MENYEMBUNYIKAN INFORMASI RAHASIA PADA CITRA BITMAP MENGGUNAKAN METODE BIT PLANE COMPLEXCITY SEGMENTATION

I Wayan Simpen[1]
Jurusan Teknik Informatika STMIK Dipanegara Makassar
Alamat : Jl. Perintis Kemerdekaan Km.9 Makassar Telp. (0411) 587194
Email: Dipanegara@dipanegara.ac.id website: http://dipaegara.ac.id

Diterima: 20 April 2012 / Disetujui: 10 Mei 2012

ABSTRACT

With the growing popularity of digital media, attention to the level of security becomes increasingly important. One important issue is the security level of the delivery of information. This can be done using encryption or steganography. Steganography is a method to insert a piece of confidential information in an object other media. Data hiding in steganography and cryptography are very different. If the cryptography, data that was encrypted (ciphertext) remain available, then the steganography, the ciphertext can be hidden so that third parties do not know it existed. In this project, the proposed media is the use of media such as image files JPG, GIF and BMP as input data a secret message carrier (carrier file). By using the method Compexcity Bit Plane Segmentation and DES encryption algorithms expect data confidentiality is guaranteed. The results of this project is to prove a technique of hiding secret messages in the media image. After going through the process and embeding data extraction process again from the stego file, confidential information may be disclosed again without damage or loss of information.

Keywords : confidential information, cryptography, data hiding, steganography

ABSTRAK

Dengan semakin populernya media digital, perhatian pada tingkat keamanan menjadi semakin penting. Salah satu isu penting adalah tingkat keamanan pengiriman suatu informasi. Hal ini dapat dilakukan dengan menggunakan enkripsi atau steganography. Steganography merupakan suatu metode untuk menyisipkan potongan sebuah informasi rahasia dalam suatu objek media lain. Data hiding dalam steganography dan kriptografi sangat berbeda. Jika pada kriptografi, data yang telah disandikan (ciphertext) tetap tersedia, maka dengan steganography, ciphertext dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya. Dalam proyek ini, media yang diajukan adalah penggunaan media image seperti pada file-file JPG, GIF dan BMP sebagai data masukan media pembawa pesan rahasia (carrier file). Dengan menggunakan metode Bit Plane Compexcity Segmentation dan algortima enkripsi DES diharapkan kerahasiaan data lebih terjamin. Hasil proyek ini membuktikan suatu teknik penyembunyian pesan rahasia dalam media image. Setelah melalui proses embeding data dan proses pengekstrakan kembali dari berkas stego, informasi rahasia dapat diungkapkan kembali tanpa mengalami kerusakan atau kehilangan informasi.

Kata kunci : informasi rahasia, kriptografi, data hiding, steganography

PENDAHULUAN

Kebutuhan manusia untuk mengirimkan pesan-pesan rahasia sudah berlangsung lama. Teknik menulis pesan rahasia tersebut disebut *Steganography*. Perkembangan komputer membawa orang ke metode-metode yang lebih rumit dalam menuliskan pesan rahasia. Salah satu metode yang cukup populer adalah dengan menyembunyikan pesan tersebut ke dalam *file* gambar. Pesan tersebut dapat berupa kalimat ataupun gambar disisipkan ke dalam gambar lain. Pengamat yang tidak jeli akan melihat bahwa gambar tersebut tampak seperti gambar umumnya, tetapi jika diproses lebih lanjut pesan yang disisipkan akan muncul. Gambar digital semakin umum digunakan dalam komunikasi internet. Hampir semua halaman

[1] Dosen STMIK Dipanegara Makassar Jurusan Teknik informatika

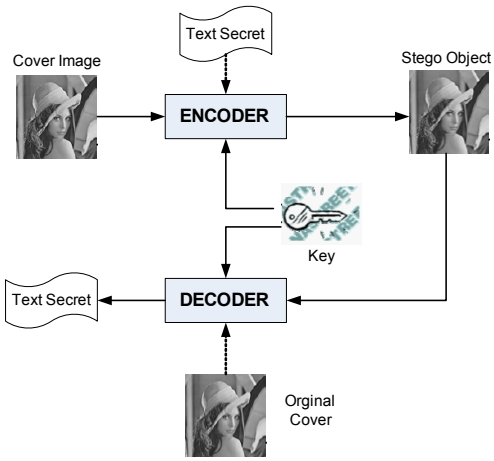
web sekarang ini penuh dengan warna bergambar. Orang senang melihat informasi penuh warna semacam ini di internet. Maka mengirim dan menerima gambar berwarna lewat internet tidak lagi diperhatikan secara khusus.

Sesuai dengan latar belakang masalah yang penulis kemukakan diatas, maka yang menjadi pokok permasalahan adalah bagaimana cara menyisipkan data pada sebuah citra bitmap 24 bit tanpa harus mengubah karakteristik citra digital yang berfungsi sebagai *data – carier*?

BAHAN DAN METODE

Steganography

Steganography (*covered writing*) didefinisikan sebagai ilmu dan seni untuk menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia [4]. Media yang digunakan umumnya merupakan suatu media yang berbeda dengan media pembawa informasi rahasia, dimana disinilah fungsi dari teknik *steganography* yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video. Penggunaan *steganography* antara lain bertujuan untuk menyamarkan eksistensi (keberadaan) data rahasia sehingga sulit dideteksi, dan melindungi hak cipta suatu produk. *Steganography* dapat dipandang sebagai kelanjutan kriptography. Jika pada kriptography, data yang telah disandikan (*ciphertext*) tetap tersedia, maka dengan *steganography ciphertext* dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya. Data rahasia yang disembunyikan dapat diekstraksi kembali persis sama seperti keadaan aslinya.
Gambar berikut menunjukkan bagaimana informasi tersembunyi dapat dipecah ke dalam area berbeda. *Steganography* dapat digunakan untuk menyembunyikan suatu pesan untuk diperoleh kembali oleh suatu individu spesifik atau kelompok. Dalam hal ini bertujuan agar mencegah pesan dapat dideteksi oleh pihak lain.



Gambar 1. Skema Penyisipan Teks ke Media Image

Steganography memiliki hubungan yang erat dengan kriptography, tapi metoda ini sangat berbeda dengan kriptography. Kriptography mengacak pesan sehingga tidak dimengerti, sedangkan *steganography* menyembunyikan pesan sehhingga tidak terlihat. Pesan dalam *ciphertext* mungkin akan menimbulkan kecurigaan sedangkan pasan yang dibuat dengan *steganography* tidak menimbulkan kecurigaan. Kedua teknik ini dapat digabungkan untuk menghasilkan metoda pengiriman pesan rahasia yang sulit dilacak.

Kriteria *Steganography*

Penyembunyian data rahasia ke dalam citra digital akan mengubah kualitas citra tersebuut. Kriteria yang harus diperhatikan dalam penyembunyian data adalah:

1. ***Fidelity***. Mutu citra penampung tidak jauh berubah. Stelah penambahan data rahasia, citra hasil

steganography masih terihat baik. Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.

2. ***Robustness***. Data yang disembunyikan harus tahan (*robust*) terhadap berbagai operasi manipulasi yang dilakukanpada citra penampung, seperti pengubahan kontras, penajaman, pemampatan, rotasi, perbesaran gambar, pemotongan (*cropping*), enkripsi, dan sebagainya. Bila pada citra penampung dilakukan operasi pengolahan citra digital tersebut, maka data yang disembunyikan seharusnya tidak rusak (tetap valid jika diekstraksi kembali)
3. ***Recovery***. Data yang disembunyikan harus dapat diungkapkan kembali (*reveal*). Karena tujuan *steganography* adalah data hiding, maka sewaktu waktu data rahasia di dalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

Bit-Plane Complexity Segmentation BPC

Bit-plane complexity segmentation (*BPCS*) merupakan teknik steganografi yang diperkenalkan oleh Eiji Kawaguchi dan Richard O. Eason pada tahun 1998. Teknik ini merupakan teknik steganografi yang memiliki kapasitas besar, karena dapat menampung data rahasia dengan kapasitas yang relatif besar jika dibandingkan dengan metode steganografi lain seperti *LSB (Least Significant Bit)*. Teknik *BPCS* ini adalah teknik steganografi yang tidak berdasarkan teknik pemrograman, tetapi teknik yang menggunakan sifat penglihatan manusia. Sifat penglihatan manusia yang dimanfaatkan yaitu ketidakmampuan manusia menginterpretasi pola biner yang sangat rumit. Dokumen citra tersebut dibagi menjadi beberapa segmen dengan ukuran 8x8 piksel setiap segmennya (Kawaguchi dan Eason, 1998). Pada dokumen citra 8-bit, setiap satu segmen akan memiliki 8 buah *bit plane* yang merepresentasikan piksel-piksel dari setiap bit tersebut. Proses pembagian segmen 8x8 piksel menjadi 8 buah *bit plane* disebut proses *bit slicing*. Representasi kedelapan *bit plane* ini merupakan *PBC system (Pure Binary Code)*. Pada *BPCS*, proses penyisipan dilakukan pada *bit plane* dengan sistem *CGC (Canonical Gray Code)* karena proses *bit slicing* pada *CGC* cenderung lebih baik dibandingkan pada *PBC* [4]. Sehingga pada proses penyisipan, *bit plane* dengan representasi *PBC* diubah menjadi *bit plane* dengan representasi *CGC*.

Bit Plane

Sebuah citra *multi-valued* dengan kedalaman *n*-bit dapat diuraikan menjadi n-gambar biner (*bit plane*) dengan operasi *bit slicing*. Sebagai contoh, misalkan ada citra *P* dengan kedalaman n-bit, dapat ditunjukkan

$$P = (P1, P2, ..., Pn)$$

Pi merupakan *bit plane* ke-i, dengan i = 1, 2, ..., n.

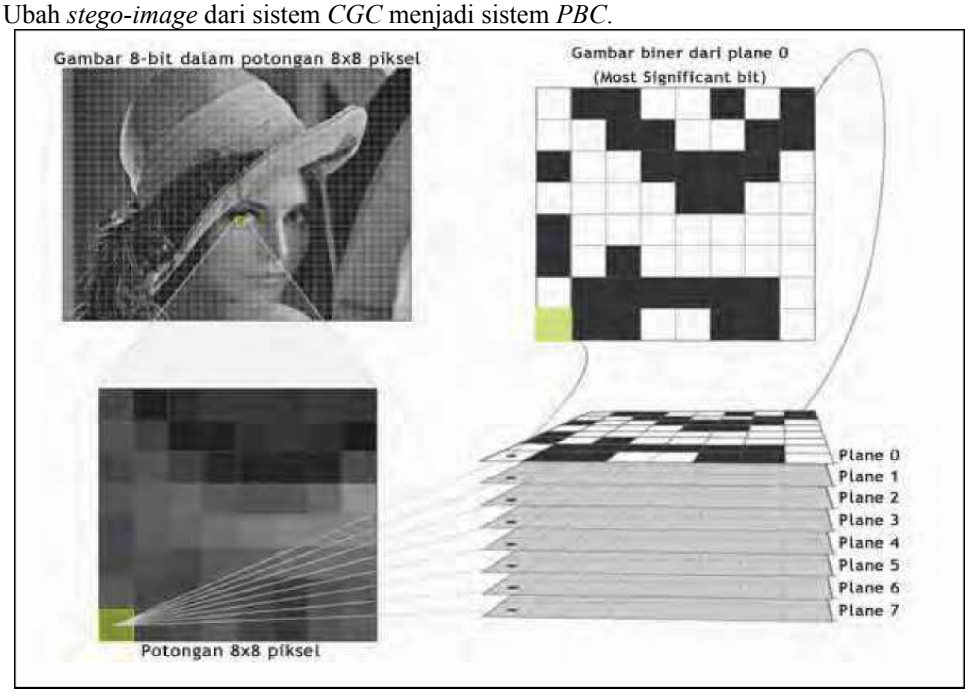
Jika citra *P* terdiri dari 3 warna, *red, green, blue*, maka dapat ditunjukkan
P = (*PR1*, *PR2*, ..., *PRn*, *PG1*, *PG2*, ..., *PGn*, *PB1*, *PB2*, ..., *PBn*)
PRi: *bit-plane* ke-i untuk *red*
PGi: *bit-plane* ke-i untuk *green*
PBi: *bit-plane* ke-i untuk *blue*

Algoritma *Bit-plane Complexity Segmentation (BPCS)*

Menggantikan daerah kompleks dalam tiap–tiap *bit-plane* dari gambar berwarna dengan pola binary acak tidak akan tampak oleh mata manusia. *Property* ini dapat digunakan sebagai strategi penyembunyian informasi. Dalam metode ini gambar wadah disebut sebagai gambar "*dummy*". gambar adalah gambar dalam format bitmap, yang menyembunyikan informasi rahasia (dalam format *file*). Kita membagi tiap file rahasia kedalam serangkaian blok yang masing masing memiliki data 8 byte. Blok tersebut dianggap sebagai pola gambar 8 x 8. blok ini dinamakan sebagai blok rahasia. Algoritmanya melewati tahap sebagai berikut: [4]

1. *Cover image* dengan sistem *PBC* diubah menjadi sistem *CGC*, kemudian gambar tersebut di-*slice* menjadi *bit-plane* dalam bentuk gambar biner. Setiap *bit-plane* mewakili bit dari setiap piksel pada gambar.
2. Segmentasi setiap *bit-plane* pada *cover image* menjadi *informative* dan *noise like region* dengan menggunakan nilai batas/*threshold* (α). Nilai umum dari = 0,3.
3. Kelompokkan *byte-byte* pesan rahasia menjadi rangkaian blok pesan rahasia.
4. Jika blok(*S*) kurang kompleks dibandingkan dengan nilai batas, maka lakukan konjugasi terhadap *S* untuk mendapatkan *S** yang lebih kompleks. Blok konjugasi (*S**) pasti lebih kompleks dibandingkan dengan nilai batas.
5. Sisipkan setiap blok pesan rahasia ke *bit-plane* yang merupakan *noise-like region* (atau gantikan semua bit pada *noise-like region*). Jika blok *S* dikonjugasi, maka simpan data pada "*conjugation map*".

6. Sisipkan juga *conjugation map* seperti yang dilakukan pada blok pesan rahasia.
7. Ubah *stego-image* dari sistem *CGC* menjadi sistem *PBC*.



Gambar 2. Proses Pengubahan Citra Menjadi Segmen-Segmen Bit-Plane

Algoritma untuk *decoding* hanyalah prosedur kebalikan dari langkah memasukkan kode. Inovasi *steganography BPCS* adalah sebagai berikut:

1. Bagian tiap bit-plane dari gambar berwarna ke dalam daerah " *informative*" dan " *noise like*"
2. Pengenalan batas BW (*black – white*) berdasarkan pengukuran kompleksitas (α) untuk pembagian daerah.
3. Pengenalan operasi konjugasi untuk mengubah blok rahasia sederhana menjadi blok yang kompleks.
4. Menggunakan *image* plane CGC dan bukan *image* plane PBC

Algoritma *steganography* BPCS memiliki beberapa para meter untuk penerapan program praktis. Berapa diantaranya adalah

1. Lokasi *header* dari file rahasia
2. Parameter enkripsi dari file rahasia
3. Parameter kompresi dari file rahasia.

Algoritma DES Encryption

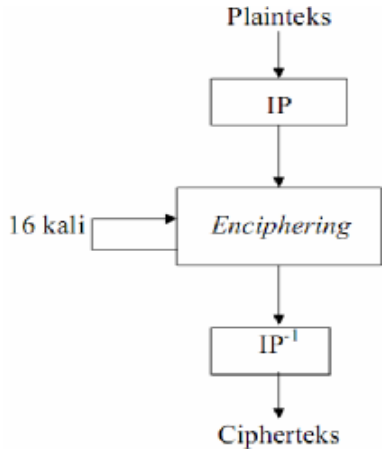
Data Encryption Standard (DES) adalah algoritma *cipher* blok yang populer karena dijadikan standard algoritma enkripsi kunci-simetri, meskipun saat ini standard tersebut telah digantikan dengan algoritma yang baru, *AES,* karena *DES* sudah dianggap tidak aman lagi. Sebenarnya *DES* adalah nama standard enkripsi simetri, nama algoritma enkripsinya sendiri adalah *DEA (Data Encryption Algorithm),* namun nama *DES* lebih populer daripada *DEA*. Algoritma *DES* dikembangkan di *IBM* dibawah kepemimpinan W.L. Tuchman pada tahun 1972. Algoritma ini didasarkan pada algoritma *Lucifer* yang dibuat oleh Horst Feistel. Algoritma ini telah disetujui oleh *National Bureau of Standard (NBS)* setelah penilaian kekuatannya oleh *National Security Agency (NSA)* Amerika Serikat.

DES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis *cipher* blok. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (internal key) atau upa-kunci (*subkey*). Kunci internal dibangkitkan dari kunci eksternal (*external key*) yang panjangnya 64 bit.

Cara kerja Algortima DES

1. Blok plainteks dipermutasi dengan matriks permutasi awal (*initial permutation* atau IP).
2. Hasil permutasi awal kemudian di-enchipering sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.

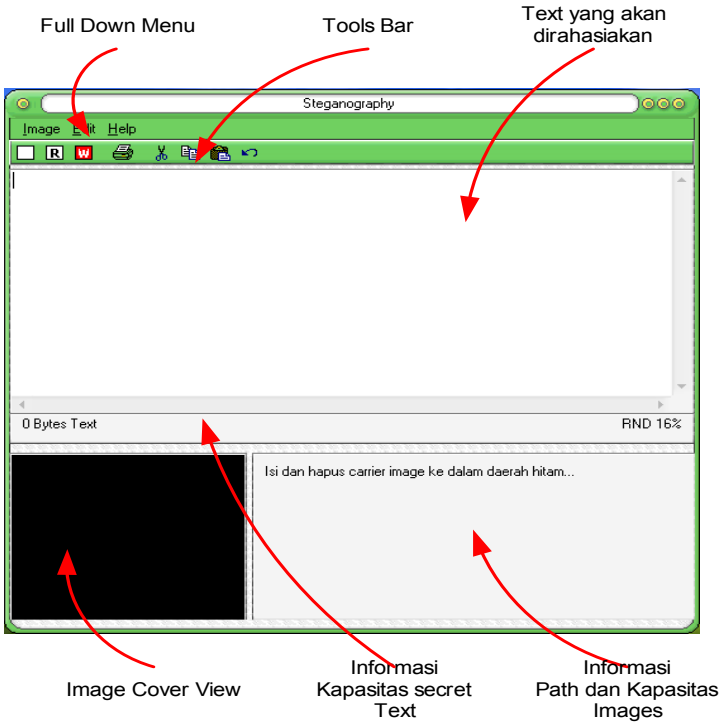
Hasil *enciphering* kemudian dipermutasi dengan matriks permutasi balikan *(invers initial permutation* atau IP^{-1}) menjadi blok cipherteks.



Gambar 3. Skema Global Algoritma DES

HASIL DAN PEMBAHASAN

a. Interface Antar Muka



Gambar 4. Interface Antar Muka

b. Inpmementasi dan Pengujian

Teks Sekret : STMIK DIPANEGARA MAKASSAR

JL. PERINTIS KEMERDEKAAN KM.9 MAKASSAR

Ukuran : 65 Byte

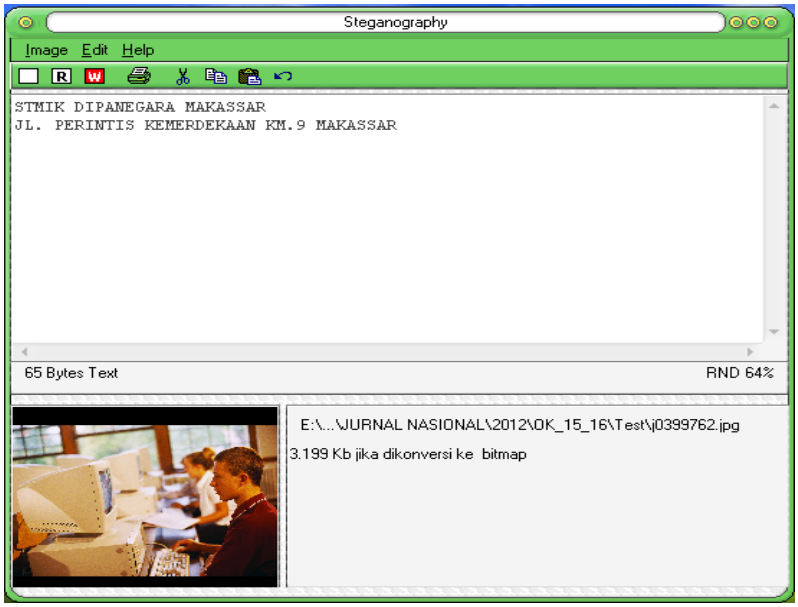
Password : dipanegara

Cover image yang dijadikan percobaan sebagai berikut:

Tabel 1. Daftar Citra JPG Sebagai Sample Test

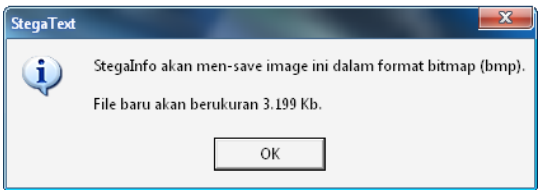
No	Nama image	Tampilan Gambar	Ukuran
1	j0399762.jpg		357 KB
2	j0401257.jpg		833 KB
3	j0406815.jpg		312 KB
4	j0409043.jpg		170 KB
5	j0409045.jpg		234 KB
6	j0409047.jpg		175 KB

Uji coba *Encoding* untuk setiap citra JPG di atas sebagai berikut



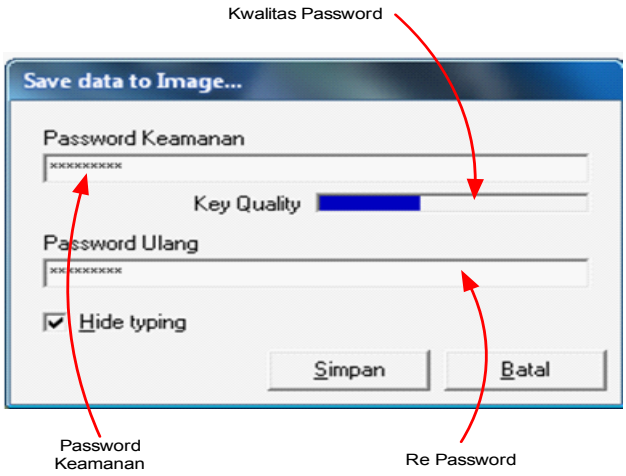
Gambar 5.Penyisipkan Tesks ke dalam Citra

Setelah dipilih citra JPG akan tampil informasi bahwa citra baru dalam format bitmap secara otomatis diubah.

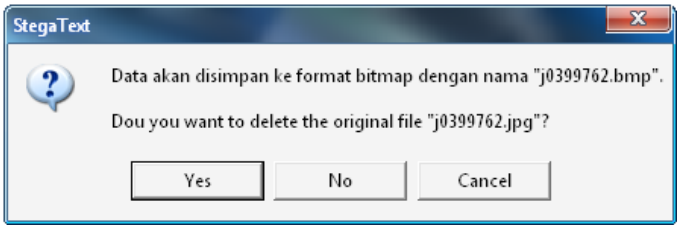


Gambar 6. Informasi bahwa citra diubah ke format bitmap

Proses penyimpanan ke format bitmap akan memasukkan password seperti berikut:

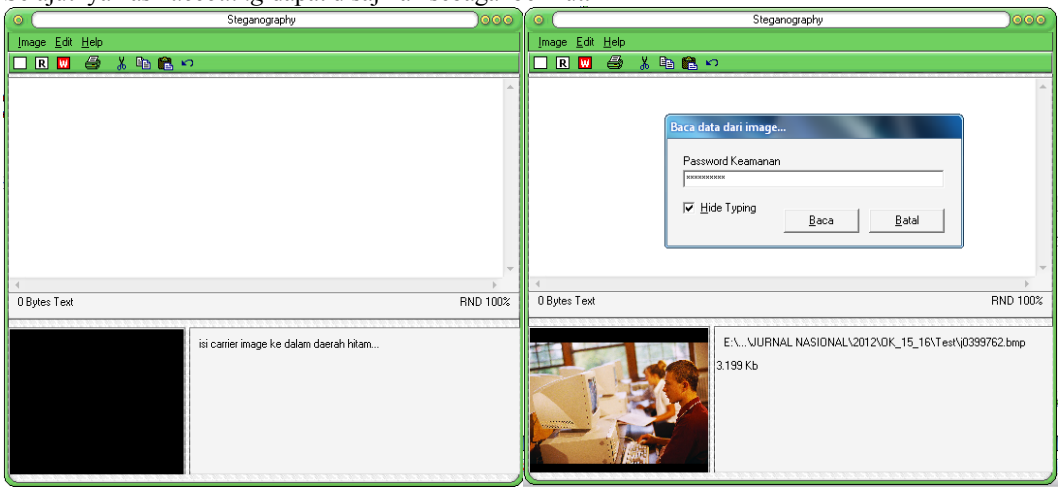


Gambar 7. Input Password dan Kwalitas Password



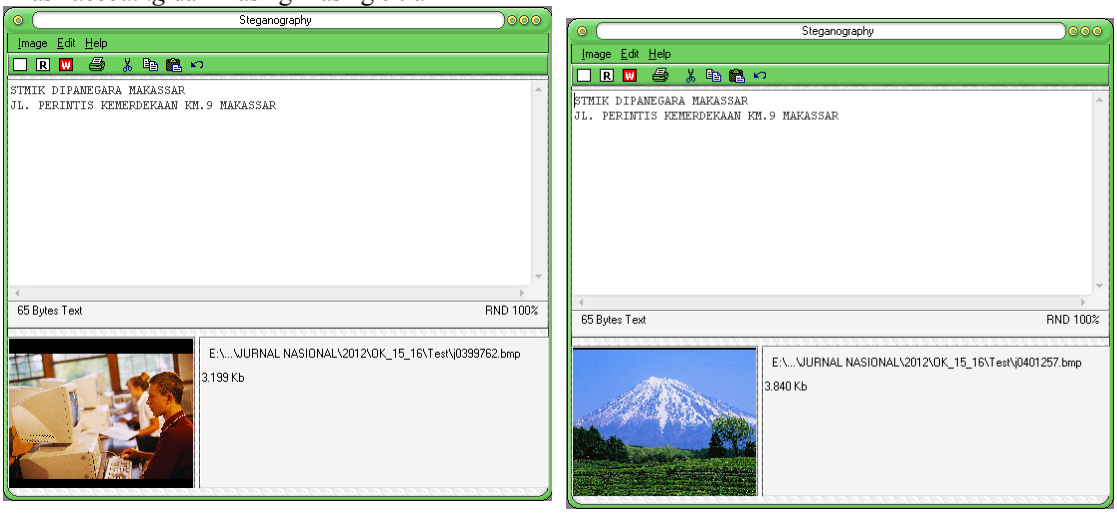
Gambar 8. Konformasi Saat Simpan Citra Tersisipi Text

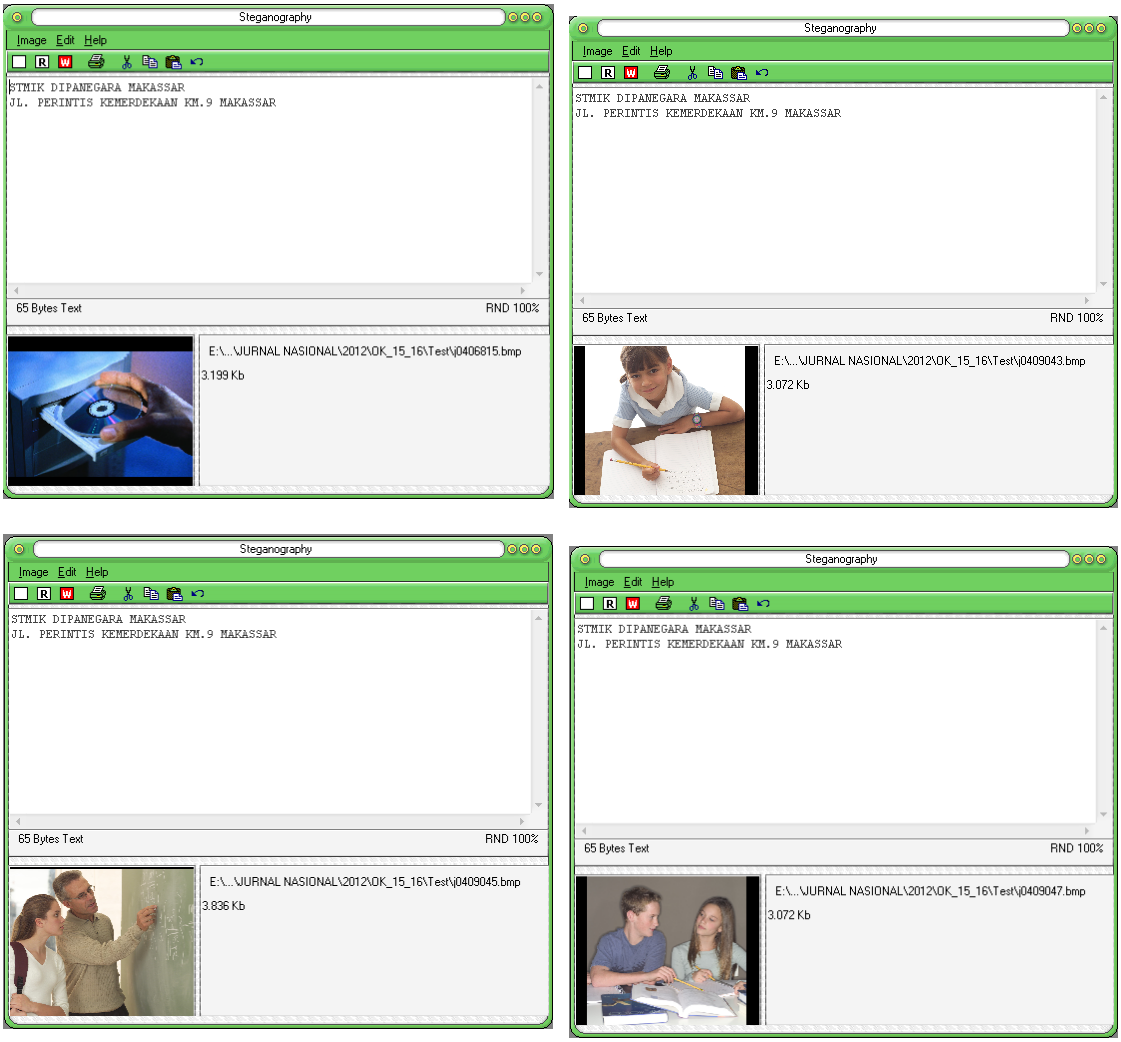
Demikian seterusnya untuk citra yang lainnya sesuai dengan Tabel 1 di atas.
Selajutnya hasil *decoding* dapat disajikan sebagai berikut:



Gambar 9. Decoding Text Hiding

Hasil *decoding* dari masing-masing citra





Gambar 10. Hasil Decoding Text Hiding Masing-Masing Citra

Tabel 1. Daftar Hasil Decoding Citra JPG Sebagai Sample Test

No	Nama image	Tampilan Gambar	Ukuran	Ukuran Baru	Hasil
1	j0399762.jpg		357 KB	3.199 KB	Teks dapat diambil
2	j0401257.jpg		833 KB	3.841 KB	Teks dapat diambil
3	j0406815.jpg		312 KB	3.199 KB	Teks dapat diambil

No	Nama image	Tampilan Gambar	Ukuran	Ukuran Baru	Hasil
4	j0409043.jpg		170 KB	3.073 KB	Teks dapat diambil
5	j0409045.jpg		234 KB	3.837 KB	Teks dapat diambil
6	j0409047.jpg		175 KB	3.073 KB	Teks dapat diambil

KESIMPULAN

Dari uraian diatas dapat ditarik beberapa kesimpulan yang berkaitan dengan proses *steganography* pada citra bitmap 24 bit sebagai berikut:

1. Penyisipan data pada data–carrier tidak merubah karakteristik data–carrier
2. Kemungkinan data tersadap pada saat pengiriman sangat kecil karena menggunakan media cover.
3. *Steganography* menngunakan gambar menurut persepsi manusia. Mata manusia akan sulit membedakan jika sebuah pixels pada sebuah gambar dengan resolusi 24 bit RGB
4. Metode penyisipan data yang digunakan adalah metode *Bit–Plane Complexcity Segmentation*, dalam teknik ini menggunakan karakteristik gambar.
5. Citra masukkan sebagai data carrier hanya citra bitmap 24 bit.
6. Adanya perubahan dalam ukuran file sesudah dan sebelum disisipi teks, hal ini dapat menimbulkan kecurigaan dalam pengiriman data.
7. Proses encode dapat bisa berjalan walaupun dengan file map yang berbeda. Walaupun hasil encode yang dihasilkan berbeda namun hal ini dapat mengurangi tingkat keamanan data.

DAFTAR PUSTAKA

1. Cummins, Jonathan., Diskin , Patrick., Lau, Samuel., and Parlett, Robert., *Steganography And*
2. *Digital Watermarking,* School of Computer Science, The University of Birmingham , 2004 Irianto, *Embedding Pesan Rahasia Dalam Gambar*, Tugas Akhir Matakuliah Keamanan Sistem Lanjut, Magister Teknik Elektro ITB, 2004
3. Johnson, F ,Neil ., *Exploring Steganography: Seeing the Unseen*, George Mason University
4. Kawaguchi, E., and Eason, O, Richard., *Principle and applications of BPCS-Steganography,* Kyushu Institute of Technology, Kitakyushu, Japan
5. Munir, Rinaldi., *Pengolahan citra digital dengan pendekatan algoritmik*, Informatika Bandung, 2005

HASIL REVIEW PAPER Selasa, 12 Juni, 2012 02:43

Dari: "henderi syafei" <henderi@pribadiraharja.com>

Kepada: Dipanegara@dipanegara.ac.id

Cc: "'Henderi Syafei'" <henderi@pribadiraharja.com>, "henderi" <henderi@yahoo.com>

Yth. Bapak I Wayan
Di-
Tempat

Selamat Pagi,

Melalui e-mail ini kami sampaikan hasil review atas paper bapak yang diterima oleh redaksi pelaksana CCIT Journal:

Judul paper:
MENYEMBUNYIKAN INFORMASI RAHASIA PADA CITRA BITMAP MENGGUNAKAN METODE BIT PLANE COMPEXCITY SEGMENTATION

1 Judul : relevan dengan isi dan dengan permasalahan yang dibahas
2 Substansi:
Data/informasi telah diolah cukup baik
Terdapat data/gambar belum cukup jelas relevansinya (gambar belum dianalisis)
3 Kesimpulan: jelas, revelan dengan latar belakang, pembahasan dan sudah baik.
4 Pustaka: terdapat 3 sumber yang tidak diketahui tahun penerbitannya

STATUS: DITERIMA DENGAN MINOR REVISION

Note dari redaksi pelaksana:
1 Paper termasuk dalam daftar yang dinyatakan diterima untuk dimuat di Jurnal CCIT
2 Periode pemuatan pada Jurnal CCIT akan ditetapkan dalam rapat dewan redaksi

Demikian hasil review ini kami sampaikan, dan terimakasih atas partisipasi bapak dalam mengirimkan paper kepada Jurnal CCIT.

Regard,

Henderi Syafei