PENERAPAN DIGITAL *WATERMARK* SEBAGAI VALIDASI KEABSAHAN GAMBAR DIGITAL DENGAN SKEMA *BLIND WATERMARK*

Adi Suheryadi[1]

[1,] Teknik Informaika - Politeknik Negeri Indramayu
[1,] Indramayu, Indonesia
E-mail : adisuheryadi@polindra.ac.id[1]

Abstrak

Digital watermarking merupakan bagian yang penting dalam perkembangan teknologi yang saat ini telah berkembang pada era digital. Era digital memberi motivasi untuk menyebarkan gambar di internet melalui *website* dengan skala besar. Disisi lain gambar digital merupakan objek yang sangat mudah untuk diubah atau dimanipulasi, dan bahkan disalin tanpa bertanggungjawab. Sebaliknya sangat sulit membuktikan gambar itu telah diubah dengan peralatan yang ada saat ini, selain itu sulit juga untuk dibuktikan kepemilikannya. Hal ini menjadi masalah penting, ketika gambar tersebut merupakan salah satu alat bukti untuk kasus hukum, pelaporan berita dan pengarsipan medis, dimana gambar tersebut haruslah dapat dipastikan bahwa gambar digital tersebut tidak mengalami perubahan ataupun manipulasi. Dalam penelitian ini kami menyajikan penerapan *digital watermarking* sebagai alat otentikasi dan validasi kepemilikan gambar digital. Sehingga gambar dapat dipastikan keabsahannya. Penelitian ini menerapkan skema *blind watermark* dengan menggunakan *secret key* yang disisipkan pada *least-significant bits* (LSB) gambar *host* secara *invisible*. Hasil yang didapatkan adalah gambar yang ter*watermark* mengalami penurunan kualitas yang kecil dengan nilai rata-rata PSNR dan MSE sekitar 34.08 dan 14.62.

***Kata Kunci*:** *digital watermark, host, invisible watermark, secret key, least-significant bits(LSB).*

Abstract

Digital watermarking is an important field of technological development that has now grown in the digital era. Digital era encourage the spread digital images on internet by the websites with a large scale. On the other hand, digital images are objects that are very easy to change or manipulate, and even copied irresponsibly. Meanwhile it is very difficult to prove the image has been changed by existing equipment at this time, and it is difficult to prove its ownership. This is an important issue, when the image is one of the evidences for legal cases, news reporting and medical filing, where the image must be ensured that the digital image is not subject to change or manipulation. In this paper, we present the application of digital watermarking to authentication and ownership validation of digital image so the image can be ascertained its validity. This research applies blind watermark scheme by using secret key that inserted at least-significant bits (LSB) of host image therefore the watermark is invisible watermark. The result of watermarked image has a small decrease in quality with the mean value of PSNR and MSE about 34.08 and 14.62.

***Keywords*:** *digital watermark, host, invisible watermark, secret key, least-significant bits (LSB)*

I. PENDAHULUAN

Digital watermarking adalah Teknik untuk menyisipkan informasi berupa *watermark* kedalam sebuah media digital seperti gambar, yang kemudian dapat diektrasi untuk berbagai tujuan diantaranya identifikasi atau otentikasi[1]. Tujuan utama dari digital *watermarking* adalah melindungi hak cipta. Digital *watermarking* akan menyisipkan sebuah informasi ke dalam sebuah *set host-data* dengan cara atau skema tertentu sehingga informasi tersebut tidak menggangu penggunaan *host-data* secara normal dengan tetap mempertahankan otentikasi host-data tersebut[2]. Klasifikasi skema *watermark* dapat ditentukan dari jenis informasi yang dibutuh oleh *detector*, yang mana dapat di klasifikasikan menjadi tiga skema klasifikasi yaitu skema *non-blind*, *semi-blind*, dan *blind*. Dari ketiga skema tersebut memiliki kebutuhan yang berbeda beda, pada skema *non-blind* membutuhkan *host-data* dan *secret key* untuk menyisipkan *watermark*. Skema *semi-blind* membutuhkan *secret key* dan *watermark*, sedangkan skema *blind* hanya membutuhkan *secret key*[3].

Salah satu yang menjadi tantangan besar dalam skema *blind watermarking* adalah memastikan *watermark* dapat terekstrak tanpa diberikan informasi dari berupa original *host*-nya.

Penyisipan *watermark* dalam suatu gamabar dilakukan dengan *visible*(terlihat) ataupun *invisible*(tidak terlihat) yang biasa disebut dengan *visible watermarking* dan *invisible watermarking*[4]. *Invisible watermarking* dalam beberapa dekade menjadi fokus penelitian.

Metode penyembunyian data untuk gambar dapat dikategorikan menjadi dua kategori yaitu bersifat spasial-domain dan domain frekuensi. Dalam domain spasial, pesan rahasia dalam hal ini *watermark* tertanam pada piksel gambar secara langsung. Metode yang paling umum adalah teknik histogram berbasis dan *least-significant bits* (LSB) dalam domain spasial.

Salah satu teknik spatial-domain telah dikenalkan dalam penyisipan *watermark* secara tesembunyi diantaranya datang dari Ping Wah Wang et.al [5], dimana beliau melakukan penelitian penyisipan *watermark* secara tersembunyi dengan menggunakan *secret* dan *public key* sebagai autentikasi dan verifikasi kepemilikan suatu karya digital berupa gambar. Dalam jurnal ini kami akan menerapkan konsep *invisible watermarking* dengan skema blind dan menggunakan *secret key* untuk memverifikasi karya digital berupa gambar. Jurnal ini disusun sebagai berikut. Pendahuluan diberikan Bagian I. Kajian terhadap pekerjaan terkait penelitian ada pada Bagian II. Bagian III menyajikan metode yang diusulkan. Hasil Eksperimental dibahas pada Bagian IV. Bagian V menjelaskan Kesimpulan.

II. TINJAUAN PUSTAKA

Invisible *watermarking* merupakan teknik penyisipan *watermark* secara digital dan tidak dapat dilihat scara visual. Dalam meyisipkan data secara *invisible* terdapat dua jenis teknik penyisipan yaitu spatial-domain dan frekuensi-domain. Teknik frekuensi domain akan memanfaatkan transformasi gambar pada domain frekuensi diantara metodenya adalah *discrete cosine transformation* (DCT)[8], *discrete wavelet transformation* (DWT) [9] dan lainnya. Jenis penyisipan *watermark* lainnya yaitu berdasar pada *spatio-domain* telah menjadi sangat poluler. Salah satu metode penyisipannya yaitu melalui *least-significant bit* (LSB) dan *histogram-based*.

Metode penyisipan *invisible watermark* dengan memanfaatkan *least-significant bit* (LSB) merupakan metode yang umum digunakan. Pada prinsipnya pesan yang disisipkan berada pada LSB *host image* atau *cover*. Guorong Xuan et al., [6] menggunakan trasformasi *wavelet* dan penyisipkan *threshold* untuk menysipkan data pada gambar digital. Dimana data dimasukkan ke dalam *bit-plane least least* (LSB) dari koefisien *wavelet* integer CDF frekuensi tinggi yang besarnya lebih kecil dari ambang batas yang telah ditentukan sebelumnya. Pada implemenatasinya modifikasi histogram diterapkan sebagai *preprocessing* untuk mencegah *overflow/underflow*. Selanjutnya evaluasi dari hasil percobaan menunjukkan bahwa skema ini lebih unggul dalam bentuk muatan yang lebih besar (pada PSNR yang sama) atau PSNR yang lebih tinggi (dengan muatan yang sama). Dalam penelitian ini masih membutuhkan *cover/host* untuk mengekstrak *watermark*.

Penelitian lain datang dari Ping Wah Wang et.al [5], wang menggunakan konsep LSB dengan mengenalkan dua skema yaitu menggunkan *secret key* dan *public key*. Dalam implementasinya wang berhasil menyisipkan *watermark* dengan tujuan otentikasi dan dan verifikasi kepemilikan suatu karya digital berupa gambar. Dalam penelitiannya Wang et.al menyisipkan 1-bit di LSB sehingga data dan *cover* yang digunakan relative kecil dalam *level grayscale* dan hitam-putih. Dalam penelitian ini sudah memperhatikan keamanan data/*watermark* yang digunakan dan menggunakan skema blind dalam penyisipan *watermarking*.

Fungsi *hash* berfungsi untuk mengkonversi input yang berupa string dengan ukuran yang panjang atau sembarang menuju ukuran panjang data yang fix(tetap), sebagaimana ditunjukan pada persamaan (1). Dalam penelitian ini menggunakan MD5 [7]. Panjang output dari MD5 adalah sekitar 128 bit,

$$H(S) = (d_1, d_2, \dots, d_p) \quad (1)$$

Dimana H adalah fungsi *hash*, S merupakan *string input*, d merupakan output dan p adalah panjang hasil dari fungsi hash.

Dalam penelitian ini kami menyajikan alternaif implemetasi untuk mengamankan karya digital berupa gambar digital dengan menanamkan *watermark* sebagai otentikasi dan validasi serta keabsaan kepemilikan karya digital tersebut. Metode yang digunakan adalah penyisipan LSB sebagaimana yang dijelaskan Wang et.al[5]. Level gambar digital yang akan di ujikan pada level warna(RGB), *Grayscale* ataupun hitam-putih. Skema yang kami gunakan adalah skema *blind* dalam penyisipan *watermark*ing, sehingga tidak memerlukan *cover/host image* pada saat proses ekstraksinya.

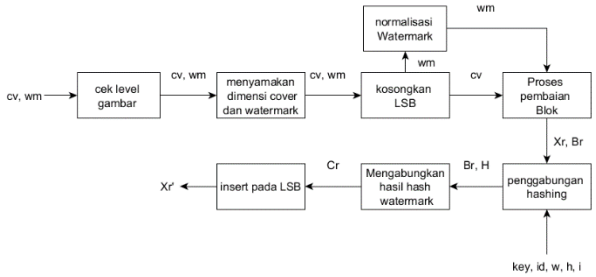
III.METODE

Pada bagian ini akan dijelaskan metode yang digunakan dalam penerapan digital *watermarking* yang diulas dalam jurnal ini. Proses dari digital *watermarking* terbagi menjadi dua bagian yaitu penyisipan *watermarking* dan ekstraksi *watermarking*. Penyisipan *watermarking* digunakan untuk menyisipkan *watermark* yang akan kita gunakan sebagai otentikasi dan validasi kepemilikan karya digital dalam hal ini adalah gambar. Sedangkan ekstraksi *watermarking* digunakan untuk penijauan otentikasi dan validasi kepemilikan karya digital tesebut.

A. Penyisipan *Watermark*

Pada gambar 1, ditampilkan blok diagram penyisipan *watermark*. Pada gambar tersebut terdapat delapan blok proses yaitu cek *level* gambar, meyamakan dimensi gambar, mengosongkan LSB *cover*, normalisasi *watermark*, pembentukan blok per blok, hashing proses, menggabungkan *watermark* dan hasil *hash*, dan terakhir penyisipan LSB. Input dari proses penyisipan *watermark*

adalah cv, wm, dimana cv adalah gambar *cover* atau *host*, dan wm merupakan *watermark* atau logo.



Gambar 1. Global Diagram Penyisipan *Watermark*

Blok cek level gambar digunakan untuk menentukan level gambar yang akan diproses level tersebut terbagi menjadi dua yaitu warna dan *grayscale*, sebagaimana terdapat pada persamaan (3). lv merupakan level gambar, F_{rgb} jika ternyata *cover* berlevel warna dimana gambar akan memiliki 3 *layer*(lr) RGB, sedangkan F_{gry} adalah jika level *cover* berupa *grayscale* memiliki 1 *layer*, persamaan (2). Setiap *layer* baik warna atau *gray level* terdiri dari 2 dimensi (2d).

$$l_{rgb} = 3,\ l_{gry} < 2 \tag{2}$$

$$lv = \begin{cases} F_{rgb}, & sz(cv) \geq lr \\ F_{gry} & \end{cases},\ lr > 1 \tag{3}$$

Pada level warna (l_{rgb}) maka akan proses penyisipan mulai dari proses pembuatan blok dilakukan sebanyak 3 kali sesuai dengan *layer* yang dimiliki.

Blok proses selanjutnya adalah menyamkan dimensi gambar. Hal ini harus dilakukan karena metode yang digunakan adalah penyisipan LSB pada *cover image* sehingga perbedaan dimensi sangat berpengaruh. Dalam menyamakan dimensi antara *cover* dan *watermark* digunakan *threshold static* (th) hal ini disesuaikan dengan kebutuhan program tersebut. Dalam implementasi kami menggunakan dimensi gambar 250 x 250, hal ini dipertimbangkan dari ideal logo yang digunakan. Hal ini ditunjukan pada persamaan (4). Proses selanjutnya adalah mengosongkan LSB *cover*, dimana tempat LSB yang dikosongkan tersebut akan digunakan tempat penyisipan *watermark*, ditunjukkan pada persamaan (5). $rem(cv, \alpha)$ merupakan proses pencarian sisa bagi, sedangkan α merupakan koefisien untuk menentukan berapa sisa bagi yang akan diproses.

$$cv(th_w\ x\ th_w), wm(th_w\ x\ th_w) \tag{4}$$

$$cv = cv - rem(cv, \alpha), \alpha \geq 2 \tag{5}$$

Proses normalisasi *watermark* digunakan untuk mengkondisikan level pixel dari *watermark* sehingga tiap level pixelnya dapat disesuaikan sebagaimana kebutuhan. Proses normalisasi ditunjukan pada persamaan (6).

$$wm = \frac{wm}{\beta},\ \beta \in 2^n \tag{6}$$

Dimana β merupakan koefisiean yang digunakan untuk normalisasi. Panjang bit yang digunakan dapat dilihat dari hasil bagi maksimum F dibagi dengan β, sebagaimana persamaan (7).

$$nBit = \left|\frac{\max(F)}{\beta}\right|, \max(F) \geq 255 \tag{7}$$

Proses pembagian blok dilakukan tidak secara *overlap*, dimensi blok (thb) sebesar 25x25, proses pembagian blok ditunjukan pada persamaan (8) dan (9). Hasil dari pembagian blok tersebut akan digunakan untuk diproses selanjutnya.

$$Xr_{j,k} = \sum_{j=1,k=1}^{n,m} cv_{(j+thb,k+thb)}, j \geq 1, k \geq 1 \tag{8}$$

$$Br_{j,k} = \sum_{j=1,k=1}^{n,m} wm_{(j+thb,k+thb)}, j \geq 1, k \geq 1 \tag{9}$$

$$setBx_i = [Xr_{j,k}, \dots, Xr_{n,m}], i \geq 1 \tag{10}$$

$$setBw_i = [Br_{j,k}, \dots, Br_{n,m}], i \geq 1 \tag{11}$$

Dimana Xr merupakan hasil dari pembentukan blok yang terbentuk dari gambar *cover*, sedangkan Br merupakan hasil dari pembentukan blok yang terbentuk dari gambar *watermark*. Sedangkan $setBx$ dan $setBm$ adalah kumpulan dari blok *cover* dan *watermark*. i, j, k merupakan index dan m, n adalah maksimal index.

Proses penggabungan (*hashing* proses) $H(Xr, Key, id, w, h, i)$ digunakan untuk menyatukan semua informasi penting yang digunakan untuk otentikasi karya digital pada saat ekstraksi *watermark*. Data input yang dibutuhkan pada proses hashing ini diantaranya Xr, key yang diperoleh dari *password* bersifat rahasia, id menggunakan NIM (Nomor Induk Mahasiswa) digunakan sebagai indetitas kepemilikan karya digital, w dan h merupakan lebar dan panjang yang merupakan dimensi gambar, serta i merupakan index dari blok, persamaan (10) dan (11). *Hashing* proses menggunakan MD5[7]. Selanjutnya menggabungkan hasil hash dan *watermark* dengan menggunakan operasi XOR, hal ini ditunjukan dengan persamaan (12).

$$Cr = H(Xr, Key, id, w, h, i) \otimes Br \tag{12}$$

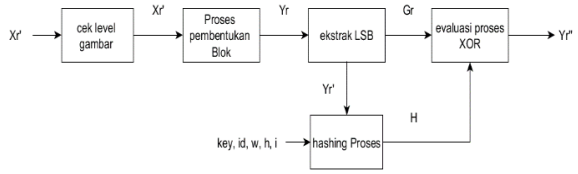
Dimana Cr merupakan hasil gabungan dari hasil hash (H) dan blok dari *watermark* (Br). Proses terakhir adalah penyisipan LSB, dalam proses ini LSB dari *cover* akan diisikan oleh Cr. Xr' merupakan hasil dari penyisipan Cr pada LSB Cover.

B. Ekstraksi *Watermark*

Proses ekstraksi *watermark* terdiri dari beberapa blok proses diantaranya adalah cek level gambar, proses pembentukan blok, ekstraksi LSB, *hashing* proses dan proses evaluasi menggunakan xor operasi. Blok diagaram dari proses ekstraksi *watermark* ditunjukan pada gambar (2).

Input dari proses ekstraksi *watermark* ini adalah gambar yang ter*watermark*. Pada proses pengecekan level gambar bertujuan untuk menentukan level baik itu

warna ataupun *grey level*, sebagaimana yang ditunjukkan pada persamaan (2) dan (3). Proses pembentukan blok digunakan untuk membagi hasil blok menjadi beberapa bagian hal ini digunakan untuk mengevaluasi gambar yang ter*watermark* secara bertahap. Adapun proses pembentukan blok ditunjukkan pada persamaan (13), blok dibentuk dengan ukuran 25 x 25 (th). Dimana Yr adalah blok hasil dari pembagian gambar yang ter*watermark* (Xr').



Gambar 2. Blok Diagram Ekstraksi Watermark

$$Yr_{j,k} = \sum_{j=1,k=1}^{n,m} Xr'_{(j+th,k+th)}, j \geq 1, k \geq 1 \quad (13)$$

Proses selanjutnya adalah ekstraksi LSB, proses ini terdapat dua sub proses yaitu setting nol LSB pada gambar yang ter*watermark* sehingga akan menghasilkan Yr'. Proses mengubah LSB menjadi nol ditunjukan pada persamaan (14).

$$Yr' = Yr - rem(Yr, \alpha), \alpha \geq 2 \quad (14)$$

Sub proses yang kedua adalah ekstraksi LSB yang berfungsi untuk mendapatkan data LSB sesuai dengan koefisien α. Hasil dari ekstraksi LSB adalah Gr. Gr dan Yr' berdimensi sama dengan Yr. Proses ekstraksi ditunjukan pada persamaan (15).

$$Gr = Yr \wedge \theta, \ \theta \geq 1 \quad (15)$$

Dimana θ adalah koefisien yang akan menjadi *operand* untuk di operasikan terhadap Yr. Besaran θ disesuaikan dengan besar LSB yang akan digunakan. Pada penelitian ini θ sebesar 3, penentuan θ ditunjukan pada persamaan (16)

$$\theta = \sum_{p=0}^{nBIt-1} 2^p, p \geq 0 \quad (16)$$

Proses penggabungan (*hashing* proses) secara konsep sama seperti pada penyisipan *watermark*. Hashing proses $H(Yr', Key, id, w, h, i)$ digunakan untuk menyatukan semua informasi penting yang digunakan untuk otentikasi karya digital pada saat ekstraksi *watermark*. Data input yang dibutuhkan pada proses hashing ini diantaranya Yr', key yang diperoleh dari *password* bersifat rahasia, id menggunakan NIM (Nomor Induk Mahasiswa) digunakan sebagai indetitas kepemilikan karya digital, w dan h merupakan lebar dan panjang yang merupakan dimensi gambar, serta i merupakan index dari blok, persamaan (17).

$$setBy_i = [Yr'_{j,k}, \dots, Yr'_{n,m}], i \geq 1 \quad (17)$$

Selanjutnya menggabungkan hasil hash dan *watermark* dengan menggunakan operasi XOR untuk mendapatkan *watermark*, yang merupakan hasil evaluasi proses. Hal ini ditunjukkan dengan persamaan (18).

$$Yr'' = H(Yr', Key, id, w, h, i) \otimes Gr \quad (18)$$

IV. HASIL DAN PEMBAHASAN

Gambar yang digunakan dalam pengujian adalah gambar yang berwarna dan graylevel pada 2 gambar *cover/host* dan 4 gambar logo/*watermark*, ditunjukkan pada gambar (3) dan (4). Ukuran dari masing-masing gambar sebesar 250x250 pixel. *Secret key* berisi huruf, angka dan simbol dalam tipe data string, sedangkan id diambil dari NIM (Nomor Induk Mahasisa) yang bertipe data integer dengan panjang 8 sampai 10-digit. Parameter koefisien α = 8, β = 128, dan θ = 128.

Performansi evaluasi kualitas *watermark* dan hasil gambar *cover* yang ter*watermark* diukur dengan menggunakan *Peak Singal to Noise Ratio*(PSNR), persamaan dari PSNR ditampilkan pada persaman (19). PSNR merupakan perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR diukur dalam satuan desibel. Sedangkan MSE(*Mean Square Error*) merupakan nilai *error* kuadrat rata-rata antara dua gambar, dalam hal ini adalah gambar *cover* dan gambar yang ter*watermark*. Peritungan matematis dari MSE ditunjukan pada persaman(20).

$$PSNR = 10 \log \frac{255^2}{MSE} \quad (19)$$

$$MSE = \sum_{i=1,j=1}^{N-1,M-1} \frac{|CV(i,j) - Xr'(i,j)|}{NxM} \quad (20)$$

Dimana N dan M adalah dimensi dari gambar, sedangkan cv adalah gambar *cover* dan Xr' adalah gambar yang ter*watermark* dan i, j merupakan index. Untuk gambar yang memiliki level warna (RGB) maka PSNR akan diproses sebanyak layer yang dimiliki, Hal ini ditunjukkan pada persamaan(21).

$$PSNR_{rgb} = \frac{\sum_{i=1}^{lr} 10 \log \frac{255^2}{MSE_i}}{lr} \quad (21)$$

Dimana lr merupakan banyak layer yang dioperasikan.

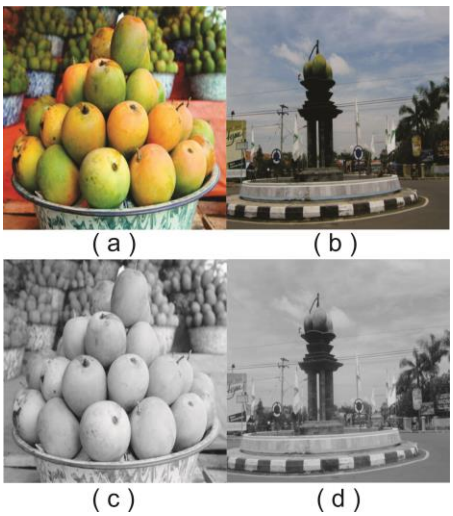
(a) (b) (c) (d)

(e) (f) (g) (h)

Gambar 3. *Watermark* : (a) logo1, (b) logo2, (c) logo3, (d) logo4, (e) logo5, (f) logo6, (g) logo7, (h) logo8.

Pada tabel diatas menunjukkan nilai PSNR rata-rata sebesar 34.08 dengan MSE rata sebesar 14.62. Nilai tersebut menujukkan kualitas gambar hasil *watermark*

mengalami penurunan. Hal ini didapat dari perbandingan antara original *cover/host* dan gambar yang ter*watermark*.



Gambar 4. Cover/Host: (a) cover1, (b) cover2, (c) cover3, (d) cover4

Gambar 5. Tampilan Aplikasi Validasi Gambar Digital

Tabel 1. Hasil Pengukuran

Host	*Watermark*	PSNR	MSE
Cover1	logo1	31.67	14.70
	logo2	31.62	14.86
	logo3	31.63	14.84
	logo4	31.77	14.36
Cover2	logo1	31.71	14.56
	logo2	31.66	14.74
	logo3	31.67	14.72
	logo4	31.80	14.24
Cover3	logo5	36.45	14.68
	logo6	36.40	14.86
	logo7	36.44	14.72
	logo8	36.55	14.32
Cover4	logo5	36.47	14.58
	logo6	36.42	14.76
	logo7	36.46	14.65
	logo8	36.56	14.29
Rata-rata		**34.08**	**14.62**

V. PENUTUP

Kesimpulan

Dalam penelitian ini kami menajikan penerapan *digital watermarking* sebagai validasi keabsahan *file multimedia* (gambar digital) dengan menggunakan skema *blind watermark*. Proses penyisipan *watermark* dilakukan dengan metode LSB yang mana panjang digit LSB yang kami gunakan adalah sebanyak 2-bit LSB. Pada penelitian ini menggunakan dua level gambar yaitu gambar warna dan gambar berlevel *grayscale*. Hal ini menjadi suatu alternatif penyisipan *invisible watermark* pada gambar dengan level warna secara spasial dengan mempertimbangkan beberapa koefisien sebagaimana telah dipaparkan pada bagian II. Hasil dari penelitian ini menunjukkan kualitas gambar yang ter*watermark* mengalami penurunan namun tidak signifikan, ditunjukan dengan nilai PSNR dan MSE relatif rendah. Keberhasilan melakukan ekstraksi *watermark* pada gambar, memudahkan proses otentikasi dan validasi kepemilikan gambar digital dengan diwakili oleh *key* yang berupa *password* dan id yang merupakan nomor unik dari pemilik gambar. Meskipun demikian hasil eksraksi gambar masih mengalami penurunan kualitas yang signifikan.

Saran

Kami menyarankan sebagai pengembangan penelitian selanjutnya yaitu memperbaiki kualitas hasil ekstraksi *watermark* yang mana dapat dimulai dengan peningkatan jumlah bit LSB dan memperhatikan proses normaslisasi *watermark* pada proses penyisipan dan ekstraski *watermark*. Selain itu dapat dikombinasikan dengan metode-metode yang berdomain frekuensi. Selanjutnya meningkatkan fungsional dan penanganan file multimedia yang dapat di operasikan.

VI. DAFTAR PUSTAKA

[1] S. Lagzian, M. Soryani, M. Fathy, "A New Robust *Watermark*ing Scheme Based on RDWT-SVD", International Journal of Intelligent Information Processing, vol. 2, no. 1, pp. 22-29, 2011.

[2] F. Hartung, M. Kutter, "Multimedia *watermark*ing techniques", Proc. IEEE, vol. 87, pp. 1079-1107, July 1999.

[3] A. Sverdlov, S. Dexter, A.M. Eskicioglu, “Robust DCT-SVD Domain Image *Watermark*ing For Copyright Protection: Embedding Data In All Frequencies”, Proceedings of the 13th European Signal Processing Conference (EUSIPCO2005), Antalya, Turkey, September 2005.

[4] V.M. Potdar, S. Han, E. Chang, "A Survey of Digital Image *Watermark*ing Techniques", Proc. IEEE International Conference on Industrial Informatics, Aug. 2005.

[5] Secret and Public Key Image *Watermark*ing Schemes for Image Authentication and Ownership Verification.

[6] Guorong Xuan, Yun Q. Shi & Chengyun Yang “Lossless Data Hiding Using Integer Wavelet Transform and Threshold Embedding Technique” 0-7803-9332-5/05/$20.00 ©2005 IEEE.

[7] R. L. Rivest, “The MD5 message digest algorithm,” Tech. Rep., 1992.
[8] N. Divecha and D. N. N. Jani, "Implementation and performance analysis of DCT-DWT-SVD based *watermark*ing algorithms for color images," International Conference on Intelligent Systems and Signal Processing (ISSP), pp. 204-208, 2013.
[9] J. Guru, H. Dhamecha and B. Patel, "Fusion of DWT and SVD digital *watermark*ing Techniques for robustness," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 9, pp. 791-797, 2014.