Pixel Value Differencing dan Least Significant Bit Subtitution pada Steganografi Video

Fakhri (13510048)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13510048@std.stei.itb.ac.id

***Abstrak*— Pada steganografi, penyisipan pesan pada umumnya dilakukan pada Least Significant Bit (LSB), yaitu bit pada suatu byte biner yang memiliki nilai paling tidak berarti. LSB sering diartikan sebagai bit bernilai paling kecil atau dengan kata lain bit paling kanan akibat perubahan terhadap bit tersebut tidak menyebabkan perubahan nilai keseluruhan yang signifikan. Dalam prakteknya, terdapat penyesuaian dalam pendefinisian ketidakberartian nilai suatu bit. LSB dapat didefinisikan sebagai bit terkecil atau dapat pula dinilai sesuai dengan pesan yang akan disisipkan. Jika disesuaikan dengan pesan yang disisipkan, akan diperoleh banyak metode dalam melakukan penyembunyian informasi (steganografi) seperti memanfaatkan Least Significant Bit Subtitution dan Pixel Value Differencing (PVD) oleh Wu et al. Selain dua hal tersebut terdapat pula penyesuaian LSB dengan menggunakan algoritma genetik, dynamic programming, dan masih banyak lagi. Pada makalah ini akan dibahas implementasi dan analisis steganografi dari Pixel Value Differencing dan metode LSB pada video.**

***Kata Kunci*—Pixel Value Differencing, LSB, Steganografi**

I. PENDAHULUAN

Steganografi adalah ilmu dan seni menyembunyikan (*embedded*) informasi dengan cara menyisipkan pesan rahasia di dalam pesan lain. Steganografi di bidang teknologi informasi sangat berkembang, yaitu untuk perangkat – perangkat digital. Informasi atau pesan yang dapat disembunyikan beragam, begitu pula dengan pesan yang menjadi objek tersisip. Variasi pesan yang biasa menjadi subjek dan objek penyisipan adalah pesan teks, pesan audio, pesan gambar, dan pesan video.

Pemanfaatan dari steganografi selain untuk penyembunyian informasi langsung atau mentah, juga dimanfaatkan sebagai sistem keamanan data pada komunikasi elektronik / digital, komunikasi tersembunyi menggunakan alat komunikasi digital, pelindungan informasi rahasia pemerinta, hak cipta, rahasia dagang, dan desain industri yang disimpan dalam format digital. Walaupun steganografi telah dimanfaatkan dan digunakan seperti pada hal - hal yang disebutkan di atas, tetap saja ada usaha pencurian atau ekstraksi oleh pihak yang tidak diharapkan informasi akibat informasi yang disembunyikan sangat berharga. Untuk mencegah hal – hal yang tidak diinginkan, maka dalam penerapannya pesan yang disembunyikan biasanya dienkripsi terlebih dahulu. Hal ini dilakukan atas dasar peningkatan keamanan, yaitu apabila pesan yang disembunyikan berhasil diekstrak, pelaku ekstraksi tidak dapat langsung memperoleh pesan, tetapi tetap harus menembus lapisan kemanan selanjutnya, yaitu dekripsi. Bagi penerima pesan yang ditargetkan, proses ekstrak dan dekripsi membutuhkan kunci yang disepakati pengirim dan penerima sehingga ekstraksi dan dekripsi dapat dilakukan dengan lancar. Proses enkripsi dan dekripsi pesan ini terlepas dari steganografi, dengan kata lain berdiri sendiri, namun merupakan fitur yang sangat membantu dalam peningkatan keamanan setelah proses steganografi.

Selain dengan menambahkan proses enkripsi, dalam meningkatkan keamanan dan penyembunyian pesan, dilakukan juga banyak pengembangan atau peningkatan di untuk metode steganografi. Pengembangan Steganografi pada umumnya tidak terlepas dari pemanfaatan Least Significant Bit (LSB), yaitu pemanipulasian bit yang memiliki nilai paling tidak berarti. Dari hal tersebut pengembangan besar yang dilakukan dikelompokkan menjadi beberapa bagian. Tiga bagian diantara bagian – bagian tersebut adalah Pixel Differenceing Value (PVD), Bit-Plane Complexity Segmentation (BPCS), dan Multiple Base Notational System (MBNS). Ketiga bagian tersebut kemudian dikembangkan lagi menjadi lebih detail baik dengan cara mencampurkannya terhadap teori lain seperti graf, algoritma genetic, *dynamic programming*, dan lain-lain maupun penambahan aspek antisipasi terhadap celah – celah keamanan ataupun kelemahannya. Pengembangan diarahkan ke dalam peningkatan Peak Sognal to Noise Ratio (PSNR), peningkatan kuantitas data yang dapat disembunyikan, ataupun peningkatan kecepatan proses steganografi.

II. DASAR TEORI

Pada bagian ini akan dijelaskan teori –teori dari sumber acuan dalam pengambilan data dan analisis dalam laporan

ini. Sumber – sumber utama yang digunakan berasal dari teori pada jurnal – jurnal pendidikan internasional seperti "A steganographic method for images by pixel-value differencing" yang ditulis oleh Da-Chun Wu dan Wen-Hsiang Tsai, lalu "Image steganographic scheme based on pixel-value differencing and LSB replacement methods" oleh H.-C. Wu, N.-I. Wu, C.-S. Tsai, dan M.-S. Hwang.

A. Least Significant Bit (LSB)

Least Significant Bit adalah bit yang memiliki nilai paling diabaikan sehingga jika ada perubahan pada bit tersebut, memberikan dampak paling minimal jika dibandingkan dengan mengubah bit lainnya. Umumnya LSB adalah bit paling kecil dari suatu bilangan.

B. Tinjauan "Steganographic method for images by pixel-value differencing" oleh Da-Chun Wu dan Wen-Hsiang Tsai

Metode Pixel-Value Differencing memanfaatkan karakteristik dari ketidaksensitifan penglihatan manusia dengan fokus pada tingkat komputasi yang mudah, kuantitas subjek penyembunyian yang besar, dan tanpa menyebabkan penurunan kualitas yang besar. Akan tetapi ada limitasi, yaitu semakin besar data yang ingin disembunyikan maka semakin besar pula penurunan kualitasnya.

Dalam prosesnya, digunakan sebuah gambar hitam putih (*greyscale*), dipilih dua pixel p_i dan p_{i+1} bersebelahan untuk seluruh bagian gambar. Untuk tiap nilai kedua p dihitung selisihnya menjadi d. Apabila nilai d mendekati 0, dapat dianggap bahwa kedua pixel tersebut adalah blok yang sangat mulus (*smooth*). Sedangkan apabila nilai d mendekati -255 atau 255, dapat dianggap bahwa kedua pixel adalah blok yang sangat kasar. Apabila nilai d diabsolutkan, maka akan diperoleh nilai positif untuk seluruh d dan jika seluruhnya disimpan pada suatu rangkaian nilai R_i untuk $i = 1, 2, \ldots, n$ maka akan diperoleh batas bawah l_i dan batas atas u_i. Setelah itu nilai di tiap rangakaian dipangkatkan 2 sehingga menimbulkan perbedaan yang lebih besar antara blok pixel yang mulus dan kasar. Pada metode ini, penyembunyian pesan memanfaatkan perubahan nilai dua pixel dengan tetap menjaga nilai selisihnya. Perubahan nilai pixel tanpa perubahan nilai selisih tersebut tidak menyebabkan mata manusia dapat mendeteksinya dengan mudah.

Proses penyembunyian pesan, diberikan sebuah blok dua pixel B dengan indeks k, selisih d, dan sebuah nilai ukuran bit n yang diperoleh dari :

$$n = \log_2 (u_k - l_k + 1)$$

yang bernilai positif karena nilai u dan k yang merupakan perpangkatan dua. Sebuah potongan pesan S dipilih dengan b adalah nilai bit dari potongan blok S. Dari b dihitung nilai selisih baru, yaitu d' dengan dua kemungkinan :

$$d' = l_k + b, \qquad d >= 0$$
$$d' = -(l_k + b), \qquad d < 0$$

nilai d' memiliki jangkauan antara l_k hingga u_k dan menjadi nilai subtitusi untuk d. Subtitusi ini tidak dapat dideteksi oleh mata manusia dengan mudah. Nilai b dapat disembunyikan akibat dapat diperoleh dengan inversi d' yang terdapat pada dua nilai pixel (g'_i , g'_{i+1}) dari pixel pada stego-image. (g'_i , g'_{i+1}) diperoleh dari nilai (g_i , g_{i+1}) melalui perhitungan invers (g'_i , g'_{i+1}) menggunakan fungsi :

$$f((g_i , g_{i+1}), m) = (g'_i , g'_{i+1})$$
$$= (g_i - \text{ceiling}_m, g_{i+1} + \text{floor}_m), d \text{ ganjil}$$
$$(g_i - \text{floor}_m, g_{i+1} + \text{ceiling}_m), d \text{ genap}$$

Dengan m adalah selilsih dari d' dan d, ceiling_m dan floor_m adalah pembulatan ke atas dan ke bawah dari $m/2$. Nilai g' dapat berada di luar 0-255 apabila selisih d' dan d lebih besar daripada nilai pixel g'. Oleh karena itu dirancang penanggulangannya, yaitu melalui nilai $(\hat{g}_i, \hat{g}_{i+1})$ yang diperoleh dari fungsi $f((g_i , g_{i+1}), u_k - d)$. $u_k - d$ adalah selisih terbesar yang dapat ditemui dan jika hal ini terjadi, penyembunyian data pada blok ini dibatalkan. Cara penanggulangan ini disebut juga *falling-off-boundary checking*.

g ataupun $\hat{g}$ adalah pengganti nilai blok pixel pada *cover* dengan pola *pseudo-random* untuk mengubahnya menjadi stego media.

Untuk ekstraksi dilakukan dengan mengikuti pola *pseudo-random* dengan *seed* seperti pada proses penyembunyian. Untuk tiap pixelnya dilakukan *falling-off-boundary checking*, yaitu untuk pixel pada stego-image $((g^*_i , g^*_{i+1})$ dan selisih d^* diperiksa nilai $f((g^*_i , g^*_{i+1}), u_k - d^*)$. Apabila hasilnya, yaitu $(\hat{g}^*_i , \hat{g}^*_{i+1})$ minimal salah satu berada di luar rentang 0-255, maka blok pixel tersebtu tidak digunakan dalam proses penyembunyian dan diskip. Akan tetapi nili b dari variable ini tetap perlu diekstrak karena dibutuhkan untuk ekstraksi selanjutnya, yaitu dengan cara

$$b = d^* - l_k , \quad d^* >= 0$$
atau
$$b = - d^* - l_k , d^* < 0$$

C. Tinjauan "Image steganographic scheme based on pixel-value differencing and LSB replacement methods" oleh H.-C. Wu, N.-I. Wu, C.-S. Tsai, dan M.-S. Hwang.

Metode ini adalah pengembangan dari PVD awal

Wu dan Tsai. Pengembangan yang dilakukan adalah peningkatan kapasitas pesan yang dapat disembunyikan. Untuk itu diperlukan nilai baru yaitu nilai pembagi. Nilai pembagi ini adalah suatu indikator yang membagi selisih blok pixel sehingga tergolong menjadi dua bagian, yaitu mulus atau kasar. Blok mulus dan kasar bisa disebut juga sebagai level bawah dan level atas. Pembagi ini juga menjadi kunci dalam melakukan penyembunyian maupun ekstraksi.

Selain penambahan indikator pembagi, metode ini juga menetapkan satu ukuran nilai / panjang bit tiap kali melakukan penyembunyian pesan pada blok level bawah, yaitu 6 bit. Berbeda dengan PVD awal yang selalu berbasis *n* bit dengan *n* diperoleh menggunakan perhitungan $\log_2 (u_k - l_k + 1)$.

Dalam penyembunyian diawali dengan penentuan indikator pembagi *Div*. agar sesuai contoh pada jurnal, asumsikan *Div* memiliki nilai 15 dan seluruh lingkup *R* dibagi menjadi 8 bagian dengan 2 bagian, yaitu 0-7 dan 8-15 termasuk bagian level bawah dan selebihnya level atas. Penyembunyian pesan layaknya PVD awal, dilakukan dengan melakukan perulangan untuk tiap blok 2 pixel p_i dan p_{i+1} yang bersebelahan di seluruh bagian gambar untuk menghitung nilai d_i yang diabsolutkan. Setelah itu dimasukkan kedalam rangkaian R_i , mencari u_i , dan l_i . Langkah selanjutnya berbeda dengan PVD awal, yaitu menyeleksi nilai absolut suatu R_i tergolong ke dalam level bawah atau atas. Jika tergolong ke dalam level atas atau dengan kata lain tergolong blok kasar, maka penyembunyian akan dilakukan layaknya metode PVD awal oleh Wu dan Tsai. Sedangkan jika tergolong nilai absolutnya tergolong level bawah, penyisipan akan dilakukan pada blok bit tersebut. Dalam proses penyembunyian pada bit p_i dan p_{i+1}, diambil 6 bit terurut dari *stream* pesan, 3 bit pertama dari pesan disubtitusi terhada 3 bit LSB pada p_i dan 3 bit selanjutnya / terakhir dari pesan disubtitusi terhada 3 bit LSB pada p_{i+1}.

Setelah subtitusi ada kemungkinan nilai absolut *d'*, yaitu selisih dari p'_i dan p'_{i+1} bernilai besar dari *Div* atau dengan kata lain tergolong level atas. Jika hal ini terjadi, diperlukan penanggulangan selanjutnya yaitu

$$(p'_i , p'_{i+1}) = (p'_i - 8, p'_{i+1} + 8) , p'_i >= p'_{i+1}$$
atau
$$(p'_i , p'_{i+1}) = (p'_i + 8, p'_{i+1} - 8) , p'_i < p'_{i+1}$$

Dengan penjumlahan dan pengurangan di atas, maka *d'* akan tergolong ke level bawah kembali.

Pada proses ekstraksi, stego-image diiterasi per blok 2 pixel yang bersebelahan di seluruh bagian gambar untuk menghitung nilai d'_i yang diabsolutkan. Setelah itu dimasukkan kedalam rangkaian R'_i, mencari u'_i , dan l'_i . Jika nilai R'_i tergolong level atas, ekstrak data sesuai PVD awal Wu dan Tsai. Namun jika tergolong level bawah, ekstrak 3 LSB p'_i dan p'_{i+1} lalu digabungkan.

D. "Secure Video Steganography with Encryption Based on LSB Technique", Yadav, Pooja., & Mishra, Nishchol., & Sharma, Sanjeev

Dalam melakukan steganografi pada video, terdapat bebreapa metode yang umum digunakan. Dalam jurnal tersebut dijelaskan beberapa metode itu. Metode – metode tersebut antara lain adalah *symmetric encryption*, *sequential encoding*, dan *LSB technique.*

Symmetric Encyption diterapkan dengan menggunakan operator XOR. Penyisipan nilai dilakukan dengan cara melakukan XOR antara stream bit pesan dengan kunci baik untuk proses penyembunyian maupun ekstraksi. Cara seperti ini tergolong ke dalam cara yang sederhana.

Sequential Encoding diterapkan layaknya melakukan steganografi secara sekuensial pada gambar, namun untuk hal ini dilakukan terhadap video. Sekuens biasanya dimulai dari kiri atas hingga kanan bawah. Di tiap sekuensnya, dilakukan penyembunyian terhadap LSB pada RGP pixel.

Teknik LSB diterapkan dengan cara melakukan subtitusi bit LSB untuk tiap RGB suatu pixel. LSB yang umum dterapkan adalah 1 bit LSB untuk tiap R, G, dan B.

Selain metode, ada perbedaan mendasar lain dalam steganografi untuk video, yaitu pengukuran *Peak Signal to Noise Ratio* (PSNR) dan *Root Mean Square Error* (RMSE). PSNR dan RMSE untuk video dapat diperoleh dengan rumus :

$$PSNR = 10\ log_2 \frac{256\ x\ 256}{RMSE^2}$$

$$= 10\ log_2 \frac{\text{(panjang x lebar x 256 x 256)}}{\sum_{x=1}^{panjang} \sum_{y=1}^{lebar} (frame\ cover - frame\ stego)^2}$$

$$RMSE = \sqrt{\frac{\sum_{x=1}^{panjang} \sum_{y=1}^{lebar} (frame\ cover - frame\ stego)^2}{panjang\ x\ lebar}}$$

III. IMPLEMENTASI

Dalam pengembangan PVD dalam metode kedua di atas, terjadi peningkatan kapasitas namun terjadi pula penurunan PSNR. Perlu diperhatikan bahwa kedua PVD di atas diterapkan pada media yaitu gambar hitam putih, karena pada implementasi ini yang menjadi media adalah file video tentunya terdapat perbedaan – perbedaan. Perbedaan tersebtu antara lain :

1. Video memiliki ukuran yang jauh lebih besar daripada gambar
2. Video yang dipakai memiliki warna, sedangkan gambar pada PVD di atas hitam-putih (*greyscale*)

Oleh karena itu pada implementasi ini didesain suatu aplikasi steganografi sesuai dasar teori yang tertera dengan beberapa modifikasi yaitu :

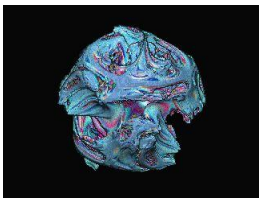
1. LSB yang diterapkan dispesifikkan menjadi 3 bit dengan masing masing R, G, dan B 1 bit, tidak dapat diatur ulang oleh *user*. Hal ini dilakukuan untuk tujuan meningkatkan PSNR.
2. Menetapkan satuan level bawah blok pixel, yaitu 15 untuk meningkatkan PSNR.
3. Tidak melakukan penyembunyian pada blok yang tergolong level atas untuk meningkatkan PSNR, namun menurunkan kuantitas.

Pengembangan aplikasi ini dilakukan pada lingkungan pengembangan sebagai berikut :

1. Windows 7 Ultimate 32 bit
2. Processor AMD Phenom 2 X4 3.0 Ghz
3. 2586 MB RAM
4. Kartu Grafis NVIDIA GeForce GT430
5. Visual Studio 2012
6. Bahasa pemrograman C#

Lalu untuk uji coba digunakan beberapa sampel video dengan format avi yang dibuat oleh Mystic Fractal sebagai berikut :

1. fp.avi



Gambar 1 screenshot video fp.avi

dengan ukuran 320 x 240, 15 fps, 311 Kb, dan durasi di bawah 1 detik.

2. fractogene.avi

Gambar 2 screenshot video fractogene.avi

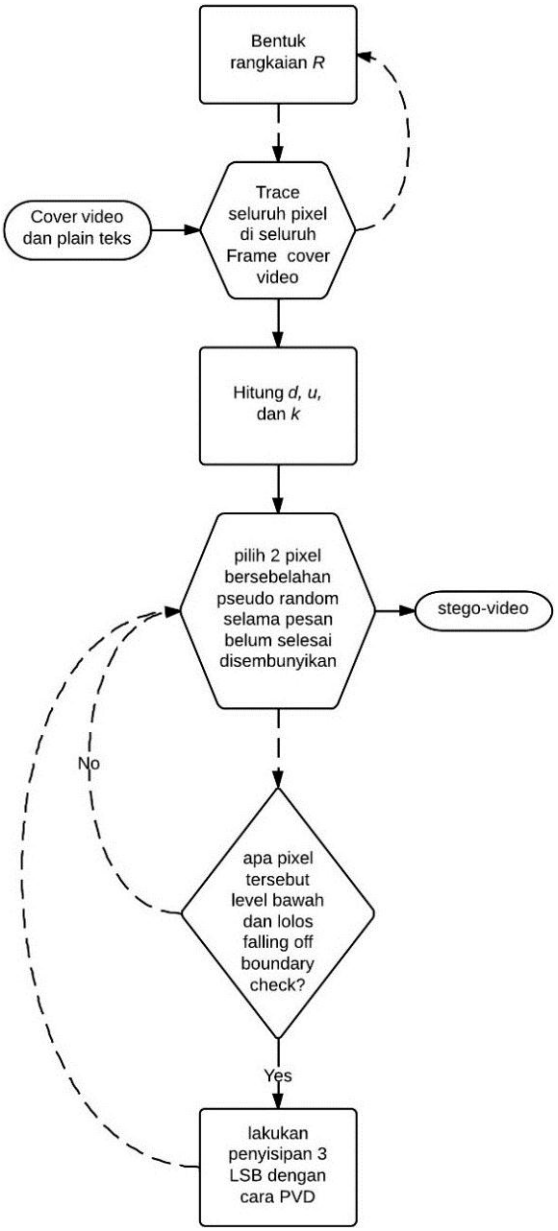
dengan ukuran 320 x 240, 15 fps, 1703KB, dan durasi 7 detik.

3. cookie.avi

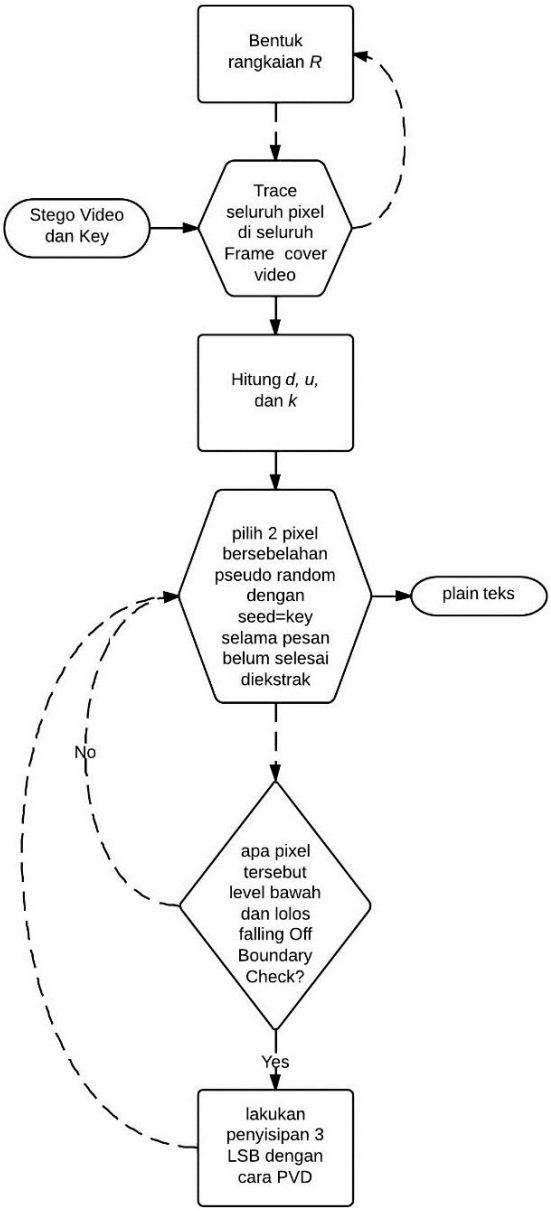
Gambar 3 screenshot video cookie.avi

dengan ukuran 800 x 600, 15 fps, 5223KB, dan durasi 3 detik.

Dengan adanya beberapa modifikasi, maka terdapat beberapa perubahan algoritma pada proses enkripsi. Penjelasan untuk perubahan tersebut dapat dilihat pada flowchart untuk program yang dibuat sebagai berikut :



Gambar 4 Flowchart algoritma pada proses penyembunyian



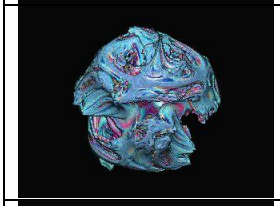
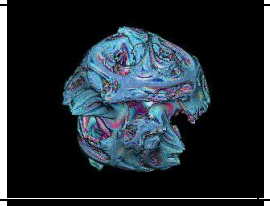
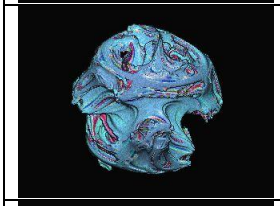
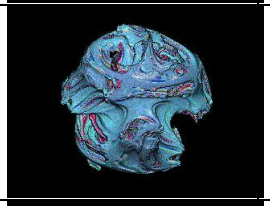
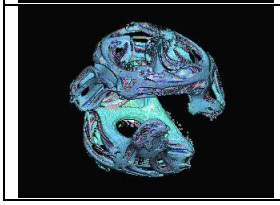
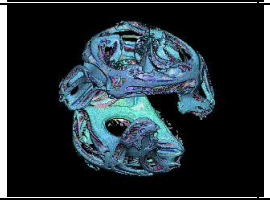
Gambar 5 Flowchart algoritma pada proses ekstraksi

Akibat adanya perubahan pada penyembunyian, maka algoritma untuk ekstraksi juga mengalami perubahan. Flowchart perubahan algoritma pada proses dekripsi dapat dilihat pada gambar berikut:

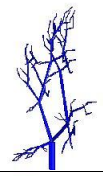
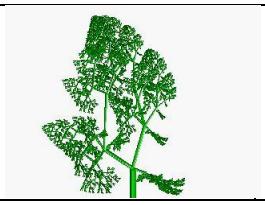
IV. ANALISIS

Frame perbandingan untuk video cover dan stego video dapat dilihat pada tabel berikut :

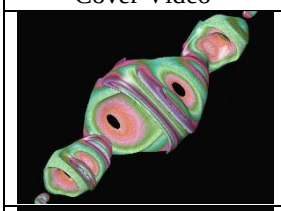
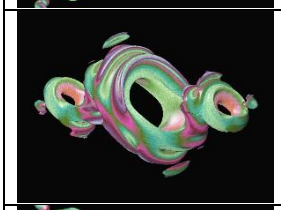
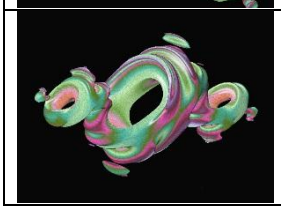
Tabel 1 Perbandingan cover video dan stego video fp.avi

Cover Video	Stego Video	Frame
		1
		3
		5
		8

Tabel 2 Perbandingan cover video dan stego video fractogene.avi

Cover Video	Stego Video	Frame
		29
		58
		87
		116

Tabel 3 Perbandingan cover video dan stego video cookie.avi

Cover Video	Stego Video	Frame
		11
		22
		33
		44

Lalu data hasil yang diperoleh pada seluruh implementasi di atas dapat dilihat pada tabel berikut ini:

Tabel 4 Data hasil Implementasi dengan PVD dan LSB modifikasi

Video	RMSE	PSNR (dB)
fp.avi	580,4	41,05
fractogene.avi	668,9	39,82
cookie.avi	354,6	45,33

Dari data yang diperoleh di atas, nilai PSNR berada di atas standar baik, yaitu 30, begitu pula untuk RMSE.

V. KESIMPULAN

Metoda penggabungan PVD dan LSB adalah salah satu langkah untuk meningkatkan ukuran ataupun PSNR dalam melakukan steganografi pada video khususnya yang berwarna. Hal ini juga dikarenakan video adalah kumpulan dari banyak gambar yang telah banyak dikembangkan untuk aspek steganografi baik PVD maupun LSB.

REFERENSI

[1] Da-Chun Wu, Wen-Hsiang Tsai. 2002. “A steganographic method for images by pixel-value differencing”. IEEE

[2] H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang. 2005. “Image steganographic scheme based on pixel-value differencing and LSB replacement methods”. IEEE

[3] Yadav, Pooja., & Mishra, Nishchol., & Sharma, Sanjeev. 2013. “A Secure Video Steganography with Encryption Based on LSB Technique”. IEEEE

[4] Tseng , Hsien-Wen., & Leng, Hui-Shih. 2013 “A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number”. Hindawi

[5] Yang, Cheng-Hsing., & Wang, Shiuh-Jeng. 2010. “Transforming LSB Substitution for Image-based Steganography in Matching Algorithms”. Taiwan : JISE.

[6] El-Alfy , El-Sayed M., & Al-Sadi , Azzat A. 2012. “Pixel-Value Differencing Steganography: Attacks and Improvements”. Dhahran : ICCIT.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 17 April 2014

Fakhri (13510048)