# *Watermarking* dengan Algoritma Kunci Publik untuk Verifikasi dan Otentikasi Citra

Angga Indra Brata
13500070

*Departemen Teknik Informatika*
*Institut Teknologi Bandung*
*Jalan Ganesha 10 Bandung 40132*

*E-mail : angga_indra@yahoo.com*

**Abstrak**

Terdapat dua kebutuhan yang berkaitan dengan penggunaan citra dijital, yaitu kebutuhan verifikasi dan kebutuhan otentikasi citra. Kebutuhan verifikasi yaitu kebutuhan untuk mengetahui apakah suatu citra dijital sudah pernah dimanipulasi atau belum, dengan kata lain untuk mengetahui keaslian suatu citra. Sedangkan kebutuhan otentikasi yaitu kebutuhan kepemilikan (*copyright*) suatu citra dijital. Otentikasi ini harus dapat dilakukan oleh publik tanpa perlu kehadiran pemilik asli citra tersebut.

Dijital watermark adalah informasi kepemilikan suatu arsip dijital. Informasi tersebut dapat berupa citra, teks, audio, ataupun video.

Untuk kebutuhan verifikasi citra, digunakan *watermark* yang bersifat *fragile* (*fragile watermark*), yaitu *watermark* yang rentan perubahan/manipulasi. Sehingga ketika suatu citra yang sudah disisipi *fragile watermark* dimanipulasi kemudian diekstrak, akan menyebabkan hasil ekstraksi menjadi citra yang tidak valid. Salah satu cara agar untuk membuat *fragile watermark* adalah dengan menggunakan algoritma hash satu arah (*one way hash*) pada prosedur penyisipan *watermark* dan ekstraksi *watermark.* Fungsi hash satu arah adalah suatu fungsi yang mengubah suatu pesan dengan panjang berapapun menjadi pesan baru (*message digest*) dengan panjang tertentu. Fungsi hash satu arah yang digunakan adalah MD5 yang menghasilkan *message digest* dengan panjang 128 bit. Algoritma *watermarking* yang digunakan adalah LSB *modification* yang sederhana.

Untuk kebutuhan otentikasi citra, agar otentitakasi dapat dilakukan oleh publik, maka digunakan algoritma kriptografi kunci publik sebagai fungsi tambahan pada prosedur penyisipan *watermark* dan ekstraksi *watermark*. Pada prosedur penyisipan *watermark*, pemilik citra menggunakan kunci rahasianya untuk melakukan enkripsi pada citra ber-*watermark.* Sedangkan pada prosedur ekstraksi *watermark*, setiap orang (publik) dapat menggunakan kunci publik pemilik untuk melakukan dekripsi pada citra ber-*watermark* untuk mengekstrak *watermark* yang disisipkan. Algoritma kriptografi kunci publik yang digunakan adalah RSA.

***Kata kunci**: verifikasi, otentikasi, citra dijital, fragile watermark, algoritma kriptografi kunci publik, hash satu arah.*

## 1. Pendahuluan

Teknologi yang semakin maju memunculkan fenomena-fenomena baru yang berkembang di masyarakat, salah satunya adalah citra dijital. Citra dijital sudah menjadi kebutuhan yang cukup penting untuk beberapa kalangan, dari perusahaan-perusahaan besar seperti penggunaan citra dijital pada GPS (*Global Positioning System*), sampai dengan perorangan.

Pengguna citra dijital seringkali melakukan manipulasi pada suatu citra dijital untuk mendapatkan tampilan citra dijital baru sesuai dengan yang pengguna tersebut inginkan. Terkait dengan hal ini, beberapa pengguna citra dijital tidak ingin citra dijital miliknya dapat berubah atau diubah, atau paling tidak mereka dapat mengetahui jika citra miliknya telah berubah atau termanipulasi, sehingga mereka bisa menentukan apakah citra tersebut layak pakai atau tidak. Pengguna seperti ini misalnya pihak medis yang mempunyai citra dijital berupa gambar dari bagian tertentu tubuh pasiennya dan pekerja di media massa yang mempunyai citra berupa fakta yang akan diberitakan di media massa. Kebutuhan seperti ini disebut kebutuhan **verifikasi** citra. Kebutuhan lain yang muncul adalah kebutuhan **otentikasi** citra yaitu kebutuhan kepemilikan (*copyright*) suatu citra dijital.

*Watermarking* dapat menjadi solusi untuk menyelesaikan kedua masalah tersebut. *Watermarking* yaitu teknik menyisipkan suatu informasi ke dalam data multimedia. Informasi tersebut dapat berupa data data citra, audio, ataupun video yang menggambarkan kepemilikan suatu pihak. Informasi yang disisipkan tersebut disebut *watermark*. *Watermark* dapat dianggap sebagai sidik dijital dari pemilik data multimedia tersebut, dalam hal ini berupa citra dijital.

## 2. Penyisipan *Watermark*

*Watermark* yang akan disisipkan harus berukuran yang jauh lebih kecil daripada ukuran citra dijital, maksimal seperdelapan dari ukuran citra dijital (tidak termasuk *header* citra). *Watermark* dapat berupa citra, teks, audio, ataupun video. *Watermark* yang disisipkan dipecah-pecah menjadi blok-blok dengan ukuran masing-masing blok adalah 128 bit sesuai dengan hasil keluaran (*message digest*) fungsi hash satu arah MD5.

Sebelumnya, citra dijital dipecah-pecah dahulu menjadi blok-blok sehingga LSB (*Least Significant Bit)* setiap blok dapat digantikan dengan blok *watermark* yang telah dikenai beberapa proses. Proses-proses yang terjadi yaitu blok *watermark* (128 bit) di-XOR dengan hasil MD5 (*message digest* dengan panjang 128 bit) dari blok citra dijital yang LSB-nya sudah diubah menjadi 0.

Kemudian hasil XOR tersebut akan dienkripsi dengan RSA menggunakan kunci rahasia dari pemilik citra dijital. Hasil dari enkripsi ini akan menggantikan LSB pada blok citra dijital yang sebelumnya diset 0.

Lihat gambar 1.

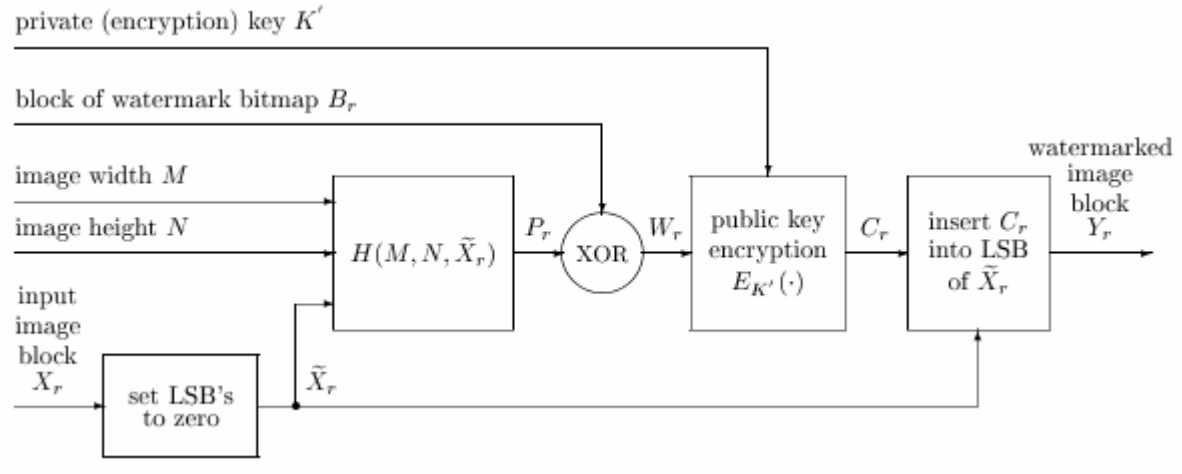
## 3. Ekstraksi *Watermark*

Dengan perhitungan yang sama, citra ber-*watermark* dibagi menjadi blok-blok. Setiap blok dari citra ber-*watermark* tersebut akan dipecah menjadi dua, yaitu blok citra ber-*watermark* yang LSB-nya diset 0 (B1) dan hasil ekstraksi LSB blok citra ber-*watermark* (B2).

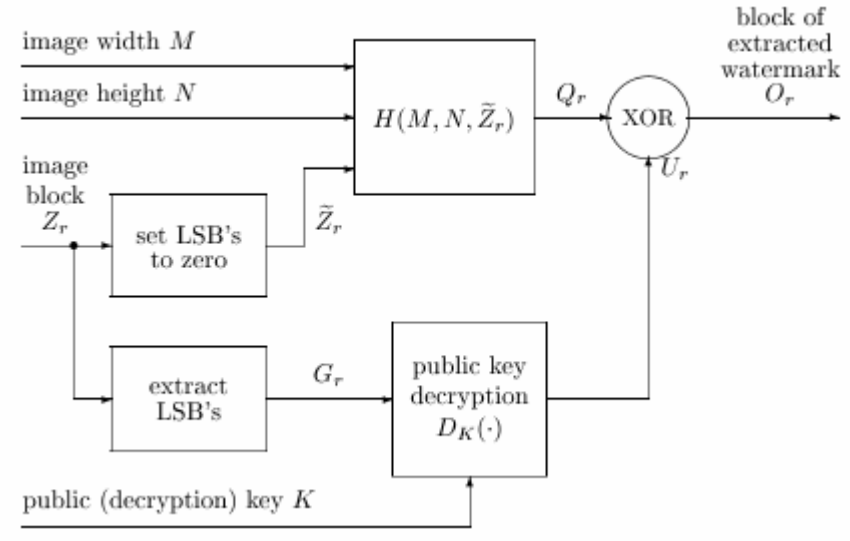
B1 akan dikenai MD5 sehingga menghasilkan *message digest* dengan panjang 128 bit. Sedangkan B2 akan didekripsi dengan RSA menggunakan kunci publik pemilik citra dijital. Jika kunci publik yang digunakan adalah kunci yang bersesuaian dengan kunci rahasia yang digunakan pada saat penyisipan maka hasil dekripsi B2 mempunyai panjang 128 bit atau kurang dari 128 bit di blok citra terakhir.

Kemudian hasil MD5 B1 di-XOR dengan hasil dekripsi RSA B2. Hasil XOR tersebut adalah blok *watermark* yang diekstrak.

Lihat gambar 2.




**Gambar 1 Skema Penyisipan *Watermark***




**Gambar 2 Skema Ekstraksi *Watermark***

## 4. Hasil Eksperimen

Jika citra ber-*watermark* belum dimanipulasi (merubah warna piksel, merubah ukuran citra, memfilter citra, atau rotasi citra) dan kunci publik yang digunakan pada saat ekstraksi adalah kunci yang bersesuaian dengan kunci rahasia yang digunakan pada saat penyisipan *watermark*, maka *watermark* hasil ekstrasi akan tepat sama dengan *watermark* yang disisipkan. Lihat gambar 1 dan 2. Jika $Z_r = Y_r$, dan $\tilde{Z}_r = \tilde{X}_r$, dan $G_r = C_r$, maka akan mengakibatkan $P_r = Q_r$ dan $U_r = W_r$. Dengan demikian, blok citra ber-*watermark* hasil ekstraksi $O_r$ akan sama dengan blok *watermark* pada saat penyisipan $B_r$.

Jika citra ber-*watermark* sudah dimanipulasi atau kunci publik yang digunakan pada saat ekstraksi adalah kunci yang tidak bersesuaian dengan kunci rahasia yang digunakan pada saat penyisipan *watermark*, maka *watermark* hasil ekstraksi hasilnya akan jauh berbeda dengan *watermark* yang disisipkan.

Perubahan ukuran citra ber-*watermark* akan sangat berpengaruh terhadap hasil ekstraksi karena parameter panjang dan lebar (M dan N) dari citra ber-*watermark* tersebut digunakan sebagai salah satu parameter pada fungsi hash MD5, lihat gambar 1 dan 2. Sehingga jika M dan N pada prosedur penyisipan berbeda dengan M dan N pada prosedur ekstraksi maka $P_r \neq Q_r$.

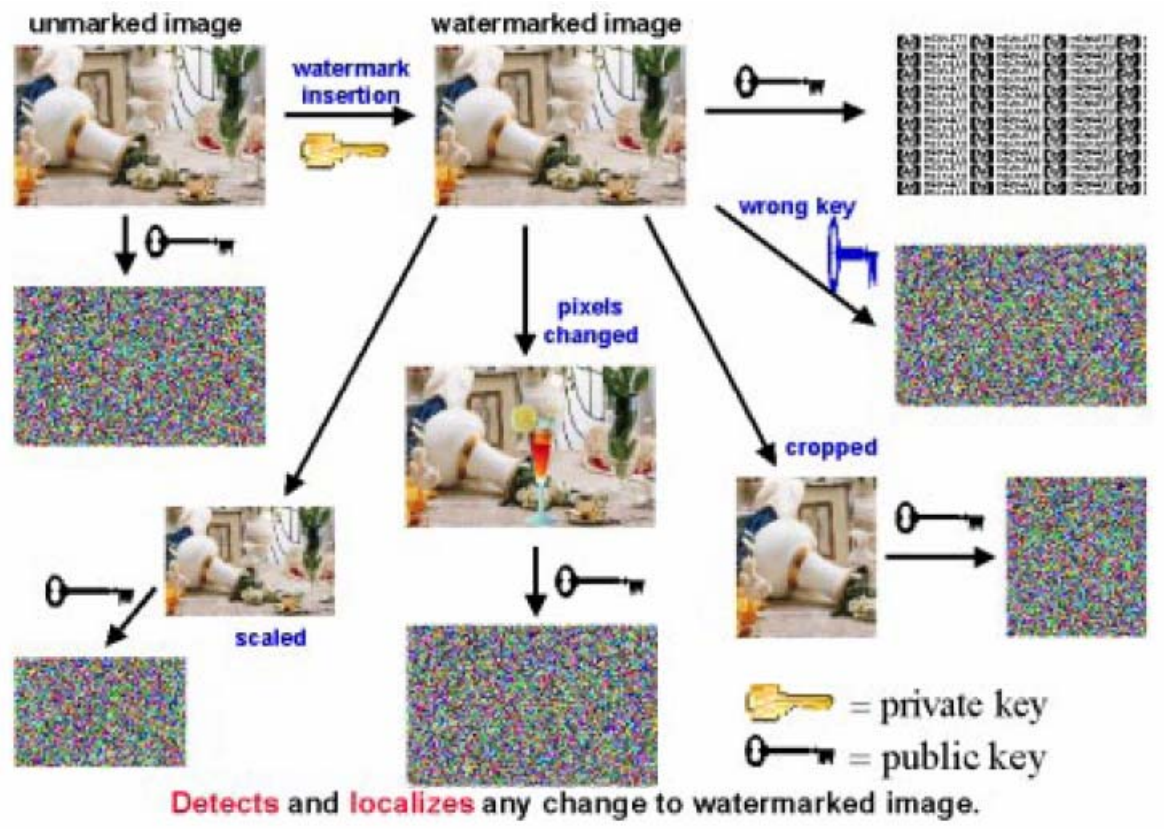
Jika kunci publik yang diinputkan pada proses ekstraksi *watermark* adalah kunci yang tidak bersesuaian dengan kunci rahasia pada proses penyisipan *watermark*, maka akan menyebabkan $U_r \neq W_r$.

Hasil eksperimen dengan menggunakan *watermark* berupa citra dapat dilihat pada gambar 3.

## 5. Kesimpulan

Beberapa kesimpulan yang dapat diambil antara lain :

1. Konsep *fragile watermarking* yang digunakan pada riset ini, menyebabkan citra ber-*watermark* rentan terhadap manipulasi citra. Sehingga jika citra ber-*watermark* tersebut dimanipulasi, akan mengekstrak *watermark* yang tidak valid, atau paling tidak sudah jauh berubah dari aslinya.
2. Kebutuhan verifikasi citra, yaitu keaslian dan integritas citra, dapat dipenuhi oleh riset ini, khususnya dengan algoritma *hashing* satu arah MD5 yang merupakan salah satu komponen fungsi yang digunakan.
3. Kebutuhan otentikasi citra, yaitu kepemilikan citra, dapat dipenuhi dengan memberikan *watermark* pada citra dijital tersebut dan dengan kriptografi kunci publik RSA sehingga setiap orang (publik) dapat melakukan otentikasi citra.
4. Kunci publik yang diinputkan harus bersesuaian dengan kunci rahasia yang digunakan saat penyisipan. Jika terjadi kesalahan, maka akan terekstrak *watermark* yang tidak valid.
5. Semua jenis *watermark*, baik citra, teks, audio, video, maupun berkas dijital yang lain dapat digunakan sebagai *watermark* pada riset ini dengan catatan ukuran *watermark* tersebut cukup untuk disisipkan pada LSB citra dijital.




**Gambar 3 Hasil Eksperimen terhadap Kesalahan Kunci dan Manipulasi Citra**

## 6. Referensi

[PIN04] http://www.tsi.enst.fr/~maitre/tatouage/icip98/ma11_07.pdf. *A Public Key Watermark for Image Verification and Authentication.* Ping Wah Wong. Hawlett Packard Company. Februari 2004.

[POL98] *Penerapan Steganografi dengan Citra Dijital Sebagai File Penampung*, Lazarus Poli. Tugas Akhir Departemen Teknik Informatika Institut Teknologi Bandung, 1998.

[RIN03] Diktat Kuliah IF5054 – Kriptografi, Rinaldi Munir. Departemen Teknik Informatika Institut Teknologi Bandung. Agustus 2003.

[RIV04] http://www.faqs.org/rfcs/rfc1321.html. *RFC 1321 - The MD5 Message-Digest Algorithm*. Ronald R. Rivest. Massachusetts Institute of Technology Laboratory for Computer Science. Maret 2004.

[SCH96] *Applied Cryptography – Protocols, Algorithms, and Source Code in C*. Bruce Schneier. John Wiley & Sons, Inc. 2004.

[SHA03] *Robust and Non Blind Watermarking* pada Citra Dijital dengan Teknik *Spread Spectrum*. Shanty Meliani Hendrawan. Tugas Akhir Departemen Teknik Informatika Institut Teknologi Bandung, 2003.