Volume 1 Tahun 2015

ISSN : 2460-4690

PROSIDING SENATKOM

SENATKOM

Seminar Ilmiah Nasional

Memberdayakan UMKM Elektronik (Usaha Mikro, Kecil dan Menengah) Untuk Meningkatkan Persaingan Lokal

Padang, Jumat 23 Oktober 2015

Penyelenggara :

Lembaga Penelitian dan Pengabdian Masyarakat
UNIVERSITAS PUTRA INDONESIA "YPTK" PADANG
Jl. Raya Lubuk Begalung Padang Indonesia 25212
Telp. 0751 (776666) Fax. 0751 (71913)

Vol. 1, Oktober 2015
ISSN : 2460 – 4690

PROSIDING SENATKOM 2015

(Seminar Nasional Teknologi Komputer)
Volume 1 – Oktober 2015

Memberdayakan UMKM Elektronik (Usaha Mikro, Kecil dan Menengah) Untuk Meningkatkan Persaingan Lokal

ISSN : 2460-4690

PENERBIT
Lembaga Penelitian dan Pengabdian Masyarakat
Universitas Putra Indonesia YPTK Padang

Alamat Editor :
Lembaga Penelitian dan Pengabdian Masyarakat
Universitas Putra Indonesia YPTK Padang
Jl. Raya Lubuk Begalung - Padang - Indonesia 25212
Telp . +62751- 776666
Fax . +62751 – 71913
e-mail : senatkom2015@gmail.com / lppm_upi_yptk@yahoo.com

Vol. 1, Oktober 201
ISSN : 2460 - 469

PROSIDING SENATKOM, Volume 1-2015

Editor : Ihsan Verdian , S.Kom, M.Kom
Disain Sampul: Vernanda Em Afdhal, S.Ds
Penerbit : Lembaga Penelitian dan Pengabdian Masyarakat
Universitas Putra Indonesia YPTK Padang

ISSN : 2460-4690

Vol. 1, Oktober 2015
ISSN : 2460 – 4690

DEWAN REDAKSI

PENERBIT :

Lembaga Penelitian dan Pengabdian Masyarakat
Universitas Putra Indonesia YPTK Padang
Jl. Raya Lubuk Begalung - Padang - Indonesia 25212
Telp . +62751- 776666
Fax . +62751 - 71913
e-mail : senatkom2015@gmail.com / lppm_upi_yptk@yahoo.com

Vol. 1, Oktober 2015
ISSN : 2460 – 4690

PANITIA PELAKSANA SEMINAR

Penasehat :
Dr. H. Sarjon Defit S.Kom, M.Sc

Penanggung Jawab :
Yuhandri, S.Kom, M.Kom

Ketua Pelaksana :
Abulwafa Muhammad, S.Kom, M.Kom

Wakil Ketua Pelaksana :
Ihsan Verdian, S.Kom, M.Kom

Sekretariat :
Eka Lia Febrianti, S.Kom, M.Kom
Eka Praja Wiyata Mandala, S.Kom, M.Kom
Surmayanti, S.Kom,M.Kom
Ruri Hartika Zain, S.Kom, M.Kom

Sarana Prasarana :
Muhammad Reza Putra, S.Kom, M.Kom

Vol. 1, Oktober 2015
ISSN : 2460 – 4690

DAFTAR ISI

Vol. 1, Oktober 2015
ISSN : 2460 - 4690

APLIKASI *GEOMETRICAL ATTACK* PADA *IMAGE WATERMARKING LEAST SIGNIFICANT BIT* (LSB)

Billy Hendrik[1)], Mardhiah Masril[2)]
[1,2]**Fakultas Ilmu Komputer, Universitas Putra Indonesia YPTK Padang**
e-mail: m.haikalbilvy@yahoo.co.id, e-mail: dhie2_m@yahoo.com

ABSTRACT

Computer technology can help people to sand digital data easier, but the technology is still a problem such as digital data can be easily duplicated. The protection of copyrighted digital data or digital product is not an easy thing, to resolve this problem, we need protection of digital product One form of protection of digital products that watermarking techniques. Watermarking is the study of how to hide a digital data on other file. Watermarking has good quality if it has good robustness from various forms of attacks to images such as geometrical attack. In this research, will be analyzed image watermarking least significant bit methods if this image watermarking is given a geometric transform operation such as rotation, cropping and scaling, this analysis has aim to know robustness of image watermarking LSB. The results of this reasearch are expected to provide input to development of watermarking science.

***Key words** : image watermarking, geometrical attack, least significant bit (LSB)*

1. PENDAHULUAN

Perkembangan teknologi digital saat ini telah semakin pesat, dengan adanya teknologi digital membuat manusia lebih mudah dalam melakukan pengiriman data karena tidak terbatas ruang dan waktu dengan memanfaatkan media Internet. Namun dengan kemudahan yang diciptakan pada era digital pada proses pengiriman data bukan berarti tidak terdapat masalah. Terkadang data yang dikirim melalui media digital tersebut bisa berupa data yang penting, sehingga muncul permasalahan pada saat pengiriman data yaitu terkait dengan keamanan data. Terlebih lagi apabila data yang dikirimkan merupakan data yang bersifat rahasia atau bahkan data tersebut bisa berupa hasil karya seseorang atau produk digital yang merupakan hak eksklusif yang terdiri atas hak moral dan hak ekonomi (hak cipta).

Untuk itulah muncul pemikiran bagaimana data dapat dikirimkan secara aman dalam artian data tidak bisa dibaca secara langsung atau bahkan tidak bisa diganti oleh pihak yang tidak berwenang. Perlindungan terhadap hak cipta produk digital bukan merupakan hal yang mudah karena pembajakan yang terjadi lebih rumit untuk dideteksi kepemilikannya karena data digital dapat dengan mudah diperbanyak. Salah satu bentuk perlindungan produk digital yaitu *watermarking*.

Watermarking pada data digital disebut *digital watermarking*. *Watermarking* merupakan suatu bentuk dari *Steganography*, yaitu ilmu yang mempelajari bagaimana menyembunyikan suatu data pada data atau file digital lainnya [7,8].

Secara garis besar metode *Steganography* terdiri dari 2 bagian utama [6] , yaitu proses penyembunyian data (*hidden message*) dan proses pengembalian data ke bentuk semula (*reveal message*). Kedua proses ini dilakukan dengan menggunakan sebuah kata kunci rahasia (*secret key*) yang akan digunakan di dalam prosesnya untuk meningkatkan keamanan data. Salah satu metode dalam *Steganography* adalah metode LSB (*Least Significant Bit*). LSB dilakukan dengan mengambil bit – bit terakhir warna pada citra dan menggantinya dengan bit – bit data. Tujuan utama dari LSB adalah memanipulasi nilai suatu titik warna (pixel) sehingga data dapat disembunyikan ke dalam titik warna tersebut namun perubahan yang terjadi berusaha diminimalisasi sehingga seakan – akan perubahannya tidak dapat dideteksi oleh mata manusia.

Citra yang telah disisipi *watermark* dinyatakan memiliki kualitas yang baik selain perubahan pada citra tersebut tidak dapat dideteksi oleh mata manusia citra tersebut juga mempunyai ketahanan (*robustness*). *Robustness* ini berkaitan dengan serangan terhadap image *watermarking* jika sebuah penyisipan informasi dengan *watermarking* tersebut mudah dirusak, maka tujuan utama dalam *watermarking* akan sulit untuk disampaikan. Ilmu yang mempelajari mengenai serangan terhadap watermaking juga ikut berkembang namun teknologi ini kebanyakan digunakan untuk menganalisa kelemahan dari *watermarking* bukan untuk merusak. Selain itu pengetahuan ini membantu kita untuk lebih mengerti cara penyembunyian

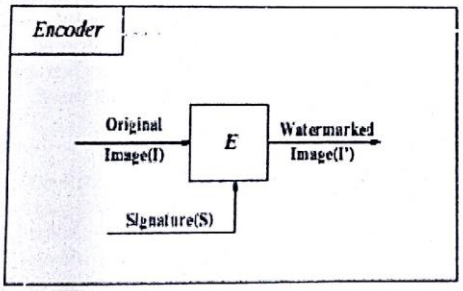
data, deteksi penyalahgunaan dan mengatur akses kontrol terhadap suatu produk digital.

Penelitian ini akan membahas tentang jenis serangan terhadap image *watermarking* yang membuat watermark tidak dapat dideteksi, dimana image *watermarking* yang mendapat serangan adalah image *watermarking* yang menggunakan metode LSB. Dengan demikian dapat diketahui tingkat *robustness* dari image *watermarking* tersebut. Dimana hasil analisa ini berguna sebagai masukan dalam perkembangan *watermarking* itu sendiri.

2. KAJIAN LITERATUR

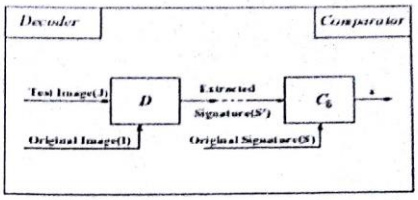
Definisi *Watermarking*

Watermarking merupakan suatu bentuk dari *Steganography*, yaitu ilmu yang mempelajari bagaimana menyembunyikan suatu data pada data atau file digital lainnya[7]. *Watermarking* atau tanda air dapat diartikan sebagai suatu teknik penyembunyian data atau informasi rahasia kedalam suatu data lainnya untuk ditumpangi, tetapi tidak disadari kehadirannya oleh indera manusia, yaitu indera penglihatan dan indera pendengaran. Proses *watermarking* [10] dapat dibagi menjadi dua bagian, pertama proses penyisipan *watermark* (*encoding/embedding*). *Encoding* dapat disertai dengan pemasukan kunci, hal ini diperlukan agar hanya dapat diekstraksi oleh pihak yang sah. Kunci juga bermanfaat untuk mencegah *watermark* dihapus oleh pihak yang tidak berhak, sedangkan ketahanan terhadap proses – proses pengolahan lainnya tergantung pada metode *watermarking* yang digunakan , proses



Gambar 1. Proses penyisipan watermark pada citra digital

Proses watermarking yang kedua adalah verifikasi *watermark*, hal ini dilakukan untuk membuktikan status kepemilikan citra digital. Proses ekstraksi ini disebut *decoding*, pada proses ini *image watermarking* diekstraksi dengan tujuan untuk mengungkap data *watermark* yang telah disisipkan dalam citra digital [10], seperti pada gambar 2



Gambar 2. Proses ekstraksi watermark

Klasifikasi *Watermarking*

Digital watermarking dapat dibagi ke dalam beberapa kategori [5] yaitu :

a. *Text watermarking*
b. *Image watermarking*
c. *Audio watermarking*
d. *Video watermarking*

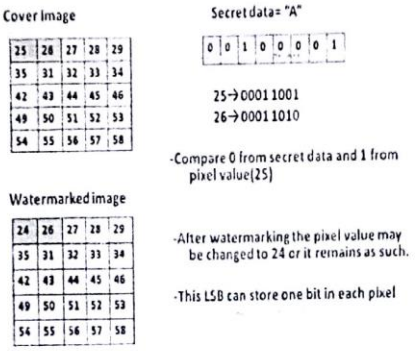
Sedangkan berdasarkan teknik atau metode cara kerjanya dapat dibagi menjadi beberapa teknik [5] yaitu :

a. Domain Spasial, merupakan teknik watermarking yang bekerja dengan cara menanamka watermark secara langsung ke dalam piksel dari suatu citra. Beberapa contoh teknik pada domain spasial adalah teknik penyisipan *Least Significant Bit* (LSB), *patchwork, masking filtering.*
b. Domain frekuensi
   Tenik watermarking yang bekerja dengan cara menanamkan watermark pada koefisien frekuensi hasil transformasi citra asalnya. Terdapat beberapa transformasi untuk menghasilkan koefisien frekuensi, antara lain *Discrete fourier transform* (DFT), *Discrate Cosine Transform* (DCT), *Discrete Wafalet Transform* (DWT), *Spreas Spectrum*, domain kompresi dan *hybrid.*

Least Significant bit (LSB)

LSB (Least Significant Bit) merupakan salah satu metode dalam *Steganography*. Pada LSB penyembunyian data dilakukan dengan mengganti deretan bit – bit belakang pada pixel gambar dengan bit – bit data rahasia[4]. Banyak cara yang dapat dilakukan untuk mengganti bit – bit warna pada citra, antara lain dengan melakukan operasi penambahan atau pengurangan nilai warna pada citra. Mengubah bit LSB dilakukan dengan mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya, sedangkan untuk memperkuat teknik penyembunyian data, bit – bit data rahasia tidak digunakan mengganti byte – byte yang

berurutan namun dipilih susunan byte secara acak. Tujuan utama dari LSB adalah memanipulasi nilai suatu titik warna (pixel) sehingga data dapat disembunyikan ke dalam titik warna tersebut namun perubahan yang terjadi berusaha diminimalisasi sehingga seakan – akan perubahannya tidak dapat dideteksi oleh mata manusia. Penggambaran teknik LSB [4,5] dapat dilihat lebih jelas pada gambar 3



Gambar 3. Representasi teknik LSB

Berdasarkan gambar 3 diatas dapat dijelaskan sebagai contoh cover image atau citra awal mempunyai nilai asal dari satu pixelnya yang berkoordinat 0,0 adalah 25 dengan nilai biner 0001 1001, sedangkan data rahasia atau watemark yang akan disisipkan memiliki nilai biner 00100001, satu bit dari data rahasia disisipkan pada bit akhir dari biner citra awal sehingga menjadi 00011000. Sehingga nilai pixel pada citra ter*watermark* dengan koordinat 0,0 adalah 24 atau 00011000 dalam biner.

Geometrical attack

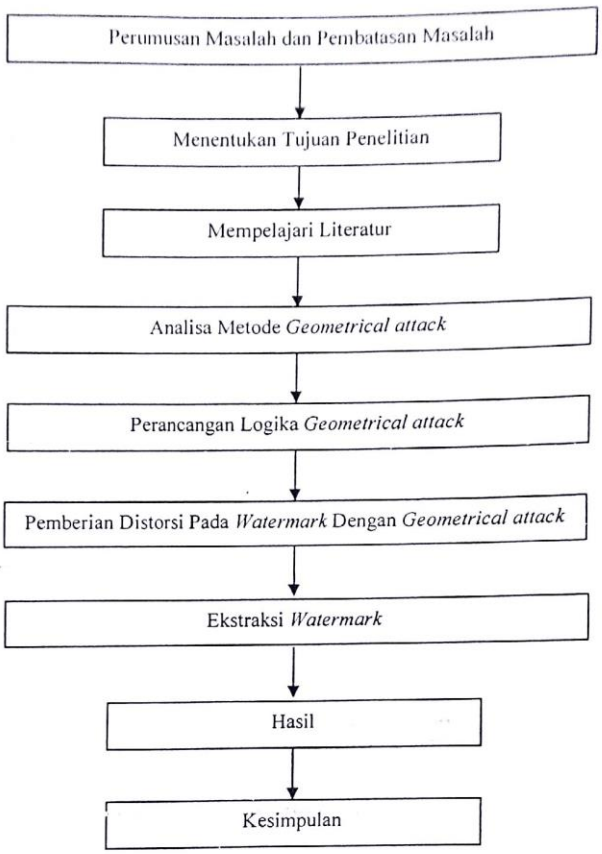
3. METODE PENELITIAN

Untuk memberikan panduan pada penelitian ini maka perlunya ada susunan kerangka kerja yang menjelaskan tahapan – tahapan yang akan dilakukan dalam penelitian ini. Seperti yang terlihat pada gambar 4.

Jenis serangan ini berkaitan dengan Transformasi Geometris yaitu jenis serangan yang paling dasar dalam teknik serangan terhadap *watermark*. Serangan jenis ini banyak dilakukan pada serangan awal, namun banyak media ber- *watermark* yang tidak lolos dari serangan sederhana ini, beberapa operasi transformasi geometris[5] yaitu:

1. Horizontal Flip
   Serangan ini dilakukan hanya dengan membalikkan gambar secara horizontal. Metode ini tampak sangat sederhana, namun beberapa skema watermarking tidak lolos dari serangan ini.
2. Rotasi
   Rotasi dilakukan biasanya dengan derajat perputaran yang sangat kecil, sehingga citra tampak tidak berubah. Namun karena perputaran yang kecil tersebut, *watermark* tidak dapat terdeteksi lagi.
3. Cropping
   Pemotongan citra menjadi bagian-bagian kecil. Hal ini mengakibatkan *watermark* tidak utuh dan kemudian menjadi tidak terdeteksi lagi.
4. Scaling
   Penskalaan dapat dibedakan menjadi 2 jenis, uniform dan non-uniform. Penskalaan uniform mengubah ukuran citra dengan faktor skala yang sama, baik vertikal maupun horizontal. Sedangkan pada non-uniform scaling faktor skala vertikal dan horizontal berbeda.
5. Penghapusan Garis atau Kolom
   Cara ini dilakukan dengan menghapus satu kolom atau satu baris pada citra. Cara ini sangat efektif dilakukan untuk melawan teknik spread-spectrum.
6. Random Geometric Distortion
   Melakukan distorsi geometris secara acak. Biasanya merupakan gabungan dari teknik- teknik dasar.

Vol. 1, Oktober 2015
ISSN : 2460 - 4690



Gambar 4. Kerangka Kerja

Dari kerangka kerja yang digambarkan diatas maka dapat diuraikan pembahasan sebagai berikut :

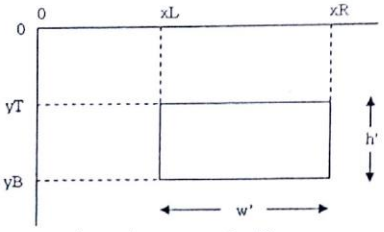
1. Perumusan dan pembatasana masalah
   Dalam penelitian ini masalah yang dirumuskan adalah bagaimana *watermark* yang terdapat pada *image watermarking* LSB jika mendapat serangan *geometrical attack.*
2. Menentukan tujuan penelitian
   Tujuan dari penelitian ini adalah untuk mengetahui tingkat kekokohan (*robustness*) dan kelemahan dari *image watermarking* LSB jika diberi *geometrical attack.*
3. Mempelajari literatur
   Selanjutnya melakukan peninjauan pustaka untuk mendukung analisa masalah yang akan diteliti. Pada tahap ini penulis merujuk kepada jurnal nasional, jurnal internasional, proceeding, hasil penelitian pada skripsi/thesis, buku dan data – data lain yang terkait dengan penelitian ini.
4. Analisa Metode *Geometrical attack.*
   Pada tahapan ini akan dijelaskan bagaimana *geometrical attack* dapat memberikan distorsi terhadap *watermark* yang terdapat pada *image watermarking* sehingga *watermark* tersebut tidak dapat dideteksi. Pada penelitian ini *geometrical attack* yang akan diberikan

Vol. 1, Oktober 2015
ISSN : 2460 - 4690

dalam bentuk rotasi searah jarum jam 45^0 dan *cropping*, peskalaan terhadap citra ter*watermark*.

Pada operasi cropping yang merupakan kegiatan memotong satu bagian dari citra dengan analisa yang digunakan

x' = x – xL untuk x = xL sampai xR
y' = y – yT untuk y = yT sampai yB



adalah memperkecil ukuran *image watermarking* analisa yang digunakan adalah

x' = Sh x
y' = Sv y

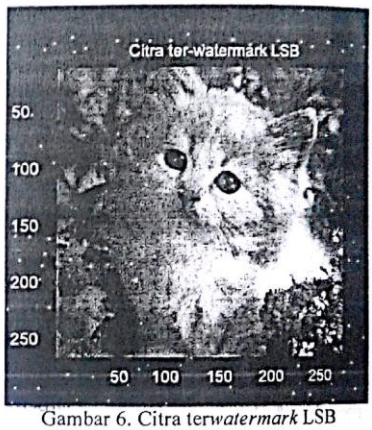
Sh = faktor skala horisontal
Sv= faktor skala vertikal
Ukuran citra berubah menjadi

w' = Sh w
h' = Sv h

5. Pemberian distorsi pada *watermark* dengan memberikan *geometrical attack*.
   Pada penelitian ini penulis akan menguji *image watermarking* dengan operasi transformasi geometris yang pertama rotasi 45° searah jarum jam dan cropping terhadap *image watermarking* sehingga terjadi perubahan koordinat dan terjadi pemotongan pada bagian tertentu dari *image watermarking* kemudian operasi geometris yang kedua adalah penskalaan (scaledown) dengan merubah ukuran pixel menjadi setengah dari ukuran sebelumnya, sehingga terjadi perubahan ukuran *image watermarking* menjadi lebih kecil 50 % dari citra awal.
6. Ekstraksi *Watermark*
   Proses ekstraksi ini digunakan untuk mengambil kembali *watermark* yang telah disisipkan kedalam citra awal. Proses ekstraksi dilakukan dengan tahapan yaitu pertama *image watermarking* dirubah kedalam bentuk matriks (bit). Selanjutnya diekstraksi untuk memisahkan *image* awal dengan *watermark*. Ekstraksi ini dilakukan dalam bentuk bit biner (*pixel*).
7. Hasil
   Setelah *image watermarking* mendapat distorsi *geometrical attack* dilakukan ekstraksi terhadap *watermark* yang terdapat pada *image watermarking* tersebut kemudian dilihat apakah terjadi perubahan pada *watermark* yang telah diekstraksi atau tidak.
8. Penarikan kesimpulan
   Berdasarkan hasil ekstraksi *watermark* akan ditarik kesimpulan bagaimana tingkat kekokohan *image watermarking* LSB terhadap *geometrical attack*.

4. HASIL DAN PEMBAHASAN

Pada pembahasan ini citra asli yang digunakan adalah citra dengan size 256 x 256. Citra telah diberlakukan penyisipan *watermark* dengan algoritma LSB (gambar 6). Citra ter*watermark* inilah yang akan dianalisa untuk mendapat perlakuan *geometrical attack*.

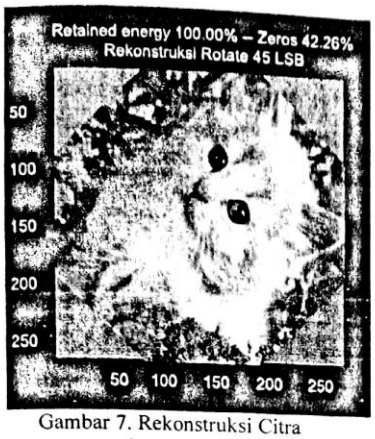


Gambar 6. Citra ter*watermark* LSB

Geometrical attack bertujuan untuk memberikan distorsi pada image yang telah ter*watermark*, sehingga *watermark* yang disisipkan pada citra awal saat diekstrak tidak dapat dideteksi. Beberapa gangguan (attack) yang akan diberikan tersebut antara lain adalah cropping (pemotongan citra), rotasi citra dan penskalaan citra.

1. Rotasi terhadap *image watermarking*
   Rotasi citra adalah salah satu cara untuk merusak *watermark* yang disisipkan pada citra awal, untuk menstimulasi efek rotasi ini maka dibangkitkan melalui fungsi 'bilinear', 'crop' pada Matlab. Pada penelitian ini gambar akan dirotasi dengan sudut searah putaran jarum jam dengan sudut 45°. Dari uji coba yang dilakukan maka diperoleh hasil seperti gambar 7.

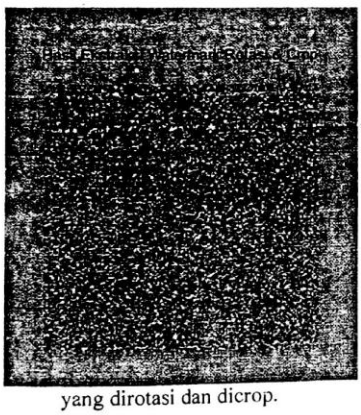
Vol. 1, Oktober 2015
ISSN : 2460 - 4690



Gambar 7. Rekonstruksi Citra ter*watermark image watermarking* LSB yang dirotasi dan dicrop

Dari gambar 7, *image watermarking* yang telah dicrop dan dirotasi telah kehilangan nilai – nilai intensitas pikel dibeberapa tempat yang menyebabkan hilangnya bit – bit *watermark* dari *image watermarking*, tetapi hilangnya bit – bit ini secara visual tidak begitu terlihat.

Selanjutnya akan dibuktikan apakah *watermark* mengalami perubahan atau tidak, dengan mengekstraksi *image watermarking* yang telah dirotasi dan dicrop.

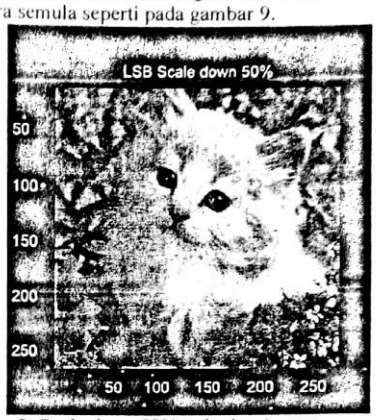


yang dirotasi dan dicrop.

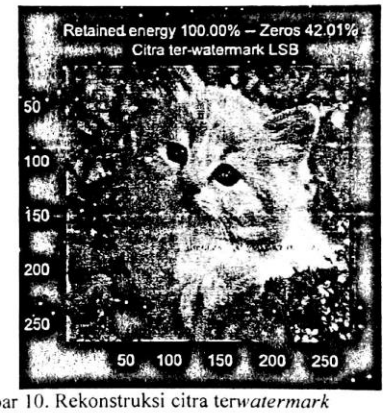
Dari gambar 8. Dapat dilihat hasil ekstraksi pada *image watermarking* LSB tidak dapat diekstrak dengan sempurna atau mengalami kerusakan, hali ini disebabkan oleh adanya bit – bit *watermark* yang hilang karena dirotasi dan dicrop.

2. Rescaling *image watermarking*

Serangan juga dapat berupa penskalaan citra pada citra ter*watermark*. Operasi penskalaan yang dilakukan adalah *zoom in* (pengecilan) terhadap citra ter*watermark* yaitu dengan mengalikan ukuran citra ter*watermark* dengan faktor skala = ½ sehingga didapat ukuran citra setengah dari ukuran citra semula seperti pada gambar 9.

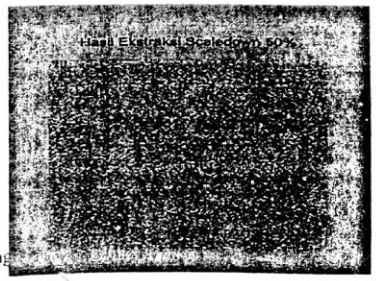


Gambar 9. *Scale down* 50% terhadap *image watermarking* LSB



Gambar 10. Rekonstruksi citra ter*watermark* scaledown 50 % pada *image watermarking* LSB

Kemudian dilakukan ekstraksi terhadap citra ter*watermark* untuk melihat perubahan yang terjadi pada *watermark* setelah mengalami penskalaan.



Billy Hendrik[1], Mardhiah Masril[2]
[1,2]Fakultas Ilmu Komputer, Universitas Putra Indonesia YPTK Padang

Vol. 1, Oktober 2015
ISSN : 2460 - 4690

Gambar 11. Hasil ekstraksi *watermark* terhadap *image watermarking* LSB scaledown 50 %

Pada gambar 11. Dapat dilihat hasil ekstraksi *watermark* terhadap citra ter*watermark* yang telah mengalami perubahan ukuran citra dimana *watermark* mengalami kerusakan.

5. KESIMPULAN

Berdasarkan pembahasan dan hasil yang diperoleh maka dapat ditarik kesimpulan sebagai berikut:

1. Pada metode LSB penyembunyian data dilakukan dengan mengganti bit-bit data didalam segmen citra dengan bit-bit data rahasia. Ternyata meode LSB berfungsi sangat baik ketika *image* yang digunakan dalam format *grayscale* karena perubahannya akan sulit dideteksi oleh mata.
2. *Image watermarking* LSB yang mendapat perlakuan *geometrical attack* seperti rotasi 45° dan *cropping* kemudian juga *Scale down* 50%, *watermark* yang terdapat didalamnya tidak dapat diekstrak dengan baik; hal ini dapat dilihat pada hasil ekstraksinya yang berbeda dengan *watermark* awal. Dengan demikian dapat dinyatakan tingkat kekokohan *(Robustness) image watermarking* LSB terhadap transformasi geometris masih perlu ditingkatkan.

6. REFERENSI

[1] Arhami, M dan Desiani, A. 2004. *Pemrograman Matlab*. Edisi 1. Andi. Yogyakarta.

[2] Arnorld, M. Scmucker & Wolthusen. 2003. Techniques and Applications of Digital Watermarking and Content Protection. Artech House. Inc, Boston.

[3] Ch, Wijaya dan Prijono, A. 2007. *Pengolahan Citra Digital Menggunakan Matlab Image Processing Toolbox*. Edisi 1. Informatika. Bandung

[4] Gurpreet, Kamaljeet. 2013. Image Watermarking Using LSB (Least Significant Bit). *International Journal of Advances Research in Computer Science and Software Engineering*. 3 (4): 858-859.

[5] Goyal, R. Kumar, N. 2014. LSB Based Digital Watermarking Technique. *International Journal of Application or Innovation in Engineering & Management (I JAI EM)*. 3 (9): 15-16.

[6] Kharrazi, Mehdi., Husrev T. Sencar, and Nasir Memon. 2004. Image Steganography:
Concepts and Practice

[7] Munir, R. 2004. *Pengolahan Citra Digital dengan pendekatan Algoritmik*. Edisi 1. Informatika.Bandung.

[8] Putri, D. Kusuma, A. Hidayati, N. Torang,J. Trstanto,Y. Wicaksana, I. 2008. Membandingkan Steganography dan Watermarking Pada Keamanan File Grafik. Proceeding Seminar Ilmiah Nasional Komputer dan Sistem Intelijan Auditorium Universitas Gunadarma, 20-21 Agustus 2008, Depok. Hal. 419 -422.

[9] Rini, S. 2012. Perbandingan Performasi Citra Steganography Untuk Proteksi Hak Cipta Dengan Metode Least Significant Bit Insertion Dan Discrete Wavelet Transform. *Skripsi*. Universitas Dian Nuswantoro, Semarang.

[10] Sharma, P. Rajni. 2012. Analysis of Image Watermarking Using Least Significant Bit Algorithm. *International Journal of Information Sciences and Techniques (IJIST)*. 2 (4) : 96-98.

[11] Sugiharto, A. Sarwoko, E. 2004. Watermarking pada beberapa keluarga wavelet. *Jurnal Matematika dan Komputer*. 7 (3):18-25.