BAB II
LANDASAN TEORI

2.1 Pengertian Optimalisasi

Menurut Kamus Besar Bahasa Indonesia optimalisasi adalah berasal dari kata dasar optimal yang berarti terbaik, tertinggi, paling menguntungkan, menjadikan paling baik, menjadikan paling tinggi, pengoptimalan proses, cara, perbuatan mengoptimalkan (menjadikan paling baik, paling tinggi, dan sebagainya) sehingga optimalisasi adalah suatu tindakan, proses, atau metodologi untuk membuat sesuatu (sebagai sebuah desain, sistem, atau keputusan) menjadi lebih/sepenuhnya sempurna, fungsional, atau lebih efektif [8].

Dalam steganografi, optimalisasi ditujukan agar hasil yang dicapai dapat lebih baik dari yang sebelumnya. Sebagai contoh adalah penyisipan sebuah pesan ke dalam suatu media dapat dioptimasi hal keamanannya menggunakan tambahan metode kriptografi atau bisa juga mengoptimasi kualitas gambar yang telah disisipi pesan agar terlihat sama dengan gambar aslinya[9].

2.2 Steganografi

Steganografi adalah suatu teknik untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya akan tampak seperti informasi normal lainnya[1]. Media yang digunakan umumnya merupakan suatu media yang berbeda dengan media pembawa informasi rahasia, dimana disinilah fungsi dari teknik steganografi yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas[3]. Steganografi di dunia modern biasanya mengacu pada informasi atau suatu arsip yang telah disembunyikan ke dalam suatu arsip citra digital, audio, atau video. Steganografi dalam penerapannya terhadap data digital, dapat diterapkan pada berbagai metode. Ada empat jenis metode steganografi, yaitu Least Significant Bit Insertion (LSB), Algorithms and Transformation, Redundant Pattern Encoding, dan *Spread Spectrum*[2]. Metode steganografi yang digunakan adalah metode *Spread Spectrum*. Metode tersebut dibagi menjadi dua proses

utama, yaitu proses encode dan decode. Pada proses encode dilakukan operasi penyisipan pesan embedded-image kedalam cover-image. Sedangkan proses decode dilakukan proses penyaringan hasil penyisipan dan kemudian dikembalikan menjadi pesan awal. Metode *Spread Spectrum* memiliki keunggulan dalam ketangguhan terhadap berbagai serangan, meskipun di lain sisi metode ini memiliki kompleksitas yang tinggi [2].

Dalam menyembunyikan pesan, ada beberapa kriteria yang harus dipenuhi, diantaranya adalah [4]:

1. *Imperceptibility*. Keberadaan pesan tidak dapat dipersepsi oleh indrawi. Jika pesan disisipkan ke dalam sebuah citra, citra yang telah disisipi pesan harus tidak dapat dibedakan dengan citra asli oleh mata. Begitu pula dengan suara, telinga haruslah mendapati perbedaan antara suara asli dan suara yang telah disisipi pesan.

2. *Fidelity*. Pengujian terhadap aspek mutu (fidelity) citra hasil steganografi dapat dilakukan dengan beberapa metode. Salah satu metode yang paling banyak digunakan adalah dengan mengukur nilai *MSE (Mean Square Error) dan PSNR (Peak Signal to Noise Ratio)*. Keduanya merupakan sebuah nilai yang memiliki satuan dB (desibels). Semakin rendah nilai MSE maka kualitas citra semakin baik. Sementara itu, mutu stego-image dikatakan baik jika nilai PSNR 40 dB atau lebih.

3. *Robustness*. Tingkat ketahanan citra hasil steganografi terhadap operasi dasar seperti rotasi dan *resize* merupakan aspek yang cukup penting. Pesan yang terkandung di dalam stego-image seharusnya tidak rusak walaupun citra diputar, diperbesar atau diperkecil. Pengujian terhadap tingkat ketahanan citra dapat dilakukan dengan mengenakan operasi tertentu terhadap citra stego lalu dilihat apakah pesan yang disisipi masih dapat diambil atau tidak.

4. *Recovery*. Pesan yang disembunyikan harus dapat diungkap kembali. Tujuan steganografi adalah menyembunyikan informasi, maka sewaktu-waktu informasi yang disembunyikan ini harus dapat diambil kembali untuk dapat digunakan lebih lanjut sesuai keperluan.

Manfaat Steganografi

Steganografi dapat digunakan untuk menyembunyikan informasi rahasia ke dalam media lain, untuk melindunginya dari pencurian dan dari orang-orang yang tidak berhak untuk mengetahuinya. Steganografi juga dapat digunakan untuk pengiriman pesan secara rahasia tanpa diketahui bahwa pesan sedang dikirim. Ini membuat pihak ketiga tidak menyadari keberadaan pesan. Di sisi lain steganografi juga bisa digunakan sebagai sarana kejahatan.

Steganografi dapat digunakan untuk mencuri data yang disembunyikan pada data lain sehingga dapat dikirim ke pihak lain tanpa ada yang curiga. Steganografi juga dapat digunakan oleh para teroris untuk saling berkomunikasi dengan yang lain[2].

2.3 Citra Digital

Citra (*image*) adalah suatu persepsi visual hasil dari pantulan cahaya yang menerangi objek dan dipantulkan kembali sebagian dari berkas cahaya tersebut[1]. Alat-alat optik seperti mata manusia, kamera, *scanner* menangkap pantulan cahaya tadi sehingga bayangan objek yang disebut citra terekam. Secara sederhana dapat dikatakan sebagai suatu gambar pada bidang dua dimensi. Citra digital direpresentasikan sebagai sebuah matriks yang indeks baris dan kolomnya mengidentifikasikan sebuah titik pada citra dan nilai dari elemen matriks yang bersangkutan merupakan tingkat warna pada titik tersebut. Elemen tersebut disebut elemen citra, elemen gambar *(picture elements), pixels*, atau pels. Resolusi citra pada sebuah citra digital ditentukan oleh piksel. Semakin tinggi resolusi yang dihasilkan, semakin kecil ukuran pikselnya yang berarti bahwa citra yang dihasilkan semakin halus[1].

2.4 *Spread Spectrum*

Metode *Spread Spectrum* adalah sebuah teknik pentransmisian dengan menggunakan *pseudonoise code*, yang independen terhadap data informasi, sebagai modulator bentuk gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi *(bandwidth)* yang lebih besar daripada sinya jalur

komunikasi informasi[2]. Oleh penerima, sinyal dikumpulkan kembali menggunakan replika *pseudonoise code* tersinkronisasi. Berdasarkan definisi, dapat dikatakan bahwa steganografi menggunakan metode *Spread Spectrum* memperlakukan *cover-image* baik sebagai derau *(noise)* ataupun sebagai usaha untuk menambahkan derau semu *(pseudonoise)* kedalam *cover-image*. Proses penyisipan pesan menggunakan metode *Spread Spectrum* ini terdiri dari tiga proses, yaitu *spreading*, modulasi, dan penyisipan pesan ke citra. Sedangkan proses ekstraksi pesan menggunakan metode *Spread Spectrum* ini terdiri dari tiga proses, yaitu pengambilan pesan dari matriks frekuensi, demodulasi, dan *de-spreading*[2].

Pada steganografi, pembangkitan bilangan semu acak dapat digunakan untuk menentukan kunci penyisipan dan ekstraksi data dari berkas media. Komputer mampu menghasilkan bilangan semu acak *(pseudorandom)*. Deret bilangan *pseudorandom* adalah deret bilangan-bilangan yang kelihatan acak dengan kemungkinan pengulangan yang sangat kecil atau periode pengulangan yang sangat besar. Berikut adalah proses penyisipan pesan menggunakan metode *Spread Spectrum*[2].

1. *Spreading*

Proses *spreading* dilakukan sesuai dengan bilangan pengali skalar yang ditentukan, pada tugas akhir ini menggunakan bilangan pengali skalar 4. Pada proses ini citra rahasia diambil nilai intensitas per-piksel nya, lalu diubah kedalam bilangan biner. Kemudian bilangan biner tersebut disebar sesuai bilangan pengali skalar yang telah ditentukan, maka hasil keluaran dari proses spreading ini adalah deret bilangan biner yang telah tersebar dengan panjang setiap deretnya sebesar 32 bit.

2. Modulasi Pesan

Proses ini merupakan proses pengacakan pesan yang telah disebar dengan bilangan pseudonoise yang telah dibangkitkan menggunakan algoritma. Panjang dari bilangan pseudonoise ini disesuaikan dengan panjang dari pesan. Jika panjang pesan lebih kecil dari panjang bilangan pseudonoise, bilangan pseudonoise tersebut akan dipotong sesuai dengan ukuran pesan. Sebaliknya, jika

panjang pesan lebih besar dari panjang bilangan pseudonoise, maka bilangan tersebut akan diulang sampai panjangnya sama dengan panjang pesan. Proses modulasi tersebut dilakukan dengan menggunakan fungsi XOR *(Exclusive OR)*. Nilai yang dihasilkan dari proses modulasi inilah yang kemudian akan disisipkan ke dalam berkas citra *cover*.

3. Penyisipan Pesan

Pesan yang akan disisipkan dalam tahap ini adalah hasil dari proses modulasi yang telah dilakukan sebelumnya. Penyisipan pesan pada matriks frekuensi dilakukan dengan cara menyisipkan bit pesan pada bit terakhir dari nilai yang terdapat di matriks frekuensi. Hal lain yang perlu diperhatikan dalam menyisipkan pesan pada matriks frekuensi adalah pembagian penyisipan yang merata pada seluruh matriks frekuensi yang terdapat pada berkas citra cover. Untuk itu penyisipan akan dilakukan secara selang-seling berdasarkan jumlah matriks frekuensi yang ada pada berkas citra cover tersebut. Keluaran dari proses ini adalah citra stego yang telah tersisipi citra rahasia [2].

Sementara untuk tahap ekstraksi pesan, metode *Spread Spectrum* melewati beberapa tahap, berikut adalah 3 tahap ekstraksi pesan dalam *Spread Spectrum*;

1. Pembacaan Data Melalui Matriks Frekuensi

Pembacaan akan dilakukan secara berselang-seling pada matriks frekuensi yang terdapat pada citra dan berlangsung sampai data yang dibaca besarnya sama dengan informasi ukuran berkas yang disisipkan.

2. De-modulasi

Setelah data tersembunyi berhasil dikumpulkan, dilakukan proses demodulasi terhadap data tersebut. Proses demodulasi ini melibatkan bilangan acak yang dibangkitkan dari kunci masukan. Adapun proses pembangkitan bilangan acak yang dilakukan pada tahap ekstraksi pesan sama seperti proses pembangkitan bilangan acak pada tahap penyisipan pesan.

3. De-spreading

Hasil dari proses demodulasi tersebut akan mengalami proses de-spreading. Proses despreading ini bekerja menggunakan faktor besaran pengali yang dimasukkan oleh pengguna pada proses penyisipan pesan. Proses de-spreading ini adalah proses yang dilakukan untuk mendapatkan bit-bit dari pesan tersembunyi, maka hasil keluaran dari proses *de-spreading* ini adalah deret bilangan biner yang telah disusutkan dengan panjang setiap deretnya sebesar 8 bit. Lalu bit-bit tersebut dikonversi kedalam bilangan desimal, yang selanjutnya akan disusun sebagai nilai intensitas tiap pixel pada citra rahasia [2].

2.5 Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya, meski dalam ilmu kriptografi modern yang diamankan bukan hanya sebuah pesan tapi bisa keseluruhan data [6]. Dalam ilmu kriptografi, terdapat dua buah proses yaitu melakukan enkripsi dan dekripsi. Pesan yang akan dienkripsi disebut sebagai *plaintext* (teks biasa). Disebut demikian karena informasi ini dengan mudah dapat dibaca dan dipahami oleh siapa saja. Algoritma yang dipakai untuk mengenkripsi dan mendekripsi sebuah plaintext melibatkan penggunaan suatu bentuk kunci. Pesan *plaintext* yang telah dienkripsi (atau dikodekan) dikenal sebagai ciphertext (teks sandi) [6].

Di dalam kriptografi kita akan sering menemukan berbagai istilah atau terminology. Beberapa istilah yang harus diketahui yaitu :

1. Pesan, Plaintext, dan Ciphertext

Pesan (message) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah (*plaintext*) atau teks jelas *(cleartext)*.

2. Pengirim dan Penerima

Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim *(sender)* adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima *(receiver)* adalah entitas yang menerima pesan.

3. Enkripsi dan dekripsi

Proses menyandikan plainteks menjadi cipherteks disebut enkripsi *(encryption)* atau enciphering (standard nama menurut ISO 7498-2). Sedangkan proses mengembalikan ciphertext menjadi plaintext semula disebut dekripsi *(decryption)* atau *deciphering* (standard nama menurut ISO 7498-2).

4. Cipher dan kunci

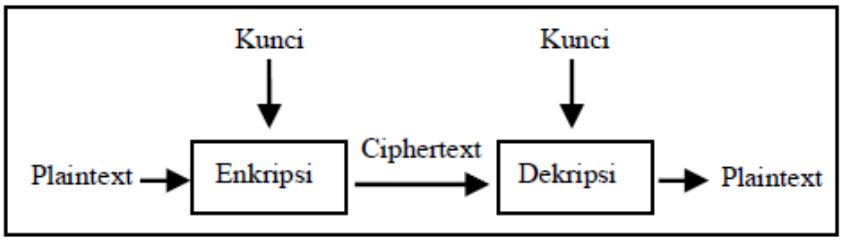
Algoritma kriptogarfi disebut juga cipher, yaitu aturan untuk enkripsi dan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa cipher memerlukan algoritma yang berbeda untuk enkripsi dan dekripsi. Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara dua buah himpunan yang berisi elemen-elemen plainteks dan himpunan yang berisi cipherteks. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen antara dua himpunan tersebut. Misalkan P menyatakan plainteks dan C menyatakan cipherteks, maka :

E(P) = C „³ fungsi enkripsi E memetakan P ke C

D(C) = P „³ fungsi dekripsi D memetakan C ke P

Karena proses enkripsi kemudian dekripsi mengembalikan pesan ke pesan asal, maka persamaan D(E(P)) = P harus benar. Kriptografi mengatasi masalah keamanan data dengan menggunakan kunci, yang dalam hal ini algoritma tidak dirahasiakan lagi, tetapi kunci harus tetap dijaga kerahasiaannya. Kunci (key) adalah parameter yang digunakan untuk transformasi enkripsi dan dekripsi. Kunci biasanya berupa string atau deretan bilangan.

Dengan menggunakan kunci K, maka fungsi enkripsi dan dekripsi dapat ditulis sebagai skema diperlihatkan pada Gambar 1.



Gambar 2.1. Skema enkripsi dan dekripsi dengan menggunakan kunci

2.5.1 Algoritma Simetri

Kriptografi algoritma simetri memiliki kunci yang sama dalam proses enkripsi dan dekripsi. Sistem kriptografi kunci simetri, mengasumsikan pengirim dan penerima pesan sudah berbagi kunci yang sama sebelum bertukar pesan. Algoritma simetri memiliki kunci yang bersifat rahasia, yang hanya diketahui oleh pihak pihak tertentu (secret-key cryptography). Waktu proses enkripsi dan dekripsi algoritma simetri cepat karena efisien dalam pemakaian kunci (hanya terdapat satu kunci dalam prosesnya). Yang termasuk algoritma kunci simetri adalah OTP, DES, RC2, RC4, RC5, RC6, IDEA, Twofish, Magenta, FEAL, SAFER, LOKI, CAST, Rijndael(AES), Blowfish, GOST, A5, Kasumi dan lain – lain[9].

2.5.2 Algoritma Asimetri

Kriptografi algoritma asimetri adalah algoritma kriptografi yang berbeda kunci untuk enkripsi dan kunci untuk dekripsinya. Hal ini disebabkan kunci untuk enkripsi tidak rahasia, diumumkan ke publik dan dapat diketahui oleh siapa saja (public-key cryptography), sementara dalam proses dekripsi, kuncin hanya diketahui oleh penerima pesan (kunci dekripsi bersifat rahasia). Pada kriptografi jenis ini, setiap orang yang berkomunikasi mempunyai sepasang kunci, yaitu kunci privat dan kunci publik. Yang termasuk algoritma asimetri adalah ECC, LUC, RSA, ElGamal dan DH [10].

2.5.3 Algoritma Hybrid

Kriptografi algoritma hybrid adalah metode kriptografi yang menggunakan kombinasi antara metode kriptografi algoritma simetri dan kriptografi algoritma asimetri. Proses enkripsi data menggunakan metode simetri karena prosesnya lebih cepat, tetapi kuncinya memakai metode asimetri agar tingkat keamanannya terjamin [10].

2.6 Sejarah Kriptografi

Sejarah kriptografi sebagian besar merupakan sejarah kriptografi klasik, yaitu metode enkripsi yang menggunakan kertas dan pensil atau mungkin dengan bantuan alat mekanik sederhana. Secara umum algoritma kriptografi klasik dikelompokkan menjadi dua kategori, yaitu algoritma transposisi (transposition cipher) dan algoritma substitusi (substitution cipher). Cipher transposisi mengubah susunan huruf-huruf di dalam pesan, sedangkan cipher substitusi mengganti setiap huruf atau kelompok huruf dengan sebuah huruf atau kelompok huruf lain [10].

2.7 Tujuan kriptografi

Dari paparan awal dapat dirangkumkan bahwa kriptografi bertujuan untuk member layanan keamanan. Yang dinamakan aspek-aspek keamanan:

1. *Confidentiality* (Kerahasiaan)

   Merupakan aspek yang menjamin kerahasiaan data atau informasi untuk tidak bisa diakses oleh pihak ketiga.

2. *Integrity* (Integritas Data)

   Merupakan aspek yang menjamin bahwa data tidak boleh berubah selama proses pengiriman sampai penerimaan informasi.

3. *Availability* (Ketersediaan Data)

   Availability merupakan aspek yang menjamin bahwa data tersedia ketika kapan pun dibutuhkan.

4. *Access Control* (Hak Akses)

   Berguna untuk memastikan seseorang memiliki autorisasi yang sesuai pihak-pihak yang dapat mengakses informasi atau masuk dalam suatu jaringan hanyalah orang yang memiliki autorisasi ke dalam jaringan dan bukan pihak lain yang sebenarnya tidak diizinkan untuk mengakses informasi dalam suatu

2.8 Kriptografi *Affine Cipher*

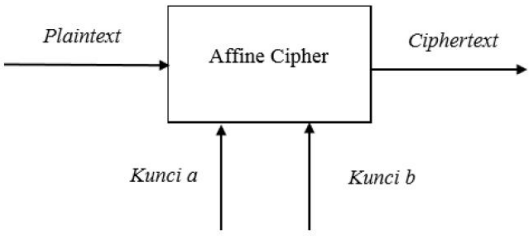
Affine Cipher adalah teknik cipher yang merupakan perluasan dari Caesar cipher. *Affine Cipher* merupakan metode kriptografi yang menggunakan kunci simetris, yang mana kunci yang digunakan untuk melakukan enkripsi sama dengan kunci yang digunakan untuk dekripsi [6]. Adapun terdapat dua proses dalam penggunaan *Affine Cipher*, yaitu:

2.8.1. Proses Enkripsi *Affine Cipher*

Proses enkripsi menggunakan *Affine Cipher* membutuhkan 2 buah kunci yaitu kunci 1 (a) dan kunci 2 (b) untuk dapat menghasilkan *ciphertext*. *Plaintext* (Pi) akan dikonversikan menggunakan table konversi sehingga menjadi bentuk decimal, kemudian *ciphertext* (Ci) akan diperoleh dengan mengenkripsi *plaintext* dengan persamaan :

$$Ci = (m\ Pi + b) \bmod 255 \quad .... (1)$$

Ci merupakan *ciphertext* dari pergeseran karakter yang terdapat pada *plaintext*. Pi merupakan pergeseran karakter pada *plaintext*. m merupakan kunci berupa bilangan bulat yang relatif prima dengan 255, apabila m tidak relatif prima dengan 255 maka dekripsi tidak akan bisa dilakukan. Sedangkan kunci b merupakan pergeseran nilai relatif prima dari m. Agar dapat memperoleh *ciphertext* maka perlu dilakukan perhitungan dengan persamaan (1) adapun hasil yang diperoleh masih berupa bilangan desimal, kemudian dari bilangan desimal tersebut akan dikonversi menggunakan tabel menjadi *ciphertext* yang diinginkan.



Gambar 2.2 Proses Enkripsi *Affine Cipher*

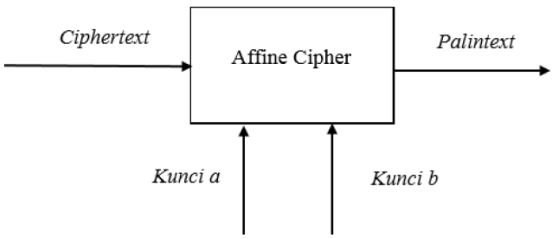
Gambar 2.2 menjelaskan bahwa untuk memperoleh *ciphertext* menggunakan *Affine Cipher* dibutuhkan input berupa plaintext yang akan dienkripsi menggunakan dua buah kunci [6].

2.8.2. Proses Dekripsi *Affine Cipher*

Proses dekripsi menggunakan *Affine Cipher* membutuhkan dua buah kunci yang mana kedua kunci yang dipakai haruslah sama dengan kunci yang digunnakan pada proses enkripsi. Agar dapat memperoleh *plaintext* maka kunci 1 (m) akan diubah dalam bentuk invers m (mod 255), dinyatakan dengan a^{-1}. Jika m^{-1} ada, maka dekripsi akan dilakukan dengan persamaan

$$Pi = m^{-1}(Ci - b) \bmod 255 \quad \ldots\ldots\ldots (2)$$

Pi merupakan *plaintext* dari pergeseran karakter yang terdapat pada *ciphertext*. Ci merupakan pergeseran karakter pada *ciphertext*. m dan b merupakan kunci yang sama dengan kunci yang digunakann pada proses enkripsi. Agar dapat memperoleh *plaintext* maka diperlukan perhitungan menggunakan persamaan (2). Sebelum melakukan perhitungan terlebih dahulu Pi dan Ci harus dikonversikan kedalam bentuk decimal menggunakan tabel konversi. Hasil dari perhitungan yang dilakukan akan berbentuk bilangan decimal yang kemudian akan dikonversi menggunakan tabel konversi untuk memperoleh plaintext[4].



Gambar 2.3 Proses Dekripsi *Affine Cipher*

Gambar 2.3 menjelaskan bahwa untuk memperoleh *plaintext* menggunakan *Affine Cipher* dibutuhkan input berupa *ciphertext* yang akan dienkripsi menggunakan dua buah kunci.

Kekuatan dari *Affine Cipher* ini terletak pada kunci yang dipakai. Kunci ini merupakan nilai integer yang menunjukkan pergeseran karakter-karakter.

Selain itu *Affine Cipher* juga menggunakan barisan bilangan-bilangan yang berfungsi sebagai pengali kunci. Barisan yang digunakan dapat berupa bilangan tertentu seperti deret bilangan genap, deret bilangan ganjil, deret bilangan prima, deret fibonaci dapat juga deret bilangan yang dibuat sendiri. Dengan adanya kemungkinan pemilihan kunci yang dipilih lebih bervariatif dan lebih banyak algoritma enkripsi subtitusi lain menjadikan *Affine Cipher* sebagai sistem enkripsi yang paling sempurna dibandingkan dengan algoritma enkripsi subtitusi lainnya [12].

2.9 MATLAB

MATLAB adalah kependekan dari *MATrix LABoratory* dikarenakan setiap data pada MATLAB menggunakan dasar matriks. MATLAB adalah bahasa pemrograman tinggi, tertutup, dan *case sensitive* dalam lingkungan komputasi numerik yang dikembangkan oleh *MathWorks*. Salah satu kelebihannya yang paling populer adalah kemampuan membuat grafik dengan baik. MATLAB mempunyai banyak *tools* yang dapat membantu berbagai disiplin ilmu. Ini merupakan salah satu penyebab industri menggunakan MATLAB. Selain itu MATLAB mempunyai banyak *library* yang sangat membantu untuk menyelesaikan permasalahan matematika seperti membuat simulasi fungsi, pemodelan matematika dan perancangan GUI [13].