SKRIPSI

IMPLEMENTASI STEGANOGRAFI UNTUK PENGAMANAN CITRA DIGITAL MENGGUNAKAN METODE *BIT-PLANE COMPLEXITY SEGMENTATION* (BPCS)

Disusun dan diajukan oleh:

REDHA KAMILUL INSAN

H071171506

PROGRAM STUDI SISTEM INFORMASI

DEPARTEMEN MATEMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS HASANUDDIN

MAKASSAR

2023

IMPLEMENTASI STEGANOGRAFI UNTUK PENGAMANAN CITRA DIGITAL MENGGUNAKAN METODE *BIT-PLANE COMPLEXITY SEGMENTATION* (BPCS)

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Sains pada Program Studi Sistem Informasi Departemen Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Hasanuddin

REDHA KAMILUL INSAN

H071171506

PROGRAM STUDI SISTEM INFORMASI

DEPARTEMEN MATEMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS HASANUDDIN

MAKASSAR

2023

PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini :

Nama	: Redha Kamilul Insan
NIM	: H071171506
Program Studi	: Sistem Informasi
Jenjang	: S1

Menyatakan dengan ini bahwa karya tulisan saya berjudul:

Implementasi Steganografi Untuk Pengamanan Citra Digital Menggunakan Metode *Bit-Plane Complexity Segmentation* (BPCS)

Adalah karya tulisan saya sendiri dan bukan merupakan pengambilan alihan tulisan orang lain dan bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri.

Apabila dikemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan isi skripsi ini hasil karya orang lain, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Makassar, 13 Januari 2023

Yang Menyatakan

Redha Kamilul Insan

NIM : H071171506

IMPLEMENTASI STEGANOGRAFI UNTUK PENGAMANAN CITRA DIGITAL MENGGUNAKAN METODE *BIT-PLANE COMPLEXITY SEGMENTATION* (BPCS)

Disusun dan diajukan oleh

REDHA KAMILUL INSAN

H071171506

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka Penyelesaian Studi Program Sarjana Program Studi Sistem Informasi Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Hasanuddin Pada tanggal 13 Januari 2023 dan dinyatakan telah memenuhi syarat kelulusan.

Menyetujui

Pembimbing Utama,	Pembimbing Pendamping
Dr. Hendra, S.Si., M.Kom.	Andi Muhammad Anwar, S.Si., M.Si.
NIP. 197601022002121001	NIP. 199012282018031001

Ketua Program Studi,

Dr. Muhammad Hasbi, M.Sc.
NIP. 196307201989031003

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh	:
Nama	: Redha Kamilul Insan
NIM	: H071171506
Program Studi	: Sistem Informasi
Judul Skripsi	: Implementasi Steganografi Untuk Pengamanan Citra Digital Menggunakan Metode *Bit-Plane Complexity Segmentation* (BPCS)

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Sains Pada Program Studi Sistem Informasi Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Hasanuddin.

DEWAN PENGUJI

		Tanda Tangan
1. Ketua	: Dr. Hendra, S.Si., M.Kom.	(.....)
2. Sekretaris	: Andi Muhammad Anwar, S.Si., M.Si.	(.....)
3. Anggota	: Supri Bin Hj Amir, S.Si., M.Eng.	(.....)
4. Anggota	: A. Muh Amil Siddik, S.Si., M.Si.	(.....)

Ditetapkan di : Makassar

Tanggal : 13 Januari 2023

KATA PENGANTAR

Puji syukur Alhamdulillah kehadirat **ALLAH SWT** atas berkat dan rahmat dan hidayah-Nya yang diberikan kepada penulis sehingga dapat menyelesaikan penulisan skripsi yang berjudul "**Implementasi Steganografi Untuk Pengamanan Citra Digital Menggunakan Metode *Bit-Plane Complexity Segmentation* (BPCS)"**. Pembuatan skripsi ini merupakan salah satu syarat untuk menyelesaikan studi penulis pada jenjang pendidikan Strata Satu Program Studi Sistem Informasi, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Hasanuddin.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, penulis berharap dapat belajar lebih banyak lagi dalam mengimplementasikan ilmu yang didapatkan. Skripsi ini tentunya tidak lepas dari bimbingan, masukan, dan arahan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Rektor Universitas Hasanuddin Bapak **Prof. Dr. Ir. Jamaluddin Jompa, M.Sc.** dan seluruh Wakil Rektor dalam Lingkungan Universitas Hasanuddin.
2. Bapak Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Bapak **Dr. Eng. Amiruddin, S.Si., M.Si.** dan para Wakil Dekan serta seluruh staf yang telah memberikan bantuan selama penulis mengikuti pendidikan di FMIPA Universitas Hasanuddin.
3. Bapak **Prof. Dr. Nurdin, S.Si., M.Si.** selaku Ketua Departemen Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam.
4. Bapak **Dr. Muhammad Hasbi, M.Sc.** sebagai Ketua Program Studi Sistem Informasi Universitas Hasanuddin.
5. Bapak **Dr. Hendra, S.Si., M.Kom**. sebagai pembimbing utama yang telah banyak memberikan arahan ide, motivasi serta dukungan kepada penulis dalam banyak hal.
6. Bapak **Andi Muhammad Anwar, S.Si., M.Si.** sebagai pembimbing pendamping yang senantiasa memberikan masukan kepada penulis.

7. Bapak **Supri Bin Hj Amir, S.Si., M.Eng.** dan Bapak **A. Muh. Amil Siddik, S.Si., M.Si.** sebagai tim penguji atas saran dan masukan pada penelitian yang telah dilakukan kepada penulis.
8. Orangtua tercinta, Ayahanda **Drs. Andi Mappaselle** dan Ibunda **Ir. Sri Setijawati** serta kakak **Kaisar Reza Wicaksono** yang telah mendoakan, memberikan dukungan dan memotivasi dalam menyelesaikan skripsi ini.
9. Teman-teman seperjuangan **Program Studi Sistem Informasi Angkatan 2017**, **H071171001, H071171002, H071171003, H071171004, H071171005, H071171006, H071171007, H071171008, H071171009, H071171010, H071171011, H071171012, H071171013, H071171014, H071171016, H071171301, H071171302, H071171303, H071171304, H071171305, H071171306, H071171307, H071171308, H071171310, H071171311, H071171312, H071171313, H071171314, H071171316, H071171501, H071171502, H071171503, H071171504, H071171505, H071171507, H071171508, H071171509, H071171510, H071171511, H071171512, H071171513, H071171514, H071171515, H071171516, H071171518, H071171519, H071171520, H071171522, H071171523, H071171524, H071171525, H071171526, H071171527, H071171528, H071171529, H071171530 dan H071171532** yang telah mendukung dan berjuang bersama dalam suka dan duka selama ini.
10. Kakak-kakak dan adik-adik **Program Studi Sistem Informasi Angkatan 2014, 2015, 2016, 2018, 2019, 2020, 2021** dan **2022**.
11. Teman-teman **BALANCE FIB 317 Ilmu-Budaya Angkatan 2017, A021171026, A021171535, A021171806, A031171803, B011171004, B011171078, B011171306, B011171407, B021171318, C021171010, C041171502, E011171002, E031171004, E031171315, E041171312, F011171301, F041171011, G011171327, G021171522, G031171525, G041171020, H041171311, H051171004, H061171508, I01171015, J011171029, K011171327, K011171803, L011171322, L011171501, L041171306, L051171517, M011171056, M011171306, N011171005 dan N011171035** terima kasih atas pengalaman kebersamaan walaupun cuma lima kali pertemuan.

12. Teman-teman **KKN Panakukang 1 Gelombang 104, A011171301, A021171525, A031171340, B011171304, B011171321, B011171339, B011171372, B011171410, B011171571, B011171601, B011171608, B021171511, D12116514, D22116505, D021171022, D021171023, D131171701, E011171007, E071171514, F081171306, L011171014, L011171526, L031171521 dan L051171521** terima kasih atas pengalaman dalam membagi masker di empat kelurahan berbeda.
13. Terima kasih kepada **5371 Mahasiswa Universitas Hasanuddin Angkatan 2017** yang tidak disebutkan namanya satu per satu atas kebersamaan menemani penulis selama masa kuliah.

Penulis berharap semoga skripsi ini dapat bermanfaat dan semoga Allah SWT berkenan meridhoi segala yang telah kita kerjakan.

Makassar, 13 Januari 2023

Penulis

PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Hasanuddin, saya yang bertanda tangan di bawah ini:

Nama	: Redha Kamilul Insan
NIM	: H071171506
Program Studi	: Sistem Informasi
Departemen	: Matematika
Fakultas	: Matematika dan Ilmu Pengetahuan Alam
Jenis Karya	: Skripsi

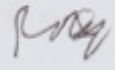
demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Hasanuddin **Hak Bebas Royalti Noneksklusif** (***Non-exclusive Royalty-Free Right***) atas karya ilmiah saya yang berjudul:

"Implementasi Steganografi Untuk Pengamanan Citra Digital Menggunakan Metode *Bit-Plane Complexity Segmentation* (BPCS)"

beserta perangkat yang ada (jika diperlukan). Terkait dengan hal di atas, maka pihak universitas berhak menyimpan, mengalih-media/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.
Dibuat di Makassar Pada tanggal 13 Januari 2023

Yang menyatakan



(Redha Kamilul Insan)

ABSTRAK

Steganografi adalah teknik untuk menyembunyikan data ke dalam citra *cover* tanpa menimbulkan kecurigaan. *Bit-Plane Complexity Segmentation* (BPCS) merupakan bagian dari steganografi yang menawarkan penyembunyian data dengan kapasitas yang lebih besar dibandingkan dengan metode *Least Significant Bit* (LSB). Prinsip utama dari teknik *Bit-Plane Complexity Segmentation* (BPCS) adalah citra *cover* dibagi menjadi *informative region* dan *noise like region*. Data rahasia disembunyikan kedalam *noise like region* pada citra *image* tanpa adanya kerusakan apapun. Dalam penelitian ini penulis menggunakan prinsip *Bit-Plane Complexity Segmentation* (BPCS) dan menggunakan empat buah citra *image* dengan format .png serta data rahasia yang disembunyikan berupa teks dalam bentuk .txt. Untuk mengetahui kualitas citra *image* dan citra stego dihitung nilai *Peak Signal-to-Noise Ratio* (PSNR). Dalam penelitian ini diperoleh nilai *Peak Signal-to-Noise Ratio* (PSNR) dalam rentang 30 db sampai 40 db dan pesan berhasil diekstrak secara utuh.

Kata Kunci : Steganografi, *Bit-Plane Complexity Segmentation*, *Informative Region*, *Noise Like Region*, *Peak Signal-to-Noise Ratio*.

ABSTRACT

Steganography is a technique to hide data into a cover image without arousing suspicion. Bit-Plane Complexity Segmentation (BPCS) is a part of steganography that offers data hiding with a greater capacity than the Least Significant Bit (LSB) method. The main principle of the Bit-Plane Complexity Segmentation (BPCS) technique is that the cover image is divided into informative regions and noise like regions. The secret data is hidden into the noise like region of the image without any damage. In this study the author uses the principle of Bit-Plane Complexity Segmentation (BPCS) and uses four images in .png format and hidden secret data in the form of text in .txt format. To determine the quality of the image and stego image, the Peak Signal-to-Noise Ratio (PSNR) value was calculated. In this study, the Peak Signal-to-Noise Ratio (PSNR) value was obtained in the range of 30 db to 40 db and the message was successfully extracted in its entirety.

Keywords : Steganography, Bit-Plane Complexity Segmentation, Informative Region, Noise Like Region, Peak Signal-to-Noise Ratio.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam era globalisasi seperti sekarang ini kebutuhan akan teknologi informasi merupakan suatu kebutuhan yang sangat penting. Dengan adanya internet maka komunikasi akan terjadi dalam waktu yang sangat cepat dan tanpa batas. Informasi mudah kita dapatkan kapanpun, dimanapun dan dapat diakses oleh siapa saja sehingga dibutuhkan keamanan data agar data tidak bisa diakses oleh sembarang orang yang tidak berhak sehingga keamanan dan kerahasiaan dapat terjamin. Untuk mengatasi hal tersebut diperlukan suatu teknik yang mampu menyembunyikan pesan pada suatu media sehingga pesan tersebut aman dari gangguan orang-orang yang tidak berhak untuk mengaksesnya. Teknik yang digunakan adalah steganografi. Steganografi berasal dari bahasa Yunani yang berarti tulisan tersembunyi.

Steganografi berasal dari kata stega + nografi. Stega berarti tertutup berasal dari kata Yunani *stegos* dan *nography* berarti tulisan yang berasal dari kata Yunani *graphia*. Dengan demikian, steganografi berarti tulisan tertutup. Steganografi adalah ilmu pengetahuan dan seni untuk menyembunyikan informasi rahasia pada suatu media digital agar tidak terlihat seperti seharusnya. Steganografi menyembunyikan informasi atau pesan kedalam media lain seperti citra digital, teks, suara atau video sehingga tidak menimbulkan kecurigaan orang lain. Properti yang digunakan dalam steganografi ada dua yaitu informasi atau data yang mau disembunyikan dan media penampung. Media penampung yang digunakan adalah citra digital. Penyisipan informasi pada citra digital berlangsung pada bit-bit piksel pada citra digital. Steganografi adalah seni kuno menyampaikan pesan secara rahasia sehingga hanya penerima yang mengetahui keberadaan pesan tersebut. Pesan disembunyikan di media lain sehingga media yang ditransmisikan tampak bermakna bagi penyerang. Jika pesan tersembunyi diekstraksi, teknik steganografi gagal. Teknik steganografi memungkinkan satu pihak berkomunikasi dengan pihak lain tanpa disadari pihak ketiga bahwa komunikasi sedang terjadi. Steganografi adalah metode penyandian data rahasia sedemikian rupa sehingga keberadaan

informasi tersebut disembunyikan. Biasanya, data disembunyikan di dalam sampul yang tidak berbahaya sehingga bahkan jika agen musuh menemukan sampul itu, tidak ada kecurigaan tentang keberadaan data di sampul itu. Steganografi dan kriptografi mempunyai kesamaan yaitu dalam keamanan. Namun, teknik kriptografi dan steganografi berbeda satu sama lain. Dalam kriptografi, pesan asli diacak, yaitu struktur aslinya diubah secara berurutan untuk membuatnya tidak berarti. Jadi, ketika penyerang menemukan pesan, masih sulit baginya untuk mendapatkan kembali pesan aslinya. Kriptografi tidak berusaha menyembunyikan pesan. Dalam steganografi, pesan disembunyikan secara diam-diam di dalam file gambar, audio atau video. Dengan demikian tidak timbul kecurigaan terhadap penyerang. Steganografi tidak berusaha mengacak pesan asli. Tujuan dari steganografi dan kriptografi adalah untuk melindungi pesan asli dari penyerang (Khaire & Nabalwar, 2010).

Steganografi pada citra digital adalah teknik menyembunyikan suatu informasi rahasia pada suatu media digital agar tidak terlihat seperti semestinya. Salah satu metode steganografi adalah *Bit-Plane Complexity Segmentation* (BPCS). *Bit-Plane Complexity Segmentation* (BPCS) memanfaatkan karakteristik dari *human vision system* yaitu manusia tidak melihat informasi visual dalam area yang mengandung *noise* dalam sebuah citra. Kelebihan metode ini adalah memiliki rasio penyisipan yang besar jika dibandingkan menggunakan metode *Least Significant Bit* (LSB) (Widyastutiningsih, 2011). Metode *Bit-Plane Complexity Segmentation* (BPCS) merupakan pengembangan dari metode *Least Significant Bit* (LSB). Metode *Bit-Plane Complexity Segmentation* (BPCS) dapat menyimpan kapasitas yang lebih besar dan kualitas citra yang lebih baik daripada metode *Least Significant Bit* (LSB). Untuk gambar normal kira-kira 50% data dapat diganti dengan data rahasia sebelum degradasi gambar terlihat dengan jelas. Metode *Bit-Plane Complexity Segmentation* (BPCS) dikemukakan pertama kali oleh Eiji Kawaguchi dan Richard O. Eason pada tahun 1998.

Maka dari latar belakang yang dibahas peneliti tertarik mengambil judul "**Implementasi Steganografi Untuk Pengamanan Citra Digital Menggunakan Metode *Bit-Plane Complexity Segmentation* (BPCS)**".

1.2 Rumusan Masalah

Rumusan masalah dari penelitian ini sebagai berikut:

1. Bagaimana mengimplementasikan steganografi dengan metode *Bit-Plane Complexity Segmentation* (BPCS) untuk pengamanan citra digital?
2. Bagaimana menganalisis tingkat kemiripan *image secret* sebelum disisipkan dan sesudah diekstraksi dengan parameter *Peak Signal-to-Noise Ratio* (PSNR) dan *Mean Squared Error* (MSE)?

1.3 Batasan Masalah

Batasan masalah dari penelitian ini sebagai berikut:

1. Penelitian ini membahas teknik penyembunyian pesan rahasia dengan menggunakan metode *Bit-Plane Complexity Segmentation* (BPCS).
2. Media penampung gambar yang digunakan adalah format gambar png dan format teks yang digunakan adalah txt.
3. Parameter penelitian ini adalah kualitas file citra dengan menghitung nilai *Peak Signal-to-Noise Ratio* (PSNR) dan *Mean Squared Error* (MSE).
4. File citra *cover* yang digunakan adalah citra berukuran kelipatan 8×8.
5. Nilai kompleksitas (*alpha*) yang dipakai adalah 0,3.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini sebagai berikut:

1. Mengimplementasikan steganografi dengan metode *Bit-Plane Complexity Segmentation* (BPCS) untuk pengamanan citra digital.
2. Menganalisis tingkat kemiripan *image secret* sebelum disisipkan dan sesudah diekstraksi dengan parameter *Peak Signal-to-Noise Ratio* (PSNR) dan *Mean Squared Error* (MSE).

1.5 Manfaat Penelitian

Manfaat dari penelitian ini sebagai berikut:

1. Dapat mengimplementasikan *Bit-Plane Complexity Segmentation* (BPCS) untuk penyembunyian data.

2. Untuk bisa menyembunyikan pesan rahasia tanpa diketahui oleh indera penglihatan manusia.
3. Untuk bisa mengekstrak pesan rahasia secara utuh dan tidak rusak.

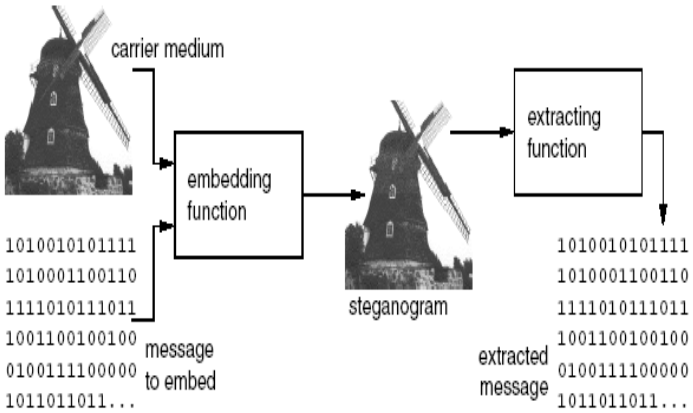
BAB II

TINJAUAN PUSTAKA

2.1 Steganografi

Steganografi merupakan suatu cabang ilmu yang mempelajari tentang bagaimana menyembunyikan suatu informasi rahasia di dalam suatu informasi lainnya (Darwis & Kisworo, 2017). Steganografi adalah jenis komunikasi yang tersembunyi, yang secara harfiah berarti tulisan tertutup. Pesannya terbuka, selalu terlihat, tetapi tidak terdeteksi bahwa adanya pesan rahasia. Deskripsi lain yang popular untuk steganografi adalah *Hidden in Plain Sight* yang artinya tersembunyi di depan mata. Sebaliknya, kriptografi adalah tempat pesan acak, tak dapat dibaca dan keberadaan pesan sering dikenal (Syawal dkk, 2016).

Di masa lalu, orang-orang menggunakan tato tersembunyi atau tinta tak terlihat untuk menyampaikan isi steganografi. Sekarang, teknologi jaringan dan komputer menyediakan cara *easy-to-use* jaringan komunikasi untuk steganografi. Proses penyembunyian informasi di dalam suatu sistem steganografi dimulai dengan mengidentifikasi suatu sampul media yang mempunyai bit berlebihan (yang dapat dimodifikasi tanpa menghancurkan integritas media). Proses menyembunyikan (*embedding*) menciptakan suatu proses stego *medium* dengan cara menggantikan bit yang berlebihan dengan data dari pesan yang tersembunyi (Wijaya & Prayudi, 2004). Bisa dilihat di Gambar 2.1.



Gambar 2.1 Sistem Steganografi (Sumber: Teknik Steganografi dengan Menggunakan Metode *Visual Attacks* dan *Statistical Attacks*)

Satu hal esensial yang menjadi kelebihan steganografi adalah kemampuannya untuk menipu persepsi manusia, manusia tidak memiliki insting untuk mencurigai adanya arsip-arsip yang memiliki informasi yang tersembunyi di dalamnya, terutama bila arsip tersebut tampak seperti arsip normal lainnya. Namun begitu terbentuk pula suatu teknik yang dikenal dengan *steganalysis*, yaitu suatu teknik yang digunakan untuk mendeteksi penggunaan steganografi pada suatu arsip. Seorang *steganalyst* tidak berusaha untuk melakukan dekripsi terhadap informasi yang tersembunyi dalam suatu arsip, yang dilakukan adalah berusaha untuk menemukannya (Irfan, 2013).

2.2 Citra Digital

Pengolahan citra digital (*digital image processing*) adalah bidang ilmu yang mempelajari tentang bagaimana suatu citra itu dibentuk, diolah, dan dianalisis sehingga menghasilkan informasi yang dapat dipahami oleh manusia (Pamungkas, 2017). Citra yang dimaksud disini adalah gambar diam (foto) maupun gambar bergerak (video). Citra (*image*) adalah suatu cahaya pada bidang dua dimensi. Ditinjau dari sudut pandang matematis, citra merupakan fungsi kontinyu dari intensitas cahaya pada bidang dua dimensi. Berdasarkan bentuk sinyal penyusunnya, citra dapat digolongkan menjadi dua jenis yaitu citra analog dan citra digital. Citra analog adalah citra yang dibentuk dari sinyal analog yang bersifat kontinyu, sedangkan citra digital adalah citra yang dibentuk dari sinyal digital yang bersifat diskrit (Pamungkas, 2017).

Citra digital tidaklah selalu merupakan hasil langsung dari data rekaman sebuah sistem. Tetapi terkadang merupakan hasil rekaman data yang sifatnya kontinyu seperti gambar pada monitor tv, foto pada sinar-x dan lain-lain. Dengan begitu untuk memperoleh suatu citra digital dibutuhkan sebuah proses konversi, sehingga selanjutnya citra tersebut bisa diproses menggunakan komputer (Temukan Pengertian, 2013). Citra digital adalah gambar dua dimensi yang bisa ditampilkan pada layar komputer sebagai himpunan nilai digital yang disebut piksel (*picture elements*) (Temukan Pengertian, 2013). Citra digital merupakan representasi dari fungsi intensitas cahaya dalam bentuk diskrit pada bidang dua dimensi. Sebuah citra digital dapat diwakili oleh sebuah matriks dua dimensi $f(x, y)$ yang terdiri dari M kolom dan N baris, dimana perpotongan antara kolom dan baris disebut piksel

(*pixel* = *picture element*) atau elemen terkecil dari sebuah citra (Kusumanto & Tompunu, 2011). Penulisan matriks pada citra digital dapat ditulis sebagai berikut:

$$f(x,y) \approx \begin{bmatrix} f(0,0) & f(0,1) & \cdots & f(0,M-1) \\ f(1,0) & f(1,1) & \cdots & f(1,M-1) \\ \vdots & \vdots & \vdots & \vdots \\ f(N-1,0) & f(N-1,1) & \cdots & f(N-1,M-1) \end{bmatrix} \quad (2.1)$$

Suatu citra $f(x,y)$ dalam fungsi matematis dapat dituliskan sebagai berikut:

$$0 \leq x \leq M-1 \quad (2.2)$$

$$0 \leq y \leq N-1 \quad (2.3)$$

$$0 \leq f(x,y) \leq G-1 \quad (2.4)$$

Dimana M = jumlah piksel baris (*row*) pada *array* citra, N = jumlah piksel kolom (*column*) pada *array* citra, dan G = nilai skala keabuan (*graylevel*). Besarnya nilai M, N dan G pada umumnya merupakan perpangkatan dari dua dapat ditulis sebagai berikut:

$$M = 2^m \quad (2.5)$$

$$N = 2^n \quad (2.6)$$

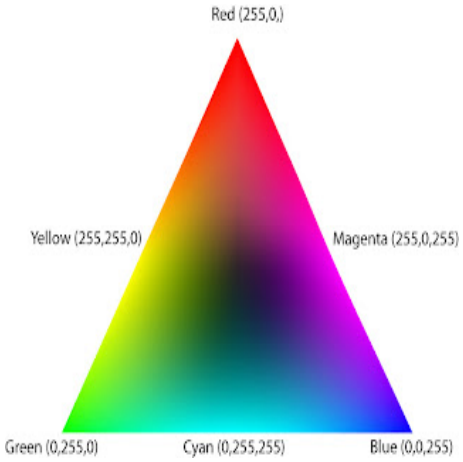
$$G = 2^k \quad (2.7)$$

Dimana nilai m, n dan k adalah bilangan bulat positif. Interval (0,G) disebut skala keabuan (*grayscale*). Besar G tergantung pada proses digitalisasinya. Biasanya keabuan 0 (nol) menyatakan intensitas hitam dan 1 (satu) menyatakan intensitas putih. Untuk citra 8 bit, nilai G sama dengan 2^8 = 256 warna (derajat keabuan).

2.3 Jenis-Jenis Citra Digital

Berdasarkan kombinasi warna pada piksel, citra dibagi menjadi tiga jenis yaitu citra *Red Green Blue* (RGB), citra *grayscale* dan citra biner. Citra *Red* (merah), *Green* (hijau), dan *Blue* (biru) merupakan warna dasar yang dapat diterima oleh mata manusia. Warna pada tiap piksel ditentukan berdasarkan kombinasi dari warna *Red*, *Green*, *Blue*. Setiap warna memiliki intensitas tersendiri dengan nilai minimum 0 dan maksimum 255 (8 bit). Pilihan skala 256 didasarkan pada cara mengungkap 8 digit bilangan biner yang digunakan oleh komputer. Sehingga akan diperoleh warna campuran sebanyak $256 \times 256 \times 256 = 16.777.216$ jenis warna.

Bentuk representasi warna dari sebuah citra digital dapat dilihat pada Gambar 2.2.



Gambar 2.2 Warna RGB pada Citra Digital (Sumber: Model Warna RGB)

Representasi citra RGB dan masing-masing kanal warna penyusunnya ditunjukkan pada Gambar 2.3, Gambar 2.4, Gambar 2.5 dan Gambar 2.6.

Gambar 2.3 Citra RGB

Gambar 2.4 Kanal Merah

Gambar 2.5 Kanal Hijau

Gambar 2.6 Kanal Biru

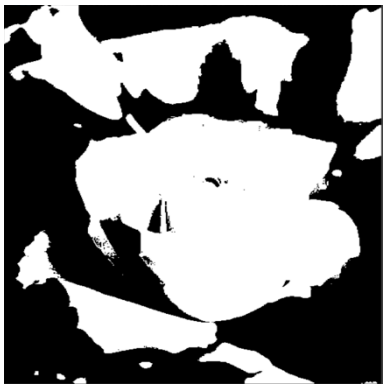
Citra *grayscale* (*black and white*) merupakan citra yang nilai intensitas pikselnya berdasarkan pada derajat keabuan. Pada citra *grayscale* (*black and white*) 8 bit, derajat warna hitam sampai dengan putih dibagi kedalam 256 derajat keabuan dimana warna hitam sempurna direpresentasikan dengan nilai 0 dan putih sempurna dengan nilai 255. Format ini sangat membantu dalam pemrograman karena manipulasi bit yang tidak terlalu banyak. Rentang warna pada citra *grayscale* (*black and white*) sangat cocok digunakan untuk pengolahan file gambar. *Grayscale* (*black and white*) sebenarnya merupakan hasil rata-rata dari *color image* dengan demikian persamaanya dapat dituliskan sebagai berikut (Kusumanto & Tompunu, 2011):

$$I_{BW}(x,y) = \frac{I_R(x,y) + I_G(x,y) + I_B(x,y)}{3} \tag{2.8}$$

Dimana I_{BW} adalah citra *grayscale* (*black and white*), I_R adalah citra *red*, I_G adalah citra *green*, dan I_B adalah citra *blue*. Citra hasil konversi RGB menjadi *grayscale* ditunjukkan pada Gambar 2.7.

Gambar 2.7 Citra *Grayscale*

Citra biner adalah setiap piksel hanya terdiri dari warna hitam atau putih, karena hanya ada dua warna untuk setiap piksel, maka hanya perlu 1 bit per piksel (0 dan 1) atau apabila dalam 8 bit (0 dan 255), sehingga sangat efisien dalam hal penyimpanan. Gambar yang direpresentasikan dengan biner sangat cocok untuk teks (dicetak atau tulisan tangan), sidik jari (*finger print*), atau gambar arsitektur (Kusumanto & Tompunu, 2011). Citra *grayscale* dapat dikonversi menjadi citra biner melalui proses *thresholding*. Dalam proses *thresholding*, dibutuhkan suatu nilai *threshold* sebagai nilai pembatas konversi. Nilai intensitas piksel yang lebih besar atau sama dengan nilai *threshold* akan dikonversi menjadi 1. Sedangkan nilai intensitas piksel yang kurang dari nilai *threshold* akan dikonversi menjadi 0 (Pamungkas, 2017). Citra hasil konversi *grayscale* menjadi biner ditunjukkan pada Gambar 2.8.



Gambar 2.8 Citra Biner

2.4 *Bit-Plane Complexity Segmentation* (BPCS)

Bit-Plane Complexity Segmentation (BPCS) adalah salah satu teknik steganografi yang diperkenalkan oleh Eiji Kawaguchi dan R. O. Eason pada tahun 1998, untuk mengatasi kekurangan teknik steganografi tradisional seperti teknik *Least Significant Bit* (LSB), *Transform embedding technique*, *Perceptual masking technique*. Teknik tradisional ini membatasi kapasitas data yang dapat disembunyikan dan hanya dapat menyembunyikan hingga 10 – 15% dari jumlah besarnya media penampung. Sedangkan *Bit-Plane Complexity Segmentation* (BPCS) dapat menampung pesan hampir 50% dari jumlah besarnya media penampung. Hal ini terjadi karena penyisipan dilakukan tidak hanya pada *Least Significant Bit* (LSB), tapi pada seluruh *bit-plane* termasuk pada *Most Significant Bit* (MSB). Sedangkan untuk citra hasil steganografi terlihat sama seperti citra aslinya, tidak terlihat perbedaannya secara visual (Arianto dkk, 2017).

Prinsip dasar dari *Bit-Plane Complexity Segmentation* (BPCS) adalah citra biner dibagi menjadi *informative region* dan *noise-like region*. Data rahasia disembunyikan kedalam *noise-like region* dari citra penampung tanpa ada kerusakan gambar. Dalam *Bit-Plane Complexity Segmentation* (BPCS) misal terdapat citra multi-nilai (P) yang terdiri dari n-bit piksel dapat dibagi menjadi himpunan citra n-biner. Biasanya data gambar biasa direpresentasikan dengan menggunakan *Pure Binary Code* (PBC) yang biasa digunakan dalam pemrosesan gambar. Meskipun *Canonical Gray Code* (CGC) itu lebih mudah daripada *Pure Binary Code* (PBC) dalam *Bit-Plane Complexity Segmentation* (BPCS) misal P adalah n-bit citra abu-abu katakan n = 8. Karena itu P = [P_7, P_6, P_5, P_4, P_3, P_2, P_1, P_0] dimana P_7 adalah *Most Significant Bit* (MSB) *bit-plane* dan P_0 adalah *Least Significant Bit* (LSB) *bit-plane*. Setiap *bit-plane* dibagi menjadi *informative region* dan *noise-like region*. *Informative region* terdiri dari pola sederhana sedangkan *noise-like region* terdiri dari pola kompleks. *Bit-Plane Complexity Segmentation* (BPCS) mengganti setiap *noise-like region* dengan pola *noise-looking* yang lain tanpa mengubah kualitas gambar secara keseluruhan. Dengan demikian, steganografi *Bit-Plane Complexity Segmentation* (BPCS) memanfaatkan sifat sistem penglihatan manusia (Khaire & Nabalwar, 2010).

Sementara itu, kompleksitas citra biner adalah suatu parameter kerumitan dari suatu citra biner. Perubahan warna hitam dan putih dalam gambar biner pada setiap baris dan kolom secara horizontal (kiri ke kanan) dan vertikal (atas ke bawah) adalah ukuran yang baik untuk menghitung nilai kompleksitas. Jika perubahan warna yang terjadi banyak, maka gambar tersebut memiliki tingkat kompleksitas tinggi. Jika sebaliknya, maka gambar tersebut merupakan gambar yang *simple*. Kompleksitas gambar dilambangkan dengan α dan diberikan persamaan:

$$\alpha = \frac{k}{2 \times 2^n \times (2^n - 1)} \tag{2.9}$$

Dimana k adalah perubahan warna hitam-putih dan α adalah nilai kompleksitas. Untuk sebuah citra biner persegi dengan ukuran $2^n \times 2^n$, kemungkinan maksimal perubahan warna adalah $2 \times 2^n \times (2^n - 1)$ dan kemungkinan minimum perubahan warnanya adalah 0, diperoleh untuk gambar semua hitam atau semua putih. Untuk membangun sebuah konjugasi S^* dari sebuah gambar S, dapat dilakukan dengan rumus berikut, dimana $\oplus$ menandakan operasi *exclusive* OR (XOR) (Hikmatiyar, 2012).

$$S^* = S \oplus W_c \tag{2.10}$$

$$(S^*)^* = S \tag{2.11}$$

$$S^* \neq S \tag{2.12}$$

Jika $\alpha(S)$ adalah kompleksitas dari S, maka:

$$\alpha(S^*) = 1 - \alpha(S) \tag{2.13}$$

Langkah-langkah yang dilakukan pada algoritma *Bit-Plane Complexity Segmentation* (BPCS) pada saat menyisipkan data adalah sebagai berikut (Habibi, 2018):

1. *Cover image* dengan sistem *Pure Binary Code* (PBC) diubah menjadi sistem *Canonical Gray Code* (CGC), kemudian gambar tersebut di-*slice* menjadi *bit-plane* dalam bentuk gambar biner. Setiap *bit-plane* mewakili bit dari setiap piksel pada gambar. Berikut adalah rumus konversi *Pure Binary Code* (PBC) ke *Canonical Gray Code* (CGC).

$$CGC_1 = PBC_i \tag{2.14}$$

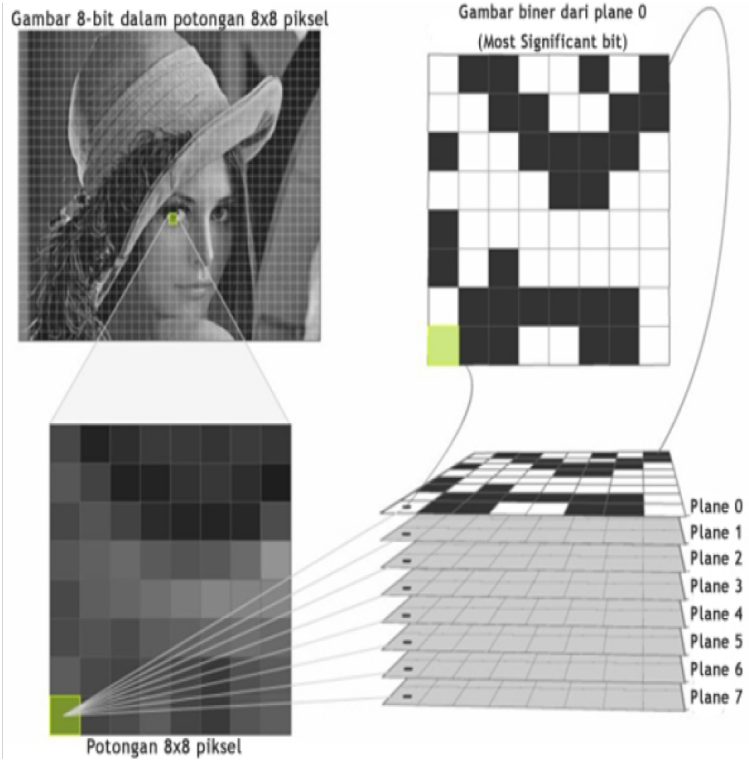
$$CGC_i = PBC_{i-1} \oplus PBC_i \tag{2.15}$$

2. Segmentasi setiap *bit-plane* pada *cover image* menjadi *informative* dan *noise-like region* dengan menggunakan nilai batas (*threshold*) (α_0). Nilai umum dari $\alpha_0 = 0{,}3$.
3. Kelompokkan byte-byte pesan rahasia menjadi rangkaian blok pesan rahasia.
4. Jika blok (S) kurang kompleks dibandingkan dengan nilai batas, maka lakukan konjugasi terhadap S untuk mendapatkan S^* yang lebih kompleks. Blok konjugasi (S^*) pasti lebih kompleks dibandingkan dengan nilai batas.
5. Sisipkan setiap blok pesan rahasia ke *bit-plane* yang merupakan *noise-like region* (atau gantikan semua bit pada *noise-like region*). Jika blok S dikonjugasi, maka simpan data pada *conjugation map*.
6. Sisipkan juga *conjugation map* seperti yang dilakukan pada blok pesan rahasia.
7. Ubah stego-image dari sistem *Canonical Gray Code* (CGC) menjadi sistem *Pure Binary Code* (PBC).

Adapun proses ekstraksi pada algoritma *Bit-Plane Complexity Segmentation* (BPCS) sebagai berikut (Munir, 2016):

1. Bagi *stego-image* menjadi blok 8×8 piksel.
2. Bentuk setiap blok 8×8 piksel menjadi sistem *Pure Binary Code* (PBC) yang terdiri dari 8 buah *bit-plane.*
3. Ubah sistem *Pure Binary Code* (PBC) menjadi sistem *Canonical Gray Code* (CGC).
4. Hitung kompleksitas setiap *bit-plane*. Jika kompleksitasnya di atas nilai ambang α_0, maka *bit-plane* tersebut bagian dari pesan. Tabel konjugasi yang disisipkan juga dibaca untuk melihat proses konjugasi yang perlu dilakukan pada tiap blok pesan.

Misalkan sebuah dokumen citra akan disisipi sebuah pesan rahasia M_S. Pertama piksel pada citra asli (*cover image*) dibagi menjadi segmen-segmen gambar biner seperti ditunjukkan pada Gambar 2.9. Kemudian pesan rahasia dibagi menjadi blok yang masing-masing berukuran 64 bit, dan direpresentasikan pada matriks berukuran 8×8.



Gambar 2.9 Proses Pengubahan Gambar Menjadi Segmen-Segmen *Bit-Plane* (Sumber: Penyembunyian Pesan Pada Citra Terkompresi dengan Metode *Bit-Plane Complexity Segmentation* (BPCS) dan Teknik Permutasi Blok)

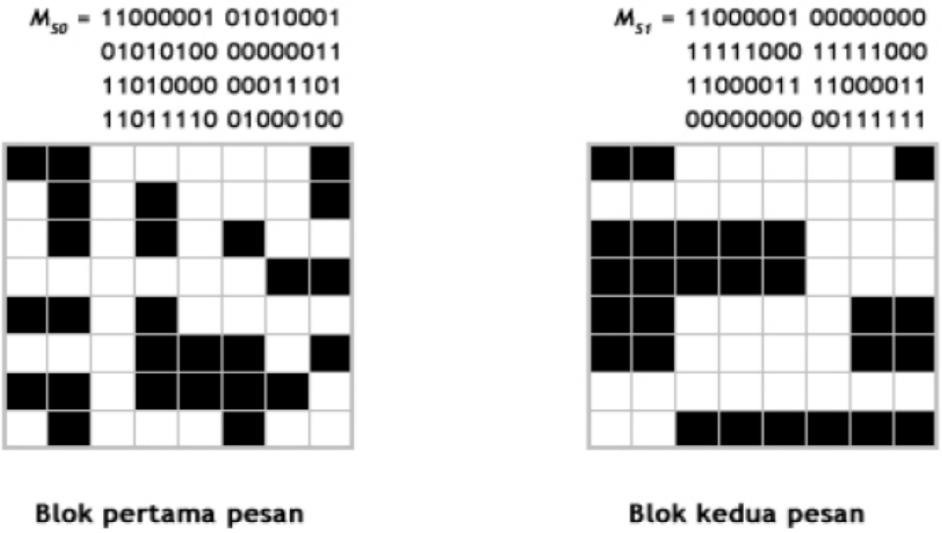
Pada *bit-plane* tersebut dihitung nilai kompleksitasnya. Jumlah pergantian warna hitam-putih pada *bit-plane* 0 adalah sebanyak 47 kali. Jumlah maksimum perubahan warna pada gambar biner dengan ukuran 8×8 adalah 112 kali, sehingga nilai k = 47 dan $2 \times 2^n \times (2^n - 1) = 112$. Melalui persamaan 2.9 didapatkan nilai kompleksitas dari *bit-plane* 0 tersebut, yaitu $\alpha = 0{,}42$.

Dengan menggunakan nilai *threshold* $\alpha_0 = 0{,}3$ maka *bit-plane* 0 dikategorikan sebagai *noise-like region* sehingga dilakukan penyisipan di dalamnya. Jika $\alpha < \alpha_0$, maka tidak dilakukan penyisipan karena segmen tersebut merupakan *informative region*. Selanjutnya bit pesan rahasia dibagi menjadi segmen-segmen yang masing-masing berukuran 64 bit. Jika bit pesan rahasia tersebut adalah M_S maka blok pertama pesan rahasia adalah M_{S0} dan blok berikutnya adalah M_{S1}.

M_S = 11000001010100010101010000000011
11010000000111011101111001000100
11000001000000001111100011111000
11000011110000110000000000111111

M_{S0} = 11000001010100010101010000000011
11010000000111011101111001000100
M_{S1} = 11000001000000001111100011111000
11000011110000110000000000111111

Representasi blok pesan dalam gambar biner dapat dilihat pada Gambar 2.10. Blok pesan M_{S0} akan disisipkan pada blok gambar yaitu *bit-plane* 0 (karena tergolong *noise-like region*), dan blok M_{S1} akan disisipkan pada *bit-plane* berikutnya yang tergolong *noise-like region* juga.



Gambar 2.10 Representasi Blok Pesan dalam Gambar Biner (Sumber: Penyembunyian Pesan Pada Citra Terkompresi dengan Metode *Bit-Plane Complexity Segmentation* (BPCS) dan Teknik Permutasi Blok)

Sebelum melakukan penyisipan, gambar biner yang merupakan representasi blok pesan tersebut dihitung nilai kompleksitasnya terlebih dahulu. Pada blok pesan pertama (M_{S0}), jumlah perubahan warna adalah 54 kali, sehingga dengan persamaan 2.9 diperoleh $\alpha\ M_{S0} = 0{,}48$. Karena blok pesan ini memiliki kompleksitas $\alpha\ M_{S0} > \alpha_0$, maka blok *bit-plane* pada citra diganti oleh 64 bit pesan ini.

Pada blok kedua pesan rahasia, jumlah perubahan warna 32, sehingga didapatkan nilai $\alpha\ M_{S1} = 0{,}29$. Nilai kompleksitas $\alpha\ M_{S1} < \alpha_0$ menunjukkan bahwa blok kedua pesan tidak cukup kompleks untuk disisipkan, karena itu blok pesan tersebut harus dikonjugasi terlebih dahulu. Matriks konjugasi ditulis sebagai berikut:

$$W_C = \begin{bmatrix} 1\,0\,1\,0\,1\,0\,1\,0 \\ 0\,1\,0\,1\,0\,1\,0\,1 \\ 1\,0\,1\,0\,1\,0\,1\,0 \\ 0\,1\,0\,1\,0\,1\,0\,1 \\ 1\,0\,1\,0\,1\,0\,1\,0 \\ 0\,1\,0\,1\,0\,1\,0\,1 \\ 1\,0\,1\,0\,1\,0\,1\,0 \\ 0\,1\,0\,1\,0\,1\,0\,1 \end{bmatrix}$$

Hasil konjugasi yaitu α M_{S1}* akan memiliki kompleksitas 0,71 menurut persamaan 2.13. Hasil konjugasi inilah yang kemudian disisipkan pada *noise-like region* pada citra digital.

Saat proses ekstraksi pesan, yang perlu dilakukan hanyalah mengambil segmen bit yang memiliki kompleksitas diatas *threshold*. Jika nilai kompleksitas segmen tersebut lebih besar dari *threshold*, maka segmen tersebut merupakan bagian dari pesan rahasia.

2.5 *Peak Signal-to-Noise Ratio* (PSNR)

Peningkatan citra atau peningkatan kualitas visual dari citra digital dapat bersifat subjektif. Dapat dikatakan bahwa satu metode memberikan kualitas gambar yang lebih baik dapat bervariasi dari orang ke orang. Untuk alasan ini, perlu untuk menetapkan langkah-langkah kuantitatif atau empiris untuk membandingkan efek dari algoritma peningkatan gambar pada kualitas gambar.

Peak Signal-to-Noise Ratio (PSNR) merupakan contoh parameter yang biasa digunakan sebagai indikator untuk mengukur kemiripan dua buah citra. Parameter tersebut sering digunakan untuk membandingkan hasil pengolahan citra dengan citra awal atau citra asli (Pamungkas, 2017). *Peak Signal-to-Noise Ratio* (PSNR) sering dinyatakan dalam skala logaritmik dalam desibel (dB). Nilai *Peak Signal-to-Noise Ratio* (PSNR) jatuh dibawah 30 dB mengindikasikan kualitas yang relatif rendah, dimana distorsi yang dikarenakan penyisipan terlihat jelas. Akan tetapi kualitas citra stego yang tinggi berada pada nilai 40 dB dan diatasnya (Ketutrare, 2014). Nilai *Peak Signal-to-Noise Ratio* (PSNR) yang lebih tinggi pasti akan menghasilkan akurasi yang lebih baik, akan tetapi meningkatkan citra ke kualitas terbaik akan menguras sumber daya dan beban komputasi yang tinggi (Sajati, 2018). Persamaan yang digunakan untuk menghitung parameter tersebut adalah sebagai berikut:

$$PSNR = 10 \cdot log_{10}\left(\frac{MAX_I^2}{MSE}\right) \quad (2.16)$$

Dimana MAX_I = nilai piksel maksimum pada citra asli dan MSE = *Mean Squared Error*.

2.6 *Mean Squared Error* (MSE)

Mean Squared Error (MSE) merupakan rata-rata kuadrat nilai kesalahan antara citra asli dengan hasil kompresi (Munandar dkk, 2011). Dengan kata lain *Mean Squared Error* (MSE) adalah kesalahan kuadrat rata-rata sinyal piksel citra hasil pemrosesan sinyal terhadap sinyal asli (Doo dkk, 2019). Secara matematis dapat dituliskan sebagai berikut:

$$MSE = \frac{1}{mn}\sum_{x=0}^{m-1}\sum_{y=0}^{n-1}\left|\left(f(x,y) - g(x,y)\right)^2\right| \quad (2.17)$$

Dimana x dan y adalah koordinat dari gambar, m dan n adalah dimensi dari gambar, $f(x,y)$ adalah citra stego dan $g(x,y)$ adalah citra *cover*. Semakin mirip kedua citra maka nilai *Mean Squared Error* (MSE) semakin mendekati nilai nol (Pamungkas, 2017).