# IMPLEMENTASI PENGAMANAN CITRA DIGITAL BERBASIS ENKRIPSI 2D LOGISTIC MAP DAN DNA ENCODING DENGAN PENYISIPAN LSB DAN DWT

**Deddy Rudhistiar**
Program Studi Teknik Informatika S1, Fakultas Teknologi Industri, Institut Teknologi Nasional Malang
JL. Raya Karanglo KM. 2, Tasikmadu, Kec. Lowokwaru, Kota Malang, Jawa Timur 65153
*rudhistiar@lecturer.itn.ac.id*

**ABSTRAK**

Pertukaran data yang sangat mudah di internet menyebabkan data menjadi rentan terhadap modifikasi dan pelanggaran hak cipta. Salah satu teknik untuk pengamanan data digital, termasuk data citra, dari hal-hal tersebut adalah pengaplikasian *watermarking* berbasis enkripsi. Dalam penelitian ini, dilakukan teknik *watermarking* berbasis enkripsi 2D *Logistic Map* dan DNA *Encoding*. Penggabungan DNA *Encoding* terhadap 2D *Logistic Map* diharapkan meningkatkan keamanan terhadap citra watermark. Penelitian ini membandingkan kinerja teknik *watermarking* LSB *(Least Significant Bit*), yang termasuk salah satu *spatial domain watermark*, dan DWT (*Discrete Wavelet Transform*), yang merupakan salah satu frequency domain watermark yang berbasis enkripsi 2D *Logistic Map* dan DNA *Encoding*. Dalam hal ini, teknik *watermarking* akan dibandingkan berdasarkan nilai MSE (*Mean Squared Error*), NC (*Normalized Cross-Correlation*), PSNR (*Peak Signal to Noise Ratio*), dan waktu pemrosesan. Hasil penelitian menunjukkan nilai rata-rata MSE pada teknik *watermarking* LSB sebesar 0.1445 sedangkan teknik *watermarking* DWT adalah nol. Nilai rata-rata PSNR pada teknik *watermarking* LSB sebesar 51.26 db sedangkan teknik *watermarking* DWT sebesar 44.59db. Nilai rata-rata NC pada teknik *watermarking* LSB dan teknik *watermarking* DWT masing-masing bernilai 1. Dan waktu proses yang dibutuhkan pada teknik *watermarking* LSB jauh lebih besar daripada teknik *watermarking* DWT.

**Keyword :** *Watermarking, LSB, DWT, Enkripsi, 2D Logistic map, DNA Encoding*

## 1. PENDAHULUAN

Pada masa sekarang, pertukaran data melalui internet sudah menjadi kebutuhan sehari-hari dengan maraknya penggunaan media sosial di masyarakat. Salah satu tipe data yang banyak digunakan dan sekaligus disimpan adalah citra digital. Data digital memberikan berbagai keuntungan, antara lain memudahkan dalam penggandaan tanpa kehilangan kualitas secara signifikan, juga memudahkan penyimpanannya untuk digunakan lagi. Kemudahan inilah yang banyak dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab sehingga pihak-pihak tersebut dengan seenaknya menggandakan gambar-gambar tanpa memperhatikan hak cipta dan memodifikasikannya. Bahkan bisa saja gambar-gambar tersebut diakui sebagai gambar sendiri. Oleh karena itu, dibutuhkan metode untuk melindungi hak cipta untuk suatu produk data digital.

*Watermarking* adalah salah satu teknik yang dapat digunakan dalam mengamankan suatu hak cipta dari data digital. *Watermarking* merupakan proses penamaan data atau pemberian label ke dalam suatu data digital. Data digital bisa berupa teks, audio, citra dan video. *Watermarking* citra digital dapat dikategorikan menurut domain pemrosesan menjadi dua kelas: domain spasial dan domain frekuensi. Dalam domain spasial, gambar diperlakukan langsung dengan mengubah pikselnya. Contoh metode *watermarking* dalam domain spasial adalah LSB (*Least Significant Bit*). Dalam domain frekuensi, *watermarking* disisipkan oleh perubahan pita frekuensi. Contoh metode *watermarking* dalam domain frekuensi adalah DWT (*Discrete Wavelet Transform*). Domain frekuensi lebih akurat daripada domain spasial karena menganalisis gambar untuk menurunkan koefisien.

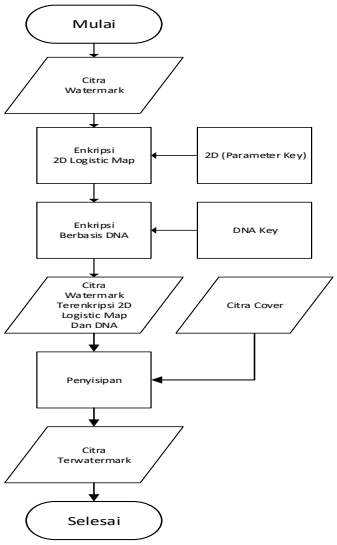
Metode yang dapat dilakukan untuk memodifikasi nilai piksel sebelum ditanamkan ke suatu objek citra adalah dengan mengenkripsinya terlebih dahulu. Sejumlah teknik *watermarking* dengan kombinasi enkripsi ditawarkan demi mengamankan data digital. Salah satu yang paling popular adalah mengkombinasikan *watermarking* dengan enkripsi berbasis *chaotic map*. Enkripsi berbasis *Chaotic map* mulai dikombinasi dengan algoritme lain seperti DNA *Encoding*. DNA *Encoding* adalah bidang penelitian baru yang dikembangkan sebagai kombinasi bidang ilmu komputer dan biologi molekular. DNA *Encoding* memiliki kemampuan komputasi paralel yang kuat. Pengimplementasian DNA *Encoding* pada enkripsi berbasis *Chaotic map (Tent Map)* terbukti meningkatkan keamanan dari serangan berupa *statistical* dan *differential attack*. Oleh karena itu, DNA *Encoding* merupakan salah satu algoritma yang mulai banyak diminati untuk dijadikan alternatif untuk dikombinasikan dengan algoritma enkripsi citra digital, termasuk enkripsi citra *watermark*.

## 2. TINJAUAN PUSTAKA

### 2.1 Teknik Watermarking

Teknik *watermarking* secara umum dibagi menjadi dua bagian inti, yaitu : *Spatial Domain Watermark* dan *Transform Domain Watermark*.

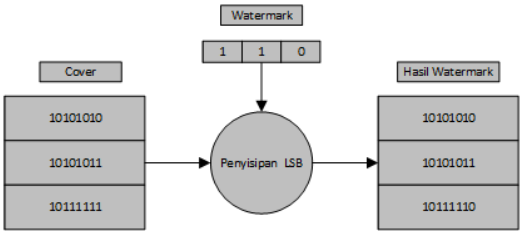
Dalam teknik *domain spasial*, nilai-nilai piksel dari citra *cover* akan diubah secara langsung dengan menanamkan bit *watermark*. Teknik dengan domain spasial tidak bisa menolak pemrosesan citra atau serangan geometris lainnya. Beberapa metode/ teknik dalam domain spasial adalah *Least Significant Bit* (LSB). Selanjutnya dalam teknik Transform Domain *Watermark*, citra *cover* akan ditransformasikan ke beberapa rentang frekunesi tertentu dan kemudian *watermark* akan disematkan ke koefisien dari citra yang ditransformasikan. Untuk mengambil sinyal asli, transformasi inversi dari koefisien yang dimodifikasi perlu diambil. Menanamkan *watermark* di domain yang ditransformasikan terbukti lebih kuat terhadap serangan seperti kompresi JPEG. Terdapat banyak teknik *watermarking* domain transformasi salah satunya *Discrete Wavelet Transform* (DWT). Metode ini memberikan persepsi yang lebih tinggi dan lebih kuat untuk manipulasi citra dan serangan pemrosesan sinyal umum, tetapi biaya perhitungannya lebih tinggi daripada metode *watermarking* domain spasial. *Discrete Wavelet Transform* (DWT) memiliki keunggulan seperti kecepatan komputasi untuk *watermarking*, tetapi teknik ini tidak dapat memciptakan keseimbangan antara inversibilitas dan ketahanan secara otomatis dalam *watermarking*. Artinya, Hasil ekstraksi watermark cenderung tidak sempurna ketika intensitas penyisipannya diturunkan. (Sutojo dkk., 2017).




Gambar 1. Skema proses penyisipan citra *watermark* terenkripsi

## 2.2 Least Significant Bit (LSB)

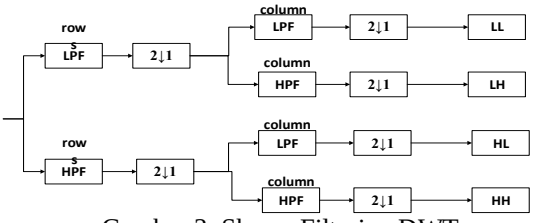
*Least Significant Bit* atau yang selanjutnya disebut LSB adalah metode pada steganografi yang mengambil bit yang paling tidak signifikan atau yang tidak mempunyai pengaruh besar pada sebuah data (Joshi & Avinash Karkade, 2015). LSB semula lebih banyak digunakan pada data gambar, tetapi kemudian berkembang ke data suara. Penyembunyian data dengan metode LSB dilakukan dengan melakukan penempelan bit yang menimbulkan distorsi yang minimal pada sinyal yang ditempeli. Selanjutnya dibuat tahap-tahap implementasi proses sehingga tercapai tujuan yang diharapkan. Tahap ini dibagi menjadi dua bagian yaitu tahap penyisipan informasi dan tahap pengambilan informasi atau ekstraksi. Tahap penyisipan dilakukan dengan me-*replace* bagian LSB dari *cover* dengan bit dari *watermark*-nya. Gambar 2 menunjukkan penyisipan citra *watermark* ke citra *cover*.




Gambar 2. Penyisipan LSB

## 2.3 TRANSFORMASI WAVELET DISKRIT (DWT)

Secara umum Transformasi Wavelet Diskrit adalah proses dekomposisi citra yang berdasarkan nilai frekuensi dari subband citra tersebut. Komponen subband transformasi wavelet didapatkan melalui proses penurunan dari level dekomposisi suatu citra. Implementasi Transformasi Wavelet Diskrit memanfaatkan *lowpass filter* dan *highpass filter* dengan cara melewatkan sinyal dan melakukan *downsampling* pada keluaran tiap level *filter* pada tahap dekomposisi. *Highpass filter* tentunya dapat menentukan frekuensin tersebut jika bernilai tinggi dan *lowpass filter* juga digunakan juga dalam mengenali frekuensi rendah (Sutojo dkk, 2017). Pada gambar 3 merupakan skema *filtering* pada DWT.




Gambar 3. Skema Filtering DWT

LL, LH, HL dan HH merupakan hasil dekomposisi. Proses transformasi dimulai dengan membagi citra menjadi blok. Nilai a, b, c dan d adalah nilai piksel dari citra yang di dekomposisi.

## 2.4 2D Logistic Map

Teori acak ataupun yang biasanya disebut juga dengan teori *chaos* adalah salah satu metode yang sudah lama ada, Henri Poincare termasuk seorang penggagas sekaligus penemu teori *chaos*. Henri Poincare menemukan bahwa terdapat orbit yang bersifat non-periodik, yang bisa diartikan tidak memiliki proses kemunculan yang formulatif atau

yang dimaksud disini adalah proses kemunculan secara tetap pada tahun 1880. Pada pertengahan abad ke-20 teori *chaos* mulai diformulasikan oleh beberapa orang dijaman tersebut, dengan seseorang yang mulai merintis yang bernama Edward Lorenz. Edward Lorenz mendapati adanya permasalahan teori *chaos* dalam menentukan peramalan cuaca disekitar tahun 1961. Lorenz mencoba suatu simulasi peramalan cuaca dengan menggunakan mesin yang telah ia buat. Lalu Lorenz mendapati tentang prediksi yang telah dibuat dengan bantuan mesin, kemudian didapatkan hasil berbeda dengan kenyataan disekitarnya. Inilah yang mendasari perkembangan teori *chaos* yang telah ada sebelumnya. Setelahnya mulai banyak ahli yang mulai mempelajari teori *chaos* dan melakukan penerapan di bidang-bidang tertentu, mulai dari dunia meteorologi, biologi, matematika, sampai dunia keamanan yang disebut dengan kriptografi(Çavuşoğlu et al., 2017).

Persamaan chaos digunakan untuk membangkitkan aliran kunci (*key stream*) bilangan acak yang digunakan untuk me-*mask* nilai-nilai piksel *plain image*, dengan cara mengiterasi persamaan *chaos* berdasarkan nilai awal yang diberikan. Keuntungan dari persamaan *chaos* adalah kita dapat membangkitkan bilangan yang acak secara terus menerus. Bilangan yang dibangkitkan ini tanpa pola yang akan berulang walaupun kita telah melakukan proses berkali-kali(Ramalingam et al., 2017) .

*Logistic map 2D* merupakan salah satu fungsi *chaos* yang memiliki perilaku yang sangat kompleks. Nilai parameter awal yang digunakan terbukti mampu menghasilkan nilai acak. Enkripsi menggunakan transposisi dan difusi logistik 2D mampu menahan serangan kriptografi dan teknik cryptalysis yang ada. Seperti serangan statistik dan serangan diferensial. (Wu Yue dkk,2012)

*Logistic map 2D* secara diskrit didefinisikan pada persamaan dibawah ini

$$2D\ logistic\ map: \begin{cases} x_{i+1} = r\,(3y_i + 1)x_i(1 - x_i) \\ y_{i+1} = r(3x_{i+1} + 1)y_i(1 - y_i) \end{cases} \quad (1)$$

dengan

$x_i, y_i$ : Bilangan real di antara 0 dan 1 yang disebut juga sebagai nilai *chaos* dengan ($0 \leq x_i \leq 1$ dan $0 \leq y_i \leq 1$)

$r$ : Bilangan positif yang merepresentasikan laju pertumbuhan ($0 \leq r \leq 4$).

Pemilihan nilai $r$ sangat mempengaruhi dinamika sistem yang berdampak pada kondisi acak sempurna pada sistem. Ketika r meningkat maka sifat non-linier sistem juga naik.

### 2.5 DNA Encoding

*Deoxyribonucleic Acid* (*DNA)* adalah suatu entitas yang menyimpan informasi dari semua jenis makhluk hidup. Terdapat empat *nucleic acid* yaitu A (*Adenine*), C (*Cytosine*), G (*Guanine*) dan T (*Thymine*) yang digunakan pada DNA *sequence*(Akhavan et al., 2017). Dalam *DNA sequence*, A merupakan komplemen dari T dan C merupakan komplemen dari G (Jain, 2016). Keempat *nucleic acid* ini dapat direpresentasikan dalam bilangan biner, dengan aturan-aturan seperti pada Tabel 1.

Tabel 1. Aturan DNA *Encoding*

| *Rule* / *NA* | *1* | *2* | *3* | *4* | *5* | *6* | *7* | *8* |
|---|---|---|---|---|---|---|---|---|
| A | 00 | 00 | 11 | 11 | 10 | 01 | 10 | 01 |
| T | 11 | 11 | 00 | 00 | 01 | 10 | 01 | 10 |
| C | 10 | 01 | 10 | 01 | 00 | 00 | 11 | 11 |
| G | 01 | 10 | 01 | 10 | 11 | 11 | 00 | 00 |

Tabel 1 merupakan aturan-aturan dari DNA *Encoding*, mulai dari rule 1 sampai dengan rule 8. Aturan dari setiap *nucleic acid* dikonversikan ke dalam bentuk bit yang terdiri dari angka 0 dan 1.

## 3. METODE PENELITIAN

### 3.1 Tahapan Penelitian

Diproses tahapan penelitian dilakukan dengan melaksanakan langkah-langkah yang ada dibawah ini sebagai berikut:

1. Studi Literatur
   Diproses awal dalam melakukan sebuah penelitian, dilaksanakan pengumpulan data dari buku, artikel, jurnal, dan karya ilmiah maupun situs internet mengenai pengolahan citra digital, teknik *watermarking*, teori *chaos* dan DNA *Encoding*.
2. Perancangan Algoritma
   Setelah studi literatur, tahapan selanjutnya adalah merancang algoritma yang diusulkan dan parameter pengujiannya.
3. Implementasi
   Selanjutnya dilakukan proses pembuatan perangkat lunak yang telah disesuaikan, berdasarkan hasil analisa dan perancangan algoritme yang tentunya telah ditetapkan sebelumnya. Perangkat lunak akan dibuat dengan menggunakan bahasa pemrograman MATLAB.
4. Pengujian
   Pada tahap ini dilakukan pengujian skema *watermarking* yang diusulkan, dengan tujuan mengetahui hasil penelitian yang telah dilaksanakan telah sesuai dengan tujuan dari penelitian tersebut dan menjawab rumusan masalah pada penelitian ini. Oleh karena itu, untuk setiap citra yang dipilih, diuji dengan masing-masing skema yang diusulkan.

## 4. HASIL DAN PEMBAHASAN

### 4.1 Hasil Pengujian MSE

Nilai MSE adalah nilai parameter yang dapat digunakan untuk mengetahui error antara citra asli dibandingkan citra hasil penyisipan. Jika nilai MSE yang didaptkan cukup tinggi maka menunjukan terjadinya penurunan kualitas atau telah terjadi perubahan yang cukup besar pada citra yang telah disisipi *watermark*. Tabel 2 menunjukan hasil penghitungan nilai MSE untuk masing-masing teknik yang diuji. Rata-rata nilai MSE untuk algotime DWT adalah 0, sedangkan rata-rata nilai MSE untuk teknik LSB adalah 0.1438. Jika ditinjau dari nilai MSE maka dapat diketahui bahwa teknik DWT memberikan hasil penyisipan yang lebih baik dari LSB.

Tabel 2. Hasil Nilai MSE

| Citra Cover | | Citra Watermark Terenkripsi | | Penyisipan | |
|---|---|---|---|---|---|
| | | | | LSB | DWT |
| Nama Citra | Ukuran | Nama Citra | Ukuran | MSE | MSE |
| cover1024gunung.png | 1024 x 1024 | hasilenkripsi64.bmp | 64 x 64 | 0.16383 | 0 |
| cover1024sepeda.png | 1024 x 1024 | hasilenkripsi256.bmp | 256 x 256 | 0.10761 | 0 |

Tabel 2 merupakan hasil nilai dari pengujian MSE dari penyisipan LSB dan DWT. Berdasarkan Tabel 2 terlihat pula variasi dari nilai MSE untuk teknik LSB. Nilai MSE terbesar yaitu 0,16383 diperoleh ketika menyisipkan citra lenna berukuran 64×64 piksel ke dalam *cover* berukuran 1024 × 1024 piksel. Sedangkan Nilai MSE terkecil yaitu 0,10761 diperoleh ketika menyisipkan citra lenna berukuran 256 × 256 piksel kedalam citra *cover* berukuran 1024 × 1024 piksel. Untuk teknik LSB terlihat bahwa semakin besar ukuran pesan yang disisipkan maka semakin kecil nilai MSE yang diperoleh. Hal ini dibuktikan dengan ketika ukuran citra *watermark* divariasikan maka nilai MSE cenderung mengecil. Namun hal ini tidak terlihat untuk teknik DWT.

### 4.2 Hasil Pengujian PSNR

*Peak Signal to Noise Ratio* (PSNR) adalah nilai yang digunakan untuk membandingkan hasil nilai citra *cover* awal dengan nilai suatu citra *cover* yang telah tersisipakan citra *watermark*. Tentunya jika semakin tinggi nilai PSNR dari suatu citra yang telah disisipkan, maka tingkat kemiripan antara citra *cover* dengan citra yang telah dimanipulasi semakin baik. Nilai PSNR bisa didapatkan dengan menghitung terlebih dahulu nilai *Mean Square Error* (MSE) dari kedua citra yang dibandingkan.

Tabel 3. Hasil nilai PSNR

| Citra Cover | | Citra Watermark Terenkripsi | | Penyisipan | |
|---|---|---|---|---|---|
| | | | | LSB | DWT |
| Nama Citra | Ukuran | Nama Citra | Ukuran | PSNR | PSNR |
| airplane512.bmp | 512 x 512 | hasilenkripsi64.bmp | 64 x 64 | 51.1739 | 42.7952 |
| pepper512.bmp | 512 x 512 | hasilenkripsi64.bmp | 64 x 64 | 51.1739 | 45.6254 |
| cover1024pantai.png | 1024x1024 | hasilenkripsi128.bmp | 128 x128 | 51.0638 | 44.627 |
| cover1024sepeda.png | 1024x1024 | hasilenkripsi64.bmp | 64 x 64 | 51.8627 | 44.2998 |

Tabel 3 merupakan hasil nilai dari pengujian PSNR pada penyisipan citra *watermark* terenkripsi ke dalam citra *cover* menggunakan teknik *watermarking* LSB dan DWT. Berdasarkan Tabel 3 terlihat bahwa rata-rata nilai PSNR pada teknik *watermarking* LSB sebesar 51.26 dB sedangkan teknik *watermarking* DWT sebesar 44.59 dB. Hal ini menunjukan teknik LSB cenderung memberikan hasil yang cenderung lebih baik dari teknik DWT. Hal ini terlihat dari selesih rata-rata nilai PSNR sebesar 6,67 dB. Sebaran nilai PSNR untuk teknik LSB berada pada minimum 51,0638 dB dan maksimum 51,8627 dB. Sedangkan untuk teknik DWT ada diantara 42,7952 dB – 45,6254 dB. Berdasarkan penelitian tersebut tidak terlihat adanya pengaruh ukuran citra terhadap nilai PSNR

### 4.3 Hasil Pengujian NC

Nilai Normalized Cross-Correlation (NC) yang terdapat pada tabel 4 digunakan untuk menguji seberapa baik hasil ekstraksi citra *watermark* jika dibandingkan dengan citra w*atermark* yang asli. Nilai NC yang sempurna adalah satu, sehingga nilai NC yang mendekati satu maka hasil ekstraksi citra *watermark* semakin mirip dengan citra *watermark* asli.

Tabel 4. Hasil Nilai NC

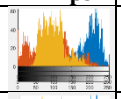
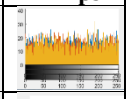
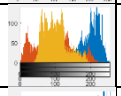
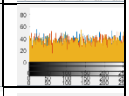
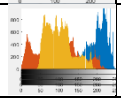
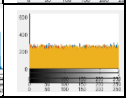
| Citra watermark | Citra watermark Terenkripsi | Ekstraksi LSB | Ekstraksi DWT | Dekripsi Ekstraksi LSB | Dekripsi Ekstraksi LSB |
|---|---|---|---|---|---|
| | | NC | NC | NC | NC |
| lenna64.bmp | hasilenkripsi64.bmp | 1 | 1 | 1 | 1 |
| lenna96.bmp | hasilenkripsi96.bmp | 1 | 1 | 1 | 1 |
| lenna128.bmp | hasilenkripsi128.bmp | 1 | 1 | 1 | 1 |
| lenna256.bmp | hasilenkripsi256.bmp | 1 | 1 | 1 | 1 |

Tabel 4 menunjukan nilai NC yang diperoleh untuk masing-masing citra yang diproses. Terlihat bahwa semua citra memberikan hasil NC sebesar 1. Hal ini menunjukan bahwa proses penyisipan dan ekstraksi pada teknik yang diusulkan tidak membuat kerusakan pada citra *watermark* yang diekstrak. Proses tanpa gangguan atau serangan apapun meciptakan kondisi yang lossless

### 4.4 Hasil Pengujian Parameter Enkripsi

Tabel 5 merupakan hasil dari pengujian entropi untuk citra lenna yang berukuran 64x64, 96x96 dan 256x256. Ditunjukkan dengan nilai entropi dan gambar histogram citra *watermark* sebelum dan setelah di enkripsi.

Tabel 5. Hasil Pengujian Enkripsi

| Citra Watermark Awal | Ukuran | Entropi | Histogram | |
|---|---|---|---|---|
| | | | Citra Watermark Sebelum Enkripsi | Citra Watermark Setelah Enkripsi |
| lenna64.bmp | 64 x 64 | 7.9604 |  |  |
| lenna96.bmp | 96 x 96 | 7.9803 |  |  |
| lenna256.bmp | 256 x 256 | 7.9973 |  |  |

Berdasarkan Tabel 5 diperoleh bahwa nilai entropy rata-rata sebesar 7.9793. Hal ini menunjukan bahwa sebaran nilai piksel sangat teracak sempurna dan merata. Persebaran piksel yang merata juga ditunjukan oleh histogram masing-masing citra. Citra asli yang memiliki nilai piksel yang berkumpul pada beberapa titik tertentu telah disebar cukup merata.

### 4.5 Hasil Pengujian Waktu Proses

Tabel 6 merupakan hasil pengujian waktu proses dari proses penyisipan LSB dan DWT serta terdapat juga waktu proses ekstraksi pada LSB dan DWT.

Tabel 6. Hasil Pengujian Waktu Proses

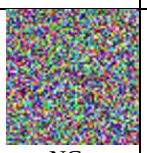
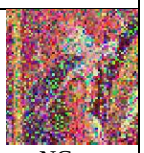
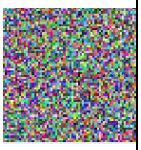
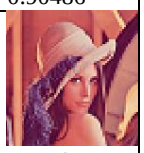
| Waktu Proses Penyisipan | | Waktu Proses Ekstraksi | |
|---|---|---|---|
| LSB | DWT | LSB | DWT |
| 18.1445 | 0.6912 | 19.3618 | 0.40965 |
| 97.5305 | 0.45076 | 279.345 | 0.43068 |
| 18.7692 | 1.1536 | 20.1151 | 0.86212 |
| 1278.723 | 1.0273 | 8198.1493 | 0.93309 |

Waktu pemrosesan ini bertujuan untuk meninjau waktu yang dibutuhkan untuk melakukan penyisipan untuk masing-masing teknik. Berdasarkan Tabel 6 diketahui bahwa waktu pemrosesan rata-rata untuk teknik penyisipan DWT selama 0,7823 detik sedangkan untuk proses ekstraksinya selama 0,6219 detik. Kemudian untuk teknik LSB diperoleh rata-rata waktu pemrosesan penyisipan selama 239,1176 detik. Berdasarkan data tersebut dapat diketahui bahwa ukuran dari pesan yang disisipkan tidak mempengaruhi waktu pemrosesan teknik DWT. Sebaliknya, teknik LSB sangat dipengaruhi oleh ukuran dari pesan yang disisipkan. Teknik LSB cenderung lebih lama karena banyaknya proses yang perlu dilakukan sangat banyak menyesuaikan banyaknya bit pesan yang akan disisipkan.

### 4.6 Hasil Pengujian Serangan

Tabel 7 dan Tabel 8 menunjukan hasil pengujian serangan *watermarking*. Informasi yang apat kita peroleh adalah Teknik LSB cenderung lebih rentan terhadap serangan/perubahan sekecil apapun. Perubahan nilai piksel sebesar satu intensitas warna piksel akan mengubah nilai LSB ari piksel tersebut. Oleh karena itu, Teknik LSB cenderung sangat rapuh/fragile. Berbeda dengan Teknik LSB, Teknik DWT masih bisa tahap terhadap beberapa serangan. Informasi pesan yang disisipkan masih dapat terlihat walau ada noise yang cukup besar.

Tabel 7. Pengujian serangan citra *cover* terwatermark pada LSB

| Serangan Pada DWT | | |
|---|---|---|
| Hasil Serangan | Hasil Ekstraksi | Hasil Dekripsi |
|  | Gagal ekstraksi | Gagal Dekripsi |
|  |  NC = 0.95771 |  NC = 0.90486 |
|  kompres.jpeg |  NC = 1 |  NC = 0.99924 |

Tabel 7 merupakan hasil dari pengujian serangan citra *cover* terwatermark pada LSB. Dari 3 serangan yang dilakukan terdapat 1 serangan yang membuat citra *cover* terwatermark gagal untuk di dekripsi pada serangan rotasi.

Tabel 8. Pengujian serangan citra *cover* terwatermark pada DWT

| Serangan Pada LSB | | | |
|---|---|---|---|
| **Serangan** | **Hasil Serangan** | **Hasil Ekstraksi** | **Hasil Dekripsi** |
| Rotasi |  | Gagal ekstraksi | Gagal Dekripsi |
| Gaussian noise |  |  NC = 0.75562 | Gagal Dekripsi |
| JPEG compression |  kompres.jpeg |  NC = 0.74501 | Gagal Dekripsi |

Tabel 8 merupakan hasil dari pengujian serangan citra *cover* terwatermark pada DWT. Dari 3 serangan yang dilakukan yaitu serangan rotasi, *Gaussian Noise* dan *JPEG compression*, semuanya serangan tersebut membuat citra *cover* terwatermark gagal untuk di dekripsi.

## 5. KESIMPULAN DAN SARAN

Kesimpulan pada penelitian ini telah didapatkan hasil bahwa kedua teknik *watermarking* yang diimplementasikan yaitu teknik *watermarking* berbasis domain frekuensi (DWT memberikan hasil penyisipan yang lebih baik dari domain spasial (LSB) jika ditinjau dari nilai rata-rata MSE sebesar nol dengan nilai rata-rata PSNR sebesar 44.59db. Berdasarkan waktu proses teknik DWT juga lebih cepat dari teknik LSB untuk semua ukuran data yang di proses. Teknik yang dikembangkan dalam penelitian ini memiliki kelemahan besar dari segi waktu proses. Oleh karena itu, diperlukan penelitian lebih lanjut demi mengoptimalkan waktu proses dengan tetap memperhatikan aspek *robustness*-nya.

## DAFTAR PUSTAKA


[1] Akhavan, A., Samsudin, A., & Akhshani, A. (2017). Cryptanalysis of an image encryption algorithm based on DNA encoding. *Optics & Laser Technology*, *95*, 94–99. https://doi.org/10.1016/j.optlastec.2017.04.022

[2] Çavuşoğlu, Ü., Akgül, A., Zengin, A., & Pehlivan, I. (2017). The design and implementation of hybrid RSA algorithm using a novel chaos based RNG. *Chaos, Solitons and Fractals*, *104*, 655–667. https://doi.org/10.1016/j.chaos.2017.09.025

[3] Jain, A., & Rajpal, N.,2016, A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. *Multimedia Tools and Applications*, *75*(10), 5455–5472

[4] Joshi, M. R., & Avinash Karkade, R. (2015). Network Security with Cryptography. *International Journal of Computer Science and Mobile Computing*, *41*(1), 201–204.

[5] Ramalingam, B., Rengarajan, A., & Rayappan, J. B. B. (2017). Hybrid image crypto system for secure image communication– A VLSI approach. *Microprocessors and Microsystems*, *50*, 1–13. https://doi.org/10.1016/j.micpro.2017.02.003

[6] Sutojo , E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, 2017, "Fast and Efficient Image Watermarking Algorithm using Discrete Tchebichef Transform," in International Conference on Information Technology for Cyber and IT Service Management (CITSM), Denpasar.

[7] Wu, Y., 2012, Image Encryption Using The Two-dimensional Logistic Chaotic Map, Department of Electrical and Computer Engineering, Tufts University Medford, Massachusetts 02155, United States