

Reversible Watermarking dengan Metode Modifikasi Histogram pada *Difference Image*

Y. Retno dan A. Harjoko

Abstract— *Reversible watermarking schemes are widely used to maintain the authenticity of the digital image. This research will discuss a method on histogram modification of difference image in which the difference image is created from the difference value of adjacent pixels of the image grayscale.*

Embedding process begins by dividing the host image and watermark into b blocks, followed by making a difference image of the host image block. From the difference image histogram, determine the peak value, and modify the histogram based on the peak value. Then, insert each block of the watermark to the difference image that has been modified and transform back into the grayscale image.

Extraction and recovery process is the inverted version of the embedding stage. This process begins by dividing the watermarked image into b blocks, followed by making a difference image of each block. Then, extract the data and shift difference image histogram using a peak value. That difference image is transformed back into a grayscale image.

Experimental results demonstrate that the average insertion capacity is 14% greater than Xue's with PSNR value over 48 dB for 4×4 pixels and 23 % greater with PSNR over 46 dB for 8×8 pixels. From the comparison of robustness to line and salt n' pepper on the density of 0.05 noises is obtained that the watermark with ECC is more robust than a watermark without ECC. JPEG compression in lossless mode may be applied to the watermarked image. Multiple insertion of watermark can be done with the consequence that the more insertions will result in lower PSNR values.

Keywords—*difference image, histogram modification, reversible watermarking*

1. PENDAHULUAN

Perkembangan teknologi yang pesat mendorong penelitian mengenai *reversible watermarking*, khususnya untuk autentikasi dalam bidang medik dan citra satelit pada penginderaan jauh dalam bidang militer.

Yustina Retno, Staf Pengajar STMIK Sinar Nusantara, Jl. KH. Samanhudi 84-86 Surakarta 57142 (0271-716500, e-mail : yustina_retno@yahoo.com).

Agus Harjoko, Staff Pengajar Jurusan Ilmu Komputer dan Elektronika, FMIPA UGM, Yogyakarta, e-mail : aharjoko@ugm.ac.id

Penggunaan teknik ini dapat memperoleh kembali media asli setelah *watermark* dikeluarkan dari media yang tertanami *watermark* tersebut. Penelitian *reversible watermarking* dengan pergeseran histogram telah dilakukan Ni, dkk [1] yang memilih peak point dan menggeser histogram citra untuk menyisipkan data pada peak point. Ni, dkk [1] menghasilkan nilai PSNR sebesar >48 dB. Penelitian Ni, dkk [1] dikembangkan oleh Fallahpour dan Sendaaghi [2] yang membagi citra menjadi beberapa blok, kemudian metode Ni diterapkan pada setiap blok citra. Penelitian ini menghasilkan nilai PSNR > 47 dB dengan kapasitas lebih besar. Penelitian dengan modifikasi histogram juga dilakukan oleh Lee dan Ho [3]. Lee dan Ho [3] mengemukakan konsep baru yakni modifikasi histogram pada *difference image*. Citra ini dibentuk dari perbedaan nilai piksel kolom ganjil dan genap. Penelitian ini menghasilkan nilai PSNR > 51 dB. Xue dan Lu [4] mengembangkan metode Lee dan Hoo dengan membagi citra menjadi blok dan kemudian menerapkan metode Lee pada setiap blok citra. Citra *ter-watermark* pada penelitian Xue menghasilkan nilai PSNR > 51 dB.

Hal ini mendorong penelitian terhadap *reversible watermarking* dengan modifikasi metode Xue dan Lu [4] sehingga dapat menghasilkan kapasitas penyisipan yang lebih besar, membandingkan nilai PSNR kedua metode, serta menganalisis ketahanan *watermark* (*robustness*) terhadap serangan (*attack*) *noise* garis, *salt and pepper* dan kompresi JPEG.

Adapun batasan masalah dalam penelitian ini adalah:

- Media yang digunakan adalah citra *grayscale* 8 bit.
- Citra *watermark* berupa citra biner dan *grayscale*.
- Kode deteksi kesalahan yang digunakan adalah kode Bose-Chaudhuri Hocquenghem (BCH).
- Serangan (*attack*) yang diujikan untuk mengetahui ketahanan (*robustness*)

watermark berupa *noise* garis, *salt and pepper* dan kompresi JPEG.

2. METODE PENELITIAN

2.1. Citra Digital

Citra merupakan matriks dua dimensi dari fungsi intensitas cahaya. Citra dipresentasikan oleh dua variabel yang menunjukkan posisi pada bidang dengan sebuah fungsi intensitas cahaya sebagai fungsi $f(x,y)$, dimana f adalah nilai amplitudo pada koordinat spasial (x,y) . Karena cahaya merupakan salah satu bentuk energi, maka fungsi $f(x,y)$ merupakan bilangan berhingga yang tidak pernah berharga nol atau negatif seperti pada persamaan

$$0 < f(x, y) < \infty \quad (1)$$

Citra merupakan cahaya yang direfleksikan dari sebuah objek. Fungsi $f(x,y)$ dapat dilihat sebagai fungsi yang memiliki dua unsur. Unsur pertama adalah kekuatan sumber cahaya yang melingkupi pandangan terhadap objek (*illumination*), sedangkan unsur kedua adalah intensitas cahaya yang direfleksikan oleh objek (*reflectance components*). Kedua unsur tersebut masing-masing dapat dituliskan sebagai fungsi $i(x,y)$ dan $r(x,y)$ yang digabungkan sebagai perkalian fungsi untuk membentuk fungsi $f(x,y)$. Sehingga $f(x,y)$ dapat ditulis sebagai :

$$f(x,y) = i(x,y) * r(x,y) \quad (2)$$

di mana $0 < i(x,y) < 1$ dan $0 < r(x,y) < 1$.

Ketika citra digital dapat direpresentasikan sebagai suatu matriks dengan ukuran $M \times N$, maka setiap pasangan indeks baris dan kolom menyatakan suatu titik pada citra. Sedangkan nilai dari elemen matriksnya menyatakan tingkat keabuan atau warna pada titik tersebut. Titik-titik tersebut dinamakan sebagai elemen citra atau *pixel* (*picture element*) [5], sehingga citra digital yang direpresentasikan dalam bentuk matriks $M \times N$ ditulis sebagai berikut:

$$f(x,y) = \begin{bmatrix} f(1,1) & f(1,2) & \dots & f(1,N) \\ f(2,1) & f(2,2) & \dots & f(2,N) \\ \vdots & \vdots & \ddots & \vdots \\ f(M,1) & f(M,2) & \dots & f(M,N) \end{bmatrix}$$

(3)

dimana elemen-elemen matriks atau piksel menunjukkan nilai keabuan atau warna.

2.2 Histogram

Histogram secara umum merupakan sebaran atau distribusi frekuensi. Histogram suatu citra didefinisikan sebagai sebaran nilai derajat keabuan citra [6]. Suatu histogram h dari citra

grayscale dengan derajat keabuan $[0, L-1]$ akan memiliki sebanyak L derajat keabuan. Misalkan terdapat citra *grayscale* 8 bit memiliki $L = 2^8 = 256$. Histogram citra digital dengan derajat keabuan $[0, L - 1]$ adalah suatu fungsi diskrit:

$$h(i) = n_i \quad (4)$$

di mana n_i = jumlah piksel dengan derajat keabuan i dan $h(i)$ = histogram citra digital pada derajat keabuan i .

2.3 Watermarking

Watermarking merupakan salah satu cabang ilmu *steganography*. Sedangkan *steganography* merupakan ilmu yang mempelajari tentang bagaimana menyembunyikan suatu data pada data yang lain. Ada perbedaan antara *steganography* dengan *cryptology*. Perbedaan tersebut terletak pada proses penyembunyian data dan hasil akhir dari proses tersebut. Jika pada kriptografi data asli diacak sedemikian rupa sehingga menghasilkan data terenkripsi yang benar-benar acak dan berbeda dengan data asli, maka pada data *steganography* data disembunyikan pada data lain (*host*) yang akan ditumpanginya dengan menggunakan teknik tertentu sehingga tidak terlihat adanya perbedaan antara *host* sebelum dan sesudah ditumpanginya data.

Watermarking dapat didefinisikan sebagai teknik menyembunyikan data rahasia (*watermark*) ke data *host* yang tidak disadari oleh orang lain [7]. Hal ini dilakukan dengan cara menyembunyikan atau menyisipkan data ke dalam suatu data digital lainnya dengan memanfaatkan kekurangan-kekurangan sistem indera manusia, seperti mata dan telinga, sehingga tidak diketahui kehadirannya oleh manusia dan mampu menghadapi proses-proses pengolahan sinyal digital yang tidak merusak kualitas data yang ter-*watermark* sampai pada tahap tertentu [8] Jadi seolah-olah tidak ada perbedaan antara data *host* sebelum dan sesudah proses *watermarking*.

Beberapa karakteristik *watermarking* adalah [9]:

a. Robustness

Robustness pada *watermarking* diartikan bahwa *watermark* harus tahan terhadap beberapa operasi pemrosesan digital pada umumnya, seperti konversi dari digital ke analog atau sebaliknya, kompresi dan sebagainya.

b. Fidelity

Fidelity merupakan derajat degradasi atau penurunan kualitas data *host* setelah ditumpanginya *watermark* dibandingkan dengan sebelum

ditumpangi *watermark*.

c. *Temper resistance*

Temper resistance adalah ketahanan sistem *watermark* terhadap kemungkinan adanya serangan (*attack*) atau usaha untuk menghilangkan, merubah atau memberikan *watermark* palsu pada data *host*.

Selain karakteristik tersebut, *reversible watermarking* juga memiliki karakteristik tambahan berikut [10]:

1) *Blind*:

Reversible watermark dapat memperoleh kembali citra asli secara langsung dari citra *ter-watermark*. Oleh karena itu *reversible watermark* disebut *blind*, yang berarti proses ekstraksinya tidak membutuhkan citra asli.

2) *Higher Embedding Capacity*:

Ukuran kapasitas informasi yang dapat disisipkan disebut *embedding capacity*. Skema *reversible watermarking*, membutuhkan *embedding capacity* lebih besar daripada skema *watermarking* konvensional.

Beberapa aplikasi digital *watermark* yang pernah dikemukakan dalam tulisan antara lain [9]:

- a. Monitoring Penyiaran
- b. Identifikasi Kepemilikan
- c. Bukti Kepemilikan
- d. Autentikasi
- e. *Fingerprinting*
- f. *Copy Control*
- g. *Covert Communication*

2.4 *Peak signal to noise ratio (PSNR)*

Nilai PSNR digunakan untuk menentukan kualitas citra. Nilai ini diperoleh dengan membandingkan setiap piksel pada citra asli dengan citra yang *ter-watermark*. Semakin besar nilai PSNR mempunyai arti bahwa penanaman *watermark* ke dalam citra *host* tidak mengakibatkan penurunan kualitas citra yang berarti. Sebaliknya jika nilai PSNR semakin kecil maka terjadi penurunan yang berarti pada kualitas citra yang dikarenakan proses penanaman *watermark*. Misalkan citra *host* $w(i,j)$ dan citra *ter-watermark* $w'(i,j)$ berukuran $M_1 \times M_2$ memiliki derajat keabuan [0, 255] dengan nilai intensitas maksimum adalah 255, maka rumus untuk menghitung PSNR adalah sebagai berikut [11]:

$$PSNR = 10 \cdot \log_{10} \left(\frac{MaxI^2}{MSE} \right) \quad (5)$$

di mana *MaxI* adalah nilai intensitas maksimum pada citra dalam hal ini nilainya adalah 255.

Sedangkan nilai MSE didapatkan dengan rumus sebagai berikut:

$$MSE = \frac{1}{M_1 \times M_2} \sum_{i=1}^{M_1} \sum_{j=1}^{M_2} (w(i,j) - w'(i,j))^2 \quad (6)$$

2.5 *Kapasitas*

Fallahpour dan Sedaaghi [2] dalam jurnalnya menyatakan bahwa kapasitas penyembunyian data adalah penjumlahan *peak point* seluruh blok, yang mana banyaknya *peak point* suatu blok mungkin berbeda dengan blok lain. Jika jumlah *peak point* pada blok ke i adalah $h(p_i)$ dan banyaknya data yang disisipkan pada blok ke i adalah $h_i(p)$, maka:

$$h_i(p) \leq h(p_i) \quad (7)$$

Bila terdapat blok citra sejumlah N , maka:

$$\sum_{i=1}^N h_i(p) \leq \sum_{i=1}^N h(p_i) \quad (8)$$

$$h(p) \leq \sum_{i=1}^N h(p_i) \quad (9)$$

2.6 *Kode BCH*

Kode BCH ini dapat diimplementasikan untuk $m \geq 3$ dan $t < 2^{m-1}$ dan memiliki properti sebagai berikut:

Panjang blok yang dikirimkan : $n=2^m-1$

Bit informasi : k

Jumlah *error* maksimal : t

Secara garis besar, prosedur kerja dan metode kode BCH ini dapat dirincikan sebagai berikut [12]:

- a. Proses *Encoding*, proses pembentukan kumpulan *checkbit* yang akan dikirimkan bersama informasi.
- b. Proses *Decoding*, proses pendeteksian *error* dan pengoreksian *error* apabila ditemukan *error* pada bit yang diterima.

2.7 *Analisa*

Reversible watermarking yang diusulkan terdiri atas dua bagian yakni penyisipan dan ekstraksi *recovery*. Sistem yang dikembangkan mengacu pada metode Xue [4] dengan modifikasi pada beberapa bagian yaitu:

1. Pembuatan *difference image*.

Xue dan Lu [4] membentuk *difference image* dari perbedaan derajat keabuan dari kolom berpasangan. Metode yang diusulkan membuat *difference image* dari perbedaan derajat keabuan piksel yang bertetangga (berdekatan), sehingga diharapkan kapasitas citra *ter-watermark* menjadi lebih besar.

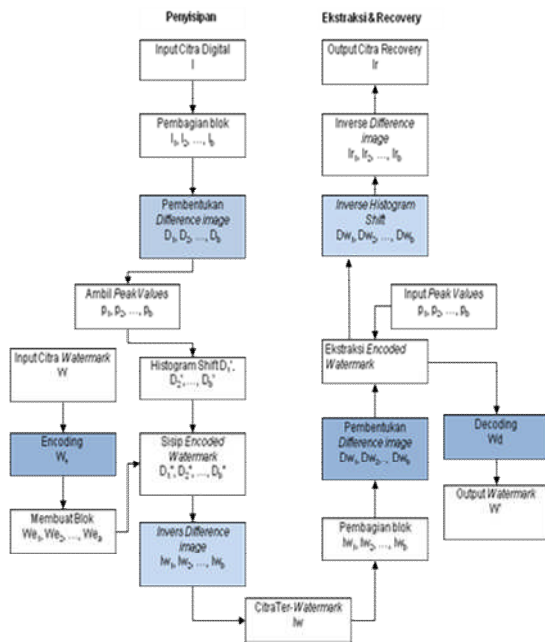
2. *Inverse difference image*

Pembentukannya *difference image* yang berbeda mempengaruhi proses *inverse difference image*.

3. *Encoding dan decoding*.

Metode yang diusulkan juga menambahkan proses *encoding* dan *decoding* pada *watermark*, dengan harapan *watermark* lebih tahan terhadap serangan.

Media penyisipan dalam penelitian ini adalah citra *grayscale* dan citra yang disisipkan adalah citra biner dan *grayscale*. Proses penyisipan dan ekstraksi *recovery* diilustrasikan pada gambar 1.



Gambar 1. Proses penyisipan dan ekstraksi *recovery*

Citra *host* yang digunakan dalam penelitian ini adalah citra *grayscale*, sedangkan *watermark* dapat berupa citra biner ataupun *grayscale*. Langkah-langkah penyisipan *watermark* ke dalam citra *host* melalui tahapan berikut.

2.7.1 *Proses Penyisipan*

Citra *host* yang digunakan dalam penelitian ini adalah citra *grayscale*, sedangkan *watermark* dapat berupa citra biner ataupun *grayscale*. Langkah-langkah penyisipan *watermark* ke dalam citra *host* melalui tahapan berikut.

- Pembagian citra ke blok citra

Citra *host* dibagi menjadi *b* blok, sehingga terdapat citra $I_1, I_2, I_3, \dots, I_b$. Ukuran yang digunakan dalam penelitian ini adalah 4×4 dan 8×8 piksel.

- Pembentukan *difference image*

Difference image dibentuk dari perbedaan derajat keabuan piksel bertetangga. Bila terdapat blok citra I_b berukuran $A \times B$, maka *difference image* $D_b(i,j)$ berukuran $A \times (B-1)$ dibentuk dengan formula berikut:

$$D_b(i,j) = I_b(i,j+1) - I_b(i,j), 1 \leq i \leq A, 1 \leq j \leq B-1 \quad (10)$$

- *Peak value*

Peak value diperoleh dari nilai piksel dengan frekuensi tertinggi pada histogram *difference image*. Bila terdapat blok citra D_1, D_2, \dots, D_b , maka terdapat *peak value* p_1, p_2, \dots, p_b . Karena sebagai acuan atau kunci *watermark*, *peak value* setiap blok disimpan dan dalam penyimpanannya ini diberi tanda positif bila blok tersebut disisip *watermark*, dan negatif bila tidak.

- *Histogram shift*

Bila terdapat blok citra D_b berukuran $A \times B-1$ dan P_b adalah *peak* blok tersebut, maka pergeseran histogram mengikuti aturan berikut:

$$D_b'(i,j) = \begin{cases} D_b(i,j) + 1 & \text{jika } D_b(i,j) > P_b, \\ D_b(i,j) - 1 & \text{jika } D_b(i,j) < -P_b, \\ D_b(i,j) & \text{jika lainnya,} \end{cases} \quad (11)$$

di mana $1 \leq i \leq A, 1 \leq j \leq B-1$.

- *Encoding*

Citra *watermark* di-encode menggunakan kode bch. *Watermark* biner berukuran 30×90 piksel menggunakan BCH(255,91,25) sedangkan *watermark grayscale* 8 bit berukuran 17×15 piksel menggunakan BCH(31,11,5) untuk setiap pikselnya.



a. *Watermark* biner b. *watermark grayscale*

Gambar 2 Citra *watermark* yang digunakan

- *Sisip encoded watermark*

Watermark disisipkan pada *difference image* yang telah dimodifikasi. Jika D_b' adalah *difference image* setelah digeser yang berukuran $A \times B-1$, P_b adalah *peak value* dan W_e adalah data yang disisipkan maka D_b'' dibentuk menggunakan persamaan (12).

$$D_b''(i,j) = \begin{cases} D_b'(i,j) + 1 & \text{jika } D_b(i,j) = P_b, W_e = 1, \\ D_b'(i,j) - 1 & \text{jika } D_b(i,j) = -P_b, W_e = 1, \\ D_b'(i,j) & \text{jika } W_e = 0, \end{cases} \quad (12)$$

untuk $1 \leq i \leq A, 1 \leq j \leq B-1$.

- *Inverse difference image*

Proses ini untuk mengubah *difference image* kembali menjadi citra dengan derajat keabuan dengan mengikuti persamaan (13), di mana I_{w_b} adalah citra ter-*watermark*, I_b adalah citra *host* berukuran $A \times B$, dan D_b'' adalah *difference*

image yang sudah disisip watermark berukuran A x B-1.

$$I_{w_b}(i,j) = \begin{cases} I_b(i,1) & \text{jika } j=1, \\ I_{w_b}(i,j) + D_b''(i,j-1) & \text{jika } j>1. \end{cases} \quad (13)$$

untuk $1 \leq i \leq A, 1 \leq j \leq B$.

2.7.2 Tahap ekstraksi dan recovery

Tahap ini adalah tahap bagaimana pesan yang disisipkan akan diekstrak dan citra ter-watermark di-recovery asli. Langkah-langkah untuk proses ekstraksi dan recovery adalah sebagai berikut.

- Pembagian citra ter-watermark

Citra ter-watermark dibagi menjadi b blok, dengan ukuran yang sama dengan saat penyisipan yakni 4 x 4 piksel atau 8 x 8 piksel.

- Pembentukan difference image citra ter-watermark

Setiap blok citra ter-watermark dibuat difference image. Bila terdapat blok citra I_{w_b} berukuran A x B, maka difference image $Dw_b'(i,j)$ berukuran A x (B-1) dibentuk menggunakan persamaan:

$$Dw_b'(i,j) = I_{w_b}(i,j+1) - I_{w_b}(i,j), \quad 1 \leq i \leq A, 1 \leq j \leq B-1 \quad (14)$$

di mana I_{w_b} = citra ter-watermark blok ke-b dan Dw_b' = difference image dari I_{w_b} .

- Ekstraksi watermark

Peak value yang diperoleh saat penyisipan, digunakan sebagai acuan ekstraksi dan recovery. Bila Dw_b' = difference image berukuran A x B-1, P_b = peak value blok ke-b, dan We_b' = watermark, maka We :

$$We_b'(i,j) = \begin{cases} 0, & \text{jika } Dw_b'(i,j) = P_b \text{ atau } -P_b, \\ 1, & \text{jika } Dw_b'(i,j) = P_b+1 \text{ atau } -(P_b+1), \end{cases} \quad (15)$$

untuk $1 \leq i \leq A$ dan $1 \leq j \leq B-1$.

Kemudian lanjutkan dengan persamaan (16) untuk mengembalikan nilai Dw_b' setelah pesan diperoleh.

$$Dw_b(i,j) = \begin{cases} P_b & \text{jika } Dw_b'(i,j) = P_b+1 \\ -P_b & \text{jika } Dw_b'(i,j) = -(P_b+1) \\ Dw_b'(i,j) & \text{jika lainnya} \end{cases} \quad (16)$$

di mana Dw_b adalah citra setelah proses ekstraksi.

- Decoding

Proses decoding ini akan mengembalikan citra watermark yang ter-encode menjadi watermark dan mengkoreksi bila terdapat noise. Hasil ekstraksi dari semua blok disusun kembali, kemudian dilakukan decoding dengan panjang codeword yang digunakan adalah 255 untuk citra biner dan 31 per piksel untuk grayscale.

- Inverse histogram shift

Proses recovery dimulai dengan melakukan inverse histogram shift pada difference image dengan mengacu pada peak value. Bila Dw_b adalah difference image setelah ekstraksi yang

berukuran A x B-1, P_b adalah peak value blok ke-b, maka diperoleh Dr_b :

$$Dr_b(i,j) = \begin{cases} Dw_b(i,j) - 1 & \text{jika } Dw_b(i,j) > P_b + 1, \\ Dw_b(i,j) + 1 & \text{jika } Dw_b(i,j) < -(P_b + 1), \\ Dw_b(i,j) & \text{jika lainnya,} \end{cases} \quad (17)$$

untuk $1 \leq i \leq A$ dan $1 \leq j \leq B-1$.

- Inverse difference image

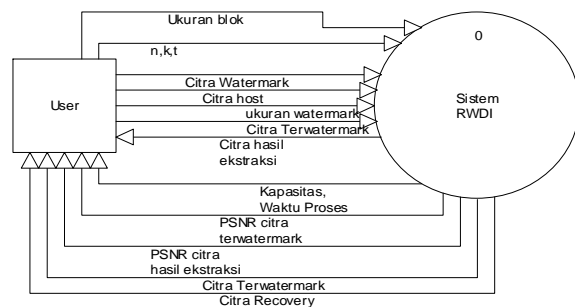
Proses ini merupakan akhir dari recovery citra. Proses yang digunakan untuk mengembalikan difference image ke citra dengan derajat keabuan ini membutuhkan citra ter-watermark I_{w_b} berukuran A x B dan difference image Dr_b berukuran A x B-1 yang telah melalui proses inverse histogram shift. Langkah ini dilakukan dengan mengikuti persamaan berikut:

$$I_r(i,j) = \begin{cases} I_{w_b}(i,1) & \text{jika } j=1, \\ I_r(i,j) + Dr_b(i,j-1) & \text{jika } j>1, \end{cases} \quad (18)$$

untuk $1 \leq i \leq A$ dan $1 \leq j \leq B$.

2.8 Perancangan sistem

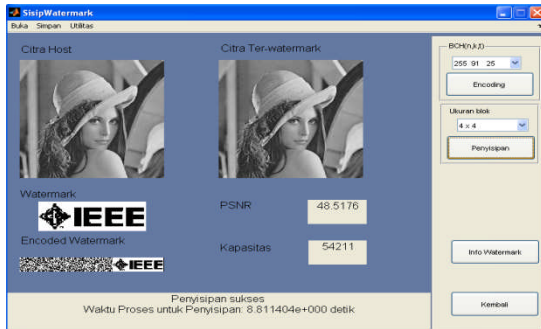
Sistem yang dikembangkan dalam penelitian ini memiliki sejumlah input dan output seperti yang terlihat dalam diagram konteks sistem pada gambar 3. Citra host, citra watermark, ukuran blok, dan encoder merupakan input untuk proses penyisipan. Sedangkan citra ter-watermark, nilai PSNR citra ter-watermark, waktu proses, dan kapasitas penyisipan data merupakan output proses penyisipan ini. Input proses ekstraksi dan recovery berupa citra yang dicurigai ter-watermark, ukuran watermark, dan parameter decoder (n,k,t) yang digunakan. Output yang diharapkan adalah citra watermark hasil ekstraksi, citra hasil recovery, dan PSNR citra hasil ekstraksi.



Gambar 3. Diagram Konteks Sistem

2.9 Implementasi

Reversible watermarking dengan modifikasi histogram difference image ini diimplementasikan menggunakan Matlab2009b. Antarmuka pemakai dibangun menggunakan GUIDE matlab yang terdiri atas antarmuka penyisipan dan ekstraksi recovery.



Gambar 4. Antarmuka penyisipan watermark



Gambar 5. Antarmuka ekstraksi recovery

3. HASIL DAN PEMBAHASAN

Pengujian dilakukan untuk memperoleh kapasitas penyisipan dan kualitas citra serta mengetahui ketahanan citra ter-watermark terhadap noise garis, salt and pepper, dan kompresi JPEG. Penelitian ini menggunakan dua tipe watermark yakni watermark biner dan grayscale. Watermark yang disisipkan berupa encoded watermark (dengan ECC) dan watermark dengan ECC. Citra host berupa citra grayscale berukuran 512 x 512 piksel. Penelitian ini menggunakan 20 citra uji sebagai citra host.

1. Perbandingan kapasitas

Rata-rata kapasitas untuk setiap metode disajikan pada tabel 1.

TABEL 1 PERBANDINGAN KAPASITAS METODE XUE DAN METODE YANG DIUSULKAN

Metode	Kapasitas(bit)	
	4 x 4 piksel	8 x 8 piksel
Xue	45.891	34.796
Yang diusulkan	62.320	56.545
Prosentase Xue vs yang diusulkan	14,7 %	23,1 %

Rata-rata prosentase kapasitas penyisipan yang diperoleh adalah metode yang diusulkan memiliki 14,7 % lebih besar untuk blok berukuran 4 x 4 dan 23 % lebih besar untuk blok berukuran 8 x 8 piksel bila dibandingkan dengan Xue.

2. Perbandingan nilai PSNR

Rata-rata nilai PSNR untuk setiap metode disajikan pada tabel 2.

TABEL 2 PERBANDINGAN NILAI PSNR METODE XUE DAN METODE YANG DIUSULKAN

Metode	Watermark	Nilai PSNR (dB)	
		4 x 4 piksel	8 x 8 piksel
Xue	Biner	51,072	50,806
	tanpa ECC	48,835	46,911
Yang diusulkan	Biner	dengan ECC	48,794
		tanpa ECC	46,92
	Grayscale	tanpa ECC	48,724
		dengan ECC	46,853
		48,739	46,874

Citra ter-watermark dengan watermark biner, untuk blok berukuran 4 x 4 piksel memiliki nilai PSNR > 48 dB sedangkan blok 8 x 8 piksel memiliki PSNR > 46 dB, sedangkan citra dengan watermark grayscale untuk blok 4 x 4 memiliki nilai PSNR > 48 dB dan blok 8 x 8 memiliki nilai PSNR > 46 dB. Berdasarkan tabel di atas diperoleh kualitas citra ter-watermark pada blok berukuran 4 x 4 piksel lebih baik dari blok berukuran 8 x 8 piksel.

3. Pengujian terhadap noise garis

Citra ter-watermark diberi noise garis tidak beraturan yang kemudian dilakukan proses ekstraksi. Rata-rata nilai PSNR citra watermark hasil ekstraksi diperlihatkan pada tabel 3.

TABEL 3 PENGUJIAN TERHADAP NOISE GARIS

Noise garis	Watermark	Nilai PSNR (dB)			
		Blok 4 x 4		Blok 8 x 8	
		Tanpa ECC	ECC	Tanpa ECC	ECC
3 Garis tidak beraturan	Biner	47,450	MSE=0	46,829	MSE=0
	Grayscale	38,723	MSE=0	37,091	MSE=0
12 Garis tidak beraturan	Biner	45,283	MSE=0	44,739	MSE=0
	Grayscale	37,578	MSE=0	35,353	MSE=0

Tabel 3 memperlihatkan bahwa ekstraksi terhadap citra yang disisipi encoded watermark dapat menghasilkan watermark dengan MSE=0, sebaliknya bila tanpa proses encoding akan menghasilkan watermark yang terdistorsi. Berdasarkan hal tersebut disimpulkan bahwa watermark dengan ECC memiliki ketahanan lebih baik terhadap noise garis.

4. Pengujian terhadap noise salt and papper

Ketahanan citra ter-watermark tanpa ECC dan dengan ECC diuji dengan noise salt and pepper. Terdapat empat metode pengujian, yakni:

- Noise ukuran 100 x 100 diletakkan pada bagian kiri atas citra ter-*watermark*, dengan densitas 0,05.
- Diterapkan pada seluruh bagian citra ter-*watermark*, dengan densitas 0,05.
- Diterapkan pada seluruh bagian citra ter-*watermark*, dengan densitas 0,25.
- Diterapkan pada seluruh bagian citra ter-*watermark*, dengan densitas 0,5.

TABEL 4 PENGUJIAN TERHADAP NOISE SALT AND PEPPER

Noise salt 'n pepper	Watermark	Nilai PSNR (dB)			
		Blok 4 x 4		Blok 8x 8	
		Tanpa ECC	ECC	Tanpa ECC	ECC
densitas 0,05, 100 x 100	Biner	45,249	MSE=0	47,463	MSE=0
	Grayscale	35,019	MSE=0	36,842	MSE=0
densitas 0,05	Biner	42,244	MSE=0	42,112	46,580
	Grayscale	32,144	MSE=0	31,836	37,001
densitas 0,25	Biner	38,803	38,879	38,824	38,715
	Grayscale	27,831	28,163	27,881	27,533
densitas 0,5	Biner	37,714	37,668	37,687	37,5474
	Grayscale	26,243	25,557	26,134	25,4977

Tabel 4 memperlihatkan bahwa nilai PSNR *watermark* pada densitas 0,25 dan 0,5 adalah rendah, sedangkan pada densitas 0,05 memiliki nilai PSNR yang tinggi bahkan MSE=0. Nilai MSE=0 berarti tidak ada perbedaan nilai piksel antara *watermark* hasil ekstraksi dengan sebelum penyisipan. Berdasarkan hasil pengujian ini dapat disimpulkan *Watermark* dengan ECC memiliki ketahanan lebih baik terhadap *noise salt and pepper* pada densitas 0,05.

5. Pengujian terhadap kompresi JPEG

Kompresi JPEG diujikan baik pada citra ter-*watermark* yang disisipkan tanpa ECC maupun berupa *encoded watermark*. Kompresi yang digunakan adalah kompresi dengan mode *lossless* dan *lossy*. Pengujian dan hasil ekstraksi *watermark* disajikan pada tabel 5.

TABEL 5 PENGUJIAN TERHADAP KOMPRESI JPEG

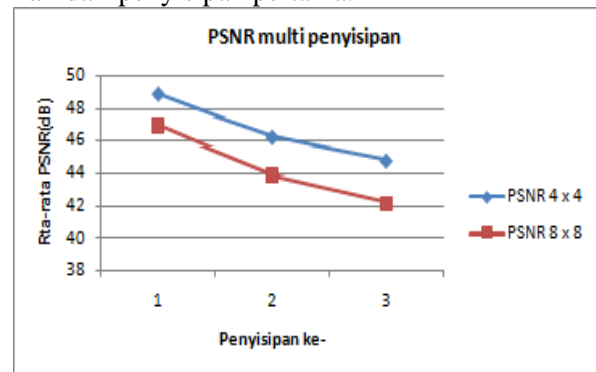
Mode Kompresi	Watermark	Nilai PSNR(dB)			
		Blok 4 x 4		Blok 8x 8	
		Tanpa ECC	ECC	Tanpa ECC	ECC
Lossless	Biner	MSE=0	MSE=0	MSE=0	MSE=0
	Grayscale	MSE=0	MSE=0	MSE=0	MSE=0
Lossy 100%	Biner	40,158	40,233	39,946	39,91
	Grayscale	30,268	32,128	30,031	42,579
Lossy 95 %	Biner	37,583	37,570	37,668	37,652
	Grayscale	27,150	27,273	27,441	27,401

Data pada tabel diatas memperlihatkan bahwa *watermark* tidak tahan terhadap kompresi JPEG

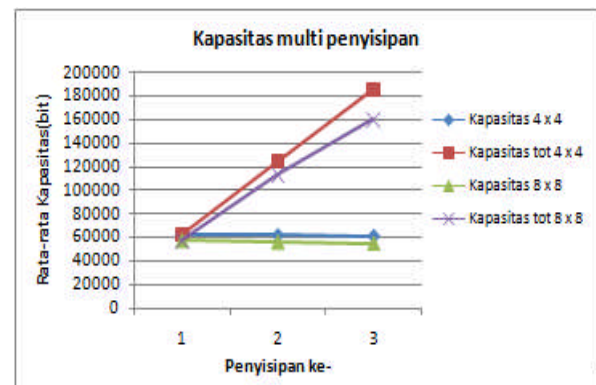
pada mode *lossy*, namun tetap dimungkinkan pada mode *lossless*.

6. Multi penyisipan

Sistem yang dikembangkan dirancang untuk dapat menyisipkan *watermark* sebanyak tiga kali. Gambar 6 memperlihatkan bahwa rata-rata nilai PSNR penyisipan ke-2 lebih rendah dari penyisipan pertama, dan rata-rata nilai PSNR penyisipan ke-3 lebih rendah dari penyisipan ke-2. Gambar 7 memperlihatkan bahwa kapasitas penyisipan pada penyisipan 1, 2, dan 3 adalah hampir sama, sehingga bila dihitung kapasitas total untuk tiga kali penyisipan adalah hampir 3 kali dari penyisipan pertama.



Gambar 6. Rata-rata PSNR multi penyisipan



Gambar 7. Rata-rata kapasitas multi penyisipan

Berdasarkan gambar 6 dan 7 diatas diperoleh bahwa semakin banyak penyisipan, maka nilai PSNR akan rendah namun kapasitas total yang diperoleh akan lebih besar.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, dapat ditarik beberapa kesimpulan yaitu:

- Kapasitas penyisipan metode yang diusulkan lebih besar dari metode Xue. Rata-rata prosentase kapasitas penyisipan yang diperoleh adalah 14,7 % lebih besar untuk blok berukuran 4 x 4 dan 23 % lebih

besar untuk blok berukuran 8 x 8 piksel bila dibandingkan dengan Xue.

- Kualitas citra ter-*watermark* pada blok berukuran 4 x 4 piksel lebih baik dari blok berukuran 8 x 8 piksel. Citra ter-*watermark* dengan *watermark* biner, untuk blok berukuran 4 x 4 piksel memiliki nilai PSNR > 48 dB sedangkan blok 8 x 8 piksel memiliki PSNR >46 dB, sedangkan citra dengan *watermark grayscale* untuk blok 4 x 4 memiliki nilai PSNR > 48 dB dan blok 8 x 8 memiliki nilai PSNR > 46 dB.
- *Watermark* dengan ECC memiliki ketahanan lebih baik terhadap *noise* garis. Berdasarkan pengujian terhadap *noise* garis, ekstraksi terhadap citra yang disisipi *encoded watermark* dapat menghasilkan *watermark* dengan MSE=0, sebaliknya bila tanpa proses *encoding* akan menghasilkan *watermark* yang terdistorsi.
- *Watermark* dengan ECC memiliki ketahanan lebih baik terhadap *noise salt and pepper* pada densitas 0,05.
- *Watermark* tidak tahan terhadap kompresi JPEG pada mode *lossy*, namun tetap dimungkinkan pada mode *lossless*.
- Kode BCH dapat digunakan untuk menambah ketahanan *watermark* terutama untuk *noise* garis dan *salt and pepper*.
- Semakin banyak penyisipan, maka nilai PSNR akan rendah namun kapasitas total yang diperoleh akan lebih besar.

5. SARAN

Saran untuk pengembangan penelitian lanjutan adalah:

1. Penggunaan kode bch pada penelitian ini mampu mendeteksi *error* yang ada dengan menambahkan *parity* bit dalam jumlah besar ke dalam *watermark*. Sebagai contoh untuk ukuran 30 x 90 piksel citra biner (2700 bit), bila di-*decode* dengan bch(255,91,25), *encoded watermark* berukuran 7650 bit. *Parity* untuk *watermark* diatas adalah 4950 bit dengan maksimal *error* yang terkoreksi 2250 bit (25 bit per baris). Diperlukan penelitian lebih lanjut untuk penggunaan *encoder* yang dapat menghemat bit namun memiliki kemampuan untuk mengkoreksi *watermark* dengan lebih baik.
2. Penyisipan *watermark* masih terbatas pada citra *grayscale* 8 bit dan citra berwarna 24 bit pada satu layer saja

(warna merah). Penelitian dapat dikembangkan untuk penyisipan pada citra berwarna 24 bit dan 16 bit.

3. Penyisipan multi *watermark* masih terbatas untuk tiga kali penyisipan. Penelitian dapat dikembangkan untuk menganalisis penyisipan lebih dari 3 kali.
4. *Watermark grayscale* yang digunakan masih berukuran kecil. Hal ini karena konversi *grayscale* ke biner memerlukan waktu yang lama. Oleh karena itu, diperlukan penelitian lanjutan sehingga citra *grayscale* berukuran besar dapat disisipkan ke dalam citra *host* dalam waktu yang relatif lebih cepat.

DAFTAR PUSTAKA

- [1] Ni, Z., Shi, Y. Q., dan Su, W., 2006, "Reversible Data Hiding", *IEEE Transactions on Circuits and Systems for Video Technology*, 16, 3, 354-362.
- [2] Fallahpour, M dan Sedaaghi, M. H, 2007, "High Capacity Lossless Data Hiding Based on Histogram Modification", *IETICE Electronics Express*, 4, 7, 205-210
- [3] Lee, S., Suh, Y., and Ho, Y., 2006, "Reversible image authentication based on watermarking", *IEEE Proc. Of ICME*, Juli, 1321-1324.
- [4] Xue, D. W., dan Lu, Z. M., 2008, "Difference image Watermarking Based Reversible Image Authentication with Tampering Localization Capability", *IJCSES International Journal of Computer Sciences and Engineering Systems*, 2, 3, 213-218.
- [5] Gonzalez, R.C. dan Woods, R. E., 2008, *Digital Image Processing*, Ed. 3, Prentice Hall
- [6] Burger, W. dan Burge, M., 2009, *Principles of digital image processing: fundamental techniques*, Springer Verlag London.
- [7] Munir, R., 2004, *Pengolahan Citra Digital dengan Pendekatan Algoritmik*, Informatika, Bandung.
- [8] Suhail, A. M., 2005, *Digital Watermarking for Protection of Intellectual Property*, *Multimedia security: steganography and digital watermarking Techniques for protection of intellectual property*, Idea Group Inc.
- [9] Wibawa, H.A, 2008, Autentikasi citra digital menggunakan transformasi integer, *Tesis*, Program Studi S2 Ilmu Komputer, Universitas Gadjah Mada
- [10] Feng, J-B, Lin, I-C, dan Tsai, C-S dan Chu Y-P, 2006, "Reversible Watermarking: Current Status and key issue", *International Journal of Network Security*, 2, 3, 161-171.
- [11] Mery, D. dan Rueda, L., 2007, *Advances in image and video technology*, Springer-Verlag Berlin Heidelberg, Germany.
- [12] Susanto. E., 2010, "Analisis Kinerja Kode BCH", *Tugas Akhir*, Departemen Teknik Elektro, Universitas Sumatera Utara.