

# Analisis Beberapa Teknik *Watermarking* dengan Domain Spasial pada Citra Digital

Athia Saelan (13508029)<sup>1</sup>

Program Studi Teknik Informatika

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung, Jl. Ganessa 10 Bandung 40132, Indonesia

<sup>1</sup>if18029@students.if.itb.ac.id

**Abstrak**— Dokumen digital sangat mudah disebarkan melalui berbagai media dan sangat mudah diedit. Karena itu, kepemilikan dan keaslian dari sebuah dokumen digital seringkali menjadi bias. Untuk itu, digunakanlah teknik watermarking, yaitu teknik untuk menyisipkan suatu tanda yang disebut watermark pada sebuah dokumen. Watermarking ini sebaiknya memenuhi tiga kriteria, yaitu imperceptible (tidak dapat dipersepsi), robustness (ketahanan), dan secure (aman). Salah satu dokumen digital yang banyak tersebar adalah citra (gambar). Teknik yang dapat dilakukan untuk watermarking pada citra terdiri dari dua domain, yaitu domain spasial dan domain frekuensi. Pada domain spasial, bit watermark disisipkan pada piksel-piksel citra. Ada beberapa teknik watermarking yang termasuk domain spasial, antara lain visible watermarking, teknik LSB (Least Significant Bit), dan teknik adaptif. Pada makalah ini, ketiga teknik watermarking tersebut dibahas berdasarkan kriteria watermarking yang baik serta aspek lain yang berhubungan.

**Kata Kunci**—citra digital, domain spasial, watermarking

## I. PENDAHULUAN

Saat ini, penggunaan dokumen digital semakin luas. Dokumen digital ini sangat praktis, selain mudah disimpan, juga mudah digandakan, diedit, serta disebarluaskan.

Namun, ada beberapa masalah dengan kemudahan ini. Sebegitu mudahnya seseorang mendapatkan dokumen dari orang lain, kemudian menggandakannya dan menyebarkan pada orang lain lagi, dan seterusnya, sehingga seringkali pemilik asli dari dokumen tersebut tidak diketahui.

Selain mudah digandakan, dokumen digital juga mudah diedit. Seseorang bisa saja mendapatkan dokumen milik orang lain, kemudian mengeditnya, dan menyebarkannya ke pihak lain sehingga keaslian dokumennya menjadi tercemar.

Untuk mengatasi masalah tersebut, dapat digunakan watermarking. Watermarking merupakan penyisipan suatu tanda yang khusus sebagai identifikasi dari kepemilikan suatu dokumen.

## II. WATERMARKING

Pada awalnya, watermark atau tanda air adalah suatu tanda gambar atau pola yang dicetak bersama kertas, dan akan terlihat ketika diterawangkan ke cahaya. Watermark ini biasanya digunakan untuk keamanan dokumen penting.

Setelah muncul dokumen digital yang juga membutuhkan keamanan, muncullah digital watermark. Digital watermarking ini menggunakan teknologi steganografi, yaitu penyisipan pesan pada arsip lain sehingga tidak mencurigakan. Beberapa persyaratan umum digital watermarking adalah:

- Imperceptible  
Watermark yang disisipkan sebaiknya tidak mudah dideteksi oleh indera.
- Robustness  
Watermark yang disisipkan sebaiknya tahan dari kerusakan. Kerusakan pada watermark menyebabkannya tidak lagi berguna. Kerusakan bisa diakibatkan oleh pengeditan atau penyebaran melalui berbagai media.
- Secure  
Watermark yang disisipkan sebaiknya tidak mudah diekstraksi, disimpan, atau dipindahkan ke dokumen lain. Kemudahan pemindahan dapat mengakibatkan penyalahgunaan watermark.

Digital watermarking dikategorikan berdasarkan ketahanannya.

1. Fragile Watermark  
Pada fragile watermarking, watermark memang sengaja dibuat mudah rusak. Tujuannya adalah untuk mengetahui apakah suatu citra masih asli atau sudah pernah diedit. Pada watermarking jenis ini, robustness tidak masuk sebagai persyaratan.
2. Robust Watermarking  
Pada robust watermarking, watermark dibuat agar sebisa mungkin tidak mudah rusak.

Tujuannya adalah sebagai identifikasi kepemilikan dari suatu citra.

Selain itu, digital watermarking juga bisa dikategorikan berdasarkan kenampakannya.

1. Visible watermarking  
Pada visible watermarking, watermark memang sengaja ditampakkan untuk alasan tertentu. Pada watermarking jenis ini, imperceptible tidak masuk sebagai persyaratan. Watermarking jenis ini mudah dibuat dengan menggunakan program pengolah citra. Namun, kelemahannya adalah watermark mudah dihapus dengan menggunakan program yang sama.
2. Invisible watermarking  
Pada invisible watermarking, penyisipan watermark seharusnya tidak mengubah kualitas citra, yaitu citra sebelum diberi watermark dan sesudahnya harus tampak sama. Watermarking jenis ini lebih sulit dibuat, dengan teknik-teknik yang akan dijelaskan pada bagian selanjutnya.

Ada banyak teknik yang dapat digunakan untuk menyisipkan watermark pada citra. Namun, pada dasarnya, ada dua domain dalam penyisipan watermark dalam citra digital.

1. Domain spasial  
Pada domain spasial, watermark disisipkan dalam bit-bit citra penampungnya, misalnya dengan mengubah beberapa bit dari beberapa piksel pada citra.
2. Domain frekuensi  
Pada domain frekuensi, penyisipan dilakukan dengan cara mengubah citra menjadi suatu frekuensi tertentu, kemudian menyisipkan watermark, dan mengembalikannya menjadi citra yang sudah berwatermark.

Pada makalah ini, akan lebih difokuskan pada watermarking dengan domain spasial.

### III. WATERMARKING PADA DOMAIN SPASIAL

Pada bagian ini, akan dibahas beberapa teknik yang dapat dilakukan untuk watermarking pada domain spasial. Selain itu, akan dibahas juga kelayakan masing-masing teknik berdasarkan persyaratan umum dari digital watermarking.

#### A. Visible Watermarking

Visible watermarking merupakan metode yang paling mudah digunakan untuk membuat watermark. Cara ini hanya membutuhkan program pengolah citra biasa untuk membuatnya, dan hanya membutuhkan mata untuk mendeteksinya.



Gambar 1 citra dengan visible watermark

Namun, teknik ini tentunya tidak memenuhi beberapa persyaratan umum digital watermarking. Misalnya untuk imperceptible, metode ini jelas-jelas membuat watermarknya terlihat dengan mata. Meskipun begitu, pengguna metode ini tentu menyadari keterlihatan watermark dan sengaja membuatnya terlihat dengan alasan tertentu.

Selain itu, metode ini juga tidak memenuhi persyaratan secure. Karena terlihat dengan jelas, orang lain akan dengan mudah memindahkan watermarknya dan menyimpannya, atau menggunakannya pada citra yang lain.

Meskipun begitu, metode ini tahan dalam persyaratan robustness, kecuali jika memang ada yang sengaja menghapus. Dengan cara ini, watermark akan tetap ada ketika sebuah citra diubah intensitasnya, dikompresi, diputar, atau diskala.

#### B. LSB

Salah satu metode yang sering digunakan untuk watermarking pada domain spasial adalah LSB (Least Significant Bit). Pada metode LSB, bit-bit pesan disisipkan pada bit terakhir, atau bit paling kanan, dari pixel-pixel citra penampung.

Sebagai contoh, misalnya beberapa pixel dari citra adalah sebagai berikut:

100110101 01100111 110110000 110011010

Kemudian watermark yang akan disisipkan:

0110

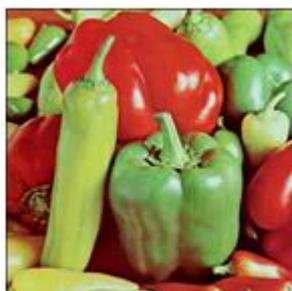
Maka hasil penyisipannya adalah:

100110100 01100111 110110001 110011010

Metode ini memanfaatkan kelemahan indera manusia yang tidak dapat melihat perbedaan warna satu atau dua bit. Karena itu, metode ini sangat imperceptible.



(a)



(b)

**Gambar 2 4** (a) contoh citra sebelum diberi watermark dan (b) contoh citra setelah diberi watermark dengan teknik LSB.

Namun, metode ini hanya dapat digunakan pada citra bitmap dengan jumlah warna yang cukup banyak, misalnya 24-bit. Untuk bitmap yang warnanya tidak banyak, perbedaan warna akan mudah dipersepsi oleh mata manusia. Sedangkan untuk yang bukan bitmap, metode ini tidak dapat digunakan karena dasar dari metode ini adalah penyisipan pada bit sehingga harus disimpan data per bitnya. Karena itu, metode ini sangat tidak robust untuk dikompresi ke jenis lain seperti JPEG.

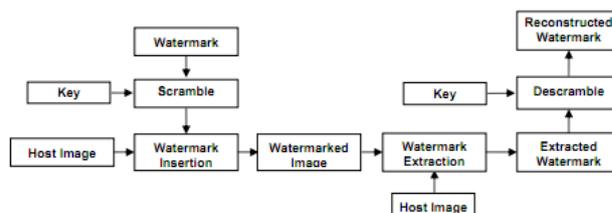
Selain itu, metode ini juga tidak robust jika diubah intensitasnya, atau diputar dan diskala. Dengan cara itu, watermark bisa hilang sama sekali. Namun untuk crop, watermark hanya akan hilang sebagian, atau bahkan tidak hilang apabila bagian yang dicrop tidak mengandung watermark. Cara ini dapat digunakan untuk fragile watermarking untuk mengetahui apakah sebuah citra digital sudah pernah diedit atau masih asli.

Untuk persyaratan secure, watermark ini sangat tidak aman. Untuk mendapatkan watermark, cukup diambil bit terakhir dari setiap pikselnya. Bit terakhir ini dapat saja diambil dan dipindahkan ke citra yang lain sehingga citra yang lain tersebut juga memiliki watermark yang sama.

### C. Metode Adaptif

Mirip dengan LSB, metode ini juga memanfaatkan kelemahan indera penglihatan manusia yang tidak dapat membedakan perbedaan warna beberapa tingkat. Namun, untuk memperkuat robustnessnya, bit yang diubah tidak hanya pada satu piksel, dan perubahannya tidak hanya dilakukan pada bit terakhir atau kedua dari terakhir, dengan tetap memperhatikan sensitivitas penglihatan manusia.

Pada metode ini, hal yang pertama dilakukan adalah mengacak watermark dengan menggunakan kunci tertentu. Setelah diacak, watermark disisipkan ke dalam citra. Sebelumnya, citra terlebih dahulu dibagi ke dalam blok-blok sejumlah watermark yang akan disisipkan. Misalnya watermark berukuran 200 bit, maka citra harus dibagi sejumlah 200 blok untuk disisipkan satu bit watermark di setiap bloknya.



**Gambar 3** skema adaptive watermarking

Setelah watermark diacak dan citra dibagi ke dalam blok-blok, dilakukanlah penyisipan. Penyisipan satu bit watermark ke dalam satu blok citra dilakukan dengan aturan sebagai berikut.

1. Hitung intensitas rata-rata ( $y_{mean}$ ), maksimum ( $y_{max}$ ), dan minimum ( $y_{min}$ ) dari blok tersebut.
2. Hitung intensitas rata-rata  $m_H$  dan  $m_L$

$$m_H = \frac{(y_{max} + y_{mean})}{2}$$

$$m_L = \frac{(y_{mean} + y_{min})}{2}$$

3. Sisipkan nilai bit watermark dengan memodifikasi nilai intensitas piksel pada blok dengan aturan berikut:

Jika nilai bit = 0:

$$y' = y_{max} \quad \text{jika } y > m_H$$

$$y' = y_{mean} \quad \text{jika } m_L \leq y < m_{mean}$$

$$y' = y + \delta \quad \text{untuk lainnya}$$

Jika nilai bit = 1:

$$y' = y_{min} \quad \text{jika } y < m_L$$

$$y' = y_{mean} \quad \text{jika } m_{mean} \leq y < m_H$$

$$y' = y - \delta \quad \text{untuk lainnya}$$

$y'$  adalah intensitas yang baru dan  $\delta$  adalah sebuah nilai yang telah ditentukan nilainya.

Untuk ekstraksinya, cukup dengan membandingkan citra yang belum diberi watermark dan citra yang telah diberi watermark. Jika jumlah intensitas citra yang telah diberi watermark lebih besar, berarti nilainya 1, sedangkan jika lebih kecil berarti nilainya 0. Setelah itu, dilakukan penyusunan nilai bit watermark berdasarkan kunci yang digunakan untuk pengacakannya.



(a)



(b)

**Gambar 4** (a) contoh citra sebelum diberi watermark dan (b) contoh citra setelah diberi watermark dengan teknik adaptif.

Metode ini cukup bergantung pada nilai delta ( $\delta$ ) yang

dimasukkan. Nilai delta ini akan mempengaruhi ketahanan (robustness) dan ketidakterlihatan (imperceptibility) watermark. Semakin besar nilai delta, maka ketahanan akan semakin baik, tetapi keterlihatannya semakin jelas. Sebaliknya, semakin kecil nilai delta, ketahanan akan semakin lemah, tetapi watermark semakin tidak terlihat.

Karena disisipkan di beberapa blok, secara umum, metode ini cukup tahan terhadap serangan misalnya kompresi, perubahan ukuran, dan rotasi. Saat dikompresi, secara umum data akan berubah secara berkelompok, sehingga penyisipan data pada satu kelompok piksel citra akan lebih baik daripada hanya pada satu piksel. Semakin besar jumlah piksel dalam satu blok akan semakin baik. Hal tersebut juga berlaku untuk skala dan rotasi.

Selain itu, karena posisi watermark diletakkan secara random, metode ini juga cukup tahan terhadap serangan crop. Jika dicrop, maka yang hilang adalah bagian-bagian tertentu yang letaknya acak sehingga hasil ekstraksi watermark masih bisa dipersepsi dengan mata. Namun jika yang dicrop terlalu banyak, informasi yang hilang akan terlalu banyak sehingga akan lebih sulit untuk mempersepsi hasil ekstraksi.

Namun, karena yang dilihat adalah perbandingan intensitas citra asli dan citra yang telah diberi watermark, cara ini kemungkinan tidak akan tahan terhadap perubahan intensitas. Jika intensitas citra yang telah diberi watermark dinaikkan, hasil ekstraksi akan cenderung bernilai satu. Sebaliknya jika intensitas diturunkan, hasil ekstraksi akan cenderung bernilai nol.

Untuk persyaratan secure, metode ini sudah cukup aman. Selain posisi bit watermarknya sudah diacak, nilai bit yang disisipkan tidak bisa mengetahui apabila citra asli tidak dimiliki. Hal ini terjadi karena proses ekstraksi yang dilakukan adalah dengan membandingkan intensitas citra asli dengan citra yang sudah diberi watermark.

#### IV. ANALISIS

Dari beberapa teknik watermarking yang sudah dibahas, pada bagian ini akan dilakukan perbandingan antar metode untuk setiap kriteria.

##### A. Imperceptible

Seperti yang sudah disebutkan pada bagian-bagian sebelumnya, imperceptible adalah tidak dapat terdeteksi oleh indera manusia, dalam hal ini indera penglihatan.

Untuk visible watermark, sudah jelas bahwa watermark dapat dilihat dengan mudah menggunakan mata manusia. Namun, biasanya hal ini memang disengaja oleh pembuatnya karena suatu alasan, misalnya untuk kepentingan komersial.

Untuk dua metode yang lain, yaitu metode LSB dan metode adaptif, dapat dilihat dari cara penyisipan pesannya. Pada metode LSB, yang diubah hanya bit terakhir saja. Sedangkan metode adaptif juga mengubah

beberapa bit sebelum terakhir. Karena itu, watermark pada metode LSB akan lebih tidak terlihat daripada watermark pada metode adaptif. Meskipun begitu, metode adaptif masih tetap memenuhi kriteria imperceptible karena keberadaan watermark tidak dapat terdeteksi oleh mata.

### B. Robustness

Robustness adalah ketahanan suatu watermark terhadap serangan. Serangan yang diberikan biasanya berupa kompresi, atau pengeditan seperti crop, pemutaran dan perubahan ukuran.

Pada visible watermarking, hampir semua perlakuan tidak akan berpengaruh pada keberadaan watermark pada citra, kecuali jika serangan memang sengaja ditujukan untuk menghilangkan watermark. Pengcropan tidak akan berpengaruh selain jika watermark itu sendiri yang dicrop. Sedangkan yang lain seperti kompresi, pemutaran, perubahan ukuran, serta perubahan intensitas hampir tidak berpengaruh sama sekali.

Metode LSB robustnessnya sangat lemah. Metode LSB ini membutuhkan data citra per pixel yang sangat persis, sehingga jika misalnya intensitasnya diubah sedikit saja, maka data pada bit terakhirnya kemungkinan besar akan berubah sehingga watermark pun hilang. Begitu juga dengan rotasi, karena pada dasarnya, ketika gambar dirotasi, tidak semua pikselnya memiliki tempat untuk digambarkan sehingga ada kemungkinan nilainya berubah. Sedangkan untuk kompresi, metode LSB ini juga sangat lemah karena cara kompresi citra pada umumnya tidak menyimpan data setiap piksel secara utuh.

Sedangkan metode adaptif cenderung tahan terhadap serangan, kecuali perubahan intensitas. Hal ini terjadi karena dasar dari penyisipan pada metode adaptif ini adalah perubahan intensitas dan perbandingan intensitas dengan citra asli. Jika intensitasnya diubah, perbandingan intensitas akan menjadi kurang relevan. Untuk serangan yang lainnya, secara umum teknik adaptif sudah cukup baik. Karena disisipkan di beberapa blok, secara umum, metode ini cukup tahan terhadap serangan misalnya kompresi, perubahan ukuran, dan rotasi. Saat dikompresi, secara umum data akan berubah secara berkelompok, sehingga penyisipan data pada satu kelompok piksel citra akan lebih baik daripada hanya pada satu piksel. Semakin besar jumlah piksel dalam satu blok akan semakin baik. Hal tersebut juga berlaku untuk skala dan rotasi.

Selain itu, karena posisi watermark diletakkan secara random, metode ini juga cukup tahan terhadap serangan crop. Jika dicrop, maka yang hilang adalah bagian-bagian tertentu yang letaknya acak sehingga hasil ekstraksi watermark masih bisa dipersepsi dengan mata.

### C. Secure

Secure atau keamanan yang dibutuhkan dari watermarking adalah watermark tidak mudah diambil dan dipindahkan secara sembarangan. Hal ini dimaksudkan

agar tidak terjadi penyalahgunaan watermark yang digunakan pada dokumen lain yang tidak seharusnya.

Misalnya watermark milik suatu perusahaan berhasil didapatkan oleh pihak ketiga. Kemudian pihak ketiga tersebut menggunakan watermark tersebut untuk menandai dokumen yang tidak baik. Jika dokumen tersebut dilaporkan, dan ditemukan watermark milik perusahaan itu, maka perusahaan tersebut dapat dituduh sebagai pemilik dokumen tersebut.

Pada visible watermarking, watermark dapat terlihat dengan jelas. Tentu saja hal tersebut menyebabkan watermark pada teknik ini dapat ditiru dengan mudah oleh pihak ketiga untuk menandai dokumen lain.

Pada watermarking dengan metode LSB, seluruh bit watermark sudah diketahui diletakkan pada bit terakhir di setiap piksel. Karena itu, pihak ketiga juga akan dengan mudah mengambil seluruh bit terakhir dan memindahkannya ke citra yang lain untuk membuat watermark yang sama.

Sedangkan untuk metode adaptif, pengambilan data watermark akan sangat sulit. Pengambilan data watermark pada metode ini membutuhkan perbandingan intensitas dengan citra asli. Jika pihak ketiga tidak memiliki citra aslinya, maka ekstraksi watermark nyaris tidak mungkin dilakukan. Selain itu, posisi watermark juga sudah diacak sehingga pengambilan watermark tanpa informasi mengenai kunci yang digunakan juga akan sulit.

Secara umum, analisis dari ketiga teknik yang dibahas pada ketiga kriteria tersebut dirangkum dalam tabel berikut.

**Tabel 1** perbandingan teknik watermarking

Kriteria	Visible watermarking	LSB	adaptif
Imperceptible	tidak	ya	ya
Robust	ya	tidak	cukup
Secure	tidak	tidak	ya

## V. SIMPULAN

Dari teknik-teknik yang telah dibahas pada makalah ini, dapat diambil kesimpulan sebagai berikut.

1. Setiap teknik watermarking pada domain spasial memiliki kelebihan dan kekurangan masing-masing.
2. Teknik yang paling imperceptible adalah teknik LSB (Least Significant Bit).
3. Teknik yang paling robust adalah dengan visible watermarking.
4. Teknik yang paling secure adalah teknik adaptif.
5. Secara umum, teknik yang paling memenuhi seluruh persyaratan adalah teknik adaptif.

## REFERENSI

Slide kuliah kriptografi, bagian steganografi dan watermarking  
Daniel Setiadikarunia dan Yohanes Danandy, Teknik Adaptive  
Watermarking pada Domain Spasial untuk Penyisipan Label pada  
Citra Digital,  
[http://lemlit.unila.ac.id/file/arsip%202009/SATEK%202008/VERS  
I%20PDF/bidang%205/5-23.pdf](http://lemlit.unila.ac.id/file/arsip%202009/SATEK%202008/VERS<br/>I%20PDF/bidang%205/5-23.pdf)  
Teknologi Watermarking pada Citra Digital,  
[http://www.keepandshare.com/doc/595717/4-steganography-  
teknologi-watermarking-doc-may-26-2008-8-53-am-362k?dn=y](http://www.keepandshare.com/doc/595717/4-steganography-<br/>teknologi-watermarking-doc-may-26-2008-8-53-am-362k?dn=y)  
Watermark, <http://en.wikipedia.org/wiki/Watermark>

## PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya  
tulis ini adalah tulisan saya sendiri, bukan saduran, atau  
terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 23 Maret 2011



Athia Saelan  
13508029