Bahan Kuliah ke-7

IF5054 Kriptografi

Steganografi dan *Watermarking*

Disusun oleh:

Ir. Rinaldi Munir, M.T.

Departemen Teknik Informatika
Institut Teknologi Bandung
2004

7. Steganografi dan *Watermarking*

7.1 Definisi Steganografi

- Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia.

- Kata steganorafi berasal dari Bahaya Yunani yang berarti "tulisan tersembunyi" (*covered writing*).

- Steganografi membutuhkan dua properti: wadah penampung dan data rahasia yang akan disembunyikan.

- Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara, teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video.

- Steganografi dapat dipandang sebagai kelanjutan kriptografi. Jika pada kriptografi, data yang telah disandikan (*ciphertext*) tetap tersedia, maka dengan steganografi cipherteks dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya.

- Di negara-negara yang melakukan penyensoran informasi, steganografi sering digunakan untuk menyembunyikan pesan-pesan melalui gambar (*images*), video, atau suara (*audio*).

7.2 Sejarah Steganografi

- Steganografi sudah dikenal oleh bangsa Yunani. Herodatus, penguasa Yunani, mengirim pesan rahasia dengan menggunakan kepala budak atau prajurit sebagai media. Dalam hal ini, rambut budak dibotaki, lalu pesan rahasia ditulis pada kulit kepala budak. Ketika rambut budak tumbuh, budak tersebut diutus untuk membawa pesan rahasia di balik rambutnya.

- Bangsa Romawi mengenal steganografi dengan menggunakan tinta tak-tampak (*invisible ink*) untuk menuliskan pesan. Tinta tersebut dibuat dari campuran sari buah, susu, dan cuka. Jika tinta digunakan untuk menulis maka tulisannya tidak tampak. Tulisan di atas kertas dapat dibaca dengan cara memanaskan kertas tersebut.

- Sebagai contoh ilustrasi, di bawah ini adalah citra lada (`peppers.bmp`) yang akan digunakan untuk menyembunyikan sebuah dokumen *word* (`hendro.doc`).

Gambar 7.1. `peppers.bmp`

LETTER OF RECOMMENDATION

To Whom It May Concern,

Herewith I highly recommend **Mr. R. Hendro Wicaksono** continue his postgradu study at your university. My recommendation is based on my experience as lecturer in several courses for the past four years.

He has shown me his excellent attitude and personality. He is a hard working pers and he has a lot of creative ideas. He is also a very intelligent student and cooperates very well with his peers whenever they had to work together.

During his study, he showed diligence and eagerness to achieve his goal. He sets ve high standard for himself and organizes himself very well to achieve the standard am confident that if he can maintain his goal work, he should be able to complete t postgraduate program well within the stipulated time.

I am sure that his abilities and his personal qualities along with his acaden capabilities will help his to obtain his Master's degree at your university, which w be very useful for our country.

Bandung, November 15, 2002
Yours Sincerely,

Ir. Rinaldi Munir, M.Sc.
Senior Lecturer
Informatics Engineering Department,
Institute Technology of Bandung (ITB)
Jl. Ganesha No. 10, Bandung 40132
Email : rinaldi@informatika.org
Phone +62-22-2508135
Indonesia

Gambar 7.2. hendro.doc

Hasil penyembunyian data (`peppers.bmp` + `hendro.doc`)

Gambar 7.3. Citra lada setelah "diisi" dengan data teks.

7.3 Kriteria Steganografi yang Bagus

- 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.

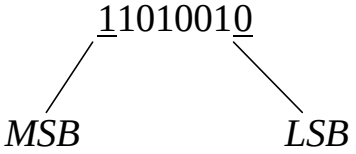
3. *Recovery*. Data yang disembunyikan harus dapat diungkapkan kembali (*recovery*). Karena tujuan steganografi adalah *data hiding*, maka sewaktu-waktu data rahasia di dalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

7.4 Teknik Penyembunyian Data

- Penyembunyian data dilakukan dengan mengganti bit-bit data di dalam segmen citra dengan bit-bit data rahasia. Metode yang paling sederhana adalah metode **modifikasi *LSB*** (*Least Significant Bit Modification*).

- 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*).

- Perhatikan contoh sebuah susunan bit pada sebuah *byte*:



LSB = Least Significant Bit
MSB = Most Siginificant Bit

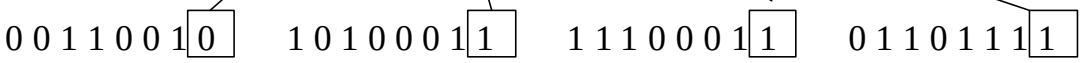
Bit yang cocok untuk diganti adalah bit *LSB*, sebab perubahan tersebut hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan

byte tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti. Lagi pula, mata manusia tidak dapat membedakan perubahan yang kecil.

- Misalkan segmen data citra sebelum perubahan:

0 0 1 1 0 0 1 1 1 0 1 0 0 0 1 0 1 1 1 0 0 0 1 0 0 1 1 0 1 1 1 1

Segmen data citra setelah ‘0 1 1 1 ‘ disembunyikan:



- Untuk memperkuat teknik penyembunyian data, bit-bit data rahasia tidak digunakan mengganti *byte-byte* yang berurutan, namun dipilih susunan *byte* secara acak. Misalnya jika terdapat 50 *byte* dan 6 bit data yang akan disembunyikan, maka maka *byte* yang diganti bit *LSB*-nya dipilih secara acak, misalkan *byte* nomor 36, 5, 21, 10, 18, 49.

- Bilangan acak dapat dibangkitkan dengan program *pseudo-random-number-generator* (*PRNG*). *PRNG* menggunakan kunci rahasia untuk membangkitkan posisi *pixel* yang akan digunakan untuk menyembunyikan bit-bit.

- *PRNG* dibangun dalam sejumlah cara, salah satunya dengan menggunakan algoritma kriptografi berbasis blok (*block cipher*). Tujuan dari enkripsi adalah menghasilkan sekumpulan bilangan acak yang sama untuk setiap kunci enkripsi yang sama. Bilangan acak dihasilkan dengan cara memilih bit-bit dari sebuah blok data hasil enkripsi.

- Sayangnya, metode modifikasi *LSB* kurang bagus untuk steganografi, karena *robustness*-nya rendah. Selain itu, dapat terjadi kasus penurunan jumlah warna (*fidelity* rendah). dilakukan

7.5 Ukuran Data Yang Disembunyikan

- Ukuran data yang akan disembunyikan bergantung pada ukuran citra penampung. Pada citra 24-bit yang berukuran 256×256 *pixel* terdapat 65536 *pixel*, setiap *pixel* berukuran 3 *byte* (komponen *RGB*), berarti seluruhnya ada $65536 \times 3 =$ 196608 *byte*. Karena setiap *byte* hanya bisa menyembunyikan satu bit di *LSB*-nya, maka ukuran data yang akan disembunyikan di dalam citra maksimum

  196608/8 = 24576 *byte*

  Ukuran data ini harus dikurangi dengan panjang nama berkas, karena penyembunyian data rahasia tidak hanya menyembunyikan isi data tersebut, tetapi juga nama berkasnya.

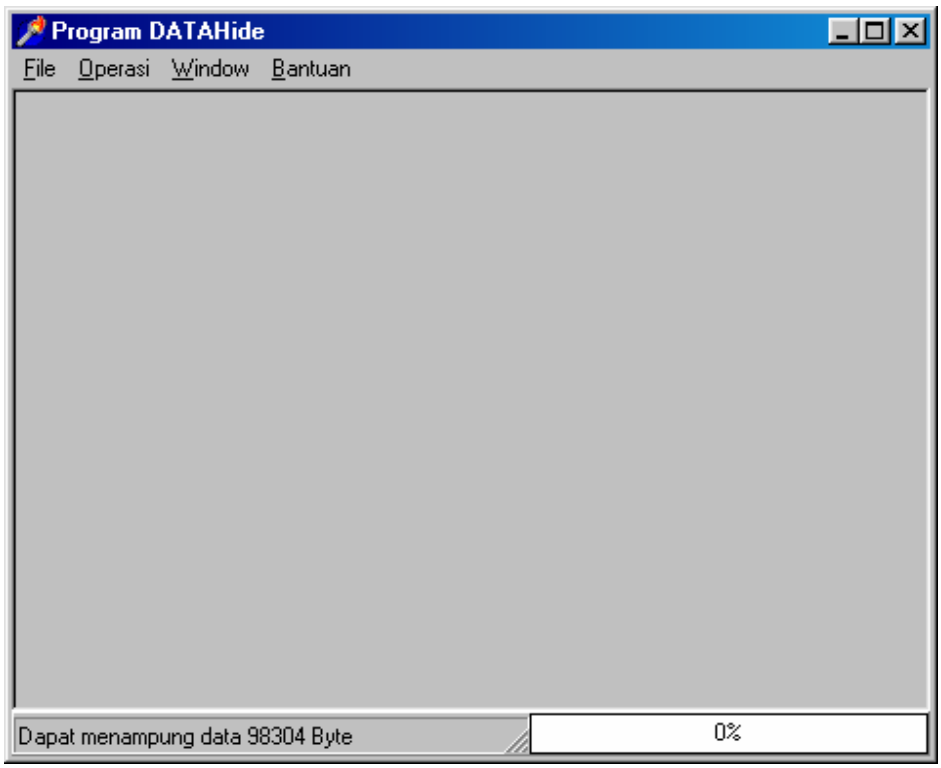
- Semakin besar data disembunyikan di dalam citra, semakin besar pula kemungkinan data tersebut rusak akibat manipulasi pada citra penampung.

- Untuk memperkuat keamanan, data yang akan disembunyikan dapat dienkripsi terlebih dahulu. Sedangkan untuk memperkecil ukuran data, data dimampatkan sebelum disembunyikan. Bahkan, pemampatan dan enkripsi dapat juga dikombinasikan sebelum melakukan penyembunyian data.

7.6 Teknik Ektsraksi Data

- Data yang disembunyikan di dalam citra dapat dibaca kembali dengan cara pengungkapan (*reveal* atau *extraction*). Posisi *byte* yang menyimpan bit data dapat diketahui dari bilangan acak yang dibangkitkan. Bilangan acak yang dihasilkan harus sama dengan bilangan acak yang dipakai pada waktu penyembunyian data. Dengan demikian, bit-bit data rahasia yang bertaburan di dalam citra dapat dikumpulkan kembali.
- Contoh program steganografi adalah **DATAhide** (dari program Tugas Akhir Lazarus Poli, NIM : 13593601, *Penerapan Steganografi dengan Citra Dijital Sebagai File Penampung*, Tugas Akhir Teknik Informatika, 1998).

  Untuk setiap contoh, digunakan kunci enkripsi yang sama: `informatika`



Upa-menu pada Operasi: `Penyembunyian data` dan `Pengungkapan data`.

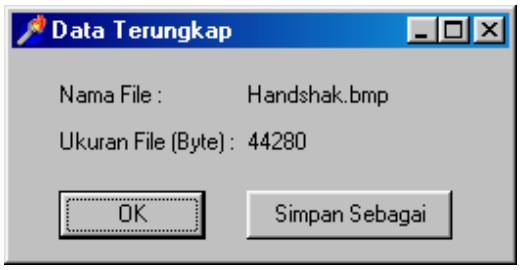
Citra 24 bit

Penampung: citra `peppers.bmp` (512 × 512 *pixel*, 769 KB)

Data yang disembunyikan: citra `handshak.bmp` (44 KB)

Hasil penyembunyian data (`peppers.bmp` + `handshake.bmp`):

Hasil ekstraksi data:



Berkas `handshak-stega.bmp` hasil ekstraksi:

Citra penampung: `pepper.bmp` (512×512 *pixel*), lihat Gambar 7.1.
Data yang disembunyikan: citra `hendro.doc` (20 KB)

LETTER OF RECOMMENDATION

To Whom It May Concern,

Herewith I highly recommend **Mr. R. Hendro Wicaksono** continue his postgradua study at your university. My recommendation is based on my experience as his lecturer several courses for the past four years.

He has shown me his excellent attitude and personality. He is a hard working person a he has a lot of creative ideas. He is also a very intelligent student and he cooperates ve well with his peers whenever they had to work together.

During his study, he showed diligence and eagerness to achieve his goal. He sets ve high standard for himself and organizes himself very well to achieve the standard. I a confident that if he can maintain his goal work, he should be able to complete t postgraduate program well within the stipulated time.

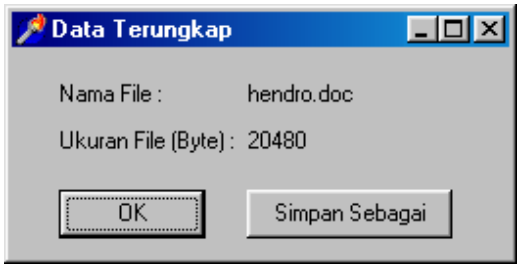
I am sure that his abilities and his personal qualities along with his academic capabilit will help his to obtain his Master's degree at your university, which will be very use for our country.

Bandung, November 15, 2002
Yours Sincerely,

Ir. Rinaldi Munir, M.Sc.
Senior Lecturer
Informatics Engineering Department,
Institute Technology of Bandung (ITB)
Jl. Ganesha No. 10, Bandung 40132
Email : rinaldi@informatika.org
Phone +62-22-2508135
Indonesia

Hasil penyembunyian data (`peppers.bmp` + `hendro.doc`)

Hasil ekstraksi data:



Berkas `hendro-stega.doc` hasil ekstraksi:

LETTER OF RECOMMENDATION

To Whom It May Concern,

Herewith I highly recommend **Mr. R. Hendro Wicaksono** continue his postgradua study at your university. My recommendation is based on my experience as his lecturer several courses for the past four years.

He has shown me his excellent attitude and personality. He is a hard working person a he has a lot of creative ideas. He is also a very intelligent student and he cooperates ve well with his peers whenever they had to work together.

During his study, he showed diligence and eagerness to achieve his goal. He sets ve high standard for himself and organizes himself very well to achieve the standard. I a confident that if he can maintain his goal work, he should be able to complete t postgraduate program well within the stipulated time.

I am sure that his abilities and his personal qualities along with his academic capabilit will help his to obtain his Master's degree at your university, which will be very use for our country.

Bandung, November 15, 2002
Yours Sincerely,

Ir. Rinaldi Munir, M.Sc.
Senior Lecturer
Informatics Engineering Department,
Institute Technology of Bandung (ITB)
Jl. Ganesha No. 10, Bandung 40132
Email : rinaldi@informatika.org
Phone +62-22-2508135
Indonesia

Citra 8 bit

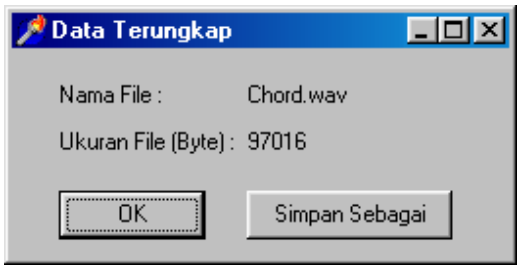
Penampung: citra `barbara.bmp` (512 × 512 *pixel*, 258 KB)

Data yang disembunyikan: `chord.wav` (95 KB) – berkas musik dari Windows.

Hasil penyembunyian data (`barbara.bmp` + `chord.wav`)

Terjadi penurunan kualitas gambar karena pengaruh penurunan jumlah warna (*color quantization*)!

Hasil ektraksi data:



7.7 *Watermarking*

- Salah satu karya intelektual yang dilindungi adalah produk dalam bentuk digital, 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 atas produk digital tersebut tentu dirugikan karena ia tidak mendapat royalti dari usaha penggandaan tersebut.

- Salah satu cara untuk melindungi hak milik intelektual atas produk multimedia (gambar/foto, audio, teks, video) adalah dengan menyisipkan informasi ke dalam data multimedia tersebut dengan teknik *digital 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.

- Pemberian *signature* dengan teknik *watermarking* ini dilakukan sedemikian sehingga informasi yang disisipkan tidak merusak data digital yang dilindungi.

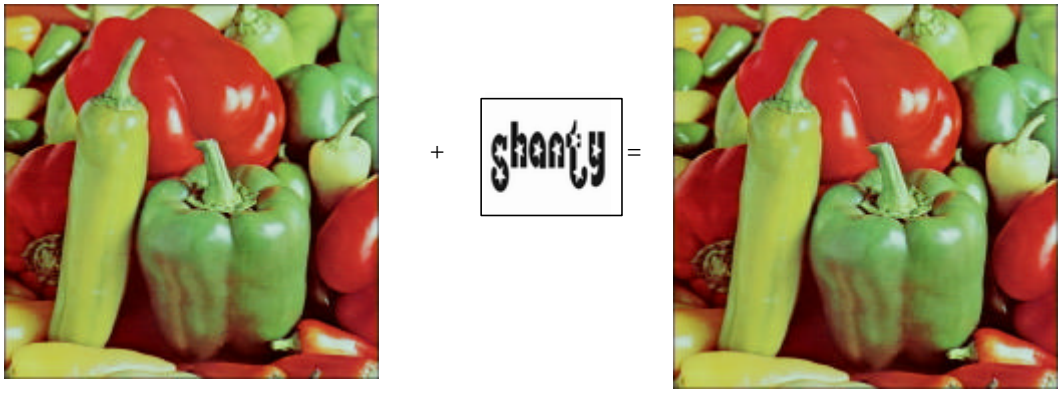
- *Watermark* di dalam data digital tidak dapat dideteksi oleh orang yang tidak mengetahui rahasia skema penyisipan *watermark*, dan juga *watermark* tidak dapat diidentifikasi dan dihilangkan.

- Watermark dapat digunakan sebagai bukti kepemilikan untuk membantu *digital publisher* melindungi materi yang mempunyai hak cipta (*copyright*).

- Jika ada orang lain yang mengklaim bahwa produk digital yang didapatkannya adalah miliknya, maka pemegang hak cipta atas karya multimedia tersebut dapat membantah klaim tersebut dengan proses verifikasi. Caranya, *watermark* diekstraksi dari produk digital yang disengketakan. *Watermark* yang diekstraksi tersebut dibandingkan dengan *watermark* pemegang hak cipta. Jika sama, berarti memang dialah pemegang hak cipta produk multimedia tersebut.

- Pada dasarnya, teknik *watermarking* adalah 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 rusak akibat pemrosesan lanjutan tersebut.

- Gambar 7.4 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 7.4. Memberi *watermark* pada citra *peppers*
(*output* program Tugas Akhir Shanty Meliani H., 13599059, *Robust and Non Blind Watermarking pada Citra Dijital dengan Teknik Spread Spectrum*)

- Berdasarkan tipe dokumen yang diberi *watermark*, *watermarking* dapat diklasifikasikan menjadi:
  1. *Image Watermarking*
  2. *Video Watermarking*
  3. *Audio Watermarking*
  4. *Text Watermarking*

- *Watermarking* dapat juga dikategorikan sebagai *visible watermarking* (*watermark* terlihat oleh indera manusia) dan *invisible watermarking* (*watermark* tidak tampak).

- *Watermarking* dapat juga dikategorikan sebagai *blind watermarking* (proses verifikasi watermark tidak membutuhkan citra asal) dan *non blind watermarking* (proses verifikasi watermark membutuhkan citra asal).

7.8 Sejarah *Watermarking*

- *Watermarking* sudah ada sejak 700 tahun yang lalu. Pada akhir abad 13, pabrik kertas di Fabriano, Italia, membuat kertas yang diberi *watermark* atau tanda-air dengan cara menekan bentuk cetakan gambar atau tulisan pada kertas yang baru setengah jadi. Ketika kertas dikeringkan terbentuklah suatu kertas yang ber-*watermark*. Kertas ini biasanya digunakan oleh seniman atau sastrawan untuk menulis karya mereka. Kertas yang sudah dibubuhi tanda-air tersebut sekalius dijadikan identifikasi bahwa karya seni di atasnya adalah milik mereka.

- Ide *watermarking* pada data digital (sehingga disebut *digital watermarking*) dikembangkan di Jepang tahun 1990 dan di Swiss tahun 1993. *Digital watermarking* semakin berkembang seiring dengan semakin meluasnya penggunaan internet, objek digital seperti video, citra, dan suara yang dapat dengan mudah digandakan dan disebarluaskan.

7.9 Perbedaan Steganografi dengan *Watermarking*

- *Watermarking* merupakan aplikasi dari steganografi, namun ada perbedaan antara keduanya. Jika pada steganografi informasi rahasia disembunyikan di dalam media digital dimana media penampung tidak berarti apa-apa, maka pada *watermarking* justru media digital tersebut yang akan dilindungi kepemilikannya dengan pemberian label hak cipta.

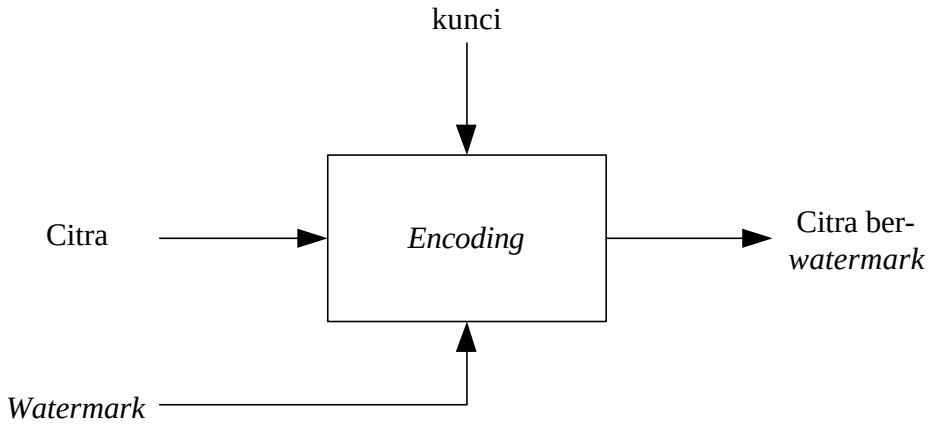
- Meskipun steganografi dan *watermarking* tidak sama, namun secara prinsip proses penyisipan informasi ke dalam data digital tidak jauh berbeda.

- Data *watermark* yang lazim disisipkan ke dalam data digital adalah teks, citra, atau suara. *Watermark* berupa teks misalnya pernyataan atau pesan yang mengindikasikan kepemilikan dokumen (*copyright notification*). *Watermark* berupa teks mengandung kelemahan karena kesalahan satu bit akan menghasilkan hasil teks yang berbeda pada waktu verifikasi (ektraksi).

- *Watermark* berupa suara atau citra lebih disukai karena kesalahan pada beberapa bit *watermark* tidak menghasilkan perubahan yang berarti pada waktu verifikasi. Hasil ekstraksi *watermark* yang mengandung kesalahan tersebut masih dapat dipersepsi secara visual (atau secara pendengaran jika *watermark*-nya berupa suara). Citra yang sering digunakan sebagai *watermark* biasanya logo perusahaan atau lambang.

7.10 Penyisipan Watermark

- Di sini kita hanya meninjau *watermarking* pada citra digital. Proses penyisipan *watermark* ke dalam citra disebut *encoding* dan ditunjukkan Gambar 7.5. *Encoding* dapat disertai dengan pemasukan kunci atau tidak memerlukan kunci. Kunci diperlukan agar *watermark* hanya dapat diekstraksi oleh pihak yang sah. Kunci juga dimaksudkan untuk mencegah *watermark* dihapus oleh pihak yang tidak berhak.



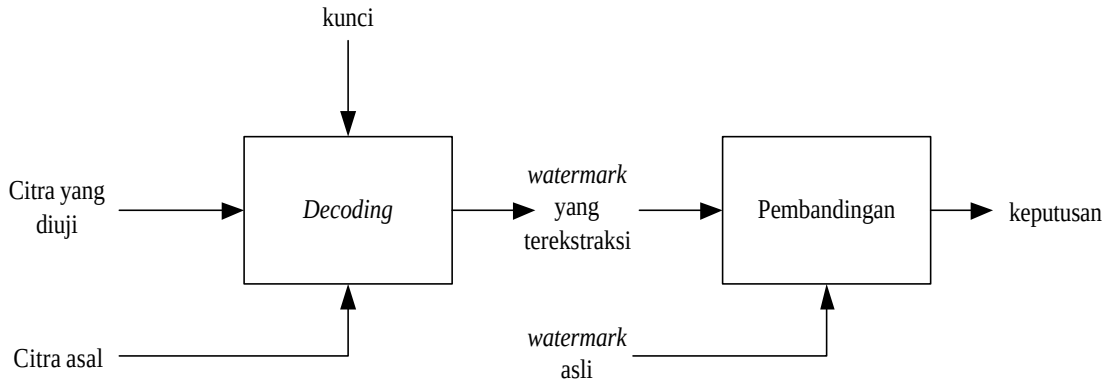
Gambar 7.5 Proses penyisipan *watermark* pada citra digital

7.11 Verifikasi *Watermark*

- Verifikasi *watermark* dilakukan untuk membuktikan status kepemilikan citra digital yang disengketakan. Verifikasi *watermark* terdiri atas dua sub-proses, yaitu ekstraksi *watermark* dan pembandingan.

- Sub-proses ekstraksi *watermark* disebut juga *decoding*, bertujuan mengungkap *watermark* dari dalam citra. *Decoding* dapat mengikutsertakan citra asal (yang belum diberi *watermark*) atau tidak sama sekali, karena beberapa skema *watermarking* memang menggunakan citra asal dalam proses *decoding* untuk meningkatkan unjuk kerja yang lebih baik [HEN03].

- Sub-proses pembandingan bertujuan membandingkan *watermark* yang diungkap dengan *watermark* asli dan memberi keputusan tentang *watermark* tersebut. Proses verifikasi *watermark* ditunjukkan pada Gambar 7.6.



Gambar 7.6 Proses verifikasi *watermark* pada citra digital

7.12 Tujuan *Watermarking* Lainnya

- Selain untuk tujuan pelabelan hak cipta (*copyright labelling*), *watermarking* juga dimanfaatkan untuk tujuan-tujuan lain sebagai berikut [SUP00]:

  1. *Tamper-proofing*. *Watermarking* digunakan sebagai alat untuk mengidentifikasi atau menunjukkan bahwa data digital telah mengalami perubahan dari aslinya.

  2. *Feature location*. *Watermarking* digunakan untuk mengidentifikasi isi dari data digital pada lokasi-lokasi tertentu.

  3. *Annotation/caption*. *Watermarking* digunakan hanya sebagai keterangan tentang data digital itu sendiri.

7.13 *Watermarking* pada Media Digital Lain

- Sebagian besar penelitian, publikasi, dan aplikasi di bidang *watermarking* ditujuan untuk citra digital. Namun, *watermarking* juga dapat diterapkan pada jenis multimedia lain seperti suara (misalnya musik MP3), video, dan teks.

- Sedangkan *watermarking* pada video digital harus sedemikian rupa sehingga peralihan gambar dari satu *frame* ke *frame* lainnya harus tetap baik dan tidak terlihat dimodifikasi. Karena video digital ukurannya relatif besar daripada citra, maka *watermark* yang disisipkan dapat lebih banyak.

- Khusus *watermarking* pada data audio, kehati-hatian perlu dilakukan pada perancangan algoritma *watermarking*-nya, karena suara lebih sensitif daripada gambar. Hal ini berarti suara digital lebih mudah rusak bila ditambahkan *watermarking*.

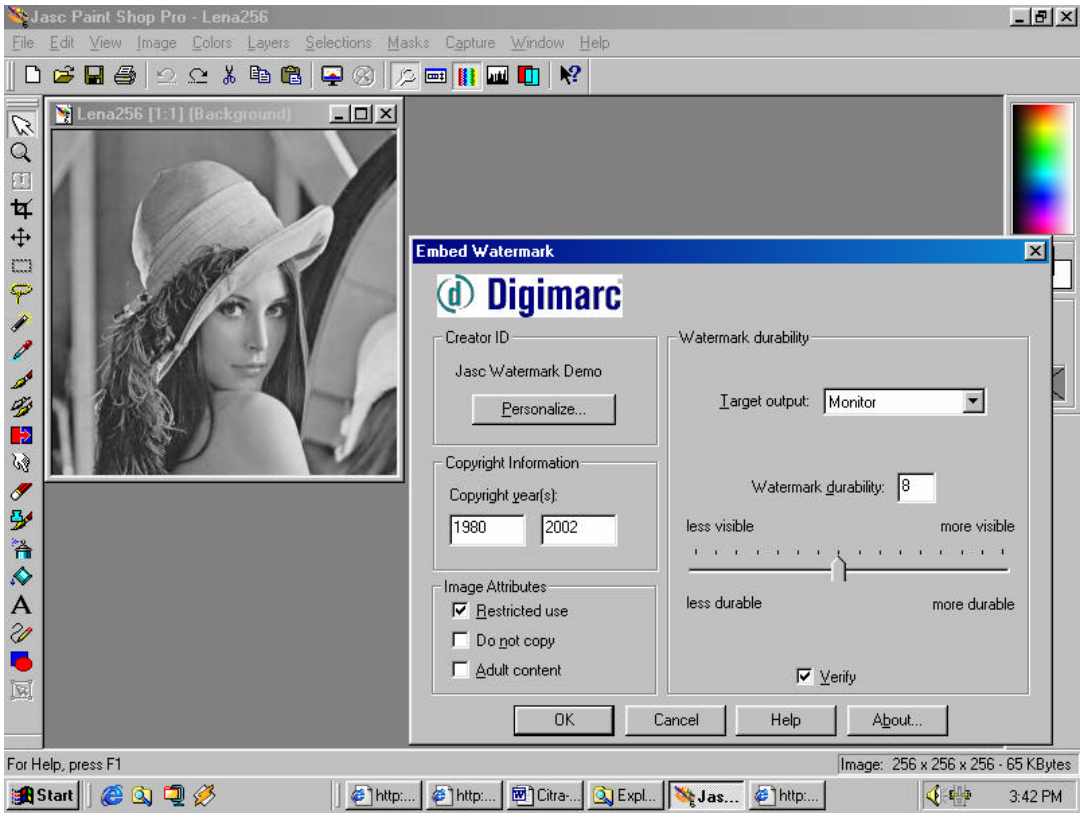
- Saat ini, *Microsoft* sedang meneliti untuk mengembangkan sistem *watermarking* untuk audio digital, yang akan dimasukkan ke dalam media player *Windows*. Dengan sistem *watermarking* ini, data seperti informasi lisensi disisipkan ke dalam musik/lagu; *media player* tidak akan memainkan *file* audio yang memuat *watermark* yang salah.

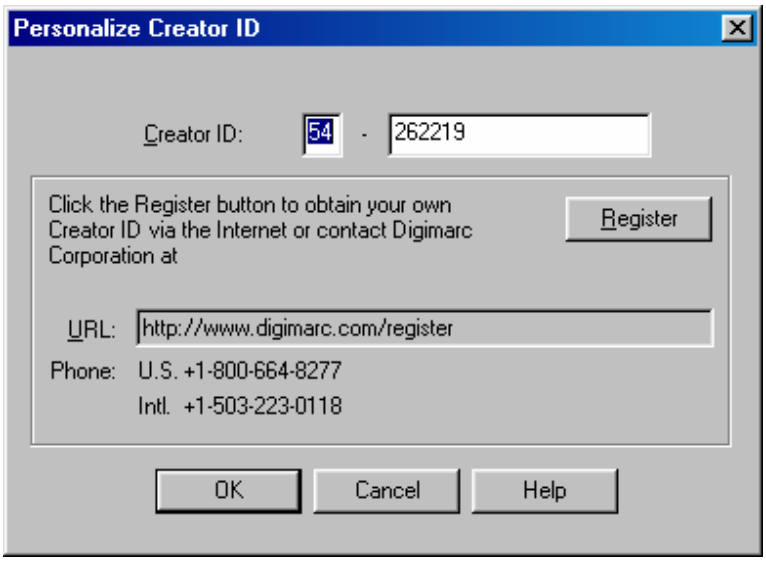
- Terakhir, *watermarking* pada dokumen teks menggunakan metode yang berbeda daripada 3 media lainnya. Salah satunya dengan menyisipkan spasi antara dua buah kata atau antara dua buah kalimat di dalam dokumen.

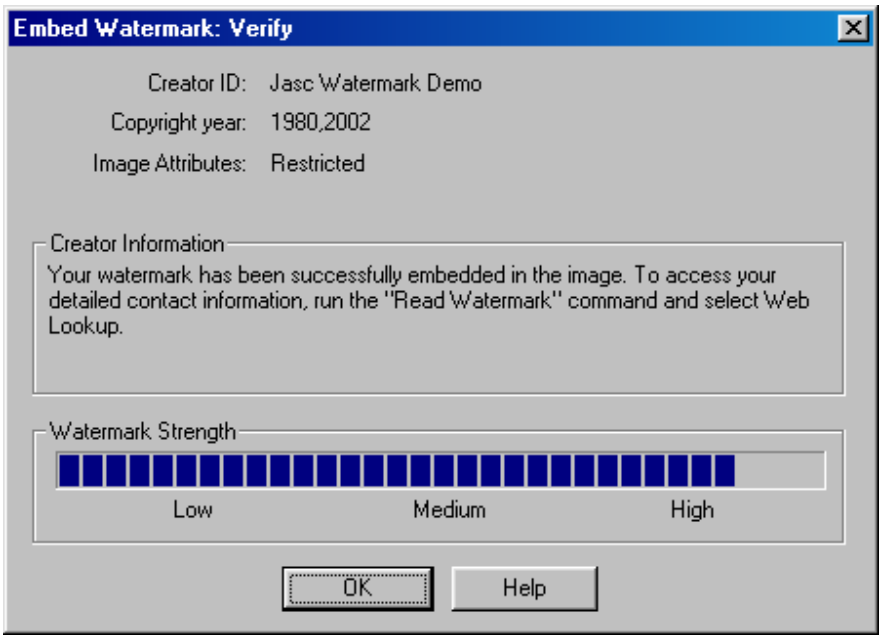
7.14 *Watermarking* pada Program Komersil

- Banyak program multimedia komersil dilengkapi dengan menu untuk menambahkan *watermark*, seperti pada *Adobe Photoshop 5.5* (www.adobe.com) dan *PaintShop Pro. 6.*

- Contoh menu *watermark* pada program **Paintshop Pro. 6**:




Personalize Creator ID
Creator ID:
54
-
262219
Click the Register button to obtain your own Creator ID via the Internet or contact Digimarc Corporation at
Register
URL:
http://www.digimarc.com/register
Phone:
U.S. +1-800-664-8277
Intl. +1-503-223-0118
OK
Cancel
Help


Embed Watermark: Verify
Creator ID:
Jasc Watermark Demo
Copyright year:
1980,2002
Image Attributes:
Restricted
Creator Information
Your watermark has been successfully embedded in the image. To access your detailed contact information, run the "Read Watermark" command and select Web Lookup.
Watermark Strength
Low
Medium
High
OK
Help

- Citra Lena sesudah pengisian informasi *watermark*:

- Perangkat lunak *digital watermarking* dari *Blue Spike's Giovanni*™ (www.bluespike.com) menggunakan kunci kriptografi untuk membangkitkan *watermark* ke dalam musik dan citra digital.

- Perusahaan *software* yang menawarkan solusi *digital watermarking* adalah *Digimarc* (www.digimark.com) dan *Cognicity* (www.cognicity.com).

- Situs *web* yang lain tentang steganografi dan *digital watermaking* yang perlu dikunjungi:

  1. www.outguess.org
     Menyediakan secara gratis kakas steganografi.

  2. www.demcom.com
     Perangkat lunak *Steaganos Security Suite* dari *DemCom* mengizinkan anda untuk mengenkripsi dan menyembunyikan arsip ke dalam berkas audio, video, teks, atau HTML.

3. www.cl.cam.ac.uk/~fapp2/steganography/index.html

   Homepage mengenai *information hiding* yang memiliki informasi teknis, berita, dan *link* yang berkaitan dengan digital watermarking dan steganografi.

4. www.digimarc.com

   Homepage lainnya dari Digimarc.