Penggunaan Steganografi dengan Metode *End of File* (EOF) pada *Digital Watermarking*

Martono[#1], Irawan[#2]

[#]*Program Pascasarjana Magister Ilmu Komputer – Universitas Budi Luhur*
Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, Indonesia (12260)
Telp. (021)5853753, Fax.(021)5853752
[1]martono_libra@yahoo.com
[2]irend_irawan@yahoo.co.id

***Abstraksi*— Salah satu karya yang dilindungi adalah barang dalam bentuk digital, seperti *software* dan produk multimedia seperti teks, musik, gambar, dan video digital. Selama ini penggandaan atas produk digital tersebut dilakukan secara bebas. Ini akan menimbulkan sisi negatif yaitu jika tidak ada hak cipta pelindung terhadap file digital yang disebarkan tersebut, maka file digital tersebut akan sangat mudah diakui kepemilikannya oleh pihak lain. Salah satu cara untuk melindungi hak cipta tersebut adalah dengan menyisipkan informasi ke dalam data tersebut dengan teknik *watermarking*. Teknik *watermarking* adalah proses menambahkan kode identifikasi secara permanen ke dalam data digital atau bisa disebut juga dengan *digital watermarking*. Kode identifikasi tersebut dapat berupa teks, gambar, suara, atau video. Metode yang digunakan untuk penyisipan watermark dalam aplikasi digital *watermarking* ini adalah metode *End Of File* (EOF). Metode EOF bekerja dengan cara menyisipkan informasi atau pesan ke dalam sebuah file, dimana informasi atau pesan disisipkan di akhir file tersebut.**

***Kata Kunci*— Steganografi, *End Of File (EOF), Digital Watermarking*.**

Abstract*— *One of the works that are protected in the form of digital goods , such as software and multimedia products such as text , music , images , and digital video . So far, doubling over the digital products done freely . This will cause the negative side is if there is no copyright protection against the spread of digital files , the digital files will be very easily recognized ownership by other parties . One way to protect copyright is to insert information into the data with watermarking techniques . Watermarking technique is the process of adding a permanent identification code into digital data or can be referred to as digital watermarking . The identification code can be text , images , sounds , or video . The method used for embedding watermark in digital watermarking applications are methods End Of File (EOF) . EOF method works by inserting information or messages into a file , in which the information or message is inserted at the end of the file.

***Keywords*— *Steganography, End Of File (EOF), Digital Watermarking*.**

I. PENDAHULUAN

Pada saat ini media digital telah menggantikan peran media analog dalam berbagai aplikasi. Hal ini disebabkan karena kelebihan yang dimiliki media digital. Kemudahan penyebaran (pendistribusian) file digital melalui berbagai media, diantaranya melalui media internet memiliki sisi positif dan negatif terutama bagi pemilik file digital tersebut. Sisi positif dari kemudahan penyebaran (pendistribusian) tersebut adalah dengan cepatnya pemilik file digital dapat menyebarkan (mendistribusikan) file digital tersebut ke berbagai tempat di dunia. Sedangkan sisi negatifnya adalah jika tidak ada hak cipta pelindung terhadap file digital yang disebarkan tersebut, maka file digital tersebut akan sangat mudah diakui kepemilikannya oleh pihak lain.

Digital *watermarking* dikembangkan sebagai salah satu jawaban untuk melindungi hak cipta suatu file digital. Dengan diterapkannya *digital watermarking* ini maka hak cipta file digital yang dihasilkan akan terlindungi dengan cara menyisipkan informasi tambahan seperti informasi kepemilikan file (bisa berupa teks ataupun gambar / logo) ke dalam file digital tersebut.

Digital watermarking merupakan aplikasi dari steganografi. Steganografi adalah suatu ilmu dan seni untuk menyembunyikan (*embedded*) informasi atau pesan dengan cara menyisipkan informasi atau pesan tersebut di dalam file lain sedemikian rupa sehingga orang lain tidak menyadari ada informasi atau pesan di dalam file tersebut. Informasi atau pesan tersebut dapat berupa teks, gambar, suara (audio), video, dan file lainnya. Digital *watermarking* merupakan salah satu teknik penyembunyian informasi atau pesan yang fungsinya untuk melindungi hak milik (hak cipta), *copyright*, dan sebagainya. *Digital watermarking* memiliki beberapa jenis teknik yang memiliki keunggulan dan kelemahan masing-masing. Biasanya teknik *watermarking* yang kuat (susah dipecahkan oleh berbagai serangan) memiliki kualitas *watermark* yang kurang memuaskan, sedangkan teknik *watermarking* yang menghasilkan kualitas *watermark* yag memuaskan biasanya kurang kuat menghadapi serangan.

Metode atau teknik yang digunakan pada digital *watermarking* dalam jurnal ini adalah *End Of File* (EOF).

Metode *End Of File* (EOF) bekerja dengan cara menyisipkan informasi atau pesan ke dalam sebuah file, dimana informasi atau pesan disisipkan di akhir file tersebut.

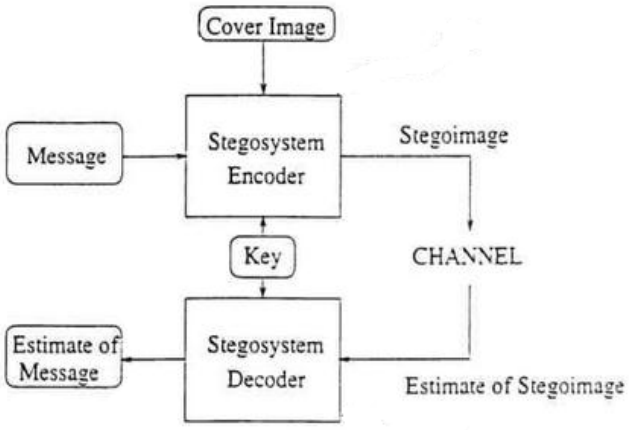
II. DASAR TEORI

A. *Definisi Steganografi*

Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan dengan suatu cara sehingga selain *sender* dan *receiver*, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia [1]. Kata steganografi (*steganography*) berasal dari bahasa Yunani yaitu *steganos* yang artinya tersembunyi atau terselubung dan graphein, yang artinya menulis, sehingga kurang lebih artinya adalah menulis sesuatu yang tersembunyi atau terselubung.

Penggunaan steganografi antara lain bertujuan untuk menyamarkan keberadaan data rahasia sehingga sulit dideteksi dan melidungi hak cipta suatu produk. Steganografi dapat dipandang sebagai kelanjutan kriptografi. Jika pada kriptografi, data yang telah disandikan (*ciphertext*) tetap tersedia, maka dengan steganografi *ciphertext* dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya. Data rahasia yang disembunyikan dapat diekstraksi kembali persis sama seperti keadaan aslinya. Steganografi membutuhkan dua poperti 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, daftar barang, kode program atau pesan lain.

Keuntungan steganografi dibandingkan dengan kriptografi adalah bahwa pesan yang dikirim tidak menarik perhatian sehingga media penampung yang membawa pesan tidak menimbulkan kecurigaan bagi pihak ketiga. Ini berbeda dengan kriptografi dimana *ciphertext* menimbulkan kecurigaan bahwa pesan tersebut merupakan pesan rahasia. Berikut gambaran dari aliran proses steganografi :



Gbr 1. Aliran Proses Steganorafi [2]

B. *Kriteria Steganografi*

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

- *Imperceptibility* [3]

Keberadaan pesan rahasia tidak dapat dipersepsi oleh inderawi. Misalnya jika *covertext* berupa citra, maka penyisipan pesan membuat citra *stegotext* sukar dibedakan oleh mata dengan citra *covertext* nya. Jika *covertext* berupa *audio*, maka indera telinga tidak dapat mendeteksi perubahan pada audi stegotext-nya.

- *Fidelity* [4]

Mutu citra penampung tidak jauh berubah. Setelah penambahan data rahasia, citra hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.

- *Robustness* [5]

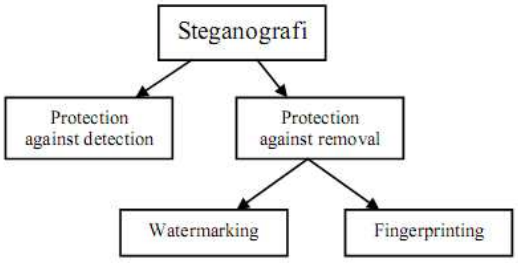
Data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada citra penampung. Bila pada citra dilakukan operasi pengolahan citra, maka data yang disembunyikan tidak rusak.

- *Recovery* [5]

Pesan yang disembunyikan harus dapat diungkap kembali (*reveal*). Karena tujuan steganografi adalah data *hiding*, maka sewaktu-waktu pesan rahasia di dalam *stegotext* harus dapat diambil kembali untuk digunakan lebih lanjut.

C. *Pembagian Steganografi*

Berikut ini gambaran dari pembagian steganografi :



Gbr 2. Pembagian Steganorafi

1) Protection aginst detection [2]

Model proteksi ini banyak digunakan dalam dunia maya sebagai *security tools* dalam suatu pengiriman data atau dokumen melalui *internet* atau media lainnya. Proteksi ini mempunyai metode agar suatu file/media sampul yang telah disisipi data tidak dapat dideteksi oleh steganalisis, sehingga data yang dikirimkan aman sampai orang yang ditujukan.

2) Protection against removal [2]

Model proteksi ini banyak digunakan dalam media digital *security.* Biasanya model ini berfungsi sebagai penanda hak cipta (*copyright*) agar tidak dapat dihilangkan maupun diganti oleh pihak-pihak lain yang tidak bertanggung jawab. Pada metode ini terdapat dua metode yang dapat digunakan, yaitu *watermarking* dan *fingerprinting*. *Watermarking* merupakan satu bentuk metode dari steganografi dalam mempelajari

teknik-teknik bagaimana penyimpanan suatu data digital kedalam data sampul digital yang lain. Parameter-parameter yang ada dalam penerapan metode *watermarking* adalah jumlah data yang disembunyikan (*bit rate*), ketahanan terhadap proses pengolahan sinyal (*robustness*), tak terlihat atau output tidak berbeda dengan input awal (*invisibilty*).

D. *Metode Steganografi*

Berikut beberapa metode steganografi untuk perbandingan :

1) Metode Least Significant Bit (LSB)

Salah satu metode steganografi yang banyak digunakan adalah metode modifikasi LSB (*Least Significant Bit*)**.** Metode modifikasi LSB tergolong metode yang menggunakan teknik substitusi. Metode LSB terutama digunakan untuk steganografi berbasis media (*media-based steganography*) [6].

Metode LSB menyembunyikan data rahasia dalam bit-bit tak signifikan (*least significant bit*) dari berkas wadah (*cover*). Pengubahan tersebut pada dasarnya memberikan pengaruh terhadap berkas wadah, tetapi karena perubahan yang terjadi sangat kecil, sehingga tidak tertangkap oleh indra manusia. Kenyataan inilah yang akhirnya dimanfaatkan sebagai teknik penyembunyian data atau pesan (steganografi). Sebagai ilustrasi cara penyimpanan data dengan metode LSB, misalnya pixel-pixel wadah berikut :

```
01001101 00101110 10101110 10001010 10101111
10100010 00101011 101010111
```

Digunakan untuk menyimpan karakter ‘H’ (01001000), maka pixel – pixel wadah tersebut akan dirubah menjadi :

```
01001100 00101111 10101110 10001010 10101111
10100010 00101010 101010110
```

Perubahan yang tidak signifikan ini tidak akan tertangkap oleh indra manusia (jika media wadah adalah gambar, suara atau video) [6] .

Penggantian pixel tak signifikan juga dapat dilakukan secara tak terurut, bahkan hal ini dapat meningkatkan tingkat keamanan data (*imperceptability*). Disamping itu juga mungkin melakukan pengubahan pixel tidak pada bagian awal berkas wadah. Pengubahan pixel juga dapat dipilih mulai dari tengah, atau dari titik lain dari berkas wadah yang dimungkinkan untuk menyimpan seluruh informasi rahasia, tanpa menimbulkan permasalahan saat pengungkapan data.

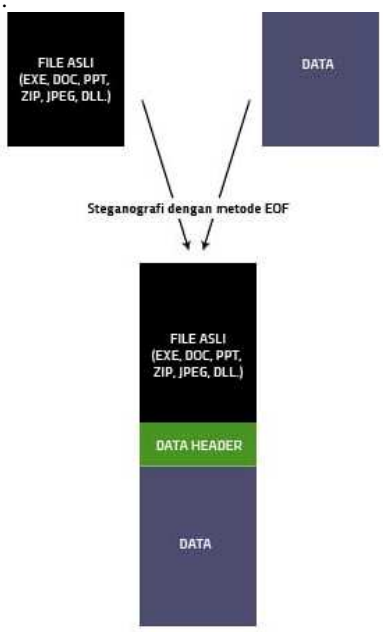
Meskipun metode LSB mudah diterapkan, akan tetapi steganografi dengan metode ini akan menghasilkan berkas stego yang mudah rusak (dirusak).

Steganografi dengan metode LSB juga hanya mampu menyimpan informasi dengan ukuran yang sangat terbatas. Misalnya suatu citra 24-bit (R=8-bit, G=8-bit, B=8-bit) digunakan sebagai wadah untuk menyimpan data berukuran 100 bit, jika masing – masing komponen warnanya (RGB) digunakan satu pixel untuk menyimpan informasi rahasia tersebut, maka setiap pixelnya disimpan 3 bit informasi, sehingga setidaknya dibutuhkan citra wadah berukuran 34 pixel atau setara 34 x 3 x 8 = 816 bit (8 kali lipat). Jadi suatu citra 24-bit jika digunakan untuk menyimpan informasi rahasia hanya mampu menampung informasi maksimum berukuran 1/8 dari ukuran citra penampung tersebut.

2) Metode End of File (EOF)

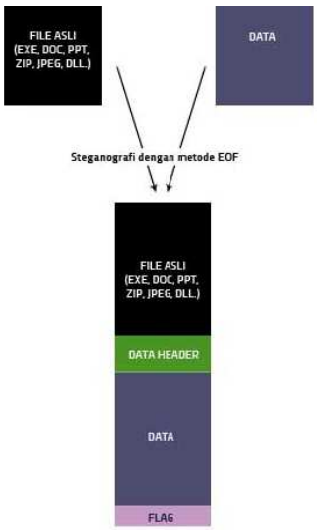
Secara umum teknik steganografi menggunakan *redundant bits* sebagai tempat menyembunyikan pesan pada saat dilakukan kompresi data, dan kemudian menggunakan kelemahan indera manusia yang tidak sensitive sehingga pesan tersebut tidak ada perbedaan yang terlihat. Teknik EOF atau *End Of File* merupakan salah satu teknik yang digunakan dalam steganografi. Teknik ini digunakan dengan cara menambahkan data atau pesan rahasia pada akhir file. Perhitungan ukuran file yang telah disisipkan data sama dengan ukuran file sebelum disisipkan data ditambah ukuran data rahasia yang telah diubah menjadi *encoding file* [3].

Dengan metode EOF, secara umum media steganografi (file yang akan disisipi data) memiliki struktur seperti gambar dibawah ini :



Gbr 3. Struktur File Steganografi dengan Metode EoF [7]

Penanda data header atau flag akan kita letakkan di awal atau akhir file, di mana tidak ada looping yang digunakan untuk mencarinya. Pada beberapa file seperti exe dan zip, penempatan flag di awal file asli tidak akan menjadi masalah, namun untuk jenis file lain semisal JPG, BMP dan DOC, penempatan flag di awal file akan merusak file asli karena mengganggu isi file asli dan merusak CRC file tersebut. Kita akan menempatkannya di akhir file sehingga tidak membawa bencana meskipun kita mengunakan berbagai jenis file. Ini juga sesuai dengan konsep EOF pada steganografi ini :



Gbr 4. Struktur File Steganografi dengan Metode EoF Disertai Flag [7]

E. *Watermarking*

Salah satu karya yang dilindungi adalah barang dalam bentuk digital, seperti *software* dan produk *multimedia* seperti teks, musik, gambar, dan video digital. Selama ini penggandaan atas produk digital tersebut dilakukan secara bebas. Pemegang hak cipta atas produk digital tersebut tentu dirugikan karena tidak mendapat royalti dari penggandaan tersebut.

Salah satu cara untuk melindungi hak cipta tersebut adalah dengan menyisipkan informasi ke dalam data tersebut dengan teknik *watermarking*. Informasi yang disisipkan ke dalam data tersebut disebut *watermark,* dan *watermark* dapat dianggap sebagai sidik digital (*digital signature*) dari pemilik atas produk tersebut. Pemberian *watermark* dengan teknik *watermarking* ini dilakukan sedemikian sehingga informasi yang disisipkan tidak merusak data asli yang dilindungi. Sehingga, seseorang yang membuka produk yang sudah disisipi *watermark* tidak menyadari bahwa di dalam data multimedia tersebut terkandung label kepemilikan pembuatnya.

Pada umumnya, teknik *watermarking* adalah proses menambahkan kode identifikasi secara permanen ke dalam data digital. Kode identifikasi tersebut dapat berupa teks, gambar, suara, atau video. Selain tidak merusak data digital produk yang asli, kode yang disisipkan seharusnya memiliki ketahanan (*robustness*) dari berbagai pemrosesan lanjutan [8].

Watermarking merupakan aplikasi dari steganografi, namun ada perbedaan antara keduanya. Jika pada steganografi informasi rahasia disembunyikan di dalam media digital dimana media penampung tidak berarti apa-apa, sedangkan pada *watermarking* justru media digital tersebut yang akan dilindungi kepemilikannya dengan pemberian *watermark* [8].

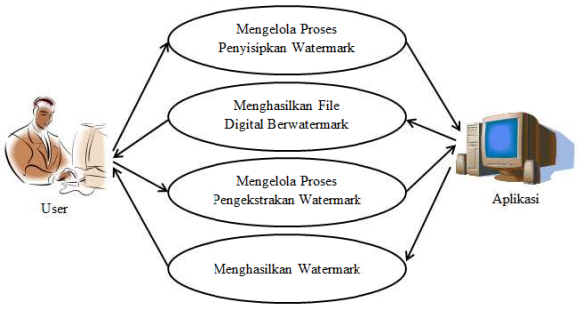
III. PERANCANGAN DAN IMPLEMENTASI

A. *Perancangan*

Perancangan yang dimaksud dalam jurnal ini adalah melakukan proses analisis dan rancangan dari aplikasi digital *watermarking* yang akan dibuat. Perancangan tersebut meliputi :

- *Perancangan Fungsi*

Perancangan fungsi adalah merancang fungsi-fungsi apa saja yang akan ada dalam aplikasi digital *watermarking* yang akan dibuat. Adapun fungsi-fungsi tersebut digambarkan sebagai berikut :



Gbr 5. Perancangan Fungsi

- *Perancangan Antarmuka (Interface)*

Perancangan antarmuka (*interface*) adalah merancang tampilan-tampilan apa saja yang akan ada dalam aplikasi digital *watermarking* yang akan dibuat. Adapun antarmuka (*interface*) yang ada dalam aplikasi digital *watermarking* yang akan dibuat dapat dilihat pada gambar struktur aplikasi dibawah ini :

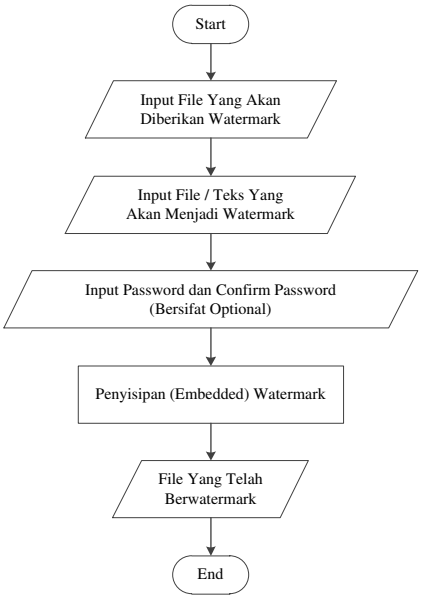
Gbr 6. Struktur Aplikasi

- *Perancangan Algoritma*

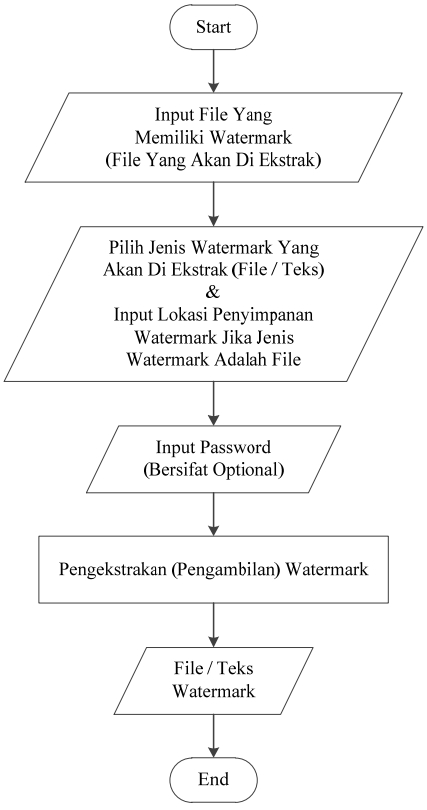
Aplikasi digital *watermarking* yang dibuat akan terdiri dari dua proses yaitu proses penyisipan *watermark* merupakan proses menyisipkan atau memasukkan *watermark* ke dalam sebuah file digital dan proses pengekstrakan *watermark* merupakan proses pengambilan kembali *watermark* yang ada dalam sebuah file digital yang telah diberikan *watermark* sebelumnya. Adapun metode yang digunakan untuk penyisipan *watermark* dalam aplikasi digital *watermarking* ini adalah metode *End Of File* (EOF).

Secara sederhana kedua proses diatas dapat digambarkan

dalam bentuk algoritma program sebagai berikut :



Gbr 7. Algoritma Penyisipan *Watermark*



Gbr 8. Algoritma Pengekstrakan *Watermark*

B. Implementasi

Implementasi yang dimaksud dalam penelitian ini adalah membuat aplikasi *digital watermarking* yang telah dirancang diatas kedalam bentuk *Graphical User Interface* (GUI) dengan menggunakan bahasa pemrograman delphi. Adapun *Graphical User Interface* (GUI) dalam aplikasi digital *watermarking* ini adalah sebagai berikut :

1) Splash Screen

Splash screen merupakan tampilan awal saat aplikasi digital *watermarking* dijalankan.

Gbr 9. *Splash Screen*

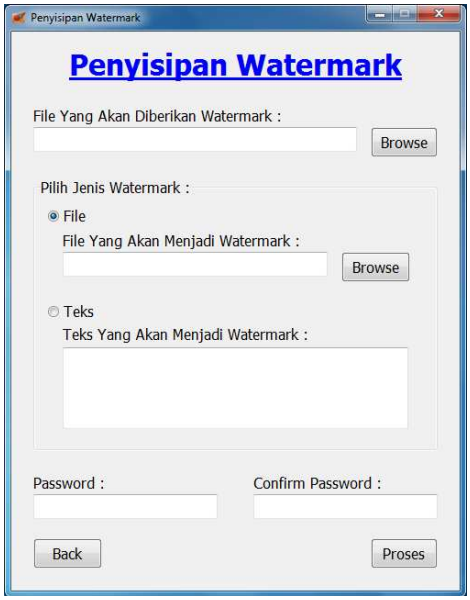
2) Menu Utama

Menu utama merupakan tampilan yang menyediakan beberapa buah menu pilihan dalam bentuk tombol (*button*) yang dapat diklik (dipilih). Adapun menu pilihan yang tersedia adalah penyisipan watermark, pengekstrakan watermark, *about*, dan *exit*.

Gbr 10. Menu Utama

3) Penyisipan Watermark

Menu penyisipan *watermark* digunakan untuk menyisipkan *watermark* ke dalam sebuah file digital. Jenis *watermark* yang digunakan disini adalah dapat berupa sebuah file (gambar / logo, audio, video, dan file lainnya) maupun teks yang diketik. Penyisipan *watermark* disini dapat diberikan *password* sehingga pada saat akan melakukan pengekstrakan watermark akan diminta mengisikan *password* tersebut.



Gbr 11. Penyisipan *Watermark*

4) Pengekstrakan Watermark

Menu pengekstrakan *watermark* digunakan untuk mengekstrak (mengambil) *watermark* yang ada pada sebuah file digital yang telah diberikan *watermark* sebelumnya. Pilihan jenis *watermark* yang diekstrak disini harus sama dengan jenis *watermark* yang digunakan pada saat *watermark* disisipkan kedalam file digital tersebut. Apabila pada saat penyisipan *watermark* diberikan *password*, maka pada saat ingin mengekstrak *watermark* tersebut kita juga harus memasukkan password yang digunakan tersebut.

Gbr 12. Pengekstrakan *Watermark*

5) About

Menu *about* akan menampilkan foto dan nama dari *programmer* yang membuat aplikasi *digital watermarking* dalam penelitian ini.

Gbr 13. *About*

IV. PENUTUP

A. *Kesimpulan*

Berdasarkan pembahasan diatas tentang digital *watermarking* dengan menggunakan metode *End Of File* (EOF), maka dapat diambil kesimpulan sebagai berikut :

- Aplikasi digital *watermarking* yang dibuat dapat digunakan untuk menyisipkan *watermark* ke dalam berbagai format file digital dan dapat digunakan untuk mengekstrak *watermark* tersebut.
- *Watermark* yang disisipkan ke dalam file digital dapat diekstrak kembali sama persis dengan *watermark* asli dan tidak mengalami perubahan.
- *Watermark* yang akan disisipkan dapat berupa teks maupun file (gambar / logo, audio, video, dan file lainnya).
- Ukuran *watermark* yang akan disisipkan kedalam file digital tidak terbatas.
- Pada proses penyisipan *watermark* dapat ditambahkan password untuk membantu memproteksi *watermark* pada saat akan diekstrak.
- Kualitas file digital yang diberikan *watermark* tidak mengalami perubahan sedikit pun, hal ini dikarena proses penyisipan *watermark* dilakukan pada akhir file digital tersebut, sehingga tidak merubah bit data dari file digital tersebut yang mempengaruhi kualitas dari suatu file digital.
- Ukuran file digital yang telah disisipkan *watermark* adalah sama dengan ukuran file digital sebelum disisipkan *watermark* ditambah dengan ukuran *watermark*.
- File digital yang telah diberikan *watermark* masih rentan (kurang kuat menghadapi serangan) terhadap proses pengolahan file (modifikasi file) yang akan

mempengaruhi isi *watermark* yang ada dalam file digital tersebut.

B. Saran

Berdasarkan pembahasan diatas tentang digital *watermarking* dengan menggunakan metode *End Of File* (EOF) dan masih terdapat kekurangan, maka dapat diberikan saran sebagai berikut :

- Karena file digital yang telah diberikan *watermark* masih rentan (kurang kuat menghadapi serangan) terhadap proses pengolahan file (modifikasi file) yang akan mempengaruhi isi *watermark* yang ada dalam file digital tersebut, maka disarankan untuk pengembangan berikutnya dapat dibuat sebuah aplikasi digital *watermarking* dengan menggunakan metode yang lebih kuat menghadapi serangan terhadap proses pengolahan file (modifikasi file), sehingga tidak akan mempengaruhi isi *watermark* yang ada dalam file digital tersebut.
- Untuk pengembangan berikutnya diharapkan dapat membuat sebuah aplikasi digital *watermarking* yang dapat memisahkan kembali antara file digital asli sebelum diberikan *watermark* dengan *watermark* tersebut.

DAFTAR PUSTAKA

[1] Yogie Aditya, Andhika Pratama, Alfian Nurlifa. 2010. *Studi Pustaka Untuk Steganografi Dengan Beberapa Metode*. Seminar Nasional Aplikasi

[2] Adiputra Sejati. 2010. *Studi dan Perbandingan Steganografi Metode EOF (End of File) dengan DCS (Dynamic Cell Spreading).* Teknik Informatika Institut Teknologi Bandung : Bandung. http:// informatika.stei.itb.ac.id /~rinaldi. munir/ Kriptografi / 2009 - 2010/ Makalah1 / Makalah1_ IF3058_2010_ 028.pdf, 30 Agustus 2013.

[3] Wasino., Tri Puji Rahayu., Setiawan. 2012. *Implementasi Steganografi Teknik End Of File Dengan Enkripsi Rijndael.* Seminar Nasional Teknologi Informasi dan Komunikasi 2012 : Yogyakarta. http : //fti.uajy.ac.id/ sentika/ publikasi /makalah /2012/2012-20.pdf, 01 September 2012.

[4] Hasbian Saputra, M. Zen Samsono Hadi, Nanang Syahroni. 2011. *Implementasi Algoritma Steganografi Embedding Dengan Metode Least Significant Bit (Lsb) Insertion Dan Huffman Coding Pada Pengiriman Pesan Menggunakan Media Mms Berbasis J2me.* Institut Teknologi Sepuluh Nopember (ITS) : Surabaya. http: //www.eepis-its.edu/uploadta/ downloadmk.php?id=1372, 30 Agustus 2013.

[5] Rinaldi Munir. 2004. Bahan Kuliah IF5054 Kriptografi : *Steganografi dan Watermarking*. http: //informatika.stei. itb.ac.id/ ~rinaldi.munir / Kriptografi/ Steganografi%20dan%20Watermarking.pdf, 29 Agustus 2013.

[6] Muhammad Hakim A. 2007. *Studi dan Implementasi Steganografi Metode LSB dengan Preprocessing Kompresi data dan Ekspansi Wadah.* Teknik Informatika Institut Teknologi Bandung : Bandung. http: // informatika .stei .itb .ac.id /~ rinaldi. Munir / Kriptografi / 2007 – 2008 / Makalah1 / MakalahIF5054 - 2007 -A-077.pdf, 01 September 2013.

[7] Joko Rivai. 2012. *Steganography Dengan Metode EOF*. http : //cenadep. org/ 2012/ 05/18/steganography-dengan-metode-eof/. Diakses : 29 Agustus 2013.

[8] Rinaldi Munir. 2004. Bahan Kuliah IF5054 Kriptografi : *Steganografi dan Watermarking*. http: //informatika.stei. itb.ac.id/ ~rinaldi.munir / Kriptografi/ Steganografi%20dan%20Watermarking.pdf, 29 Agustus 2013.