PENGAMANAN TEXT DENGAN TEKNIK STEGANOGRAFI MENGGUNAKAN METODE *LEAST SIGNIFICANT BIT* (LSB)

Pratomo Djati Nugroho, S.Pi., M.Kom
Dosen STMIK Insan Pembangunan, Bitung. Tangerang.
HP : +6285646684418. Email : nextservo@gmail.com

Mahbubul Wathoni, S.Si., M.Kom
PLP DIKJAR Komputer Matematika Universitas Islam Negeri Syarif Hidayatullah Jakarta.
HP : +628561611408. Email : mahbubul.wathoni@gmail.com

ABSTRAK

Dengan semakin terjangkaunya kamera DSLR dan semakin baiknya kualitas foto pada handphone, membuat masyarakat di indonesia maupun di dunia semakin menggemari dunia fotografi. Di indonesia sendiri banyak pencinta fotografi membuat komunitas-komunitas fotografi dan tidak sedikit dari komunitas-komunitas tersebut melahirkan hasil karya yang cukup baik. Tentu merupakan sebuah kepuasan tersendiri bagi penikmat hobi ini jika hasil gambar yang mereka buat dapat dipublikasi di dalam media sosial, sehingga dapat diakses oleh banyak orang. Namun, dengan hal tersebut disalah gunakan oleh beberapa oknum yang tidak bertanggung jawab. Sehingga terjadi pengakuan hak milik karena citra tersebut tidak memiliki tanda kepemilikan. Salah satu teknik yang dapat dipakai untuk menangani hal tersebut adalah steganografi. Steganografi merupakan ilmu dan seni yang mempelajari cara penyembunyian informasi rahasia ke dalam suatu media sedemikian rupa sehingga manusia tidak dapat menyadari keberadaan pesan tersebut. Penelitian ini membahas tentang penerapan steganografi pada berkas gambar dan metode steganografi yang digunakan adalah metode *Least Significant Bit* (LSB) untuk menyisipkan text ke dalam citra hasil fotografi dan AES untuk enskripsi text sisipan. Dari hasil uji coba, diketahui bahwa dengan metode *Least Significant Bit* (LSB) penyisipan dan ekstraksi pesan dapat dilakukan dengan baik. Jenis pesan yang dapat disisipkan adalah pesan text.

Kata kunci: Steganografi, Gambar, Text, *Least Significant Bit* (LSB), AES.

PENDAHULUAN

1. Latar Belakang Masalah

Banyak kita jumpai beberapa situs fotografi salah satunya www.fotografer.net. Dimana dalam situs tersebut para fotografer dapat menampilkan atau menyuguhkan karya-karya mereka sehingga dapat dinikmati masyarakat banyak. Media seperti ini memang sangat positif bagi para fotografer untuk menilai diri mereka mengenai kemampuan seni dan teknik mereka dalam tiap komentar yang diberikan oleh para pengunjung situs.

Terkadang hal positif tentu diikuti dengan hal yang negatif. Para oknum-oknum yang tidak bertanggung jawab mulai menyelewengkan fasilitas situs ini. Beberapa penyimpangan tersebut dapat berupa peng-copy-an data atau citra hasil fotografer kemudian diakui sebagai hak cipta oknum-oknum tersebut. Sehingga banyak para fotografer menambahkan nama mereka atau logo ciri khas mereka pada hasil foto mereka dan mengurangi nilai keindahan foto tersebut.

Oleh karena itu, salah satu teknik untuk mengamankan data citra tersebut dari pengakuan hak cipta orang lain adalah dengan menggunakan steganografi. Steganografi adalah teknik menyamarkan atau menyembunyikan pesan ke dalam sebuah media pembawa (*carrier)*. Kelebihan steganografi terletak pada sifatnya yang tidak menarik perhatian atau kecurigaan orang lain.

Salah satu media yang dapat digunakan sebagai *carrier* adalah berkas gambar. Teknik steganografi pada berkas gambar memanfaatkan kelemahan penglihatan manusia, karena kualitas gambar antara berkas gambar asli dengan berkas gambar yang telah disisipkan pesan rahasia tidak jauh berbeda. Salah satu metode steganografi gambar yang sering digunakan *Least Significant Bit* (LSB). Metode ini diterapkan dengan mengganti bit-bit yang tidak terlalu berpengaruh dari berkas gambar dengan bit-bit pesan.

Adapun tujuan dari penelitian ini adalah menerapkan steganografi pada berkas gambar dengan menggunakan metode *Least Significant Bit* (LSB). Metode *Least Significant Bit* (LSB) ini diujicoba untuk melakukan proses penyisipan dan ekstraksi tanda hak cipta.

Dimana jenis tanda hak cipta yang dapat disisipkan adalah sebuah text.

2. Rumusan Masalah

Dari latar belakang yang telah dipaparkan sebelumnya, dapat kita menarik sebuah rumusan sebagai berikut:

”Bagaimana mengimplementasikan steganografi – watermarking terhadap sebuah citra dengan menyisipkan text dalam sebuah komputer?”

3. Batasan Masalah

Implementasi aplikasi ini, dibuat dengan batasan sebagai berikut:

1. Images yang akan di proses adalah images yang ber-extention *.jepg dan hasil proses adalah *.png.
2. Text yang akan di sisipkan bisa di encripsi terlebih dahulu atau tidak, sesuai kebutuhan.
3. Proses enskripsi data terhadap text yang disisipkan menggunakan AES. Program dibuat dengan menggunakan Bahasa pemrograman C# (CShrap) [2][21] dengan Visual Studio 2010 sebagai developer toolsnya.

DASAR TEORI

2.1 Steganografi

2.1.1 Pengertian Steganografi

Steganografi merupakan suatu ilmu atau seni dalam menyembunyikan informasi dengan memasukkan informasi tersebut ke dalam pesan lain. Dengan demikian keberadaan informasi tersebut tidak diketahui oleh orang lain.

Tujuan dari steganografi adalah menyembunyikan keberadaan pesan dan dapat dianggap sebagai pelengkap dari kriptografi yang bertujuan untuk menyembunyikan isi pesan. Oleh karena itu, berbeda dengan kriptografi, dalam steganografi pesan disembunyikan sedemikian rupa sehingga pihak lain tidak dapat mengetahui adanya pesan rahasia. Pesan rahasia tidak diubah menjadi karakter ‘aneh’ seperti halnya kriptografi. Pesan tersebut hanya disembunyikan ke dalam suatu media berupa gambar, teks, musik, atau media digital lainnya dan terlihat seperti pesan biasa.

Dalam steganografi dikenal beberapa terminologi. *Cover-data* atau *cover-text* merupakan media penyembunyi pesan. Sedangkan hasil penggabungan antara *cover data* dengan pesan yang disembunyikan disebut *stego-text, stego-data* atau *stego-object*. Algoritma yang menghasilkan *stego text* disebut *stegosystem*. Pihak yang menciptakan *stegosystem* disebut steganografer.

Secara umum *stegosystem* terdiri dari tiga tahap yaitu algoritma untuk mendapatkan kunci, mengkodekan pesan, dan men-*decode* pesan. Algoritma tersebut dibungkus dalam suatu teknik tehnik penyembunyian pesan yang bermaca-macam [1][3][7][9][10][23].

2.1.2 Sejarah Steganografi

Steganografi adalah seni dan sains untuk menulis pesan tersembunyi dengan cara tertentu sehingga tidak seorangpun selain si pengirim dan si penerima akan menyadari ada sebuah pesan tersembunyi. Singkatnya, kriptografi mengacak arti dari sebuah pesan, tetapi kriptografi tidak menutupi kenyataan bahwa ada sebuah pesan dalam media tertentu.

Kata steganografi berasal dari bahasa Yunani yang berarti tertutup atau tulisan tersembunyi. Steganografi sudah dikenal sejak 440 SM. Herodotus menyebutkan dua contoh steganografi di dalam “*Histories of Herodotus*”. Demeratus mengirimkan peringatan akan serangan Yunani yang selanjutnya dengan menuliskan pesan tersebut di atas sebuah papan kayu dan melapisinya dengan lilin.

Keuntungan steganografi jika dibandingkan dengan kriptografi adalah bahwa pesan-pesan tidak menarik perhatian terhadap pesan itu sendiri, terhadap pengirim atau terhadap si penerima. Sebuah pesan kode yang tidak tersembunyi, tidak peduli serumit apapun pesan tersebut diacak, akan menimbulkan kecurigaan dan keterbatasan karena di beberapa negara kriptografi dicap illegal [1][3][7][9][10][23].

2.1.3 Kriteria Steganografi

Kriteria yang harus diperhatikan dalam melakukan penyembunyian data dengan menggunakan teknik steganografi adalah sebagai berikut :

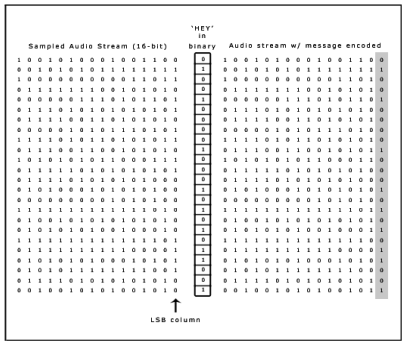
1. *Imperceptibility* : Keberadaan pesan dalam media penampung tidak dapat dideteksi.
2. *Fidelity* : Mutu media penampung setelah ditambahkan pesan rahasia tidak jauh berbeda dengan mutu media penampung sebelum ditambahkan pesan.
3. *Recovery* : Pesan rahasia yang telah disisipkan dalam media penampung harus dapat diungkap kembali.
4. *Robustness* : Pesan yang disembunyikan harus tahan terhadap berbagai operasi

manipulasi yang dilakukan pada media penampung [1][3][7][9][10][23].

2.1.4 Metode Steganografi

Metode-metode umum yang digunakan untuk menyembunyikan data dalam sebuah digital images antara lain [1][3][7][9][10][23]:

1. *Least Significant Bit Insertion* (LSB)
   Metode ini adalah metode yang sangat popular dimana LSB dari setiap byte dalam sebuah citra digunakan untuk menyimpan data rahasia (Gambar 2.1).

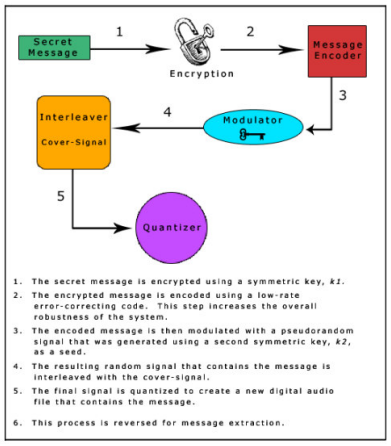


Gambar 2.1 *Least Significant Bit* (LSB)

2. *Masking* dan *Filtering*
   Kedua metode ini menyembunyikan informasi dengan cara mirip dengan penanda kertas. Hal ini dapat dilakukan, contohnya dengan memodifikasi luminance sebagian dari citra, tetapi apabila dilakukan dengan hati-hati distorsi baru dapat terlihat [6][18].

3. *Transformations*
   Discrete Cosine Transformation (DCT) adalah salah satu metode transformasi untuk mentransformasi 8*8 blok pixel dari sebuah citra secara berurutan kedalam masing-masing koefisien 64 DCT. Alat steganografi dapat menggunakan LSB dari koefisien DCT yang terbagi-bagi utnuk menyembunyikan informasi (metode JSteg). Sebagai tambahan DCT, citra dapat diproses dengan FFT atau dengan Wavelet Transformation. Properti citra yang lain seperti luminance juga dapat dimanipulasi.

4. *Spread Spectrum Image Steganography*
   Metode-metode yang didasari oleh teknologi ini menyandikan pesan yang diinginkan agar tersembunyi. Untuk menyandikan, digunakan sebuah *pseudorandom noise generator* yang lebar untuk membuat sebuah barisan yang tersebar. *Inner leaver* juga dapat mempergunakan kunci untuk mendikte algoritma interleaving. Sinyal ini sekarang digabungkan dengan cover dari citra untuk menghasilkan citra stego, yang sudah dibagi-bagi dengan layak untuk memelihara dynamic range awal dari cover citra. Citra stego tersebut kemudian diteruskan kepada penerima pesan. Untuk lebih jelasnya, lihat gambar berikut:



Gambar 2.2 *Spread Spectrum*

2.2 Watermark

Pada dasarnya, teknik *watermark* adalah proses penambahan kode identifikasi secara permanent kedalam data digital. Kode identifikasi tersebut dapat berupa teks, suara, gambar, atau video. Selain tidak merusak data digital yang dilindungi, kode identifikasi seharusnya memiliki ketahanan (*robustness*) terhadap bebagai pemrosesan lanjutan seperti pengubahan, kompresi, enkripsi, dan lain sebagainya.

Teknologi yang semakin maju memunculkan fenomena-fenomena baru yang berkembang di masyarakat, salah satunya adalah citra digital. Citra digital sudah menjadi kebutuhan yang cukup penting untuk beberapa kalangan, dari perusahaanperusahaan besar seperti penggunaan citra digital pada GPS (*Global Positioning System*), sampai dengan perorangan.

Kebutuhan seperti ini disebut kebutuhan **verifikasi** citra. Kebutuhan lain yang muncul adalah kebutuhan **otentikasi** citra yaitu kebutuhan kepemilikan (*copyright*) suatu citra digital. *Watermarking* dapat menjadi solusi untuk menyelesaikan kedua masalah tersebut. *Watermarking* yaitu teknik menyisipkan suatu informasi ke dalam data multimedia. Informasi tersebut dapat berupa data data citra, audio, ataupun video yang menggambarkan kepemilikan suatu pihak. Informasi yang

disisipkan tersebut disebut *watermark*. *Watermark* dapat dianggap sebagai sidik digital dari pemilik data multimedia tersebut, dalam hal ini berupa citra digital [1][8][11][12][14][15][16][20][22][24][25].

2.2.1 Tujuan Penggunaan *Watermark*

Dokumen merupakan representasi riwayat organisasi secara eksplisit. Dokumen dalam bentuk elektronik dapat memudahkan pembukaan serta penelusuran isi dari riwayat dokumen tersebut yang sebelumnya susah untuk dilakukan pada dokumen dalam bentuk kertas, memungkinkan pembagian informasi (*information sharing*) yang efektif, serta dapat memberikan kontribusi pada penyebarluasan pengetahuan pada lingkungan-lingkungan terkait.

Penyisipan *watermark* pada dokumen memiliki berbagai macam tujuan. Untuk aplikasi perlindungan hak cipta, tanda yang disisipkan pada dokumen (gambar, teks atau audio) digunakan sebagai identifier yang menunjukkan hak kepemilikan atau hak penggunaan dokumen. Jenis tanda air mempengaruhi keefektifan tanda air itu sendiri dalam setiap aplikasinya. Baik tanda air *perceptible* maupun *imperceptible*, keduanya dapat mencegah terjadinya penyalahgunaan, namun dengan cara yang berbeda. Tanda air digital digunakan untuk memberikan identifikasi sebuah dokumen atas informasi sumber daya, penulis, kreator, pemilik, distributor, dan konsumer yang berhak atas dokumen tersebut.

2.2.2 Karakteristik Watermark

Ada beberapa karakteristik yang diinginkan dari penggunaan *watermark* pada suatu dokumen, diantaranya tidak dapat terdeteksi (*imperceptible*), *robustness*, *security, fragility* dan *tamper resistance*.

1. *Imperceptible*: memberikan karakteristik *watermark* agar sebisa mungkin harus tidak dapat terlihat atau berbeda dengan dokumen aslinya. Hal ini dimaksudkan untuk tidak merubah status dokumen yang bernilai tinggi secara hukum maupun komersial.

2. *Robustness*: Karakteristik ini tergantung aplikasi dari *watermark* itu sendiri. Apabila digunakan sebagai identifikasi kepemilikan atau *copyright*, *watermark* harus memiliki ketahanan terhadap berbagai macam modifikasi yang mungkin bisa dilakukan untuk merubah/menghilangkan *copyright*. Jika digunakan untuk otentikasi *content*, *watermark* sebisa mungkin bersifat *fragile*, sehingga apabila isinya telah mengalami perubahan, maka *watermark* akan mengalami perubahan atau rusak, sehingga dapat terdeteksi adanya usaha modifikasi terhadap isi.

3. *Security*: Teknik *watermark* harus dapat mencegah usaha-usaha untuk mendeteksi dan memodifikasi informasi watermark yang disisipkan ke dalam dokumen. Kunci *watermark* menjamin hanya orang yang berhak saja yang dapat melakukan hal tersebut. Namun aspek ini tidak dapat mencegah siapapun untuk membaca dokumen yang bersangkutan.

4. *Fraggility*: berlawanan dengan *robust*, konsep ini menghendaki *watermarking* bersifat rapuh. Tentu saja hal ini dilakukan dalam beberapa aplikasi tertentu. Sebagai contoh adalah *watermarking* fisik yang diberikan pada surat-surat yang berharga yang dibuat sehingga *watermarking* tersebut tidak akan tahan terhadap proses pengkopian. Tujuannya tentu saja untuk menjaga keotentikannya. Kelihatannya pembuatan *watermarking* itu sengaja didesain rapuh terhadap beberapa modifikasi, namun juga tahan terhadap modifikasi tertentu. Jenis *watermarking* ini biasanya tidak diimplementasikan dalam bentuk digital.

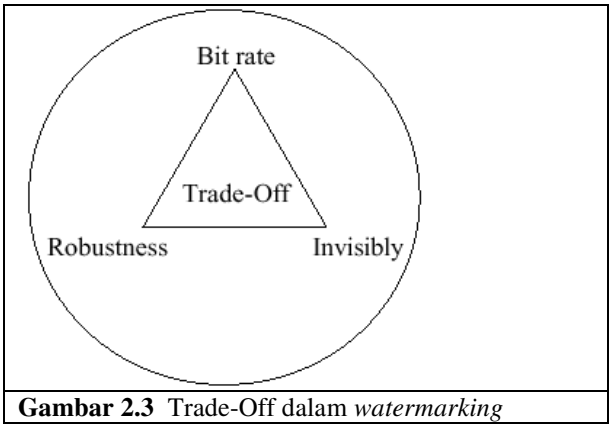
5. *Tamper Resistance*: konsep ini menghendaki *watermarking* tahan terhadap segala modifikasi yang dilakukan terhadap sinyal media yang memang dilakukan dengan tujuan untuk menghilangkan *watermarking*, dibandingkan dengan konsep *robust* yang menghendaki ketahanan terhadap sinya media. Modifikasi dengan tujuan semacam ini dinilai berhasil jika mampu merusak *watermarking* tanpa menurunkan kualitas sinyal media secara drastis. Penurunan kualitas ini tentunya dinilai secara *perceptual* bersifat signifikan sehingga jika *watermarking* rusak, maka sinyal media akan mengalami penurunan kualitas secara pendengaran.

2.2.3 Trade-Off dalam *Watermarking*

Parameter-parameter yang diperlukan dalam penerapan *watermarking*:

1. Jumlah data (*bit rate*) yang akan disembunyikan,
2. Ketahanan (*robustnes*) terhadap proses pengolahan sinyal.

Terdapat suatu *trade-off* diantara kedua parameter (*bitrate* dan *robustness*) tersebut dengan *Invisibly* (tidak tampak). Bila diinginkan *robustness* yang tinggi maka *bitrate* akan menjadi rendah, sedangkan akan semakin *visibl*e, dan sebaliknya semakin *invisible* maka *robustness* akan menurun. Jadi harus dipilih nilai-nilai dari parameter tersebut agar memberikan hasil yang sesuai dengan yang kita inginkan (sesuai dengan aplikasi). Hubungan *Invisibility* dengan *Robustness* dapat diterangkan sebagai berikut: misalkan suatu data asli diubah (ditambah atau dikurangi) sesedikit mungkin dengan maksud memberikan efek *invisible* yang semakin tinggi, maka dengan adanya sedikit proses pengolahan digital saja, perubahan tadi akan berubah/hilang. Dengan demikian dikatakan *robustness* rendah, tetapi *invisibility* tinggi.



Gambar 2.3 Trade-Off dalam *watermarking*

2.2.4 *Masking* dan *Filtering*

Teknik *masking* dan *filtering*, hanya terbatas ke gambar 24-bit dan gray-scale, informasi disembunyikan dengan menandai suatu gambar dengan cara seperti *paper watermark*. Teknik *watermarking* dapat di aplikasikan dengan resiko rusaknya gambar dalam kaitannya dengan *lossy compression,* sebab mereka lebih menyatu ke dalam gambar.

Masking lebih *robust* dari pada penyisipan LSB dengan hasil kompresi, *cropping*, dan beberapa pemrosesan gambar. Tehnik masking menempelkan informasi dalam area significant sehingga pesan yang tersembunyi itu lebih bersatu dengan gambar cover dari pada penyembunyian dalam level "noise" [6][18].

2.2.5 Penyisipan *Watermark*

Loop melalui piksel gambar. Dalam setiap iterasi, mendapatkan nilai RGB masing-masing dalam bilangan bulat terpisah. Untuk masing-masing R, G, dan B, membuat LSB sama dengan 0. Bit ini akan digunakan dalam menyembunyikan karakter.Dapatkan karakter saat ini dan mengubahnya ke integer. Kemudian menyembunyikan 8 bit yang di R1, G1, B1, R2, G2, B2, R3, G3, di mana angka mengacu pada jumlah piksel. Dalam setiap LSB elemen (dari R1 ke G3), menyembunyikan bit karakter berturut-turut. Ketika 8 bit karakter diproses, melompat ke karakter berikutnya, dan ulangi proses sampai semua teks diproses. Teks dapat disembunyikan di bagian kecil dari gambar sesuai dengan panjang teks. Jadi, harus ada sesuatu untuk menunjukkan bahwa di sini kita mencapai akhir teks. Indikator ini hanya 8 nol secara berurutan. Hal ini akan dibutuhkan ketika mengekstrak teks dari gambar [16].

2.2.6 Ekstraksi *Watermark*

Hanya melewati piksel gambar sampai Anda menemukan 8 nol secara berurutan. Seperti Anda lewat, memilih LSB dari setiap elemen pixel (R, G, B) dan melampirkan ke nilai kosong. Ketika 8 bit nilai ini dilakukan, mengubahnya kembali ke karakter, kemudian menambahkan karakter bahwa untuk hasil teks yang Anda cari.

2.2.7 *Watermarking* untuk Pelabelan Hak Cipta

Masalah Hak Cipta dari dahulu sudah menjadi hal yang utama dalam segala ciptaan Manusia, ini digunakan untuk menjaga *originalitas* atau *kreatifitas* pembuat akan hasil karyanya. Hak cipta terhadap data-data digital sampai saat ini belum terdapat suatu mekanisme atau cara yang handal dan efisien, dikarenakan adanya berbagai faktor-faktor tadi (faktor-faktor yang membuat data digital banyak digunakan).

Beberapa cara yang pernah dilakukan oleh orang-orang untuk mengatasi masalah pelabelan hak cipta pada data digital, antara lain [13] [14]:

- *Hearder Marking*; dengan memberikan keterangan atau informasi hak cipta pada header dari suatu data digital.

- *Visible Marking*; merupakan cara dengan memberikan tanda hak cipta pada data digital secara eksplisit.

- *Encryption*; mengkodekan data digital ke dalam representasi lain yang berbeda dengan representasi aslinya (tetapi dapat dikembalikan ke bentuk semula) dan memerlukan sebuah kunci dari pemegang hak cipta untuk mengembalikan ke representasi aslinya.

- *Copy Protection*; memberikan proteksi pada data digital dengan membatasi atau dengan memberikan proteksi sedemikian rupa sehingga data digital tersebut tidak dapat diduplikasi.

Cara-cara tersebut diatas memiliki kelemahan tersendiri, sehingga tidak dapat banyak diharapkan sebagai metoda untuk mengatasi masalah pelabelan hak citpa ini. Contohnya:

- *Header Marking*; Dengan menggunakan software sejenis Hex Editor, orang lain dengan mudah membuka file yang berisi data digital tersebut, dan menghapus informasi yang berkaitan dengan hak cipta dan sejenisnya yang terdapat di dalam header file tersebut.

- *Visible Marking*; Penandaan secara eksplisit pada data digital, memang memberikan sejenis tanda semi-permanen, tetapi dengan tersedianya software atau metoda untuk pengolahan, maka dengan sedikit ketrampilan dan kesabaran, tanda yang semipermanen tersebut dapat dihilangkan dari data digitalnya.

- *Encryption*; Penyebaran data digital dengan kunci untuk decryption tidak dapat menjamin penyebarannya yang legal. Maksudnya setelah data digital terenkripsi dengan kuncinya telah diberikan kepada pihak yang telah membayar otoritas (secara legal), maka tidak dapat dijamin penyebaran data digital yang telah terdekripsi tadi oleh pihak lain tersebut.

- *Copy Protection*; Proteksi jenis ini biasanya dilakukan secara hardware, seperti halnya saat ini proteksi hardware DVD, tetapi kita ketahui banyak data digital saat ini tidak dapat diproteksi secara hardware (seperti dengan adanya Internet) atau dengan kata lain tidak memungkinkan dengan adanya proteksi secara hardware.

Dengan demikian, kita memerlukan suatu cara untuk mengatasi hal yang berkaitan dengan pelanggaran hak cipta ini, yang memiliki *sifat-sifat* seperti:

- *Invisible atau inaudible*; Tidak tampak (untuk data digital seperti citra, video, text) atau tidak kedengaran (untuk jenis audio) oleh pihak lain dengan menggunakan panca indera kita (dalam hal ini terutama mata dan telinga manusia).

- *Robustness*; Tidak mudah dihapus/diubah secara langsung oleh pihak yang tidak bertanggung jawab, dan tidak mudah terhapus/terubah dengan adanya proses pengolahan sinyal digital, seperti kompresi, filter, pemotongan dan sebagainya.

- *Trackable*; Tidak menghambat proses penduplikasian tetapi penyebaran data digital tersebut tetap dapat dikendalikan dan diketahui.

Teknik *watermarking* tampaknya memiliki ketiga sifat-sifat diatas, karena faktor-faktor *invisibility* dan *robustness* dapat kita atur, dan data yang terwatermark dapat diduplikasi seperti layaknya data digital. *Watermarking* sebagai metoda untuk pelabelan hak cipta dituntut memiliki berbagai kriteria (ideal) sebagai berikut agar memberikan unjuk kerja yang bagus:

- Label Hak Cipta yang unik mengandung informasi pembuatan, seperti nama, tanggal, dst, atau sebuah kode hak cipta seperti halnya ISBN (*International Standard for Book Notation*) pada buku-buku.

- Data terlabel tidak dapat diubah atau dihapus (*robustness*) secara langsung oleh orang lain atau dengan menggunakan software pengolahan sinyal sampai tingkatan tertentu.

- Pelabelan yang lebih dari satu kali dapat merusak data digital aslinya, supaya orang lain tidak dapat melakukan pelabelan berulang terhadap data yang telah dilabel.

METODE PENELITIAN

3.1 Metode Pengumpulan Data

3.1.1 Studi Pustaka

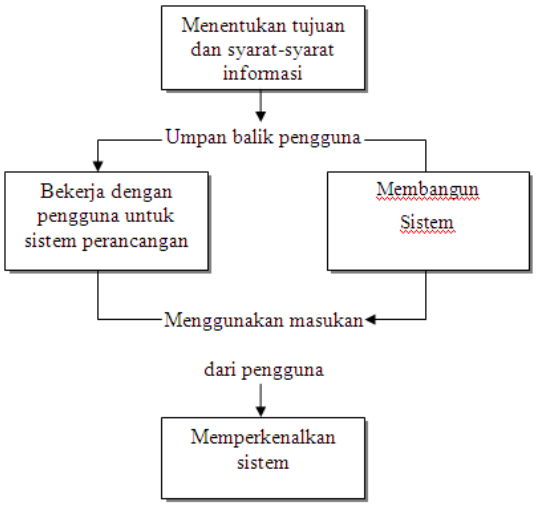
Dengan metode ini, penulis mendapatkan informasi apa saja yang berkaitan dengan steganografi melalui buku-buku referensi dan mencari melalui berbagai situs–situs di internet yang berkaitan, sehingga penulis dapat mengumpulkan data dan informasi yang diinginkan.

3.1.2 Studi Literatur

Penulis mencoba mencari perbandingan dengan studi sejenis dari beberapa penulisan di beberapa karya ilmiah, seperti jurnal dan skripsi.

3.2 Metode Pengembangan Sistem

Model Rapid Application Development adalah pendekatan berorientasi objek yang digunakan terhadap pengembangan sistem yang mencakup suatu metode pengembangan perangkat-perangkat lunak. Model RAD adalah proses pengembangan perangkat lunak sekuensial linear yang menekankan siklus pengembangan yang pendek. Hal ini akan mempersingkat waktu dalam perancangan dan berusaha memenuhi syarat-syarat bisnis yang cepat berubah. Metode ini diperkenalkan oleh James Martin pada tahun 1991. Ilustrasi mengenai RAD ditujukan pada Gambar 3.1.



Gambar 3.1 Skema Sistem Model RAD

3.3 Spesifikasi Komputer

a. Spesifikasi Hardware

Dalam pembuatan program aplikasi ini digunakan komputer dengan spesifikasi sebagai berikut :

1. Processor : Pentium I5 2.3GHz
2. RAM : 8 GB
3. Harddisk : 500 GB
4. Monitor : 14” LED

b. Spesifikasi Software

Spesifikasi software yang digunakan dalam pembuatan program aplikasi ini adalah :

1. Visual Studio 2010
2. Sistem Operasi Windows 7

3.4 Cara Kerja Program Aplikasi

Pada saat program pertama kali dijalankan, akan muncul form menu utama seperti pada gambar dibawah ini.

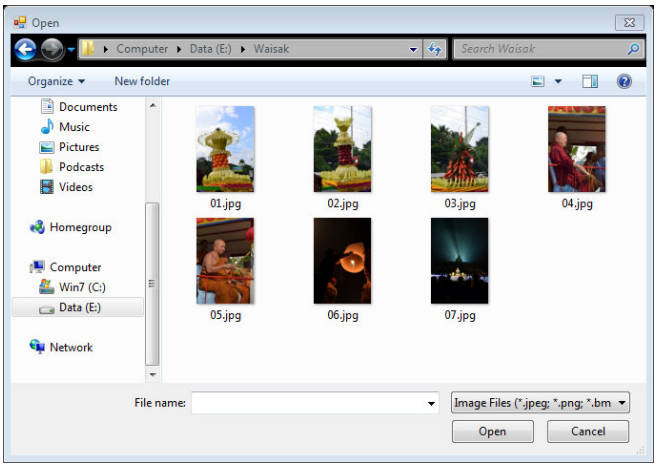
Gambar 3.2 Form Menu Utama

3.4.1 Proses Penyisipan

Jika user ingin melakukan penyisipan pesan gambar maka user harus memilih Menu File > Open > Images.

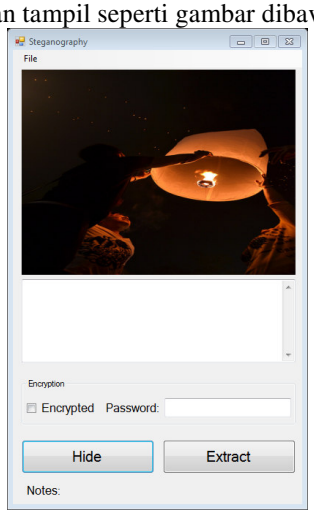
Gambar 3.3 Form Menu Pilih Images

Setelah itu akan tampil *dialog box* untuk memilih file gambar seperti gambar berikut.



Gambar 3.4 Dialog box pilih file gambar

Setelah dipilih gambar yang diinginkan maka akan tampil seperti gambar dibawah ini.

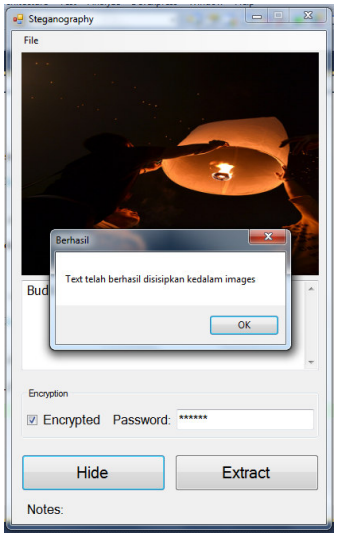


Gambar 3.5 Tampilan setelah pilih gambar

Setelah itu akan dilanjutkan dengan menginput text yang ingin disisipkan lalu checklist Encrypted dan masukan password seperti gambar berikut.

Gambar 3.6 Input text

Setelah itu tekan tombol hide maka akan tampil seperti gambar berikut ini.



Gambar 3.7 Tampilan setelah pilih tekan tombol hide

Setelah itu diwajibkan menyimpan file yang telah disisipkan text seperti pada gambar dibawah ini.

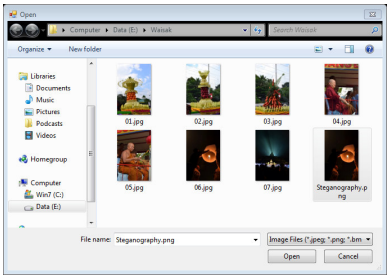
Gambar 3.8 Tampilan simpan file

3.4.3 Proses Ekstraksi

Jika user ingin melakukan ekstraksi terhadap gambar stego maka user harus memilih images yang sudah di sisipkan text dengan memilih menu File > Open > Images Gambar Seperti gambar berikut.

Gambar 3.9 Form Pilih Images

Setelah itu akan tampil *dialog box* untuk memilih file gambar yang sudah di sisipkan text seperti gambar berikut.

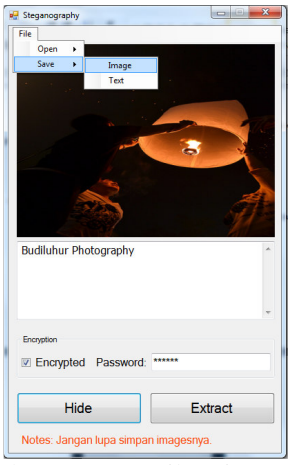


Gambar 3.10 Dialog box pilih file gambar steganografi

Setelah itu akan dilanjutkan dengan checklist Encrypted dan masukan password sebelumnya untuk mendecript lalu tekan tombol extrct maka akan memunculkan pesan text seperti gambar berikut

Gambar 3.11 Tampilan memunculkan pesan

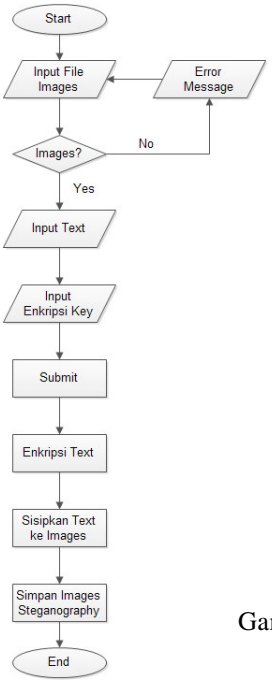
Setelah itu file yang telah ter extract seperti pada gambar dibawah ini.



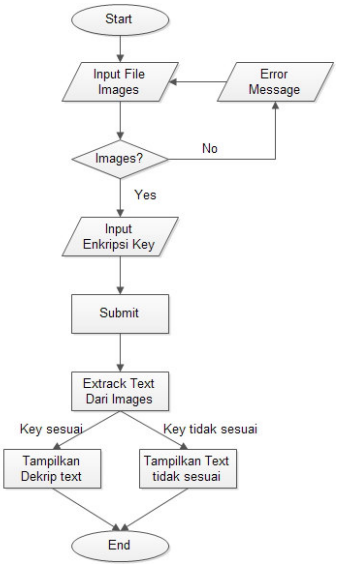
Gambar 3.12 Tampilan simpan file

3.5 FLOWCHART ALGORITMA

Berikut adalah gambar flowchat saat proses penyisipan pesan :



Gambar 3.13 Flowchart Encode



Gambar 3.14 Flowchart Decode

HASIL DAN ANALISA

4.1 Hasil

Pada percobaan ini, dilakukan terhadap enam gambar dengan dimensi yang sama (333 x 500 pixel) serta ukuran gambar yang berbeda, yang akan disisipkan dengan sebuah text. Berikut ini contoh enam gambar yang ingin diuji coba :

Tabel 4.1 Gambar yang akan disisipkan text

Gambar 1

Gambar 2

Gambar 3

Gambar 4

Gambar 5

Gambar 6

Dari kelima gambar di atas, akan kita lakukan percobaan penyisipan text dan akan kita lihat besar perubahan ukuran file dan juga perubahan yang terjadi setelah dilakukan penyisipan text. Text yang akan kira masukan adalah “Buliluhur Photography” dengan key “waisak”.

4.2 Analisa

Dari Hasil Penyisipan text ke dalam gambar, didapatkan data berikut ini:

Tabel 4.2 Perbedaan antara citra masukkan dengan hasilnya

Nama Gambar	*Dimensi Gambar Sebelum disisipkan logo (pixel)*	*Ukuran Gambar Sebelum disisipkan logo*	*Ukuran Gambar Setelah disisipkan logo*	*Dimensi Gambar Sesudah disisipkan logo(pixel)*	*Prosentase perubahan ukuran citra*
01.jpg	333 x 500	125 kb	488 kb	333 x 500	390.4 %
02.jpg	333 x 500	136 kb	488 kb	333 x 500	358.8 %
03.jpg	333 x 500	131 kb	488 kb	333 x 500	372.5 %
04.jpg	333 x 500	113 kb	488 kb	333 x 500	431.8 %
05.jpg	333 x 500	56.3 kb	488 kb	333 x 500	866.8 %
06.jpg	333 x 500	38.1 kb	488 kb	333 x 500	1280.8 %

Citra Asli

Citra Hasil Watermarking

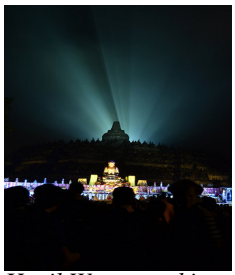
Citra Asli

Citra Hasil Watermarking


Citra Asli *Citra Hasil Watermarking*


Citra Asli *Citra Hasil Watermarking*


Citra Asli *Citra Hasil Watermarking*

Citra Asli *Citra Hasil Watermarking*

KESIMPULAN

5.1 Kesimpulan

1. Teknik steganografi dengan metode *Least Significant Bit* (LSB) untuk menyembunyikan pesan teks pada gambar bitmap dapat diaplikasikan menggunakan C# (Csharp).
2. Kriptografi dan steganografi dapat diintegrasikan menjadi satu dalam sebuah sistem aplikasi. Pesan teks terlindungi dengan algoritma kriptografi dan tersembunyi dalam sebuah gambar.

5.2 Saran

1. Teknik steganografi dapat dikembangkan untuk implementasi penyisipan pesan ke dalam media lain seperti audio dan video.
2. Implementasi steganografi pada gambar perlu dikembangkan untuk dapat mengimplementasikan proses penyisipan pesan ke dalam format gambar selain gambar seperti JPG dan PNG.
3. Perlu pengembangan untuk teknik steganografi agar dapat menyisipkan data/file ke dalam media penyamar.
4. Implementasi program perlu dikembangkan untuk dapat berfungsi dalam berbagai sistem operasi, seperti Linux dan MacOSX.

DAFTAR PUSTAKA

[1] Ahmad Ni'ami Wafi. Steganografi dan Watermarking. http://guritac-tecnologi4.blogspot.com/2010/04/steganografi-dan-watermarking.html. Diakses tanggal 14 Mei 2014.

[2] Anonymous. Csharp. http://www.csharp-station.com/tutorial.aspx. Diakses tanggal 14 Mei 2014.

[3] Anonymous. Steganografi. http://agcrypt.wordpress.com/2007/11/30/steganografi-sebagai-salah-satu-teknik-penyandian-data/. Diakses tanggal 14 Mei 2014.

[4] Bayu Adi Persada. Studi dan Implementasi Non Blind Watermarking dengan Metode Spread Spectrum. Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung.

[5] Cogierb201. Teknik Menyembuyikan Pesan dengan Steganografi. http://cogierb201.wordpress.com/2012/05/08/teknik-menyembuyikan-pesan-dengan-steganografi/. Diakses tanggal 14 Mei 2014.

[6] Fitri Susanti. Steganografi Pada Image Digital dengan Masking – Filtering. http://digilib.ittelkom.ac.id/index.php?option=com_repository&Itemid=34&task=detail&nim=113058009. Diakses tanggal 14 Mei 2014.

[7] Harry da Vinci Faozisokhi Hulu. Steganografi. http://davinzhu87.blogspot.com/2011/09/steganografi.html Diakses tanggal 14 Mei 2014.

[8] Harry da Vinci Faozisokhi Hulu. Teknologi Watermarking Pada Citra Digital.

http://davinzhu87.blogspot.com/2011/08/teknologi-watermarking-pada-citra.html. Diakses tanggal 14 Mei 2014.

[9] Indrakrn. Steganografi. http://rjuhedy.wordpress.com/2010/05/05/steganografi/. Diakses tanggal 14 Mei 2014.

[10] Indrakrn. Steganografi. http://user36.wordpress.com/2008/06/09/steganografi-adalah-suatu-ilmu-teknik-dan-seni-tentang-bagaimana-menyembunyikan-data-rahasia-didalam-wadah-media-digital-sehingga-keberadaan-data-rahasia-tersebut-tidak-diketahui-oleh-orang-lain/. Diakses tanggal 14 Mei 2014.

[11] I Gede Supaca Darma Tuladi. Digital Watermarking. http://digilib.ittelkom.ac.id/index.php?option=com_content&view=article&id=479:digital-watermarking&catid=20:informatika&Itemid=14. Diakses tanggal 14 Mei 2014.

[12] Lusia Rakhmawati dan Hapsari Peni A.T. Pengembangan Teknik Watermarking Untuk Deteksi Kerusakan dan Memperbaiki Citra Digital Warna. Jurusan Teknik Elektro, Fakultas Teknik, Unesa Gedung A5 Lantai 3, Kampus Unesa, Jalan Ketintang. Surabaya.

[13] Mulaab. Teknik Watermarking dalam Domain Wavelet untuk Proteksi Kepemilikan pada Data Citra Medis. Laboratorium Pemrograman, Jurusan Teknik Informatika Universitas Trunojoyo Madura.

[14] Mirko Luca Lobina and Luigi Atzori. Masking Models and Watermarking : A Discussion on Methods and Effectiveness. University of Cagliari, Italy.

[15] Muhammad Zulkurnain Pancawardana. Watermark. http://digilib.ittelkom.ac.id/index.php?option=com_content&view=article&id=865:watermark&catid=21:itp-informatika-teori-dan-pemograman&Itemid=14. Diakses tanggal 14 Mei 2014.

[16] Prahadi Digdoyo, Rosny Gonydjaja dan Rina Refianti Mutiara. Penyisipan Watermark Pada Citra Grayscale Berbasis SVD. Universitas Gunadarma. Jakarta.

[17] Rep. Penggunaan Watermark Pada Foto dalam Penerapan Fungsi Digital Right Management. http://edukasi.kompasiana.com/2012/12/11/penggunaan-watermark-pada-foto-dalam-penerapan-fungsi-digital-right-management-515028.html. Diakses tanggal 14 Mei 2014.

[18] Sony Nuryadin Syarifuddin. Analisis Filtering Citra dengan Metode Mean Filter dan Median Filter. Jurusan Teknik Informatika Fakultas Teknik dan Ilmu Komputer Universitas Komputer Indonesia.

[19] The SilverBullet. Steganografi. http://chandra-halimy.blogspot.com/2010/04/steganografi.html. Diakses tanggal 14 Mei 2014.

[20] Wiki. Steganography and Digital Watermarking. http://wiki.cas.mcmaster.ca/index.php/Steganography_and_Digital_Watermarking. Diakses tanggal 14 Mei 2014.

[21] Wikipedia. C Sharp (programming language). http://en.wikipedia.org/wiki/C_Sharp_%28programming_language%29. Diakses tanggal 14 Mei 2014.

[22] Wikipedia. Digital Watermarking. http://en.wikipedia.org/wiki/Digital_watermarking. Diakses tanggal 14 Mei 2014.

[23] Wikipedia. Steganografi. http://id.wikipedia.org/wiki/Steganografi. Diakses tanggal 14 Mei 2014.

[24] Wikipedia. Watermark. http://en.wikipedia.org/wiki/Watermark. Diakses tanggal 14 Mei 2014.

[25] Wikipedia. Watermarking. http://id.wikipedia.org/wiki/Watermarking. Diakses tanggal 14 Mei 2014.