BAB II

TINJAUAN PUSTAKA

2.1. Tinjauan Pustaka

Penelitian tentang implementasi Steganografi pada file video sudah bukan lagi untuk yang pertama kalinya. Pada penelitian sebelumnya yang sudah dilakukan menunjukkan bahwa implementasi Steganografi pada file video dapat dilakukan dengan berbagai metode. Berikut merupakan beberapa penelitian yang terdahulu:

2.1.1. Implementasi Steganografi Video dengan menggunakan Metode Egypt, *Least Significant Bit* (LSB) dan *Least Significant Bit* (LSB) Fibonacci Edge Pixel

Pada penelitian ini menggunakan 3 metode yaitu metode Egypt, *Least Significant Bit* (LSB) dan *Least Significant Bit* (LSB) Fibonacci Edge Pixel untuk membandingkan diantara 3 metode tersebut, untuk membuktikan metode mana yang paling optimal untuk digunakan dalam analisis video steganografi. Analisis video steganografi ini bertujuan untuk mendeteksi video yang mengandung unsur pesan rahasia yang kemungkinan untuk pengintaian. Dalam proses steganografi pada file video didapatkan hasil dari data video steganografi yaitu PSNR, similarity, decode time, encode time dan different size. Hasil PSNR yang didapat dari penelitian ini rata-rata 40.46 GB dan menghasilkan rata-rata presentase similarity 30.67%. Rata-rata pada MSE untuk penelitian ini yaitu sebesar 0.50657. Kemudian hasil dari percobaan metode Egypt, LSB dan LSB Fibonacci terbukti menghasilkan PNSR lebih kecil dan metode yang paling optimal yang digunakan untuk video steganografi adalah metode Egypt dengan hasil similarity mencapai 100% dan rata-rata PSNR yaitu 43.67 GB.[5]

2.1.2. Analisa Perbandingan *Least Significant Bit* dan *End Of File* untuk Steganografi Citra Digital Menggunakan Matlab

Pada penelitian ini menganalisa perbandingan antara dua metode yaitu *Least Significant Bit* (LSB) dan *End Of File* (EOF) untuk

Steganografi pada citra digital. Dalam penelitian ini menjelaskan proses penyembunyian pesan rahasia ke dalam citra digital berdasarkan 2 metode yaitu LSB dan EOF serta melakukan perbandingan terhadap kualitas citra output dari masing masing metode tersebut, sehingga dapat mengetahui metode yang lebih efisien dan efektif dalam menyembunyikan pesan rahasia terutama terhadap kualitas dan size citra yang dihasilkan. Hasil yang diperoleh dari penelitian ini terdapat beberapa aspek yang diketahui yaitu proses penyisipan pesan pada metode LSB dan EOF memiliki perbedaan, dimana metode LSB pada penyisipan bit pesan menggantikan bit terakhir dari citra cover, sedangkan metode EOF pada penyisipan pesan di tempatkan pada piksel yang baru di citra cover. Kemudian dari segi keunggulan lebih banyak didapatkan pada metode LSB dibandingkan dengan metode EOF karena tidak terlalu berpengaruh pada kualitas citra sehingga tidak tampak diketahui oleh mata manusia, sedangkan pada metode EOF mengalami perubahan yang signifikan pada kualitas citra. Adapun hasil dari perbandingan 2 metode tersebut pada output atau tampilan cita setelah penyisipan pesan teknik yang lebih baik adalah metode LSB, karena citra akhir tidak diperlihatkan perbedaan secara signifikan oleh penghilatan mata manusika jika dibandingkan dengan citra yang awal.[6]

2.1.3. Steganografi Video Digital dengan Algoritma LSB (*Least Signifikan Bit*) dan Rijndael

Penelitian ini menggunakan 2 metode yaitu metode *Least Signifikan Bit* (LSB) dan Rijndael. Metode Rijndael digunakan untuk enkripsi pesan pada salah satu frame video saat disisipkan. Penyisipan pesan pada frame video menggunakan 8 metode LSB, Ekstraksi frame pada video menggunakan software ffmpeg. Penelitian ini juga menggunakan pengujian kualitatif dimana untuk melihat perubahan frame video dengan indera manusia, sedangkan pengujian kuantitatif dilakukan untuk menguji 6 video dengan resolusi yang berbeda dan pesan yang disisipkan ada 5 pesan dengan panjang Byte yang bervariasi. Dari hasil

pengujian ini akan menunjukan perbandingan dari 2 metode tersebut yang mana metode LSB dan Rijndael tidak dapat menyisipkan pesan dengan ukuran Byte-nya lebih besar dari daya tampung video cover. Perubahan kualitas citra terjadi apabila ukuran Byte pesan yang disisipkan semakin besar.[7]

2.1.4. Implementasi Steganografi Pesan Text Ke Dalam File Sound (.Wav) Dengan Modifikasi Jarak Byte Pada Algortma *Least Significant Bit* (LSB)

Penulis menggunakan Steganografi dengan modifikasi dari metode *Least Significant Bit* (LSB) sebagai media untuk menyembunyikan informasi berupa setiap nilai-nilai bit data ke dalam nilai-nilai bit media audio. Bit-bit data yang akan disembunyikan atau diamankan menggunakan LSB ke dalam media audio. Dari hasil analisis dan implementasi dapat diperoleh bahwa nilai-nilai bit yang disisipkan ke dalam media audio masih tampak seperti normal sehingga tidak menimbulkan kecurigaan bagi orang yang mendengar. Kemudian jika di ekstrak maka akan di dapat kembali nilai-nilai bit yang telah disisipkan sebelumnya secara utuh, maka akan terpenuhi kriteria-kriteria Steganografi yang baik yaitu *imperceptibility, fidelity,* dan *recovery.* Berdasarkan hasil dari penelitian ini bahwa Steganografi data berupa pesan text atau informasi data ke dalam media audio dapat diimplementasikan menggunakan metode *Least Significant Bit* (LSB) yaitu dengan mengkonversi setiap nilai-nilai bit data ke dalam nilai-nilai bit media audio, pada ukuran dari daya tampung media audio tidak dapat mempengaruhi seberapa besar jumlah data yang dapat disembunyikan. Ukuran pada media audio harus lebih besar dari jumlah data yang akan disembunyikan. Perubahan yang terjadi pada Steganografi tidak signifikan dan masih tampak seperti audio normal, karena bit yang disisipkan tidak mempengaruhi pada media audio. Karena byte yang dipake adalah byte yang terendah.[8]

2.1.5. Teknik penyembunyian dan Enkripsi pesan pada Citra Digital dengan kombinasi Metode LSB dan RSA

Pada penelitian ini menggunakan teknik Steganografi dan Kriptografi dengan metode LSB dan RSA. RSA merupakan teknik Kriptografi yang populer dapat diterapkan pada citra digital. Nilai piksel pada citra digital hanya berkisar 0 sampai 255, hal ini membuat kunci yang digunakan pada RSA cukup terbatas sehingga kurang aman. Dalam penelitian ini mengkonversi nilai piksel citra menjadi 16-bit sehingga kunci yang digunakan dapat lebih bervariasi. Hasil dari analisis ini dapat diketahui melalui perhitungan PSNR dan MSE. Berdasarkan hasil dari penelitian menunjukkan bahwa penggunaan RSA 16-bit pada penyandian citra pesan dapat meningkatkan keamanan, karena nilai *p* dan *q* dapat lebih bervariasi. Dengan variasi yang semakin banyak, maka enkripsi RSA dapat lebih aman. Metode ini juga digabungkan dengan metode LSB sehingga keamanan pesan dapat meningkat. Teknik ini terbukti bahwa tahan terhadap serangan *salt* and *paper* yaitu dengan hasil PSNR 57.2258dB, MSE 0.1232dB dan CC 1.0000. Dari hasil tersebut menunjukkan metode ini mampu melindungi dan mengamankan citra pesan *grayscale* dari pencurian pesan.[9]

Tabel 1.1 Tinjauan Pustaka

No	Judul	Perbandingan	Kontras	Mengkritik	Mempersatukan	Kesimpulan
1.	Implementasi Steganografi Video dengan menggunakan Metode Egypt, *Least Significant Bit* (LSB), dan *Least Significant Bit* (LSB) Fibonacci Edge Pixel	Pada penelitian ini menggunakan metode Egypt, LSB, dan LSB Fibonacci Edge Pixel. Dari ketiga metode tersebut diuji melalui perhitungan PSNR, MSE dan rata-rata presentase similarity, dimana perhitungan tersebut untuk mengetahui kinerja dari ketiga metode tersebut yang digunakan sebagai analisis video Steganografi. Analisis video Steganografi bertujuan untuk mendeteksi video yang mengandung	Penelitian ini melakukan pengujian dari ketiga metode tersebut menggunakan perhitungan PSNR dan MSE untuk mengetahui kinerja dari 3 metode tersebut yang optimal sebagai analisis pada Video Steganografi.	Pada bagian hasil dan pembahasan dijelaskan bahwa terdapat 6 video yang akan diuji, namun di dalam tabel pada perhitungan PSNR dan MSE hanya 3 video saja yang dimasukan.	Penelitian ini melakukan analisis terhadap video yang menggunakan metode Egypt, *Least Significant Bit* (LSB), dan *Least Significant Bit* (LSB) Fibonacci Edge Pixel. Dalam analisis tersebut bertujuan untuk mengetahui kinerja dari 3 metode tersebut yang digunakan sebagai proses penyisipan pesan rahasia ke dalam	Berdasarkan hasil penelitian yang telah dilakukan bahwa perhitungan PSNR dan MSE dari 3 metode tersebut membuktikan bahwa metode yang optimal yaitu metode Egypt dengan rata-rata PSNR 43.67 dB dan hasil similarity mencapai 100%.

		unsur pesan rahasia yang kemungkinan untuk pengintaian.			video melalui perhitungan MSE dan PSNR pada citra.	
2.	Analisa Perbandingan *Least Significant Bit* dan *End Of File* untuk Steganografi Citra digital menggunakan matlab	Penelitian ini melakukan perbandingan metode LSB dan EOF pada citra gambar. Hasil dari perbandingan tersebut dapat mengetahui metode manakah yang lebih optimal pada proses menyembunyikan dan mengeluarkan pesan yang telah disisipkan.	Pada penelitian ini melakukan perbandingan terhadap metode LSB dan EOF pada citra gambar sebagai proses penyembunyian dan mengeluarkan pesan.	Pada tahap pengujian, tabel perhitungan MSE/PSNR pada metode EOF hasilnya sama dengan metode LSB namun tidak dijelaskan secara detail, mengapa hasilnya bisa sama.	Penelitian melakukan analisis perbandingan terhadap metode LSB dan EOF pada citra gambar. Dari hasil perbandingan tersebut dapat disimpulkan metode yang optimal untuk digunakan proses enkripsi dan ekstraksi pesan pada gambar.	Hasil penelitian yang dilakukan dari hasil perbandingan metode LSB dan EOF bahwa metode yang baik pada saat proses penyisipan pesan adalah metode LSB karena mengalami sedikit penurunan pada kualitas citra dibandingkan dengan metode

						EOF.
3.	Steganografi Video Digital dengan Algoritma LSB (*Least Significant Bit*) dan Rijndael	Penelitian ini menggunakan metode LSB dan Rijndael. Metode Rijndael digunakan untuk enkripsi salah satu frame pada video, sedangkan metode LSB digunakan untuk menyisipkan pesan pada frame tersebut. Proses ekstraksi pada frame menggunakan *software* ffmpeg. Pengujian pada penelitian ada 2 kategori yaitu kualitatif dan kuantitatif.	Penelitian ini melakukan pengujian kualitatif dan kuantitatif pada metode LSB dan Rijndael. Kualitatif yaitu melihat perubahan pada frame video dengan indera manusia, sedangkan kuantitatif menguji resolusi video dan pesan yang disisipkan dengan panjang byte yang bervariasi.	Pada tahap pengujian, terdapat 6 video yang diuji kan dengan resolusi yang berbeda, namun hanya 1 video saja yang dijelaskan pada tabel dengan resolusi yang berbeda.	Penelitian melakukan implementasi pada video digital menggunakan metode LSB dan Rijndael. Metode Rijndael digunakan untuk enkripsi salah satu frame pada video, sedangkan LSB untuk menyisipkan pesan pada frame tersebut.	Hasil pengujian pada penelitian ini bahwa metode LSB dan Rijndael tidak bisa digunakan untuk penyisipan pesan dengan ukuran byte yang lebih besar dari daya tampung video cover. Perubahan kualitas citra terjadi jika ukuran byte yang disisipkan semakin besar.

4.	Implementasi Steganografi Pesan Text Ke Dalam File Sound (.Wav) Dengan Modifikasi Jarak Byte Pada Algortma *Least Significant Bit* (LSB)	Peneliti melakukan implementasi terhadap Steganografi dengan modifikasi metode LSB untuk menyembunyikan informasi ke dalam nilai-nilai bit pada media audio.	Penelitian ini focus kepada proses penyisipan pesan ke dalam nilai-nilai bit pada media audio menggunakan metode LSB.	Tidak ada penjelasan terkait pengujian yang dilakukan dari hasil penelitian yang dilakukan.	Penelitian melakukan penyisipan pesan text ke dalam nilai-nilai bit pada media audio. Kemudian bit-bit data yang disembunyikan atau diamankan oleh LSB ke dalam media audio. Hasil dari implementasi yang diperoleh bahwa audio yang disisipkan oleh pesan masih tampak seperti audio normal sehingga tidak menimbulkan kecurigaan oleh orang lain.	Hasil penelitian yang telah dilakukan bahwa Steganografi data berupa pesan text ke dalam media audio dapat diimplementasikan menggunakan metode LSB dengan mengkonversi nilai-nilai bit ke dalam nilai-nilai bit media audio. Perubahan yang terjadi pada Steganografi tidak significant dan

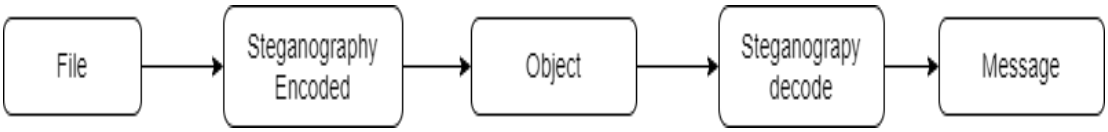
						masih tampak seperti audio normal, karena bit yang mempengaruhi pada audio adalah byte yang terendah
5.	Teknik penyembunyian dan Enkripsi pesan pada Citra Digital dengan kombinasi Metode LSB dan RSA	Pada penelitian ini menggunakan teknik Steganografi dan Kriptografi dengan metode LSB dan RSA. Dalam penelitian ini mengkonversi nilai piksel menjadi 16-bit yang digunakan oleh RSA untuk penyandian pesan serta menggunakan perhitungan PSNR dan MSE untuk mengetahui	Penelitian ini melakukan proses enkripsi pesan pada citra, dengan menggabungkan metode LSB dan RSA sehingga mendapatkan hasil implementasi yang baik.	Pada tahap pengujian, peneliti melakukan komparasi dan implementasi metode steganografi selain dari metode RSA dan LSB tidak sesuai dengan pembahasan yang diusulkan.	Pada penelitian ini melakukan enkripsi pesan pada citra gambar menggunakan teknik Steganografi dan Kriptografi dengan metode LSB dan RSA. Hasil dari penelitian ini menggunakan perhitungan PSNR dan MSE untuk	Berdasarkan hasil penelitian yang dilakukan bahwa menggabungkan metode RSA dan LSB dapat meningkatkan keamanan pesan, terbukti pada perhitungan PSNR 57.2258dB, MSE 0.1232dB CC

		hasil analisis dari penelitian ini.			menentukan hasil analisis yang dilakukan.	1.0000 lebih baik dari penelitian sebelumnya.

2.2. Landasan Teori

2.2.1. Steganografi

Steganografi merupakan teknik untuk menyembunyikan pesan rahasia ke dalam wadah (media) digital sehingga tidak dicurigai oleh pihak lain. Steganografi membutuhkan 2 properti yaitu media penampung dan pesan rahasia yang akan disembunyikan. Kemudian pada Steganografi digital menggunakan media digital sebagai wadah penampung seperti gambar, audio maupun video. Pesan rahasia yang disembunyikan juga berupa gambar, suara, teks ataupun video [10]. Berikut merupakan gambar alur dari rumus Steganografi yang menggambarkan proses penyisipan pesan rahasia ke dalam wadah penampung dan menghasilkan output dari proses penyisipan yang telah dilakukan.



Gambar 2.1 Alur dari Rumus Steganografi

Tujuan dari Steganografi sendiri yaitu berguna untuk menyembunyikan atau merahasiakan sebuah pesan atau informasi agar tidak diketahui oleh orang lain. Dalam prakteknya, kebanyakan pesan yang disembunyikan dengan membuat sedikit perubahan pada digital lain yang isinya tidak menarik namun tidak menarik untuk diperhatikan oleh penyerang potensial, misal nya saja terdapat objek gambar yang tidak terlihat berbahaya, akan tetapi di dalamnya terdapat informasi yang cukup penting.

2.2.2 *Joint Photographic Expert Assemble* (JPEG)

Merupakan jenis data yang dikembangkan oleh Joint Photographic Experts Assemble (JPEG) yang merupakan standar baku untuk para fotografer professional. JPEG adalah format file gambar terkompresi. Ini adalah format

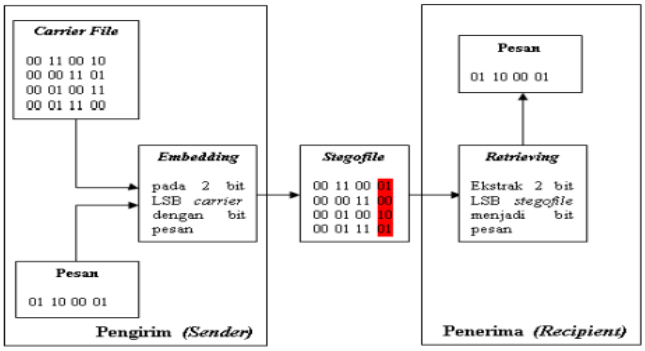
yang sangat populer dan dapat ditemukan berkali-kali dalam kehidupan sehari-hari.[11]

2.2.3 *Portable Network Graphic* (PNG)

Jenis data yang dikembangkan sebagai alternatif lain untuk format GIF, dengan menggunakan paten LZW- algoritma kompresi. PNG merupakan format gambar yang sangat baik untuk tampilan pada grafis internet, karena sudah mendukung transparansi di dalam sebuah browser dan memiliki ciri khas tersendiri yang tidak bisa di dapat diberikan oleh format GIF atau bahkan dengan format dalam bentuk JPEG. Kelebihan dari file PNG yaitu adanya unsur warna transparan dan *alpha*. Unsur warna pada *alpha* memungkinkan sebuah objek gambar menjadi transparan, tetapi gambar tersebut masih dilihat oleh mata seperti samar-samar atau bening.[12]

2.2.4 *Least Significant Bit* (LSB)

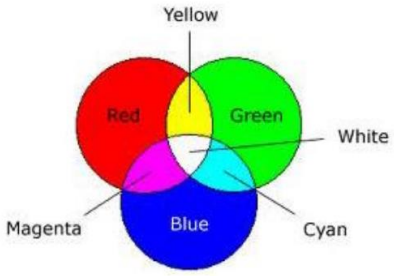
Least Significant Bit (LSB) merupakan teknik Steganografi yang digunakan untuk proses Steganografi berbasis media (*media-based steganography*) [13]. Teknik ini dilakukan dengan mengubah bit LSB pada setiap *byte piksel citra*. LSB piksel diganti dengan bit informasi pesan yang akan disisipkan. Metode LSB dilakukan dengan cara mengubah nilai bit terkecil yang terletak pada barisan paling akhir atau paling kanan dari bit data. Berikut merupakan gambar dari proses LSB:



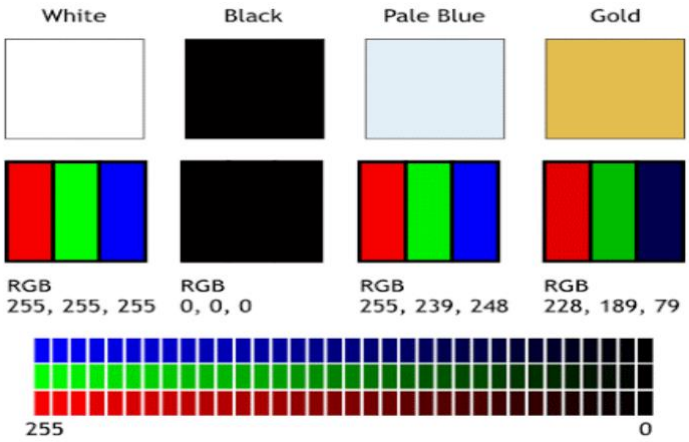
Gambar 2.2 Proses *Least Significant Bit* (LSB)

2.2.5 *Red, Green, Blue* (RGB)

Citra warna RGB merupakan matriks 3D yang dimensi pertama mewakili warna merah, dan dimensi kedua mewakili warna hijau, sedangkan dimensi ketiga mewakili warna biru seperti yang ditunjukkan pada gambar 2.3. Intensitas setiap warna berkisar antara 0 hingga 255 dan piksel warna dapat diperoleh dengan mencampurkan ketiga warna seperti yang ditunjukkan pada gambar 2.4.[14]



Gambar 2.3 Ruang Warna RGB



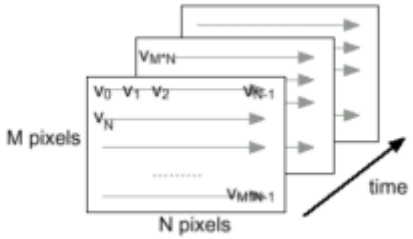
Gambar 2.4 Membuat warna dengan piksel RGB

Gambar berwarna dianggap sebagai salah satu jenis data digital yang paling penting karena penggunaannya dalam banyak aplikasi vital seperti sistem keamanan dan aplikasi pengenalan komputer. Gambar berwarna saat ini

memiliki resolusi yang sangat tinggi, yang meningkatkan ukurannya, yang menyebabkan penurunan efisiensi sistem verifikasi gambar melalui penggunaan proses perbandingan langsung, yang membutuhkan waktu yang lama untuk membuat perbandingan antara gambar yang berbeda. Pada model RGB sering digunakan untuk analisis gambar berwarna, dimana pada masing-masing bidang warna akan mengalami perhitungan, dan kemudian digabungkan menjadi satu untuk mendapatkan hasil pengukuran kualitas suatu gambar. RGB ini digunakan untuk melakukan perhitungan parameter kualitas suatu gambar dengan menggunakan PSNR. Data-data yang diambil dari RGB untuk perhitungan dari setiap intensitas warna yang digunakan untuk mendapatkan nilai PSNR. Penjelasan dari PSNR dapat dilihat pada bab 3.

2.2.*6* Video Digital

Video Digital merupakan jenis sistem video recording yang bekerja menggunakan sistem digital dibandingkan dengan analog dalam hal representasi videonya. Digital video memiliki banyak kelebihin dibandingkan analog video, yang paling penting adalah ketepatan yang tinggi dalam proses transmisi (high fidelity) dibandingkan dengan sinyal analog. Pada sinyal analog, saat penerimaan akhir transmisi akan sulit membedakan antara sinyal asli dan noise yang mungkin diperkenalkan selama transmisi. Dengan transmisi yang berulang-ulang maka akumulasi tidak dapat dihindari. Lain halnya dengan sinyal digital yang dapat membedakan antara sinyal asli dan noise. Sinyal digital juga dapat ditransmisikan berulang-ulang sebanyak yang kita inginkan tanpa mengurangi kualitasnya. Video digital tersusun atas serangkaian frame yang ditampilkan dengan kecepatan tertentu (frame/detik). Jika laju frame cukup tinggi, maka mata manusia akan melihat sebagai rangkaian continue. Setiap frame merupakan gambar atau citra digital. Suatu citra digital direpresentasikan dengan sebuah matriks yang masing-masing elemennya merepresentasikan nilai intensitas atau kedalaman warna [15].



Gambar 2.5 Ilustrasi tiga dimensi Video

2.2.7 Matlab

Matlab merupakan singkatan dari *Matrices Laboratory* yang dikembangkan oleh *MathWork*. Matlab dikembangkan sebagai bahasa pemrograman sekaligus sebagai alat untuk visualisasi yang menawarkan banyak kemampuan untuk menyelesai berbagai kasus yang berhubungan dengan ilmu matematika seperti bidang rekayasa teknik, fisika, statistika, komputasi dan modelling. Dengan memanfaatkan matlab, pengguna dapat melakukan analisis data serta mengembangkan algoritma, dan membuat model maupun aplikasi. Kemudian dari segi bahasa, tools, dan fungsi-fungsi builtin akan memudahkan pengguna untuk mengeksplorasi berbagai pendekatan dan memperoleh solusi yang cepat dibandingkan menggunakan spreadsheets atau Bahasa Pemrograman tradisional, seperti C/C++ atau Java.

Matlab menggunakan konsep array/matriks sebagai standar variable elemen tanpa memerlukan pendeklarasian array seperti pada bahasa yang lain. Dalam ilmu Pendidikan ilmiah, Matlab menjadi alat pemrograman standart bidang Matematika dan Rekayasa. Dalam lingkungan industry, matlab menjadi pilihan paling produktif untuk riset, komputasi dan analisa. Pada tahun 2004, *MathWorks* mengklain bahwa matlab telah dimanfaatkan oleh lebih dari satu juga pengguna di dunia Pendidikan dan industry. Matlab pertama kali diadopsi oleh insiyur control, namun tidak lama kemudian akhirnya menyebar secara cepat ke berbagai bidang lain. Kini digunakan dalam bidang Pendidikan, khususnya untuk pengajaran aljabar linear dan

analisis numerik serta populer di kalangan ilmuwan yang menekuni bidang pemrosessan citra [6]. Matlab mendukung format gambar PNG dan JPG berdasarkan pada jurnal ***Digital Colour Image Steganography for PNG Format and Secured Based on Encoding and Clustering*** **format** menggunakan metode pemadatan yang tidak menghilangkan bagian dari citra tersebut. Pada JPG sinyal informasi akan banyak sekali hilang karena proses kompresi data yang lebih kecil sehingga ukuran byte pada gambar menjadi lebih kecil dibandingkan PNG yang tidak terlalu banyak melakukan kompresi data.[12]