

Penyembunyian Pesan Rahasia Dalam Gambar dengan Metoda

JPEG - JSTEG

Hendry Hermawan / 0622097

Email : e3n_17@yahoo.com

Jurusan Teknik Elektro, Fakultas Teknik, Universitas Kristen Maranatha

Jalan Prof. drg. Suria Sumantri, MPH 65, Bandung 40164, Indonesia

ABSTRAK

Di era modern ini, pendistribusian media digital (teks, citra, suara, video, dll) melalui internet banyak dilakukan. Pengamanan dalam pendistribusian media digital perlu dilakukan apabila media digital yang akan didistribusikan bersifat rahasia. Steganografi adalah salah satu teknik penyembunyian pesan, yang dapat berupa teks, citra, suara, dll, dengan cara menyisipkan pesan tersebut pada media digital lain

Discrete Cosine Transform (DCT) banyak digunakan pada teknik steganografi. Pada tugas akhir ini diimplementasikan steganografi dengan metoda *Jpeg- Jsteg* pada suatu citra sebagai media host dan teks sebagai pesan yang akan disembunyikan. Proses DCT dilakukan pada citra yang digunakan sebagai media host dan kemudian dikuantisasi. Pesan rahasia akan disisipkan pada koefisien DCT terkuantisasi. *Run Length Encoding* (RLE) dilakukan untuk proses kompresi sehingga akhirnya dihasilkan citra-stego.

Dari hasil ujicoba, didapat nilai PSNR dan MOS untuk tiap citra. Citra “baboon” yang telah disisipi pesan memiliki nilai PSNR $\geq 30,7$ dB dan nilai MOS $\geq 4,6$. Citra “lena” yang telah disisipi pesan memiliki nilai PSNR $\geq 33,81$ dB dan nilai MOS $\geq 3,4$. Citra “water lilies” yang telah disisipi pesan memiliki nilai PSNR $\geq 30,08$ dB dan nilai MOS ≥ 4 .

Kata Kunci : Steganografi, Jpeg-Jsteg, Discrete Cosine Transform, dan Run Length Encoding.

Hiding Secret Message in an Image with JPEG – JSTEG Method

Hendry Hermawan / 0622097

Email : e3n_17@yahoo.com

Electrical Engineering, Engineering Faculty, Maranatha Christian University

Prof. drg. Suria Sumantri, MPH 65 Street, Bandung 40164, Indonesia

ABSTRACT

In this modern day, the distribution of digital media (texts, images, sounds, videos, etc) throughout the internet is commonly used. The security in digital media distribution has to taken if the digital media which will be distributed is a confidential file. Steganography is one of the techniques for hiding messages (texts, images, sounds, etc) by embedding it to another digital media.

Discrete Cosine Transform (DCT) is often used on stenography techniques. In this final project, steganography is implemented with a Jpeg-Jsteg method on an image as the host media and texts as the secret message. The DCT process is applied to the host image and then quantized. The secret message will be embedded into the quantized DCT coefficient. Run Length Encoding (RLE) is used in data compression process to produce a stego-image.

From the experiments, we obtain the PSNR and MOS value of each image. The “baboon” image that has been embedded with the secret message has a PSNR value of $\geq 30,7$ dB and a MOS value of $\geq 4,6$. The “lena” image that has been embedded with the secret message has a PSNR value of $\geq 33,81$ dB and a MOS value of $\geq 3,4$. The “water lilies” image that has been embedded with the secret message has a PSNR value of $\geq 30,08$ and a MOS value of ≥ 4 .

Keywords : Steganography, Jpeg-Jsteg, Discrete Cosine Transform, and Run Length Encoding

DAFTAR ISI

	Halaman
ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR	iii
DAFTAR ISI	v
DAFTAR TABEL	vii
DAFTAR GAMBAR	viii
BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Perumusan Masalah	2
1.3 Tujuan Tugas Akhir	2
1.4 Pembatasan Masalah	2
1.5 Sistematika Penulisan	2
BAB II LANDASAN TEORI	
2.1 Citra Digital	4
2.1.1 Pembentukan Citra Digital	4
2.2 Steganografi	5
2.2.1 Sejarah Steganografi	7
2.2.2 Kriteria Stegnografi	8
2.3 Jpeg-Jsteg	9
2.4 Discrete Cosine Transform (DCT)	10
2.4.1 Discrete Cosine Transform Dimensi Satu (1-D DCT)	10
2.4.2 Discrete Cosine Transform Dimensi Dua (2-D DCT)	11
2.5 Pengurutan Zig-Zag	13
2.6 Kuantisasi	13

2.7 Run Length Encoding (MOS).....	14
2.8 Warna dan Ruang Warna.....	15
2.8.1 RGB (Red Blue Green).....	15
2.8.2 YCbCr.....	16
2.9 Peak Signal to Noise Ratio (PSNR) dan Mean Square Error (MSE).....	18
2.10 Mean Opinion Score.....	18
BAB III PERANCANGAN DAN REALISASI PERANGKAT LUNAK	
3.1 Gambaran Umum Steganografi	20
1.2 Proses Penyisipan Pesan Rahasia.....	21
3.2.1 Penjelasan Tahapan Proses Penyisipan Pesan Rahasia	25
3.3 Proses Ekstraksi Pesan Rahasia	28
BAB IV PEMBAHASAN DAN HASIL	
4.1 Tampilan Program dan Fungsi Tombol.....	31
4.2 Jenis dan Ukuran Citra Host	33
4.3 Pesan Rahasia yang Disisipkan.....	34
4.4 Hasil Pengujian dan Analisis Percobaan I, II, dan III	34
4.5 Hasil Pengujian dan Analisis Percobaan IV	39
4.6 Hasil Pengujian dan Analisis Percobaan Citra Host dengan Format File Jpeg	40
BAB V KESIMPULAN DAN SARAN	
5.1 Kesimpulan	42
5.2 Saran	42
DAFTAR PUSTAKA	44
LAMPIRAN A CITRA	A-1
LAMPIRAN B PENILAIAN SUBJEKTIF	B-1
LAMPIRAN C PERANGKAT LUNAK.....	C-1

DAFTAR TABEL

	Halaman
Tabel 2.1 Kategori penilaian Mean Opinion Score	19
Tabel 3.1 Tabel kuantisasi standar luminance untuk JPEG	21
Tabel 3.2 Tabel kuantisasi standar chrominance untuk JPEG	22
Tabel 4.1 Citra yang akan digunakan untuk ujicoba	33
Tabel 4.2 Hasil pengujian pada citra “baboon”	34
Tabel 4.3 Hasil pengujian pada citra “lena”	35
Tabel 4.4 Hasil pengujian pada citra “water lilies”	35
Tabel 4.5 Hasil pengujian pada citra berwarna polos	39
Tabel 4.6 Hasil pengujian pada citra “baboon.jpg”	40
Tabel 4.7 Hasil pengujian pada citra “lena.jpg”	41

DAFTAR GAMBAR

		Halaman
Gambar 2.1	Citra digital.....	5
Gambar 2.2	Contoh Jpeg-Jsteg (a) blok 8x8 pixel (b) koefisien DCT (c) koefisien DCT terkuantisasi.....	10
Gambar 2.3	Delapan basis vektor untuk DCT dengan $n = 8$	11
Gambar 2.4	Pengurutan secara zig-zag.....	13
Gambar 2.5	Tabel kuantisasi standar untuk JPEG (a) luminance (b) chrominance.....	14
Gambar 2.6	Ruang warna RGB.....	16
Gambar 2.7	Citra “winter” (a) dalam RGB (b) komponen Y (c) komponen Cb (d) komponen Cr.....	17
Gambar 3.1	Proses penyisipan pesan rahasia.....	21
Gambar 3.2	Diagram alir perhitungan maksimum pesan rahasia yang dapat disisipkan.....	23
Gambar 3.3	Diagram alir penyisipan pesan rahasia.....	24
Gambar 3.4	Nilai Y suatu citra.....	25
Gambar 3.5	Hasil DCT nilai Y.....	25
Gambar 3.6	Hasil kuantisasi koefisien DCT.....	26
Gambar 3.7	Hasil pembulatan nilai DCT koefisien terkuantisasi.....	26
Gambar 3.8	Pengurutan secara zig-zag.....	27
Gambar 3.9	Pesan yang akan disisipkan.....	27
Gambar 3.10	Pesan yang telah dienkrpsi.....	27
Gambar 3.11	Nilai koefisien DCT terkuantisasi yang telah disisipkan pesan	28
Gambar 3.12	Hasil dari proses RLE.....	28
Gambar 3.13	Proses ekstraksi pesan rahasia.....	28
Gambar 3.14	Diagaram alir ekstraksi pesan rahasia.....	30

Gambar 4.1	Tampilan perangkat lunak untuk menyisipkan pesan rahasia	31
Gambar 4.2	Tampilan perangkat lunak untuk mengekstrak pesan rahasia	32
Gambar 4.3	Tampilan proses ekstraksi pesan rahasia citra “baboon” 256x256 yang disisipkan pesan 100% atau 1172 karakter .	37
Gambar 4.4	Gambar 4.4 Perbandingan citra ukuran 256x256 <i>pixel</i> sebelum dan sesudah dilakukan penyisipan 100% kapasitas penyimpanan	38
Gambar 4.5	Perbandingan terhadap citra warna hijau (a) citra host (b) citra yang telah disisipkan pesan rahasia	39
Gambar 4.6	Perbandingan terhadap citra warna hitam (a) citra host (b) citra yang telah disisipkan pesan rahasia	40