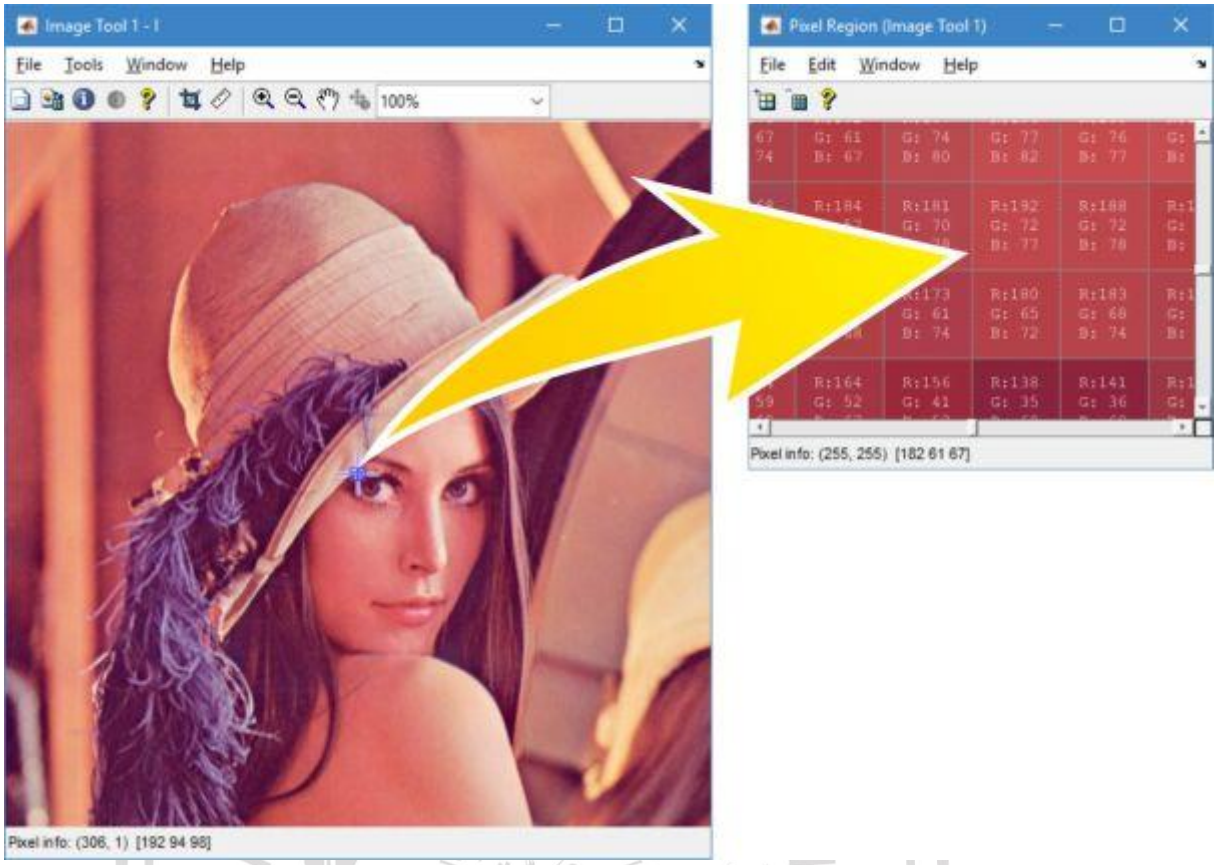
# BAB II
# LANDASAN TEORI

## 2.1. Citra Digital

Bidang studi pengolahan citra digital mengkaji tentang pengolahan, analisis, dan pembentukan citra digital agar dapat menghasilkan informasi yang dapat dimengerti oleh manusia. Sebelum mempelajari lebih lanjut mengenai pengolahan citra digital, penting untuk memahami definisi dari citra itu sendiri. Citra adalah representasi intensitas cahaya dalam bidang dua dimensi, yang dapat diklasifikasikan menjadi dua jenis berdasarkan bentuk sinyal penyusunnya, yaitu citra analog dan digital. Gambar yang bersifat analog dibentuk oleh sinyal analog yang kontinu, sementara gambar digital dibentuk oleh sinyal diskrit yang terdiri dari angka-angka.

Sinyal analog yang diterjemahkan oleh alat akuisisi gambar seperti mata manusia dan kamera analog menghasilkan gambar analog. Gambar analog dapat ditemukan dalam berbagai bentuk, seperti gambar yang dilihat oleh mata manusia dan gambar yang diambil menggunakan kamera analog seperti foto atau film. Meskipun gambar analog memiliki resolusi yang tinggi dan detail yang baik, gambar ini memiliki kelemahan karena tidak dapat disimpan, diproses, dan diduplikasi di komputer.

Dalam citra digital, intensitas cahaya direpresentasikan secara diskrit pada bidang dua dimensi. Citra terdiri dari sejumlah piksel atau elemen citra, masing-masing dengan koordinat (x,y) dan nilai amplitudo f(x,y) yang merepresentasikan intensitas warna. Gambar 2.1 yang tertera di bawah ini menunjukkan cara representasi citra digital beserta piksel-piksel penyusunnya.




**Gambar 2.1. Citra dan piksel penyusunnya**

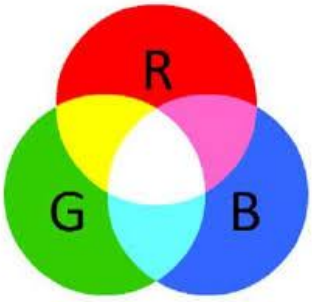
Kategori-kategori utama gambar adalah RGB, grayscale, dan biner, dan setiap piksel pada gambar mempunyai kombinasi warna yang berbeda-beda. Pada Gambar 2.1, jenis gambar yang digunakan adalah gambar RGB truecolor 24-bit, yang terdiri dari tiga warna dasar yaitu merah, hijau, dan biru. Setiap kanal warna memiliki nilai intensitas piksel dengan kedalaman 8-bit, sehingga memiliki variasi warna sebanyak 2^8 derajat warna (dari 0 hingga 255).

Nilai 255 merepresentasikan warna merah yang paling intens pada kanal merah, sedangkan nilai 0 merepresentasikan warna hitam pada kanal tersebut. Demikian pula pada kanal hijau, nilai 255 merepresentasikan warna hijau yang paling intens, sementara nilai 0 merepresentasikan warna hitam. Hal yang sama berlaku pada kanal biru, di mana nilai 255 merepresentasikan warna biru yang paling intens, sedangkan nilai 0 merepresentasikan warna hitam.

### 2.1.1. Citra RGB

RGB dikenal sebagai warna aditif karena warna tersebut dihasilkan dari cahaya. Beberapa perangkat yang menggunakan warna RGB meliputi mata manusia, proyektor, TV, kamera video, kamera digital, dan perangkat-perangkat yang menghasilkan cahaya. Warna RGB diciptakan dengan mencampurkan tiga warna dan mengatur intensitas masing-masing warna dengan skala 0 hingga 255.

Apabila intensitas warna Merah (Red) sebesar 255, serta intensitas warna Hijau (Green) dan Biru (Blue) juga sama besar, maka warna yang dihasilkan adalah Putih. Namun, jika intensitas ketiga warna tersebut bernilai 0, maka warna yang dihasilkan adalah Hitam, seperti saat berada di dalam ruangan gelap yang tidak ada cahaya. Sebagai contoh, ketika menonton film di bioskop lama yang menggunakan proyektor tiga warna dengan lubang terpisah, cahaya yang dipancarkan dari proyektor dapat berkurang ketika film menunjukkan adegan yang mengambil tempat di ruangan gelap. [Novi. DE. 2012].




**Gambar 2.2** Warna RGB

### 2.1.2 Citra Gray

Citra grayscale adalah sebuah citra digital yang terdiri dari piksel-piksel dengan satu saluran nilai saja, yang terdiri atas nilai RED, GREEN, dan BLUE, dan digunakan untuk mengindikasikan tingkat intensitas. Citra tersebut hanya memiliki tiga warna, yakni hitam, abu-abu, dan putih. Warna abu-abu sendiri terdiri atas beragam tingkat kegelapan, mulai dari hitam hingga mendekati putih. Dalam citra grayscale tersebut, terdapat 256 kombinasi warna abu-abu yang tersedia, dengan kedalaman warna 8 bit.

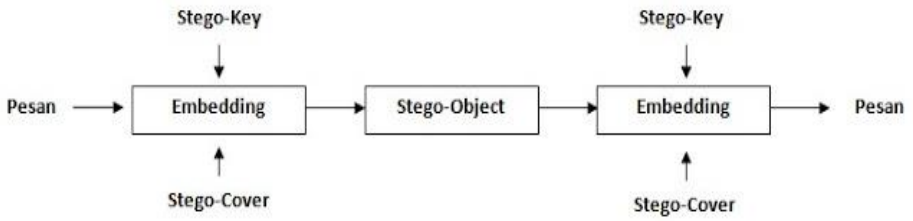
**Gambar 2.3.** Citra Grayscale

## 2.2. Steganografi

### 2.2.1. Konsep Steganografi

Steganografi adalah ilmu untuk menyembunyikan komunikasi. Sebuah sistem perekaman kriptografi menyembunyikan isi data dalam jangkauan komunikasi yang tidak terdeteksi oleh rata-rata orang agar tidak menimbulkan kecurigaan di antara mereka yang melihatnya, Ilustrasi pada Gambar 2.4 menggambarkan konsep misteri yang diterapkan pada zaman dahulu dengan menggunakan tato tersembunyi atau tinta tak terlihat sebagai bentuk steganografi untuk menyampaikan pesan secara rahasia. Namun, teknologi komputer dan jaringan saat ini telah menyediakan media komunikasi jaringan yang mudah digunakan untuk merekam kriptografi.

Langkah pertama dalam menerapkan sistem steganografi adalah mencari media yang memiliki bit yang tersedia yang dapat dimodifikasi tanpa merusak media tersebut. Selanjutnya, informasi yang ingin disembunyikan akan disisipkan dengan mengganti bit-bit yang tersedia dengan data pesan yang ingin disimpan secara rahasia, sehingga menghasilkan sebuah media yang disebut stego. Langkah-langkah ini diilustrasikan pada Gambar 2.4.




Gambar 2.4. Ilustrasi Dasar Steganografi

### 2.2.2 Sejarah Penggunaan Steganografi

Steganografi telah digunakan sebagai alat dalam berbagai kepentingan seperti politik, militer, diplomatik, dan pribadi selama 2.500 tahun. Sejarawan Yunani, Herodotus, mencatat penggunaan steganografi yang dicetak pertama kali. Ia mengirimkan pesan rahasia melalui media kepala budak atau tentara. Caranya adalah dengan menuliskan pesan pada kepala budak yang botak, lalu membiarkan rambut tumbuh kembali sehingga pesan tersembunyi di balik rambut yang tumbuh tersebut dan dapat dibawa oleh budak tersebut.

Steganografi telah digunakan sejak zaman Romawi Kuno, yaitu dengan cara menulis pesan rahasia menggunakan tinta tak kasat mata (invisible ink). Campuran serat buah, susu, dan cuka digunakan untuk membuat tinta yang tidak terlihat ketika digunakan untuk menulis. Namun, tulisan yang ditulis dengan tinta tersebut dapat dibaca dengan memanaskan kertas di atas sumber panas. Dengan cara ini, pesan rahasia dapat disembunyikan dalam tulisan yang tampak seperti kosong di atas kertas.

Serangan teroris pada 11 September 2001 di Amerika Serikat telah meningkatkan popularitas steganografi di era modern. Pada waktu itu, para pelaku teroris menggunakan metode tersebut untuk menyembunyikan pesan teror dalam berbagai jenis media seperti gambar, audio, dan video. Dalam kasus tersebut, para pelaku teroris berhasil menyembunyikan peta, foto target, dan perintah untuk aktifitas teroris lainnya. Dengan memanfaatkan teknik steganografi, pesan rahasia dapat disembunyikan dalam media yang terlihat seperti biasa sehingga sulit dideteksi oleh pihak yang tidak berwenang.

### 2.2.3 Kriteria dan Aspek dalam Steganografi

Proses penyisipan data rahasia ke media digital dapat memengaruhi kualitas media tersebut. Beberapa faktor yang perlu dipertimbangkan dalam proses penyisipan data antara lain:

1. **Fidelity**. Kualitas gambar wadah tidak banyak berubah. Setelah menambahkan data yang dirahasiakan, gambar kriptografi masih terlihat sanhgat bagus.

Pengamat tidak dapat mengetahui bahwa pada gambar tersebut terdapat data yang tealah rahasiakan.

2. **Robustness**. Data yang dirahasiakan diharuskan bisa bertahan dari manipulasi yang dilakukan kepada gambar wadah (seperti mengubah kontras, mempertajam, kompresi, menambahkan noise, memperbesar gambar, memotong, mengkodekan, dan sebagainya.). Jika operasi pemrosesan gambar dilakukan pada gambar, data tertutup tidak rusak.
3. **Recovery**. Harapannya data yang tersembunyi dapat dipulihkan kembali, mengingat tujuan dari steganografi adalah untuk menyembunyikan data. Oleh karena itu, data gambar yang berperan sebagai tempat penyimpanan rahasia harus bisa diambil kembali untuk digunakan di waktu yang akan datang. Terdapat tiga aspek pada steganografi yang dapat menentukan apakah steganografi tersebut berhasil atau tidak dalam menyelesaikan tugasnya. (Ermadi dkk, 2004), yaitu:

1. **Kapasitas (capacity)**. Kapasitas merujuk pada seberapa banyak informasi yang dapat disembunyikan dalam media yang digunakan. Kerahasiaan merujuk pada kemampuan pembaca untuk tidak dapat mendeteksi pesan yang tersembunyi, sedangkan ketahanan merujuk pada jumlah revisi yang dapat dilakukan pada media stego sebelum pesan rahasia yang disembunyikan menjadi tidak dapat dipulihkan akibat upaya musuh untuk menghancurkannya.
2. **Keamanan (security).** Dalam sistem steganografi tradisional/*classic*, keamanan sistem tergantung pada kerahasiaan enkripsi yang digunakan. Secara teori, informasi dapat membantu kita untuk lebih akurat dalam menentukan arti dari suatu sistem yang aman.
3. **Ketahanan (robustness)**. Stabilitas mengacu pada data gambar penampang (misalnya, mengubah kontras, mempertajam, memutar, memperbesar, memotong dan sebagainya.). Ketika operasi pemrosesan gambar dilakukan pada gambar, data yang tersembunyi tidak rusak.

### 2.2.4 Jenis – Jenis Teknik Steganografi

Terdapat tujuh jenis teknik steganografi yang dibedakan berdasarkan teknik yang digunakan, seperti berikut Ariyus (2009):

1. ***Injection***. Secara umum, *Injection* atau *embedding* adalah suatu teknik dimana kita menyisipkan sebuah pesan rahasia ke dalam suatu media tempat wadah. Namun, Istilah embedding seringkali digunakan untuk menyebut teknik yang memiliki kelemahan, yaitu menyebabkan ukuran media yang diinjeksi menjadi lebih besar daripada ukuran aslinya sehingga mudah terdeteksi.
2. **Substitusi**. Pada umumnya, teknik ini mengganti informasi standar dengan informasi rahasia. Dalam kebanyakan kasus, teknik ini tidak akan mengubah ukuran data asli secara signifikan, tergantung pada jenis media dan data yang ingin disembunyikan, teknik substitusi yang digunakan untuk menyembunyikan informasi tersebut dapat menurunkan kualitas dari media yang telah didistribusikan.
3. **Transformasi Domain**. Transformasi domain merupakan teknik yang sangat efektif untuk menyembunyikan data. Pada dasarnya, teknik ini menyembunyikan data pada ruang transformasi sehingga pesan rahasia tidak terlihat pada tampilan asli. Dengan menggunakan teknik ini, informasi dapat disembunyikan dengan lebih baik tanpa mempengaruhi kualitas visual dari media yang digunakan.
4. ***Spread Spectrum***. Teknik *Spread Spectrum transmission* memanfaatkan kode *pseudo-noise* sebagai bentuk modulasi gelombang untuk menyebarkan energi sinyal melalui jalur komunikasi yang memiliki *bandwidth* lebih besar daripada jalur komunikasi sinyal. Walaupun kode *pseudo-noise* tidak bergantung pada data informasi, penerima masih mampu memulihkan sinyal dengan mengikuti kode *pseudo-noise* yang disinkronkan. Dengan menggunakan teknik ini, sinyal dapat dikirim melalui jalur komunikasi yang lebih aman dan efisien.
5. **Statistical Method**. Teknik tersebut dikenal sebagai steganografi pola 1-bit. Teknik ini memungkinkan untuk menyisipkan satu bit informasi ke dalam media penyimpanan dan mengubah statistik meskipun hanya satu bit. Setiap perubahan statistik diwakili oleh angka 1 dan tidak ada perubahan yang

dianggap sebagai 0. Sistem ini bekerja berdasarkan kemampuan penerima untuk membedakan antara data yang telah diubah dan yang tidak diubah. Dengan teknik ini, pesan rahasia dapat disembunyikan dalam media dengan cara yang hampir tidak terlihat.

6. **Distortion**. Metode ini mencakup perubahan pada objek yang digunakan untuk menyimpan informasi rahasia. Dalam prosesnya, objek tersebut dimodifikasi atau dimanipulasi dengan tujuan menyembunyikan pesan rahasia. Teknik ini dapat digunakan pada berbagai objek, termasuk teks, gambar, audio, atau video, dan tergantung pada objek yang digunakan, perubahan dapat dilakukan dengan berbagai cara. Namun, tujuannya tetap sama, yaitu menyembunyikan informasi rahasia dengan cara yang tidak terlihat.
7. **Cover Generation**. Berbeda dengan metode steganografi lainnya, metode ini memiliki keunikan tersendiri, objek penutup dipilih dengan sengaja untuk menyembunyikan pesan rahasia. Dalam metode ini, objek penutup, seperti gambar atau audio, dihasilkan secara khusus dan digunakan untuk menyembunyikan pesan rahasia. Dalam prosesnya, pesan rahasia disisipkan ke dalam objek penutup tanpa mengubah tampilan atau kualitas objek penutup tersebut secara signifikan. Dengan demikian, metode ini memungkinkan untuk menyembunyikan pesan rahasia secara efektif dan aman dalam objek penutup yang telah dirancang khusus untuk tujuan tersebut.

## 2.3 *Least Significant Bit* (LSB)

Menggunakan teknik least significant bit (LSB) dalam steganografi adalah cara yang mudah untuk menyembunyikan informasi rahasia di dalam gambar digital atau media lainnya. Dalam metode ini, bit-bit terakhir dari setiap byte dalam media penutup digunakan untuk menyimpan pesan rahasia. Teknik ini memungkinkan untuk menyisipkan pesan rahasia secara efisien tanpa mengganggu tampilan atau kualitas media penutup.

Namun, jika media penutup diubah dari format GIF atau BMP yang menggunakan kompresi tanpa kehilangan (lossless) menjadi format JPEG yang menggunakan kompresi dengan kehilangan (lossy), maka pesan rahasia yang

disisipkan menggunakan metode LSB dapat hilang atau rusak. Hal ini terjadi karena kompresi JPEG menghilangkan informasi yang dianggap tidak penting, termasuk bit-bit terakhir yang digunakan dalam metode LSB. Oleh karena itu, jika media penutup diubah kembali ke format aslinya, pesan rahasia tidak dapat direkonstruksi dengan sempurna karena bit-bit terakhir yang digunakan dalam metode LSB telah hilang. (Finna dan Entik, 2016).

Teknik penyembunyian data dengan mengganti bit data berperforma rendah dengan bit data rahasia di dalam segmen gambar disebut teknik least significant bit (LSB). Dalam teknik ini, bit-bit yang digunakan untuk menyimpan pesan rahasia adalah bit-bit yang paling tidak signifikan (LSB) sehingga tidak mempengaruhi kualitas visual gambar secara signifikan. Namun, pesan rahasia dapat dengan mudah terganggu atau dihapus oleh manipulasi pada gambar tersebut, sehingga teknik ini perlu digunakan dengan hati-hati dan dilengkapi dengan teknik pengamanan tambahan untuk memastikan keamanan pesan rahasia. Berikut adalah contoh susunan bit dalam satu byte:

MSB = **1**1010010 = LSB

Dalam teknik penyembunyian data menggunakan bit LSB, bit yang tepat untuk diganti adalah bit LSB karena perubahan pada bit tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Biasanya, byte yang digunakan untuk menyimpan pesan rahasia adalah byte yang mewakili warna merah pada citra digital. Mengubah satu bit pada byte tersebut tidak secara signifikan memengaruhi nilai warna merah dan sulit terdeteksi oleh mata manusia. Oleh karena itu, teknik ini cukup populer digunakan dalam steganografi. (Andra,2008).

Metode Least Significant Bit (LSB) yang digunakan pada aplikasi tersebut adalah teknik steganografi yang melakukan penyisipan pesan rahasia dengan cara mengubah bit terakhir dari satu byte data. Teknik ini memilih bit LSB karena perubahan pada bit tersebut hanya akan mengubah nilai byte satu lebih atau kurang dari nilai sebelumnya, sehingga tidak secara signifikan memengaruhi nilai asli dari data yang sedang disembunyikan. Dalam aplikasi tersebut, bit yang akan diganti pada setiap byte data adalah bit LSB. Dengan menggunakan teknik ini, pesan

rahasia dapat disembunyikan dalam citra digital tanpa terdeteksi oleh mata manusia. (Darmayanti dan Awang,2016).

Sebuah citra terdiri dari piksel-piksel yang membentuk gambar. Dalam citra berwarna 24-bit, setiap piksel terdiri dari 3 byte, masing-masing merepresentasikan warna merah, hijau, dan biru (RGB). Contohnya, jika terdapat 2 piksel dalam citra tersebut, maka intensitas setiap warna pada setiap piksel dapat dikonversi ke bentuk biner sebagai berikut :

(00100111 11101001 11001000)
(00100111 11001000 11101001)

Jika kita ingin menyisipkan karakter "C" dengan bilangan biner 01000011 kedalam 2 pixel citra warna tersebut menggunakan teknik LSB, maka setiap 2 bit dari pesan tersebut dimulai dari MSB akan disisipkan ke dalam 2 bit LSB dari setiap byte citra warna, dimulai dari byte pertama ke byte ketiga, dan seterusnya sebagai berikut:

(00100101 11101000 11001000)
(00100111 11001000 11101001)

## 2.4 *Matlab (Matrix Laboratory)*

Matlab merupakan sebuah aplikasi perangkat lunak yang didesain khusus untuk mempermudah pemrograman dan visualisasi dalam menyelesaikan berbagai masalah teknis. Penggunaan Matlab mencakup berbagai bidang, antara lain matematika, ilmu komputer, rekayasa, fisika, kimia, biologi, dan keuangan. Dalam matematika, Matlab digunakan untuk melakukan perhitungan numerik, analisis data, dan simulasi model matematika. Ilmu komputer menggunakan Matlab untuk pengembangan perangkat lunak, pengolahan citra, dan pengenalan suara. Bidang rekayasa menggunakan Matlab untuk analisis struktur, pengendalian sistem, dan optimasi desain. Dalam fisika, Matlab digunakan untuk memodelkan fenomena alam, mengolah data, dan menguji teori. Kimia menggunakan Matlab untuk

simulasi dan peramalan perilaku molekul dan reaksi kimia. Dalam biologi, Matlab digunakan untuk analisis data genomik, perancangan obat, dan pengolahan citra medis. Di bidang keuangan, Matlab digunakan untuk analisis pasar saham, manajemen risiko, dan pengembangan produk keuangan.

Matlab memiliki fitur yang dikembangkan yang dikenal sebagai toolkit atau kotak peralatan. Kotak peralatan ini terdiri dari berbagai fungsi Matlab (file M) yang telah dikembangkan di lingkungan Matlab untuk memecahkan masalah. Saat ini, terdapat banyak area yang dapat diatasi menggunakan kotak peralatan ini, seperti pemrosesan sinyal, sistem kontrol, jaringan saraf, logika fuzzy, wavelet, dan masih banyak lagi.