Digital Watermarking untuk Melindungi Informasi *Multimedia*

Achmad Solichin

Email: achmad.solichin@budiluhur.ac.id

Fakultas Teknologi Informasi, Universitas Budi Luhur,

Jakarta

ABSTRAKSI

Melindungi informasi termasuk dokumen *multimedia* merupakan suatu kebutuhan utama dalam era keterbukaan informasi seperti saat ini. Multimedia dalam berbagai bentuk seperti teks, gambar, audio dan *video* mudah sekali menyebar dengan menggunakan media internet. Keaslian dari dokumen *multimedia* tersebut perlu dilindungi.

Paper ini memaparkan mengenai *digital watermarking* sebagai salah satu metode untuk melindungi keaslian informasi yang terkandung dalam dokumen *multimedia*. Dalam paper juga dibahas mengenai berbagai teknik *watermarking* yang dapat diterapkan di berbagai dokumen *multimedia*. Di bagian akhir paper akan dijelaskan juga mengenai batasan dan operasi yang dapat menghambat atau mengganggu dokumen *multimedia* yang sudah disisipi *watermark*.

1. PENDAHULUAN

Dalam era teknologi informasi dan komputer saat ini, informasi dalam bentuk dan media dapat tersebar dengan begitu cepat. Apalagi dengan adanya internet yang penyebarannya begitu pesat, informasi dapat menyebar dengan cepat dan mudah tanpa mengenal ruang dan waktu. Informasi dalam bentuk *digital* memiliki sifat yang mudah untuk diubah dan dimodifikasi, sehingga dapat mengakibatkan permasalahan kepemilikan informasi itu sendiri. Keaslian informasi dalam berbagai bentuk dan medita tidak lagi terjaga karena setiap orang dapat mengubah dan memodifikasinya untuk kemudian disebarkan kembali.

Oleh karena itu, diperlukan adanya suatu teknik dan metode untuk melindungi keaslian informasi di dalam suatu media. Salah satu teknik yang dapat digunakan untuk melindungi isi dan informasi yang terkandung dalam berbagai media adalah teknik *digital watermarking*.

Paper ini berusaha memaparkan berbagai teknik *digital watermarking* yang dapat diterapkan untuk melindungi informasi di dalam berbagai bentuk media *digital*.

2. MULTIMEDIA

Dalam [2], dinyatakan bahwa terminologi *multimedia* secara sederhana merupakan suatu media yang tidak hanya terdiri dari teks. Namun secara lengkap, *multimedia* dapat diartikan sebagai gabungan dari dua atau lebih media termasuk teks, gambar, audio, *video* dan animasi.

Beberapa definisi *multimedia* menurut para ahli:

a) Kombinasi dari komputer dan *video* (Rosch, 1996)
b) Kombinasi dari tiga elemen: suara, gambar dan teks (McComick, 1996)
c) Kombinasi dari paling sedikit dua media input atau output. Media ini dapat berupa audio (suara, musik), animasi, *video*, teks, grafik dan gambar (Turban dkk, 2002)
d) Alat yang dapat menciptakan presentasi yang dinamis dan interaktif yang mengkombinasikan teks, grafik, animasi, audio dan *video* (Robin dan Linda, 2001)
e) Multimedia dalam konteks komputer menurut Hofstetter, 2001 adalah pemanfaatan komputer untuk membuat dan menggabungkan teks, grafik, audio, *video* dengan menggunakan *tool* yang memungkinkan pemakai berinteraksi, berkreasi dan berkomunikasi.
f) *Any combination of two or more media, represented in a digital form, sufficiently well integrated to be presented via a single interface, or manipulated by a single computer program* [17]

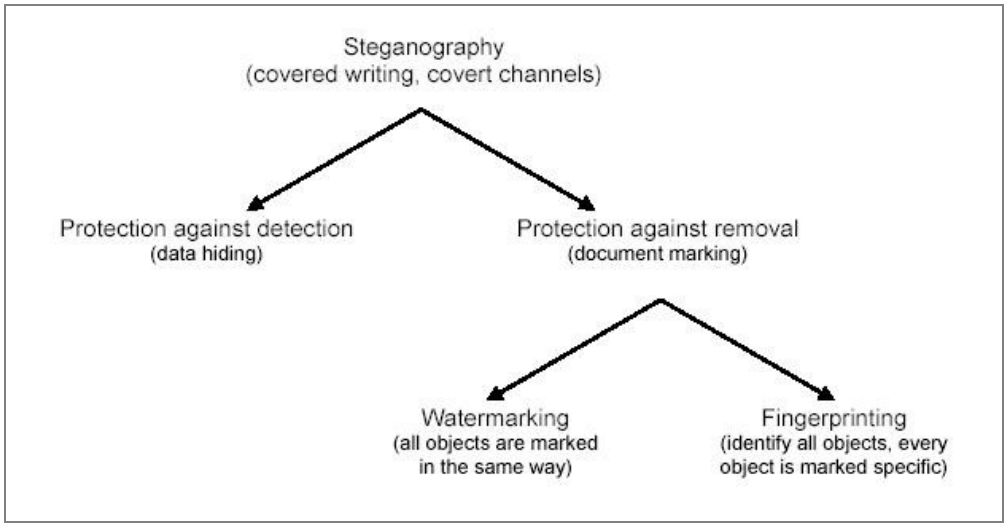
Dari keseluruhan definisi tersebut, terdapat kesamaan bahwa *multimedia* terdiri dari beberapa bentuk media dasar yang saling terintegrasi dan mengandung suatu pesan tertentu. Adapun bentuk-bentuk media pada dasarnya terdiri dari 4 (empat) bentuk, yaitu:

a. *Text* (.doc, .txt, .pdf dan sebagainya)
b. *Image* (.jpg, .gif, .png, .tiff, .bmp dan sebagainya)
c. Audio (.mp3, .wav, .au, dan sebagainya)
d. *Video* (.avi, .dat, .mov dan sebagainya)

3. DIGITAL WATERMARKING

Secara hierarkis, *watermarking* merupakan suatu proses yang berakar pada konsep ilmu *steganography*. *Steganography* sendiri sudah dikenal sejak jaman Mesir kuno. Menurut Cachin dalam [3], *steganography* diartikan sebagai suatu seni dan ilmu untuk menyembunyikan pesan yang sebenarnya sehingga orang awam tidak dapat mendeteksinya.

Menurut Popa dalam [19], *steganography* dapat dibagi menjadi 2 (dua) bagian yaitu *protection against detection* (*data hiding*) dan *protection against removal* (*document marking*). *Watermarking* merupakan salah satu jenis dari *document marking*. Pembagian *steganography* dapat terlihat dalam gambar sebagai berikut.



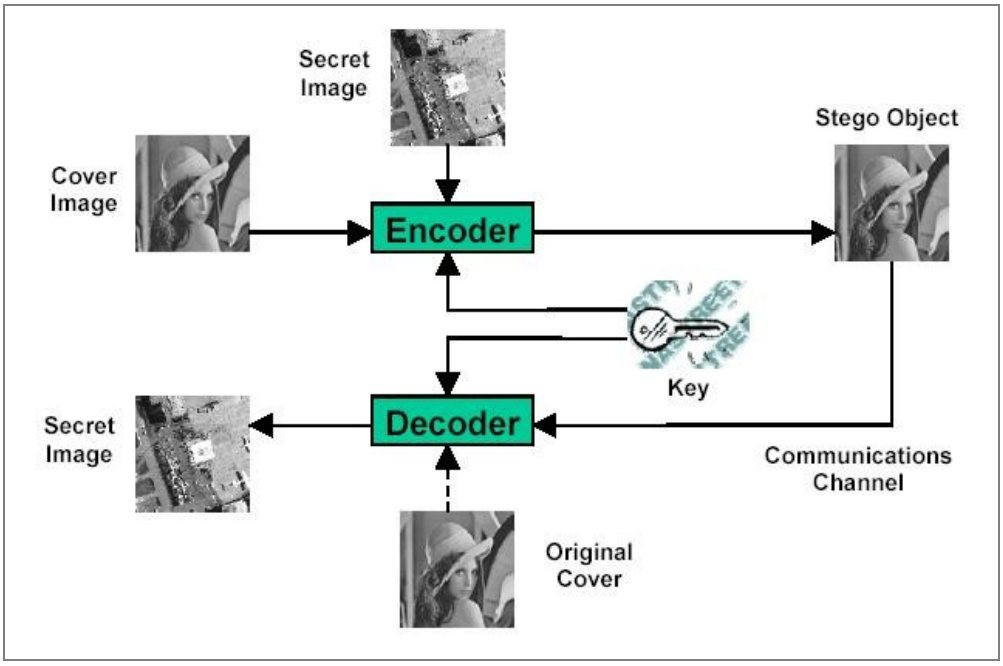
Gambar 1. Pembagian *Steganography*

Steganography juga digunakan selama perang dunia kedua, antara lain untuk mengirim pesan-pesan rahasia agar tidak diketahui oleh musuh. Sebagai contoh, seorang mata-mata German pernah mengirimkan pesan "**Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects for pretext embargo on by-products, ejecting suets and vegetable oils.**" Rangkaian pesan tersebut ternyata memiliki pesan tersembunyi yang akan terlihat dengan mengambil huruf kedua dari tiap kata. Pesan sebenarnya adalah "**Pershing sails for NY June 1**".

Perkembangan dunia internet yang memungkinkan semua bentuk media dapat menyebar dengan mudah, mendorong pembuat dokumen *multimedia* untuk menambahkan suatu tanda di dalam dokumen *multimedia* yang dibuat. Tanda (*marking*) yang ditambahnya umumnya berupa identitas atau *copyright* dari dokumen tersebut.

Watermarking merupakan teknik penyisipan data ke dalam elemen *multimedia* seperti citra, audio atau *video* [4]. Data yang disisipkan tersebut kemudian harus dapat diekstrak atau

dideteksi berada di dalam *multimedia* tersebut. Dari pengertian tersebut, terdapat dua proses utama dalam *watermarking*, yaitu proses menyisipkan data (*encode*) dan proses mengekstrak data (*decode*). Secara umum proses yang terjadi dalam *watermarking* terlihat dalam gambar berikut ini.



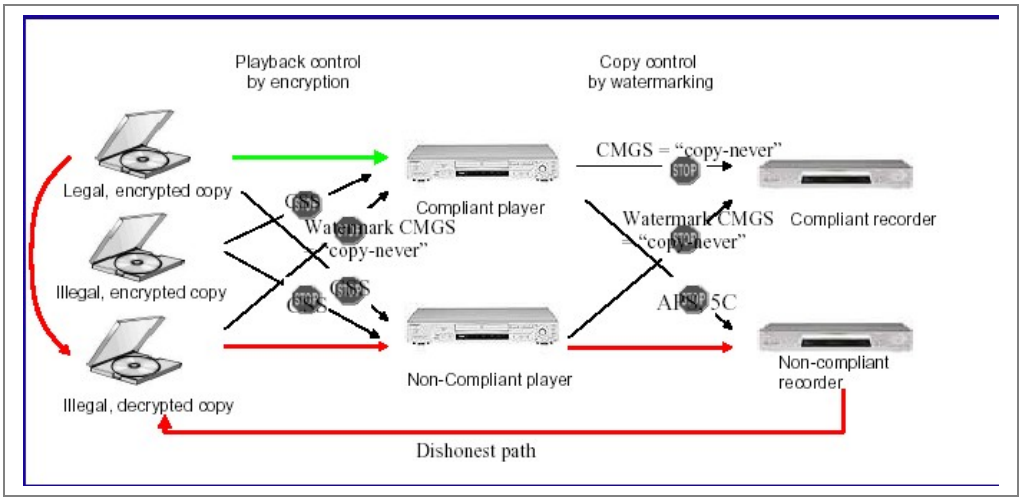
Gambar 2. Proses Watermarking

Dari gambar tersebut terlihat bahwa gambar asli akan di-*encode* dengan menambahkan gambar rahasia dan kunci tertentu. Gambar yang sudah di-*encode*, selanjutnya dapat ditransfer melalui suatu jalur komunikasi dan jika akan diperiksa keasliannya atau ingin mendapatkan gambar aslinya, maka dilakukan proses *decoder*. Proses *decoder key* (kunci) yang sama dengan kunci pada proses *encode*.

Menurut [5], teknik *digital watermarking* dapat diaplikasikan dalam berbagai hal, antara lain:

1. ***Ownership Assertion***. Kepemilikan dari dokumen *multimedia* dapat dilindungi dengan menambahkan *watermark* yang berisi informasi pemilik dari dokumen *multimedia*. Pemilik juga dapat mempublikasikan dokumen *multimedia* yang sudah disisipi *watermark* dengan aman tanpa harus mempublikasikan dokumen *multimedia* yang asli. Jika terjadi terjadi klaim dari orang lain mengenai dokumen *multimedia* tersebut, tentu dapat diketahui secara otentik siapa pemilik sebenarnya.
2. ***Fingerprinting***. *Watermarking* dan *fingerprinting* pada dasarnya sama, hanya saja pada *fingerprinting*, penyisipan *watermark* biasanya bersifat unik untuk suatu dokumen *multimedia*. Dokumen *multimedia* yang sama dapat memiliki *fingerprint* yang berbeda.

3. ***Copy prevention or control***. Teknik *watermarking* juga dapat dilakukan untuk mencegah dokumen *multimedia* untuk diduplikasi dengan *hardware* atau *software* tertentu. Misalnya untuk mencegah suatu dokumen *multimedia* yang tersimpan dalam *CD* atau *DVD* agar tidak diduplikasi dengan *CD* atau *DVD copier*.



Gambar 3. Copy Control

4. ***Fraud and tamper detection***. *Watermarking* juga dapat digunakan untuk mendeteksi adanya pembajakan terhadap suatu dokumen *digital*.
5. ***ID card security***. Informasi berupa passport atau ID juga dapat disertakan sebagai *watermark* ke dalam foto orang yang bersangkutan, sehingga jika suatu saat dokumen seperti passport dimanipulasi oleh orang lain dengan mengganti fotonya maka dapat dideteksi.

A. Teknik-teknik *Watermarking* terhadap Berbagai Bentuk *Multimedia*

Setiap bentuk dan jenis *multimedia* memiliki katakteristik tersendiri sehingga dalam proses *watermarking* juga memiliki teknik yang berbeda-beda. Namun secara umum, teknik *watermarking* yang baik harus memenuhi kriteria sebagai berikut:

- ***Imperceptibility***. Secara kasat mata manusia, antara media asli dan media yang sudah disisipi *watermark* harus tidak dapat dibedakan.
- ***Trustworthiness***. *Watermark* harus dapat menjamin kepemilikan asli dari media tersebut, artinya *watermark* harus sulit untuk dipalsukan.
- ***Robustness***. *Watermark* yang dihasilkan harus tangguh dan tahan terhadap perubahan yang terjadi pada media.

Berikut ini teknik-teknik *watermarking* untuk jenis media text, *image*, audio dan *video*.

1. *Text Watermarking*

Proses *watermarking* terhadap dokumen teks sebenarnya telah dilakukan di dalam kehidupan sehari-hari, misalnya dengan mencetak dokumen teks pada media khusus seperti kertas segel. Namun untuk melakukan *watermarking* pada teks yang tersimpan dalam dokumen *digital*, teknik yang dilakukan tidaklah sama. Berikut ini beberapa teknik *watermarking* terhadap teks.

- ***Line Shift Coding Protocol***

  Teknik *watermarking* ini dilakukan dengan mengurangi jarak antar teks dari sisi baris. Jarak yang dikurangi tersebut dibuat sekecil mungkin (misalnya 1/300 inch) sehingga tidak akan terdeteksi oleh mata telanjang, namun dapat dideteksi dengan mudah dengan komputer.

- ***Word Shift Coding Protocol***

  Word Shift Coding Protocol pada dasarnya sama dengan teknik *Line Shift Coding Protocol*, hanya saja yang dikurangi bukan spasi antar baris, namun spasi antar kata (*word*).

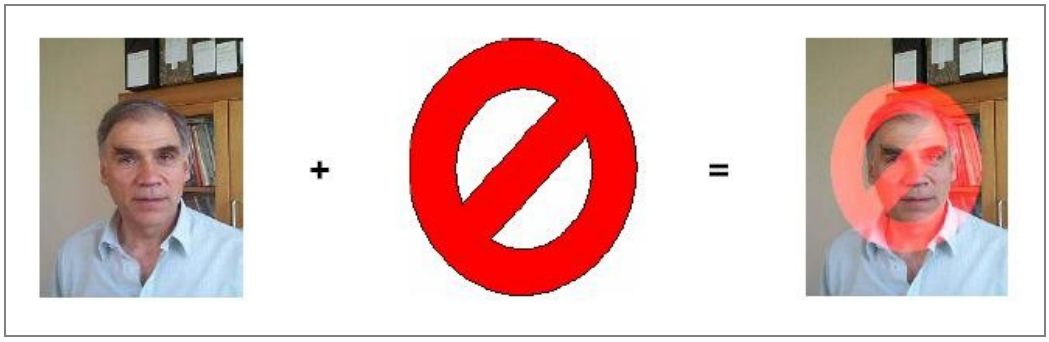
- ***White Space Manipulation***
- ***Text Content***

2. *Image Watermarking*

Watermarking terhadap gambar (*image*) paling banyak dilakukan untuk melindungi gambar seperti foto. Saat ini cukup banyak teknik maupun algoritma *watermarking* terhadap gambar yang ditawarkan. Beberapa diantaranya sebagai berikut:

- ***Simple Watermarking***

  Teknik ini merupakan teknik yang paling sederhana dimana *watermarking* dilakukan dengan menambahkan gambar atau teks tertentu pada gambar asli. Dan untuk mendapatkan gambar asli kembali, *watermark* yang ditambahkan dapat dibuang dengan teknik, tool dan keahlian tertentu. Gambar berikut ini merupakan contoh *watermarking* sederhana.



Gambar 4. Contoh Watermarking Sederhana

- ***Least Significant Bit Hiding (Image Hiding)***

  Menurut [10], metode *LSB (Least Significant Bit)* merupakan salah satu metode *watermarking* yang bekerja dalam mode warna *RGB (Red, Green, Blue)*. Metode ini bekerja dengan cara menyisipkan informasi pada bit-bit paling kanan dari setiap elemen *RGB*. Perubahan bit paling kanan hanya menimbulkan perubahan nilai *RGB* sebesar 1 dari 256 warna yang ada. Perubahan tersebut tidak dapat dideteksi dengan mata telanjang. Namun dengan komputer, misalnya menggunakan metode *Enhanced LSB*, dapat dideteksi dengan mudah apakah gambar mengandung *watermark* atau tidak. Metode *LSB* mudah untuk dideteksi karena penyisipan informasi dilakukan secara langsung dalam bit-bit dokumen tanpa melalui proses pengacakan.

- ***Hue Saturation Lightness (HSL)***

  Metode *watermarking* dengan HSL pada dasarnya mirip dengan metode *LSB*. Metode *HSL* bekerja pada mode warna *HSL* sedangkan metode *LSB* bekerja pada mode *RGB*. Evan dalam [10] mencoba memanfaatkan metode *HSL* ini untuk melakukan *watermarking* pada citra *bitmap*. Hasilnya metode *HSL* lebih baik dibanding metode *LSB*.

- ***Discrete Cosine Transformation (DCT)***

  Sebelum dilakukan *encoding*, gambar asli dibagi terlebih dahulu menjadi beberapa bagian, misalnya matriks 8 x 8. Algoritma dalam teknik *DCT* ini selain digunakan untuk menyembunyikan informasi, juga digunakan untuk melakukan kompresi terhadap gambar, terutama yang bertipe *JPEG*. Menurut [14], teknik *DCT* memiliki kelebihan dalam optimasi dan kecepatannya.

- ***Discrete Wavelet Transformation (DWT)***

  Teknik ini merupakan teknik yang lebih efektif dibanding *DCT*, dimana memiliki tingkat kompresi yang lebih tinggi.

- ***Independent Component Analysis (ICA)***

Dalam [7] dan [1] dijelaskan mengenai prinsip dasar *independent component analysis (ICA)* dan penerapannya dalam *signal processing*. Saat ini ICA juga diterapkan dalam teknik *watermarking*, misalnya dalam [22], algoritma ICA diterapkan dalam blok dari *host image* dan *watermark image*. Di dalam [18] didiskusikan mengenai penerapan *blind content based watermarking* dengan memanfaatkan konsep ICA dan DCT. Hasilnya jauh lebih baik dan akurat dibanding teknik tanpa ICA, akan tetapi memiliki kelemahan dalam hal kecepatannya.

- ***Singular Value Decomposition (SVD)***

  Pemanfaatan teknik SVD dalam *watermarking* dijelaskan dalam [4]. Teknik ini dapat digunakan untuk melakukan autentifikasi citra berdasarkan nilai korelasi *watermark* yang di-ekstrak. Teknik ini cukup *robust* terhadap beberapa pengolahan citra.

- ***Spread Spectrum Watermarking***

  Metode *spread spectrum watermarking* melakukan penyisipan dan pendeteksian *watermark* dalam ranah transform [20]. Mula-mula citra ditransformasikan ke dalam ranah frekuensi, lalu bit *watermark* disisipkan pada koefisien transformasi (misalnya koefisien DCT, FFT, DWT). Metode ini lebih *robust* terhadap gangguan atau serangan seperti kompresi, *cropping* dan *low pass filtering*.

3. *Sound Watermarking*

Selain untuk dokumen berupa *image*, teknik *Spread Spectrum* juga dapat diterapkan di dokumen *multimedia* jenis audio. Teknik *Spread Spectrum* merupakan teknik yang cukup populer saat ini. Pesan yang akan disampaikan dianggap sebagai sinyal *narrowband* bukan sinyal *wideband*. Teknik yang digunakan dalam *Spread Spectrum* adalah dengan menyebarkan bit-bit *watermark* di atas saluran frekuensi rendah.

4. *Video Watermarking*

Watermarking terhadap dokumen *multimedia* berupa *video* dapat melibatkan beberapa teknik *watermarking*, misalnya *watermarking* terhadap gambar dan suara. Dalam melakukan *watermarking* terhadap *video*, beberapa hal perlu diperhatikan [11] yaitu *robustness* terhadap kompresi, perubahan geometris maupun pemotongan *frame*, kebenaran pengkodean *frame* tanpa *visual artefact* dan harus memperhatikan *runtime* atau performa kecepatan dari *video* yang dihasilkan. Beberapa contoh algoritma yang dapat diterapkan dalam *video watermarking* antara lain algoritma Zhao Koch [24] dan algoritma Fridrich [23]. Menurut [11], algoritma Zhao Koch memiliki kelebihan jika diterapkan pada *video* jenis MPEG,

sementara algoritma Fridrich memiliki keuntungan karena dapat menyisipkan lebih banyak informasi.

B. Batasan dan Gangguan terhadap *Watermarking*

Media yang sudah disisipi *watermark* tidaklah sepenuhnya aman, karena pada dasarnya teknik *watermarking* hanyalah teknik menyembunyikan suatu informasi. *Watermarking* memiliki batasan-batasan dan juga beberapa faktor (operasi) yang dapat mempengaruhi *watermarking* itu sendiri. Salah satu keterbatasan dari teknik *watermarking* adalah keterbatasan jumlah data atau informasi yang dapat disisipkan ke dalam dokumen *digital*. Semakin banyak informasi yang disisipkan tentu akan membuat dokumen *digital* semakin besar dari sisi ukurannya. Selain itu, *watermarking* juga dapat terganggu oleh beberapa operasi terhadap dokumen *multimedia*. Gangguan tersebut dapat menyebabkan kerusakan bahkan kehilangan informasi dalam *watermark*.

Menurut M. Kutter dan F. A. P. Petitcolas dalam [15], beberapa gangguan (attack) dapat mempengaruhi *watermarking* yaitu:

- ***JPEG Compression***. Kompresi terhadap file *multimedia* terutama JPEG dapat mempengaruhi atau merusak *watermark* di dalamnya.
- ***Geometric Transformation***. Perubahan posisi geometris media yang sudah disisipi *watermark* juga dapat mempengaruhi *watermark* tersebut. Perubahan geometris antara lain *horizontal flip, rotation, cropping, scalling, deletion of lines or columns* dan *geometric distortions*.
- ***Enhanchement Techniques***. Operasi seperti *low pass filtering, sharpening, histogram modification*, dan *gamma corrections* dapat mempengaruhi dan merusak *watermark* dalam suatu media.
- Penambahan *noise* dalam media.
- Proses *printing* dan *scanning* media.
- *Statistical averaging and collusion*
- *Over-marking*
- *Oracle Attack*.

4. KESIMPULAN

Teknik *digital watermarking* dapat dilakukan untuk melindungi informasi dalam dokumen *multimedia* dengan cara menambahkan suatu tanda (*mark*) tertentu secara tersembunyi. Teknik *digital watermarking* dapat diterapkan di berbagai jenis dokumen *multimedia* seperti teks, gambar, suara dan *video*. Teknik *digital watermarking* hingga saat ini masih terus berkembang dan masih terus dicari teknik dan metode terbaik dan *robust* terhadap berbagai jenis serangan dan gangguan.

DAFTAR PUSTAKA

[1]. Aapo Hyvärinen and Erkki Oja. 2000. Independent Component Analysis: Algorithms and Applications. Neural Networks, 13(4-5):411-430, 2000

[2]. Borko Furht. 2007. Encyclopedia of Multimedia. Springer

[3]. C. Cachin, "An Information-Theoretic Model for *Steganography*", Proceedings of 2nd Workshop on Information Hiding, MIT Laboratory for Computer Science, May 1998

[4]. Cahyana; T. Basarudin dan Danang Jaya. 2007. Teknik *Watermarking* Citra berbasis SVD. National Conference on Computer Science & Information Technology 2007. Januari 29-30, 2007.

[5]. Chandramouli, R. and Memon, Nasir and Rabbani, Majid. 2002. Digital *Watermarking*. United States

[6]. Cheung, Samson. 2004. Lecture 23: Digital *Watermarking* I.

[7]. Comon, Piere. 1994. Independent component analysis, A new concept?. Signal Processing 36, p287-314

[8]. Digimarc. Digital Image *Watermarking* Guide. www.digimarc.com

[9]. Dwitya Putri dkk. 2008. Membandingkan *Steganography* Dan *Watermarking* Pada Keamanan File Grafik. Proceeding Seminar Ilmiah Nasional Komputer dan Sistem Intelijen (KOMMIT 2008).

[10]. Evan. 2009. Studi Digital *Watermarking* Citra Bitmap dalam Mode Warna Hue Saturation Lightness, Institut Teknologi Bandung, Bandung.

[11]. Fery Sinambela, Ranto Pramono, dan Krisna Adirama. 2006. Teknologi *Watermarking* yang Kuat pada Video MPEG. Institut Teknologi Bandung, Bandung.

[12]. Hajjara,Suhad; Abdallah, Moussa and Hudaib, Amjad. 2009. Digital Image *Watermarking* Using Localized Biorthogonal Wavelets. European Journal of Scientific Research, ISSN 1450-216X Vol.26 No.4 (2009), pp.594-608, EuroJournals Publishing, Inc. 2009

[13]. Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett. 2004. *Steganography* and Digital *Watermarking*. School of Computer Science, The University of Birmingham

[14]. Khayam, Syed Ali. 2003. The Discrete Cosine Transform (DCT): Theory and Application. ECE 802 – 602: Information Theory and Coding

[15]. M. Kutter and F. A. P. Petitcolas. 1999. A fair benchmark for *image watermarking* systems Electronic Imaging '99. Security and *Watermarking* of Multimedia Contents, vol. 3657, The International Society for Optical Engineering, Sans Jose, CA, USA.

[16]. Milano, Dominic. 2007. Content Control: Digital *Watermarking* and Fingerprinting. Rhozet: A Business Unit of Harmonic Inc.

[17]. Nigel Chapman. 2009. Digital Multimedia, 3rd edition. Wiley Publishing

[18]. Parameswaran, Latha and Anbumani, K. 2008. Content-Based *Watermarking* for Image Authentication Using Independent Component Analysis. Informatica 32, p299-306.

[19]. R. Popa, An Analysis of Steganographic Techniques, The "Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, http://ad.informatik.uni-freiburg.de/mitarbeiter/will/dlib_bookmarks/*digital-watermarking*/popa/popa.pdf, 1998

[20]. Rinaldi Munir. 2006. Sekilas Image *Watermarking* untuk Memproteksi Citra Digital dan Aplikasinya pada Citra Medis. Seminar ICTEL 2006 di STTTelkom Bandung, 20 September 2006

[21]. Todorov, Todor. 2004. Spread Spectrum *Watermarking* Technique For Information System Securing. International Journal "Information Theories & Applications" Vol.11

[22]. Francisco J. Gonzalez-Serrano, Harold. Y. Molina-Bulla,and Juan J. Murillo- Fuentes," Independent component analysis applied to *digital image watermarking*," International Conference on Acoustic, Speech and Signal Processing (ICASSP), vol. 3, pp. 1997-2000, May 2001.

[23]. Fridrich, J., Methods for data hiding, Center for Intelligent Systems & Department of Systems Science and Industrial Engineering, 1997.

[24]. Koch, E. and Zhao, J., Towards Robust and Hidden Image Copyright Labelling, IEEE Workshop on Nonlinear Signal and Image Processing, 1995.