JPPI Vol 8 No 2 (2018) 109 - 122
Jurnal Penelitian Pos dan Informatika
771/AU1/P2MI-LIPI/08/2017
32a/E/KPT/2017

e-ISSN: 2476-9266
p-ISSN: 2088-9402

DOI:10.17933/jppi.2018.080204

TEKNIK PENGUJIAN KEAMANAN DATA TEKS BERTINGKAT DENGAN METODE *STEGANOGRAPHY LSB* DAN TEKNIK ENKRIPSI

TECHNIQUES FOR TEXT DATA SECURITY TESTING INCREASED BY LSB STEGANOGRAPHY METHOD AND ENCRYPTION ENGINEERING

Hillman Akhyar Damanik[1] Merry Anggraeni[2]
Program Studi Magister Ilmu Komputer Universitas Budi Luhur[12]
Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, DKI Jakarta, Indonesia 12260[12]
Email: hillmanakhyardamanik@gmail.com[1] merryanggraeni1230@gmail.com[2]

Naskah diterima: 7 Oktober 2017 ; Direvisi : 15 Maret 2018 ; Disetujui : 25 Juli 2018

Abstrak

Internet adalah media komunikasi paling populer saat ini, tetapi komunikasi melalui internet menghadapi beberapa masalah seperti keamanan data, kontrol hak cipta, kapasitas ukuran data, otentikasi dan lain sebagainya.Pada penelitian ini peneliti memperkenalkan skema untuk menyembunyikan data yang terenkripsi. Dimana kami menggunakan citra sebagai *embedding* dan *cover image* untuk *text hiding*. Fitur utama skema adalah cara penyematan data teks ke *cover image* terenkripsi. Peneliti berkonsentrasi menggunakan metode RGB-LSB untuk penyematan data teks dan memverifikasi kinerja menggunakan metode RGB-LSB dalam hal indeks kualitas yaitu PSNR, MSE, *imperceptibility* dan indeks *recovery*. Kombinasi algoritma *Least Significant Bit* (LSB) dan Kriptograpi RO13 untuk penyisipan file gambar pada gambar yang berformat *.jpg. Pengujian pada algoritma *Least Significant Bit* (LSB) yang sudah disisipi jumlah pesan yang berbeda-beda tetap menghasilkan nilai SME dan PSNR yang sama. Nilai SME pada jumlah pesan yang disisipi sebanyak 407 kata adalah nilai MSE 0.8310 dan nilai PSNR 48.9348.pada jumlah pesan yang disisipi sebanyak 507 kata adalah nilai MSE 0.8322 dan nilai PSNR 48.9285. Nilai kriteria *imperceptibility* pada *stego image* yang dihasilakan juga menghasilkan hasil *image* dan nilai-nilai *pixel* pada masing-masing *cover image*tidak mengalami perubahan. Berdasarkan hasil perbandingan ini dapat diketahui bahwa algoritma LSB memiliki hasil yang baik pada teknik penyisipan sebuah pesan pada file citra

Kata kunci: Citra digital, Steganografi, Least Significant Bit, Kriptografi, ROT13.

Abstract

The internet is the most popular communication media today, but communication via the internet faces several problems such as data security, copyright control, data size capacity, authentication and so on. In this study researchers introduced a scheme to hide encrypted data. Where we use imagery as embedding and cover image for text hiding. The main feature of the scheme is how to embed text data into an encrypted image cover. Here the researcher concentrated on using the RGB-LSB method for embedding text data and verifying the performance using the RGB-LSB method in terms of quality indexes namely PSNR, MSE, imperceptibility and recovery index. The combination of Least Significant Bit (LSB) and Cryptography RO13 algorithms for inserting image files in images that are * .jpg format. Testing on the Least Significant Bit (LSB) algorithm that has been inserted by a number of different messages still results in the same SME and PSNR values. The SME value on the number of messages inserted as many as 407 words is the MSE value of 0.8310 and the PSNR value of 48.9348. on the number of messages inserted as many as 507 words is the value of MSE 0.8322 and the value of PSNR 48.9285. The value of the imperceptibility criteria in the stego image that is produced also produces image results and the pixel values in each image cover do not change. Based on the results of this comparison it can be seen that the LSB algorithm has good results on the insertion technique of a message in the image file.

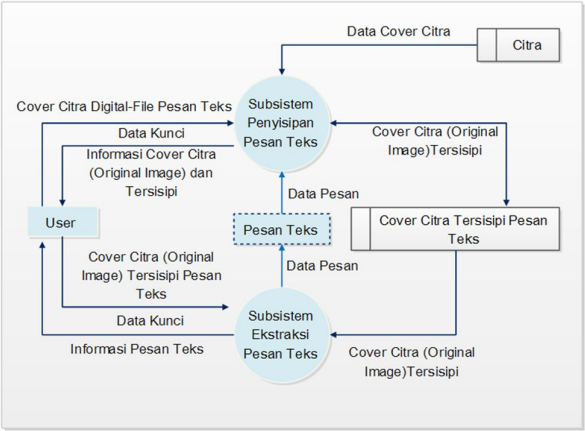
***Keywords**: Digital Image, Steganografi, Least Significant Bit, Cryptography, ROT13,*

PENDAHULUAN

Baru-baru ini, teknik penyembunyian informasi telah menarik banyak minat penelitian dari bidang keamanan informasi. Steganografi gambar adalah cabang utama teknik penyembunyian informasi, yang dapat digunakan untuk komunikasi tersembunyi melalui saluran publik. Pengiriman pesan teks dalam bentuk biasa memiliki risiko tinggi untuk data yang rentan dicuri. untuk mengurangi risiko, teknik keamanan data harus diterapkan. Teknik keamanan data dapat dilakukan menggunakan kriptografi dan steganografi(Prashanti *et al*. 2013). Berdasarkan literatur, kombinasi kriptografi dan steganografi dapat meningkatkan hasil pada proses transaksi pengiriman data teks tersebut. Kriptografi sebagai salah satu ilmu dalam keamanan informasi, yang digunakan dalam proses pengamanan citra (Takur *et al*. 2016). Salah satu metode kriptografi yang telah digunakan untuk mengamankan data adalah ROT13. Algoritma ini sering diimplementasikan untuk proses enkripsi. Pada penelitian ini, penulis mengajukan teknik pengamanan pesan rahasia Steganografi dengan keamanan berlapis, dengan menambahkan kriptografi terhadap pesan rahasia yang akan disisipkan kedalam citra digital kemudian pesan disisipkan kedalam citra digital melalui Steganografi menggunakan metode LSB. Proses Algoritma kriptografi ROT13 dan kombinasi pada metode steganografi ini, dapat mengurangi masalah-masalah yang sering terjadi seperti, Autentikasi, penyalahgunaan data teks dan

merusak data teks, ROT13 dan metode steganografi dapat membantu dengan mempersulit para kriptanalis dalam pencurian atau perusakan data teks.

Dalam penelitian ini, kami mengusulkan metode steganografi berbasis LSB yang efisien yang menggunakan kunci rahasiaROT 13 untuk menyembunyikan informasi ke dalam piksel masukan dari *cover image* tanpa menghasilkan distorsi. Metode yang peneliti usulkan terlebih dahulu mengenkripsi pesan gambar menggunakan enkripsi ROT13 sebelum proses *embedding*. Proses ini menghasilkan data yang tidak terlihat, yang akan dapat disebabkan kecurigaan orang lain ataupun pihak yang tidak bertanggung jawab. Dalam penelitian ini, untuk menyembunyikan pesan teks yang dienkripsi, peneliti menggunakan metode steganografi *embedding* dan *least significant bit*. Proses *embedding* menghasilkan media stego dengan mengganti informasi dengan data dari pesan tersembunyi. Proses penelitian yang diusulkan dapat dilihat pada Gambar I.1 dibawah sebagai berikut:



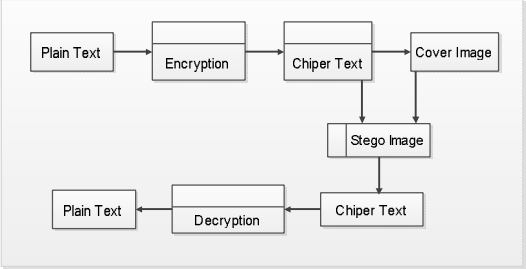
Gambar .1 Teknik Pengujian *Steganography* LSB dan Teknik Enkripsi

Steganografi dan Kriptografi

Steganografi adalah teknik menyembunyikan teks informasi seperti gambar, teks, audio, dan video

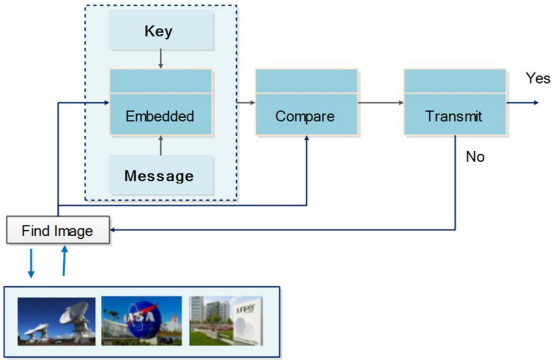
(Chauhan*et al*. 2017) Ada berbagai jenis Steganografi:

- Text *Steganography*: Tidak sering digunakan karena teks file memiliki jumlah data redundan yang kecil.
- Gambar Steganografi: digunakan secara luas untuk menyembunyikan informasi dalam *cover image*.
- Audio/Video steganography.



Gambar.2 Kombinasi kriptografi dan Steganografi

Menyembunyikan pesan rahasia dalam *cover image* yang tepat harus dipilih. Sangat penting untuk menyembunyikan informasi dalam gambar digital, karena ada kesempatan untuk kehilangan informasi pada saat komunikasi (Thangadurai dan Devi, 2014). Gambar.3 menunjukkan proses pemilihan cover image.



Gambar 3. Cover Image Selection

Metode pada steganografi dijelaskan sebagai berikut (Garg, 2012):

- Satu Bit Stego

  Dalam metode ini ketika gambar digunakan sebagai operator diSteganografi mereka dimanipulasi dengan mengubah satu atau lebih dari bit-bit dari byte yang membentuk piksel sebuah gambar. Ini adalah metode yang paling aman dibandingkan dengan metode lain.
- Dua Bits Stego

  Dalam metode ini dua LSB dari salah satu warna dalamNilai RGB dari pikselakan digunakan untuk menyimpan pesan bit dalam gambar.
- Tiga Bits Stego

  Dalam metode ini tiga LSB dari salah satu warna dalamNilai RGB dari pikselakan digunakan untuk menyimpan bit pesan.
- Empat Bits Stego

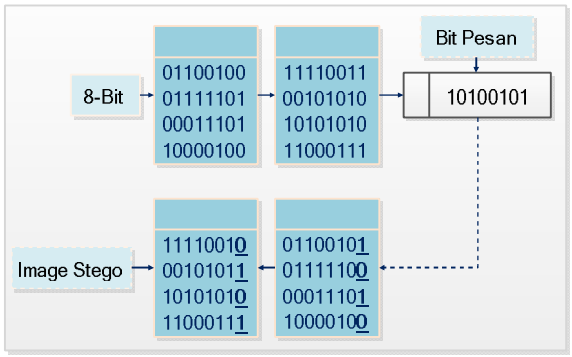
  Dalam metode ini empat LSBs salah satu warna dalamNilai RGB dari piksel akan digunakan untuk menyimpan bit pesan.
- Warna Siklus Stego

  Untuk melakukan pendeteksian data tersembunyilebih sulit diputuskan untuk menggilir nilai warna di masing-masing piksel.

Algoritma Least Significant Bit (LSB)

LSB adalah salah satu metode steganografi sederhana dalam domain spasial di mana pesan secara langsung dimasukkan ke dalam *pixel* dari *cover image* (Hussain dan Hussain, 2013). Metode ini memiliki nilai tak terlihat yang bagus, sehingga, visi manusia tidak dapat mendeteksi

perubahan gambar (Thomas, 2013).Proses penyisipan dilakukan dengan mengubah bidang bit LSB dari setiap piksel sesuai dengan bit pesan. Sebagai contoh: Gambar Sampul, yang memiliki delapan piksel dan masing-masing diwakili ke dalam bentuk biner 8-bit:



Gambar 4. *Cover Image Selection*

Bit yang digaris bawahi dan tebal adalah LSB yang berubah berdasarkan pada bit pesan. Perubahan bit terakhir dari bidang bit tidak berpengaruh besar pada nilai tak terlihat, sehingga mata manusia tidak dapat mendeteksinya.

Cover Image:

Cover image digunakan untuk menyembunyikan data teks asli di dalamnya. Bit bit ditutupi oleh OR dengan *zero*. Setelah *masking*, tidak ada informasi dalam *cover image* LSB.

Embedding:

Memasukkan N bit ke dalam gambar *cover* sesuai *space* yang tersedia.

Teks yang disisipkan pada gambar:

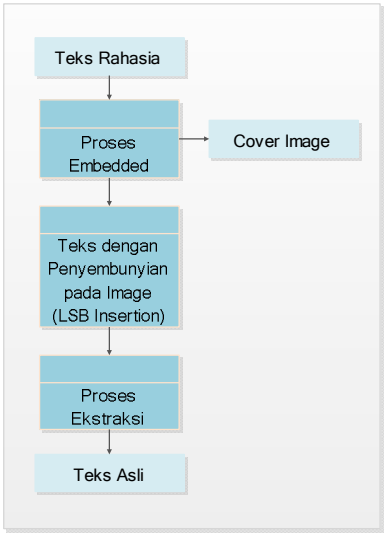
Setelah penyisipan nilai *bit* ke *cover image* selanjutnya mendapatkan teks tersembunyi. Kita tidak bisa melihat teks tersembunyi itu.Dalam data asli teks terenkripsi tidak terlihat selama transmisi.

Original Image: Teks direkonstruksi setelah ekstraksi

Bit yang diekstraksi:

Ini adalah proses mengembalikan dari *embedding* bit ke dalam *cover image* untuk teks asli.

Proses aliran detail penyisipan LSB pada gambar 4



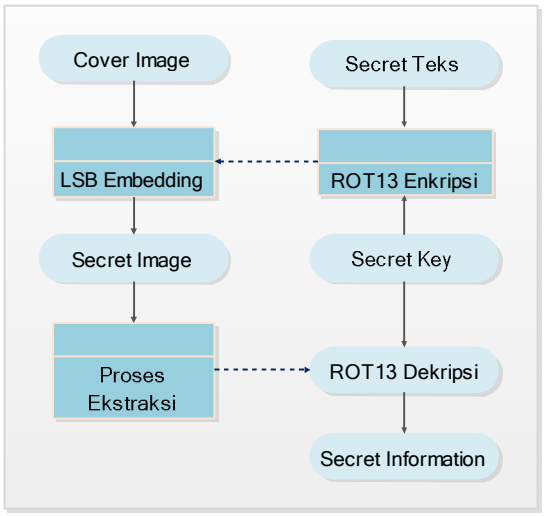
Gambar 5 Penyisipan Teks LSB pada steganografi

Penyisipan Bit ke LSB (Pada Gambar 5):

Pertama temukan jumlah bit yang akan dimasukkan ke dalam *cover image*. Kemudian cari ukuran total dari bit target data (teks asli). Setelah menemukan ukuran total bit target data. Kemudian cari ukuran total dari data target ruang bit yang dapat dimasukkan. Kemudian terapkan kondisi, jumlah bit yang akan disisipkan lebih besar dari total ukuran target data *bit space* yang dimasukkan. Jika TIDAK maka tampilkan jumlah bit yang akan dimasukkan melebihi. Jika YA menghitung aliran bit dan mengalokasikannya ke dalam *array* dan menyisipkan ke LSB. Setelah penyisipan bit *stop* penyisipan bit &mengirimkannya. Cara penyisipan bit ke LSB dilakukan diuraikan pada gambar 6

Selanjutnya pada gambar 7 dijelaskan kombinasi pada proses usulan pendekatan untuk keamanan teks yang disediakan pada kualitas enkripsi yang baik. ROT13 digunakan untuk mengenkripsi teks asli untuk menghasilkan teks *cipher*. Teks asli diubah menjadi teks biner, teks biner dienkripsi dengan kunci.Teks disembunyikan oleh *cover image*, untuk menyembunyikan teknik LSB. Kita dapat menanamkan teks terenkripsi dalam *cover image* untuk memastikan tidak ada media komunikasi lain yang dapat menyerang komunikasi. Pada proses percobaan dilakukan operasi enkripsi dua kali dan dengan ukuran dan jumlah teks yang berbeda. Dapat di katakan seperti enkripsi teks ganda. Karena dua kali enkripsi proses, ini memberikan lebih banyak jaminan (Pravalika *et al*. 2014).

Gambar 6. *Flowchart insertBit* pada LSB



Gambar 7 Kombinasi pada proses usulan pendekatan Enkripsi Teks dengan Steganografi

METODE PENELITIAN

A. Instrumen Penelitian

Metode penelitian yang merupakan strategi untuk menyelesaikan penelitian ini adalah dengan mengukur efektifitas dari algoritma yang digunakan dengan perhitungan nilai MSE dan PSNR, dan berdasarkan kriteria aspek *imperceptibility* dan *recovery*.Kemudian dianalisa hasil pengukurannya sehingga didapatkan kesimpulan tentang kualitas citra setelah dilakukan steganografi LSB dengan algoritma ROT13. Tujuan dari penelitian ini yaitu untuk memberikan keamanan berlapis pada Steganografi dengan cara menambahkan kriptografi pada pesan rahasia yang disisipkan pada *cover image*, dan kriptografi yang digunakan merupakan modifikasi kriptografi *Caesar Cipher*(Agham *et al*. 2014).

1. Dataset Citra

Pada penelitian ini, pengujian dilakukan dengan menggunakan standard *dataset image* berupa *file* citra dengan format JPG yang telah distandarisasi

oleh SIPI (*Signal and Image Processing Institute*) *laboratory* sebagaimana ditampilkan pada table. Citra *cover* yang akan dilakukan ujicoba adalah*cover image* Qatar Airways, Juniper Network, Roses dan satellite hub III.1 sebagai berikut:

Tabel 1. Dataset Citra*cover image*

No.	Cover Image	Preview	Kapasitas	Resolusi Cover	Panjang Karakte
1	Qatar Airways		1.75MB	960x640	64
2	Juniper Network		147KB	298x169	110
3	Roses		148KB	249x203	61
4	Satellite Hub		963KB	701x469	158

Metode Algoritma pada Penelitian

1. Algoritma *Encoding* LSB

Proses *embedding* pesan teks dilakukan dengan menyandikan pesan rahasia atau *plain text*, menggunakan algoritma enkripsi ROT13. Parameter teks harus tidak dapat dipahami maknanya atau *cipher text*, setelah proses *embedding* pada media *image* atau *cover image* berupa file citra menggunakan metode LSB.

Hasil dari proses penyisipan adalah *file* gambar JPG 24 bit yang disebut dengan *stego text*(Namita *et al*.2010).

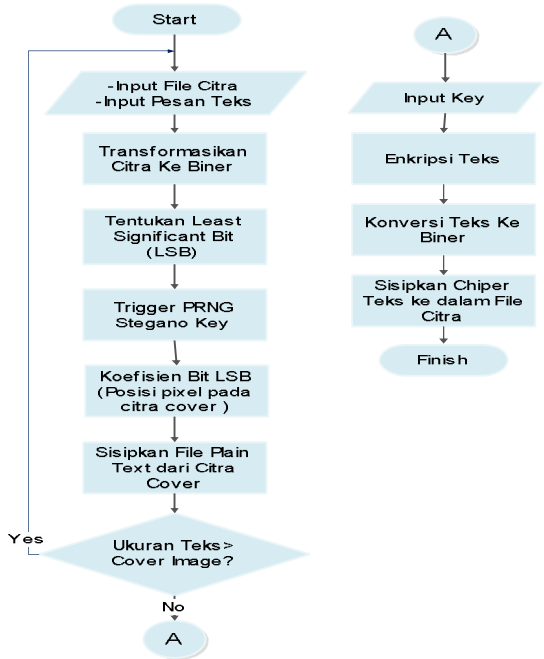
Step 1:

Dari gambar 8 diuraikan proses penyisipan file pesan dimulai dengan memilih citra *cover*, pesan teks kemudian mengubah file citra cover dan file pesan menjadi deretan biner, selanjutnya memasukkan *password*, yang berfungsi sebagai*seed* untuk membangkitkan PRNG, kemudian dibangkitkan bilangan acak semu atau *pseudo-random number*, dipilih bit LSB dari setiap *pixel* yang urutannya sesuai dengan bilangan acak semu yang dibangkitkan, menyisipkan *bit-bit* dari file pesan pada *bit-bit* LSB dari setiap *pixel* yang terpilih, menyisipkan kembali bit-bit yang telah disisipi ke dalam citra *cover*, mengubah kembali deretan bit menjadi bentuk pixel, menyimpan citra yang telah berisi pesan ke dalam file (citra *stego*), kemudian menampilkan citra stego (Thakur *et al*. 2016).

Proses perulangan ketika ukuran teks lebih besar dari *cover image* (Juneja *et al*. 2009).

Step.2:

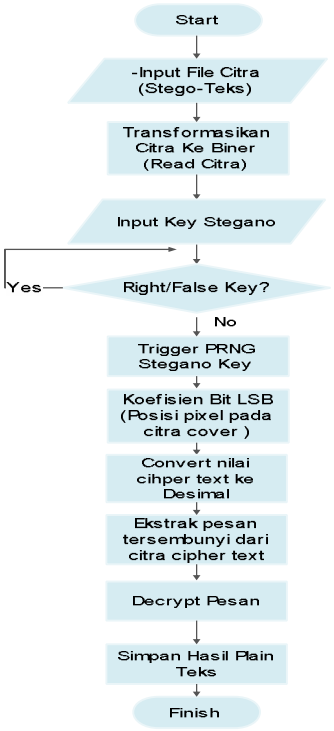
Proses selanjutnya meng-input kunci untuk proses enkripsi, melakukan konversi teks pesan pada bit-bit dari file. Pada proses enkripsi akan melakukan *embedding* chipper teks pada citra.



Gambar 8. Flowchart Algoritma Proses *Encoding*

2. Algoritma *Decoding* LSB

Proses penguraian pesan teks dilakukan dengan mengambil cipher text dari stego text dan mengubah cipher text menjadi plain text dengan menggunakan algoritma dekripsi ROT13. Gambar 9 merupakan flowchart proses penguraian atau ekstraksi pesan tersembunyi dari *cover image*(Zhang *et al*. 2010). Proses ekstraksi pada gambar 9



Gambar 9 Flowchart Algoritma Proses *Decoding*

PENGUJIAN PENELITIAN

Perhitungan *Mean Square Error* (MSE) Dan *Peak Signal To Noise Ratio* (PSNR)

Dalam metode evaluasi obyektif, indeks yang paling umum digunakan adalah *Peak Signal To Noise Ratio* (PSNR) [8]. Dalam perhitungan PSNR, pertama-tama kita harus menghitung Square Error Mean (MSE) antara teks tersembunyi dan *cover image*. PSNR diukur dalam satuan desibel.Pada penelitian ini, PSNR digunakan untuk mengetahui perbandingan kualitas citra *cover* sebelum dan sesudah disisipkan pesan.

Menentukan nilai PSNR, terlebih dahulu harus ditentukan MSE (*Mean Square Error*).MSE adalah nilai error kuadrat rata-rata antara citra *cover* dengan citra steganografi, persamaan dapat dirumuskan seperti pada persamaan (1) sebagai berikut:

$$MSE = \frac{1}{MN}\sum_{X}^{M} = 1 \sum_{Y}^{N} = 1 \ (S_{xy} - C_{xy})^2 \quad \text{Persamaan (1)}$$

Dimana:

MSE: *Mean Square Error* dari citra
M: panjang citra dalam *pixel*
N: lebar citra dalam *pixel*
x,y: koordinat masing-masing *pixel*
S: nilai bit citra pada koordinat x,y
C: nilai derajat keabuan citra pada koordinat x,y.

Setelah diperoleh nilai MSE maka nilai PSNR dapat dihitung dari kuadrat nilai maksimum dibagi dengan MSE. Persamaan nilai PSNR dirumuskan seperti pada persamaan (2).

$$PSNR=10\log_{10}\frac{(MAXi)2}{MSE} \qquad \text{Persamaan (2)}$$

Dimana :

MSE adalah Nilai MSE; MAXi adalah Nilai maksimum dari *pixel* citra (i). Semakin rendah nilai MSE maka akan semakin baik, dan semakin besar nilai dari PSNR maka semakin baik kualitas citra pada steganografi.Tahap pengujian PSNR digunakan untuk mengukur kualitas citra sebelum dan sesudah proses *embedding*(Joshi *et al*. 2016). Algoritma *pseudocode* PSNR yang diterapkan pada penelitian ini diuraikan pada gambar 10 sebagai berikut:

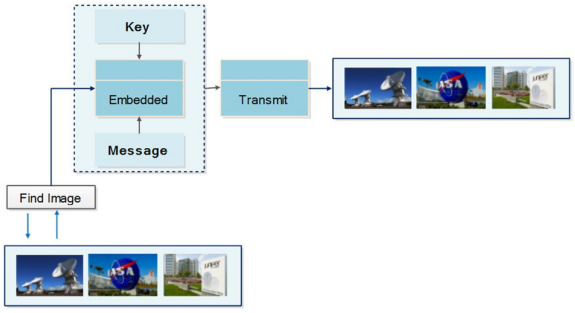
```
CitraFile CitraFile1 = new CitraFile();
CitraFile CitraFile2 = new CitraFile();

final int size = CitraFile1.getHeight()
* CitraFile1.getWidth();
for (int i = 0; i < CitraFile1.getWidth(); i++) {
for (int j = 0; j < CitraFile1.getHeight(); j++) {
    final CitraColor CitraColor1 =
    new  CitraColor(CitraColor1.getRGB(i, j));
    final CitraColor CitraColor2 =
    new CitraColor(CitraColor2.getRGB(i, j));
    final double distance
    getCitraColorDistance(CitraColor1, CitraColor2);
    totalDistance += Distance;
if (Distance > maxDistance) {
        maxDistance = Distance;
        maxX = i; maxY = j;
        }
    final int redDiff =
        CitraColor1.getRed()-
        CitraColor2.getRed();

        if (redDiff > maxRed) {
        maxRed = redDiff;
        worstRedX = i; worstRedY = j;
    }
    final int greenDiff =
        CitraColor1.getGreen()-
        CitraColor2.getGreen();
    if (GreenDiff > maxGreen) {
        maxGreen = GreenDiff;
        worstGreenX = i;worstGreenY = j;  }
    final int BlueDiff =
        CitraColor1.getBlue() -
        CitraColor2.getBlue();
    if (BlueDiff > maxBlue) {
        maxBlue = BlueDiff;
        worstBlueX = i;worstBlueY = j;  }
    totalRed += redDiff * RedDiff;
    totalGreen += greenDiff * GreenDiff;
    totalBlue += blueDiff * BlueDiff;  }
}
float meanSquamerahError =
    (totalRed + totalGreen + totalBlue) /
    (CitraColor1.getWidth() *
    CitraColor1.getHeight() * 3);
double peakSignalToNoiseRatio =
     10 * StrictMath.log10((255 * 255) /
    meanSquamerahError);   }
}
```

Gambar 10 *Pseudocode* PSNR

Pengujian Berdasarkan Kriteria

Aspek Kriteria *Imperceptibility*

Pada penelitian ini kriteria aspek *imperceptibility* menekankan bahwa algoritma steganografi yang baik membuat keberadaan pesan rahasia pada stego object tidak dapat dipersepsi oleh inderawi. Dalam penelitian ini, *cover object* yang digunakan adalah berkas citra digital, sehingga diharapkan penyisipan pesan ke dalam *cover object* akan menghasilkan *stego object* yang sukar dibedakan oleh mata dengan *cover object*-nya. Penentuan apakah keberadaan pesan rahasia dapat dipersepsi atau tidak ditentukan dari penglihatan manusia atau indera mata. Pada gambar 11 pengujian diberikan terhadap beberapa *cover image* yang telah disisipi pesan terlebih dahulu untuk membuktikan apakah algoritma LSB telah memenuhi aspek *imperceptibility* atau tidak. Dari penyisipan pesan tersebut akan dihasilkan *stego image*. Dimana aspek *imperceptibility*akan terlihat dari perbandingan antara *cover image* dan *stego image* yang dihasilkannya. Apabila perbedaan di antara kedua berkas citra digital tersebut tidak dapat terlihat secara kasat mata (Mukhedkar 2016).



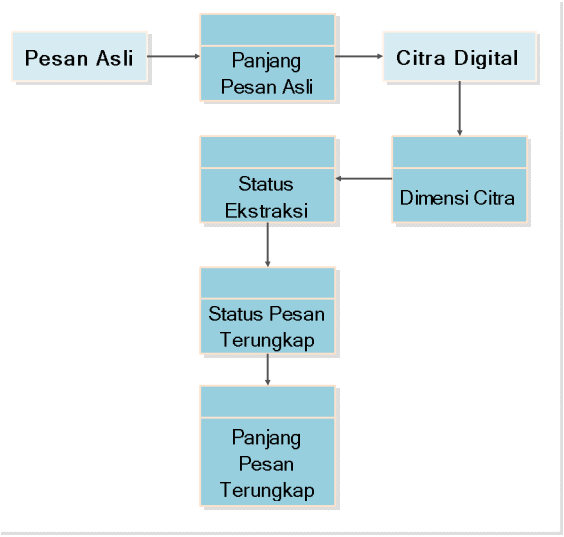
Gambar 11. Proses *imperceptibility*

Aspek Kriteria Recovery

Aspek *Recovery* menyatakan bahwa pesan yang disembunyikan dalam stego image harus dapat diungkapkan kembali.untuk mengukur keberhasilan aspek *recovery*. Dalam algoritma *Least Significant Bit* (LSB), dapat dilihat dari kesesuaian plainteks yang berhasil diekstraksi dari *stego image*.

Hasil pengujian terhadap aspek *recovery*

untuk contoh masukan *stego image* hasil *embedding* pada pengujian sebelumnya ditunjukkan pada gambar 12 dibawah berikut:



Gambar 12. Proses Aspek Kriteria *Recovery*

HASIL DAN PEMBAHASAN

Pemantauan kualitas citra dilakukan secara visual pada citra hasil steganografi yang dibandingkan dengan citra *cover*.Penyisipan data dilakukan menggunakan citra sebagai berikut. Hasil dari pengujian yang dilakukan tampak pada Gambar III.5 berikut ini:

1. Metode *Embedding* (*Original Cover* Citra)

Metode LSB (*Original File*)

No.	*Cover Image*	*Cover Image*	Kapasitas	Resolusi Cover Data	Panjang Karakter
1	Qatar Airways		1.75MB	960x640	64
2	Juniper Network		147KB	298x169	110
3	Roses		148KB	249x203	61
4	Satellite Hub		963KB	701x469	158

Gambar 13. Citra Cover sebelum disisipkan

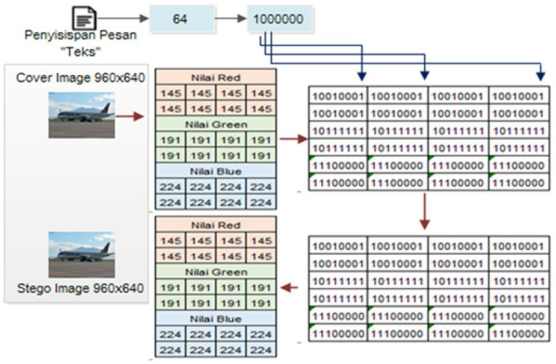
2. Metode *Extraction* (*Stego* Citra)

Metode LSB (*Extraction)*

No.	*Cover Image*	*Stego Image*	Kapasitas	Resolusi Cover Data	Panjang Karakter
1	1495716007-Qatar-Air-StegoIma		1.75MB	960x640	64
2	1495722936-Juniper-Network		147KB	298x169	110
3	1495724277-Roses		148KB	249x203	61
4	1495725357-Satelite-Hub		963KB	701x469	158

Gambar 14 Citra stego setelah proses ekstraksi

Pada gambar 13 dan gambar 14, dapat dilihat bahwa antara *citra stego* 1495716007-Qatar-Air-StegoImage.JPG dan *citra cover* Qatar Airways. JPG adalah sama. Hal ini menunjukkan bahwa penyisipan file pesan dalam citra *cover*adalah tidak mempengaruhi kualitas citra *stego* dalam penglihatan manusia.



Gambar 15. Penyisipan Pesan Teks ke dalam Citra Cover (LSB *Method*)

Berdasarkan gambar 15. menunjukkan bahwa tidak terjadinya perubahan terhadap nilai-nilai *decimal pixel* citra hasil (*stegano image*). Oleh nilai-nilai bit akhir dari *pixel* citra *cover image*.

Parameternilai *pixel* yang tidak mengalami perubahan tersebut secara penglihatan mata manusia tidak begitu terlihat secara signifikan, sehingga *stegano image* masih terlihat sama dengan citra *cover image*.

Proses penyisipan pesan teks pada *cover* citra yang dijadikan sebagai media penampung yaitu dengan tahapan memilih citra *cover image*, tahap pertama:

Step.1: Membaca nilai desimal *cover*

Step.2: Konversi kedalam bilangan biner dan kemudian masukkan pesan.

Step.3: Parameter jumlah pesan yang dijadikan sebagai *key*, digabungkan dengan pesan yang ingin disispkan (disembunyikan). Selanjutnya penggabungan pesan dan *key* menjadi pesan yang akan disisipkan ke dalam citra *cover image*. Setelah itu nilai pesan dikonversi ke dalam bilangan biner.

Step.4: Apabila jumlah biner pesan teks dapat ditampung semua pada citra *cover* berdasarkan kriteria perhitungan, jumlah piksel dibagi dengan 8 bit, maka dapat dilakukan proses penukaran bit.

Step.5: Setelah disisipkan pesan pada *cover image*, hasil dari nilai biner *cover* baru dikonversi kembali ke dalam bilangan desimal dan kemudian dipetakan menjadi citra baru atau *stegoimage*.

Proses ekstraksi pesan teks dari hasil *stegoimage*, yaitu dengan tahapan masukkan *stegoimage*:

Step.1: Membaca nilai piksel *stegoimage*.

Step.2: Konversi ke bilangan biner, kemudian ambil nilai *key* dari 8 bit LSB biner citra awal stegoimage dan dikonversi ke bilangan decimal.

Step.3: Selanjutnya nilai kunci dikalikan dengan 8 bit untuk mengambil nilai bit pesan.

Step.4: Setelah itu ambil bit LSB dari setiap elemen piksel RGB dimulai dari bit ke-9 hingga sejumlah perkalian kunci dengan 8 bit lalu ditambahkan dengan 8 bit kunci LSB. kemudian kelompokkan nilai bi-bit LSB menjadi 8 bit perkelompok.

Step.5: Lakukan konversi kedalam bilangan *decimal*, Setelah didapatkan bilangan

desimal dari biner pengelompokan, konversi ke karakter, karakter yang dihasilkan akan menjadi pesan yang telah disembunyikan sebelumnya setelah proses ekstraksi.

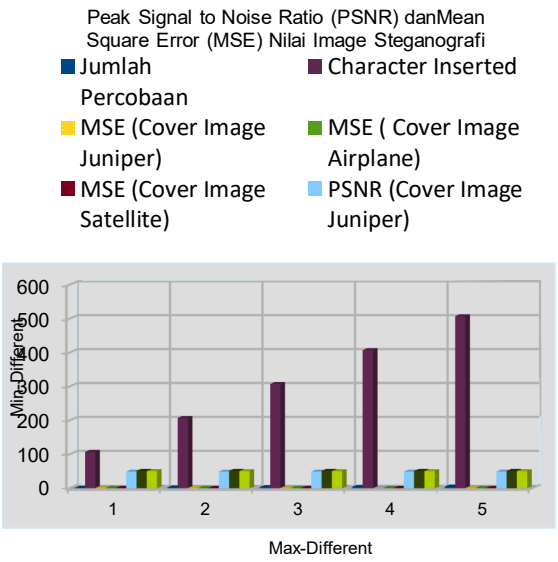
Perhitungan dan Pengujian Citra Steganography

A. PSNR dan MSE Citra Stego

Pengujian dan perhitungan *Peak Signal to Noise Ratio* (PSNR) dan *Mean Square Error* (MSE), dilakukan dimana PSNR digunakan untuk mengetahui perbedaan. Penyisipan *hidden text* ke dalam *cover image* memiliki pengaruh terhadap kualitas citra hasil steganografi (*stego image*).Selanjutnya perbandingan kualitas citra sebelum dan setelah di sisipkan teks diukur dengan metode PSNR dan dikur dalam satuan dB. Perhitungan PSNR dan MSE antara gambar awal (*cover image*) dengan gambar terstego (*stego-image*) pada berbagai jenis gambar, resolusi dan panjang karakter yang berbeda. Parameter yang digunakan antara lain: dimensi gambar adalah 960x640, jumlah karakter adalah 158 dan jenis gambar yang diuji adalah JPG. Sehingga pengujian ini mendapatkan korelasi antara jenis gambar berbeda dengan MSE dan PSNR yang dihasilkan oleh *stego image* nya.

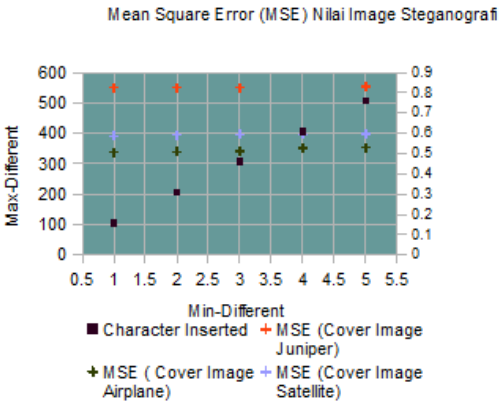
Tabel IV.1 Perhitungan PSNR dan MSE antara gambar awal (*cover image*) dengan gambar *stego-image*

Char Insert	PSNR (Juniper)	PSNR (Airplane)	PSNR (Satellite)	MSE (Juniper)	MSE (Airplane)	MSE (Satellite)
107	48.963	51.086	50.494	0.8255	0.51	0.5877
207	48.957	51.065	50.408	0.8267	0.51	0.5919
307	48.957	51.036	50.383	0.8267	0.51	0.5954
407	48.935	50.920	50.383	0.831	0.53	0.5954
507	48.928	50.885	50.374	0.8322	0.53	0.5968



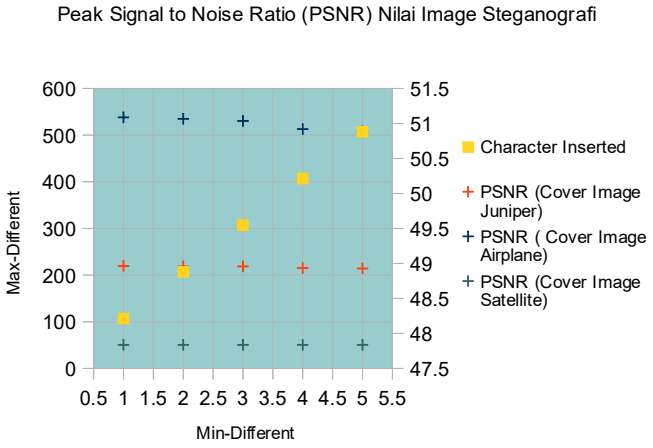
Gambar 16. Nilai MSE dan PSNR pada Stego Citra

Gambar 16 menunjukkan perbandingan bahwa nilai MSE dari keseluruhan stego citra rata-rata adalah 0.6 dB dan nilai rata-rata PSNR adalah 50 dB.Hal ini menunjukkan bahwa secara keseluruhan kualitas dari citra stego yang dihasilkan adalah cukup baik. Penyisipan sebuah file pesan yang sama pada citra *cover* yang berbeda-beda menghasilkan nilai MSE dan PSNR yang berbeda pula. Semakin kecil kapasitas citra *cover* maka nilai MSE akan semakin besar dan nilai PSNR semakin kecil, begitu pula sebaliknya semakin besar kapasitas citra *cover* maka nilai MSE semakin kecil dan nilai PSNR akan semakin besar.



Gambar 17. Nilai MSE pada Stego Citra

Dari tabel 17 dapat diketahui bahwa nilai MSE rata-rata adalah 0.5 dB. Citra *cover* yang disisipkan file pesan, yang memiliki ukuran yang berbeda dan tipe file citra yang berbeda. Hal ini menunjukkan bahwa penyisipan dari beberapa *file* pesan dengan tipe file yang berbeda-beda namun memiliki ukuran yang sama pada citra *cover* yang sama menghasilkan nilai MSE yang sama.

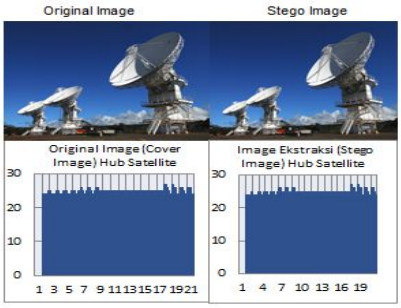


Dari tabel 18 dapat diketahui bahwa nilai PSNR rata-rata adalah 50 dB.*cover* yang disisipkan file pesan, yang memiliki ukuran yang berbeda dan tipe file citra yang berbeda. Hal ini menunjukkan bahwa penyisipan dari beberapa file pesan

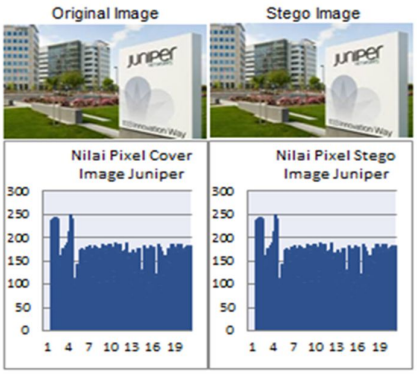
dengan tipe file yang berbeda-beda namun memiliki ukuran yang sama pada citra *cover* yang sama menghasilkan nilai PSNR yang sama.

Pengujian Kriteria Aspek *Imperceptibility*

Pengujian diberikan terhadap beberapa *cover image* yang telah disisipi pesan terlebih dahulu untuk membuktikan apakah algoritma LSB telah memenuhi aspek *imperceptibility* atau tidak. Dari penyisipan pesan tersebut akan dihasilkan *stego image*. Dimana *aspek imperceptibility*akan terlihat dari perbandingan antara *cover image* dan *stego image* yang dihasilkannya. Pada gambar dan grafik IV.6 dan IV.7 sample penelitian untuk ujicoba, dimana hasil menunjukkan pada masing-masing nilai *pixel cover image* dan stego image yang telah berisi pesan teks, secara kasat mata tidak terlihat sama sekali dan tidak terlihat perbedaan sedikitpun dan juga dimensi citra sebelum dan setelah disisipkan pesan tidak mengalami perubahan. Hal ini disebabkan perubahan *byte-byte* diagonal komponen warna merah pada *cover image* hanya akan menghasilkan perubahan beberapa byte lebih tinggi atau lebih rendah, pergantian tersebut tidak akan menampilkan perubahan yang berarti pada *stego image*.



Gambar 19. Aspek *Imperceptibility cover image-stegoHub Satellite image* 701x469

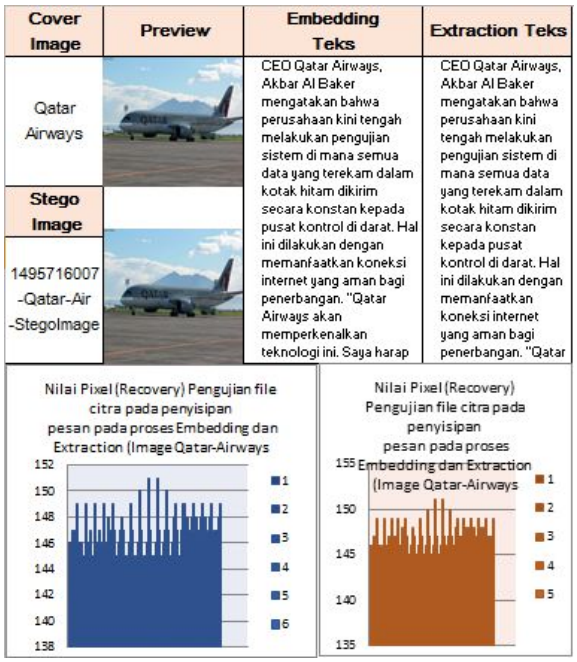


Gambar 20. Aspek *Imperceptibility cover image-stego image* Juniper 298x169

Pengujian Kriteria Aspek *Recovery*

Aspek kriteria *recovery*pada hasil seperti gambar 21 menghasilkan bahwa pesan yang disembunyikan dalam *stego image* harus dapat diungkapkan kembali. untuk mengukur keberhasilan aspek *recovery* dalam algoritma *Least Significant Bit* (LSB), dapat dilihat dari kesesuaian plainteks yang berhasil diekstraksi dari *stego image*.

Stego image dilakukan dengan ukuran file 960x640 dengan panjang karakter teks 64. Pengujian juga dilakukan dengan mengambil nilai-nilai *pixel* pada RGB, seperti pada grafik pada gambar IV.8. Nilai *pixel* yang dihasilkan juga memiliki nilai yang sama setelah proses ekstraksi sample penelitian untuk ujicoba, dimana hasil menunjukkan pada masing-masing nilai pixel *cover image* dan *stego image* yang telah berisi pesan teks



Gambar 21. Aspek *recovery cover image-stegoHub Satellite image* 960x640

PENUTUP

Dalam penelitian ini diterapkan keamanan pada steganografi dengan menambahkan kriptografi ROT13 yang membuat pesan rahasia kemudian bergeser 13 karakter. Setelah mengenkripsi pesan rahasia tersebut kemudian dimasukkan ke dalam *cover* citra dengan metode Least Significant Bit (LSB) yaitu setiap bit pesan rahasia yang dimasukkan ke dalam bit terakhir dari gambar digital.

LSB memenuhi Aspek*Imperceptibility* dan *recovery*. Adanya pesan rahasia tidak bisa dirasakan oleh indera. Misalnya, jika *covertext* adalah gambar, maka penyisipan pesan membuat gambar stegotext sulit dibedakan secara mata dengan gambar covertext-nya. Pada nilai RGB *pixel* juga tidak terdapat perubahan pada masing-masing *cover image* setelah proses ekstraksi.

LSB memenuhi kriteria pemulihan. Skema yang diusulkan menggunakan penyembunyian data teks dan pemulihan data tanpa kerusakan atau kehilangan data pesan. Baik pada nilai-nilai RGB pixel pada *cover image* setelah proses ekstraksi *stego image*. Metode yang diusulkan memiliki transparansi yang tinggi, pemulihan penuh dan menunjukkan kebenaran data yang dipulihkan. Metode ini memiliki ruang lingkup masa depan untuk enkripsi tingkat yang lebih tinggi.

Saran yang bisa diberikan oleh penulis sebagai rujukan untuk kombinasi algoritma MCO (*multiple cover*)dalam penelitian selanjutnya adalah sebagai berikut: Dalam penelitian lebih lanjut disarankan agar media yang disisipkan pesan rahasia bisa berupa file audio atau video.

UCAPAN TERIMA KASIH

Kami ucapkan kepada Universitas Budi Luhur yang turut mendukung penelitian ini.

DAFTAR PUSTAKA

Prashanti .G, Sandhya Rani.K, Deepthi.S “LSB and MSB Based Steganography for Embedding Modified DES Encrypted Text”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 8, August 2013, pp.788-799.

S. Chauhan, Jyotsna, J. Kumar and A. Doegar, "Multiple layer text security using variable block size cryptography and image steganography," *2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT)*, Ghaziabad, 2017, pp. 1-7. S.

Thangadurai, K., & Sudha Devi, G. (2014). An analysis of LSB based image steganography techniques. 2014

International Conference on Computer Communication and Informatics: Ushering

in Technologies of Tomorrow, Today, ICCCI 2014, 3–6.

Mr. Rohit Garg, "Comparison Of Lsb & Msb Based Steganography In Gray-Scale Images Vol.1, Issue 8,Oct 2012".,International Journal of Engineering Research and Technology (IJERT).

Thakur, R. K., & Saravanan, C. (2016).LSB for ColorImages, 2154–2158.

M. Hussain and M. Hussain, "A survey of image steganography techniques," International Journal of Advanced Science and Technology, vol. 54, pp. 113-124, 2013.

P. Thomas, "Literature survey on modern image steganographic techniques," International Journal of Engineering Research and Technology, vol. 2, 2013.

Pravalika, S. L., Joice, C. S., & Joseph Raj, A. N. (2014). Comparison of LSB based and HS based reversible data hiding techniques. Proceedings of the IEEE International Caracas Conference on Devices, Circuits and Systems, ICCDCS, 5–8.

Namita Tiwari, Dr.Madhu Shandilya,"Evaluation of Various LSB based Methods of Image Steganography on GIFFile Format",International Journal of Computer Applications, Vol. 6– No.2, September 2010 , pp .1-4.

Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia,"Application of LSB Based Steganographic Technique for 8-bit Color Images, World Academy of Science, Engineering and Technology, 2009.

Zhang, T., Li, W., Zhang, Y., & Ping, X. (2010). Detection of LSB matching steganography based on the Laplacian model of pixel difference distributions. Proceedings - International Conference on Image Processing, ICIP, 221–224.

Nadu, T., & Agham, V. (2014). Data Hiding Technique By Using Rgb-, (978).Proceedings of the IEEE International

Joshi, K., Yadav, R., & Allwadhi, S. (2016). PSNR and MSE based investigation of LSB. 2016 International Conference on Computational Techniques in Information and Communication Technologies, ICCTICT 2016 - Proceedings, 280–285.

Thakur, R. K., & Saravanan, C. (2016). LSB for Color Images, 2154–2158.Thakur, R. K., & Saravanan, C. (2016). LSB for Color Images, 2154–2158.

Mukhedkar, M., Powar, P., & Gaikwad, P. (2015). Secure non real time image encryption algorithm development using cryptography & steganography. 2015 Annual IEEE India Conference (INDICON), 1–6.