

Penerapan Teknik Digital Watermarking untuk perlindungan Citra Digital BITMAP IMAGE dengan metode LSB dan MD5

**Sri Esti T S, Nikmatus Sholihah
STMIK Pradnya Paramita (STIMATA) Malang**

Abstrak Perubahan penyajian data dari analog menjadi digital ternyata membawa masalah pada perlindungan hak cipta dan otentikasi citra digital. Hal ini terjadi karena begitu mudahnya penggandaan yang dapat dilakukan terhadap citra digital.

Digital watermarking dapat diterapkan untuk menyisipkan label hak cipta ke dalam citra digital secara invisible. Hal ini akan mempersulit pihak yang tidak berwenang untuk menghapus label hak cipta sehingga hanya pihak yang berwenang saja yang mampu mengungkap label hak cipta tersebut. Metode yang digunakan adalah metode LSB (Least Significant Bit). Untuk melindungi otentikasi citra digital terhadap modifikasi dapat digunakan metode MD5 (Message Digest 5) karena perubahan sekecil apapun terhadap citra akan merubah nilai MD5.

Oleh karena itu, tujuan dari Skripsi ini adalah menciptakan aplikasi software yang mengimplementasikan metode LSB dan MD5 untuk melindungi Hak Cipta dan Otentikasi citra digital diam.

Kata Kunci: Digital Watermarking, LSB, MD5, Hak Cipta, Otentikasi

Abstract Changes in presentation of data from analog to digital was brought problems on copyright protection and authentication of digital images. This happens because of the ease with which copies can be made on a digital image. Digital Digital watermarking can be applied to insert a copyright tag to the digital image is invisible. This would make an unauthorized person to remove the copyright labels so that only authorized parties are able to uncover the copyright label. The method used is the method of LSB (least significant bit). To protect the authentication of digital images for modification of the method can be used MD5 (Message Digest 5) because the slightest change to the image will change the MD5 value.

Therefore, the purpose of this thesis is to create software applications that implement the LSB method and MD5 to protect the Copyright and authentication of digital still images.

*Key word : Digital water marking, **LSB**, **MD5**, Copyright, Authentication.*

1. Pendahuluan

1.1 Latar Belakang

Berdasarkan berbagai kelebihan tersebut, teknik Watermarking dapat digunakan sebagai suatu cara perlindungan hak cipta, dan prosedur pengecekan keaslian hasil karya fotografi digital dalam format Bitmap Image (BMP). Dalam implementasinya, penerapan teknik Watermarking perlu diikuti dengan penerapan metode penyisipan data Watermarking, yang menjamin tidak terjadinya kerusakan/perubahan Bitmap Image yang dilindungi secara signifikan.

Banyak algoritma yang dapat digunakan untuk penerapan teknik Watermarking. Baik yang bekerja pada domain spasial maupun domain transformasi. Pada domain spasial, Watermark bekerja langsung pada *pixel-pixel* media penampung, sehingga mudah diimplementasikan. Contohnya adalah metode LSB (*Least Significant Bit*) yang bekerja dengan menggantikan bit-bit terakhir media penampung, dengan bit-bit data Watermark yang digunakan. Sedangkan pada domain transformasi, watermark bekerja pada hasil transformasi media penampung secara matematis sehingga diperlukan pemahaman teori matematika yang rumit. Contohnya adalah melalui *Discrete Cosinus Transform* (DCT) maupun *Wavelet Transform*.

Selain itu data digital watermark juga perlu dienkripsi dengan suatu metode tertentu agar tidak mudah terbaca oleh pihak lain. Watermark juga harus memiliki kunci yang unik untuk penyisipan dan ekstraksinya. Watermark unik untuk tiap citra, bisa didapatkan dari nilai *hash* citra dengan menggunakan metode MD5 (*Message Digest 5*). MD5 adalah fungsi *hash* satu arah yang dibuat oleh Ronald Rivest pada tahun 1991.

Algoritma MD5 menerima masukan berupa pesan dengan ukuran sembarang dan menghasilkan *message digest* yang panjangnya 128 bit (Munir, 2006:220). Dengan algoritma MD5, dimungkinkan setiap citra digital yang dilindungi, memiliki nilai *hash* citra yang unik (berbeda dengan lainnya), serta mudah untuk ekstraksi ulang. Sebagaimana dipaparkan oleh Ramayanti (2007:9).

1.2 Perumusan Masalah

Bagaimana mengimplementasikan teknik digital watermarking untuk melindungi hak cipta dan keaslian citra digital berformat BMP, dengan menggunakan metode Least Significant Bit (LSB) dan Message Digest 5 (MD5) dalam bentuk software aplikasi komputer ?.

1.3 Tujuan Penelitian

Tujuan pokok penelitian ini adalah :

1. Mengimplementasikan dan menguji ketahanan metode LSB (*Least Significant Bit*) dan metode MD5 (*Message Digest 5*) untuk melindungi hak cipta serta otentikasi citra digital diam dg bahasa pemrograman Delphi 6.

1.4 Batasan Penelitian.

Batasan penelitian ini adalah sebagai berikut :

1. Data digital yang digunakan sebagai media dan label hak cipta (*watermark*) adalah citra digital diam (*still image*) dengan format BMP.
2. Penyisipan dan pengungkapan kembali label hak cipta (*watermark*) menggunakan metode LSB (*Least Significant Bit*).
3. Otentikasi citra menggunakan metode MD5 (*Message Digest 5*).
4. Pengujian ketahanan metode LSB (*Least Significant Bit*) dan metode MD5 (*Message Digest 5*) dengan memberikan beberapa serangan berupa *cropping*, kompresi GIF, perubahan kontras, penggandaan dan pemberian *noise* terhadap citra hasil *watermark*.

1.5 Kajian Teori.

a. Citra Digital BMP

Sub bab ini akan membahas definisi citra digital dan format *file* BMP menurut pakar. Menurut Rachmat & Roswanto (2005:5-6):

Citra digital merupakan suatu fungsi dengan nilai-nilai yang berupa **intensitas cahaya pada tiap-tiap titik** pada bidang yang telah diquantisasikan (diambil sampelnya pada interval diskrit). Titik dimana suatu gambar di-sampling disebut *picture element* (pixel). Nilai intensitas warna pada suatu pixel disebut *gray scale level*.

1 bit → *binary-valued image* (0-1)

8 bits → *gray level* (0-255)

16 bits → *high color* (2^{16})

24 bits → 2^{24} *true color*

32 bits → *true color* 2^{32}

Sedangkan format *file* BMP menurut Syahbana (2007:5) :

Format *file* BMP (Bitmap Image) merupakan format grafis yang fleksibel untuk platform Windows sehingga dapat dibaca oleh program grafis manapun. Format ini mampu menyimpan informasi dengan kualitas tingkat 1 bit sampai 24 bit. Format *file* ini mampu menyimpan gambar dalam mode warna RGB, *Grayscale*, *Indexed Color*, dan Bitmap.

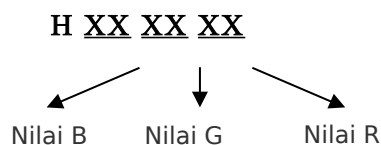
b. Mode Warna RGB

Menurut Syahbana (2007:3) bahwasanya:

Mode warna RGB (*Red, Green, Blue*) merepresentasikan gambar dengan 3 *channel*, *red* (merah), *green* (hijau), dan *blue* (biru). Masing-masing *channel* disimpan sebagai informasi 8 bit yang akan mempunyai 256 nilai gradasi. Jadi yang bisa direpresentasikan dengan sistem 24 (8x3) bit ini adalah 16 juta variasi warna dari kombinasi ketiga *channel*.

Sedangkan penjelasan mengenai masing-masing *channel* seperti tertulis pada *paper* ilmiah Puspitasari (2007:9-10) bahwasanya:

Masing-masing *channel* nilainya berada dalam *range* h00 (0 desimal) sampai dengan hFF (255 desimal) atau mempunyai nilai derajat keabuan $256=2^8$. Definisi warna tersebut adalah sebagai berikut, variabel H menyatakan angka dibelakangnya adalah hexadesimal.



Gambar 2.2 Susunan Bit RGB dalam Hexadesimal

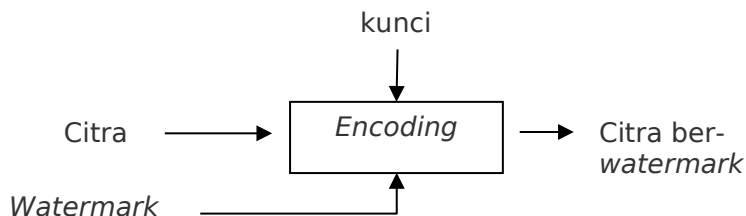
c. Sekilas Mengenai *Watermarking* Digital

Menurut Munir (2006:311-313) bahwasanya:

Teknik *watermarking* secara umum terdiri dari 2 tahapan yakni:

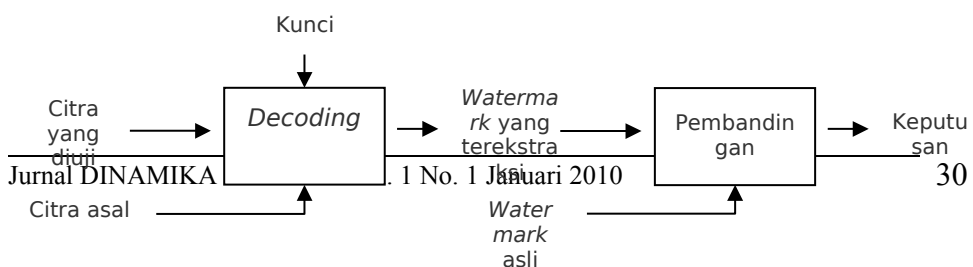
- Penyisipan *watermark* (*watermark embedding*)
- Ekstraksi atau pendeteksian *watermark*

Penyisipan *watermark* dapat dipandang sebagai superposisi data *watermark* pada citra dengan suatu cara sedemikian sehingga superposisi tersebut tidak mempengaruhi persepsi visual terhadap citra. Gambar 2.6 memperlihatkan sebuah *encoder* yang melakukan penyisipan *watermark*. *Encoder* menerima masukan berupa citra, *watermark*, dan kunci. *Encoder* menghasilkan citra ber-*watermark*. Citra asal dan citra ber-*watermark* hampir mirip secara statistik, atau secara visual mempunyai persepsi yang sama.



Gambar 2.6 Proses Penyisipan *Watermark* ke dalam Citra

Watermark harus dapat diekstraksi atau dideteksi kembali. *Decoder* menerima masukan berupa citra uji, kunci *k*, dan menghasilkan *watermark* terekstrak. *Decoder* dapat mengikutsertakan citra asal yang belum diberi *watermark* (*non-blind watermarking*) atau tidak sama sekali (*blind watermarking*). Selanjutnya *watermark* terekstraksi dibandingkan dengan *watermark* asli dengan fungsi komparator untuk menghasilkan keputusan berupa keluaran biner (1 menyatakan cocok, 0 menyatakan sebaliknya).



Gambar 2.7 Proses Ekstraksi dan Verifikasi *Watermark* dari dalam Citra

2. Metode Penelitian.

1. Tahap persiapan

- Melakukan studi literatur pada beberapa jurnal maupun *paper* ilmiah yang diperoleh dari internet serta beberapa buku yang berhubungan dengan citra digital.
- Melakukan pemahaman dan analisa cara kerja masing-masing metode.

2. Pengembangan model awal

- a. Perancangan *interface* program *digital watermarking*.
- b. Mengimplementasikan metode MD5 untuk otentikasi citra.
- c. Mengkombinasikan metode LSB dengan MD5 untuk unikasi *watermark*.
- d. Memanfaatkan *header* bitmap untuk menyimpan *ciphertext* hasil operasi XOR ukuran *watermark*.

3. Uji kelayakan program.

- 4. Pembuatan model akhir dengan menggabungkan unit-unit program yang sudah dibuat menjadi sebuah aplikasi *digital watermarking* yang utuh.
- 5. Melakukan pengujian secara individual terhadap citra hasil *digital watermarking* terhadap serangan berupa *cropping*, kompresi GIF, perubahan kontras, penggandaan dan pemberian *noise*.

6. Melakukan pengujian aplikasi *digital watermarking*.

3. Hasil dan Pembahasan Penelitian.

1. Pengujian Ketahanan Citra Hasil *Embedding*

1.1.1 Pengujian Ketahanan Citra Hasil terhadap Proses *Cropping*

Pengujian dilakukan dengan memotong bagian tertentu dari citra hasil proses *embedding*. Kemudian dilakukan *extracting* menggunakan aplikasi MyImage untuk mengetahui apakah label hak cipta masih terbaca dan apakah citra dinyatakan tidak otentik.

Dari hasil pengujian didapatkan prosentase keberhasilan pembacaan label sebesar 100% serta prosentase otentikasi sebesar 66,67%. Dengan menganalisa hasil otentikasi didapatkan bahwasanya jika pemotongan dilakukan pada sebagian kecil citra dan tidak mengenai bit yang menyimpan nilai MD5, maka citra dibaca sebagai citra otentik.

1.1.2 Pengujian Ketahanan Citra Hasil terhadap Proses Kompresi GIF

Pengujian dilakukan dengan menyimpan citra hasil proses *embedding* ke dalam format *file* GIF menggunakan bantuan program Adobe Photoshop. Kemudian dilakukan penyimpanan kembali ke dalam format *file* BMP menggunakan Adobe Photoshop lalu dilakukan *extracting* menggunakan aplikasi MyImage untuk mengetahui apakah label hak cipta masih terbaca dan apakah citra dinyatakan tidak otentik.

Dari hasil pengujian didapatkan prosentase keberhasilan pembacaan label sebesar 44,44% serta prosentase otentikasi sebesar 66,67%. Dengan menganalisa hasil pembacaan label didapatkan bahwa kompresi GIF pada citra *grayscale* dengan label hitam putih hanya menyebabkan perubahan warna label sehingga label masih dapat dibaca. Sedangkan pada citra hitam putih tidak terpengaruh proses kompresi GIF sehingga label bisa terbaca. Dari hasil otentikasi didapatkan bahwasanya kompresi GIF tidak merubah nilai MD5 yang ada pada citra hitam putih sehingga citra dibaca sebagai citra otentik.

1.1.3 Pengujian Ketahanan Citra Hasil terhadap Proses Perubahan Kontras

Pengujian dilakukan dengan melakukan auto kontras citra hasil proses *embedding* dengan bantuan program Adobe Photoshop. Kemudian dilakukan *extracting* menggunakan aplikasi MyImage untuk mengetahui apakah label hak cipta masih terbaca dan apakah citra dinyatakan tidak otentik.

Dari hasil pengujian didapatkan prosentase keberhasilan pembacaan label sebesar 33,33% serta prosentase otentikasi sebesar 66,67%. Dengan menganalisa hasil pembacaan label didapatkan bahwa auto kontras pada citra hitam putih tidak merusak label sehingga label masih dapat dibaca. Sedangkan dari hasil otentikasi didapatkan bahwasanya auto kontras tidak merubah nilai MD5 yang ada pada citra hitam putih sehingga citra dibaca sebagai citra otentik.

1.1.4 Pengujian Ketahanan Citra Hasil terhadap Proses Penggandaan

Pengujian dilakukan dengan melakukan *copy-paste* citra hasil proses *embedding*. Kemudian dilakukan *extracting* menggunakan aplikasi MyImage terhadap citra hasil penggandaan untuk mengetahui apakah label hak cipta masih terbaca dan apakah citra dinyatakan otentik.

Dari hasil pengujian didapatkan prosentase keberhasilan pembacaan label sebesar 100% serta prosentase otentikasi sebesar 100%. Dengan menganalisa hasil pembacaan label serta hasil otentikasi didapatkan bahwasanya penggandaan tidak merubah bit-bit citra sehingga label dapat terbaca dan citra dibaca sebagai citra otentik.

1.1.5 Pengujian Ketahanan Citra Hasil terhadap Proses Pemberian Noise

Pengujian dilakukan dengan memberi *noise* pada citra hasil proses *embedding* dengan bantuan program Adobe Photoshop. Kemudian dilakukan *extracting* untuk mengetahui apakah label hak cipta masih terbaca dan apakah citra dinyatakan tidak otentik.

Dari hasil pengujian didapatkan prosentase keberhasilan pembacaan label sebesar 0% serta prosentase otentikasi sebesar 100%. Dengan menganalisa hasil pembacaan label serta hasil otentikasi didapatkan bahwasanya pemberian *noise* merubah bit-bit citra sehingga label tidak dapat terbaca dan citra dibaca sebagai citra tidak otentik.

5. Kesimpulan dan Saran.

a. Kesimpulan

Berdasarkan analisa yang dilakukan, dengan adanya implementasi *digital watermarking* yang sudah dibuat serta pengujian yang dilakukan dapat diambil kesimpulan bahwa metode LSB (*Least Significant Bit*) cukup handal digunakan sebagai metode untuk *digital watermarking* dengan bahasa pemrograman Delphi 6, dikarenakan tingkat invisibilitasnya yang tinggi. Dengan prosentase keberhasilan otentikasi sebesar 80%, maka dapat disimpulkan bahwasanya metode MD5 (*Message Digest 5*) cukup handal digunakan untuk otentikasi citra dengan bahasa pemrograman Delphi 6. Rata-rata keberhasilan pembacaan label hak cipta hasil *digital watermarking* dengan mengimplementasi metode LSB (*Least Significant Bit*) dan MD5 (*Message Digest 5*), setelah diberi serangan berupa *cropping*, kompresi GIF, perubahan kontras, penggandaan dan pemberian *noise* adalah 55,55% berarti cukup *robust*.

b. Saran

Dari implementasi *digital watermarking* yang sudah dibuat serta pengujian yang sudah dilakukan, terdapat beberapa kelebihan dan kekurangan. Kelebihannya antara lain kesederhanaan implementasi metode LSB yang tidak menuntut model matematika yang rumit serta kemampuan invisibilitas hasil metode LSB yang tinggi, dilihat dari kesamaan visual antara citra asli dan citra yang sudah diberi label. Sedangkan kekurangannya antara lain bahwasanya bit-bit hasil metode LSB kurang mampu bertahan dari proses pengolahan citra yang bisa merubah nilai bit. Kekurangan lainnya adalah nilai otentikasi kurang *valid* jika terjadi modifikasi kecil yang tidak mengenai bit tempat menyimpan nilai MD5 pada citra hasil *embedding*. Oleh karenanya untuk pembuatan dan pengembangan aplikasi perlindungan hak cipta serta otentikasi citra lebih lanjut, disarankan:

1. Pengimplementasian metode selain LSB untuk meningkatkan *robustness* hasil *digital watermarking* terhadap jenis serangan yang lebih variatif dan kompleks.
2. Teknik penyisipan MD5 secara berulang pada label hak cipta maupun pengimplementasian metode selain MD5 untuk meningkatkan kemampuan otentikasi citra hasil *digital watermarking*.
3. Pengembangan jenis media yang mampu diproses dalam *digital watermarking*. Baik itu dari format *file*, citra bergerak, media audio, dll.
4. Pengembangan teknik penyimpanan *password* dan system keamanan aplikasi.

DAFTAR PUSTAKA.

<http://id.wikipedia.org/wiki/Enkripsi> (diakses tanggal 15 November 2007).

Munir, Rinaldi. 2005. *Image Watermarking untuk Memproteksi Citra Digital dan Aplikasinya pada Citra Medis*. Bandung: Institut Teknologi Bandung.

Munir, Rinaldi. 2006. *Kriptografi*. Bandung: Informatika.

Puspitasari, Ratna. 2007. *Aplikasi Watermarking Guna Pelabelan Citra Digital Menggunakan Metode LSB*. Malang: Join Program BA.

Rachmat, Antonius S.Kom dan Roswanto, Alphone S.Kom. <http://lecturer.ukdw.ac.id/anton/download/multimedia2.pdf>. (download tanggal 18 September 2007).

Rachmat, Basuki. 2004. <http://library.gunadarma.ac.id/files/disk1/2/jbptguna-darma-gdl-s1-2004-basukirach-93-bab2.pdf>. Jakarta:Gunadarma. (download tanggal 25 Januari 2008)

Ramayanti, Desi. <http://www.cert.or.id/~budi/courses/security/2006-2007/Report-Desi-Ramayanti.pdf> (download tanggal 15 November 2007)

Sari, Dian Kartika, SH., LL.M. *Potensi Cipta Universitas Goes To Market*. 2006-09-05. <http://www.ipcenter-ui.org/artikel.php?artikelid=32>. (telah diterbitkan pada Buletin "KONVERGENSI" Edisi III tanggal 28 Agustus 2006).

Swanson, M., D., Zhu, B., Chau, B., dan Tewfik, A., H. 1997. *Multiresolution Video Watermarking using Perceptual Models and Scene Segmentation*, Proceeding of the IEEE International Conference of Image Processing 1997: Vol II, pp.558-561. http://debut.cis.nctu.edu.tw/~ykleee/Research/Watermarking/Ahmed_H_Tewfik/IEEE-ICIP-1997-1.pdf.

Syahbana, Tiuh. http://dosen.palcomtech.ac.id/syahbana/tiuh/2007/01/format-file-pada-photoshop/January_19,2007. (download tanggal 18 September 2007).

Zakaria, Teddy Marcus. 2003. *Pemrograman Delphi untuk Pemula: IDE dan Struktur Pemrograman*. <http://www.ilmukomputer.com>

Zine. http://ezine.echo.or.id/ezine14/04_Algoritma_Enkripsi_One_Time_Pad.txt (download tanggal 15 November 2007).

