**PERBANDINGAN CITRA HASIL STEGANOGRAFI MENGGUNAKAN METODE DCT DAN LSB**

Proposal Tugas Akhir



Diajukan oleh:

Valery Nicolay

22105011

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS KRISTEN DUTA WACANA

YOGYAKARTA

2015

Perbandingan citra hasil Steganogfrafi menggunakan metode DCT dan LSB

|  |  |  |  |
| --- | --- | --- | --- |
| Bidang Minat | : | Keamanan Komputer |  |
| Mata kuliah pendukung | : | 1. Keamanan Komputer | B |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
| Nama Mahasiswa | : | Valery Nicolay |
| N I M | : | 22105011 |
| IPK | : |  |

Proposal ini diajukan sebagai persyaratan untuk memulai penulisan tugas akhir.

Proposal I

Semester Gasal 2014/2015

2015

1. **Latar belakang**

Pesatnya perkembangan teknologi, telah membuat banyak perkembangan di dalam kehidupan sehari – hari, seperti berkomunikasi, menyampaikan dan bertukar informasi telah menjadi semakin mudah. Melalui media digital, berkomunikasi menjadi semakin mudah karena tidak terkendala jarak dan waktu dan dapat dilakukan secara *real time*. Tetapi permasalahan muncul ketika seseorang ingin mengirimkan suatu informasi yang bersifat rahasia, media digital yang banyak digunakan saat ini masih mempunyai beberapa kekurangan, sehingga informasi yang ingin dikirimkan rentan terhadap pencurian. Ada beberapa hal yang dapat digunakan untuk mengurangi resiko pencurian data, diantaranya adalah dengan menggunakan enkripsi terhadap informasi yang ingin dikirim. Salah satu teknik enkripsi yang digunakan adalah steganografi

Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui. Teknik steganografi ini menyisipkan pada media lain (*cover object*) yang umum digunakan dalam kehidupan. Pesan yang dikirimkan melalui media yang telah disisipi pesan (*stego-object*) tidak akan mengundang kecurigaan orang lain, karena perbedaannya tidak dapat dilihat secara kasat mata. Media yang paling mudah dimanfaatkan untuk steganografi adalah berkas multimedia. Berkas yang sering dijumpai adalah citra digital.

Dalam tugas akhir ini, peneliti akan membahas mengenai bagaimana suatu pesan disisipkan kedalam pesan lainnya yaitu citra menggunakan metode *Discrete Cosine Transform (DCT), Least Significant Bit (LSB)* ,serta melakukan perbandingan pada kualitas citra yang dihasilkan pada setiap metode.

1. **Rumusan masalah**

Berdasarkan latar belakang masalah diatas, maka rumusan masalah penelitian ini adalah :

1. Bagaimana melakukan penyembunyian dan pengambilan pesan ke dalam citra digital dengan metode  *DCT* dan *LSB*?
2. Bagaimana membandingkan kualitas atau ukuran file antara citra digital asli dengan citra digital yang sudah disisipkan pesan?
3. **Batasan masalah**

Pada penelitian ini penulis membatasi permasalahan dalam ruang lingkup, sebagai berikut :

1. Penyembunyian pesan dilakukan pada citra digital berformat JPEG, PNG, dan BMP 24bit.
2. Algoritma yang digunakan dalam metodeDCT dan LSB*.*
3. Citra digital yang digunakan untuk pengujian adalah *true color*.
4. Aplikasi dibuat pada MATLAB
5. **Tujuan penelitian**

Tujuan dari penelitian ini adalah melakukan analisa citra steganografi melalui pengujian menggunakan metode DCT dan LSB pada format citra yang berbeda.

1. **Landasan teori**
2. **Kriptografi**

Menurut Kamus Besar Bahasa Indonesia, kriptografi adalah penyelidikan tentang kode rahasia;  teknik yang mengubah data menjadi berbeda dari aslinya dengan menggunakan algoritma matematika sehingga orang yang tidak mengetahui kuncinya tidak akan dapat membongkar data tersebut. Dengan kata lain dapat disebut sebagai sebuah cabang ilmu pengetahuan yang mempelajari bagaimana mengamankan data sehingga orang yang tidak mempunyai hak tidak dapat mengakses data tersebut.

Menurut Rakhmat & Fairuzabadi (2010), kriptografi didefinisikan sebagai ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya.

Dari banyak jenis skema yang digunakan untuk kriptografi terdapat 3 jenis kriptografi yaitu.

* Secret key Cryptography

Tipe kriptografi jenis ini hanya menggunakan single key saja. Pengirim membuat key untuk enkrip sebuah pesan dan penerima menggunakan key yang sama untuk melakukan dekrip. Enkripsi jenis ini disebut juga sebagai symmetric encryption. Permasalahan terbesar dari teknik ini adalah distribusi dari key tersebut.

* Public key Cryptography

Tipe kriptografi jenis ini menggunakan dua buah key, yang dapat membuat komunikasi secara aman di jalur yang kurang terjaga keamanannya. Enkripsi jenis ini disebut juga sebagai asymmetric encryption.

Pada metode ini, setiap pihak mempunyai dua buah key yaitu public dan private key. Private key bersifat rahasia dan tidak disebarkan sedangkan public key dibagikan kepada setiap pihak yang ingin berkomunikasi. Jika Alice ingin mengirimkan pesan kepada Bob, maka Alice akan melakukan enkrip menggunakan Bob public key dan Bob akan dapat melakukan dekrip dengan menggunakan private key-nya.

* Hash function

Teknik ini tidak menggunakan key melainkan menggunakan sebuah nilai hash tertentu yang telah dikomputasi kepada sebuah plain text. Fungsi hash digunakan untuk menggecek keabasahan sebuah pesan, untuk meyakinkan bahwa pesan tersebut tidak pernah dimodifikasi oleh pihak lain ataupun terkena virus.

Dalam kehidupan sehari-hari tidak semua informasi yang akan kita berikan kepada seseorang bersifat umum, oleh karena itu informasi yang bersifat bukan untuk komsumsi umum atau pribadi sebaiknya diamankan dengan menggunakan kriptografi.

1. **Steganografi**

Menurut Bhattacharya, Tanmay, Dey (2012), Steganografi adalah proses penyembunyian pesan rahasia didalan sebuah pesan biasa dan melakukan ekstrasi pesan ketika sampai pada tujuannya. Steganografi (*steganography*) berasal dari bahasa Yunani yaitu *steganos* yang berarti tersembunyi atau terselubung, dan *graphein* yang artinya menulis. Steganografi dapat diartikan tulisan tersembunyi (*covered writing*). Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui.

Steganografi membutuhkan dua properti, yaitu media penampung dan pesan rahasia. Media penampung yang umum digunakan adalah gambar, suara, video, atau teks. Pesan yang disembunyikan dapat berupa sebuah artikel, gambar, kode program, atau pesan lain. Proses penyisipan pesan ke dalam media *covertext* dinamakan encoding, sedangkan ekstraksi pesan dari *stegotext* dinamakan decoding. Kedua proses ini mungkin memerlukan kunci rahasia (yang dinamakan *stegokey*) agar hanya pihak yang berhak saja yang dapat melakukan penyisipan pesan dan ekstraksi

1. **Citra Digital**

Citra digital adalah suatu matriks yang terdiri dari baris dan kolom dimana setiap pasang indeks baris dan kolom menyatakan suatu titik pada citra. Nilai dari setiap matriks menyatakan nilai kecerahan titik tersebut. Titik-titik tersebut dinamakan sebagai elemen citra atau *pixel*.Untuk menunjukan tingkat intensitas cahaya suatu *pixel*, seringkali digunakan bilangan bulat warna hitam dan 255 untuk warna putih.

Teknologi dasar untuk menciptakan dan menampilkan warna pada citra digital berdasarkan penelitian bahwa sebuah warna merupakan kombinasi dari tiga warna dasar, yaitu merah, hijau, dan biru (*Red*, *Green*, *Blue* – RGB).

1. **JPEG (Joint Photographic Experts Group)**

*JPEG* merupakan skema kompresi citra bitmap. Karena ukuran file yang relative lebih kecil dan ringan maka format ini digunakan dikalangan fotografer maupun desainer webpage karena mudah ditampilkan pada halaman web.

Keuntungan lain dari format JPEG adalah dapat diterima pada hampir semua program-program komputer. Sedangkan kelemahan dari format JPEG ini adalah kompresi citra pada format ini mempengaruhi kualitas citra itu sendiri.

1. **PNG (Portable Netwok Graphics)**

Tipe file PNG merupakan kompresi citra yang bagus dengan warna yang lebih banyak. Berbeda dengan JPG yang menggunakan teknik kompresi yang menghilangkan data, file PNG menggunakan kompresi yang tidak menghilangkan data (*lossles compression*). Kelebihan file PNG adalah adanya warna transparan dan *alpha*. Warna *alpha* memungkinkan sebuah citra transparan, tetapi citra tersebut masih dapat dilihat mata seperti samar-samar atau bening. Kekurangan dari PNG adalah ukurannya yang besar.

1. **BMP**

Bitmap merupakan representasi dari citra grafis yang terdiri dari susunan titik (*pixel*) yang tersimpan di memori komputer. Nilai setiap titik diawali oleh satu bit data (untuk citra hitam putih) atau lebih (untuk citra berwarna). Kerapatan titik-titik tersebut dinamakan resolusi, yang menunjukkan seberapa tajam citra ini ditampilkan, ditunjukkan dengan jumlah baris dan kolom (contoh 800×600).

Citra bitmap sangat bergantung pada resolusi. Jika citra diperbesar maka citra akan tampak kurang halus atau pecah, sehingga mengurangi detailnya. Selain itu citra bitmap akan mempunyai ukuran file yang lebih besar. Semakin besar

Keuntungan dan kekurangan dari citra bitmap tergantung dari resolusinya. Semakin besar resolusi citra akan semakin besar pula ukuran filenya. Resolusi yang semakin tinggi membuat gambar tidak mudah pecah ketika di zoom.

1. **Discrete Cosine Transform** **(DCT)**

Menurut Uma (2011) DCT merupakan sebuah metode yang telah diterapkan di berbagai bidang pengetahuan. DCT merupakan metode yang mentransfrormasikan sebuah informasi dari domain ruang atau waktu ke dalam domain frekuensi dengan tujuan untuk mempercepat transmisi, mengurangi penyimpanan di dalam memori, menyediakan representasi *compact*, dan sebagainya.

Keunggulan dari DCT adalah memiliki invers yang artinya nilai keluaran setelah transformasi dapat digunakan kembali untuk menghasilkan nilai asli sebelum ditransformasikan. Langkah yang pertama kali dilakukan ketika melakukan proses DCT adalah dengan membagi citra kedalam blok – blok berukuran tertentu. Ukuran blok yang umum digunakan adalah berukuran 8 x 8.

Menurut Nelson, Mark, and Gailly (1996) semakin besar ukuran blok yang digunakan mungkin akan memberikan hasil yang lebih baik, tetapi tidak memakan waktu yang lama hingga mencapai *Point of diminishing returns.* DCT dengan blok berukuran 64x64 mungkin tidak lebih baik dari 4 blok berukuran 16x16. Dan yang membuat lebih jelek adalah, waktu pengerjaan penghitungannya akan lebih lama.

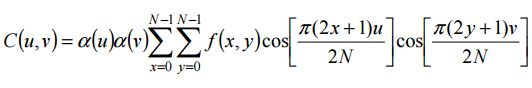


Gambar 1. Proses penyembunyian pesan dengan metode DCT



Gambar 2. Proses ekstrasi pesan

Rumus DCT secara umum[[1]](#footnote-1) adalah sebagai berikut:

****

Dengan α u dan α v = jika u dan v = 0 , dan

bernilai jika kondisi nilai u dan v = 0 tidak terpenuhi.

Dimana :

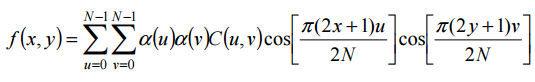
C(u,v) = Nilai pixel hasil transformasi pada baris ke-u dan kolom ke-v

N = Dimensi matriks

f(x,y) = Nilai pixel citra pada baris ke-x dan kolom ke-y

α = konstanta

Dan rumus inver dari DCT[[2]](#footnote-2) adalah sebagai berikut:

****

Dengan α u dan α v = jika u dan v = 0 , dan

bernilai jika kondisi nilai u dan v = 0 tidak terpenuhi.

Dimana :

C(u,v) = Nilai pixel hasil transformasi pada baris ke-u dan kolom ke-v

N = Dimensi matriks

f(x,y) = Nilai pixel citra pada baris ke-x dan kolom ke-y

α = konstanta

1. **Least Significant Bit (LSB)**

Menurut Rakhmat & Fairuzabadi (2010) metode LSB merupakan metode steganografi yang paling sederhana dan mudah diimplementasikan. Metode ini menggunakan citra digital sebagai *covertext*. Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti (*most significant bit* atau MSB) dan bit yang paling kurang berarti (*least significant bit* atau LSB). Sebagai contoh byte 11010010, angka bit 1 (pertama, digaris-bawahi) adalah bit MSB, dan angka bit 0 (terakhir , digaris-bawahi) adalah bit LSB. Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti. Mata manusia tidak dapat membedakan perubahan kecil tersebut.

Misalkan segmen *pixel-pixel* citra/gambar sebelum penambahan bit-bit adalah:

00110011 10100010 11100010 10101011 00100110

10010110 11001001 11111001 10001000 10100011

Pesan rahasia (yang telah dikonversi ke sistem biner) misalkan '1110010111', maka setiap bit dari pesan tersebut menggantikan posisi LSB dari segmen *pixel-pixel* citra menjadi (digarisbawahi):

00110011 10100011 11100011 10101010 00100110

10010111 11001000 11111001 10001001 10100011

1. **Mean Squared Error (MSE) dan Peak Signal to Noise Ratio (PSNR)**

*Peak Signal to Noise Ratio* (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR diukur dalam satuan decibel (dB). Pada penelitian ini, PSNR digunakan untuk mengetahui perbandingan kualitas citra *cover* sebelum dan sesudah disisipkan pesan. Untuk menentukan PSNR, terlebih dahulu harus ditentukan *Mean Square Error* (MSE). Adapun MSE adalah nilai error kuadrat rata-rata antara citra *cover* dengan citra steganografi, secara matematis dapat dirumuskan sebagai berikut:



Diketahui:

MSE = Nilai Mean Square Error citra steganografi

M = Panjang citra stego (dalam *pixel*)

N = Lebar citra stego (dalam *pixel*)

I (x,y) = nilai *pixel* dari citra *cover*

K(x,y) = nilai *pixel* pada citra stego

Setelah diperoleh nilai MSE maka nilai PSNR dapat dihitung dari kuadrat nilai maksimum dibagi dengan MSE. Secara matematis, nilai PSNR dirumuskan sebagai berikut :

Diketahui:

MSE = nilai MSE,

MAXi = nilai maksimum dari *pixel* citra yang digunakan

Semakin rendah Nilai MSE maka akan semakin baik, dan semakin besar nilai PSNR maka semakin baik kualitas citra steganografi. Nilai acuan PSNR bisa dikatakan baik adalah bernilai ≥ 30.

1. **Blok Diagram**



1. **Metodologi penelitian**
2. Studi Literatur

Pada metode studi literatur, dilakukan pencarian dan pemahaman literatur yang berhubungan dengan penelitian guna dibuatnya aplikasi. Literatur yang digunakan meliputi buku referensi dan dokumentasi internet.

1. Analisis data

Pada metode ini penulis mempelajari lebih dalam tentang steganografi, dan metode yang digunakan pada penyembunyian pesan beserta teknik ekstraksinya.

1. Perencanaan dan perancangan

Pada metode ini, dilakukan perencanaan kebutuhan guna proses perancangan aplikasi berdasarkan hasil analisis pada metode sebelumnya.

1. Implementasi

Pada metode implementasi ini, aplikasi sudah dibuat secara keseluruhan pada aplikasi pendukung MATLAB. Aplikasi pada tahap ini sudah siap untuk dilakukan pengujian.

1. Pengujian

Pada metode pengujian, aplikasi yang sudah selesai dibuat untuk kemudian diujikan guna mengetahui apakah aplikasi berjalan dengan lancar tanpa ada kekurangan dan kesalahan serta menganalisa hasil uji citra digital dengan acuan data yang diperoleh dan dengan menganalisa lebih dalam mengenai teknik steganografidan algoritma yang digunakan.

1. **Daftar pustaka**
2. Bhattacharya, Tanmay, Dey, Nilanjan, Chaudhuri, S.R. Bhadra, 2012, “A Session based Multiple Image Hiding Technique using DWT and DCT”, International Journal of Computer Applications, Vol. 38, No. 5
3. Khayam,Syed Ali, “The Discrete Cosine Transform : Theory and Application”, 08-04-2015, www.lokminglui.com/DCT\_TR802.pdf
4. Nelson, Mark, and Gailly, Jean-Loup, 1996, “ The data compression Book, 2nd edition”, M &T Books, New York
5. Rakhmat, Basuki, Fairuzabadi, Muhammad, 2010, “Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vigenere Dan RC4”, Jurnal Dinamika Informatika, Vol. 5, No.2
6. Uma, R., 2011, “FPGA Implementation of 2-D DCT for JPEG Image Compression”, International Journal of Advanced Engineering Sciences and Technologies, Vol. 7, No. 1

Mulyanta, E.S. (2005). “Menjadi Desainer Layout Andal dengan Adobe InDesign”. ANDI. hlm. 175.

Perbandingan algoritma LSB dan DCT pada steganografi oleh Nizar Arif Amrullah 2008 043009

1. Khayam,Syed Ali, “The Discrete Cosine Transform : Theory and Application”, 08-04-2015, hal 7 [↑](#footnote-ref-1)
2. Khayam,Syed Ali, “The Discrete Cosine Transform : Theory and Application”, 08-04-2015, hal 7 [↑](#footnote-ref-2)