

## PENYISIPAN TANDA AIR PADA CITRA DIJITAL BERBASIS DEKOMPOSISI NILAI SINGULIR (DNS)

T. Basaruddin, dan Cahyana

Fakultas Ilmu Komputer, Universitas Indonesia, Depok 16424, Indonesia

### Abstrak

Tanda air (*watermark*) merupakan teknik yang banyak digunakan untuk melindungi citra digital dari pemalsuan. Makalah ini akan membahas teknik penyisipan tanda air (*watermarking*) yang didasari konsep dekomposisi matrik yang disebut dekomposisi nilai singular (*singular value decomposition*) dan disingkat DNS. Target utama yang ingin dicapai adalah bahwa tanda air yang disisipkan tidak mengganggu tampilan citra digital di mana tanda air tersebut disisipkan (*imperceptible*) dan bahwa tanda air tersebut dapat diekstrak dengan utuh meskipun pada citra tersebut telah dilakukan berbagai perubahan (*robustness*). Hasil penelitian kami menunjukkan bahwa kedua target tersebut dapat dipenuhi oleh teknik yang didasari oleh DNS seperti ditunjukkan oleh nilai korelasi yang cukup tinggi setelah dilakukan beberapa transformasi seperti PSNR, RML dan Kompresi.

### Abstract

**Imperceptible of Watermarking in Digital Image Based Singular Value Decomposition.** Watermarking is a commonly used technique to protect digital image from unintended used such as counterfeiting. This paper will address one of the techniques to embed a watermark to digital image which is based on the singular value decomposition. The primary target to be achieved by a good watermarking technique is that the watermarked image is imperceptible and that the inserted image can still be perfectly retrieved even though various transformations are done to the watermarked image. Our works show that the SVD-based watermarking demonstrates both imperceptibility as well as robustness of the watermarking scheme as indicated by significantly high value of correlation between the inserted and retrieved logo after some transformation such as PSNR, RML and Compression.

*Keywords: watermarking, singular value, digital image, imperceptibility, robustnes*

### 1. Latar Belakang

Perkembangan teknologi informasi dan komunikasi telah memungkinkan terjadinya penyimpanan dan penyebaran citra digital secara mudah dan meluas. Kemudahan yang dimaksud antara lain dengan berkembangnya teknologi media rekam dan media penyimpanan citra digital yang memungkinkan disajikannya suatu citra digital dengan mutu yang sangat tinggi (baik dari aspek tingkat resolusi maupun variasi warna). Sementara itu, pemanfaatan jalur komunikasi pita lebar (*broad-band network*) juga telah memungkinkan penyebaran data citra secara mudah dan cepat.

Di pihak lain, kemajuan dan perkembangan di atas diikuti pula oleh kebutuhan untuk melindungi citra digital dari tangan-tangan yang tak bertanggungjawab seperti pemalsuan atau pengakuan atas kepemilikan suatu citra. Untuk melindungi citra digital dari perlakuan tak diinginkan seperti tersebut di atas, digunakan suatu teknik yang disebut dengan penyisipan tanda air digital (*watermarking*). Watermarking digital didefinisikan sebagai penyisipan suatu informasi pada suatu citra digital tanpa mengganggu penampilan citra yang disisipi. Teknik ini sebenarnya sudah digunakan pada dokumen konvensional, misalnya untuk uang kertas, atau surat bergarga lainnya.

Suatu citra digital biasanya disimpan dalam bentuk matrik segiempat yang ukurannya disesuaikan dengan ukuran dan tingkat resolusi citra dimaksud. Suatu citra tak berwarna cukup disimpan dalam satu matrik yang elemen-elemennya berupa bilangan bulat non-negatif yang menyatakan tingkat keabuan (*gray scale*). Sedangkan citra berwarna memiliki tiga komponen warna pokok yaitu merah, hijau dan biru, sehingga membutuhkan tiga matrik yang berbeda dalam

penyimpanannya. Pada perkembangannya, penyimpanan citra ini menggunakan format-format yang sudah dibakukan seperti bitmap atau jpg (untuk citra tak bergerak), atau avi dan mpeg (untuk citra video). Dalam format baku tersebut, penyimpanan citra juga sudah dilengkapi dengan teknik pemampatan (*compression*) sehingga dapat menghemat kebutuhan ruang dan memory penyimpanan. Untuk keperluan penelitian ini diasumsikan bahwa citra dimaksud disimpan dalam bentuk primitive berupa matriks.

Tanda air yang akan disisipkan pada suatu citra digital juga berupa citra digital, yang selanjutnya disebut logo. Penggunaan istilah logo ini cukup berkesan mengingat citra yang disisipkan biasanya berukuran tidak terlalu besar dan memiliki informasi khas dan spesifik yang digunakan untuk menandai suatu dokumen.

## 2. Dekomposisi Nilai Singular (DNS)

Misalkan  $A$  adalah suatu matrik berukuran  $m \times n$  dengan elemen bilangan riil. Maka terdapatlah matrik ortogonal  $U$  dan  $V$  serta matrik diagonal  $S$  sehingga

(1)

dengan

dan

serta

dengan  $u_i$  dan  $v_i$ . Vektor  $u_i$  dan  $v_i$  berturut-turut dinamakan vektor singular kiri dan vektor singular kanan ke- $i$  untuk matrik  $A$ , sedangkan  $\sigma_i$  dinamakan nilai singular ke- $i$  dari matrik  $A$ . Matriks  $U$  sering juga disebut sebagai matrik *hanger* dan  $S$  disebut matrik *stretcher*, sedangkan  $V$  disebut matrik *aligner*. Penamaan tersebut dikaitkan dengan sifat geometris ketiga matrik tersebut, yang dalam hal ini  $U$  berfungsi sebagai matrik penggantung suatu kurva pada suatu kerangka siku-siku tertentu,  $S$  akan menarik kurve sesuai dengan lebar spektrum nilai singular, dan  $V$  akan mengembalikan posisi kurva hingga selaras dengan sumbu kartesian.

Perhatikan bahwa  $U$ ,  $S$  dan  $V$  menyimpan karakteristik yang sangat penting dari matrik  $A$ . Banyaknya nilai singular yang positif akan menyatakan rank dari matrik  $A$ . Jika misalnya  $r = \text{rank}(A)$ , maka matrik  $A$  akan secara tepat direpresentasikan oleh  $r$  kolom pertama dari matrik  $U$  dan  $V$  mengingat

(2)

Dekomposisi nilai singular suatu matrik membutuhkan komputasi yang cukup intensif dan merupakan persoalan non-linier. Algoritma penghitungan DNS yang banyak dipakai umumnya dikembangkan dari metode penyelesaian persoalan eigen khususnya yang berbasis dekomposisi orthogonal seperti QR antara lain yang diusulkan oleh Golub dkk [1]. Dalam makalah ini algoritma penghitungan DNS tidak akan dibahas secara mendetil. Perhatikan bahwa kolom-kolom matrik  $V$  merupakan vektor eigen matrik  $A^T A$ , mengingat

(3)

Tampak juga bahwa  $\sigma_i^2$  merupakan nilai eigen dari  $A^T A$ . Juga dapat ditunjukkan bahwa kolom-kolom matrik  $U$  adalah vektor eigen matrik  $A A^T$ .

### 3. Teknik Penyisipan Tanda Air berbasis DNS

Untuk menyederhanakan penyajian, dalam makalah ini suatu citra digital akan dinotasikan sebagai suatu matrik  $A$  dan logo dinotasikan dengan matrik  $W$ . Terdapat berbagai teknik untuk menyisipkan  $W$  pada  $A$  yang antara lain melalui DNS. Penggunaan DNS untuk menyisipkan  $W$  pada  $A$  juga terdapat beberapa variasi antara lain yang diajukan oleh Sverdllov dkk [2] yaitu dengan menyisipkan nilai singular matrik  $W$  pada matrik *stretch* untuk  $A$  yaitu  $S$ . Dalam hal ini

(4)

di mana  $\lambda$  adalah nilai singular matrik  $W$  dan  $c$  adalah konstanta untuk mengatur tingkat intensitas. Selanjutnya citra yang telah diberi tanda air diperoleh melalui  $A_w$  dimana  $V$  adalah matrik yang memuat nilai singular hasil sisipan, yaitu seperti tertera di atas.

Sementara itu, Kauffman [3] mengajukan teknik penyisipan tanda air melalui matrik  $V$ . Idenya dikembangkan untuk menyisipkan tanda air pada citra video dan beberapa frame gambar dijadikan sebagai sampel untuk disisipkan tanda air. Salah satu frame gambar didekomposisi menggunakan DNS dan beberapa kolom dari matrik  $V$  dijadikan sebagai logo yang akan disisipkan pada beberapa frame gambar yang juga didekomposisi melalui DNS.

Teknik yang akan dibahas pada penelitian ini menggunakan penyisipan  $W$  pada  $S$  yang diajukan oleh Liu dan Tan [4] sebagaimana dijelaskan berikut ini:

1. Lakukan DNS pada citra  $A$ :
2. Sisipkan logo  $W$  pada  $S$ :  
dengan  $c$  konstanta untuk mengatur intensitas logo
3. Lakukan DNS pada  $A_w$ :
4. Konstruksikan citra baru yang memuat tanda air:

$A_w$  dalam hal ini merupakan citra yang telah diberi tanda air  $W$  dan dianggap sudah terlindung dari kemungkinan terjadinya upaya pemalsuan. Jika misalnya ditemukan citra serupa dan diklaim oleh pihak lain, maka kita dapat menyatakan bahwa citra tersebut memuat tanda air yang tidak tampak dan hanya dapat mengekstrak logo tersebut sajalah yang berhak mengklaim kepemilikan atas citra tersebut.

Proses ekstraksi logo  $W$  dari dalam  $A_w$  dapat dilakukan melalui proses berikut (yaitu dengan membalik proses penyisipan di atas):

1. Lakukan DNS pada  $A_w$ :
2. Konstruksikan  $S_t$ :
3. Ekstraksi  $W$ :

Perhatikan bahwa hanya pemilik logo yang mengetahui  $U_w$ ,  $V_w$ , dan  $S$ . Sehingga logo  $W$  hanya akan dapat diekstraksi oleh pemilik logo yaitu pemilik citra asli.

Faktor skala  $c$ , sebagaimana telah dijelaskan sebelumnya merupakan factor intensitas logo agar tingkat imperceptibility (ketersembunyian) logo tersebut dapat dijaga. Nilai  $c$  yang kecil tentu saja akan lebih tersembunyi jika dibandingkan dengan  $c$  yang lebih besar. Namun dipihak lain,  $c$  yang terlalu kecil akan menurunkan tingkat

kehandalan khususnya bila citra yang telah disisipkan logo tersebut dimanipulasi seperti pemampatan, pemotongan, dan lain sebagainya.

Untuk mengkuantifikasi tingkat kemiripan antara logo asli dengan logo hasil ekstrak digunakan nilai korelasi yang didefinisikan sebagai berikut:

(5)

dengan  $M$  adalah matrik yang memuat logo hasil ekstraksi. Nilai  $\alpha$  yang diharapkan adalah 1. Norm yang digunakan adalah norm Frobenius untuk menjaga agar  $\alpha$  konsisten dengan sifat korelasi.

#### 4. Percobaan Numerik

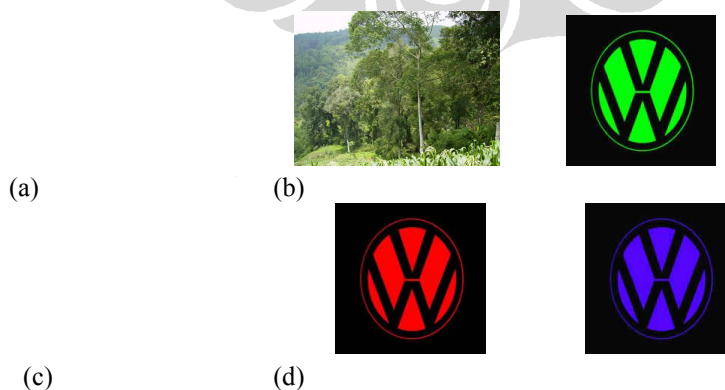
Untuk menjamin bahwa citra yang digunakan benar-benar asli dan belum disisipkan tanda air, maka citra yang digunakan dalam penelitian ini adalah citra yang dibuat khusus, yaitu berupa gambar hutan yang diambil menggunakan kamera digital dengan ukuran 512x384 piksel, sedangkan logo berupa symbol berukuran 200x200 seperti tertera pada Gambar 1.

Untuk melihat pengaruh warna dominan pada logo terhadap tingkat ketersembunyiannya pada citra, digunakan 3 jenis warna dominan yaitu merah, hijau dan biru yang merepresentasikan 3 warna dasar dalam citra.

Untuk mengukur tingkat kehandalan teknik watermarking yang digunakan, peneliti menggunakan perangkat lunak *benchmark* yaitu Stirmark yang dikembangkan oleh Fabient Petitcolas [5]. Adapun transformasi yang kami lakukan pada percobaan ini adalah transformasi *affine*, rotasi, konvolusi, *scaling*, *cropping*, *remove line*, tes PSNR, kompresi JPEG, filter median dan penambahan noise. Nilai parameter yang diambil adalah nilai bawah, tengah dan atas.

#### 5. Hasil Percobaan dan Analisis

Berdasarkan percobaan, ternyata *watermark* yang di-ekstrak dari citra memiliki nilai korelasi yang sangat bagus. Semua *watermark* yang ter-ekstrak sama seperti *watermark* aslinya, sehingga nilai korelasi yang dihasilkan adalah satu. Nilai korelasi ini tidak terpengaruh oleh nilai  $\alpha$  yang digunakan, maupun warna logo yang disisipkan.

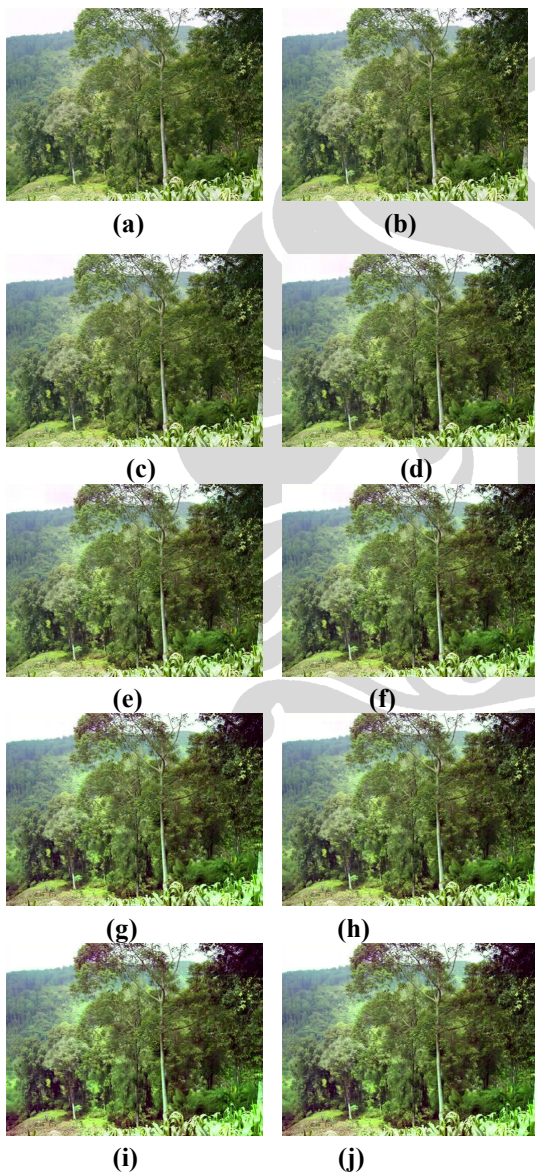


Gambar 1. Citra host (a) dan Logo yang disisipkan (b), (c) dan (d)

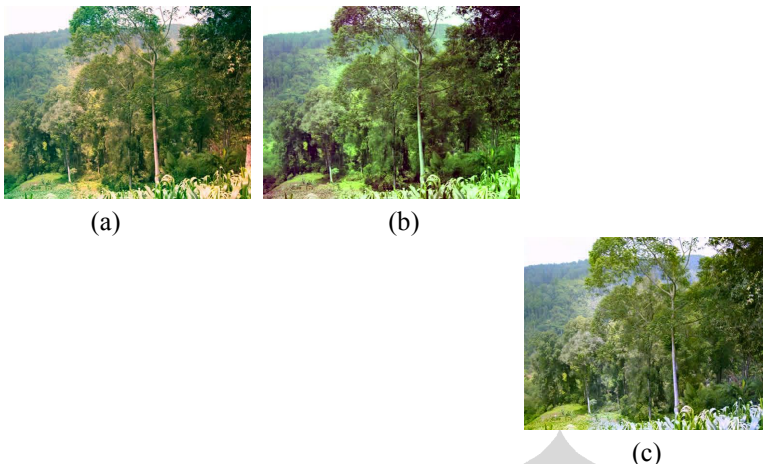
Tabel 1. Perbandingan Nilai PSNR Citra Watermark

Nilai $\alpha$	Logo Biru	Logo Hijau	Logo Merah
----------------	-----------	------------	------------

0,1	53.619	54.451	54.706
0,2	45.459	45.777	46.327
0,3	40.287	40.850	41.104
0,4	36.464	36.306	36.921
0,5	34.302	32.994	33.321
0,6	31.576	31.395	31.766
0,7	29.057	29.394	29.792
0,8	26.995	27.458	27.846
0,9	25.302	25.761	26.112
1	23.906	24.257	24.586



Gambar 2. Citra *Watermark* dengan nilai  $\alpha=0,1$  (a); 0,2 (b) ; 0,3 (c); 0,4 (d) ;0,5 (e); 0,6 (f); 0,7 (g); 0,8 (h); 0,9 (i); dan 1 (j)



**Gambar 3. Citra Watermark dengan logo Hijau (a), Merah (b) dan Biru (c);  $\alpha = 1$**

Berbeda dengan nilai korelasi, PSNR dipengaruhi secara signifikan oleh nilai  $\alpha$ , di mana semakin besar nilai  $\alpha$  menyebabkan nilai PSNR semakin turun. Hal ini menandakan bahwa tingkat ketersembunyian logo yang disisipkan akan menurun bilai  $\alpha$  diperbesar.

Gambar 2 memperlihatkan citra yang telah disisipi watermark dengan nilai berbagai nilai  $\alpha$ . Terlihat bahwa makin besar nilai  $\alpha$ , makin besar pula degradasi yang terjadi pada citra.

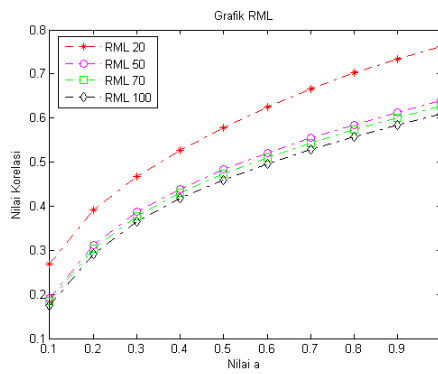
Kemudian, tingkat degradasi citra juga dipengaruhi oleh besar *watermark*, yang dalam hal ini terlihat dari nilai norm *watermark* tersebut. Dalam percobaan kami, *watermark* berupa logo berwarna biru memiliki norm lebih tinggi daripada kedua warna logo lainnya. Dengan demikian, tingkat degradasi citra yang ditimbulkan oleh *watermark* tersebut juga lebih besar daripada dua logo lainnya. Pada nilai  $\alpha = 0,4$ ; citra yang disisipi oleh logo *watermark* berwarna biru sudah mulai terlihat degradasinya, sementara citra yang disisipi *watermark* dengan warna lain belum. Selain itu, warna dominan pada citra dan *watermark* juga mempengaruhi tingkat degradasi citra. Ditunjukkan oleh gambar 3, masing-masing *watermark* akan merubah warna citra sesuai dengan komponen warna dominan pada *watermark*. Makin tinggi nilai norm komponen tersebut, makin terlihat warnanya pada citra.

## 6. Nilai Korelasi setelah Pemrosesan dengan StirMark

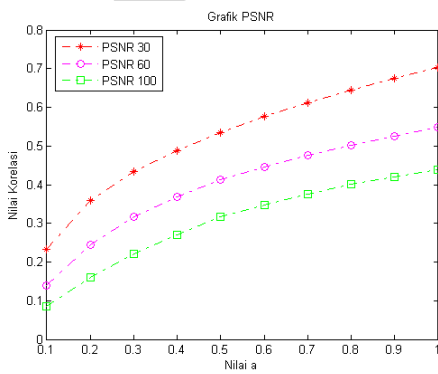
Nilai korelasi yang diperoleh setelah pemrosesan dengan StirMark tidak terlalu baik. Kecenderungan nilai korelasi pada seluruh *attack* adalah sama, makin besar nilai  $\alpha$ , makin tinggi nilai korelasi *watermark*. Korelasi tertinggi hanya mencapai kisaran 0,7, berbeda jauh dengan nilai korelasi awal yang mencapai 1. Bahkan pada beberapa *attack*, nilai korelasi yang diperoleh adalah minus. Namun, *watermark* yang di-ekstrak masih dapat terlihat utuh (tidak blur) pada nilai korelasi 0,4.

*Watermark* memiliki korelasi terendah ketika pada citra dilakukan teknik konvolusi. Konvolusi ini merupakan gabungan teknik filter Gaussian dengan teknik *re-sharpening*. Demikian pula ketika pada citra dilakukan filter median, hasil korelasi tidak terlalu bagus. Nilai korelasi juga tidak baik pada pemrosesan dengan rotasi, *cropping*, *rescaling* dan penambahan *noise*. Namun, ketika pada citra dilakukan proses penghilangan garis atau kolom (RML), yaitu menghilangkan cuplikan  $k$  pada interval regular pada barisan *pseudo random*  $(-1,1)$  (dan menggeser yang berikutnya), nilai korelasi yang diperoleh cukup baik. Demikian pula ketika pada citra dilakukan pengujian PSNR (menguji kekuatan *watermark* yang disisipkan), transformasi affine dan kompresi JPEG. Dengan kata lain, teknik ini tidak dapat bertahan terhadap *attack* yang mengakibatkan perubahan bentuk citra dan jika serangan melibatkan proses *filtering*.

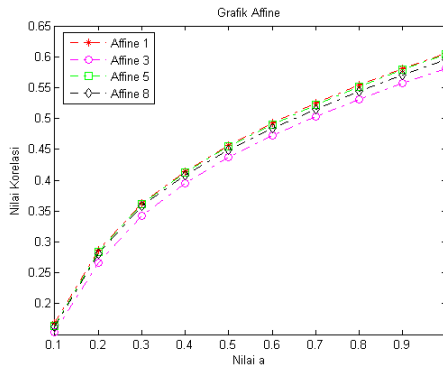
Dari pengujian juga terlihat bahwa proses DNS yang dilakukan dalam teknik ini menyebabkan *watermark* tersebar pada seluruh matriks citra. Hal ini terlihat terutama pada pengujian *cropping*, dimana pemotongan pada gambar akan mengakibatkan *watermark* mengalami degradasi, namun tidak menghilangkan *watermark* secara keseluruhan.



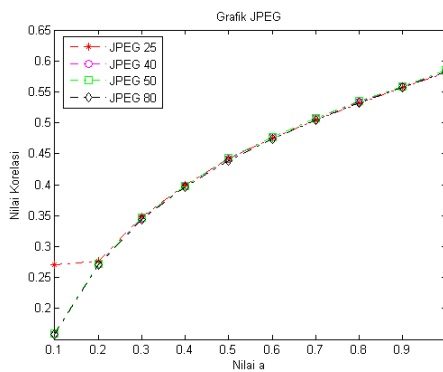
Gambar 4. Grafik RML dengan *Watermark Hijau*



Gambar 5. Grafik PSNR dengan *Watermark Hijau*



Gambar 6. Grafik *Affine* dengan *Watermark Hijau*



Gambar 7. Grafik Kompresi JPEG dengan *Watermark Hijau*

Gambar 5-7 memperlihatkan nilai korelasi *watermark* untuk *attack* RML, PSNR, transformasi *affine* dan kompresi JPEG.

Sebagai perbandingan, kami mencoba melakukan proses perubahan pada citra yang disisipi logo dengan warna merah dan biru. Kami memilih transformasi PSNR, RML dan konvolusi dimana nilai korelasi yang diperoleh baik dan terburuk. Dari percobaan diperoleh hasil, untuk nilai  $\alpha$  yang sama, *watermark* dengan warna biru menghasilkan nilai korelasi yang lebih baik daripada *watermark* dengan warna lainnya. Sementara *watermark* warna merah memiliki nilai korelasi terendah dibandingkan dengan warna lainnya. Jadi, *watermark* dengan norm yang lebih tinggi akan lebih *robust* daripada *watermark* dengan norm yang lebih rendah.

## 7. Kesimpulan

Semakin rendah nilai  $\alpha$ , semakin baik tingkat *invisibility watermark*. Namun, tingkat *robustness watermark* menurun. Kemudian, pada nilai korelasi 0,4 *watermark* masih dapat terlihat utuh. Nilai korelasi tersebut dapat diperoleh pada nilai  $\alpha = 0,5$  untuk rata-rata percobaan. Pada nilai tersebut, tingkat *invisibility watermark* juga tidak buruk, masih dapat diterima. Karena itu, kami menyimpulkan bahwa nilai  $\alpha = 0,5$  merupakan nilai yang optimum.

Tingkat *robustness watermark* juga tergantung pada norm *watermark* tersebut. Makin tinggi nilai norm-nya, makin *robust watermark* terhadap perubahan-perubahan yang dilakukan pada citra. Pada percobaan terlihat, teknik watermarking yang digunakan tidak cukup *robust* terhadap serangan yang mengakibatkan perubahan bentuk citra dan jika serangan melibatkan proses *filtering*

Proses DNS yang dilakukan pada watermark menyebabkan watermark tersebar pada keseluruhan citra.

## Referensi

- [1] Golub, G.H. and Van Loan, C.F., "Matrix Computation", John Hopkin University Press, 1989.
- [2] A. Sverdlov, S. Dexter, and A. M. Eskicioglu. "Robust DCT-SVD domain image watermarking for copyright protection", private communication 2006.
- [3] J.R. Kauffman, "Digital video watermarking using SVD and 2-D PCA", thesis College of Engineering and Technology of Ohio University, 2006.
- [4] R. Liu and T. Tan, "A SVD-Based Watermarking Scheme for Protecting Rightful Ownership," IEEE Transactions on Multimedia, 4(1), March 2002, pp.121-128.
- [5] Fabien A. P. Petitcolas dan Kutter, M., "A Fair Benchmark for Image Watermarking Systems", Electronic Imaging '99, Security and Watermarking of Multimedia Contents, Vol. 3657. The International Society for Optical Engineering, 1999.
- [6] Gorodetski, V.I., Popyack, L.J., Samoilov, V. dan Skormin, V.A., "SVD-Based Approach to Transparent Embedding Data into Digital Image", International workshop on Mathematical Methods, Models and Architectures for Computer Network Security. 2052, 2001, h263-274.
- [7] Hsu, C.-T. dan Wu, J.-L., "Hidden Digital Watermarks in Images", IEEE Transactions on Image Processing 8 (1), 1999, h58- 68.