TEKNIK STEGANOGRAFI DENGAN METODE *DISCRETE COSINES TRANSFORM (DCT)* PADA CITRA *INTERPOLASI BILINEAR* UNTUK PENGAMANAN PESAN

Garno[1], Arip Solehudin[2]
[1,2]*Jurusan Informatika, Fakultas ILMU KOMPUTER, Universitas SINGAPERBANGSA Karawang*
Jl.H.S. Ronggowaluyo Telukjambe Timur Karawang 41361
E-mail : garno@staff.unsika.ac.id[1], arip.solehudin@gmail.com[2]

Abstract—This study discusses the security of data by inserting messages on a media image or steganography, previous research is still a lot of message insertion in the form of text only sentence and some use txt format file, Current research content of messages can be some important files that have various formatting extensions such as doc, docx, pdf, compressed files such as rar. The contents of each file also have a text only and there is also a mixture with pictures and formulas and all have different capacities, so in this study realize the insertion of messages with steganography technique with discrete cosine transformation (DCT) method performed on the image processed interpolation bilinear first. The study contributed to enlarge the insertion capacity as a capacity by using a technique of combining DCT method techniques and bilinear interpolation. The results of the study have various combinations of test results of some standard performance test results on Imperectibility test successfully extracted, Fidelity successfully extracted, Robustness failed extracted and Recovery successfully extracted. The success in the category is less good, because it gets the level of accuracy with MSE worth 8.35 but the value of PSNR of 27.87 dB.

Abstrak—Penelitian ini membahas tentang keamanan data dengan penyisipan pesan pada suatu media gambar atau steganografi, penelitian sebelumnya masih banyak penyisipan pesan berupa *text* kalimat saja dan beberapa menggunakan *file* berformat *txt*. Penelitian saat ini isi pesan dapat berupa beberapa *file* penting yang memiliki *format extension* bermacam-macam seperti *doc, docx, pdf, file* terkompres seperti *rar*. Isi dari setiap *file* juga ada yang *text* saja dan ada juga campuran dengan gambar dan rumus dan semuanya memili kapasitas berbeda-beda, maka pada penelitian ini merealisasikan penyisipan pesan dengan teknik steganografi dengan metode *discrete cosine transformation* (DCT) yang dilakukan pada citra yang diproses interpolasi *bilinear* terlebih dahulu. Penelitian memberikan kontribusi untuk memperbesar kapasitas penyisipan sebagai daya tampung dengan menggunakan teknik penggabungan antara teknik metode DCT dan *interpolasi bilinear*. Hasil dari penelitian memiliki barbagai kombinasi hasil uji beberapa standar hasil pengujian performansi pada uji *Imperectibility* berhasil diekstrak, *Fidelity* berhasil diekstrak, *Robustness* gagal diekstrak dan *Recovery* berhasil diekstrak. Keberhasilan dalam kategori kurang baik, karena mendapatkan tingkat akurasi dengan MSE senilai 8.35 namun nilai PSNR sebesar 27.87 dB.

Kata Kunci—steganografi, kriptografi, discrete cosine transformation (DCT), *interpolasi bilinear*, *watermarking*, *Information hidding*.

PENDAHULUAN

Keamanan data merupakan hal yang penting, informasi yang terdapat terdapat pada data tersebut menjadi bersifat apakah rahasia atau biasa, beberapa instansi atau badan usaha juga kebanyakan memerlukan informasi penting tersebut dan menginginkan pihak lain atau kompetiter tidak mengetahuinya, contoh informasi yang penting tersebut dapat berupa resep suatu perusahaan badan usaha yang bersifat baik rutin atau berkala, data rekam medis klinik atau rumah sakit, ada juga laporan keuangan suatu badan usaha juga hal yang penting dan bersifat privat, untuk metode keamanan data banyak tekniknya, salah satunya adalah penyembunyian data pada media tertentu atau dalam bahasa asing disebut *Information hidding.*

Information hidding sebagai teknik diantara salah satu keamanan data yang didalamnya merupakan teknik penyembunyian data yang bersifat rahasia kedalam media lain sehingga keberadaan data rahasia tersebut tidak diketahui atau disadari adanya oleh orang lain, didalam *information hidding* terdapat beberapa metode diantaranya ada metode *convert channels*, metode *steganography*, metode *anonymity*, metode *copyright marking*. Teknik *steganography* didalamnya ada *linguistic steganography* dan *technical steganography*. Klasifikasi teknik steganografi terdapat dua kategori yaitu *watermarking* dan *steganography*[12].

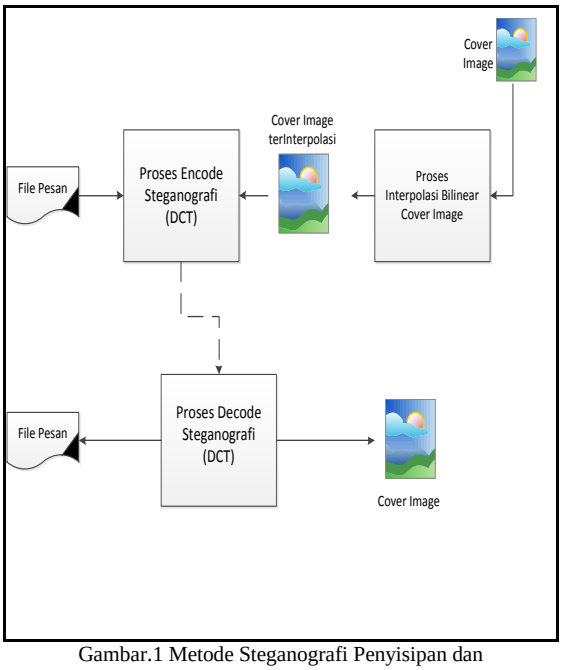
Steganography (*covered writing*) didefinisikan sebagai ilmu dan seni untuk menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia[5]. Steganografi secara teknik sama dengan *watermarking*, namun berbeda hal tentang sisi yang dianggap pentingnya, yaitu hal yang disisipkanlah yang menjadi dominasi penting, dan media untuk penyisipannya tidak menjadi objek yang

dianggap penting, arti dari hal yang disisipkan tersebut adalah dapat berupa pesan atau yang lain dan bersifat rahasia[2].

Teknik steganografi dari Penelitian sebelumnya masih banyak penyisipan pesan berupa *text* kalimat saja dan beberapa menggunakan *file* berformat *txt*, beberapa penelitian belum memiliki hasil bahwa penyisipan pesan berupa suatu *file* dengan kapasitas yang lebih besar, isi pesan dapat berupa beberapa *file* penting yang memiliki *format extension* bermacam-macam seperti *doc, docx, pdf, file* terkompres seperti *rar*, isi dari setiap f*ile* juga ada yang *text* saja dan ada juga campuran dengan gambar dan rumus serta semuanya memiliki kapasitas berbeda-beda, pada penelitian ini akan menggunakan dimensi *image* asal sebelum dilakukan *interpolasi*/pembesaran 256 x 256 *pixels*. Beberapa penelitian lain banyak melakukan kombinasi secara analisis seperti dalam jurnal-jurnal terbaru menggunakan metode-metode yang ada, kususnya dengan model penggabungan teori matematik. Pada penelitian inovasi ini penulis akan menggabungkan teknik steganografi dengan model penyisipannya menggunakan teori matematik *descrete cosine transform* yang dipadukan dengan model teori matematik *interpolasi bilinear*.

I. METODE PENELITIAN

Teknik yang menjadi metode dari proses steganografi berawal dari penyiapan media sebagai *cover image* untuk dilakukan proses *zooming* yaitu dengan teknik model *interpolasi bilinear*, kemudian dijadikan sebagai media/wadah untuk menyisipkan pesan, dan teknik penyisipannya menggunakan metode (*Discrete Cosine Transform*) DCT. Adapun metode secara arsitektur dapat digambarkan sebagai berikut:



Gambar.1 Metode Steganografi Penyisipan dan Ekstrak Pesan

A. *Proses Interpolasi*

Teknik interpolasi pada penelitian akan dipergunakan untuk memperbesar media yang akan dipergunakan sebagai wadah dalam penyisipan pesan, teknik interpolasi yang dipergunakan akan mengadopsi model teknik *bilinear interpolasi* yang memiliki metode meningkatkan atau merenggangkan jumlah *pixels* pada gambar digital

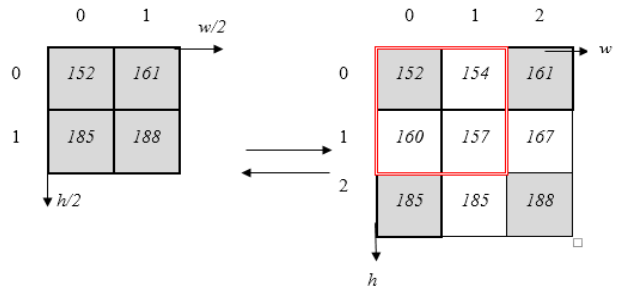
$$f(x,y) \approx \frac{f(Q_{11})}{(x_2-x_1)(y_2-y_1)}(x_2-x)(y_2-y)+ \frac{f(Q_{12})}{(x_2-x_1)(y_2-y_1)}(x_2-x)(y_2-y)+ \frac{f(Q_{21})}{(x_2-x_1)(y_2-y_1)}(x_2-x)(y_2-y)+ \frac{f(Q_{22})}{(x_2-x_1)(y_2-y_1)(x_2-x)(y_2-y)}$$

.....(1)

Simulasi metode interpolasi dengan teknik interpolasi untuk proses *zooming* citra/*image* maka terjadi perbesaran *image* dan perubahan *pixels* sebagai berikut:

$$C(i,j) = \begin{cases} I(i,j), & if\ i=2m, j=2n, \\ (I(i\text{-}1,j)+(I(i\text{-}1,j)+I(i+1,j))/2)/2, & if\ i=2m, j=2n+1, \\ (I(i\text{-}1,j)+(I(i\text{-}1,j)+I(i+1,j))/2)/2, & if\ i=2m+1, j=2n, \\ (C(i\text{-}1,j)+C(i,j\text{-}1))/2, & \text{jika tidak} \end{cases}$$

..(2)



$$154 = \{ 152 + \frac{(152+161)}{2} \} / 2$$

$$160 = \{ 152 + \frac{(152+185)}{2} \} / 2$$

$$157 = \frac{(154+160)}{2}$$

$$167 = \{161 + \frac{(161+188)}{2} \} / 2$$

$$185 = \{185 + \frac{(185+188)}{2} \} / 2$$

B. *Proses Encode*

Teknik steganografi yang menggunakan DCT (*discrete cosines transform*) dilakukan dengan transformasi yang mengubah suatu sinyal menjadi unsur komponen frekuensi. Penyembunyian pesan terjadi apabila *file* yang digunakan untuk pesan di*input* dan proses penyembunyian pesan siap dieksekusi dengan cara tahap pertama yaitu merubah media

menjadi matrik 8x8 dengan dilanjutkan proses kuantisasi dan proses *entropi coding*.
Dari hasil tersebut didapatkan perubahan frekuensi yang memiliki nilai tinggi dari kiri atas sampai kanan bawah tetapi ukuran sama. Dari bentuk itulah kemudian penyisipan pesan dapat dilakukan pada bagian frekuensi yang memiliki nilai 0, -1dan 1. Adapun proses DCT dapat dilihat pada rumus persamaan berikut:

$$S(u,v) = C(u)C(v)\sum_{x=0}^{n-1}\sum_{y=0}^{m-1} S(x,y)\cos\left[\frac{\pi(2x+1)u}{2n}\right]\cos\left[\frac{\pi(2y+1)v}{2m}\right] \quad (1)$$

dengan $u = 0, 1, ..., n - 1$ dan $v = 0, 1, ..., m - 1$

$$C(u) = C(v) = \begin{cases} \sqrt{\frac{1}{n}} & untuk \quad u = v = 0 \\ \sqrt{\frac{2}{n}} & untuk \quad lainnya \end{cases}$$

…….(3)

S(u, v) : Data pada domain frekuensi
S(x, y) : Data pada domain ruang
u, v : Koordinat pixels untuk blok transformasi
x, y : Koordinat pixels untuk citra sebelum transformasi.
C (u) : Nilai dari koefisien domain transformasi pada koordinat u
C (v) : Nilai dari koefisien domain transformasi pada koordinat u
n : Jumlah baris dalam blok yang akan ditransformasikan
m : Jumlah baris dalam blok yang akan ditransformasikan

C. *Proses Decode*

Proses *decode* digunakan untuk mengembalikan atau mengeluarkan pesan menggunakan teknik *invers* dari DCT atau sering disebut IDCT dengan teknik komponen frekuensi diubah kembali menjadi suatu sinyal. Adapun proses IDCT dapat dilihat pada rumus persamaan berikut:

$$S(x,y) = \sum_{u=0}^{n-1}\sum_{v=0}^{m-1} S(u,v)C(u)C(v)\cos\left[\frac{\pi(2x+1)u}{2n}\right]\cos\left[\frac{\pi(2y+1)v}{2m}\right] \quad (2)$$

dengan $x = 0, 1, ..., n - 1$ dan $y = 0, 1, ..., m - 1$

$$C(u) = C(v) = \begin{cases} \sqrt{\frac{1}{n}} & untuk \quad u = v = 0 \\ \sqrt{\frac{2}{n}} & untuk \quad lainnya \end{cases}$$

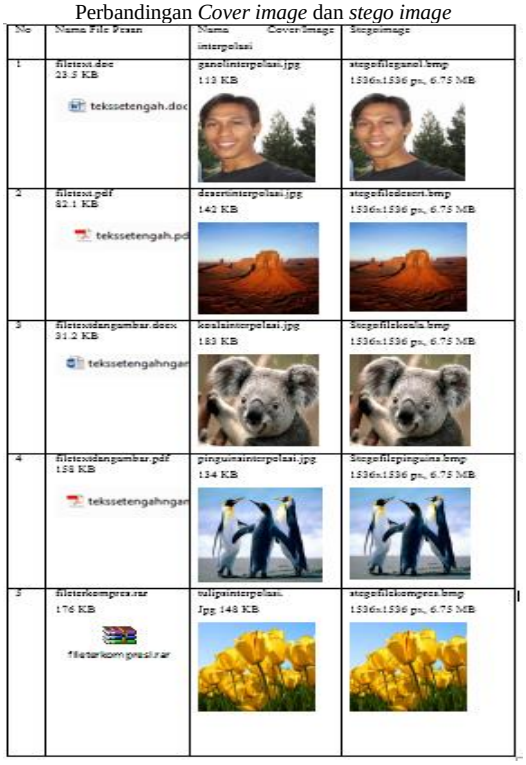
….(4)

II. HASIL DAN PEMBAHASAN

A. *Penyisipan pesan kedalam cover image*

Pada penyisipan pesan kedalam *cover image* yang telah terinterpolasi dengan berbagai bentuk pesan seperti *file* pesan ber*format extention doc, docx, pdf* dan *rar*. Isi dari setiap *file* pesan beraneka dari yang berisi *file text* saja, *text* dan gambar serta dalam *file* pesan *rar* ada *doc* dan *pdf*. Berikut tabel 1 Perbandingan *cover* asli dan hasil penyisipan *file* pesan kedalam *cover image* yang disebut *stegoimage*.

Tabel 1.
Perbandingan *Cover image* dan *stego image*



Rata-rata dari semua hasil pengujian penyisipan *file* pesan kedalam *cover image* atau sering disebut proses *encode* menjadi *stego image* semua mengalami perubahan kapasitas seperti tabel 2 berikut:

Tabel 2.
Penyisipan Pesan ke *Cover Image*

No	**Nama *File* Pesan**	**Nama *Cover/Image* interpolasi**	***Stegoimage***
1	filetext. doc 23.5 KB	ganolinterpolasi. jpg 113 KB	stegofileganol.b mp 1536x1536 px, 6.75 MB
2	filetext. pdf 82.1 KB	desertinterpolasi .jpg 142 KB	stegofiledesert.b mp 1536x1536 px, 6.75 MB
3	filetextdang ambar.docx 31.2 KB	koalainterpolasi. jpg 183 KB	Stegofilekoala.b mp 1536x1536 px, 6.75 MB
4	filetextdang ambar.pdf 158 KB	pinguinsinterpol asi.jpg 134 KB	Stegofilepinguin s.bmp 1536x1536 px, 6.75 MB
5	fileterkompr es.rar 176 KB	tulipsinterpolasi. jpg 148 KB	stegofilekompres .bmp 1536x1536 px, 6.75 MB

B. Ekstrak pesan dari stegoimage

Hasil ekstraksi pesan dari *stegoimage* melalui proses *decode* pada pengujian dapat dilihat dari tabel hasil ekstrak berikut:

Tabel 3.
File Hasil Ekstrak dari *Stegoimage*

Hasil proses *decode*/ekstrak untuk mengembalikan *file* pesan yang semula berada didalam *stegoimage* rata-rata berhasil sempurna, seperti yang diterangkan dalam tabel berikut:

Tabel 4
Daftar *file* hasil ekstrak/*decode*

No	***StegoImage***	***File* Pesan hasil *Decode***
1	stegofileganol.bmp 1536x1536 px, 6.75 MB	tekssetengah.doc 23.5 KB
2	stegofiledesert.bmp 1536x1536 px, 6.75 MB	teksetengah.pdf 82.1 KB
3	stegofilekoala.bmp 1536x1536 px, 6.75 MB	tekssetengahgambar.docx 31,2 KB
4	stegofilepinguins. bmp 1536x1536 px, 6.75 MB	tekssetengahgambar.pdf 158 KB
5	stegofilekompres. bmp 1536x1536 px, 6.75 MB	fileterkompresi.rar 176 KB

C. *Pengukuran kualitas secara objektif*

Pengukuran kualitas secara objektif dari citra hasil *stegoimage* pada aspek *fidelity* dengan pengujian mengukur setiap *image* asal dengan *image* hasil steganogarafi/ *stegoimage*. Adapun hasil uji pengukuran kualitas sebagai berikut:

Tabel 5.
Uji Aspek *Fidelity*

No	Citra Cover	Stegoimage	Akurasi
1	ganol.jpg 	stegofileganol.bmp 	MSE 36.22 PNSR 32.54 dB
2	desert.jpg 	stegofiledesert.bmp 	MSE 1.47 PNSR 26.43 dB
3	koala.jpg 	Stegofilekoala.bmp 	MSE 1.36 PNSR 26.79 dB
4	penguins.jpg 	Stegofilepinguins.bmp 	MSE 1.33 PNSR 26.88 dB
5	tulips.jpg 	stegofilekompres.bmp 	MSE 1.39 PNSR 26.71 dB

Berdasarkan tabel 5 hasil uji objektif aspek *fidelity* dari 5 kali pengujian pada setiap *cover image* terhadap *stegoimage* memiliki rata-rata MSE 8.35 dan PSNR seniali 27.87 dB.

III. KESIMPULAN DAN SARAN

A. *Kesimpulan*

Dari hasil pengujian pada teknik steganografi dengan *discrete cosines transform* (DCT) pada citra yang terinterpolasi dapat dapat menjawab hipotesis diawal penelitian yaitu bahwa aplikasi yang dibangun dapat meng*embed* data pesan yang besar seperti *doc, docx, pd*f ke dalam *cover image* bahkan dapat menampung *file* kompres *rar* yang isinya *file doc* atau *docx* serta *pdf*, semakin besar kapasitas *file* pesan yang diselipkan/*embed* maka memerlukan *cover image* sebelum diinterpolasi juga semakin besar dan proses *encode* memerlukan waktu yang lama, proses pengembalian ekstraksi data berjalan dengan mengeluarkan *file rar, doc, docx* dan *pdf* dari *cover image* dengan proses yang disebut *decode*.

Kapasitas *file cover image* yang memiliki dimensi 256 x 256 *pixels* adalah 41.46 KB dan dilakukan proses interpolasi memiliki rata-rata dimensi sebesar 1536 x 1536 *pixels* berkapasitas rata-rata menjadi 144 KB. Proses *embed file* ke dalam *cover* yang terinterpolasi dengan rata-rata besar file 94.16 KB meningkat menjadi 6.75 MB. Pengujian aspek *fidelity* memiliki rata-rata PNSR 27.87 dB dan rata-rata MSE 8.35. Nilai yang memiliki *Peak Signal to Noise Ratio* (PSNR) memiliki nilai kemaksimuman dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal belum mencapai 40 dB sehingga memiliki kategori kurang baik, namun memiliki nilai MSE (*Mean Square Error*) yang cukup kecil.

B. *Saran.*

Berdasarkan simpulan di atas maka dapat diusulkan beberapa saran demi menunjang penelitian selanjutnya yaitu kebutuhan *user* pada penggunaan teknologi informasi menuntut penggunaan yang fleksibel dan praktis yaitu salah satunya perangkat berbasiskan *mobile*, maka dalam penelitian berikutnya diharapkan untuk meneliti yang dapat *compatible* perangkat *mobile* agar dapat diimplementasikan. Penelitian ini belum mempertimbangkan aspek kecepatan maka diharapkan untuk penelitian berikutnya untuk menerapkan aspek kecepatan agar memiliki nilai manfaat yang lebih baik.

DAFTAR PUSTAKA

[1] Aditya, Y., A. Pratama, dan A. Nurlita, 2010, Studi Pustaka untuk Steganografi dengan Beberapa Metode, Jurnal , Fakultas Teknologi Industri UII.

[2] Batarius Patrisius, Martinus Maslim, 2012, Perbandingan Metode Dalam Teknik Steganografi, Seminar Nasional Teknologi Informasi & Komunikasi Terapan, ISBN 979-26-0255-0, Semarang, 23 Juni 2012

[3] Cahyo Darujati, 2014. Magnifikasi Perbaikan Citra Dijital Multi Resolusi dengan Metode Gabungan Tapis Lolos Bawah dan Interpolasi Bilinear. Jurnal ilmiah mikrotek vol. 1, no.2.

[4] Channalli, S., & Jadhav, A. (2009). Steganography An Art of Hiding Data, 1(3), 137–141. http://doi.org/10.3923/itj.2004.245.

[5] Della Babya. 2014, A Novel DWT based Image Securing Method using Steganography, International Conference on Information and Communication Technologies (ICICT 2014), Department of Electronics &Communication Engineering, SJCET Palai, Kerala, India.

[6] Ki-Hyun Jung, Kee-Young Yoo. 2014, Steganographic method based on interpolation and LSB substitution of digital images, reasearchgate.

[7] Munir, Rinaldi. 2006. Kriptografi. Informatika, Bandung.

[8] Morkel, T., JHP. Eloff, dan MS. Olivier. 2005, An Overview of Image Steganography. Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, Pretoria.

[9] Nailul Mustaqim Abdi dkk. 2011, Peningkatan Kualitas Citra Digital Menggunakan Metode Super Resolusi Pada Domain Spasial Jurnal Rekayasa Elektrika Vol. 9, No. 3, April 201.
[10] Nosrati, M., Karimi, R., & Hariri, M. (2011). An introduction to steganography methods. World Applied Programming, 1(3), 191–195. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:An+introduction+to+steganography+methods#1.
[11] Parmenter, D. ,2010. Mengembangkan, Mengimplementasikan dan Menggunakan Key Performance Indicators, Jakarta: PPM.
[12] Sahar A. El Rahman, 2016. A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information, Journal Computers and Electrical Engineering 000 (2016) 1–20, https://doi.org/10.1016/j.compeleceng.2016.09.001.
[13] Thévenaz, P., Blu, T., & Unser, M. (n.d.). Image Interpolation and Resampling, 1–39.