

# Daftar Isi

<b>1</b>	<b>Pendahuluan</b>	<b>2</b>
<b>2</b>	<b>Watermark dan Dokumen Digital</b>	<b>4</b>
2.1	Tujuan Penggunaan Watermark . . . . .	4
2.2	Karakteristik Watermark . . . . .	5
2.3	Cara Kerja Watermark . . . . .	6
<b>3</b>	<b>Watermark Pada Dokumen Teks Digital</b>	<b>8</b>
3.1	Teknik Pengkodean . . . . .	9
3.1.1	Line-shift Coding . . . . .	9
3.1.2	Word-shift coding . . . . .	10
3.1.3	Feature Coding . . . . .	12
3.1.4	Open Space Coding . . . . .	12
3.1.5	Syntactic Coding . . . . .	13
3.1.6	Semantic Coding . . . . .	14
<b>4</b>	<b>Distribusi Dokumen Elektronik</b>	<b>15</b>
4.1	Watermark dan Kriptografi . . . . .	16
4.1.1	Melindungi informasi watermark . . . . .	16
4.1.2	Melindungi proses distribusi dokumen . . . . .	16
<b>5</b>	<b>Penutup</b>	<b>19</b>

# Daftar Gambar

2.1	Prinsip kerja watermark . . . . .	6
3.1	line-shift coding . . . . .	10
3.2	word-shift coding . . . . .	11
3.3	feature coding . . . . .	12
3.4	open space coding . . . . .	13
4.1	Teknik kriptografi dalam proses watermark : proses coding . .	17
4.2	Teknik kriptografi dalam proses watermark : proses decoding/deteksi . . . . .	18

## Ringkasan

Telah banyak teknik-teknik yang dikembangkan dalam sistem penandaan digital berupa watermark bagi dokumen digital. Teknik-teknik yang dikembangkan untuk pemberian watermark pada dokumen gambar, video dan suara, tidak dapat diterapkan untuk dokumen yang berbentuk teks.

Pada paper ini, dibahas beberapa teknik khusus yang dikembangkan untuk dokumen teks digital, diantara yang memanfaatkan karakteristik *layout* dokumen, lokasi kosong pada dokumen, kemudian memanfaatkan sifat semantik dan sintaktik pada bahasa yang digunakan dalam dokumen teks. Dibahas pula bagaimana teknik kriptografi dapat dimanfaatkan dalam sistem watermarking.

# Bab 1

## Pendahuluan

Teknologi steganografi sudah dikenal ribuan tahun yang lalu, yang cukup dikenal adalah sejarah di jaman Herodotus, saat Histiaeus membuat pesan rahasia dengan mentato kepala ajudannya, kemudian membiarkannya tumbuh sebelum diutus ke Aristagoras, yang harus mencukur kepala ajudan tersebut sebelum mengetahui pesan yang dikirim. Sampai saat ini steganografi telah digunakan untuk teknik watermarking sebagai metode dalam rangka melindungi hak cipta suatu karya yang dipublikasikan dalam bentuk digital, mengingat proses duplikasi sebuah kopi digital yang hasilnya sangat identik dengan kopi asli dan menyebarkan kopi tersebut dengan sangat mudah, untuk kemudian digunakan kembali ataupun dimanipulasi datanya. Dalam hal penyebaran secara ilegal, teknik kriptografi merupakan solusi yang cukup efektif. Namun, kriptografi lebih mengutamakan pada keamanan komunikasi data, bukan dimaksudkan dalam hal perlindungan hak cipta. Sebagai contoh, kriptografi yang digunakan pada TV kabel, berhasil mengirimkan data secara aman ke pelanggan tanpa diketahui isi data tersebut oleh selain pelanggan, tapi tidak ada jaminan terhadap proses penyimpanan dipihak pelanggan seperti merekamnya kedalam pita video atau pelanggaran lainnya.

Adanya permintaan akan jaminan hak cipta dalam bentuk perangkat lunak ataupun perangkat keras menyebabkan teknologi tanda air digital sangat diperlukan. Dalam bentuk digital, penyebaran dokumen secara tidak sah da-

pat dilakukan lebih mudah. Karena dengan kemajuan komunikasi data yang semakin baik, penduplikasian dan penyebaran dokumen akan menjadi lebih cepat dan murah dibandingkan dengan dokumen berupa kertas. Berbeda dengan hasil duplikasi pada dokumen kertas, hasil duplikasi pada dokumen digital tidak akan berbeda dengan dokumen aslinya. Oleh karena itu, untuk menghindari publikasi dan distribusi dokumen secara tidak sah, adalah dengan memberi tanda air pada dokumen asli. Tanda air yang unik, ditanamkan kedalam dokumen, dengan memberikan suatu metadata yang dapat berisi informasi penulis, penerima, tanggal pembuatan, dan sebagainya. Kemudian, tanda air tersebut harus dapat tetap terdeteksi apabila dokumen tersebut mengalami proses-proses yang biasa terjadi pada dokumen, seperti pencetakan, fotokopi, ataupun ditransmisikan menggunakan faksimili.

## Bab 2

# Watermark dan Dokumen Digital

### 2.1 Tujuan Penggunaan Watermark

Dokumen merupakan representasi riwayat organisasi secara eksplisit[3]. Dokumen dalam bentuk elektronik dapat memudahkan pembukaan serta penelusuran isi dari riwayat dokumen tersebut yang sebelumnya susah untuk dilakukan pada dokumen dalam bentuk kertas, memungkinkan pembagian informasi (*information sharing*) yang efektif, serta dapat memberikan kontribusi pada penyebar-luasan pengetahuan pada lingkungan-lingkungan terkait. Dokumen elektronik mendukung pengambilan kebijakan berbasis bukti yaitu dengan menyediakan bukti dari aksi dan keputusan sebelumnya. Namun untuk menghasilkannya dokumen elektronik tersebut harus dikelola dengan baik untuk menjamin integritas dan otentisitasnya. Dokumen-dokumen elektronik yang berisi transaksi elektronik yang otentik harus dijaga sedemikian rupa sehingga tetap terjaga kualitas legal dan bobot buktinya. Untuk itulah diperlukannya teknik watermarking.

Penyisipan watermark pada dokumen memiliki berbagai macam tujuan. Untuk aplikasi perlindungan hak cipta, tanda yang disisipkan pada dokumen (gambar, teks, atau audio) digunakan sebagai *identifier* yang menunjukkan hak kepemilikan atau hak penggunaan dokumen. Jenis tanda air mengenga-

ruhi keefektifan tanda air itu sendiri dalam setiap aplikasinya. Baik tanda air *perceptible* maupun *imperceptible*, keduanya dapat mencegah terjadinya penyalahgunaan, namun dengan cara yang berbeda. Tanda air digital digunakan untuk memberikan identifikasi sebuah dokumen atas informasi sumber daya, penulis, kreator, pemilik, distributor, dan konsumen yang berhak atas dokumen tersebut.

## 2.2 Karakteristik Watermark

Ada beberapa karakteristik yang diinginkan dari penggunaan watermark pada suatu dokumen, diantaranya tidak dapat terdeteksi (*imperceptible*), *robustness*, dan *security*.

***Imperceptible:*** memberikan karakteristik watermark agar sebisa mungkin harus tidak dapat terlihat atau berbeda dengan dokumen aslinya. Hal ini dimaksudkan untuk tidak merubah status dokumen yang bernilai tinggi secara hukum maupun komersial.

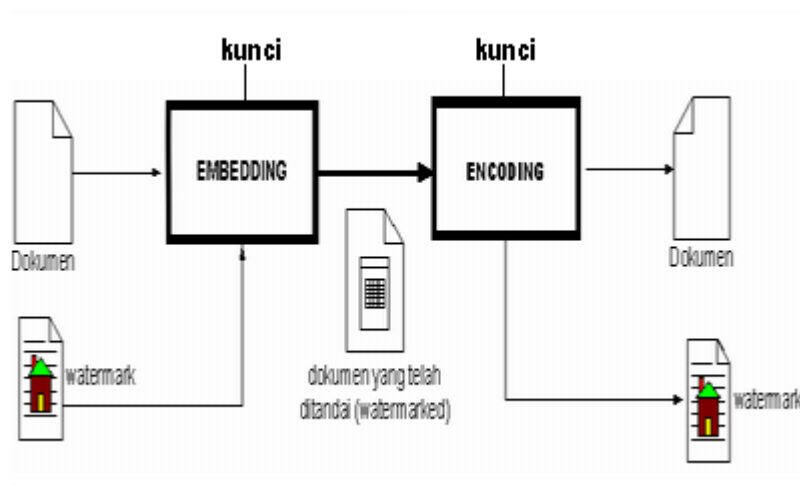
***Robustness:*** Karakteristik ini tergantung aplikasi dari watermark itu sendiri. Apabila digunakan sebagai identifikasi kepemilikan/*copyright*, watermark harus memiliki ketahanan terhadap berbagai macam modifikasi yang mungkin bisa dilakukan untuk merubah/menghilangkan *copyright*. Jika digunakan untuk otentikasi *content*, watermark sebisa mungkin bersifat *fragile*, sehingga apabila isinya telah mengalami perubahan, maka watermark akan mengalami perubahan/rusak, sehingga dapat terdeteksi adanya usaha modifikasi terhadap isi.

***Security:*** Teknik watermark harus dapat mencegah usaha-usaha untuk mendeteksi dan memodifikasi informasi watermark yang disisipkan ke dalam dokumen. Kunci watermark menjamin hanya orang yang berhak saja yang dapat melakukan hal tersebut. Namun aspek ini tidak dapat mencegah siapapun untuk membaca dokumen yang bersangkutan.

## 2.3 Cara Kerja Watermark

Watermark merupakan teknik dari steganografi yang menyisipkan suatu data ke data yang lain. Pada watermark digital, sebuah sinyal *low-energy* disisipkan ke sinyal utama sebagai *cover signal* untuk menyembunyikan sinyal *low-energy* tadi. Pada gambar 2.1 diilustrasikan sinyal *low-energy* adalah watermark, dan *cover signal*-nya adalah dokumen, yang dapat berupa gambar, video, suara, atau teks dalam format digital.

Secara umum, sistem watermarking terdiri dari *embedder* dan *detector*. *Embedder* bekerja untuk menyisipkan watermark kedalam dokumen (*cover signal*) dan *detector* akan mendeteksi watermark yang ada di dalam dokumen. Kunci watermark digunakan selama proses penyisipan dan pendeteksian. Kunci tersebut bersifat *private* dan hanya boleh diketahui oleh pihak-pihak yang diberi otoritas untuk menyisipkan atau mendeteksi watermark tersebut.



Gambar 2.1: Prinsip kerja watermark

Proses penyisipan dimodelkan sebagai memasukkan sinyal *noise* sebagai fungsi dari tanda air  $w$ , dan sebuah fungsi dari data asli  $I$ . Data setelah pemberian tanda air  $I'$  diberikan oleh persamaan:

$$I' = I + f(I, w) \quad (2.1)$$

Data yang telah ditandai dimungkinkan terdistorsi akibat usaha-usaha untuk menghilangkan atau merubah data watermark, yang dipresentasikan sebagai  $n$ . Distorsi dapat linear maupun non-linear dan *dependent* terhadap  $I$ , maka  $n = (I)$ . Sehingga data yang akan sampai ke dekoder adalah  $I''$ , diberikan oleh persamaan berikut:

$$I'' = I' + f(I, w) + n(I) \quad (2.2)$$

Proses pendeteksian dimaksudkan untuk memperoleh  $w$  dan  $I$ . Magnituda  $I$  lebih besar daripada  $f(I, w)$  dan distorsi  $n$ . akibatnya, pada input dekoder, rasio *signal-to-noise*, dimana sinyal tersebut adalah watermark  $w$ , adalah kurang dari satu. Penggunaan data asli yang belum disisipi watermark  $w$  sebagai bagian dari proses deteksi akan dapat meningkatkan rasio *signal-to-noise* dengan cara mensubstraksi data original  $I$  dari 2.2.

## Bab 3

# Watermark Pada Dokumen Teks Digital

Dokumen digital, disamping berupa gambar, suara, maupun video, ada lagi jenis dokumen digital yang sangat penting dan sering digunakan sebagai sarana pendukung berjalannya suatu proses dalam organisasi / perusahaan, yaitu dokumen teks digital. Saat ini, perkembangan teknologi komputer sangat membantu sebuah organisasi / perusahaan yang menerapkan konsep *paperless document (e-document)*.

Tidak seperti pada dokumen gambar atau audio, penyisipan watermark pada dokumen teks dilakukan dengan memodifikasi sebagian *pixel* atau frekuensi tanpa terdeteksi oleh manusia. Sebuah dokumen teks tidak memiliki keleluasaan seperti itu. Modifikasi terhadap huruf-huruf (baik dalam dokumen *image* teks itu sendiri ataupun dalam format file) akan sangat mengganggu dokumen, baik dari segi estetis maupun segi legalitas dokumen teks yang bersangkutan. Watermark sendiri tidak memberikan perlindungan terhadap *copy protection* maupun perlindungan terhadap kerahasiaan isi dokumen, namun jika terjadi penyebaran/penduplikasi dokumen secara tidak sah, maka hak kepemilikan dokumen masih dapat diketahui, dan seseorang yang bertanggung jawab atas tersebarnya dokumen tersebut secara ilegal dapat diketahui pula.

Teks dalam bentuk *raw* seperti ASCII dan *source code* program, tidak

dapat disisipkan watermark[5], karena tidak ada lokasi dimana informasi watermark dapat disisipkan. Namun bentuk akhir dari dokumen teks biasanya dalam bentuk terformat (PostScript, PDF, TeX), sehingga informasi watermark dapat disisipkan melalui informasi layout dan jenis pemformatannya (misal, serifs).

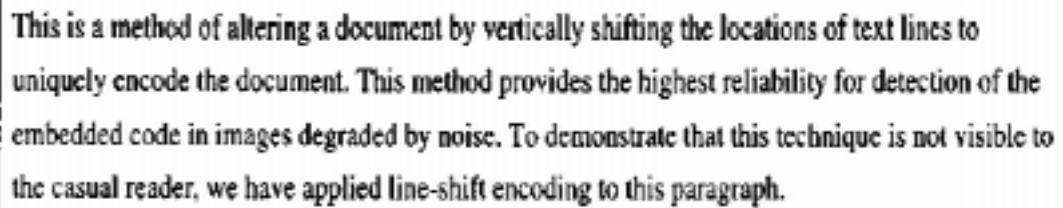
Sebuah dokumen teks biasanya terdiri atas struktur-struktur umum seperti kata, baris, dan paragraf. Ide dasarnya, memanfaatkan struktur-struktur tersebut untuk menyembunyikan tanda air di dalam dokumen, mengingat perubahan yang sangat kecil pada struktur dokumen tidak akan terlihat oleh mata manusia. Ide lain adalah memanfaatkan lahan kosong pada dokumen (baik berbentuk format file maupun *image* dokumen) untuk disisipkan kode watermark.

## 3.1 Teknik Pengkodean

Ada beberapa metode untuk untuk menyisipkan watermark pada dokumen teks digital. Diantaranya dengan melakukan proses watermark dengan memanfaatkan struktur layout dokumen[1]. Dapat pula dengan melakukan manipulasi daerah kosong pada dokumen, dan manipulasi sintak dan semantik terhadap bahasa yang digunakan pada dokumen[2].

### 3.1.1 Line-shift Coding

Melalui pendekatan ini, penandaan dokumen dilakukan dengan memanfaatkan spasi antar baris pada dokumen, yaitu menggeser posisi suatu baris secara vertikal ke atas atau ke bawah. Pada implementasinya, baris terdekat dari baris tersebut, tidak dilakukan pergeseran, hal ini dilakukan untuk menentukan lokasi referensi saat proses deteksi (*control-line*). Metode ini adalah dengan mengubah posisi baris teks secara vertikal. *Encoding* ini dapat diterapkan pada file format (PostScript, TeX, dan sebagainya), maupun format image dari halaman dokumen. Sebuah baris teks dapat ditandai secara vertikal dengan menggesernya sedikit ke atas atau kebawah dari posisi aslinya untuk memberikan satu bit *copy identifier* yang unik. Untuk mengkompen-



This is a method of altering a document by vertically shifting the locations of text lines to uniquely encode the document. This method provides the highest reliability for detection of the embedded code in images degraded by noise. To demonstrate that this technique is not visible to the casual reader, we have applied line-shift encoding to this paragraph.

Gambar 3.1: Contoh line-shift coding, baris kedua telah digeser vertikal 1/300 inchi

sasi distorsi utama, sebuah baris ditandai hanya jika baris tersebut dan dua baris disekitarnya (*control lines*) cukup panjang. Sedangkan *control lines* sendiri tidak ditandai.

Pada setiap dokumen, diberikan sebuah *codeword* yang unik untuk setiap penerima dokumen yang dituju. Setiap *codeword* menentukan sebuah set baris-baris teks yang akan dipindahkan untuk masing-masing penerima dokumen. Panjang dari *codeword* adalah jumlah maksimum dari baris yang dirubah posisinya pada area yang di kodekan.

### 3.1.2 Word-shift coding

Metode ini adalah memanipulasi dokumen dengan menggeser secara horizontal kata-kata dalam baris teks. *Encoding* ini dapat diterapkan pada format file (PostScript, T<sub>E</sub>X, dan sebagainya), maupun format *image* dari halaman dokumen. Penandaan sebuah baris secara horizontal dengan menggeser kata-kata tertentu sedikit ke kiri atau ke kanan dari posisi aslinya. Baris tersebut dibagi menjadi beberapa grup kata-kata (jumlah grup adalah ganjil), sehingga setiap grup cukup berisi sejumlah karakter. Setiap grup yang genap dilakukan pergeseran, sedangkan grup yang ganjil, disebut sebagai *control groups*, tetap pada posisinya. *Control lines* dan *control groups* digunakan untuk mengestimasi dan mengkompensasi distorsi-distorsi untuk masing-masing profil vertikal dan horizontal. dengan metode ini, sebuah dokumen tidak akan terlihat telah ditandai, jika menggunakan jarak antar

Now is the time for all men/women to ...  
Now is the time for all men/women to ...

Diagram (a) illustrates word-shift coding. It consists of two lines of text: "Now is the time for all men/women to ..." on the top line and "Now is the time for all men/women to ..." on the bottom line. Vertical lines are drawn between the words in both lines, creating columns. The word "for" in the top line is shifted to the right, so its column is aligned with the column of "all" in the bottom line. Two horizontal arrows point towards each other at the bottom of the "for" column, indicating the shift.

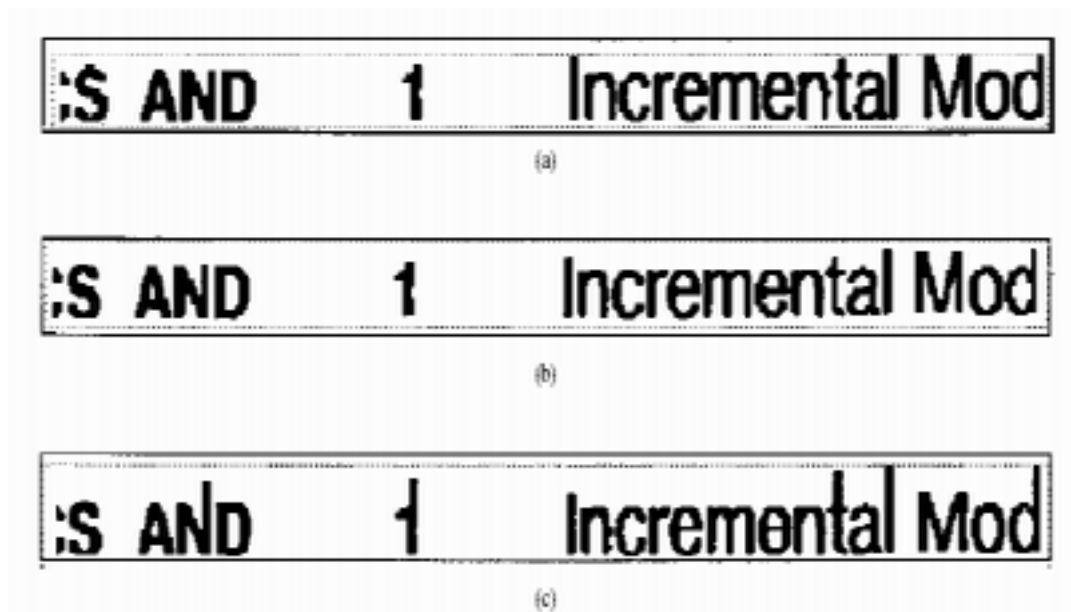
(a)

Now is the time for all men/women to ...  
Now is the time for all men/women to ...

Diagram (b) shows the same two lines of text as in (a), but without the vertical lines. The text is: "Now is the time for all men/women to ..." on the top line and "Now is the time for all men/women to ..." on the bottom line.

(b)

Gambar 3.2: Contoh word-shift coding, pada (a), baris paling atas ditambahkan spasi sebelum "for", sedangkan baris dibawahnya adalah sebelum ditambahkan spasi. Pada (b), diperlihatkan lagi tanpa bantuan garis vertikal



Gambar 3.3: Contoh feature coding, pada (a), coding belum diterapkan. Pada (b), feature-coding diterapkan pada karakter-karakter tertentu. Pada (c), memperlihatkan perubahan dengan feature-coding

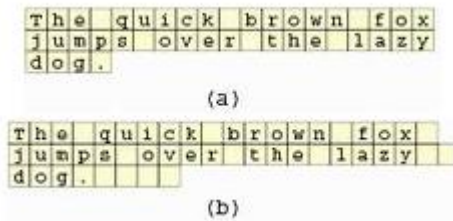
kata yang variable. Hal ini umum untuk dokumen yang menggunakan pengaturan *justify text*.

### 3.1.3 Feature Coding

Metode ini dapat diterapkan pada format file maupun format *image* sebuah dokumen. Perubahan yang dilakukan adalah pada pilihan fitur teks tertentu. Fitur tersebut dirubah atau tidak tergantung dari *codeword*-nya. Perubahan yang dipilih biasanya dari fitur yang dimiliki oleh huruf, semisal huruf *b*, *d*, *h*, dengan menambah atau mengurangi panjang ujung hurufnya satu atau beberapa pixel. Gambar 3.3 menunjukkan contoh penerapan *feature coding*.

### 3.1.4 Open Space Coding

*Open space coding / open space method*, merupakan coding yang dilakukan dengan memanfaatkan lahan kosong / *white space* pada dokumen teks.



Gambar 3.4: Contoh penerapan *open space coding*. (a) memperlihatkan teks normal, dan (b) memperlihatkan setelah penerapan coding

Ada dua alasan digunakannya metodenya untuk melakukan watermark pada dokumen, pertama merubah / menambah lahan kosong, tidak akan merubah makna atau arti dari kalimat di dalam dokumen. Kedua, perubahan pada lahan kosong tidak akan dirasakan oleh orang yang membaca dokumen tersebut.

Ada tiga cara yang dapat dilakukan untuk memanipulasi lahan kosong ini, yaitu mengeksploitasi spasi antar kalimat, spasi pada *end-of-line*, spasi antar kata pada teks dengan justifikasi. Gambar 3.4 memperlihatkan teknik *open space coding*. Metode ini dapat diterapkan selama teksnya dalam format ASCII. Pada saat dicetak, karena pada saat dicetak, kemungkinan besar data yang disembunyikan sudah tidak bisa terdeteksi kembali. Kelemahan lainnya, adalah jika digunakan *word-processor*, kemungkinan secara otomatis melakukan perubahan pada spasi untuk proses justifikasi, sehingga data yang diselipkan pada spasi kosong akan hilang.

### 3.1.5 Syntactic Coding

Dalam metode ini termasuk perubahan diksi dan struktur teks tanpa merubah arti kalimat. sebagai contoh kalimat "Setelah makan siang, mereka langsung pergi", dapat dirubah menjadi "Mereka langsung pergi setelah makan siang". Kelemahan metode ini adalah sedikitnya kesempatan untuk melakukan eksploitasi pada sintak.

### 3.1.6 Semantic Coding

Metode berikutnya adalah dengan cara merubah kata pada kalimat dengan sinonimnya. Sebagai contoh "besar" dapat disinonimkan dengan "luas", "agung", dan sebagainya. Karena satu kata dapat memiliki beberapa sinonim, kesulitannya adalah melakukan relevansi sinonim terhadap kalimatnya. Sebagai contoh, "jalan utama di daerah pantura cukup **besar** untuk dilalui kendaraan". Kata "*besar*" dalam kalimat tersebut akan terlihat tidak relevan apabila disinonimkan oleh kata "*agung*".

## Bab 4

# Distribusi Dokumen Elektronik

Perkembangan yang pesat pada perangkat komputer, printer, dan transmisi data kecepatan tinggi, menyebabkan biaya penyediaan perangkat menjadi lebih terjangkau. Hal tersebut memfasilitasi penyebaran dokumen elektronik menjadi sangat mudah. Dalam suatu organisasi, misal sebuah departemen yang memiliki perwakilan-perwakilan di tempat yang cukup jauh, maka pengiriman berita, dokumen penting, dan sebagainya cukup dilakukan secara elektronik. Sehingga dokumen yang bersifat mendesak untuk diketahui seluruh perwakilan dapat disampaikan dengan cepat. Begitu pula sebuah media massa elektronik berlangganan, berita terkini dapat lebih cepat sampai ke pelanggan.

Namun yang menjadi perhatian adalah kemudahan dalam penduplikasian dokumen. Sebuah dokumen elektronik yang bersifat terbatas penyebarannya, seperti surat panggilan dari pengadilan, atau surat kabar berlangganan yang hanya boleh dibaca atau disimpan di komputer pelanggan yang terdaftar, menjadi rawan terhadap penduplikasi dan penyebaran yang tidak sah. Hal tersebut bisa mengurangi keuntungan bagi penyedia layanan surat kabar tersebut atau terbongkarnya rahasia hukum seseorang.

Dalam[6], untuk mempersulit terjadinya distribusi semacam itu, dapat dilakukan dengan cara:

1. Menandai dokumen (watermark) sehingga dapat dilacak / diketahui penerima sebenarnya.

2. Menggunakan teknik kriptografi, sehingga informasi watermark akan sulit diketahui.
3. Mengharuskan seseorang yang mendistribusikan dokumen untuk menyertakan informasi personalnya ke dalam dokumen.

Penandaan dokumen, dilakukan untuk memberikan jaminan akan keaslian dokumen. Siapa pengirim/pembuatnya, dan siapa penerimanya. Informasi lain seperti tanggal pembuatan, tanggal pemusnahaan, dan lain-lain dapat dimasukkan ke dalam tanda dokumen (watermark). Dalam organisasi, teknik ini memberikan kepastian hukum / sebagai legalisasi[8] atas dokumen elektronik. Apabila watermark tidak sesuai dengan identitas pengirim seperti yang tertera pada isi dokumen, atau watermark tidak tersedia, maka secara hukum dokumen dianggap tidak sah dan tidak diperbolehkan dipergunakan untuk kegiatan organisasi.

## 4.1 Watermark dan Kriptografi

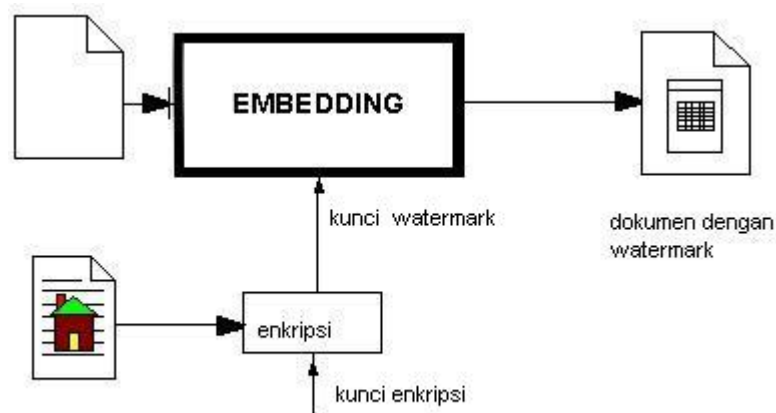
Dalam sistem watermark, kriptografi dapat bekerja di dalam dua hal yaitu melindungi informasi watermark itu sendiri dan melindungi dokumen saat proses distribusi.

### 4.1.1 Melindungi informasi watermark

Teknik kriptografi mengacak informasi watermark yang akan disisipkan ke dalam dokumen, sehingga kemungkinan saat seseorang berhasil memperoleh informasi tersebut, dia hanya akan memperoleh data yang tidak berguna, karena informasinya teracak, kecuali dia juga melakukan teknik kriptanalisis terhadap informasi tersebut. Gambar 4.1 dan gambar 4.2 menunjukkan *coding* dan *decoding* watermark.

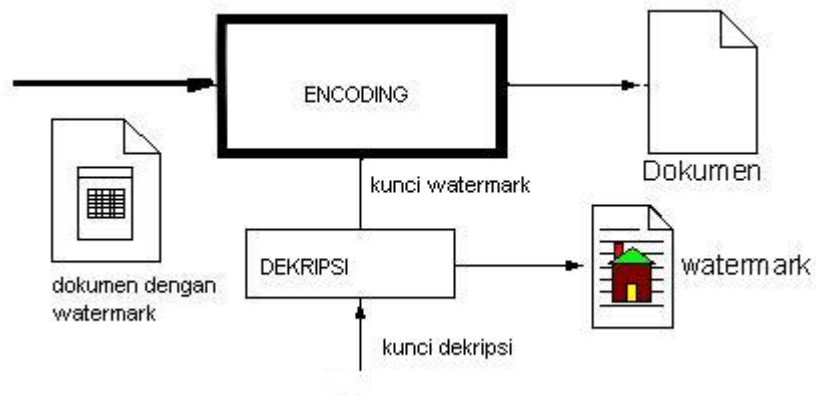
### 4.1.2 Melindungi proses distribusi dokumen

Teknik kriptografi digunakan untuk memberikan keamanan pada saat transmisi data. Dokumen yang bernilai tinggi akan sangat riskan apabila dikirim-



Gambar 4.1: Teknik kriptografi dalam proses watermark : proses coding

kan begitu saja melalui jaringan tanpa adanya pengamanan. Seseorang bisa melakukan penyadapan di tengah jalan, kemudian menggunakan informasi yang diperolehnya untuk maksud-maksud tertentu. Dengan melakukan enkripsi sebelum pengiriman dokumen, maka seorang penyadap data tidak akan bisa mengetahui informasi apapun dari dokumen tersebut. Pemilihan teknik kriptografi, sistem *private-key* atau *public-key*, tergantung dari implementasi yang akan dipakai. Sistem *private-key* dapat dipakai apabila hanya satu penerima saja yang berhak untuk membuka dokumen tersebut. Sistem *public-key* digunakan apabila penerima dokumen adalah lebih dari satu penerima.



Gambar 4.2: Teknik kriptografi dalam proses watermark : proses decoding/deteksi

## Bab 5

# Penutup

Telah dijelaskan beberapa teknik yang dipakai untuk menyisipkan watermark ke dalam dokumen teks digital. Pemilihan teknik yang tepat akan menjamin karakteristik watermark yang sesuai dengan kebutuhan dokumen yang bersangkutan.

Untuk penelitian lebih lanjut, diharapkan adanya implementasi dari teknik-teknik tersebut untuk dilakukan proses penyisipan dan deteksi watermark dalam dokumen teks, dan dilakukan percobaan serangan terhadap cover signal yang bertujuan untuk merusak atau memperoleh watermark yang disisipkan untuk mengetahui sejauh mana teknik-teknik tersebut dapat memberikan karakteristik yang sesuai sebagai sebuah watermark.

# Bibliografi

- [1] J. Brassil, S. Low, and N. Maxemchuk, "Electronic marking and identification techniques to discourage document copying," *IEEE J. Select. Areas Commun.*, vol. 3, no. 18, Oct. 1995. [Online]. Available: <http://citeseer.nj.nec.com/brassil94electronic.html>
- [2] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for data hiding," *IBM System Journal*, vol. 35, no. 3, 1996. [Online]. Available: <http://www.research.ibm.com/journal/sj/mit/sectiona/bender.html>
- [3] Tim Task Force E-Government, "Panduan sistem manajemen kerahasiaan, dan keamanan dokumen elektronik," Kementerian Komunikasi dan Informasi Republik Indonesia, 2002, draft.
- [4] J. Brassil, S. Low, and N. Maxemchuk, "Copyright protection for the electronic distribution of text document." [Online]. Available: <http://comet.ctr.columbia.edu/nick/ref.1553.ps>
- [5] J. K. Su, F. Hartung, and B. Girod, "Digital watermarking of text, image, and video documents," University of Erlangen-Nuremberg, Germany. [Online]. Available: <http://www.cg.cs.tu-bs.de/v3d2/pubs/diwa-shg98.pdf>
- [6] N. Maxemchuk, "Electronic document distribution," *AT&T Technical Journal*, 1994. [Online]. Available: <http://comet.ctr.columbia.edu/~nick/ref.1317.ps>

- [7] M. R. Sreejeth, "Digital watermarks for text documents," Indian Institute of Technology Kanpur, 1999. [Online]. Available: <http://www.cse.iitk.ac.in/research/mtech1997/9711116.html>
- [8] "Peraturan pemerintah republik indonesia," *Tentang Tata Cara Pengalihan Dokumen Perusahaan Ke Dalam Mikrofilm Atau Media Lainnya Dan Legalisasi*, no. 88, 1999.