Perancangan Aplikasi Steganografi Menggunakan Metode Adaptive Minimum Error Least Significant Bit Replacement

Wempi Simanjuntak
STMIK Budidarma Medan, Jl. Sisingamangaraja No. 338 Simpang Limun Medan.
wempi.simanjuntak@gmail.com

Abstrak- Steganografi adalah suatu metode untuk mengijinkan para pengguna untuk menyembunyikan suatu pesan didalam pesan yang lain dalam bentuk media digital, pesan yang ingin di sampaikan disembunyikan dalam suatu media digital sehingga diharapkan tidak akan menimbulkan kecurigaan dari pihak lain yang tidak di inginkan untuk mengetahui pesan rahasia tersebut. Terdapat dua tahapan umum dalam steganografi digital, yaitu proses embedding atau encoding (penyisipan) dan proses extracting atau decoding (pemekaran atau pengungkapan kembali (reveal)). Hasil yang didapat setelah proses embedding atau encoding disebut stego object (apabila media penampung hanya berupa data citra maka disebut Stego Image). Metode penyisipan AMELSBR, prosesnya tidak sama dengan metode LSB. Apabila proses penyisipan di dalam metode LSB dilakukan langsung per piksel pada byte-nya, dimana 1 bit terakhir (LSB) per byte-nya diganti dengan 1 bit data rahasia yang akan disisipkan, tetapi tidak dengan metode AMELSBR. Di dalam metode ini, citra penampung (cover image) akan dibagi dulu menjadi beberapa blok. Setiap blok akan berukuran 3 x 3 piksel atau sama dengan 9 piksel.

Kata Kunci: Steganografi, AMELSBR

Abstract- Steganography is a method to allow users to hide a message in another message in the form of digital media, the message to be conveyed is hidden in a digital media so that it is hoped that it will not cause suspicion from other parties who do not want to know the secret message the. There are two general stages in digital steganography, namely the process of embedding or encoding (insertion) and the process of extracting or decoding (revealing or revealing). The results obtained after the embedding or encoding process are called stego objects (if the storage media is only in the form of image data, it is called Stego Image). AMELSBR insertion method, the process is not the same as the LSB method. If the insertion process in the LSB method is done directly per pixel in its bytes, where the last 1 bit (LSB) per byte is replaced by 1 secret data bit to be inserted, but not by the AMELSBR method. In this method, the cover image will be divided into several blocks first. Each block will be 3 x 3 pixels or 9 pixels.

Keywords: Steganography, AMELSBR

PENDAHULUAN

Steganography (steganografi) merupakan seni untuk menyembunyikan pesan rahasia kedalam pesan lainnya sedemikian rupa sehingga membuat orang lain tidak menyadari adanya sesuatu di dalam pesan tersebut. Kata Steganography berasal dari bahasa Yunani, yaitu gabungan dari kata steganos (tersembunyi atau terselubung) dan graphein (tulisan atau menulis), sehingga makna [1]. Steganography kurang lebih bisa diartikan sebagai menulis tulisan yang tersembunyi atau tulisan tersembunyi *(hidden/covered writing)*. Sejalan dengan perkembangan maka konsep awal steganograhi di implementasikan pula dalam dunia komputer, yang kemudian dikenal dengan istilah steganografi digital [2]. Dalam hal ini, steganografi digital memiliki dua properti dasar yaitu media penampung (cover data atau data *carrier*) dan data digital yang akan disisipkan (*secret data*), dimana media penampung dan data digital yang akan disisipkan dapat berupafile multimedia (teks/dokumen, citra, audio maupun video). Pada penelitian ini akan membahas tentang bagaimana mengamankan sebuah pesan teks dengan menyisipkan pesan tersebut kedalam sebuah citra digital.

Terdapat dua tahapan umum dalam steganografi digital, yaitu proses embedding atau encoding (penyisipan) dan proses *extracting* atau *decoding* (pemekaran atau pengungkapan kembali (*reveal*). Hasil yang didapat setelah proses embedding atau encoding disebut *stego object* (apabila media penampung hanya berupa data citra maka disebut Stego Image)[3]. Berdasarkan latar belakang di atas maka diperoleh rumusan permasalahan pada penelitian ini adalah bagaimana proses penyembunyian pesan rahasia ke citra digital dengan metode *Adaptive Minimum Error least Significant Bit Replacement*, bagaimana merancang dan membuat aplikasi untuk menyembunyikan pesan rahasia ke citra digital dengan menggunakan metode *Adaptive Minimum Error least Significant Bit Replacement*[4].

Agar pembahasan dapat terfokus, maka dilakukan pembatasan masalah adalah Input citra sampul dalam format JPG, Input dokumen teks sebagai pesan rahasia yang akan disisipkan memiliki format TXT, tanpa mencakup gambar ataupun tabel, Ukuran citra yang diproses memiliki batasan minimal 100 x 100 pixel dan maksimal 1000 x 1000 pixel, Kapasitas pesan yang disisipkan tidak lebih dari 50% ukuran media penampungnya. Tujuan dari penelitian ini adalah untuk menemukan hasil teknik penyembunyian pesan rahasia pada citra digital dengan metode *Adaptive Minimum Error least Significant Bit Replacement* dan menghasilkan aplikasi steganografi dengan menggunakan Microsoft Visual Basic 2008 dengan menerapkan

metode Adaptive Minimum *Error least Significant Bit Replacement* untuk proses penyisipan pesan ke dalam citra. Manfaat dari penyusunan penelitian ini adalah dengan adanya aplikasi mempermudah bagi user dalam menyembunyikan pesan rahasia sehingga penyadap tidak mengetahui isi pesan tersebut, Untuk menambah wawasan dan ilmu pengetahuan mengenai hal-hal yang berkaitan dengan penyembunyian pesan menggunakan media citra.

.

METODOLOGI PENELITIAN

Adapun metodologi penelitian[5] yang digunakan dalam penelitian ini adalah:

1. Studi Pustaka
   Mengumpulkan data yang berkaitan dengan topik yang dibahas yang dilakukan dengan cara membahas buku-buku, literatur, internet, serta karya tulis ilmiah yang berkaitan dengan sistem informasi sekolah berbasis web.
2. Pengumpulan Data
   Teknik pengumpulan data dilakukan dengan cara:
   a. Wawancara (Interview)
      Dengan bertanya langsung pada bagian administrasi, guru, bagian keuangan dan kepala sekolah untuk mendapatkan informasi yang berhubungan dengan topik yang dibahas.
   b. Observasi (Pengamatan)
      Dengan melakukan pengamatan secara langsung prosedur kerja guru dalam melakukan pendataan nilai siswa.
3. Analisis Sistem Berjalan
   Untuk menganalisis sistem yang diterapkan SMP Yapendak Tinjowan saat ini dan kebutuhan sistem yang diperlukan.
4. Perancangan Sistem
   Meliputi rancangan model sistem dengan *Data Flow Diagram* (DFD), rancangan *output*, rancangan *input*, rancangan basis data *(database)* yang meliputi struktur tabel dan relasi antar tabel dan rancangan *user interface* yang meliputi menu dan sub-menu sistem.
5. Implementasi Sistem
   Pada tahap ini akan ditampilkan hasil sistem yang dirancang untuk diuji agar dapat diketahui apakah sistem yang dirancang telah sesuai dengan tujuan perancangan.

Steganografi adalah suatu metode untuk mengijinkan para pengguna untuk menyembunyikan suatu pesan didalam pesan yang lain dalam bentuk media digital [6]. Kerahasiaan pesan yang ingin disampaikan merupakan faktor utama dalam steganografi. Dengan metode steganografi, pesan yang ingin di sampaikan disembunyikan dalam suatu media digital sehingga diharapkan tidak akan menimbulkan kecurigaan dari pihak lain yang tidak di inginkan untuk mengetahui pesan rahasia tersebut. Sejalan dengan berkembangnya teknologi, maka tentunya teknik-teknik steganografi terus berkembang dan dimanfaatkan untuk berbagai kebutuhan.

Pada metode steganografi cara ini sangat berguna jika digunakan pada cara steganografi komputer karena banyak format berkas digital yang dapat dijadikan media untuk menyembunyikan pesan. Format yang biasa digunakan di antaranya:

1. Format image : bitmap (bmp), gif, pcx, jpeg.
2. Format audio : wav, voc, mp3.
3. Format lain : teks file, html, pdf.

Kelebihan steganografi jika dibandingkan dengan kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya. Steganalisis didefinisikan sebagai suatu seni dan ilmu dalam mendeteksi informasi tersembunyi. Sebagai tujuan dari steganografi adalah untuk merahasiakan keberadaan dari sebuah pesan rahasia, satu keberhasilan penyerangan pada sebuah sistem steganografi terdiri dari pendeteksian bahwa sebuah berkas yang diyakini berisikan data terselubung. Seperti dalam Kriptanalisis, diasumsikan bahwa sistem steganografi telah diketahui oleh penyerang. Maka dari itu, keamanan dari sistem steganografi bergantung hanya pada fakta bahwa kunci rahasia tidak diketahui oleh si penyerang.Stegosystem disini berisi tentang penyerangan-penyerangan yang dilakukan terhadap suatu

sistem steganografi, sebuah perbedaan penting harus dibuat di antara penyerangan-penyerangan pasif di mana penyerang hanya dapat memotong data, dan penyerangan-penyerangan aktif dimana penyerang juga dapat memanipulasi data

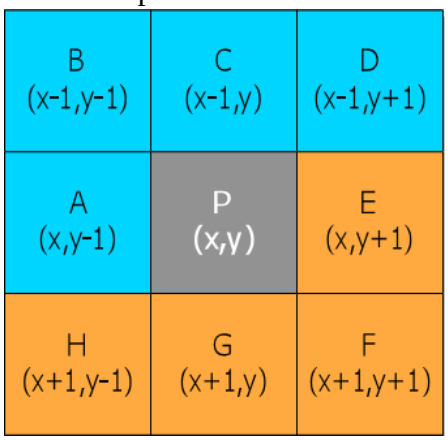
Bentuk teks terdiri dari beberapa susunan karkater (huruf) yang dibentuk menjadi satu kata, satu kalimat hingga berparagraf. Dalam Kamus Linguistiknya menyatakan bahwa teks adalah (1) satuan bahasa terlengkap yang bersifat abstrak, (2) deretan kalimat, kata, dan sebagainya yang membentuk ujaran, (3) ujaran yang dihasilkan dalam interaksi manusia. Dilihat dari tiga pengertian teks yang dikemukakan dalam Kamus Linguistik tersebut dapat dikatakan bahwa teks adalah satuan bahasa yang bisa berupa bahasa tulis dan bisa juga berupa bahasa lisan yang dahasilkan dari interaksi atau komunikasi manusia.

Dari hasil peneltian tersebut ternyata metode ini menawarkan beberapa kelebihan dibandingkan dengan metode LSB, yaitu bit data rahasia yang akan disisipkan lebih banyak (pada metode LSB umumnya hanya 1 bit) tanpa menimbulkan banyak perubahan pada media penampung (dalam hal ini adalah data citra). Dengan metode ini, setiap piksel memiliki kapasitas penyembunyian yang berbeda-beda tergantung dari nilai toleransi piksel tersebut terhadap proses modifikasi atau penyisipan. Suatu piksel pada data citra bisa dikatakan dapat ditoleransi apabila dilakukan proses modifikasi (penyisipan) dengan skala yang tinggi terhadap nilainya adalah memungkinkan tanpa merubah tampak asli dari data citra tersebut, atau dengan kata lain area yang halus dan solid pada suatu data citra memiliki kadar toleransi yang rendah (less tolerant) terhadap proses modifikasi dibandingkan dengan area yang memiliki tekstur yang kompleks.

Metode AMELSBR yang diterapkan pada citra berwarna (bitmap 24-bit) memiliki beberapa langkah atau tahapan utama untuk melakukan proses penyisipan, antara lain Capacity Evaluation, Minimum Error Replacement dan Error Diffusion, juga ditambah *Pseudo Random Number Generator* (PRNG) sebagai pembangkit nilai yang secara acak memilih dari ke-tiga komponen warna RGB disetiap piksel-nya. Untuk proses pengungkapan, tahapan yang dilakukan yaitu *Capacity Evaluation* [7].

Sebelum dilakukan proses penyisipan, maka langkah pertama yang harus dilakukan adalah mengevaluasi kapasitas penyisipan *(capacity evaluation*) dan mencari nilai *color variation*. Kemudian setelah mendapatkan nilai color variation, nilai tersebut diproses kembali untuk mendapatkan kapasitas penyisipan sejumlah K-bit, selanjutnya untuk beradaptasi dengan karakteristik lokal piksel, maka sejumlah K-bit tersebut ditangani dengan proses evaluasi kapasitas *(capacity evaluation)*. Proses selanjutnya adalah mencari MER, dimana proses ini akan menentukan apakah bitke K+1 akan dilakukan perubahan atau tidak, dan yang akan menentukan itu adalah berdasarkan pada nilai embedding error (Er).

Proses penyisipan *(embedding)* di dalam metode AMELSBR, prosesnya tidak sama dengan metode LSB. Apabila proses penyisipan di dalam metode LSB dilakukan langsung per piksel pada byte-nya, dimana 1 bit terakhir (LSB) per byte-nya diganti dengan 1 bit data rahasia yang akan disisipkan, tetapi tidak dengan metode AMELSBR [8]. Didalam metode ini, citra penampung *(cover image)* akan dibagi dulu menjadi beberapa blok. Setiap blok akan berukuran 3 x 3 piksel atau sama dengan 9 piksel. Ke-tiga tahapan utama akan diterapkan perbloknya atau peroperasi penyisipannya, dimana bit-bit data rahasia hanya akan disisipkan pada salah satu komponen warna di piksel P.



Gambar 1 Piksel dari tetangga dari piksel P

Capacity evaluation, merupakan tahap pertama dan yang paling krusial dari metode penyisipan AMELSBR. Tahap ini mengacu pada karakterisitik human visual sistem (HVS) yang tidak sensitif terhadap noise dan perubahan warna yang terdapat di dalam citra. Langkah pertama yang akan dilakukan pada

evaluasi kapasitas adalah mencari nilai color variation (V)atau variasi warna yang melibatkan piksel A, B, Cdan D. Adapun rumus dari V adalah sebagai berikut:

V = round {(|C-A|+|A-B|+|B-C|+|C-D|)/4}

dimana

V = variasi warna (color variation)

Round = fungsi matematika untuk pembulatan

Rumus di atas akan menghasilkan ketentuan toleransi modifikasi yang akurat di setiap piksel P.

Langkah ke-dua adalah mencari kapasitas penyisipan (K) pada piksel P dan dapat diterapkan rumus sebagai berikut :

K = round (|log2V|).

dimana

K = kapasitas penyisipan pada piksel P dalam bit.

V = variasi warna

Round = fungsi matematika untuk pembulatan

Tahap selanjutnya adalah mencari *Minimum-Error Replacement* (MER). Tahap ini berfungsi untuk meminimalkan terjadinya perubahan piksel pada citra penampung akibat dari proses penyisipan. Proses MER dilakukan dengan mengubah nilai bit ke K+1 pada piksel P. Perubahan ini akan terjadi pada salah satu dari ke-tiga komponen warna (R, G atau B) yang terpilih.

Citra adalah representasi dari sebuah objek. Citra merupakan kumpulan dari titik-titik yang mempunyai intensitas tertentu membentuk satu kesatuan perpaduan yang mempunyai arti baik secara artistik maupun intristik. Citra yang baik adalah citra yang dapat menampilkan gambar yang dimaksud dengan seutuhnya, yang meliputi keindahan gambar, kejelasan gambar untuk penganalisaan dan maksud-maksud lainnya. Dengan kata lain, citra yang baik adalah citra yang dapat menampilkan nilai artistik dan intristik gambar tersebut dengan baik. Citra yang dihasilkan dapat digolongkan menjadi citra analog dan citra digital

HASIL DAN PEMBAHASAN

Analisa sistem adalah pembelajaran sebuah sistem dan komponen-komponennya sebagai prasyarat *system design* / desain sistem dan spesifikasi sebuah sistem yang baru. Berpindah dari definisi klasik analisa sistem ini ke suatu yang lebih kontemporer, analisa sistem adalah sebuah istilah yang secara kolektif mendeskripsikan fase-fase awal pengembangan sistem.

Dalam proses analisa ini, seorang penganalisa akan melakukan beberapa tahapan kerja berikut:

1. Menganalisa proses kerja dari sistem yang akan dibuat.
2. Menjabarkan menganalisa masukan, proses dan keluaran secara sistematika
3. Menggambarkan model dari sistem yang akan dibuat.

3.1 Analisa Penyisipan Metode Adaptive Minimum ErrorLeast Significant Bit Replacement (AMELSBREncoding)

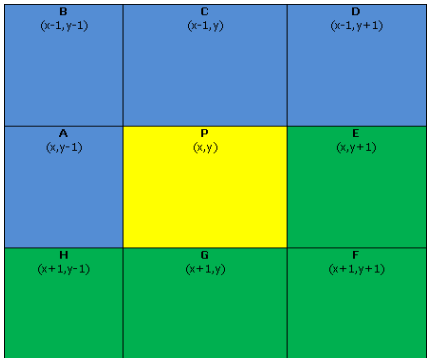
Metode penyisipan AMELSBR langkah pertama yang akan dilakukan sebelum melakukan penyisipan *(processembedding)* yaitu mengevaluasi kapasitas penyisipan *(Capacity Evaluation)* dan mencari nilai variasi warna *(colorvariation)*.Kemudian setelah mendapatkan nilai *colorvariation*, nilai tersebut diproses kembali untuk mendapatkan kapasitas penyisipan sejumlah K-bit., selanjutnya untuk beradaptasi dengan karakteristik lokal piksel, maka sejumlah K-bittersebut ditangani dengan proses evaluasi kapasitas *(capacityevaluation)*.

Proses selanjutnya adalah mencari MER, dimana proses ini akan menentukan apakah bitke K+1akan dilakukan perubahan atau tidak, dan yang akan menentukan itu adalah berdasarkan pada nilai embeddingerror (Er).

3.2. Proses Embedding

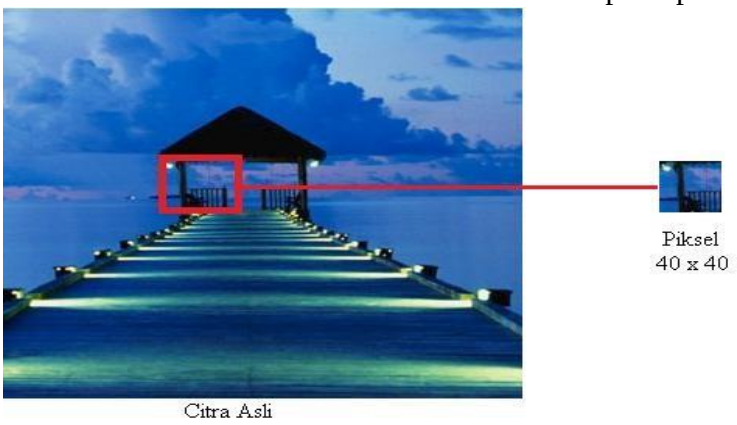
Proses penyisipan *(embedding*) didalam metode AMELSBR, prosesnya tidak sama dengan metode LSB. Apabila proses penyisipan di dalam metode LSB dilakukan langsung per piksel padabyte-nya, dimana 1 bitterakhir (LSB) per byte-nya diganti dengan 1 bitdata rahasia yang akan disisipkan, tetapi tidak dengan metode AMELSBR.

Di dalam metode ini, citra penampung *(coverimage)* akan dibagi dulu menjadi beberapa blok. Setiap blok akanberukuran 3 x 3 piksel atau sama dengan 9 piksel. Ke-tiga tahapan utama akan diterapkan per bloknya atau per operasi penyisipannya, dimana bit-bitdata rahasia hanya akan disisipkan pada salah satu komponen warna dipiksel P. Seperti pada gambar berikut:



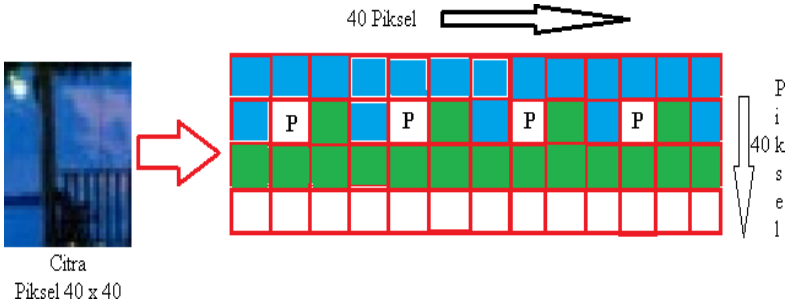
Gambar 2. Piksel Gambar tempat piksel P

Contoh proses penyisipian Gambar (digital) dengan metode AMELSBR sebagai berikut : Contoh data yang akan disisipakan biner karakter huruf "A" bernilai 01000001 akan disisipkan pada citra berikut:



Gambar 3. Citra dijadikan sampel tempat penyisipan teks dengan piksel 40x40

Dari gambar diatas dibagi jadi beberapa blok dengan ketentuan blok 3x3 piksel seperti pada gambar berikut ini:



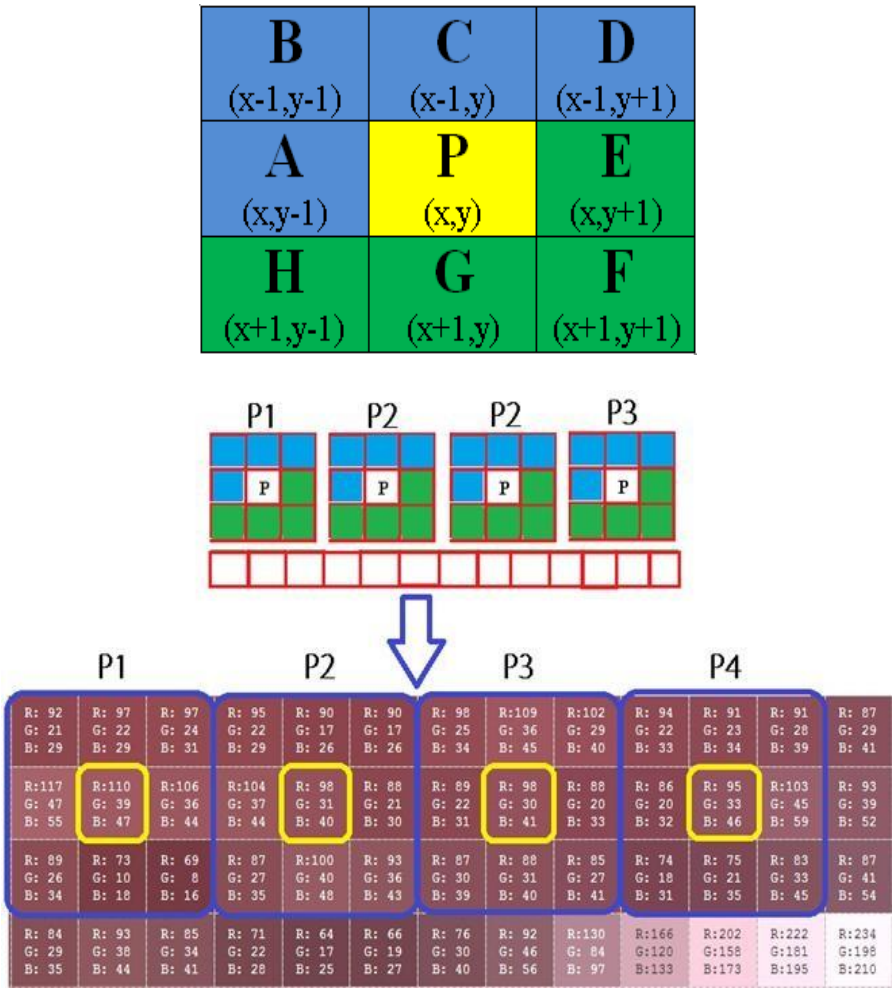
Gambar 4. Model Penyisipan Metode AMELSBR

Dari gambar diatas pada piksel yang bertuliskan "P" akan disisipkan biner huruf A yaitu 01000001. Setiap piksel pada gambar mempunyai 3 jenis nilai yaitu R (Red), G (Green), B (Blue).
Sebelum dilakukan penyisipan terlebih dahulu cari nilai variasi warna untuk evaluasi kapasitas daya tampung citra dengan rumus:

$V = \text{round } \{(|C-A|+|A-B|+|B-C|+|C-D|)/4\}$

dimana

V = variasi warna (color variation)
Round = fungsi matematika untuk pembulatan



Gambar 5. Proses mengevaluasi kapasitas tampung sebuah piksel

Sesuai gambar 4 diatas maka dapat diuraikan nilai kapasitas penyisipan pada masing-masing piksel yang telah dibagi-bagi menjadi beberapa blok yang masing-masing blok berordo 3x3, sebagai berikut:

Blok P1

Nilai Variasi warna untuk blok piksel P1:

V = round {(|C-A|+|A-B|+|B-C|+|C-D|)/4}
V = round {(|49,3 - 47,3| + |73 – 47,3| + |47,3 – 49,3| + |49,3 – 50,7|)/4}
V = round {((2)+(25,7)+(-2)+(-1,3))/4}
V = round {(27,7 + (-3,3))/4}
V = round ((24,4)/4)
V = 6,1

Maka nilai kapasitas penyisipan pada piksel P1, dengan rumus:

K = round (log2V)
K = round (log2 (6,1))
K = round (2,608809)
K = 2,61

Blok P2

Nilai Variasi warna untuk blok piksel P2:

V = round {(|C-A|+|A-B|+|B-C|+|C-D|)/4}
V = round{(|44,33 - 61,67| + |61,67 - 48,67| + |48,67 - 44,33| + |44,33 - 44,33|)/4}
V = round{(|-17,34| + |13| + |4,34| + |0|)/4}
V = round{0}
V = 0

Maka nilai kapasitas penyisipan pada piksel P2, dengan rumus:

K = round (log2V)

K = round (log2(0))
K = 0

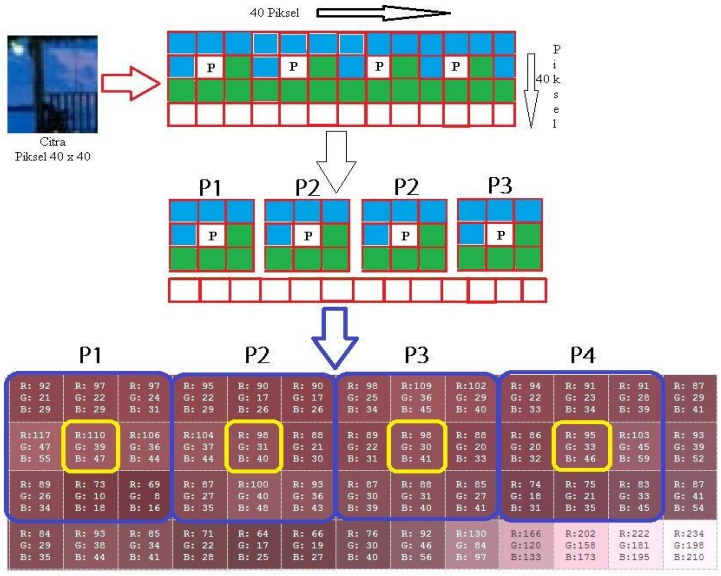
Blok P3

Nilai Variasi warna untuk blok piksel P3:
V = round {(|C-A|+|A-B|+|B-C|+|C-D|)/4}
V = round {(|63,33-47,33|+|47,33-52,33|+|52,33-63,33|+|63,33-57|)/4}
V = round {(|16|+|-5|+|-11|+|6,33|)/4}
V = round {(|16|+|-5|+|-11|+|6,33|)/4}
V = round {(|6,33|)/4}
V = round (1,5825)
V = 1,58
Maka nilai kapasitas penyisipan pada piksel P3, dengan rumus:
K = round (log2V)
K = round (log2(1,58))
K = round (0,6599)
K = 0,65

Blok P4

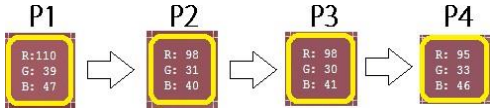
Nilai Variasi warna untuk blok piksel P3:
V = round {(|C-A|+|A-B|+|B-C|+|C-D|)/4}
V = round {(|49,33-46|+|46-49,67|+|49,67-49,33|+|49,33-52,67|)/4}
V = round {(|3,33|+|-3,67|+|0,34|+|-3,34|)/4}
V = round {(-3,34)/4}
V = round (-0,835)
V = -0,84

Maka nilai kapasitas penyisipan pada piksel P3, dengan rumus:
K = round (log2V)
K = ≠
Setelah di tentukan nilai kapasitas penyimpanan, maka proses penyisipan biner 01000001 di sisipkan pada:
Piksel (P) Pertama = R disisikan biner 0 ; G disisikan biner 1 ; B disisikan biner 0
Piksel (P) Kedua = R disisikan biner 0 ; G disisikan biner 0 ; B disisikan biner 0
Piksel (P) Ketiga = R disisikan biner 0 ; G disisikan biner 1 ; B disisikan biner “kosong”
Contoh percobaan :



Gambar 6. Pengambilan nilai blok 3x3 setiap piksel yang ada pada citra

Pada gambar 3.5 setiap blok 3x3 pada piksel dengan nilai tengah piksel akan dijadikan sebagai media tempat penyisipan teks, antara lain:



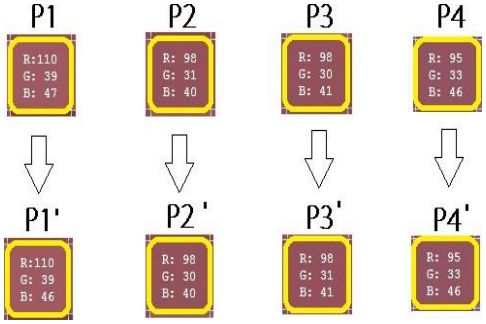
Gambar 7. Detail P1, P2, P3 dan P4

Jika data teks yang akan disipkan adalah huruf "A" dengan nilai biner "01000001", maka biner pertama dari sebelah kiri yaitu biner 010, masing-masing biner akan disisipkan pada piksel P1, kedua yaitu biner 000, masing-masing disisipkan pada piksel P2, ketika yaitu biner 01, masing-masing disisipkan pada piksel 3.

Tabel 1 Penjabaran nilai biner setiap piksel

Piksel	Warna	Nilai Desimal	Nilai Biner	Biner yang disisipkan	Perubahan Nilai Biner Setelah Penyisipan	Perubahan Nilai Desimal Setelah Penyisipan
P1	R	110	01101110	**0**	0110111**0**	110
	G	39	00100111	**1**	0010011**1**	39
	B	47	00101111	**0**	0010111**0**	46
P2	R	98	01100010	**0**	0110001**0**	98
	G	31	00011111	**0**	0001111**0**	30
	B	40	00101000	**0**	0010100**0**	40
P3	R	98	01100010	**0**	0110001**0**	98
	G	30	00011110	**1**	0001111**1**	31
	B	41	00101001	-	00101001	41
P4	R	95	01011111	-	01011111	95
	G	33	00100001	-	00100001	33
	B	46	00101110	-	00101110	46

Keterangan:
P = Piksel
R = Red (Warna Merah)
G = Green (WarnaHijau)
B = Blue (Warna Biru)
Hasil penyisipan teks kedalam piksel dapat dilihat pada gambar 6



Gambar 8. Perubahan Nilai Desimal Pada Masing-masing piksel

KESIMPULAN

Setelah menyelesaikan pembuatan perangkat lunak ini, penulis dapat menarik beberapa kesimpulan sebagai sebuah teknik steganografi dengan metode Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR) untuk menyembunyikan pesan teks pada citra JPEG dapat diaplikasikan dengan menggunakan Microsoft Visual Basic 2008**,** Aplikasi dapat digunakan untuk menyembunyikan pesan rahasia pada citra digital dimana perubahan warna citra input dengan hasil tidak kelihatan jelas. Penulis ingin

memberikan beberapa saran yang mungkin berguna untuk pengembangan lebih lanjut pada perangkat lunak, yaitu : Perangkat lunak dapat dikembangkan lagi dengan menambahkan fitur lainnya seperti fitur tutorial yang mampu menjelaskan prosedur kerja dari algoritma yang dibahas secara terperinci, Perangkat lunak dapat dikembangkan dengan menggunakan bahasa pemrograman Microsoft Visual C++ dan aplikasi lainnya sehingga proses eksekusi dari perangkat lunak dapat lebih cepat, Teknik steganografi dapat dikembangkan untuk implementasi penyisipan pesan ke dalam media lain seperti audio dan video dan Teknik Steganografi dengan metode AMELSBR dapat di kombinasikan dengan Algoritma Kriptografi yang lainnya untuk terjaminnya keamanan pesan rahasia.

DAFTAR PUSTAKA

[1] R. Munir, "Kriptografi," *Inform. Bandung*, 2006.
[2] A. Suhendra, "Steganografi Pada Citra Terkompresi Metode Huffman," *MEANS (Media Inf. Anal. dan Sist.*, vol. 1, no. 2, pp. 33–39, Dec. 2016, doi: 10.17605/JMEANS.V1I2.6.
[3] T. Arista, "Perancangan Aplikasi Pengamanan Pesan Menggunakan Algoritma Elgamal Berbasis Android," *KakifikomKumpulan Artik. Karya Ilm. Fak. Ilmu Komput.*, vol. 02, no. 01, pp. 43–48, 2020.
[4] D. Ariyus, "Kriptografi keamanan data dan komunikasi," *Yogyakarta Graha Ilmu*, 2006.
[5] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif dan R&D.* Bandung: PT Alfabet, 2016.
[6] C. Paper, A. Solichin, and U. Budi, "Implementasi Steganografi Dengan Metode Bit Plane Complexity Segmentation Untuk Menyembunyikan," no. March, pp. 2–3, 2016.
[7] Y. Prayudi and P. S. Kuncoro, "Implementasi Steganografi Menggunakan Teknik Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR)," *Snati*, vol. 2005, no. Snati, pp. 1–6, 2005.
[8] C. Paper, Y. Prayudi, and U. Islam, "Implementasi Steganografi Menggunakan Teknik Adaptive Minimum Error Least Significant Bit Replacement," no. August, pp. 87–94, 2015.