Teknik Watermarking Menggunakan Shifting LSB Untuk Proteksi Dokumen Dalam Dunia Pendidikan

by Wasilah Wasilah

Submission date: 18-Jan-2022 03:14PM (UTC+0900)
Submission ID: 1743375467
File name: Semnas_Teknik_Watermaking_menggunakan_shifting_LSB.pdf (976.8K)
Word count: 2554
Character count: 15850

Teknik Watermarking Menggunakan Shifting LSB Untuk Proteksi Dokumen Dalam Dunia Pendidikan

Wasilah[1], Dona Yuliawati[2]

[1,2]Ilmu Komputer IBI Darmajaya
Jl. Z.A Pagar Alam No.93, Bandar Lampung
Email: silamurni@gmail.com, donayuliawati@gmail.com

ABSTRAK

Kejahatan yang terjadi saat ini telah merambah disegala bidang kehidupan. Hal ini terjadi dimana saja dalam kehidupan sehari-hari dan tidak terbatas pada kejahatan fisik maupun material. Kejahatan yang dilakukan juga pada pelanggaran hak cipta atau *copy right* dan pemalsuan tanda tangan. Penelitian kali dimaksudkan untuk mengatasi atau mencegah terjadi kejahatan-kejahatan tersebut.

Dengan menggunakan teknik *watermarking*, penelitian ditujukan untuk memperkenalkan teknik atau cara baru untuk melindungi keaslian suatu dokumen yang secara cepat bisa mendeteksi apakah suatu dokumen telah dipalsukan. Aplikasi watermarking tersebut dilakukan dengan menyisipkan citra atau text yang secara spesifik menjadi pengaman bagi suatu dokumen.

Penelitian ini diharapkan dapat membatu banyak pihak dalam dunia pendidikan, baik sebagai pengelola jasa pendidikan maupun pihak lain yang terkait sebagai pengguna.

Key Word: *watermarking*, pendidikan, hak cipta

1. Pendahuluan

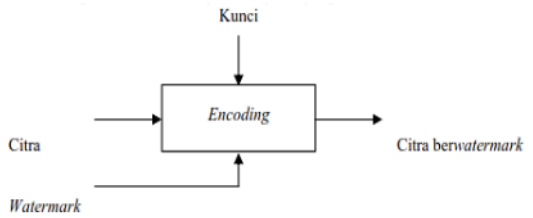
Permasalahan pelanggaran kepemilikan hak cipta tak akan pernah selesai dan akan menjadi lebih rumit ketika kepemilikan citra digital dipertanyakan pemilik sebenarnya, pemalsuan surat-surat berharga yang berdampak sangat merugikan. Oleh karena itu perlindungan terhadap surat-surat berharga sangat diperlukan. Untuk mengatasi masalah ini maka perlu dibuat suatu teknik sekaligus aplikasi proteksi hak cipta yang mampu melindungi hak cipta seseorang dari pemalsuan terhadap dokumen-dokumen penting.

Di bidang pengolahan citra atau image processing pemalsuan atau plagiarism dapat ditanggulangi dengan banyak teknik diantara teknik *watermarking*, *image blending*, dan teknik *content based i mage ret rieval.* Teknik water marking dikerjakan dengan cara menyisipkan kedalam data citra tersebut. Watermark dapat dianggap sebagai sidik digital (*digital signature*) dari pemilik sah atas produk multimedia tersebut. Dengan demikian, watermark yang disisipkan menjadi hak cipta dari pemiliknya. Pemberian penandaan dalam sebuah dokumen dengan teknik watermarking ini dilakukan sedemikian sehingga informasi yang disisipkan tidak merusak data digital yang dilindungi. Sehingga orang yang membuka produk multimedia yang sudah disisipkan watermark tidak menyadari kalau didalam data multimedia tersebut terkandung label atau *signature* kepemilikan pembuatnya. Beberapa penelitian terdahulu membuktikan *Watermarking* berbasis *SVD* dengan kuantisasi *Dither* dan deteksi sisi, dapat digunakan untuk menghasilkan citra-citra yang telah dimodifikasi dengan berbagai teknik [5]. Sedangkan pada penelitian lain, Metode Watermarking di Implementasikan dengan metode Removal DC pada DC pada audio digital yang disisipkan citra biner dengan software.[6]. Untuk penelitian berikutnya untuk metode digital Watermarking pada citra berwarna dengan metode berbasis korelasi Discreate Cosine Transform(DCT), dengan membandingkan sebuah nilai-ambang.[7]. Pada peneltian berikutnya Metode watermarking menggunakan *adaptive Digital Image Wa termarking*. Cara menyisipkan citra digital dapat mengetahui identitas pemilik asli dari citra digital tersebut sehingga dapat melakukan proteksi terhadap citra digital.[8]

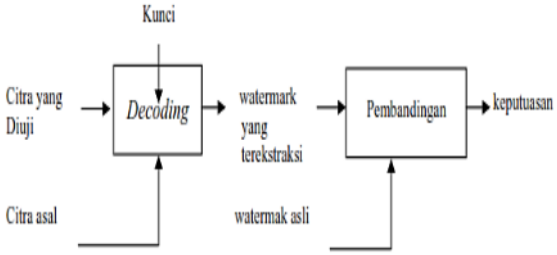
Implementasi watermarking dalam proteksi dokumen terkait dengan dunia pendidikan ini dilakukan mengunakan metode *Least S ignificant Bit* (LSB), yang dapat digunakan untuk menyisipkan ”sandi” berupa citra sebagai watermark kedalam citra digital yang lain. “sandi” yang disisipkan tidak terlihat oleh mata dan tidak merubah citra aslinya [3]

2. Proses Watermarking

Proses penyisipan *watermark* ke dalam citra disebut *encoding. E ncoding,* proses dapat disertai dengan pemasukan kunci atau tidak memerlukan kunci [2]. Kunci diperlukan agar *watermark* hanya dapat diekstraksi oleh pihak yang sah. Kunci juga dimaksudkan untuk mencegah *watermark* dihapus oleh pihak yang tidak berhak.



Gambar 1. Proses *Watermark* pada Citra *Digital*



Gambar 2. Proses *Verification* pada Citra *Digital*

Verifikasi watermark dilakukan untuk membuktikan status kepemilikan citra digital yang disengketakan. Verifikasi watermark terdiri dari dua sub-proses, yaitu ekstraksi watermark dan pembandingan. Proses ekstraksi watermark disebut juga decoding, bertujuan mengungkap watermark dari dalam citra. Decoding dapat mengikut sertakan citra asal atau tidak sama sekali, tujuannya adalah untuk meningkatkan kinerja yang lebih baik. Proses pembandingan bertujuan untuk membandingkan watermark yang diungkap dengan watermark asli dan memberi keputusan tentang watermark tersebut.

2.1. Digital Watermarking

Digital w atermarking adalah teknik untuk menyisipkan informasi tertentu kedalam sebuat data dengan suatu cara tertentu sehingga watermark itu sulit dirusak dan dihapus [1]. Secara garis besar, watermark terbagi menjadi dua tipe, yaitu *visible watermar k* dan *invisible watermark* , berikut penjelasan kedua tipe[3].

- *Visible watermark, W atermark* jenis ini dapat terlihat olehindera manusia. *Visible watermark* bersifat sangat *robust* karena keberadaan watermark dapat dikenali dengan mudah dan biasanya sangat sulit untuk dihapus.Watermark yang disisipkan dapat bersifat *solid* ataupun semitransparan, dan untuk memindahkannya membutuhkan *cropping* yang signifikan.

- *Invisible w atermark, W atermark* jenis ini tidak dapat terlihat oleh indera manusia, tetapi dapat diekstraksi dengan metode komputasional tertentu. Tujuan dari *invisible watermark* adalah untuk memverifikasi kepemilikan atau memverifikasi integritas dari suatu citra atau sejumlah informasi. Biasanya pada saat ekstraksi *invisible watermar king* dibutuhkan sebuah password yang disebut watermark key.

*2.2.Least Significant Bit Hiding (*LSB*)*

Suatu Citra dapat didefinisikan sebagai fungsi *f(x,y)* berukuran M baris dan N kolom, dengan x dan y adalah koordinat spasial, dan amplitude *f* di titik kordinat *(x,y)* dinamakan intetitas atau tingkat keabuan dari citra pada titik tersebut. Apabila nilai *x* dan *y,* dan nilai Amplitudo *f* secara keseluruhan berhingga (*finite*) dan bernilai diskrit maka dapat dikatakan bahwa citra tersebut citra digital. Nilai Pada suatu irisan antara baris dan kolom (pada posisi *x,y*) disebut sebagai *picture element atau, i mage ele ments atau pels atau pixels [9].*

Metode *LSB (Least S ignificant Bit)* merupakan salah satu metode watermarking yang bekerja dalam mode warna *RGB* (*Red*, *Green*, *Blue*). Metode ini bekerja dengan cara menyisipkan informasi pada bit-bit paling kanan dari setiap elemen RGB. Perubahan bit paling kanan hanya menimbulkan perubahan nilai *RGB* sebesar 1 dari 256 warna yang ada. Metode LBS secara langsung memanipulasi nilai intensitas dari sejumlah *pixel*. Penyembunyian data dilakukan dengan mengganti bit-bit data di dalam segmen citra dengan bit-bit data rahasia. Pada susunan di dalam sebuah *byte* (1 *byte* = 8 bit), ada bit yang kurang berarti disebut bit LSB. Bit *LSB* inilah yang akan dimanipulasi untuk penyisipan *watermark* [4].

2.3.Operasi pergeseran citra

Operasi pergeseran citra pada perancangan ini digunakan dalam melakukan peletakan *watermark* atau citra tanda agar dapat sesuai dengan apa yang dikehendaki. Berikut adalah persamaan yang digunakan pada pergeseran *watermark*:

$$Y_{step} = Y_{old} + S_y;$$

$$X_{step} = X_{old} + S_x;$$

Dengan mengunakan persamaan diatas akan didapatkan sebuah koordinat baru peletakan nilai pixel suatu citra. Dalam penelitian ini persamaan diatas digunakan sebagai pengatur peletakan posisi *watermark* pada citra. Dan satuan yang digunakan untuk S_y dan S_x adalah pixel. Jika S_y bernilai 5 maka citra akan bergeser 5 pixel ke atas, jika S_x bernilai 3 maka citra akan bergeser 3 pixel ke kanan, sedangkan jika S_x dan S_y bernilai negative arah pergeserannya akan berlawanan.

Algoritma pemutaran citra dengan mengunakan *transformasi affin e* ini digunakan sebagai pemutar citra tanda pemutaran dilakukan dengan mengunakan persamaan berikut.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos(\text{rad}) & \sin(\text{rad}) \\ -\sin(\text{rad}) & \cos(\text{rad}) \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Dengan mengunakan persamaaan diatas suatu citra akan dapat dirotasi sesuai dengan radian. Sehingga jika ingin memutar citra 45° maka nilai radian adalah $\pi/4$ radian. Algoritma penskalaan citra

Suatu citra dapat diperbesar ataupun diperkecil dengan membuat setiap piksel menjadi beberapa piksel. Pada penelitian ini penskalaan citra dilakukan dengan mengunakan rasio. Rasio didapatkan dari perbandingan tinggi dan lebar dari citra dengan tempat menampilkan citra (*viewer*). Berikut persamaan rasio tinggi dan lebar :

$$S_h = Viewer_h / H \quad (3\text{-}4)$$
$$S_w = Viewer_w / W \quad (3\text{-}5)$$

Rasio tinggi S_h didapatkan dari pembagian tinggi *viewer* dengan tinggi asli citra, sedangkan rasio lebar didapatkan dari pembagian lebar *viewer* dengan lebar asli citra.

3. Hasil

Dalam penelitian ini dihasilkan algoritma yang merupakan penyempurnaan dari algoritma-algoritama yang telah dibangun sebelumnya, Secara umum alagoritma aplikasi dapat dijelaskan sebagai berikut:

\\ mengembunyikan citra pada citra

1. *Input citra asli*
2. *Convert citra ke vector*
3. *Conver vektor to binary*
4. *Convert text to vector*
   mat= m x n matix
   Extract RGB component
   End
5. *Go to 1*

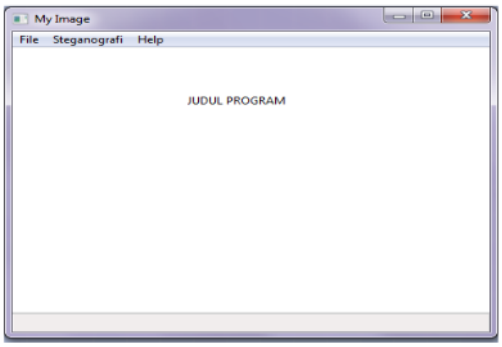
\\ mengembalikan citra yang disembunyikan pada citra

1. *Convert hided image into vector*
2. *Conver vector to binary*
3. *Take the most rigth bit from each vector n*
4. *Make number of power of 8 from step 3*
5. *Contruct RGB each pixel*

Aplikasi yang dihasilkan sangat berguna untuk menyembuyikan citra logo kedalam dokumen untuk melindungi keaslian dari dokumen tersebut. Beberapa output dari hasil pengujian terhadap aplikasi yang dihasilkan dapat dilihat pada gambar berikut ini:

3.1.1.Tampilan Program

Pada menu awal program ketika dijalankan adalah terdiri dari 3 menu yaitu file, steganografi dan help. Adapun tampilan menu awal program tersebut ditampilkan pada gambar 3 berikut ini :

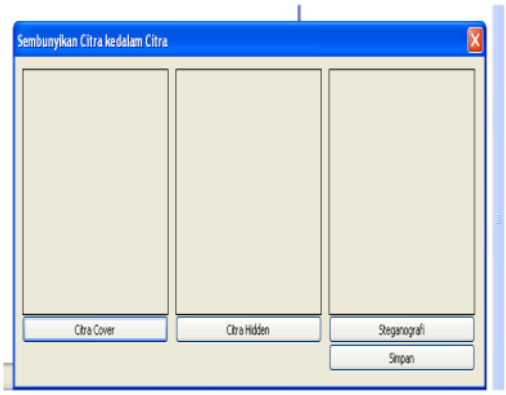


Gambar 3. Tampilan Menu Awal

3.1.2. Tampilan Menu Steganografi

Menu steganografi merupakan fasilitas proses watermarking. Dilakukan dengan menentukan citra cover berformat png, jpg dan bmp, lalu pilih citra hiden/yang akan disembunyikan. Kemudian tekan tombol

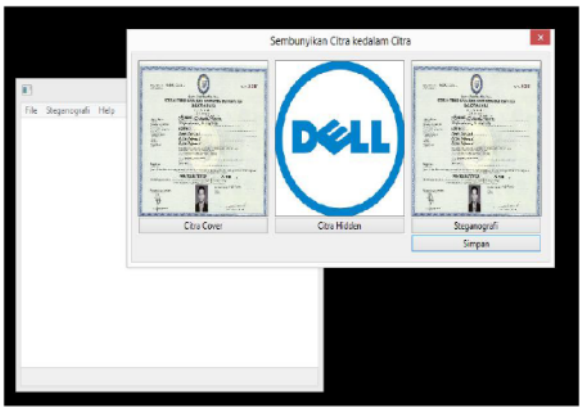
steganografi, maka akan muncul citra baru yang mengandung pesan tersembunyi. Kemudian citra tersebut dapat disimpan kedalam format .png dan .bmp. Pada menu stenografi tersebut terdapat 3 tahapan seperti ditunjukkan pada gambar 4 berikut ini :



Gambar 4. Menu Steganografi

3.1.3..Output Penyisipan Citra Kedalam Dokumen

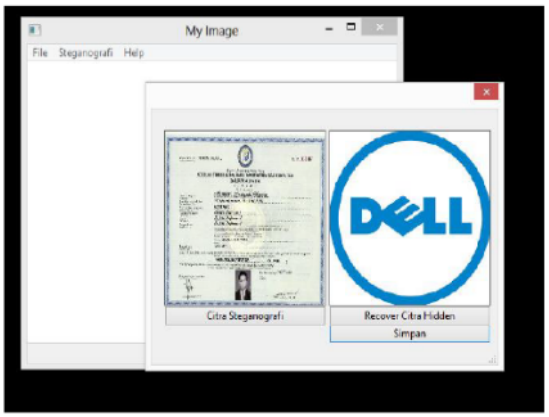
Tampilan penyisipan watermark berupa citra kedalam dokumen ditampilkan pada gambar 5 berikut ini :



Gambar 5. Snapshot menyisipan/menyembunyikan logo kedalam dukomen

3.1.4. Output Hasil Ekstraksi Watermark Citra

Watermark berupa citra yang telah disisipkan sebelumnya, dapat diekstrak kembali. Hasil ekstaraksi Citra dari dalam dokumen ditampilkan pada gambar 5 berikut ini:



Gambar 6: Snapshot memunculkan kembali logo yang disembunyikan dalam dokument

Proses Ekstraksi dilakukan dengan memilih citra steganografi (yang sebelumnya telah diinsertkan citra watermark), Dokumen tersebut berformat png dan bmp tekan tombol recover citra hidden, maka selanjutnya akan muncul citra yang disembunyikan. Kemudian citra tersebut dapat disimpan kedalam format .jpg, .png dan .bmp.

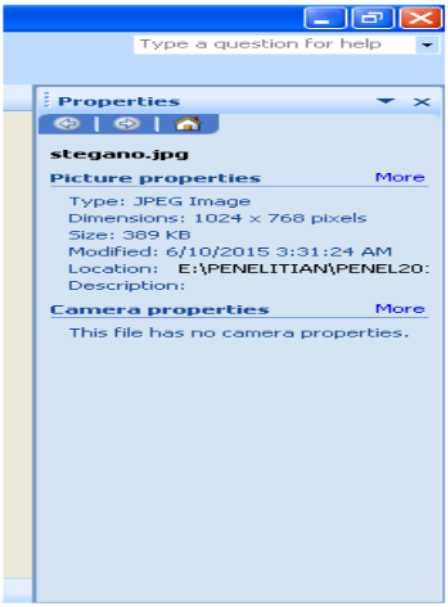
3.2. Pembahasan

Fasilitas penyisipan dan ekstraksi dapat dimanfaatkan untuk mendeteksi watermark dalam suatu dokumen. Penandaan dapat berupa gambar, atau logo. Citra selanjutnya akan di sembunyikan kedalam bentuk vector. Jika yang disembunyikan adalah text maka bentuk matriknya 1 x n-text. Citra memiliki bentuk matrik m-citra x n-citra. Diketahui m-citra adalah baris citra dan n-citra adalah kolom citra. Selanjutnya ambil nilai intensitas pixel nya berupa merah, hijau dan biru. Selanjutnya akan diubah nilai vector yang disembunyikan kedalam binary citra yang disembunyikan di masukkan kedalam biner citra cover secara berurutan dengan cara melihat nilai bit terkecil dari citra cover dan nilai biner ke n dari citra yang disembunyikan. Dalam penelitian ini adalah document text dan gambar yang kemudian discan sehingga menjadi gambar dengan format JPEG,png dan bmp.

Demikian pula halnya pada proses ekstraksi akan dilakukan tahapan pengubahan nilai matriks citra yang memiliki nilai disembunyikan ke dalam bentuk vector. Selanjutnya ubah nilai vector yang ada kedalam binary, ambil nilai bit paling kanan dari masing-masing vector biner ke –n, Jadikan bilangan desimal setiap kelipatan 8 dari rangkaian biner yang dihasilkan dan selanjutnya disusun menjadi format RGB per pixel.

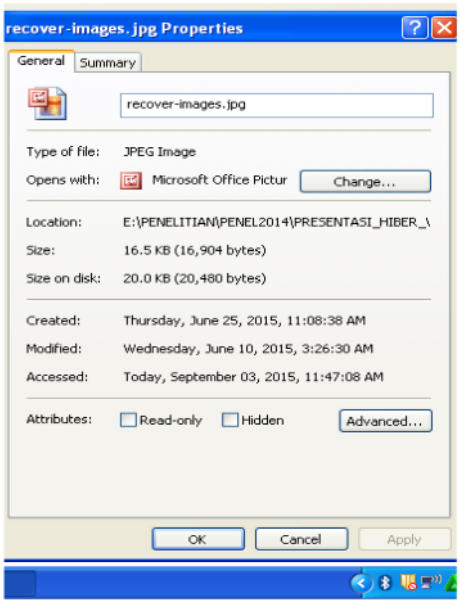
Pada proses penyisipan citra kedalam dokumen dilakukan dengan menentukan citra cover berformat png, jpg dan bmp, lalu menentukan citra hiden/yang akan disembunyikan. Dari proses penyisipan/steganografi, maka akan muncul citra baru yang mengandung pesan tersembunyi. Kemudian citra tersebut dapat disimpan kedalam format .png dan .bmp. Pengujian dilakukan untuk melihat kehandalan atau robustnes dari aplikasi ini. Berdasarkan hasil pengujian menujukan bahwa jika watermark yang disisipkan kedalam dokumen, akan terdapat perubahan terhadap dokumen cover dan watermark .

Selain itu proses pengukuran kinerja system yang dihasilkan dilakukan terhadap ukuran file. Dalam menganalisa ukuran file dilakukan dengan membandingkan ukuran dokumen sumber, ukuran citra yang akan disisipkan dan ukuran hasil *steganografi*. Adapun hasil perbandingan dilakukan terhadap file yang sama akan tetapi dengan format yang berbeda, yaitu format file Jpeg, Bmp, Png. File sumber, file citra hidden dengan format Jpeg ditunjukkan pada gambar 7 berikut ini :



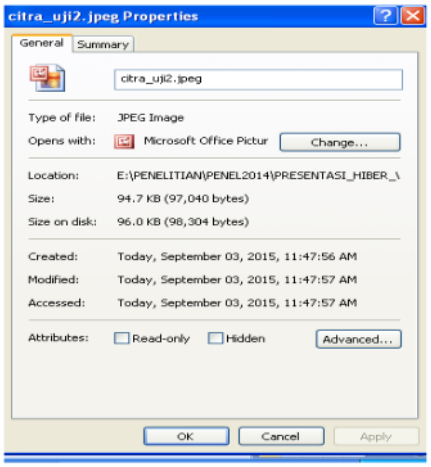
Gambar 7: Tampilan Ukuran File Sumber

Pada file sumber berukuran 389 Kb tersebut dilakukan penyisipan citra berukuran 16,5 Kb seperti ditampilkan pada gambar 8 berikut ini:



Gambar 8: Tampilan Ukuran File Citra Hidden.

Hasil dari penggabungan file citra berformat Jpeg tersebut adalah steganografi dengan ukuran file 94,7 Kb.



Gambar 9: Tampilan Ukuran File Steganografi.

Selain dilakukan terhadap file berformat Jpeg, pengujian dilakukan pula terhadap file berformat Bmp dan Png. Adapun penggabungan tersebut menghasilkan ukuran file yang berbeda-beda besarannya seperti ditunjukkan pada tabel 1 berikut ini :

File sumber		File Mark		File Hasil	
Jenis	Size	Jenis	Size	Jenis	Size
Jpeg	389 Kb	Jpeg	16.5 Kb	Jpeg	94.7 Kb
Jpeg	389 Kb	Jpeg	16.5 Kb	Bmp	2.25Mb
Jpeg	389 Kb	Jpeg	16.5 Kb	Png	975Kb

Tabel 1 menunjukkan bahwa dari ukuran file yang dihasilkan dengan menggabungkan file yang sama akan tetapi penyimpanan hasil dengan format file/ekstensi yang berbeda akan menghasilkan ukuran file yang berbeda.

Dalam proses ekstraksi citra steganografi yang dipilih berformat png dan bmp, selanjutnya dilakukan proses recover citra hidden, maka akan muncul citra yang disembunyikan dan citra hasil tersebut dapat disimpan kedalam format .jpg, .png dan .bmp.

4. Simpulan

Aplikasi yang dihasilkan menyediakan dua proses yaitu proses penyisipan watermark dan proses ekstraksi. Proses penyisipan watermark dilakukan dengan tahapan: Input citra asli, mengkonversi citra kedalam bentuk vector , selanjutnya bentuk vektor dikonversi ke binary, Masukan biner citra yang disembunyikan kedalam biner citra cover secara berurutan. Selanjutnya dilakukan proses pengubahan nilai biner yang baru ke dalam desimal dan bentuk ke dalam vector citra baru

Dokumen yang telah diberi *watermark*, dapat di *recover* melalui proses ekstraksi yaitu mengembalikan citra yang disembunyikan pada citra. Hal ini dilakukan dengan dilakukan dengan tahapan : mengkonversi yang menjadi *watermark* ke dalam bentuk vektor, selanjutnya vector akan dikonversi kedalam bentuk binary. Bedasarkan hasil konversi tersebut selanjutnya diambil nilai bit paling kanan dari masing-masing vector biner ke –n. Jadikan bilangan desimal setiap kelipatan 8 dari biner yang dihasilkan, selanjutnya dilakukan proses penyusunan menjadi format RGB per pixel.
Adanya *watermark* yang disisipkan pada sebuah dokumen berharga dalam dunia pendidikan berupa ijazah, sertifikat, piagam, dan lain-lain diharapkan dapat membantu memudahkan pihak yang berkepentingan untuk mendeteksi keaslian dokumen dalam dunia pendidikan. Hal tersebut diharapkan dapat membantu meningkatkan keamanan *(security)* dokumen sehingga dapat terjaga dari kepemilikan yang tidak syah.

Hasil pengujian menunjukkan bahwa steganografi yang dihasilkan dari penggabungan file sumber berformat Jpeg dan file citra hidden berformat Jpeg menghasilkan ukuran file terkecil dari jenis penyimpanan file steganografi lainnya yaitu Bmp dan Png. Dengan demikian hasil steganografi dengan Jpeg tersebut dapat berdampak pada efisiensi penggunaan media penyimpanan (*Storage*).

Daftar Pustaka

[1] Ajay Goel,O.P.Sahu , Ajay Goel 2011. Improved Digital Watermarking Techniques and Data Embedding In Multimedia. .CyberJournalsMultidisciplinaryJournalsinScienceand Technology,Vol. 02, No. 02, 2010, 164-168

[2] Dugelay J. L., , S. Roche, C. Rey, G. Doërr. 2006. Still-image water-marking robust to local geometric distortions.IEEE Trans. on Image Proc., vol. 15, no. 9, Pp. 2831-2842.

[3] Ema Utami.2009. Pendekatan Metode Least Bit Modification Untuk Merancang Aplikasi Steganography Pada File Audio Digital Tidak Terkompresi. Jurnal Dasi. Vol. 10 No. 1, Issn: 1411-3201

[4] Onkar Dabeer, Kenneth Sullivan, And Upamanyu Madhow. 2007. Detection Of Hiding In The Least Significant Bit. IEEE Transactions On Signal Processing, Vol. 52, No. 10

[5] Rahmatri Madiko, T Basaruddin. *Evaluasi Ske ma Watermarking C itra Ber basis Singular V alue Decomposition, Kuantisasi Dith er, Dan Det eksi Sisi*. Makara, Sains. 2010; Vol.14 No.2: 168-172

[6] Ronal Hadi. Studi dan Evaluasi *WatermarkingAudio Digital* Dengan Metode *Removal DC.* Electron : ISSN:2085-6989. 2010; Vol.2 No.2: 33-43

[7] Rinaldi Munir. *Image Wa termarking Untuk Citra Berwarna D engan Metode Berba sis Ko lerasi Da lam Ranak DCT*. Jurnal Petir: 2010: Vol.3 No.1

[8] Ryanti Irviantina, Sunario Megawan, Jonni,. Aplikasi Teknik Adaptive Digital Image Watermarking Untuk Proteksi Hak Cipta Citra Digital. JSM STMIK Mikroskil: ISSN.1412-0100: 2015 vol 16 No 1: 113-123

[9] Russ C. John. 2011. The Image Processing Handbook, Sixth Edition Hardcover. CRC Press, 6th edition.

Teknik Watermarking Menggunakan Shifting LSB Untuk Proteksi Dokumen Dalam Dunia Pendidikan

ORIGINALITY REPORT

19%	17%	7%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

2%

★ fmipa.unmul.ac.id

Internet Source

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		

Teknik Watermarking Menggunakan Shifting LSB Untuk Proteksi Dokumen Dalam Dunia Pendidikan

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6