PENGEMBANGAN APLIKASI STEGANOGRAFI *PIXEL VALUE DIFFERENCES* (PVD)

MuhamadAzhari
ktob34@yahoo.com
Program StudiIlmuKomputer FMIPA UniversitasMulawarman

ABSTRAK

Steganografi merupakan teknik yang digunakan dalam proses pengiriman pesan rahasia. Sebuah file *cover* digunakan sebagai medium untuk menyembunyikan pesan rahasia tersebut. Pada penggunaan medium citra sebagai *cover*proses penyembunyian pesan dilakukan dengan cara mengganti setiap bit-bit piksel citra *cover*dengan bit-bit pesan rahasia. LSB (*Least Significant* Bit) merupakan metode yang kerap digunakan yaitu dengan cara mengantikan bit-bit pada posisi LSB *cover* dengan bit-bit pesan rahasia.Peningkatkan daya tampung pesan dan pengurangan tingkat distorsi pada steganografi telah dilakukan dengan dikembangkannya teknik PVD (*Pixel Value Differences*). Pada teknik tersebut sebelum bit-bit pesan disisipkan ke dalam LSB *cover*, terlebih dahulu citra *cover* dibagi menjadi blok-blok piksel yang tidak saling tumpang tindih (*non-overlapping pixel blocks*). Setiap blok berisi dua piksel yang saling berdekatan. Kemudian, selisih nilai kedua piksel tersebut digunakan untuk menentukan besarnya bit pesan yang dapat disisipkan. Selisih piksel yang besar dapat menampung banyak pesan demikian sebaliknya selisih yang kecil maka hanya dapat ditampung pesan yang sedikit.
Algoritma yang ada pada teknik steganografi PVD dapat dikembangkan menjadi sebuah aplikasi dengan menggunakan pemrograman Matlab.Aplikasi ini diperlukan dalam rangka mengimplentasikan teknik PVD. Ujicoba yang dilakukan dengan menggunakan citra *cover* dan pesan berupa citra 24 bit membuktikan bahwa aplikasi yang dikembangkan dapat digunakan dalam proses penyisipan dan ekstraksi pesan. Selain itu*Peak Signal Noise Ratio* (PSNR) dapat diukur dengan aplikasi tersebut sehingga besaran distorsi yang dihasilkan pada proses penyisipan pesan dapat diketahui.

Kata kunci: Steganografi, PVD, Matlab

Pendahuluan

Kejahatan informasi kerap terjadi saat ini, terutama dalam proses pengiriman pesan. Teknik pengamanan tidak bisa hanya mengandalkan pada keamanan fisik namun perlu juga ditunjang dengan teknik-teknik keamanan informasi yang bersifat non-fisik (Guritman 2003). Oleh karena itu pada proses pengiriman pesan sangatlah memerlukan teknik pengamanan yang baik.

Dua teknik yang umum dikenal dalam pengiriman pesan rahasia yaitu kriptografi dan steganografi. Perbedaan pada kedua teknik tersebut yakni pada kriptografi pesan rahasia diacak dengan sebuah algoritma enkripsi (pengacakan) terlebih dahulu sebelum pesan tersebut dikirim. Akibatnya pesan berubah menjadi kode-kode yang tidak dimengerti oleh pihak-pihak yang tidak berhak membacanya.

Adapun pada steganografi kerahasiaan pesan terhadap pihak yang tidak berhakdilakukan dengan cara menyembunyikannya pada sebuah media yang disebut *cover*. Jika sebuah file *cover*telah disisipi pesan dan siap untuk dikirim maka file tersebut disebut *stego image*.LSB merupakan teknik steganografi yang banyak digunakan namun teknik ini memiliki kelemahan. Apabila pesan yang disembunyikan dalam jumlah besar maka stegoimage yang dihasilkan akan mengalami distorsi (Amirtharajan 2010). Perbaikan terhadap teknik LSB dilakukan dengan menggunakan teknik PVD. Cara kerja teknik PVD adalah dengan cara membagi citra cover menjadi blok-blok piksel yang tidak saling tumpang tindih (*nonoverlapping block*) (Wu, 2003). Blok-blok tersebut terdiri dari dua buah pixel yang posisinya berdekatan. Besarnya

bit pesan yang akan disisipkan ditentukan dengan besarnya selisih kedua piksel tersebut. Apabila selisih kedua piksel tersebut besar maka bit pesan yang disisipkan berjumlah besar dan apabila selisihnya kecil maka bit pesan yang disisipkan berjumlah kecil.

Berdasarkan hal tersebut teknik steganografi PVD perlu diimplementasikan dalam sebuah aplikasi. Algoritma penyisipan dan ekstraksi pesan yang ada dijadikan acuan dalam pengembangan aplikasi tersebut. Sementara itu, aplikasi yang dikembangkan juga akan digunakan untuk mengukur besaran distorsi (PSNR) yang kerap muncul dalam proses penyisipan pesan.

Metode

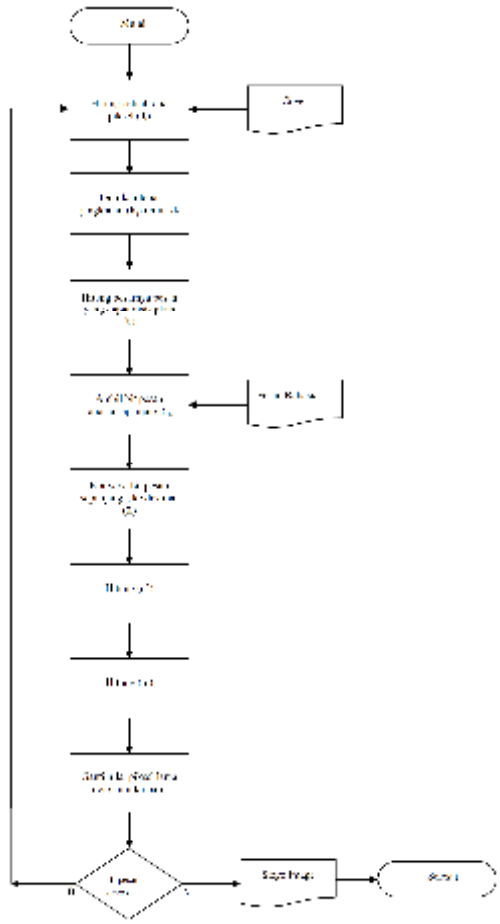
AlgoritmaPenyisipan Pesan

Padateknik steganografi PVD proses penyisipan pesan dilakukan dengan cara membagi-bagi piksel pada citra*cover* menjadi pasangan-pasanganyang saling berdekatan dan tidak saling menumpuk (*nonoverlapping block pixel*). Jumlah bit pesan yang disisipkan bergantung pada selisih setiap pasang piksel tersebut. Sebuah tabel jangkauan digunakanuntukmenentukanbanyaknya bit yang akandisisipkan.Tabeljangkauan yang digunakanpadapenelitianyaitusepertiyang tampakpadaTabel 1.

Tabel 1 Bit yang dapat disisipkan pada tiap daerah rentang

Rentang	1	2	3	4	5	6
lb (batas bawah)	0	8	16	32	64	128
ub (batas atas)	7	15	31	63	127	255
ti (jumlah bit yang disisipkan)	3	3	4	5	6	7

Jika selisih pasangan dua pixel bernilai antara 0 sampai 7 maka penyisipan berada pada rentang R_1 , sehingga aplikasi akan menyisipkan 3 bit pesan kedalam bit cover. Selisih sebesar 8 sampai 15 berada pada rentang R_2 , pesan yang disisipkan sebesar 3 bit. Pada R_1 dan R_2 ditetapkan bit pesan yang dapat disisipkan sebesar 3 bit. Pada rentang R_3dengan selisih piksel antara 16 sampai 31 dapat disisipkan pesan sebesar 4 bit. Rentang R_4dengan nilai selisih antara 32 dan 63 pesan yang disisipkan sebesar 5 bit, rentang R_5 sebesar dengan selisih antara 64 dan 127 pesan disisipkan sebesar 6 bit. Pada rentang terakhir, rentang 6 dengan selisih piksel sebesar 128 sampai 255 maka pesan yang disisipkan sebesar 7 bit.Proses penyisipan pesan dalam *cover* dijelaskan seperti diagram alir padaGambar 1.



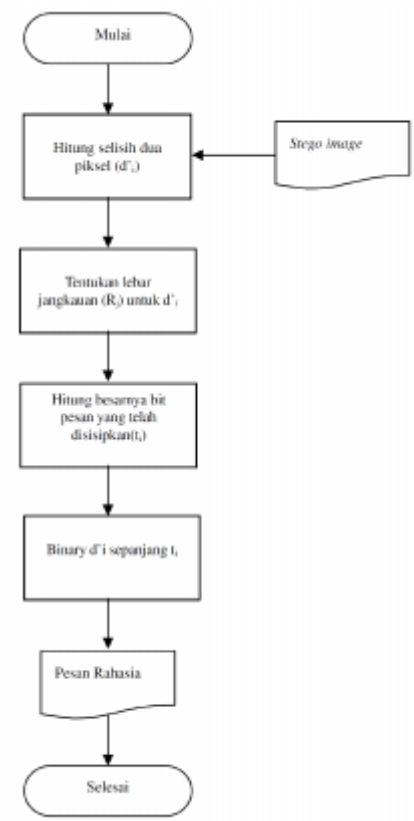
Gambar 1 Diagram alir proses penyisipanpesan

AlgoritmaEkstraksi

Algoritmayang digunakan untuk pengembangan menu *extracted message* (pengambilan pesan) tampakpada diagram alirGambar 2.Pengambilan pesan diawali dengan menginput *stego image*. Kemudian dari setiap *layerstego image* dua piksel yang berdekatan (g_x, g_{x+1}) dihitung selisihnya, masing-masing disimpan dalam 3 variabel yang mewakili layer *red*, *green* dan *blue*. Nilai selisih tersebut kemudian dimutlakkan *(absolute value)* yang dihitung sebesar *dxabs*.

Mengacu kepada tabel jangkauan dapat ditetapkan rentang area dari nilai *dxabs* tersebut. Seperti pada proses penyisipan pesan, demikian pula pada pengambilan pesan digunakan juga tabel jangkauan yang memiliki lima daerah rentang yang sama. Pada setiap iterasiyang menghitung selisih dua piksel berdekatanpada

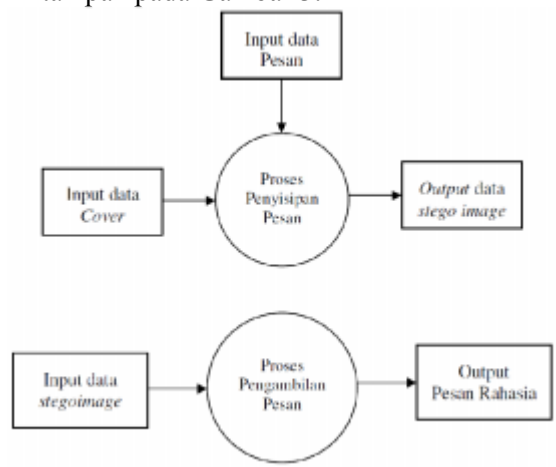
stego image, rentang-rentangpada tabel jangkauan digunakan untuk menentukan besarnya bit pesan yang telah disisipkan pada dua piksel *stego image*. Perhitungan *tistego* dimulai dengan menghitung w_j yaitu mengurangkan batas atas dengan batas bawah rentang *(uj-lj+1)*. Kemudian dilakukan operasi *log* terhadap w_j yang hasilnya merupakan besarnya *tistego* maka hasil operasi *log* terhadap $w_j$ditetapkan jika selisih piksel 0 sampai 7 dan 8 sampai 15 dapat disisipkan 3 bit pesan, selisih 16 sampai 31 disisipkan 4 bit, selisih 32 sampai 63 disisipkan 5 bit, selisih 64 sampai 127 disisipkan 6 bit dan selisih 128 sampai dengan 255 disisipkan 7 bit (Tabel 1).



Gambar 2 Diagram alir proses pengambilanpesan

Perancangan Aplikasi

Aplikasi dirancang terdiri dari dua menu yang masing-masing digunakan untuk melakukan proses penyisipan *(embedded)*dan pengambilan *(extract)*pesan. Sebagai data input *cover*dan pesannya berupa image berformat bmp dengan mode RGB.Rancangan aliran data pada proses penyisipan pesan dilakukan dengan menginput data *cover* dan pesan rahasia yang ingin disembunyikan. Proses penyisipan pesan tersebut akan menghasilkan data output *stego image*. Pada proses pengambilan pesan, rancangan aliran data dimulai dengan menginput data *stego image* kemudian dilakukanlah proses ekstraksi dengan menghasilkan output data berupa pesan rahasia yang disembunyikan pada cover. Kedua proses ini tampak pada Gambar 3.

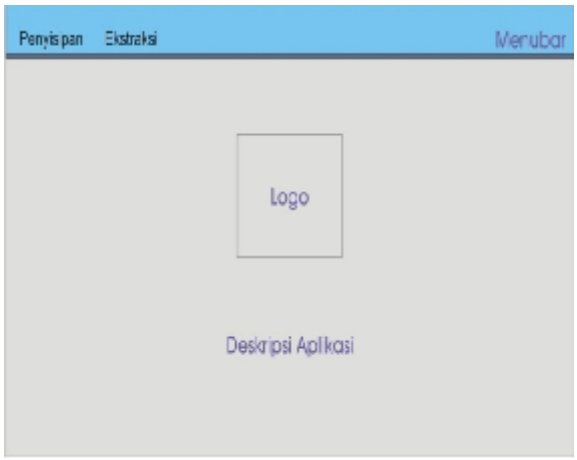


Gambar 3 Aliran data aplikasisteganografi PVD

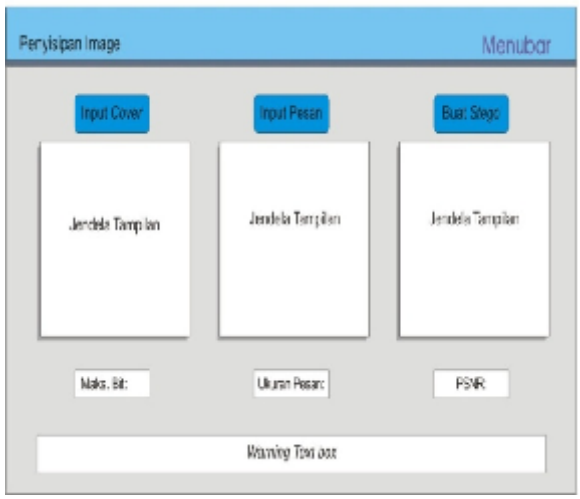
Antarmuka Grafis (GUI)

Perancangan GUI untuk aplikasi ini keseluruhan terdiri dari halaman depan, menu penyisipan pesan, dan menu pengambilan pesan *image*. Halaman depan merupakan halaman tampilan pertama aplikasi. Pada menu *bar* halaman depan terdapat menu penyisipan pesan dan pengambilan pesan. Pada menu penyisipan pesan *User* dapat memilih *file* yang dijadikan *cover* dan pesan. Kedua *file* tersebut secara visual akan ditampilkan pada layar *interface*. Tombol *build stego* digunakan untuk menyisipkan pesan ke dalam cover sekaligus menyimpan *filestego image* ke dalam memori dan menampilkannya pada jendela tampilan. Aplikasi ini juga akan menampilkan jumlah maksimal bit pesan dimiliki sebuah *cover*, nilai PSNR, dan besarnya ukuran pesan yang disisipkan.

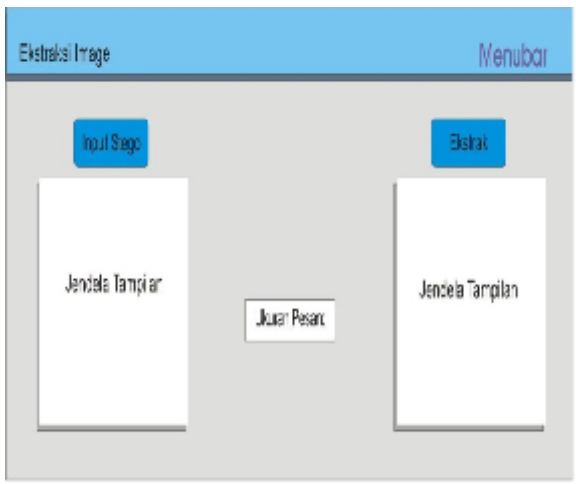
Pada menu pengambilan pesan proses ekstraksi dilakukan dengan menginput *filestego image*. *User* diminta untuk memasukan ukuran pesan untuk mengambil pesan rahasia. Ukuran panjang baris dan kolom pesan digunakan untuk mengambil pesan yang disembunyikan. Proses ekstraksi pesan selain menampilkan pesan pada jendela tampilan sekaligus menyimpan file ekstraksi pesan ke dalam memori. Gambar 4, 5, dan 6 merupakan *layout* dari GUI pada aplikasi steganografi PVD.



Gambar4*Layout* halaman depan.



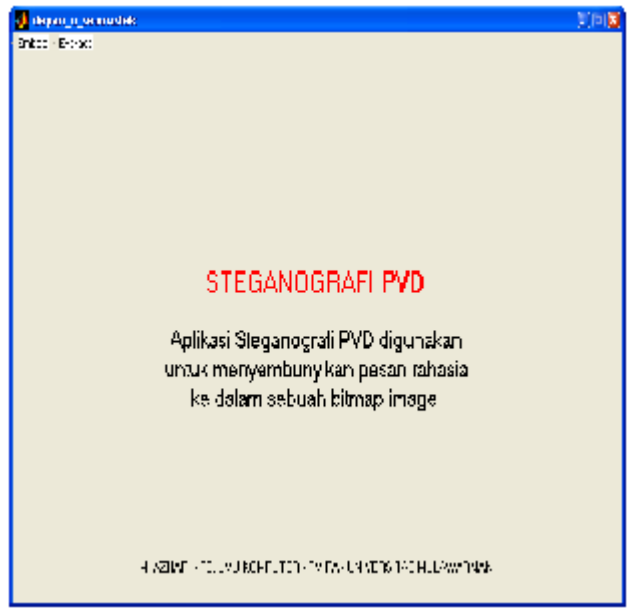
Gambar5*Layout*halamanpenyisipanpesan



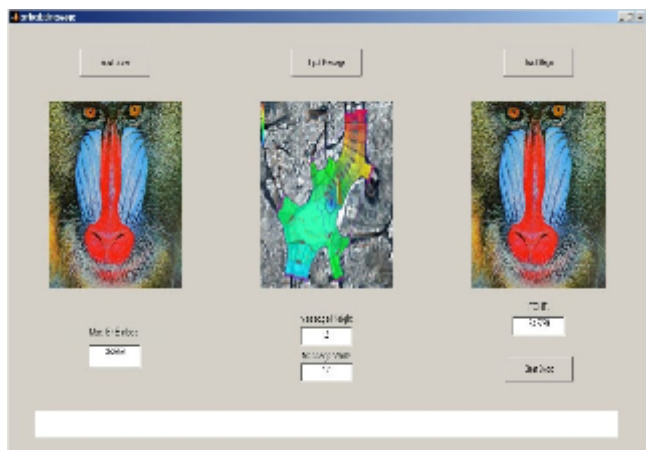
Gambar 6 *Layout* halaman pengambilan pesan

Implementasi

Pemrograman *script* m-file pada Matlab digunakan untuk pengembangan aplikasi steganografi PVD. Lima buah *scriptm-file* dibutuhkan dalam implementasinya. Dua *scriptm-file* merupakan isi program sebagai implementasi dari algoritme penyisipan pesan dan pengambilan pesan, tiga buah *script m-file* untuk mengendalikan grafik antarmuka. Selain itu lima buah*filefigure*jugadibuatuntukpengembangangrafikantarmuka. Implementasidariaplikasi yang dikembangkanpadapenelitianiniberturutdapatdilihatpadagambar7, 8, dan 9.



Gambar 7 Halaman depan aplikasi steganografi PVD.

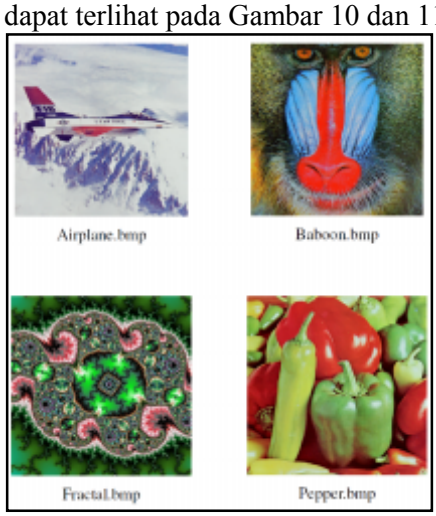


Gambar 8 Halaman penyisipan pesan aplikasi steganografi PVD.

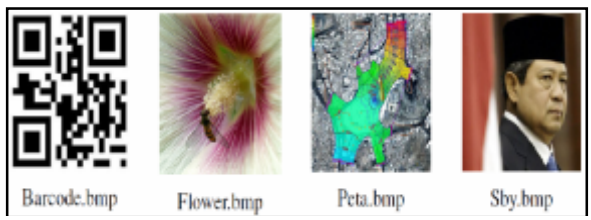
Gambar 9 Halaman pengambilan pesan aplikasi steganografi

Hasil percobaan

Aplikasi diujicoba menggunakan cover dan pesan berupa citra 24 bit berformat bmp. Sebanyak empat buah citra cover diujicoba untuk disisipi pesan. Masing-masing citra tersebut dipilih dengan mengacu pada perbedaan karakteristik visual yang mengacu pada penyebaran warna kontras dan halus citra.Empat buah citrayangdijadikan sebagai *cover* pada penelitian ini masing-masing sebesar 256x256 piksel berukuran 192 Kilobyte (KB) dan 512x512 piksel berukuran 769 KB. Adapun pesan yang disisipkan berukuran 5 KB, 10 KB, 21 KB, 31 KB, 43 KB, 50 KB, 60 KB, 80 KB dan 100 KB. Visualisasi citra cover dan pesan yang digunakan dalam ujicoba aplikasi dapat terlihat pada Gambar 10 dan 11.



Gambar 10 Citra *cover*.



Gambar11 Citra pesan.

Tabel 2 dan 3 menunjukkan teknik steganografi PVD dapat dilakukan menggunakan yang dikembangkan pada penelitian ini. Pada menu penyisipan pesan dapat dihasilkan stegoimage yang diinginkan. Sementara pada menu pengambilan pesan ekstraksi stego image pun dapat dilakukan. Aplikasiinimampu menghitung daya tampung pesan milik sebuah cover.

Tabel 2 Daya Tampung pesan pada cover berukuran 192 KB

File Cover	Daya Tampung (bit)
Airplane.bmp	313905
Babbon.bmp	323912
Fractal.bmp	381312
Pepper.bmp	310986

Tabel 3 Daya Tampung pesan pada cover berukuran 769 KB

File Cover	Daya Tampung Pesan (bit)
Airplane.bmp	1220637
Babbon.bmp	1383279
Fractal.bmp	1431057
Pepper.bmp	1218492

Selain itu tampak pada Tabel 4 dan 5 capaianPSNR di setiap proses penyisipandapatdiketahui. Pengamatan yang dilakukanhampirseluruhstego image memilikinilai di atas 20 db. Hal ini menunjukkan bahwa *noise* yang ditimbulkan setelah *cover* disisipi pesan berada di atas batas minimal (Cole 2003). Oleh karena itu, *stego image* yang dihasilkan memiliki tingkat keamanan yang baik.

Tabel 4 Capaian PSNR stego image berukuran 192 KB

		File Cover			
		Airplane.bmp	Babbon.bmp	Fraktal.bmp	Pepper.bmp
Pesan	Barcode.bmp (21 KB)	36.11	36.11	34.66	36.75
	Flower.bmp (31 KB)	34.92	34.92	34.38	35.76
	Peta.bmp (43 KB)	-	-	32.93	-
	Sby.bmp (48 KB)	-	-	-	-

Tabel 5 Capaian PSNR stego image berukuran 769 KB

Pesan	File Cover			
	Airplane.bmp	Babbon.bmp	Fraktal.bmp	Pepper.bmp
Barcode.bmp (50 KB)	38.26	38.99	38.18	39.77
Flower.bmp (60 KB)	37.50	39.44	38.46	39.44
Peta.bmp (80 KB)	36.77	38.41	37.25	38.26
Sby.bmp (100 KB)	36.35	37.90	36.64	37.76

Simpulan

Penelitian ini menghasilkan simpulan sebagai berikut:

1. Aplikasi steganografi PVD yang dikembangkan pada penelitian ini dapat digunakan untuk menghasilkan sebuah file stegoimage.
2. Ekstraksi pesan dalam stego image dapat dapat dilakukan menggunakan aplikasi yang dikembangkan pada penelitian ini.
3. Aplikasi steganografi PVD juga dapat digunakan untuk menghitung nilai PSNR yang ditimbulkan dalam proses steganografi.

Saran

Penelitian lebih lanjut disarankan untuk menerapkan hal-hal sebagai berikut:

1. Beberapa jenis tabel jangkauan perlu digunakan untuk mencari daya tampung yang lebih besar.
2. Perancanganalgoritmeuntukmempercepatwaktu proses.
3. Nilai-nilai piksel yang berada di luarjangkauanperludiatasidenganmerancang algoritme yang tepat.

Daftar Pustaka

Amirtharajan R, Akila R, Deepikachowdavarapu P, 2010. A Comparative Analysis of Image Steganography. *International Journal of Computer Applications* 2:41-47

Bender W, Gruhl D, Morimoto N, Lu A. 1996. Techniques for data hiding. *IBM Systems Journal* 35:313-336

Cole E. 2003. *Hiding in Plain Sight Steganography and the Art of Covert Communication*. Indiana: Wiley.

Guritman S. 2003. *Pengantar Kriptografi*. Bogor: Fakultas Matematika dan Ilmu Pengetahuan Alam IPB**.**

Johnson NF, Jajodia S. 1998. Exploring Steganography: Seeing the Unseen.*Computer* 31: 26-34

[MathWorks] MathWorks. 1997. *Building GUIs with MATLABVersion 5*. Natick: The MathWorks, Inc.

Medeni M.B O, Souidi EM. 2010. A Generalization of the PVD Steganographic Method. *International Journal of Computer Science and Information Security* (IJCSIS) 8:156-159.

Nugroho EP, Ratnasari K, Ramadhani KN, Putro BL. 2009. *Rekayasa Perangkat Lunak*. Bandung: Politeknik Telkom.

Wu D, Tsai W. 2003. A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters* 24: 1613–1626.