IMPLEMENTASI *VISIBLE WATERMARKING* DAN STEGANOGRAFI *LEAST SIGNIFICANT BIT* PADA FILE CITRA DIGITAL

Sri Wahyuningsih[1], Theodora V.D Pandex[2], Vanessa Stefanny[3]

[1, 2,3)]Program Studi Magister Ilmu Komputer, Program Pascasarjana, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Pesanggrahan, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5869225
[1]wiwiewahyuningsih@gmail.com, [2]erniondu zt@gmail.com, [3]fannybataona@gmail.com

ABSTRAK

Kejahatan dalam pemalsuan maupun upaya merusak suatu data digital sudah marak terjadi dewasa ini. Oleh karena itu diperlukan adanya upaya perlindungan keamanan data terutama saat terjadi pertukaran informasi. Steganografi merupakan salah satu cara mengamankan data dengan melakukan penyisipan pesan pada media penampung tertentu berupa citra digital dengan metode khusus. Selain itu, terdapat juga metode yang hampir serupa dengan steganografi yaitu teknik watermarking. Watermarking adalah suatu teknik memberi tanda keaslian pada suatu data. Penerapan steganografi dan watermarking dapat menggunakan berbagai macam metode sehingga keamanan lebih terjamin. Penulis akan melakukan steganografi dan watermarking pada data gambar dengan menggunakan teknik Least Significant Bit (LSB). Implementasi dilakukan dengan format gambar .jpg dan .bmp menggunakan program VB 6.0.

Kata Kunci *:* Steganografi*, LSB, Watermarking*

I. PENDAHULUAN

Kemajuan teknologi dewasa ini memungkinkan adanya perkembangan pertukaran data yang terjadi dalam format yang beraneka macam. Kemajuan tersebut dapat pula berdampak akan adanya upaya percobaan pemalsuan data yang akan ditukar sehingga data atau media citra yang diterima tidak sama dengan yang dikirim. Hal ini tentunya menghasilkan kesalahpahaman dalam proses komunikasi pertukaran data. Untuk mengantisipasi terjadinya pemalsuan data selama proses komunikasi maka diperlukan suatu metode yang dapat memastikan keaslian data yang diterima oleh pihak penerima.

Steganografi merupakan salah satu teknik yang dapat digunakan untuk melindungi data dari pemalsuan ataupun perbuatan merusak yang disengaja. Steganografi dipandang sebagai suatu teknik penyisipan pada media citra baik itu teks, audio maupun video. Pesan yang akan dikirim dapat berupa dokumen, gambar, audio maupun video. Pesan yang akan dikirim tersebut akan disisipkan ke sebuah media penampung dengan menggunakan metode tertentu. Media penampung dapat berupa gambar, audio, maupun video dengan ketentuan bahwa hasil penyisipan tidak mengubah tampilan media penampung jika dilihat dengan mata secara langsung sehingga pihak lain tidak dapat mengidentifikasi bahwa media tersebut mengandung pesan rahasia.

Selain itu, teknik pengamanan data lainnya adalah teknik *watermarking* atau disebut juga 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 akan dilindungi, kode yang disisipkan seharusnya memiliki ketahanan (*robustness*) dari berbagai pemrosesan lanjutan seperti pengubahan, transformasi geometri, kompresi, enkripsi, dan sebagainya. Sifat *robustness* berarti data *watermark* tidak terhapus akibat pemrosesan lanjutan tersebut.

Dalam penelitian kali ini, penulis akan membahas proses steganografi dengan metode *Least Bit Significant* (LSB) yang digabungkan dengan teknik *watermarking* pada *file* gambar. *Least Bit Significant* digunakan sebagai metode yang paling sederhana dalam mempelari konsep steganografi. Pergantian bit-bit kurang signifikan pada media penampung dengan bit-bit pada file yang akan disisipkan merupakan inti dari proses steganografi dengan metode LSB.

II. LANDASAN TEORI

A. Steganografi

Steganografi adalah suatu teknik untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya akan tampak seperti informasi normal lainnya. Steganografi merupakan seni penyembunyian pesan ke dalam pesan lainnya sedemikian rupa sehingga tidak ada yang menyadari bahwa terdapat sesuatu di dalam pesan pembawa tersebut. Media yang digunakan pada umumnya merupakan suatu media yang berbeda dengan media pembawa informasi, dimana disinilah fungsi steganografi yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat jelas. Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia.

Kata "steganografi" berasal dari bahasa Yunani "*steganos*", yang artinya "tersembunyi atau terselubung", dan "*graphein"*, "menulis". Sehingga dapat disimpulkan bahwa steganografi adalah ilmu dan seni menulis atau menyembunyikan pesan ke dalam sebuah media sedemikian

rupa sehingga keberadaan pesan tidak diketahui atau tidak disadari oleh orang selain pengirim dan penerima pesan tersebut.

Dalam melakukan teknik steganografi dibutuhkan dua aspek media yaitu sebagai penyimpan dan informasi rahasia yang akan disembunyikan. Metode steganografi sangat berguna jika digunakan pada steganografi komputer karena banyak format file digital yang dapat dijadikan media untuk menyembunyikan pesan. Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya teks, citra, suara, dan video. Data rahasia yang disisipkan juga dapat berupa teks, citra, suara, atau video. Format yang biasa digunakan pada teknik steganografi di antaranya:

- Format *image*/gambar : bitmap (bmp), gif, pcx, jpeg, dll.
- Format audio : wav, voc, mp3, dll.
- Format lain : teks file, html, pdf, dll.

Beberapa contoh media penyisipan pesan rahasia yang digunakan dalam teknik steganografi antara lain adalah :

1. Teks
   Penggunaan teks sebagai media penyisipan biasanya menggunakan teknik NLP sehingga teks yang telah disisipi pesan rahasia tidak akan mencurigakan untuk orang yang melihatnya.
2. Audio
   Format yang lumayan sering dipilih karena berukuran relatif besar. Sehingga dapat penggunaan media audio bisa menampung pesan rahasia dalam jumlah yang besar pula.
3. Citra
   Format citra adalah yang paling sering digunakan, karena format ini merupakan salah satu format yang sering digunakan dalam pertukaran informasi dalam dunia internet. Alasan lainnya adalah banyaknya tersedia algoritma metode steganografi untuk media penampung berupa citra.
   File citra pada komputer merupakan *array* bilangan yang merepresentasikan nilai intensitas cahaya yang bervariasi (*pixel*). Kumpulan *pixel-pixel* inilah yang membentuk suatu citra. Citra yang sering digunakan umum adalah citra 24 bit dan citra 8 bit (256 *colors*).

Tabel 1. Citra dilihat dari ukuran bitnya

Jumlah Bit	Keterangan
1	*binary-valued image* (0 – 1)
8	*gray level* (0 – 255)
16	*high color* (216)
24	*true color* (224)
32	*true color* (232)

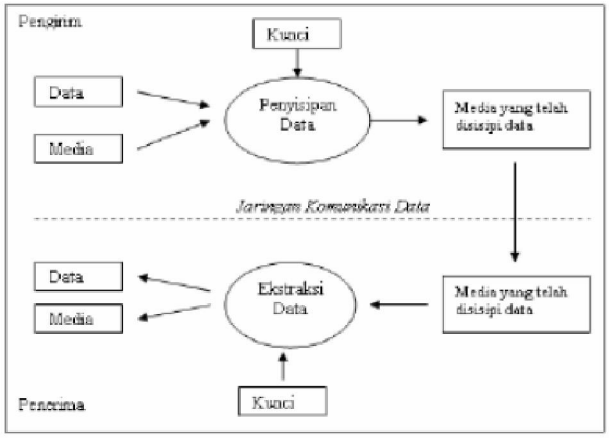
Format gambar digital memiliki 2 parameter:

- *spatial resolution* : *pixels x pixels*
- *color encoding* : *bits / pixel*
  Misal: terdapat gambar berukuran 200 *pixels* x 200 *pixels* dengan *color encoding* 24 bits dengan R=8 bits, G=8 bits, B=8 bits per *pixel*, maka *color encoding* akan mampu mewakili 0 .. 16.777.215 (mewakili 16 juta warna), dan ruang disk yang dibutuhkan = 200 * 200 * 3 byte (karena RGB) = 120.000 bytes = 120 KB atau 200 * 200 * 24 bits = 480000 bits.

4. Video
   Format ini jarang digunakan karena memang merupakan format dengan ukuran file yang relatif sangat besar sehingga mengurangi kepraktisannya dan juga kurangnya algoritma yang mendukung format ini.

Steganografi yang dibahas di sini adalah penyembunyian data di dalam citra digital saja.Meskipun demikian, penyembunyian data dapat juga dilakukan pada wadah berupa suara digital, teks, ataupun video. Penyembunyian data rahasia ke dalam citra digital akan mengubah kualitas citra tersebut. Kriteria yang harus diperhatikan dalam penyembunyian data adalah :

1. *Fidelity* : 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.
2. *Robustness* : Data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada citra penampung (seperti pengubahan kontras, penajaman, pemampatan, rotasi, perbesaran gambar, pemotongan (*cropping*), enkripsi, dan sebagainya). Bila pada citra dilakukan operasi pengolahan citra, maka data yang disembunyikan tidak rusak.
3. *Recovery* : Data yang disembunyikan harus dapat diungkapkan kembali (*recovery*). Karena tujuan steganografi adalah data hiding, maka sewaktu-waktu data rahasia di dalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut.
4. *Imperceptible* : Keberadaan pesan rahasia tidak dapat dipersepsi.

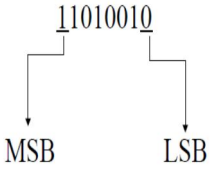


Gambar 1. Diagram Sistem Steganografi

B. *Least Significant Bit*

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.



Gambar 2. LSB dan MSB

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 biru, maka perubahan satu bit LSB tidak mengubah warna biru tersebut secara berarti. Mata manusia tidak dapat membedakan perubahan kecil tersebut.

Dapat diambil kesimpulan dari contoh 8 bit pixel, menggunakan LSB *Insertion* dapat secara drastic mengubah unsur pokok warna dari *pixel*. Ini dapat menunjukkan perbedaan yang nyata dari *cover image* menjadi *stego image*, sehingga tanda tersebut menunjukkan keadaan dari steganografi. Variasi warna kurang jelas dengan 24 bit *image*, bagaimanapun file tersebut sangatlah besar. Antara 8 bit dan 24 bit image mudah diserang dalam pemrosesan *image*, seperti *cropping* (kegagalan) dan *compression* (pemampatan).

Keuntungan dari LSB *Insertion* adalah yang paling besar dari algoritma LSB ini adalah cepat dan mudah. Dan juga algoritma tersebut memiliki *software* steganografi yang mendukung dengan bekerja di antara unsur pokok warna LSB melalui manipulasi *pallete* (lukisan).

C. *Watermarking*

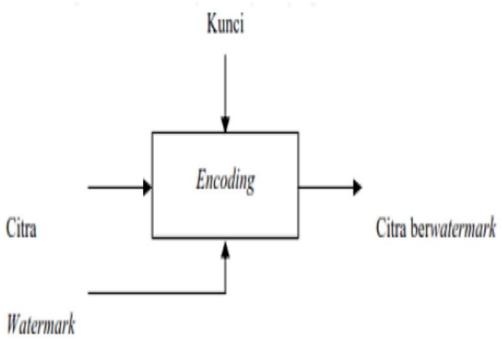
Data digital adalah salah satu jenis karya yang dilindungi, seperti *software* dan produk multimedia seperti teks, musik (dalam format MP3 atau WAV), gambar/citra (image), dan video digital (VCD). Selama ini penggandaan atas produk digital tersebut dilakukan secara bebas dan leluasa. Pemegang hak cipta dirugikan karena tidak mendapat royalti dari usaha penggandaan tersebut.

Salah satu cara untuk melindungi hak cipta multimedia (gambar/foto, suara, teks, video) adalah dengan menyisipkan informasi ke dalam data multimedia tersebut dengan teknik *watermarking*. Informasi yang disisipkan ke dalam data multimedia disebut watermark, dan watermark dapat dianggap sebagai sidik digital (*digital signature*) atau stempel digital dari pemilik yang sah atas produk multimedia tersebut.

Gambar 3 memperlihatkan sebuah gambar (*image*) paprika yang disisipi dengan watermark berupa gambar hitam putih yang menyatakan identifikasi pemiliknya (Shanty). Perhatikanlah bahwa setelah disisipi watermark, gambar paprika tetap kelihatan mulus, seolah-olah tidak pernah disisipi watermark sebelumnya. Sebenarnya tidaklah demikian, gambar paprika tersebut mengalami sedikit perubahan akibat watermarking, namun mata manusia mempunyai sifat kurang peka terhadap perubahan kecil ini, sehingga manusia sukar membedakan mana gambar yang asli dan mana gambar yang sudah disisipi *watermark*.

Gambar 3. Memberi watermark pada citra peppers

Proses penyisipan watermark ke dalam citra disebut *encoding*. *Encoding*, proses dapat disertai dengan pemasukan kunci atau tidak memerlukan kunci [1]. Kunci diperlukan agar *watermark* hanya dapat diekstraksi oleh pihak yang sah. Kunci juga dimaksudkan untuk mencegah watermark dihapus oleh pihak yang tidak berhak.



Gambar 4. Proses Watermark pada Citra Digital

D. *Digital Watermarking*

Digital *watermarking* adalah teknik untuk menyisipkan informasi tertentu ke dalam sebuah data dengan suatu cara tertentu sehingga *watermark* itu sulit dirusak dan dihapus [2]. Secara garis besar, *watermark* terbagi menjadi dua tipe, yaitu *visible* watermark dan *invisible* watermark [3]. *Visible* watermark merupakan salah satu jenis yang dapat terlihat oleh indera manusia. *Visible* watermark bersifat sangat *robust* karena keberadaan watermark dapat dikenali dengan mudah dan biasanya sangat sulit untuk dihapus.*Watermark* yang disisipkan dapat bersifat *solid* ataupun semi transparan, dan untuk memindahkannya membutuhkan *cropping* yang signifikan.

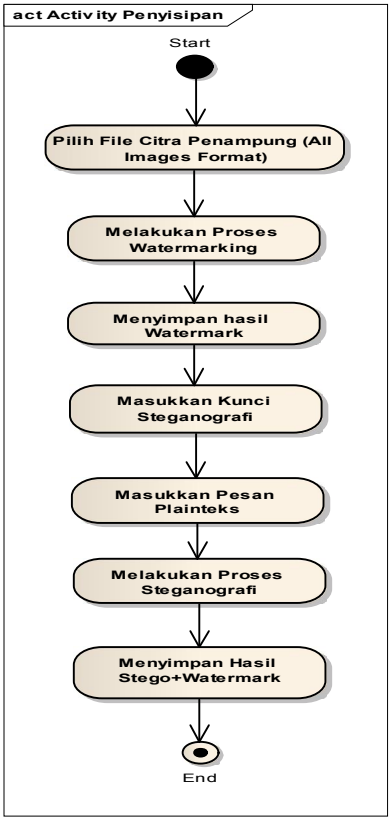
III. KAJIAN SEBELUMNYA

Beberapa penelitian mengenai steganografi dan watermarking sudah banyak dilakukan yang menjadi acuan bagi penelitian kali ini. Penelitian berjudul *Teknik Watermarking Menggunakan Shifting LSB Untuk Proteksi Dokumen Dalam Dunia Pendidikan* yang dilakukan oleh Wasilah dan Dona Yuliawati pada tahun 2015. Penelitian ini membahas proses penyisipan dan ekstraksi *watermarking* pada berbagai format citra gambar dengan metode LSB [4]. Penelitian berjudul *Implementasi Watermarking pada Citra*

Digital dengan Metode LSB yang dilakukan oleh Rina Septianingsih dari jurusan Teknik Informatika Universitas Gunadarma pada tahun 2012. Penelitian ini membahas tentang implementasi metode *watermarking* dengan metode LSB untuk melindungi data gambar dengan menggunakan aplikasi MATLAB [5]. Penelitian berjudul *Steganografi Menggunakan Metode Least Significant Bit dengan Kombinasi Algoritma Kriptografi Vigenere dan RC4* yang dilakukan oleh Basuki Rahmat dan Muhammad Fairuzabadi dari jurusan Teknik Informatika Universitas PGRI Yogyakarta pada tahun 2010. Penelitian ini membahas tentang penggabungan metode kriptografi Vigenere dan RC4 yang terintegrasi dengan metode steganografi sebagai proteksi ganda pada data [6]. Penelitian berjudul *Implementasi Teknik Steganografi dengan Metode LSB pada Citra Digital* yang dilakukanoleh Putri Alatas dari jurusan Sistem Informasi Universitas Gunadarma pada tahun 2009. Penelitian ini membahas tentang implementasi metode steganografi dengan metode LSB pada citra digital [7]. Penelitian berjudul *Implementasi Steganografi LSB dengan Enkripsi Vigenere Cipher pada Citra Jpeg* yang dilakukanoleh Tri Cahyadi dari jurusan Teknik Elektro Universitas Diponegoro pada tahun 2012. Penelitian ini membahas tentang penyisipan pesan teks ke dalam berkas citra digital berformat jpeg dan mengekstraksi kembali pesan yang telah disembunyikan [8].

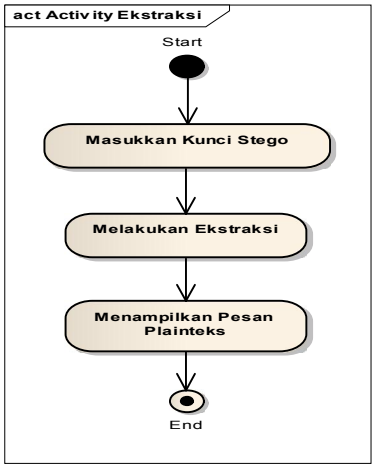
IV. IMPLEMENTASI

A. Proses Penyisipan



Gambar 5. Diagram Aktivitas Penyisipan (Encoding)

B. Proses Ekstraksi



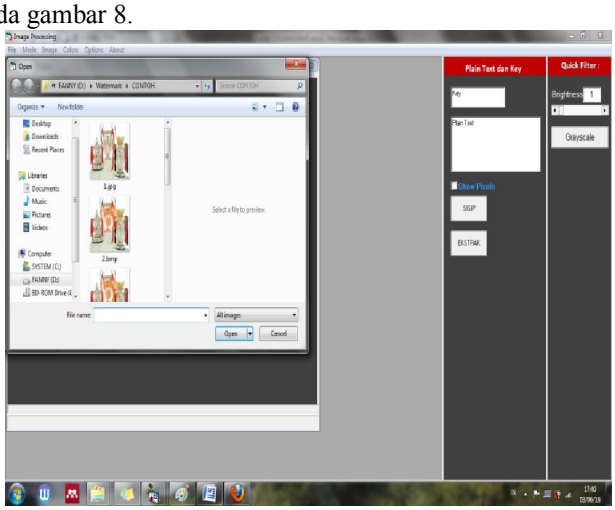
Gambar 6.Diagram Aktivitas Ekstraksi

C. Tampilan Program

Untuk melakukan proses penyisipan data dilakukan dengan aplikasi dengan bahasa pemrograman VB 6.0.

Gambar 7. Tampilan Awal Aplikasi

Gambar 7 menjelaskan bahwa aplikasi bisa di jalankan dengan memilih data informasi yang akan disisipkan dengan memilih Menu File-Open sehingga muncul kotak dialog seperti pada gambar 8.



Gambar 8. Kotak Dialog Memilih File Gambar

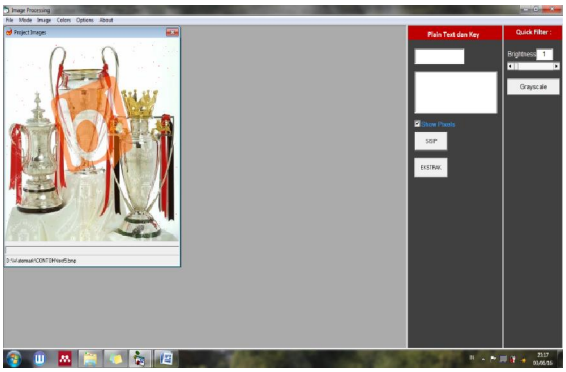
Gambar 8 yang akan menjadi media penampung dan dengan format gambar apa saja seperti .jpg, .png, .bmp, dll. Setelah memilih gambar maka selanjutnya *picture box* yang berisi kolom untuk mengisi kunci (*key*) dan pesan teks yang akan disisipkan (*plaintext*) akan aktif sehingga bisa melakukan pengisian kunci dan pesan yang akan disisipkan.

Gambar 9. Proses Input Gambar Penampung

Gambar 9 menjelaskan jika input *image* berhasil, maka mengisi pesan teks yang akan disisipkan dan kunci steganografi dan selanjutnya menekan tombol SISIP. Seperti pada gambar 10.

Gambar 10. Mengisi Kunci dan Pesan Teks yang akan Disisipkan

Maka proses steganografi dan *watermarking* akan berlangsung dan kemudian menampilkan hasil gambar yang telah diberi *watermark* dan disisipkan pesan seperti pada gambar 11.



Gambar 11. Proses Steganografi dan Watermarking Selesai

Gambar 12. Hasil Akhir Citra Steganografi dan Watermarking

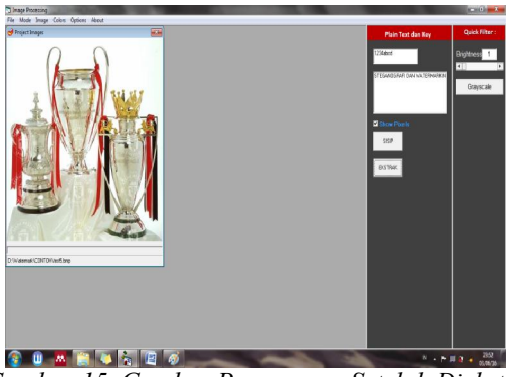
Proses pengembalian pesan pada aplikasi dilakukan dengan memasukan kunci steganografi dan menekan tombol ekstraksi. Maka pesan yang disisipkan akan keluar dan gambar media penampunga kan kembali seperti awal tanpa *watermark* seperti pada gambar 13.

Gambar 13. Proses Ekstraksi Pesan

Gambar 14 menjelaskan bahwa saat proses ekstraksi harus membuka file yang berisi pesan dan telah di *watermarking.*

Gambar 14. Mengisi Kunci Steganografi

Setelah membuka gambar maka harus mengisi kunci yang sama dengan saat penyisipan. Maka pesan yang disisipkan akan ditampilkan dan tersiksa gambar penampung seperti semula.



Gambar 15. Gambar Penampung Setelah Diekstraksi

Aplikasi steganografi dan *watermarking* disesuaikan dengan algoritma yang dibuat, hasil dari image asli dan image setelah disisipkan pesan tidak terlihat perubahan secara signifikan dalam ukuran gambar karena pesan yang disisipkan masih dalam ukuran yang kecil namun jika dilihat pixelnya maka terjadi beberapa titik-titik kecil yang menandakan adanya penyisipan pesan.

Tabel 2. Daftar Citra dan Keterangannya

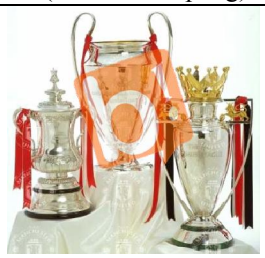
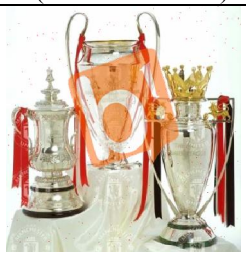
 Piala.jpg (Citra Penampung)	 Logo.bmp (Citra *watermark*)
 test6.bmp (Hanya disisipkan *watermark*)	 test6.bmp (Hasil Steganografi dan *Watermarking*)

Image yang telah disisipkan *visible watermark* dan tidak disisipkan watermark memiliki ukuran yang sama bahkan setelah disisipkan steganografi. Hal ini bisa terjadi karena panjang pesan teks yang disisipkan relatif pendek sehingga tidak mempengaruhi file dengan ukuran yang besar.

Aplikasi steganografi dan *watermarking* disesuaikan dengan algoritma yang dibuat, hasil dari *image* asli dan *image* setelah disisipkan pesan tidak terlihat perubahan secara signifikan dalam ukuran gambar karena pesan yang disisipkan masih dalam ukuran yang kecil namun jika dilihat pixelnya maka terjadi beberapa titik-titik kecil yang menandakan adanya penyisipan pesan.

V. KESIMPULAN

Dari hasil penulisan dan penelitian yang telah dilakukan bahwa metode steganografi dan *watermarking* merupakan salah satu cara yang bisa digunakan untuk mengamankan sebuah informasi dari upaya kejahatan seperti pemalsuan dan pembajakan data. Dengan menggabungkan kedua metode dapat dihasilkan tingkat keamanan yang lebih tinggi yaitu autentikasi data dan penyembunyian atau enkripsi data.

DAFTAR PUSTAKA

[1] J.Dugelay. 2006. Still-image water-marking robust to local geometric distortions. in *IEEE Trans. on Image Proc*, 2006, pp. 2831–2842.

[2] Goel.2010.Improved Digital Watermarking Techniques and Data Embedding In Multimedia. *Cyber Journals Multidiscip. Journals Sci. Technol.*. vol. 02 No.02. pp. 164–168.

[3] E. Utami. 2009. Pendekatan Metode Least Bit Modification Untuk Merancang Aplikasi Steganography Pada File Audio Digital Tidak Terkompresi. *J. Dasi*. vol. 10 No.1.

[4] D. Y. Wasilah. 2015. Teknik Watermarking Menggunakan Shifting LSB Untuk Proteksi Dokumen Dalam Dunia Pendidikan.*Konf. Nas. Inform.* pp. 258–263.

[5] R. Septianingsih. 2012. Implementasi Watermarking pada Citra Digital Menggunakan Metode LSB.

[6] Rahmat, Basuki and M. Fairuzabadi. 2010. Steganografi Menggunakan Metode Least Significant Bit dengan Kombinasi Algoritma Kriptografi Vigenere dan RC4. *J. Din. Inform.* vol. 5 No.2.

[7] P. Alatas. 2009. Implementasi Teknik Steganografi dengan Metode LSB pada Citra Digital.

[8] T. Cahyadi. 2012. Implementasi Steganografi LSB dengan Enkripsi Vigenere Cipher pada Citra jpeg.