*Jurnal Masyarakat Informatika* *ISSN: 2086-4930*
*Vol. 14, No. 1, 2023* *e-ISSN: 2777-0648*

# Analisa Visual Citra Hasil Kombinasi Steganografi dan Kriptografi Berbasis *Least Significant Bit* Dalam *Cipher*

**Ibnu Utomo Wahyu Mulyono[1)], Yupie Kusumawati[2)], Novita Kurnia Ningrum[3)]**

*Program Studi D3-Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Program Studi S1-Sistem Informasi, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
[1)]ibnu.utomo.wm@dsn.dinus.ac.id, [2)]yupie@dsn.dinus.ac.id, [3)]novita.kn@dsn.dinus.ac.id

***Abstrak***

*Kriptografi dan steganografi adalah teknik yang digunakan untuk mengamankan data untuk meminimalkan pencurian data dan akses oleh orang yang tidak berwenang. Kombinasi Rivest Cipher 4 - Least Significant Bit diusulkan dalam penelitian ini untuk memberikan perlindungan bagi pesan dan berbagai format file yang tertanam dalam gambar digital. Pesan rahasia dienkripsi dengan metode RC4 sebelum dimasukkan kedalam gambar menggunakan LSB. Studi ini juga menganalisis kinerja kombinasi algoritma LSB – RC4 pada berbagai file dan ukuran gambar sampul. Gambar sampul menggunakan gambar dengan saluran RGB. Untuk pengukuran kinerja imperceptibilitas digunakan Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), dan analisis histogram. Nilai rata – rata PSNR yang didapatkan pada penelitian ini lebih dari 30 dB, ini membuktikan bahwa kualitas gambar stego sangat baik dan kualitas gambar stego yang baik memiliki nilai PSNR minimal 30 dB. Nilai PSNR yang didapatkan secara keseluruhan lebih dari 30 dB dengan nilai terendahnya 45,15 dB dengan ukuran citra 128x128 pixel.*

***Kata kunci** : Kriptografi, LSB, RC4, Steganografi.*

***Abstract***

*Cryptography and steganography are techniques used to secure data to minimize data theft and access by unauthorized persons. The Rivest Cipher 4 - Least Significant Bit combination is proposed in this study to provide protection for messages and various file formats embedded in digital images. Secret messages are encrypted with the RC4 method before being inserted into the image using LSB. This study also analyzes the performance of the combined LSB – RC4 algorithm on various files and cover image sizes. The cover image uses an image with RGB channels. To measure imperceptibility performance, Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and histogram analysis are used. The average PSNR value obtained in this study is more than 30 dB, this proves that the stego image quality is very good and good stego image quality has a PSNR value of at least 30 dB. PSNR values obtained as a whole are more than 30 dB with the lowest value being 45.15 dB with an image size of 128x128 pixels.*

***Keywords** : Cryptography, LSB, RC4, Steganography*

## 1 PENDAHULUAN

Perkembangan teknologi internet memudahkan setiap orang untuk saling bertukar informasi kepada orang lain. Keamanan dan kerahasiaan merupakan aspek penting yang

dibutuhkan dalam proses pertukaran *file* melalui internet, karena proses pertukaran ini tidak dapat menjamin bahwa *file* yang dikirimkan akan bebas dari akses pihak yang tidak berwenang. Tanpa adanya keamanan, pihak yang tidak berwenang dapat dengan mudah mendapatkan *file* yang dikirimkan melalui internet, oleh karena itu dibutuhkan teknik keamanan *file* [1]. Berbagai macam teknik keamanan telah dikembangkan untuk melindungi dan menjaga kerahasiaan *file* dari orang yang tidak berwenang. Kriptografi adalah ilmu dan seni yang mempelajari cara mengamankan *file*. Cara mengamankan ini dengan mengenkripsi *file* bersama kunci tertentu. Sebelum *file* terenkripsi disebut *plaintext*, setelah dienkripsi disebut sebagai *chipertext*. Sedangkan steganografi adalah ilmu dan seni menyembunyikan pesan rahasia dimana pesan terkandung di media tetapi tidak diketahui keberadaanya dengan indra manusia. Dalam hal ini perlu dibuatnya sistem keamanan *file* agar *file* yang dikirimkan dapat terjaga kerahasiannya [1] [2].

Kriptografi merupakan salah satu teknik yang dapat digunakan untuk mengamankan pesan melalui penerapan algoritma. Algorita kriptografi dapat diklasifikasikan berdasarkan waktu kemunculannya yaitu modern dan klasik. Menurut jenis kunci, kriptografi terbagi menjadi bentuk kriptografi simetris dan asimetris. Beberapa algortima yang populer dalam kirptografi adalah *Rivest Cipher 4* (RC4), *Data Encryption Standard* (DES), *Advanced Encryption Standard* (AES). RC4 [1], [2] merupakan salah satu algoritma kunci simetris yang berbentuk *stream chipper* sehingga panjang karakter hasil enkripsi (*ciphertext*) mempunyai panjang karakter yang sama dengan data asli (*plaintext*). Dengan algoritma ini, proses enkripsi dan dekripsi data dapat dilakukan dengan waktu yang lebih cepat dalam segi keamanan sendiri algoritma ini umumnya dinyatakan sangat aman, karena RC4 termasuk dalam algoritma simetris maka kerahasiaan kunci harus dijaga. Terdapat tahapan pemrosessan data pada RC4, anatra lain: *Key Scheduling Algorithm* (KSA), *Pseudo Random Generation Algorithm* (PRGA) dan Proses Enkripsi dan Dekripsi [3].

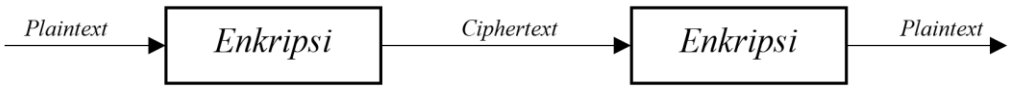
Di sisi lain, terdapat teknik yang juga dapat digunakan untuk mengoptimalkan pengamanan pesan. Steganografi merupakan ilmu yang mempelajari tentang teknik menyembunyikan pesan atau informasi yang bersifat rahasia. Steganografi merupakan cabang ilmu dari kriptografi, Steganografi membutuhkan media digital untuk mengamankan pesan atau informasi sebagai media penampung untuk menyembunyikan pesan kedalam media tertentu, salah satunya media citra [4]. Media citra dipilih sebagai media penyisipan karena pertukaran data dengan menggunakan citra lebih sering sehingga penyerang tidak akan curiga. Least Significant Bit (LSB) merupakan salah satu metode steganografi yang banyak digunakan. Algoritma LSB adalah algoritma yang relatif mudah untuk diterapkan dalam teknik steganografi dan memiliki kelebihan dalam hal *imperceptibility*. *Imperceptibility* adalah hal yang sangat penting dalam steganografi, karena nilai *imperceptibility* yang tinggi berarti pesan yang tertanam semakin tidak dapat dideteksi oleh indra penglihatan manusia. Metode *Least Significant Bit* (LSB) ini hanya mengubah nilai *bit* terakhir dalam suatu citra yang akan digunakan dengan nilai *bit* suatu *file* [5]. Penggantian nilai *bit* terakhir ini akan mengakibatkan perubahan pada nilai *byte* lebih tinggi atau lebih rendah, perubahan tersebut tidak mengubah suatu citra secara *significant* sehingga perubahan yang terjadi tidak dapat tertangkap oleh mata manusia [4]. Pada penelitian ini, akan dibuat sistem keamanan *file* yang dapat digunakan untuk memberikan keamanan pada saat bertukar *file*, aplikasi keamanan *file*

ini menggunakan metode algoritma kriptografi *Rivest Cipher 4* dan steganografi *Least Significant Bit*.

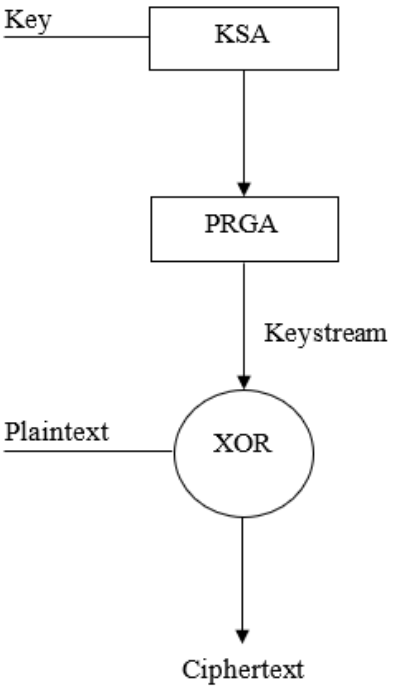
## 2 TINJAUAN PUSTAKA

### 2.1 KRIPTOGRAFI RC4

Pertukaran data digital yang aman menghasilkan sejumlah algoritma enkripsi yang berbeda dan dapat diklasifikasikan menjadi dua kelompok yaitu algoritma enkripsi simetris (algoritma kunci pribadi) dan algoritma asimetris (algoritma kunci *public*) [5]. Algoritma simetris biasanya lebih cepat untuk mengeksekusi secara elektronik daripada algoritma kunci asimetris. Kriptografi berkaitan dengan desain *cryptosystem* yang dasarnya melibatkan penggunaan kunci yang dihasilkan secara matematis. Komponen utama pada kriptografi dibagi menjadi 4 bagian yaitu, *Plaintext*, *Chipertext*, *key* dan Algoritma. *Plaintext* yaitu pesan yang dapat dibaca secara langsung oleh manusia. *Chipertext* merupakan pesan yang sudah teracak dan tidak dapat dibaca seara langsung, karena berisi pesan acak [4]. *Key* merupakan kunci untuk melakukan Teknik kriptografi. Dan yang terakhir adalah algoritma, yaitu metode untuk mengubah data yang dimengerti menjadi tidak dimengerti, sedangkan dekripsi adalah proses mengembalikan chipertext menjadi *plaintext*. Gambar 1, mengilustrasikan keseluruhan proses kriptografi dimana *plaintext* dienkripsi menggunakan algoritma dan kunci sedangkan *chipertext* didekripsi menggunakan algoritma untuk mendapatkan kembali *plaintext*.




**Gambar 1 Mekanisme Kriptografi**




**Gambar 2 Blok Diagram RC4**

Algoritma *Rivest Cipher 4* (RC4) merupakan *stream cipher* yang disebarkan pertama kali melalui sebuah *source code* yang diyakini sebagai RC4 dan dipublikasikan secara "*anonymously*" pada tahun 1994 [6]. Tahapan proses pada algoritma RC4 seperti diilustrasikan pada Gambar 2. Rivest Cipher 4 (RC4) memiliki faktor utama yang membuat algoritma ini banyak digunakan yaitu kecepatannya dan kesederhanaannya. Terdapat tahapan pemrosessan data pada RC4, anatra lain : *Key Scheduling Algorithm* (KSA), *Pseudo Random Generation Algorithm* (PRGA) dan Proses Enkripsi dan Dekripsi [3] seperti pada Gambar 2.

## 2.2 STEGANOGRAFI LSB

Kata steganografi (*steganography*) bermula dari Bahasa Yunani yaitu dari kata "*steganos*" yang memiliki arti tertutup/rahasia dan "*graphy*" yang artinya menulis atau menggambar. Jadi steganografi itu sendiri adalah tulisan tersembunyi atau rahasia. Steganografi bekerja dengan menyisipkan sebuah pesan atau berkas ke dalam suatu media yang dapat berupa *file*, suara, *video*, atau gambar sehingga keberadaan pesan tidak terlihat secara langsung oleh indera manusia. Steganografi bertujuan untuk merahasiakan, menyembunyikan suatu pesan atau sebuah informasi [3], [4]. Pesan dalam steganografi akan disembunyikan dan membuat suatu perubahan yang tidak dapat dilihat secara langsung dan tidak menarik perhatian, sebagai contoh sebuah teks yang disembunyikan pada gambar, maka teks tidak akan terlihat secara langsung. Kelebihan dari steganografi adalah pesan pada steganografi tidak menarik perhatian dari orang lain, berbeda dengan kriptografi yang tidak dapat disembunyikan dan dapat menarik perhatian orang lain [2], [5], [6]. Walaupun pesan pada kriptografi sulit untuk dipecahkan, tetapi dapat menarik perhatian dari orang lain dan menimbulkan kecurigaan. Penyembunyian pesan atau berkas dalam media digital lain dapat mengubah kualitas media tersebut. Untuk itu ada kriteria yang perlu diperhatikan dalam steganografi sebagai berikut [7]:

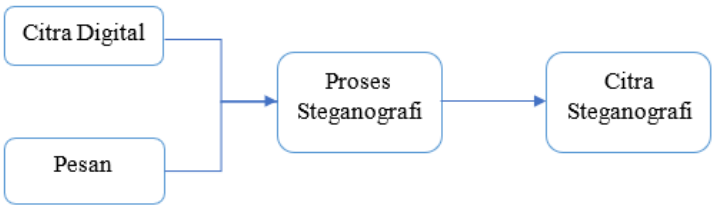
a. *Fidelity*. *Fidelity* berarti citra atau kualitas berkas pembawa tidak terlalu berubah setelah penambahan berkas atau pesan rahasia.
b. *Robustness*. Berkas pembawa pesan rahasia harus tahan terhadap manipulasi pada berkas pembawa. Contohnya adalah pengubahan kontras, ketajaman, pemangkasan, kompresi, dan sebagainya.
c. *Recovery*. Pesan atau berkas rahasia harus dapat dibaca kembali (*recovery*), karena steganografi bertujuan untuk menyembunyikan dan mengamankan pesan atau berkas damal berkas pembawa yang sewaktu – waktu pesan tersebut dapat diambil kembali.

Dalam steganografi memiliki aspek yang dapat menentukan berhasil atau tidaknya proses steganografi, aspek tersebut yaitu [8]–[10]:

a. *Capacity*. *Capacity* atau kapasitas merujuk pada jumlah pesan berkas atau informasi yang dapat disembunyikan pada berkas pembawa.
b. *Security*. Keamanan pada steganografi merujuk pada kerahasiaan *system encoding*, *decoding*, dan teknik steganografinya.
c. *Robustness*. Ketahanan berkas pembawa pesan rahasia harus tahan terhadap manipulasi pada berkas pembawa.

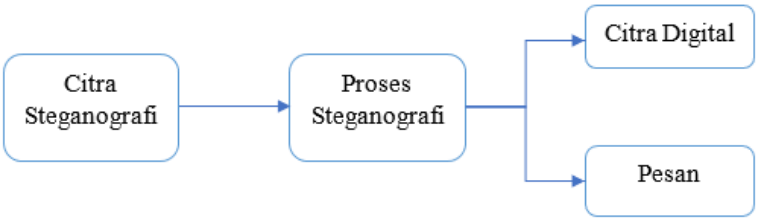
*ISSN: 2086-4930*
*e-ISSN: 2777-0648*

Steganografi mempunyai dua konsep utama yaitu penyematan (*encoding/embedding*) dan ekstraksi (*decoding/extraction*). Pesan bisa berbentuk *plaintext*, *ciphertext*, gambar, atau lainnya yang dapat ditanamkan ke dalam *bitstream*. *Encoding* adalah proses memasukkan pesan ke dalam gambar asli yang belum dimodifikasi atau biasa dinamakan *cover* media untuk menghasilkan media stego [11] seperti diilustrasikan dalam Gambar 3 dan Gambar 4.




**Gambar 3 Proses *Encoding* Steganografi**

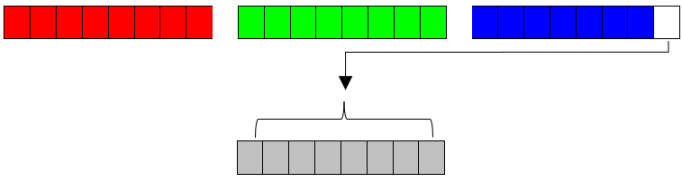
Pada Gambar 4 proses yang dilakukan untuk mendapatkan citra steganografi yaitu dengan memasukkan gambar digital dan pesan. Kemudian gambar digital dan pesan tersebut akan di proses untuk menyematkan pesan kedalam gambar yang dinamakan sebagai *Encoding* Steganografi atau biasa disebut sebagai *embedding*. Sedangkan *decoding* adalah sebuah proses yang menjabarkan pesan tersembunyi yang terdapat dalam media stego. Pada Gambar 5 proses yang dilakukan untuk memisahkan kembali citra digital dan pesan yaitu dengan memasukan citra steganografi. Kemudian citra tersebut akan diproses untuk menjabarkan pesan yang tersembunyi dalam media stego. Proses tersebut dinamakan sebagai *Decoding* Steganografi atau biasa disebut sebagai ekstraksi.




**Gambar 4 Proses *Decoding* Steganografi**

Algoritma *Least Significant Bit* (LSB) merupakan algoritma steganografi yang sederhana dan mudah untuk diterapkan. Untuk menerapkan metode ini, misalkan berkas pembawa yang akan digunakan berupa gambar atau citra digital, setiap *pixel* didalam citra dapat berukuran 1 sampai 3 *byte* [12]–[14]. Metode LSB yang digunakan pada penyembunyian pesan berbeda sesuai dengan kategori berkas. Seperti contoh pada *file* gambar, pesan disembunyikan dengan menyisipkan pesan tersebut pada *bit* rendah atau *bit* yang paling akhir (LSB) pada data *pixel file* tersebut. Pesan yang telah tersembunyi dapat dibaca kembali dengan cara melakukan *extraction* terhadap medianya. Posisi *byte* yang menyimpan *bit* pesan dapat diketahui dari bilangan acak yang dikembalikan. Dengan hasil *bit* – *bit* pesan rahasia yang disisipkan secara acak dapat dikumpulkan kembali dan disusun untuk dapat dibaca kembali, seperti pada Gambar 5.

*ISSN: 2086-4930*
*e-ISSN: 2777-0648*

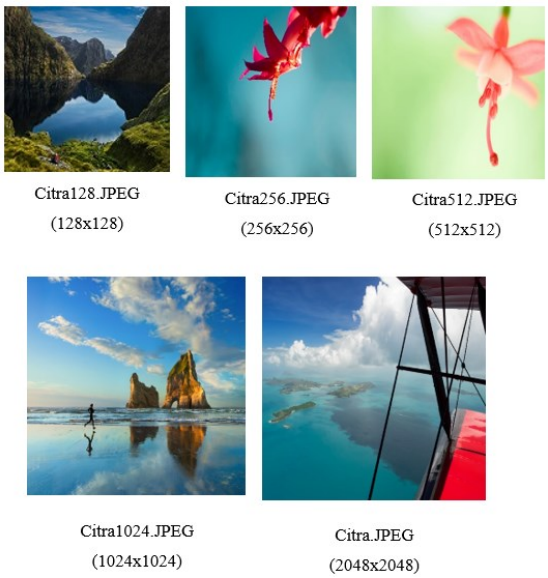



**Gambar 5 Proses LSB *Channel Blue***

## 3 METODE PENELITIAN

### 3.1 DATASET CITRA

Pada penelitian ini akan menggunakan *file* gambar **.jpeg* sebagai objek penelitian untuk mengetahui pengaruh variasi ukuran pesan teks yang ditampung pada gambar dan untuk mengetahui kualitas gambar yang telah disisipi pesan rahasia berdasarkan imperceptibilitas yang diukur dengan MSE, PSNR, dan histogram. Sedangkan untuk kualitas enkripsi akan diukur dengan entropi. Standar pengujian untuk mengukur kualitas dari citra yang telah dimodifikasi (diberi *noise* atau efek khusus) dengan citra asli dibutuhkan dalam pengujian. Citra yang sudah dimodifikasi lebih baik menyerupai citra yang asli, agar kualitas citra tetap terjaga. Pada penelitian ini menggunakan 5 gambar **.jpeg* dari *windows* (*C:\Windows\Web*) yang digunakan sebagai gambar sampul dengan ukuran asli 1920 x 1200 kemudian di *rezise* menggunakan *paint* menjadi 128 x 128 piksel, 256 x 256 piksel, 512 x 512 piksel, 1024 x 1024 piksel dan 2048 x 2048 piksel seperti pada Gambar 6.




**Gambar 6. Dataset Citra**

Sebelum menyematkan pesan kedalam gambar, pesan harus dienkripsi terlebih dahulu menggunakan algoritma RC4. Pada perhitungan pertama enkripsi RC4, hal yang harus dilakukan adalah memasukkan pesan atau biasa disebut sebagai plainteks untuk tanda bahwa inisialisasi pesan dimulai. Pada perhitungan ini *plaintext* diubah menjadi bilangan heksadesimal. Perubahan tersebut dimaksudkan untuk mempermudah dalam perhitungan.

Contoh teks yang akan di enkripsi adalah "FASILKOMUDINUSOK" sebagai *plaintext*, dan kunci yang digunakan "JAWATENGAHMANTAP". Pada proses enkripsi algoritma RC4 terdapat beberapa langkah dalam mengenkripsi, yaitu inisialisasi *state array*, penghasilan kunci enkripsi dan proses pengenkripsiannya. Dalam penginisialisasi *state array* ada 2 *state array* yang harus diinisialisasi yaitu S dan K. *Array* S diinisialisasi mulai dari 0 sampai 255 karena *array* S berjumlah @56 *byte*. Sedangkan *array* K diinisialisasi dari 1 – 256-*byte*. Jika K<256 maka lakukan *padding* menjadi 256 *byte*. Contohnya K = "hanif" 5-*byte* maka lakukan *padding* K = "hanifhanifhanifhanif……" hingga mencapai 256 *byte*.

## 3.2 TEKNIK ANALISIS DATA

Setelah data yang dibutuhkan untuk diproses penelitian, maka ada beberapa teknik dan tahapan analisis yang dilakukan dalam penelitian ini antara lain :

1. Penelitian menggunakan 5 *file* gambar **.jpeg*
2. Pesan rahasia akan di enkripsi menggunakan metode *Rivest Cipher 4* (RC4), kemudian hasil enkripsi akan disisipkan kedalam sebuah media dengan menggunakan metode *Least Significant Bit* (LSB).
3. Proses ekstraksi yang dilakukan untuk *stego image* menggunakan metode *Least Significant Bit* (LSB), kemudian diperoleh pesan rahasia yang terdapat dalam *stego image* tersebut dan didekripsi dengan kunci yang sama menggunakan metode *Rivest Cipher 4* untuk mendapatkan kembali pesan atau *plaintext* yang telah dienkripsi.
4. Analisis penelitian diperoleh dari pengukuran *Entropy* untuk metode enkripsi *Rivest Cipher 4*, dan untuk memperoleh analisis dari steganografi *Least Significant Bit* (LSB) menggunakan pengukuran MSE dan PSNR. Untuk pengukuran steganografi MSE diperoleh dari nilai ekstraksi, semakin rendah nilai MSE maka semakin tinggi kualitas gambar yang didapat. Sedangkan untuk perhitungan steganografi PSNR, semakin tinggi nilai yang didapat maka semakin bagus kualitas gambarnya. Dari pernyataan tersebut dapat disimpulkan bahwa semakin rendah nilai MSE dan semakin tinggi nilai PSNR yang didapat, maka akan semakin baik proses untuk melakukan teknik steganografi tersebut.

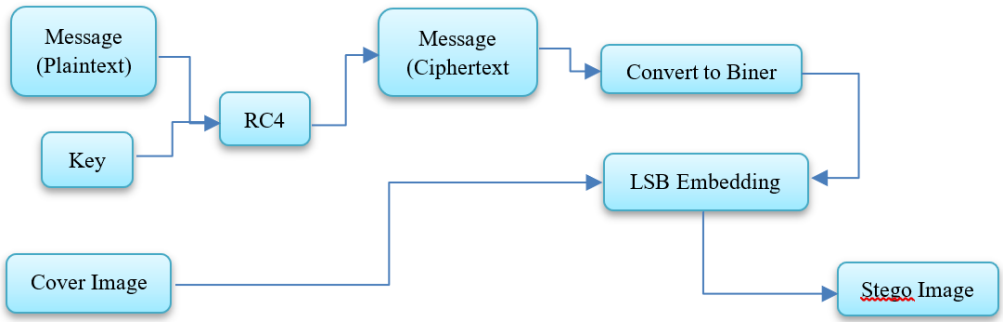
## 3.3 PENYISIPAN DAN ESKTRAKSI CITRA

Pada penelitian ini menggunakan warna RGB sebagai media atau wadah untuk menyisipkan pesan rahasia menggunakan teknik steganografi dengan metode LSB yang dikombinasikan dengan algoritma kriptografi yaitu RC4 untuk meningkatkan keamanan dan terjaminnya kerahasiaan pesan tersebut. Metode yang ingin diusulkan dibagi menjadi dua proses, yaitu proses *embedding* dan proses ektraksi, seperti Gambar 7 dan Gambar 8.

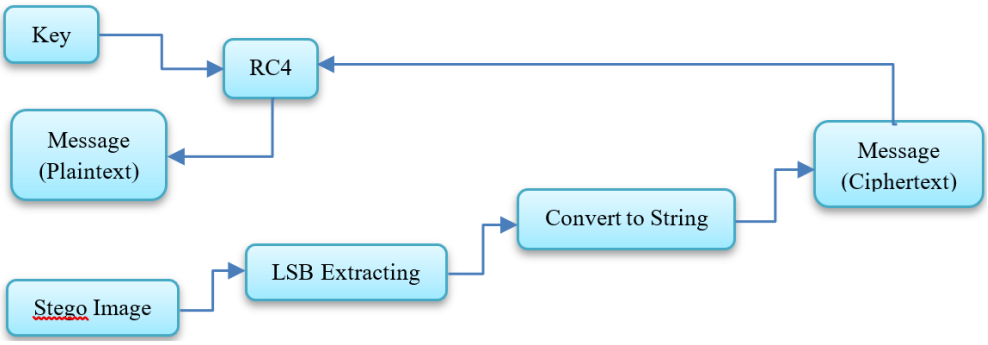
Sebelum melakukan perhitungan kualitas citra, langkah pertama *input* pesan yang akan disisipkan terlebih dahulu kemudian di enkripsi menggunakan algoritma RC4. Setelah mendapatkan hasil dari enkripsi, kemudian hasil tersebut dihitung menggunakan rumus *Entropy* untuk mendapatkan nilai kekuatan pada algoritma tersebut. Sedangkan untuk perhitungan kualitas citra, langkah pertama *input* gambar asli / *cover* dan gambar *stego* kemudian hitung nilai *error*-nya menggunakan rumus MSE. Setelah mendapatkan hasil dari

*ISSN: 2086-4930*
*e-ISSN: 2777-0648*

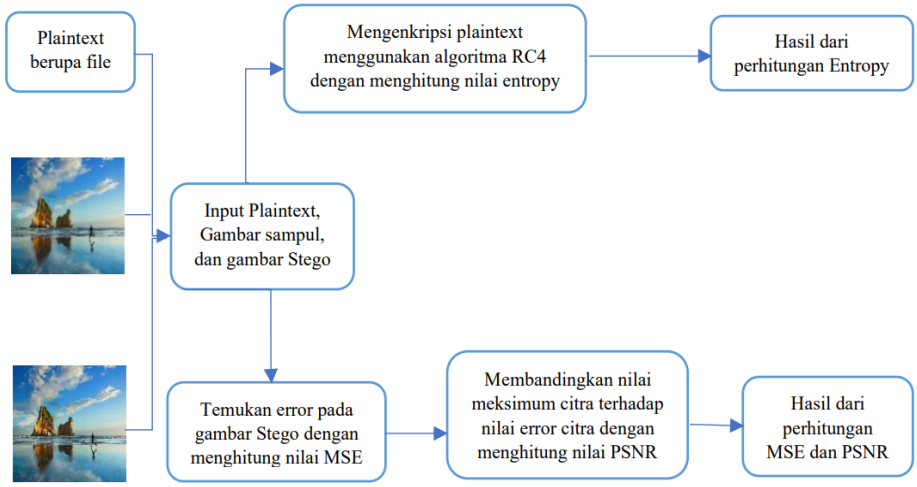
MSE tersebut, tahap berikutnya nilai MSE digunakan untuk menghitung nilai PSNR seperti pada Gambar 9.




**Gambar 7. Penyisipan Citra**




**Gambar 8. Ekstraksi Citra**




**Gambar 9. Skema perhitungan *Entropy*, MSE, dan PSNR**

## 4 HASIL DAN PEMBAHASAN

Proses penyisipan *ciphertext* pada gambar sampul menggunakan metode *Least Significant Bit* (LSB) dengan *channel* biru seperti pada Gambar 10 berikut. Gambar sampul akan disisipi *ciphertext* atau pesan rahasia kemudian akan menghasilkan gambar stegano. Hasil dari proses LSB pada gambar steganografi tidak berubah secara signifikan. Pada Tabel 2, gambar yang telah tertanam dengan *ciphertext* akan sedikit berubah jika dibandingkan dengan gambar sampul aslinya.


**Gambar 10. Penyisipan menggunakan LSB**

**Tabel 1 Nilai Biner pada hasil LSB**

| Iterasi | Piksel Gambar Biru | Biner Gambar Asli | Pesan | Gambar Stego | Piksel Stego |
|---|---|---|---|---|---|
| 1 | 8 | 00001000 | 0 | 00001000 | 8 |
| 2 | 39 | 00100111 | 1 | 00100111 | 39 |
| 3 | 68 | 01000100 | 0 | 01000100 | 68 |
| 4 | 58 | 00111010 | 0 | 00111010 | 58 |
| 5 | 22 | 00010110 | 1 | 00010111 | 23 |
| 6 | 27 | 00011011 | 1 | 00011011 | 27 |
| 7 | 40 | 00101000 | 1 | 00101001 | 41 |
| 8 | 27 | 00011011 | 1 | 00011011 | 27 |
| 9 | 70 | 01000110 | 0 | 01000110 | 70 |
| 10 | 77 | 01001101 | 1 | 01001101 | 77 |
| 11 | 31 | 00011111 | 0 | 00011110 | 30 |
| 12 | 56 | 00111000 | 0 | 00111000 | 56 |
| 13 | 27 | 00011011 | 0 | 00011010 | 26 |
| 14 | 33 | 00100001 | 0 | 00100000 | 32 |
| 15 | 65 | 01000001 | 0 | 01000000 | 64 |
| 16 | 60 | 00111100 | 1 | 00111101 | 61 |
| | | ……. | | | |
| 128 | 31 | 00011111 | 0 | 00011110 | 30 |

Pada dasarnya, proses ekstraksi dan dekripsi sama dengan proses enkripsi dan *embedding*, tetapi prosesnya dibalik. Dalam proses enkripsi dan *embedding*, pesan rahasia dienkripsi dan kemudian disematkan pada gambar sampul. Sedangkan dalam proses ekstraksi dan dekripsi, gambar steganografi ini diekstraksi kemudian melakukan proses dekripsi pesan yang tersembunyi di dalam gambar. Tabel 1 merupakan proses menampilkan pesan yang tersembunyi di gambar sampul. Proses ekstraksi sama dengan proses *embedding* yaitu menggunakan metode LSB. Sebelum mengambil pesan, gambar diurai lagi untuk memisahkan *header* dan gambar sampul. Kemudian mendeteksi *bit* pada piksel biru dari gambar *stego* dan menggunakan operasi *bitwise AND* dan *bitwise OR* untuk mengekstraksi pesan.

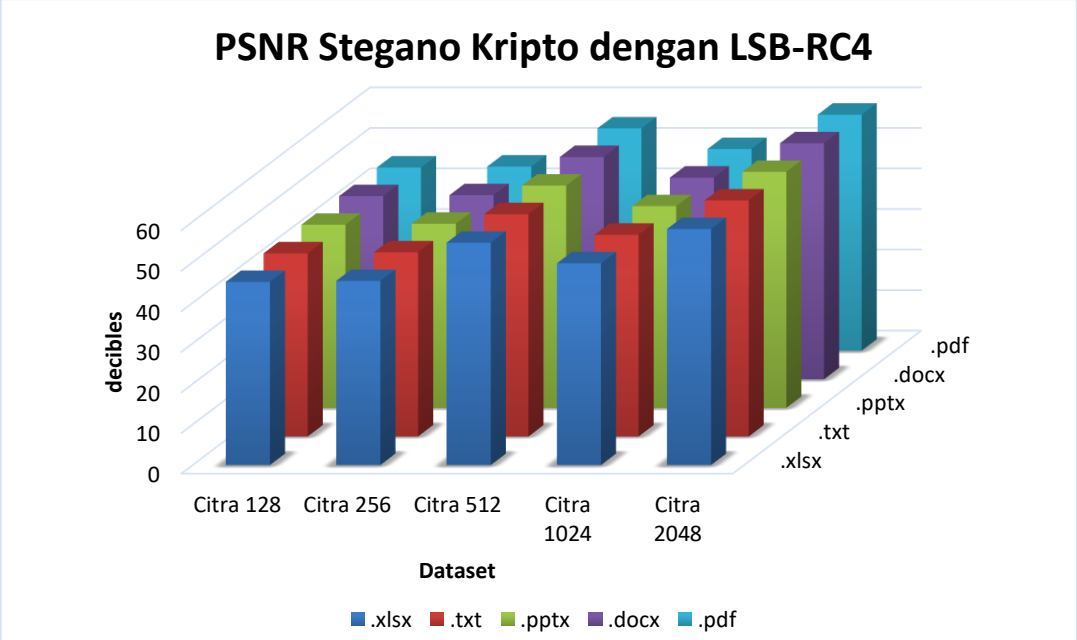
Pesan yang diperoleh masih berupa biner maka perlu dikonversi ke kode ASCII. Pada tahap ini *plaintext* masih terenkripsi, oleh karena itu dibutuhkan proses dekripsi untuk menampilkan *plaintext* yang terdapat pada gambar *stego*. Proses dekripsi yaitu mengubah *ciphertext* ke *plaintext* yang telah tertanam pada gambar *stego* dengan menggunakan *Rivest Cipher 4* (RC4). Proses dekripsi menggunakan kunci yang sama seperti proses enkripsi. Proses dekripsi RC4 yaitu melakukan operasi XOR pada *ciphertext* yang sudah didapat dari proses enkripsi dengan *pseudo-random* pada proses enkripsi dan menggunakan kunci yang sama. Setelah melakukan dekripsi dan mendapatkan *plaintext*, proses selanjutnya yaitu mengubah *plaintext* tersebut menjadi *decimal*. Setelah mendapatkan hasil dari bilangan *decimal*, kemudian diubah menjadi karakter. Tabel 2 merupakan hasil dari pengubahan *plaintext* dari *hexadecimal* menjadi karakter. Hasil PSNR dari eksperimen dapat dilihat pada

*ISSN: 2086-4930*
*e-ISSN: 2777-0648*

Gambar 11, sedangkan hasil MSE dapat dilihat pada Gambar 12. MSE terbaik di dapat oleh objek citra dengan ukuran 512x512 piksel

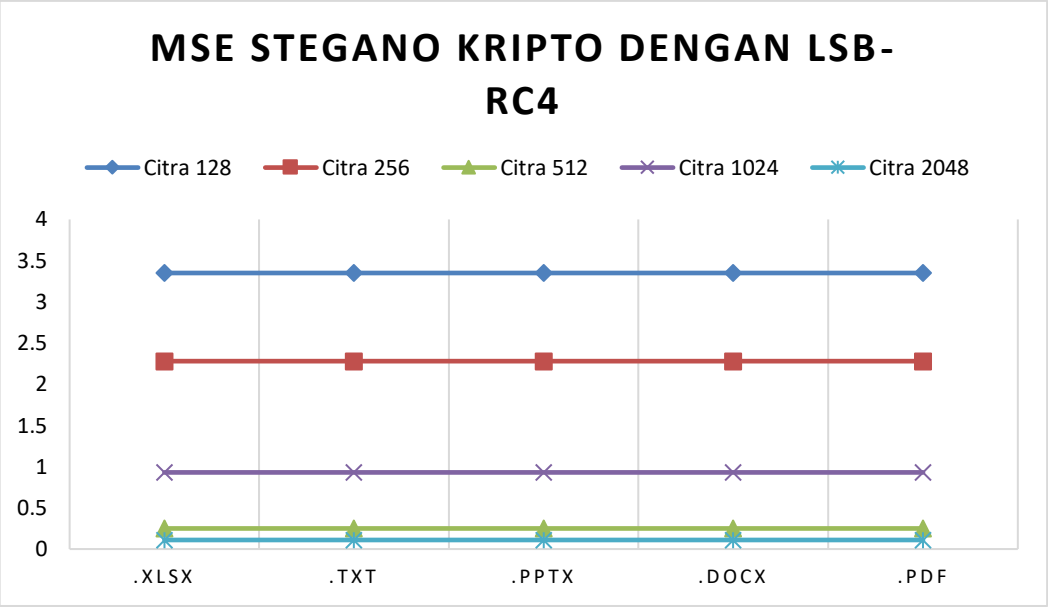
**Tabel 2 Pengubahan *Plaintext* dari *hexadecimal* ke Karakter**

| *Plaintext* | | |
|---|---|---|
| ASCII *Hexadecimal* | ASCII *Decimal* | Karakter |
| 46 | 70 | F |
| 41 | 65 | A |
| 53 | 83 | S |
| 49 | 73 | I |
| 4C | 76 | L |
| 4B | 75 | K |
| 4F | 79 | O |
| 4D | 77 | M |
| 55 | 85 | U |
| 44 | 68 | D |
| 49 | 73 | I |
| 4E | 78 | N |
| 55 | 85 | U |
| 53 | 83 | S |
| 4F | 79 | O |
| 4B | 75 | K |

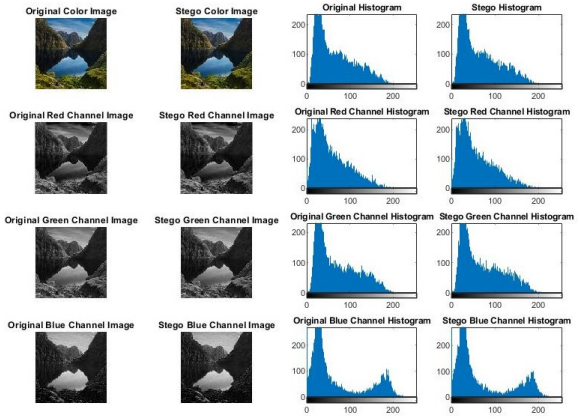



**Gambar 11. Nilai PSNR Stegano Kripto dengan LSB-RC4**

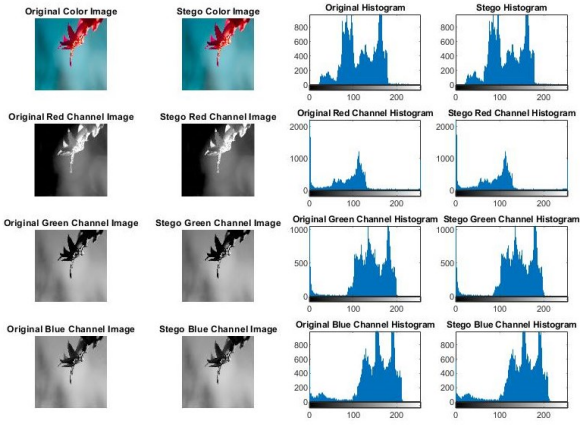
*ISSN: 2086-4930*
*e-ISSN: 2777-0648*



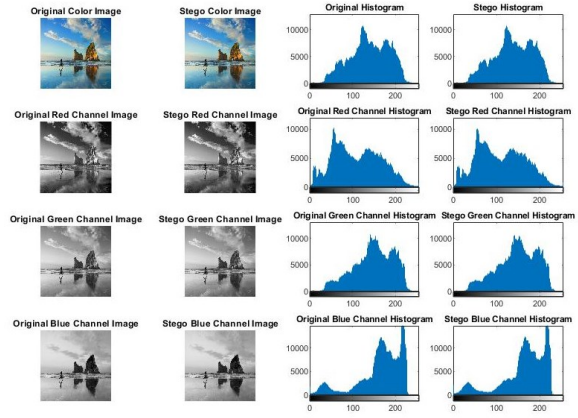

**Gambar 12. Nilai MSE Stegano Kripto dengan LSB-RC4**



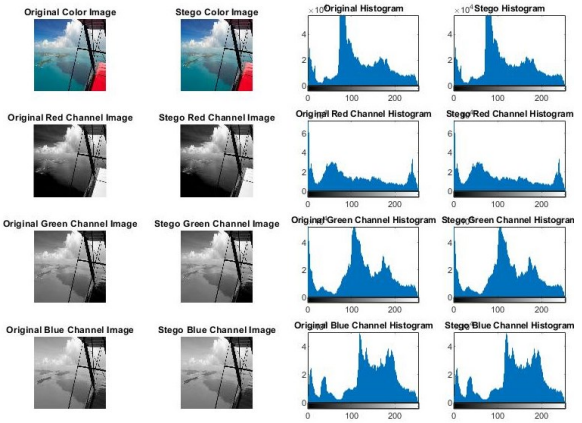

**Gambar 13 Hasil pada citra ukuran 128**



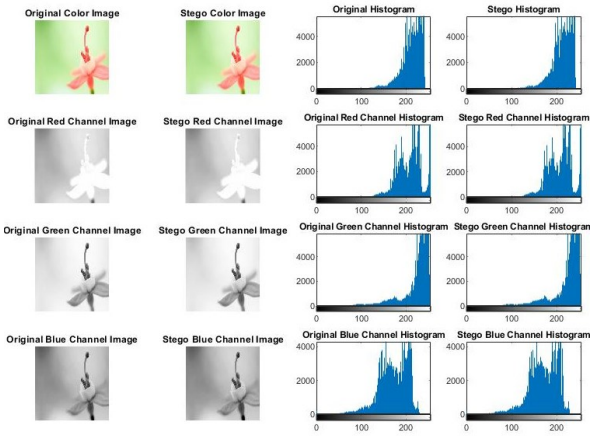

**Gambar 14 Hasil pada citra ukuran 256**




**Gambar 15 Hasil pada citra ukuran 512**




**Gambar 16 Hasil pada citra ukuran 1024**




**Gambar 17 Hasil pada citra ukuran 2048**

Berdasarkan visual hasil pada Gambar 13 sampai Gambar 17, algoritma RC4 dengan metode steganografi LSB yang menggunakan *channel* biru terbukti berkerja dengan baik. Pada Gambar 13 dengan ukuran citra 128x128 piksel telah menghasilkan visual hasil steganografi pada citra warna, citra *red*, *green* dan *blue*. Pada Gambar 13 di bawah ini merupakan contoh *output* dari hasil dekripsi dan ekstraksi dengan menggunakan *file .doc* yang mempunyai ukuran 50,5 kb. Gambar 14 menghasilkan nilai PSNR 45,15 dB dan MSE 3,35. Untuk *size* pada citra *stego* tersebut adalah 34,0 kb dengan *size* citra aslinya 9,90 kb. Gambar 15 menghasilkan nilai PSNR 45,39 dB dan MSE 2,28. Untuk *size* pada citra *stego* tersebut adalah 63,0 kb dengan *size* citra aslinya 13,9 kb. Gambar 16 menghasilkan nilai PSNR 54,80 dB dan MSE 0,25. Untuk *size* pada citra *stego* tersebut adalah 121 kb kb dengan *size* citra aslinya 25,6 kb. Gambar 17 menghasilkan nilai PSNR 49,72 dB dan MSE 0,93. Untuk *size* pada citra *stego* tersebut adalah 1,27 Mb dengan *size* citra aslinya 276 kb. Nilai PSNR di bawah 30dB menunjukkan kualitas yang relatif rendah, dimana distorsi karena penyisipan adalah jelas. Namun, kualitas gambar stego yang tinggi terletak pada 40dB ke atas [15]–[17].

Percobaan menggunakan imperceptibilitas membuktikan bahwa kualitas gambar *stego* sangat baik. Ini dibuktikan dengan kualitas gambar yang memiliki nilai rata – rata PSNR diatas 53 dB, sedangkan nilai untuk PSNR terendah dengan nilai 48 dB dengan dimensi minimal 128x128 *pixel*. Analisis histogram juga menunjukkan kualitas gambar *stego* yang baik. Dalam hal ini bahwa metode yang diusulkan dapat diterapkan untuk proses penyembunyian pesan pada gambar.

## 5 KESIMPULAN

Nilai rata – rata PSNR yang didapatkan pada penelitian ini lebih dari 30 dB, ini membuktikan bahwa kualitas gambar *stego* sangat baik dan kualitas gambar *stego* yang baik memiliki nilai PSNR minimal 30 dB. Nilai PSNR yang didapatkan secara keseluruhan lebih dari 30 dB dengan nilai terendahnya 45,15 dB dengan ukuran citra 128x128 *pixel*. Citra terbaik dengan ukuran 2048x2048 *pixel*. Citra tersebut memiliki nilai MSE yang terkecil yaitu 0,11 dan mendapatkan nilai PSNR 58,18 dB lebih besar dari citra lainnya. Pada proses enkripsi dan *embedding* pesan *file* mengalami perubahan ukuran citra *stego* yang signifikan dari sebelum disisipkan sampai sesudah disisipkan. Dalam penelitian selanjutnya, untuk menjaga kualitas citra *stego* yang baik disarankan menggunakan citra dengan ukuran dimensi

yang lebih besar, hal ini dibuktikan dengan citra 2048x2048. Untuk mendapatkan keamanan yang lebih baik, dapat ditambahkan atau mengganti algoritma kriptografi dengan algoritma yang lebih modern.

## DAFTAR PUSTAKA

[1] C. Irawan, D. R. I. Moses Setiadi, E. H. Rachmawanto, C. A. Sari, and M. Doheir, "Hybrid Encryption using Confused and Stream Cipher to Improved Medical Images Security," in *Journal of Physics: Conference Series*, 2019, vol. 1201, no. 1.

[2] H. Kevin Ronaldo Cahyono, C. A. Sari, de Rosal Ignatius Moses Setiadi, and E. H. Rachmawanto, "Dual protection on message transmission based on Chinese remainder theorem and rivest cipher 4," in *2019 International Conference on Information and Communications Technology, ICOIACT 2019*, 2019.

[3] A. E. Handoyo, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, and A. Susanto, "Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA," *J. Teknol. dan Sist. Komput.*, vol. 6, no. November 2017, pp. 37–43, 2018.

[4] I. U. WM, W. S. Sari, C. A. Sari, and D. R. I. M. Setiadi, "KOMBINASI STEGANOGRAFI-KRIPTOGRAFI CITRA MENGGUNAKAN LSB DAN DES," *SNATIF*, pp. 31–36, 2018.

[5] M. K. Samimi and T. S. Rappaport, "3-D Millimeter-Wave Statistical Channel Model for 5G Wireless System Design," *IEEE Trans. Microw. Theory Tech.*, vol. 64, no. 7, pp. 2207–2225, Jul. 2016.

[6] B. J. Simbolon, "Steganografi Penyisipan Pesan Pada File Citra Dengan Menggunakan Metode LSB (Least Significant Bit)," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 4, no. 1, pp. 1–6, 2021.

[7] C. Manikopoulos, Y. Shi, Z. Zhang, Z. Ni, and D. Zou, "Detection of block DCT-based Steganography in gray-scale images," *Network*, pp. 355–358, 2002.

[8] A. K. Agrahari, M. Sheth, and N. Praveen, "Comprehensive Survey on Image Stegnography Using LSB With AES," vol. 13, no. 8, pp. 5841–5844, 2018.

[9] M. A. Majeed and R. Sulaiman, "An improved LSB image steganography technique using bit-inverse in 24 bit colour image," *J. Theor. Appl. Inf. Technol.*, vol. 80, no. 2, pp. 342–348, 2015.

[10] Z. Y. Al-Omari and A. T. Al-Taani, "Secure LSB steganography for colored images using character-color mapping," in *2017 8th International Conference on Information and Communication Systems (ICICS)*, 2017, pp. 104–110.

[11] A. Goswami, "Coloured and Gray Scale Image Steganography using Block Level DWT DCT Transformation," *Int. J. Comput. Appl. (0975 – 8887)*, vol. 148, no. 7, pp. 4–6, 2016.

[12] A. Suheryadi, "Penerapan Digital Watermark Sebagai Validasi Keabsahan Gambar Digital Dengan Skema Blind Watermark," *JTT (Jurnal Teknol. Ter.*, vol. 3, no. 2, pp. 1–6, 2017.

[13] N. Adam, M. Mashaly, and W. Alexan, "A 3DES Double–Layer Based Message Security Scheme," in *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, 2019, pp. 1–5.

[14] F. A. Rafrastara, R. Prahasiwi, D. R. I. M. Setiadi, E. H. Rachmawanto, and C. A. Sari, "Image steganography using inverted LSB based on 2nd, 3rd and 4th LSB pattern," in *2019 International Conference on Information and Communications Technology, ICOIACT 2019*, 2019.

[15] S. K, "An Optimal RSA Encryption Algorithm for Secret Images," *Int. J. Pure Appl. Math.*, vol. 118, no. 20, pp. 2491–2500, 2018.

[16] P. Chowdhuri, B. Jana, and D. Giri, "Secured steganographic scheme for highly compressed color image using weighted matrix through DCT," *Int. J. Comput. Appl.*, vol. 7074, pp. 1–12, Aug. 2018.

[17] E. J. Kusuma, O. R. Indriani, C. A. Sari, E. H. Rachmawanto, and D. R. I. M. Setiadi, "An imperceptible LSB image hiding on edge region using des encryption," in *Proceedings - 2017 International Conference on Innovative and Creative Information Technology: Computational Intelligence and IoT, ICITech 2017*, 2018.