

OPTIMASI WATERMARKING PADA CITRA BIOMETRIK MENGUNAKAN ALGORITME GENETIKA

Muhammad Rifqi Fadhilah^{*)}, Imam Santoso, and Ajub Ajulian Zahra

Departemen Teknik Elektro, Universitas Diponegoro
Jl. Prof. Sudharto, SH, Kampus UNDIP Tembalang, Semarang 50275, Indonesia

^{*)E-mail: m.rifqifadhilah@gmail.com}

Abstrak

Watermarking atau tanda air dapat diartikan sebagai suatu teknik penyisipan informasi pada suatu berkas lainnya untuk ditumpangi, baik itu berupa citra, video, ataupun berkas lainnya. Pada penerapannya, proses watermarking tidak menyisipkan informasi secara sembarang, tetapi perlu memperhatikan parameter-parameter yang sesuai agar hasil menjadi optimal. Hasil watermarking bisa dikatakan optimal jika memiliki nilai invisibility dan robustness yang tinggi. Salah satu metode yang bisa digunakan untuk mencari parameter tersebut adalah Algoritme Genetika. Program watermarking pada penelitian ini diterapkan pada citra biometrik menggunakan domain Discrete Wavelet Transform dan Singular Value Decomposition. Penelitian ini menggunakan citra biometrik yaitu citra wajah sebagai citra host dan citra sidik jari sebagai citra watermark. Setelah dilakukan proses watermarking, dilakukan serangan-serangan untuk menguji ketahanan dari citra tersebut seperti pemberian derau salt & pepper, rotasi citra, penambahan teks dan pemampatan citra. Berdasarkan hasil pengujian didapatkan nilai invisibility yang sangat baik dari hasil watermarking dengan nilai Peak Signal to Noise Ratio paling tinggi 47,78767 dB. Tingkat robustness yang dimiliki juga cukup baik setelah dilakukan serangan dengan nilai Normalized Correlation tertinggi 0,9850766.

Kata kunci : watermarking, DWT, SVD, Algoritme Genetika.

Abstract

Watermarking can be interpreted as a technique to hide information on another file such as images, videos etc. In its application, the watermarking process does not hide information randomly, but it is necessary to consider the appropriate parameters for optimal results. Watermarking results can be said to be optimal if it has a high value of invisibility and robustness. One of method that can be used to find these parameters is Genetic Algorithm. The watermarking program in this research is applied to biometric image using Discrete Wavelet Transform and Singular Value Decomposition. This research use face image as host image and fingerprint image as watermark image. After watermarking process, the attacks to test the robustness of the image such as giving salt & pepper noise, image rotation, text addition and image compression. Based on test result got very good invisibility value with highest value of Peak Signal to Noise Ratio 47,78767 dB. Robustness level is also good after the attack with the highest Normalized Correlation value 0.9850766.

Keywords: watermarking, DWT, SVD, Genetic Algorithm

1. Pendahuluan

Internet merupakan media penyebaran dan pertukaran data yang sangat luas serta cepat, termasuk untuk data-data multimedia. Data-data multimedia yang dikirimkan melalui internet perlu mendapat perlindungan dari pembajakan atau akses dari pihak yang tidak berwenang. Untuk memberikan solusi terhadap permasalahan tersebut, maka dibutuhkan teknologi digital sebagai pelindung data, *Digital Watermarking* merupakan solusi yang tepat untuk melindungi data multimedia. *Watermarking* atau tanda air dapat diartikan sebagai suatu

teknik penyisipan dan atau penyembunyian informasi yang bersifat rahasia pada suatu data lainnya untuk ditumpangi, tetapi orang lain tidak menyadari adanya kehadiran data tambahan pada data host-nya, sehingga seolah-olah tidak ada perbedaan berarti antara data *host* sebelum dan sesudah proses *watermarking*[2]. Sebelumnya telah ada penelitian tentang watermarking citra digital menggunakan *Discrete Wavelet Transform* (DWT) dikombinasikan dengan metode *Singular Value Decomposition* (SVD)[3]. Pada penelitian tersebut DWT digunakan untuk mentransformasi citra digital, sedangkan SVD digunakan sebagai proses penyisipan dan ekstraksi

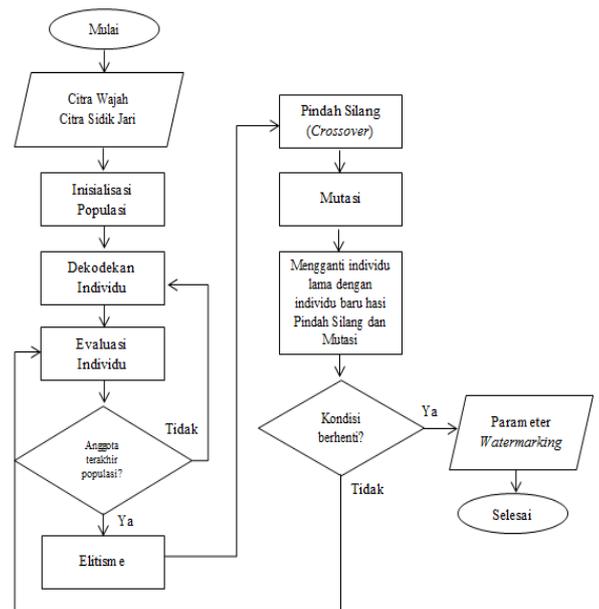
watermark. Untuk mendapatkan hasil citra watermark yang optimal, maka dibutuhkan metode optimasi, salah satunya metode Algoritme Genetika. Metode algoritme genetika tersebut digunakan dalam proses menyisipkan citra watermark agar mencapai nilai *invisibility* dan ketahanan (*robustness*) yang baik[4]-[7]. Algoritme genetika adalah metode optimasi yang digunakan untuk mencari posisi penyisipan watermark terbaik[8]. Dari penelitian yang telah dilakukan didapatkan hasil bahwa untuk mencapai citra hasil watermarking berbasis DWT yang optimal, hanya jika watermarking digunakan atau disisipkan pada subband *wavelet* tertentu dan dengan menggunakan nilai-nilai parameter tertentu pula. Teknik watermarking dengan metode optimasi tersebut juga telah diterapkan pada citra biometrik dan digunakan untuk sistem autentikasi biometrik multimodal[1], dimana dalam satu penelitian dilakukan proses optimasi watermarking menggunakan dua data biometrik.. Penelitian tersebut dilakukan menggunakan metode transformasi *Discrete Cosine Transform* (DCT) dan algoritme optimasi *Particle Swarm Optimization* (PSO). PSO pada penelitian tersebut digunakan untuk mencari koefisien DCT terbaik agar proses watermarking menjadi optimum. Penelitian tersebut bertujuan untuk mengurangi *bandwidth* meningkatkan tingkat keamanan pada sistem autentikasi biometrik multimodal. Penelitian ini melakukan penelitian lebih lanjut tentang penerapan teknik watermarking pada citra biometrik. Pada penelitian ini menggunakan metode *Discrete Wavelet Transform* (DWT) untuk tranformasi citra digital dan *Singular Value Decomposition* (SVD) sebagai metode penyisipan serta ekstraksi. Selain itu, Penelitian ini menggunakan metode Algoritme Genetika agar hasil menjadi optimal.

2. Metode

2.1. Algoritme dan Diagram Sistem

Sistem yang dirancang adalah perangkat lunak watermarking citra biometrik dengan menggunakan Algoritme Genetika. Sistem ini bekerja dengan menyisipkan citra sidik jari ke dalam citra wajah dengan menggunakan metode kombinasi antara *Discrete Wavelet Transform* (DWT) dan *Singular Value Decomposition* yang akan ditentukan parameter watermarking optimum menggunakan metode optimasi Algoritme Genetika dengan melakukan beberapa iterasi. Berikut adalah garis besar proses yang dilakukan dalam sistem watermarking ini :

- 1) Inisialisasi ukuran populasi, jumlah generasi yang akan dilakukan dan probabilitas mutasi.
- 2) Membangkitkan generasi awal dari individu algoritme genetika secara acak.
- 3) Untuk setiap generasi terdapat populasi yang dilakukan :



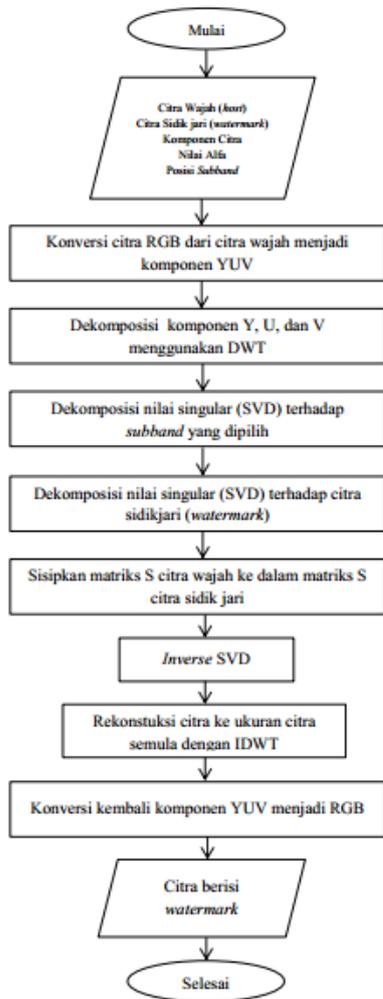
Gambar 1. Diagram alir proses watermarking dengan Algoritme Genetika

- a. Dekomposisi citra *host* menjadi empat subband yaitu *Low-Low* (LL), *High-Low* (HL), *Low-High* (LH), dan *High-High* (HH), kemudian menerapkan SVD pada salah satu *band* tersebut.
 - b. Mengubah nilai singular citra asli (*host*) dengan nilai dari citra watermark.
 - c. Menggunakan IDWT untuk mendapatkan citra wajah yang telah dilakukan watermark.
 - d. Melakukan beberapa serangan (*attack*) terhadap citra wajah yang telah disisipkan citra watermark (citra sidik jari).
 - e. Mengekstraksi citra watermark (citra sidik jari) dari setiap citra wajah yang telah dilakukan serangan.
 - f. Mengubah nilai-nilai singular untuk setiap koefisien subband dari citra yang sudah dilakukan watermark.
 - g. Mendapatkan citra sidik jari dari proses ekstraksi.
 - h. Melakukan evaluasi nilai *fitness*.
 - i. Memilih individu dengan nilai *fitness* terbaik.
 - j. Membangkitkan populasi baru dengan melakukan proses pindah silang dan mutasi pada individu yang terpilih.
- 4) Proses pada poin 3 dilakukan secara berulang-ulang sesuai dengan jumlah generasi yang ditentukan.
 - 5) Parameter watermarking yang optimal didapatkan.

2.2. Watermarking

Proses watermarking bekerja dengan cara menyisipkan citra sidik jari sebagai citra watermark ke dalam citra wajah yang berperan sebagai citra *host*.

2.2.1. Proses Penyisipan Watermarking



Gambar 2. Diagram alir proses penyisipan watermarking

Dalam penyisipan watermarking, citra RGB akan dikonversi menjadi komponen warna YUV untuk lebih memudahkan komputasi dan segmentasi citra. Citra biometrik akan ditransformasi dan didekomposisi menggunakan DWT dan SVD[3]. Setelah dilakukan penyisipan citra sidik jari, maka dilakukan inverse SVD dan IDWT untuk merekonstruksi kembali citra. Komponen warna YUV akan dikembalikan ke RGB agar citra wajah hasil watermarking memiliki penampilan yang sama dengan citra aslinya.

Setelah dilakukan penyisipan watermarking, citra akan dinilai performansinya terutama secara invisibility dengan menggunakan nilai Peak Signal to Noise Ratio (PSNR) dengan persamaan

$$PSNR = 20 \times \log_{10} \left(\frac{Q}{\sqrt{\frac{MSE(R)+MSE(G)+MSE(B)}{3}}} \right) \quad (1)$$

$$MSE(h) = \frac{1}{mn} \sum_{y=1}^m \sum_{x=1}^n [I(x, y, h) - I'(x, y, h)]^2 \quad (2)$$

dimana

MSE = Mean Square Error,

m = dimensi kolom citra,

n = dimensi baris citra,

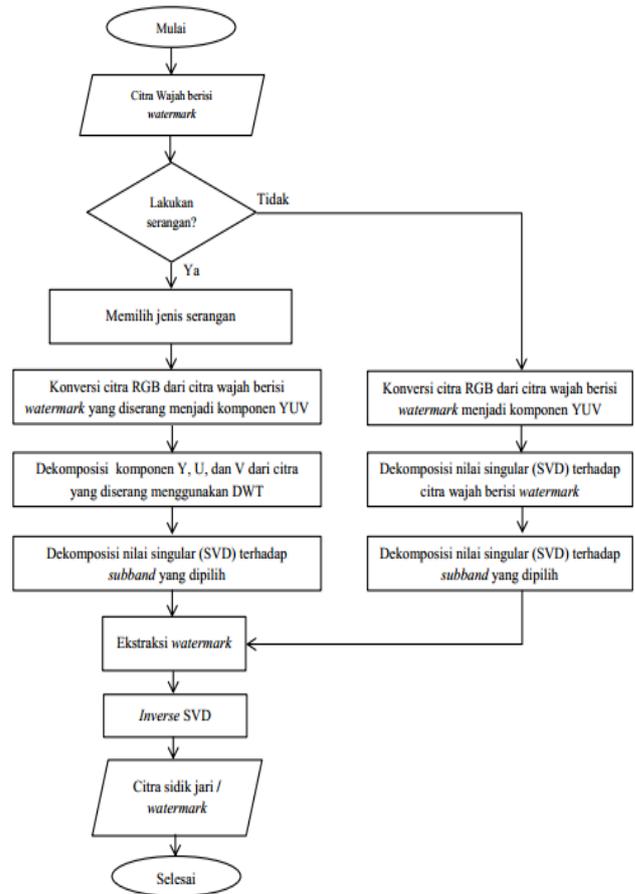
h = komponen warna citra,

(x, y, h) = koordinat piksel citra,

I(x, y, h) = citra hasil watermarking dan

I'(x, y, h) = citra asli/host.

2.2.2. Proses Ekstraksi Watermarking



Gambar 3. Diagram alir proses ekstraksi watermarking

Dalam ekstraksi watermarking, proses yang dilakukan hampir sama dengan proses yang ada pada penyisipan watermarking. Sebelum melakukan ekstraksi, citra hasil watermarking terdapat dua pilihan yaitu tidak melakukan serangan terhadap citra hasil watermarking dan tidak melakukan serangan sama sekali. Tetapi, proses utama yang dilakukan pada ekstraksi watermarking tetap sama. Setelah dilakukan ekstraksi watermarking, citra hasil ekstraksi akan dinilai kemiripannya dengan citra asli menggunakan nilai Normalized Correlation (NC) dengan persamaan :

$$NC = \frac{\sum \sum (W \times W')}{\sqrt{\sum W^2} \sqrt{\sum W'^2}} \quad (3)$$

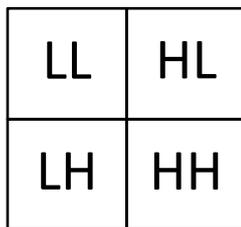
dimana

W = citra *watermark* asli dan

W' = citra *watermark* hasil ekstraksi.

2.3. Discrete Wavelet Transform (DWT)

DWT berfungsi untuk dekomposisi citra menjadi beberapa *subband* sebagai posisi penyisipan citra *watermark*. Dekomposisi pada tingkat pertama akan menghasilkan 4 *subband*, yaitu *Low-Low* (LL), *High-Low* (HL), *Low-High* (LH) dan *High-High* (HH).



Gambar 4. *Subband* hasil dekomposisi *wavelet* pada tingkat pertama

2.4. Singular Value Decomposition (SVD)

Singular Value Decomposition adalah suatu teknik untuk mendekomposisi matriks berukuran apa saja untuk mempermudah pengolahan data[3]. Hasil dari SVD adalah *nilai singular* yang disimpan dalam sebuah matriks diagonal. Nilai *singular* menyimpan informasi yang sangat penting tentang citra, yang berkontribusi paling besar terhadap variasi citra secara keseluruhan, yang disimpan pada nilai *singular* yang pertama. Pada matriks diagonal, nilai *singular* diurutkan dari nilai yang paling besar, nilai *singular* selanjutnya akan bernilai semakin kecil. Jadi apabila SVD ini diterapkan pada matriks berukuran sangat besar, akan ada banyak sekali nilai *singular* yang nilainya terlalu kecil. Nilai *singular* yang sangat kecil ini dapat diabaikan pada saat proses rekonstruksi citra tanpa mempengaruhi kualitas dari citra rekonstruksi[9]. SVD tergolong ke dalam teknik *non-blind watermarking*, karena membutuhkan citra asli dan citra berisi *watermark* untuk melakukan proses ekstraksi.

2.5. Algoritme Genetika

Algoritme Genetika merupakan algoritme pencarian yang didasarkan pada mekanisme seleksi alamiah dan genetika alamiah[10]. Algoritme Genetika banyak digunakan pada masalah praktis yang berfokus pada pencarian parameter-parameter optimal. Keuntungan penggunaan Algoritme Genetika terlihat dari kemudahan implementasi dan kemampuannya untuk menemukan solusi yang bias diterima secara cepat untuk masalah-masalah berdimensi tinggi. Ada beberapa komponen dan tahapan Algoritme

Genetika yang dipakai pada penelitian ini, yang ditunjukkan pada Gambar 1. Pada tahap “Evaluasi Individu” akan dilakukan perhitungan nilai fungsi *fitness*. Fungsi *fitness* berfungsi sebagai ukuran performansi suatu individu. Individu yang memiliki nilai *fitness* tertinggi yang akan dipilih sebagai individu terbaik. Fungsi *fitness* akan dihitung menggunakan persamaan

$$Fitness = invisibility + robustness. \quad (4)$$

Invisibility diwakilkan dengan nilai PSNR sedangkan *robustness* diwakilkan dengan nilai NC. Karena tujuan fungsi *fitness* di atas adalah untuk mendapatkan nilai *invisibility* dan *robustness* yang seimbang, maka skala nilai kedua parameter tersebut harus sama. Parameter *robustness* memiliki skala 0 – 100 yang merupakan nilai *Normalized Correlation* (0 – 1) dikali 100. Sedangkan nilai *invisibility* yang akan diambil dari PSNR citra ter-*watermark* dengan skala 0 - ∞. Oleh karena itu nilai PSNR akan diubah skalanya dengan menggunakan mekanisme berikut.

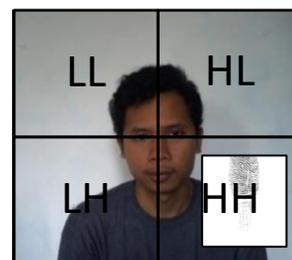
```
if (psnr <= 10)
    invisibility = 0;
elseif (10 < psnr < 50)
    invisibility = ((psnr - 10)/4)*10;
else
    invisibility = 100;
```

Rentang nilai 10-50 dB diambil berdasarkan tabel kualitas citra hasil *watermarking*[3].

3. Hasil dan Analisa

3.1. Pengujian Hasil *Watermarking*

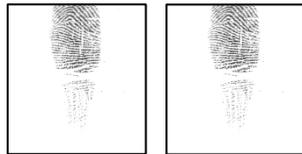
Pada penelitian ini digunakan komponen warna YUV dan menggunakan 10 pasang citra biometrik sebagai citra pengujian, yaitu citra wajah dan citra sidik jari. Citra wajah yang digunakan berjumlah 10 citra, begitu pula dengan citra sidik jari. Dari hasil pengujian didapatkan posisi *subband* terbaik berada pada *subband* HH (*High-High*) dan citra sidik jari disisipkan pada komponen warna citra Y serta nilai alfa 0,1. Nilai alfa merupakan faktor insentitas yang menentukan kekuatan *watermark*.



Gambar 5. Posisi *subband* terbaik untuk penyisipan *watermarking*



Gambar 6. Perbandingan citra wajah asli dan citra wajah hasil watermarking.



Gambar 7. Perbandingan citra sidik jari asli dan citra sidik jari hasil ekstraksi watermarking.

Tabel 1. Hasil Watermarking dengan Algoritme Genetika

Citra	PSNR (dB)	NC
Kresna.bmp	46,21375	0,9999999
Arief.bmp	47,78767	0,9999999
Fuad.bmp	39,01742	0,9999999
ArifM.bmp	44,54799	0,9999999
Albert.bmp	39,11443	0,9999999
Rifqi.bmp	42,80763	0,9999999
RifkiF.bmp	40,96173	0,9999999
Lidya.bmp	45,43272	0,9999999
Bangun.bmp	40,07966	0,9999999
Lulu.bmp	42,37569	0,9999999

Gambar 6 dan 7 merupakan hasil watermarking yang didapat. Tidak terlihat adanya perbedaan yang besar dari citra wajah asli dengan citra wajah yang berisi citra sidik jari, begitu pula dengan citra sidik jari asli dengan citra sidik jari hasil ekstraksi watermarking juga tidak terdapat perbedaan yang besar secara penglihatan mata. Tabel 1 memperlihatkan bahwa kinerja hasil penyisipan dan ekstraksi watermarking dengan optimasi Algoritme Genetika yang dilakukan sudah memiliki performansi yang sangat baik. Hasil PSNR tertinggi yang didapat adalah bernilai 47,78767 dB, sedangkan nilai NC untuk semua percobaan adalah 0,99999.

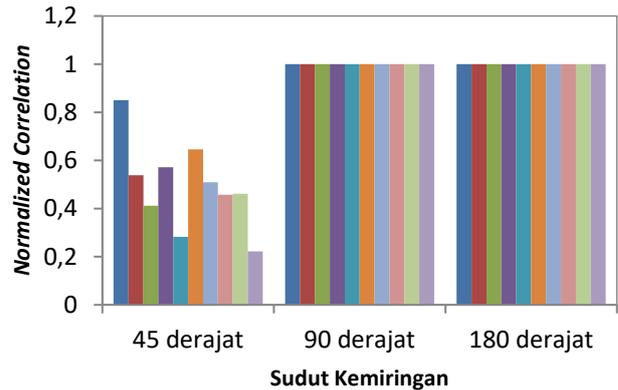
3.2. Pengujian Ketahanan (Robustness) Watermark

Pengujian ketahanan watermark atau pengujian robustness yang dimaksud adalah pengujian dengan melakukan serangan-serangan terhadap citra wajah hasil watermarking yang berisi citra sidik jari. Parameter yang dilihat untuk mengetahui ketahanan atau robustness dari adalah berdasarkan nilai Normalized Correlation (NC).

NC akan menunjukkan kemiripan antara citra sidik jari asli dengan citra sidik jari hasil ekstraksi.

3.2.1. Rotasi Citra

Pada pengujian dengan serangan rotasi citra, citra wajah yang berisi citra sidik jari akan dirotasi dengan sudut kemiringan 45, 90 dan 180 derajat.



Gambar 8. Perbandingan nilai NC dengan serangan rotasi citra

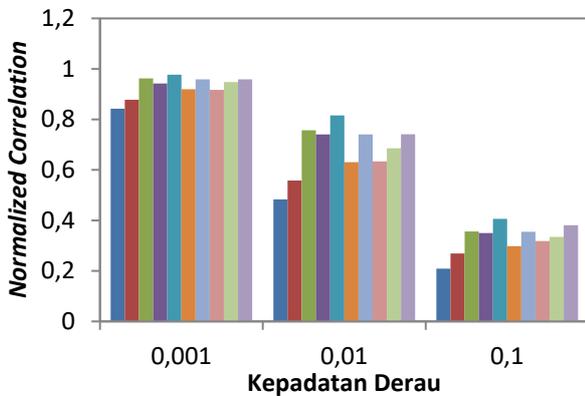
Gambar 8 memperlihatkan grafik perbandingan nilai NC dari hasil ekstraksi sepuluh pasang citra yang telah diberi serangan rotasi citra. Hasil ekstraksi citra sidik jari banyak mengalami kerusakan pada rotasi 45 derajat dengan nilai NC paling rendah berada pada nilai 0,2223125 dan nilai NC paling tinggi sebesar 0,8498722. Sedangkan pada saat diberi serangan rotasi 90 dan 180 derajat, hasil ekstraksi citra sidik jari tidak rusak dan mendapatkan nilai NC mendekati 1 yang berarti hasil tersebut sangat baik.

3.2.2. Derau Salt & Pepper

Pada pengujian dengan serangan derau salt & pepper, citra wajah yang berisi citra sidik jari akan diberi derau yang menyerupai titik-titik garam dan merica (salt & pepper). Jumlah piksel pada citra yang dipengaruhi atau diserang derau salt & pepper bergantung pada kepadatan derau dikalikan dengan jumlah elemen array dari citra yang diserang. Pengujian ini menggunakan variasi kepadatan derau dengan nilai 0,001, 0,01 dan 0,1.

Gambar 9 memperlihatkan bahwa serangan derau salt & pepper dapat merusak citra hasil ekstraksi, meskipun ada beberapa citra sidik jari yang menghasilkan nilai NC mendekati 1. Semakin tinggi kepadatan derau salt & pepper yang digunakan, maka nilai NC citra sidik jari hasil ekstraksi semakin menurun. Kepadatan noise sangat berpengaruh terhadap ketahanan citra hasil watermarking. Kepadatan derau dengan nilai 0,001 menghasilkan nilai NC yang cukup tinggi yaitu berkisar 0,84 hingga 0,97,

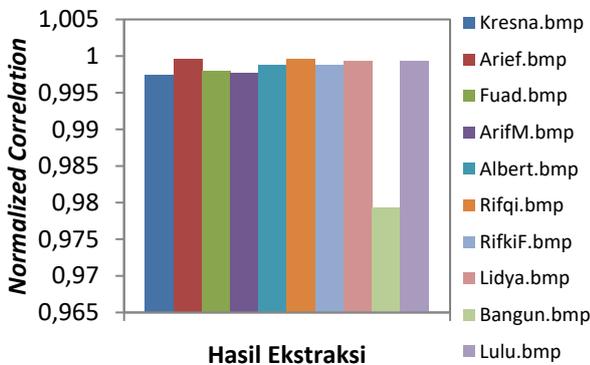
tetapi kepadatan derau dengan nilai 0,1 memiliki NC yang sangat rendah dengan rentang nilai hanya 0,20 – 0,38 saja.



Gambar 9. Perbandingan nilai NC dengan serangan derau salt & pepper.

3.2.3. Penambahan Teks

Pada pengujian ini, citra wajah hasil watermarking akan ditambahkan teks atau tulisan. Masing-masing citra yang sudah berisi citra sidik jari akan ditambahkan tulisan “Teknik Elektro UNDIP”.



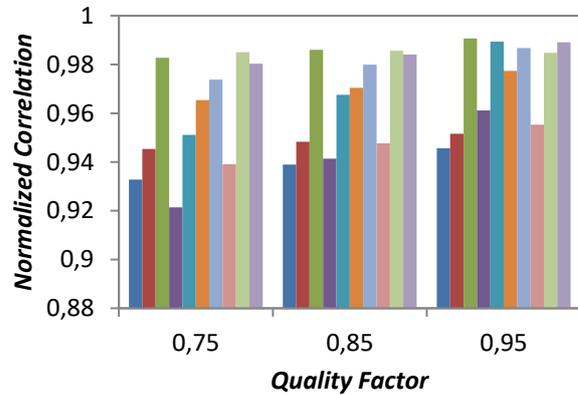
Gambar 10. Perbandingan nilai NC dengan penambahan teks.

Gambar 10 menunjukkan bahwa semua citra memiliki nilai NC yang sangat baik yaitu mendekati 1. Dari Gambar 8 dapat diketahui bahwa nilai NC paling rendah diperoleh citra Bangun.bmp dengan nilai 0,9793882. Walaupun mendapatkan nilai NC paling rendah, hasil ekstraksi citra Bangun.bmp masih bisa dikatakan sangat baik karena mendekati angka 1.

3.2.4. Pemampatan Citra JPEG

Dalam serangan pemampatan citra JPEG ini, digunakan nilai Quality Factor (QF) yang memiliki skala 0-100. QF yang semakin kecil akan mengubah ukuran citra asli

semakin kecil pula. Pada pengujian yang dilakukan, dipilih nilai QF 75, 85, dan 95. Pemilihan nilai QF ini mengacu pada batas minimum agar suatu citra dikatakan usable dimana citra harus tahan terhadap serangan pemampatan citra JPEG minimum dengan nilai QF 75-100[4].



Gambar 11. Perbandingan nilai NC dengan serangan pemampatan citra JPEG.

Gambar 11 menunjukkan bahwa nilai NC yang diperoleh sudah cukup baik karena semua citra hasil ekstraksi watermarking memiliki nilai NC mendekati 1. Setiap citra mengalami peningkatan nilai NC saat nilai QF semakin besar. Hal ini memperlihatkan bahwa saat nilai QF untuk pemampatan citra JPEG semakin tinggi, maka nilai NC citra hasil ekstraksi watermarking yang dihasilkan juga semakin baik.

4. Kesimpulan

Berdasarkan hasil pengujian yang dilakukan, didapatkan bahwa proses watermarking citra biometrik menggunakan Algoritme Genetika memiliki tingkat invisibility yang sangat baik dengan nilai PSNR berkisar 39 - 47 dB. Nilai ketahanan (robustness) yang dimiliki juga sudah cukup baik. Citra hasil watermarking memiliki tingkat ketahanan yang baik saat diserang rotasi citra dengan sudut kemiringan 90° dan 180°, penambahan teks, derau salt & pepper dengan kepadatan yang kecil serta pemampatan citra JPEG. Semua citra biometrik hasil watermarking memiliki nilai NC yang mendekati 1 saat mengalami serangan tersebut. Namun citra biometrik hasil watermarking masih memiliki tingkat ketahanan yang rendah jika mengalami serangan rotasi citra dengan sudut kemiringan selain sudut siku (90°) dan sudut lurus (180°). Hal ini terlihat saat diserang dengan rotasi citra 45°, citra hasil ekstraksi menjadi rusak dengan nilai NC paling rendah 0,2223125. Hal yang sama juga terjadi saat citra biometrik hasil watermarking diserang dengan derau salt & pepper dengan kepadatan derau yang tinggi. Saat citra diserang derau salt & pepper dengan kepadatan 0,1, citra sidik jari hasil ekstraksi menjadi sangat buruk

dengan nilai NC paling rendah 0,2089189. Penelitian ini dapat dikembangkan lebih lanjut dengan juga mengaplikasikannya langsung ke dalam sistem autentikasi atau pengenalan citra biometrik seperti pengenalan sidik jari untuk memeriksa apakah citra sidik jari hasil *watermarking* tersebut dapat dideteksi dan terverifikasi untuk sistem pengenalan. Selain itu algoritme optimasi lain juga bisa digunakan seperti *Particle Swarm Optimization* (PSO) dan algoritme evolusi lainnya agar hasil *watermarking* bisa lebih baik lagi.

Referensi

- [1] P. Bedi, R. Bansal, and P. Sehgal, "Multimodal Biometric Authentication using PSO based Watermarking," *Procedia Technol.*, vol. 4, pp. 612–618, 2012.
- [2] R. Munir, *Pengolahan Citra Digital dengan Pendekatan Algoritmik*. Bandung: Penerbit Informatika, 2004.
- [3] A. C. Simanjuntak, "Watermarking Citra Digital pada Ruang Warna YUV dengan Kombinasi Metode Discrete Wavelet Transform (DWT) dan Singular Value Decomposition (SVD)."
- [4] B. K. Balaka, T. A. Bw, and S. Violina, "Analisis dan Implementasi Algoritma Genetika Pada Watermarking Citra Dalam Domain Discrete Wavelet Transform Menggunakan Haar Wavelet," pp. 1–5, 2010.
- [5] P. Surekha and S. Sumathi, "Implementation Of Genetic Algorithm For A DWT Based Image Watermarking Scheme," pp. 244–252.
- [6] S. S. M. Ziabari, "The Optimized Image Watermarking Using Genetic Algorithm," pp. 359–363, 2013.
- [7] D. Lee, T. Kim, S. Lee, and J. Paik, "Genetic Algorithm-Based Watermarking in Discrete Wavelet Transform Domain," pp. 709–716, 2006.
- [8] T. Sridevi and S. S. Fatima, "Digital Image Watermarking Using Genetic Algorithm in DWT and SVD Transform," pp. 485–490.
- [9] L. A. Tyas. *Watermarking Citra Digital Berbasis DWT-SVD dengan Detektor Non-Blind*. Skripsi S-1. Semarang: Universitas Diponegoro; 2011.
- [10] D. E. Goldberg, *Genetic Algorithms in Search, Optimization, and Machine*