	11010000	11101111	11000000	11010000	11110000
11000000	11010000	11110000	11000000	11010000	11110000	11000000	11010000	11110000
11000000	11010000	11110000	11000000	11010000	11110000	11000000	11010000	11110000
11000000	11010000	11110000	11000000	11010000	11110000	11000000	11010000	11110000
11000000	11010000	11110000	11000000	11010000	11110000	11000000	11010000	11110000
11000000	11011111	11111111	11000000	11011111	11111111	11000000	11011111	11111111
11000000	11011111	11111111	11000000	11010000	11110000	11000000	11010000	11110000

11000000 11010000 11110000 11001111 11011111 11111111 11001111 11011111 11111111
11001111 11011111 11111111 11001111 11011111 11111111 11001111 11011111 11111111
11001111 11011111 11111111 11001111 11011111 11111111 11000000 11010000 11110000
11000000 11010000 11110000 11000000 11010000 11110000 11000000 11010000 11110000
11000000 11010000 11110000 11000000 11010000 11110000 11000000 11010000 11110000
11000000 11010000 11110000 11000000 11010000 11110000 11000000 11010000 11110000
11001111 11011111 11111111 11001111 11011111 11111111 11001111 11011111 11111111
11001111 11011111 11111111 11001111 11011111 11111111 11001111 11011111 11111111
11001111 11011111 11111111 11001111 11011111 11111111 11001111 11011111 11111111
11001111 11011111 11111111 11001111 11011111 11111111 11001111 11011111 11111111
11001111 11011111 11111111 11001111 11011111 11111111 11001111 11011111 11111111
11001111 11011111 11111111 11001111 11011111 11111111 11001111 11011111 11111111
11001111
……
……

Berikut adalah bit biner dari informasi "Universitas Khairun Ternate" yang di konversi dengan biner 8 bit :

01010101	01101110	01101001	01110110
01100101	01110010	01110011	01101001
01110100	01100001	01110011	00100000
01001011	01101000	01100001	01101001
01110010	01110101	01101110	00100000
01010100	01100101	01110010	01101110
01100001 01110100 01100101			

Setelah mendapatkan bit biner dari gambar maupun teks, selanjutnya yaitu proses penyisipan/embadding dengan mengganti bit biner dari gambar dengan masing bit biner dari teks informasi dengan metode MSB maupun LSB.

1. Metode MSB

Penyisipan dengan metode MSB yaitu dengan menggantikan bit awal biner dari gambar dengan digit biner dari informasi yang telah dikonversi sebelumnya. Sehingga memperoleh bit gambar setelah dilakukan penyisipan sebagai berikut :

00101111 11000000 **01011111** 10101111 **01000000** 11011111 **10101111** 11000000
01100000 10101111 11000000 **01100000** 10110000 11001111 11100000 **00110000**
01001111 11100000 10110000 **01001111** 11101111 **00110000** **01001111** 11101111
00110000 11001111 11101111 10111111 **01010000** 11101111 10111111 **01010000**
01101111 10111111 11010000 **01101111** **00111111** 11010000 **01101111** 10111111
01010000 11101111 10111111 11010000 **01101111** **00111111** 11010000 **01101111**
00111111 11010000 11101111 11000000 **01010000** **01110000** 11000000 11010000
01110000 11000000 11010000 **01110000** 11000000 **01010000** **01110000** 11000000
01010000 11110000 11000000 11010000 **01110000** 11000000 **01010000** **01110000**
01000000 11010000 11110000 **01000000** **01010000** **01110000** **01000000** 11010000
01110000 11000000 11010000 11110000 **01000000** **01010000** 11110000 11000000
01010000 **01110000** 11000000 **01011111** **01111111** **01000000** **01011111** **01111111**
01000000 11011111 **01111111** **01000000** 11011111 **01111111** 11000000 11010000
01110000 11000000 11010000 **01110000** 11000000 **01010000** **01110000** **01001111**
01011111 11111111 11001111 **01011111** **01111111** **01001111** **01011111** 11111111
01001111 11011111 11111111 **01001111** 11011111 **01111111** **01001111** 11011111

01111111	11001111	11011111	11111111	**01000000**	**01010000**	11110000	**01000000**
01010000	11110000	11000000	11010000	**01110000**	11000000	**01010000**	11110000
01000000	11010000	11110000	**01000000**	11010000	11110000	11000000	**01010000**
01110000	**01000000**	11010000	**01110000**	**01000000**	**01010000**	**01110000**	**01000000**
01010000	11110000	**01001111**	11011111	**01111111**	11001111	**01011111**	**01111111**
01001111	11011111	11111111	**01001111**	**01011111**	11111111	**01001111**	11011111
01111111	11001111	11011111	11111111	**01001111**	**01011111**	11111111	**01001111**
01011111	11111111	11001111	**01011111**	11111111	11001111	11011111	**01111111**
01001111	11011111	11111111	**01001111**	**01011111**	**01111111**	**01001111**	11011111
01111111	11001111	11011111	11111111	**01001111**	11011111	**01111111**	**01001111**
01011111	11111111	11001111	**01011111**	**01111111**	11001111	**01011111**	11111111
11001111							
……							
……							

Setelah melakukan penyisipan bit informasi kedalam bit gambar original dengan menggunakan metode MSB maka terjadi perubahan bit gambar sebanyak 112 perubahan bit yang ditandai dengan huruf tebal dan garis bawah, bila bit yang telah disisip tersebut di konversi kembali menjadi file gambar maka hasilnya dapat dilihat pada gambar 5.

Gambar MSB yang berisikan sedikit informasi

Gambar MSB yang berisikan banyak informasi

Gambar 5. Gambar Steganografi MSB

Pada gambar 5. terdapat 2 gambar, dimana gambar kiri tampak tidak banyak mengalami perubahan dikarenakan informasi yang di sisip adalah "Universitas Khairun Ternate", pada gambar kanan mengalami perubahan dikarenakan penyisipan informasi "Universitas Khairun Ternate" disisipkan sebanyak 30x perulangan sehingga terlihat perubahan kualitas gambar yang dapat terlihat secara drastis perubahannya.

2. Metode LSB

Penyisipan dengan metode LSB yaitu dengan menggantikan bit akhir biner dari gambar dengan digit biner dari informasi yang telah dikonversi sebelumnya. Sehingga memperoleh bit gambar setelah dilakukan penyisipan sebagai berikut :

10101110	**11000001**	**11011110**	10101111	11000000	11011111	**10101110**
11000001	11100000	10101111	**11000001**	11100000	**10110001**	11001111
11100001	10110000	**11001110**	**11100001**	**10110001**	**11001110**	11101111
10110000	**11001110**	11101111	10110000	11001111	11101111	10111111
11010000	11101111	10111111	11010000	**11101110**	10111111	**11010001**

11101110	**10111110**	**11010001**	**11101110**	10111111	11010000	11101111
10111111	**11010001**	**11101110**	**10111110**	**11010001**	**11101110**	**10111110**
11010001	11101111	**11000001**	11010000	11110000	**11000001**	**11010001**
11110000	**11000001**	**11010001**	11110000	**11000001**	11010000	11110000
11000001	11010000	**11110001**	**11000001**	**11010001**	11110000	**11000001**
11010000	11110000	11000000	**11010001**	**11110001**	11000000	11010000
11110000	11000000	**11010001**	11110000	**11000001**	**11010001**	**11110001**
11000000	11010000	**11110001**	**11000001**	11010000	11110000	**11000001**
11011110	**11111110**	11000000	**11011110**	**11111110**	11000000	11011111
11111110	11000000	11011111	**11111110**	**11000001**	**11010001**	11110000
11000001	**11010001**	11110000	**11000001**	11010000	11110000	**11001110**
11011110	11111111	11001111	**11011110**	**11111110**	**11001110**	**11011110**
11111111	**11001110**	11011111	11111111	**11001110**	11011111	**11111110**
11001110	11011111	**11111110**	11001111	11011111	11111111	11000000
11010000	**11110001**	11000000	11010000	**11110001**	**11000001**	**11010001**
11110000	**11000001**	11010000	**11110001**	11000000	**11010001**	**11110001**
11000000	**11010001**	**11110001**	**11000001**	11010000	11110000	11000000
11010001	11110000	11000000	11010000	11110000	11000000	11010000
11110001	**11001110**	11011111	**11111110**	11001111	**11011110**	**11111110**
11001110	11011111	11111111	**11001110**	**11011110**	11111111	**11001110**
11011111	**11111110**	11001111	11011111	11111111	**11001110**	**11011110**
11111111	**11001110**	**11011110**	11111111	11001111	**11011110**	11111111
11001111	11011111	**11111110**	**11001110**	11011111	11111111	**11001110**
11011110	**11111110**	**11001110**	11011111	**11111110**	11001111	11011111
11111111	**11001110**	11011111	**11111110**	**11001110**	**11011110**	11111111
11001111	**11011110**	**11111110**	11001111	**11011110**	11111111	11001111
……						
……						

Setelah melakukan penyisipan bit informasi kedalam bit gambar original dengan menggunakan metode LSB maka terjadi perubahan bit gambar sebanyak 109 perubahan bit yang ditandai dengan huruf tebal dan garis bawah, bila bit yang telah disisip tersebut di konversi kembali menjadi file gambar maka hasilnya dapat dilihat pada gambar 6.

Gambar LSB yang berisikan sedikit informasi

Gambar LSB yang berisikan banyak informasi

Gambar 6. Gambar Steganografi LSB

pada gambar 6. gambar hasil penyisipan dengan metode steganografi LSB dengan menyisipkan informasi "Universitas Khairun Ternate" baik 1 kali maupun penyisipan dengan perulangan sebanyak 30 dengan banyaknya perubahan pixcel namun kualitas gambar tidak mengalami perubahan yang signifikan.

4.2. Analisi Perbandingan Metode

Metode MSB maupun maupun metode LSB merupakan metode yang cukup populer dalam steganografi, dimana metode MSB melakukan penyisipan dengan mengganti digit biner bit gambar pada awal bit sedangkan LSB melakukan penyisipan pada akhir bit.

Dari hasil simulasi sebelumnya terlihat bit dari raster gambar yang dilakukan menggunakan metode MSB mengalami perubahan bit sebanyak 112 bit sedangkan LSB mengalami perubahan sebanyak 109 sehingga hasil perubahan bit dari raster gambar original relatife tidak jauh berbeda antara kedua metode.

Walaupun dari hasil simulasi perubahan jumlah raster biner dari gambar yang telah disisipkan informasi baik menggunakan metode MSB maupun LSB relatife sama namun hasil keduanya jauh berbeda pada kualitas gambar yang dihasilkan seperti terlihat pada gambar 4 dan gambar 5.

Metode MSB bila di sisipkan informasi yang sedikit akan mengalami perubahan raster biner yang sedikit pula sehingga perubahan kualitas gambar juga tidak banyak mengalami perubahan. Namun apabila di sisipkan informasi dalam jumlah yang banyak maka perubahan kualitas gambar sangat banyak mengalami perubahan seperti pada gambar 4.

Sementara pada metode LSB bila disisipkan informasi yang sedikit maupun banyak tetap akan mempengaruhi banyak bit biner dari raster gambar original, namun dari segi kualitas gambar baik informasi yang disipkan sedikit maupun banyak tetap tidak terlihat perubahan kualitas secara kasat mata.

Dari hasil penelitian ini tentunya dari perbandingan kedua metode dapat terlihat bahwa dengan metode MSB akan menghasilkan gambar steganografi yang robustness sedangkan metode LSB menghasilkan gambar yang relative tidak banyak megalami masalah pada kualitas gambar.

V. PENUTUP

5.1. Kesimpulan

1. Dari hasil perbandingan metode MSB dan metode LSB, metode MSB menghasilkan gambar yang relative sangat signifikan perubahan warna asli gambar, sedangkan metode LSB menghasilkan gambar yang secara kasat mata tidak mengalami perubahan warna gambar.
2. Metode MSB dan LSB merupakan algoritma steganografi yang dapat menyembunyikan informasi kedalam gambar. Dengan melakukan perbandingan kedua metode ini Penulis berkesimpulan metode LSB lebih baik dari metode MSB sebab hasil pixcel citra yang dihasilkan oleh LSB tidak merubah warna secara drastis
3. Teknik steganografi dapat diimplementasikan untuk mengamankan informasi dengan cara menyisipkan informasi kedalam media digital sehingga membuat pihak lain tidak curiga aka pesan yang disembunyikan.

5.2. Saran

1. Dalam penelitian ini penulis hanya membandingkan metode MSB dan LSB sehingga diharapkan penelitian berikutnya dapat membandingakan meode steganografi lainnya
2. Metode MSB maupun LSB dalam penyisipan bit terlihat telah diketahui pola penyisipannya sehingga untuk lebih amannya, sehingga disarankan pada penelitian berikutnya dapat menggabungkan metode steganografi dengan metode kriptografi dalam mengamankan informasi.

DAFTAR PUSTAKA

[1]. Ariyus, Dony. 2009. *Keamanan Multimedia.* Yogyakarta: Andi Offset

[2]. B. Rakhmat dan M. Fairuzabadi, Steganografi menggunakan Metodw Least Significant Bit dengan Kombinasi Algoritma Kriptografi Vigenere dan RC4, Dinamika Informatika, vol. V, no. 2, pp. 1-17, 2010

[3]. Hartini dan S. Primaini, Kriptografi Password Menggunakan Modifikasi Metode Affine Ciphers, Jurnal Sigmata, vol. II, no. 1, pp. 40-50, 2014.

[4]. Mastur, Perlindungan Hukum hak kekayaan intelektual Dibidang Paten, Jurnal Ilmiah Ilmu Hukum QISTI, vol. 6, no. 1, pp. 65-81, 2012.

[5]. Masaleno, Andino. Pengantar Steganografi, (online), Kuliah Umum Ilmu Komputer. (http://ilmuKomputer.org, diakses 1 Oktober 2017)

[6]. Rahmatri Mardiko, T. Basaruddin, Watermarking pada Video: Robustness, Impercetibility dan Pendekatan untuk Domain Terkompresi, Jurnal Ilmiah Fakultas Ilmu Komputer Universitas Indonesia (2009)