Penerapan Metode Steganografi End Of File Untuk Menyisipkan Pesan Pada Gambar Digital

Rahmad Zainul Abidin
Universitas Yudharta Pasuruan
rahmatebit@gmail.com

ABSTRAK

Berbagai teknik untuk menangkal kejahatan yang menggunakan teknologi informasi telah dilakukan, seperti teknik penyampaian pesan dengan menggabungkan kriptografi *Blowfish* dengan steganografi DCS (*Dinamic Cell Spreading*). Namun DCS memiliki kelemahan jika dibandingkan dengan steganografi Heksa. Kelemahannya adalah DCS menyisipkan data pada semua warna RGB. Hal ini akan mengakibatkan pixel akan lebih banyak berubah, mudah terdeteksi dan sistem pertahanan data ketika gambar sisipan (*stego image*) diolah/diedit data sisipan mudah hilang/rusak. Sedangkan Heksa perubahan warna pixel lebih sedikit dan data sisipan mudah dipertahankan. Berdasarkan kelemahan DCS tersebut maka penelitian ini mengusulkan teknik penggabungan steganografi Heksa sebagai teknik penyisipan data dan kriptografi Blowfish sebagai teknik enkripsi data.

Proses pengujian penelitian ini dengan dilakukan uji ketahanan steganografi Heksa. Tujuannya untuk mengetahui seberapa kuat stegano mempertahankan data sisipan jika *stego image* diolah/diedit. Kemudian diuji dengan analisis PNSR, untuk mengetahui tingkat perubahan gambar asli (*cover image*) dengan gambar sisipan.

Hasil dan kesimpulan yang didapat bahwa metode penggabungan kriptografi Blowfish dengan steganografi Heksa lebih baik dari pada steganografi DCS.

Kata kunci: *Steganografi, End of File.*

1. PENDAHULUAN

Tindak kejahatan dan kriminal pada sekarang ini sudah banyak melibatkan teknologi informasi dan komunikasi. Pemanfaatan komputer, telepon genggam, email, Internet, dan perangkat digital lainnya bisa mengundang berbagai pihak untuk melakukan kejahatan berbasis teknologi komunikasi. Oleh karena itu, dibutuhkan teknik untuk mengamankan penyampaian teks agar orang tidak mampu menyadap atau mengambil pesan teks tersebut untuk kejahatan.

Diantara teknik untuk mengamankan penyampaian pesan teks adalah dengan metode Steganografi dan kriptografi (Yadav, 2011). Steganografi adalah suatu metode untuk menyembunyikan suatu pesan di dalam pesan yang lain yang mana orang lain tidak mengetahui bahwa pesan tersebut di dalamnya ada pesan yang lebih penting. Tujuan pengembangan Steganografi adalah mempertahankan data pesan yang disisipkan pada media citra digital agar tidak bisa terdeteksi oleh aplikasi lain bahwa di dalam citra digital tersebut tersembunyi pesan teks rahasia.

Salah satu teknik penyampaian pesan teks dengan menggunakan steganografi adalah penelitian Padmaa & Venkataramani (2014) yang menggunakan algoritma steganografi Heksa. Steganografi Heksa merupakan teknik pengembangan dari stegano LSB atau steganografi sebelumnya. Namun pada penelitian tersebut hanya menggunakan steganografi saja, pesan teks yang akan disisipkan tidak dienkripsi terlebih dahulu. Enkripsi data ini perlu dilakukan, karena menurut Wijaya & Prayudi (2014) untuk meningkatkan keamanan penyampaian pesan teks adalah dengan menggabungkan metode steganografi dengan kriptografi. Oleh karena itu, penelitian Padmaa perlu dilakukan pengembangan teknik dengan cara menggabungkan steganografi Heksa dengan teknik kriptografi.

Teknik penyampaian pesan teks dengan menggabungkan steganografi dan kriptografi juga sudah dilakukan, seperti penelitian yang telah dilakukan oleh Wijaya (2014). Metode penggabungannya menggunakan kriptografi Blowfish dan Steganografi DCS (*Dinamic Cell Spreading*). Namun steganografi DCS memiliki kelemahan jika dibandingkan dengan steganografi Heksa. Kelemahannya adalah DCS menyisipkan pesan teks kepada bit terakhir semua warna RGB (merah, hijau, biru). Hal ini akan mengakibatkan setiap pixel akan lebih banyak mengalami perubahan warna dan sistem dalam mempertahankan pesan teks ketika gambar sisipan (stego image) diolah/diedit data pesan teks mudah hilang atau rusak. Berbeda dengan steganografi Heksa dalam penyisipan data menggunakan indikator R yang sebagai pemicu data disisipkan ke warna hijau atau biru. Sehingga warna setiap pixel akan lebih sedikit mengalami perubahan warna. Indikator R ini juga menyebabkan sistem dalam mempertahankan pesan teks ketika gambar sisipan (stego image) diedit data pesan teks tidak mudah hilang atau rusak.

Berdasarkan penjelasan kelemahan pada penelitian yang dilakukan Wijaya (2014) maka penelitian ini mengambil teknik Heksa sebagai metode keamanan pada steganografinya. Sedangkan untuk enkripsi data menggunakan Blowfish sebagai kriptografinya. Teknik kriptografi penelitian ini sama dengan penelitian sebelumnya, dikarenakan menurut Haldankar & Kuwelkar (2014) Blowfish sudah menjadi algoritma kriptografi yang cepat, mampu bekerja mencapai 26 clock cyly per byte, dan proses penghitungannya sederhana hanya menggunakan penjumlahan dan XOR.

Jadi fokus penelitian ini terletak pada bagaimana membangun sistem penggabungan metode kriptografi Blowfish dengan steganografi Heksa. Yang dimaksud dengan membangun sistem di sini adalah membuat algortima penggabungan metode tersebut, kemudian diwujudkan dalam bentuk program aplikasi sebagai implementasi metode penggabungan kriptografi Blowfish dan steganografi Heksa.

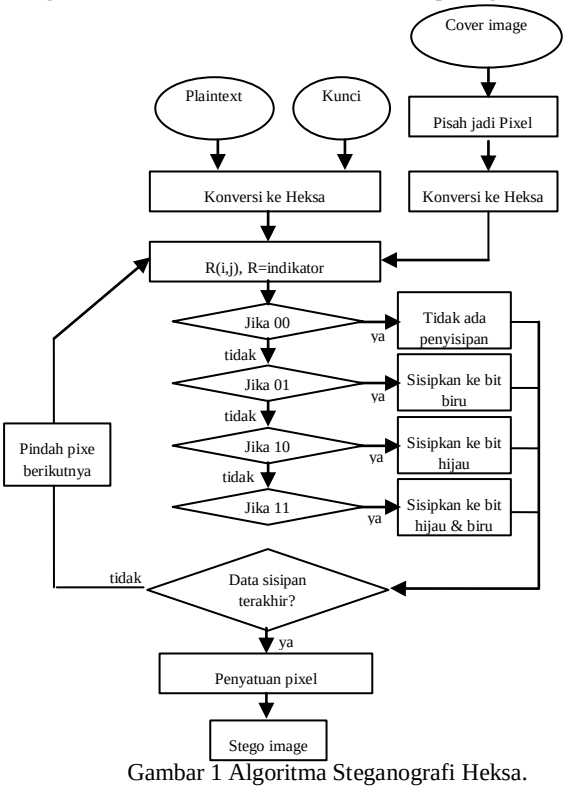
2. LANDASAN TEORI

Dalam dasar teori ini akan menguraikan teori-teori yang mendasari penelitian ini khususnya untuk teknik mengamankan data tentang Kriptografi dan Steganografi.

2.1 Konsep Steganografi Heksa

Steganografi Heksa mengurutkan secara acak yang digunakan untuk memilih urutan baris awalnya dan kemudian

sebuah warna indikator / channel mengatur embedding data antara dua saluran lainnya (saluran data). Dalam gambar warna, warna merah dapat dipilih sebagai warna indikator dimana bit paling signifikan dalam setiap pixel dalam saluran ini digunakan untuk memutuskan embedding. Sepanjang proses embedding ini, indikator warna tidak bisa diubah. Karena data yang akan disembunyikan biasanya tertanam dalam mode yang telah ditetapkan k bit. Metode ini digunakan Optimal Proses Pixel Penyesuaian untuk mengurangi kesalahan mean-square. Setelah proses tersebut di atas selesai dan 4 gambar stego yang dihasilkan setiap baris dari ini dibandingkan terhadap baris yang sesuai di gambar cover. Langkah ini memungkinkan menentukan deviasi relatif dari masing-masing sehubungan dengan gambar cover. Adapun algoritma Heksa secara umum bisa dilihat pada gambar 1



Gambar 1 Algoritma Steganografi Heksa.

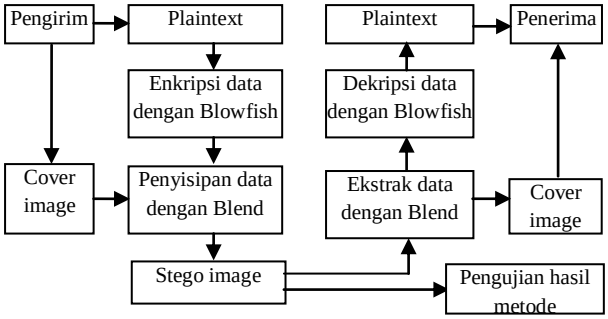
Penjelasan algoritma steganografi Heksa:

1. Data rahasia (plaintext) dienkripsi dengan 4 kunci (k1, k2, k3, k4), hasilnya menjadi datk1, datk2,datk3,datk4.
2. Mengkonversi data yang terenkripsi secara berurutan menjadi data bilangan biner, yang kemudian disebut dat_k1, dat_k2, dat_k3, dat_k4.
3. Mengacak squence generator untuk memilih urutan baris/row data yang akan disisipkan.
4. Mengisolasi komponen warna merah (R), hijau (G), biru (B) pada cover image.
5. Mengecek setiap pixel pada R dengan kondisi sebagai berikut: Posisi 2 LSB untuk setiap pixel pada i baris/row dan j kolom dengan R indikator:

   Jika r(i, j, 7)=0 dan r(i, j, 8)=0 maka tidak ada penyisipan/embed
   Jika tidak r(i, j, 7)=0 dan r(i, j, 8)=1 maka embed k bit pada plane hijau (G)
   Jika tidak r(i, j, 7)=1 dan r(i, j, 8)=0 maka embed k bit pada plane biru (B)
   Jika tidak semuanya maka embed k bit pada G dan B
6. Mengulangi langkah 4sesuai dengan jumlah data yang akan disisipkan pada cover image.
7. Menyatukan warna merah (R), stego hijau, stego biru menjadi sebuah warna baru yang disebut steg1, steg2, dan seterusnya.
8. Melakukan langkah 4 dan 5 dengan menggunakan urutan data 4 biner untuk mendapatkan 4 stego image yang berbeda (S1, S2, S3, S4).
9. Mengkomparasikan 4 stego image dengan data baris/row cover image untuk mendapatkan masing-masing deviasi plane
10. Pilih plane yang terdiri dari kombinasi hasil dari 4 parent stego image.
11. Simulasikan pilihan baris/row dengan urutan sebagai berikut:
    Row steg1 diambil dari 00
    Row steg2 diambil dari 01
    Row steg3 diambil dari 10
    Row steg4 diambil dari 11
12. Menyatukan secara berurutan pada masing-masing plane menjadi pixel (p1, p2, dan seterusnya).
13. Hasilnya menjadi 1 gambar stego image dan kunci berurutan/sequence

3. METODE

Adapun alur rancangan secara umum dari metode Kriptografi Blowfish dan steganografi Heksa bisa dilihat pada gambar 3.



Gambar 3 Alur implementasi metode penggabungan kriptografi Blowfish dengan steganografi Heksa

Penjelasan gambar 3 Alur Rancangan implementasi metode:

1. Pengirim menginputkan 2 file, yaitu file plaintext sebagai pesan teks biasa yang akan dikirimkan dan file cover image sebagai file gambar yang hanya digunakan untuk penyisipan data rahasia/plaintext.
2. Data plaintext dienkripsi dengan menggunakan kriptografi Blowfish, hasilnya disebut cypertext,
3. Setelah dienkripsi menjadi cypertext data disisipkan pada file cover image dengan teknik steganografi Heksa.
4. Hasil dari steganografi tersebut menjadi sebuah file yang disebut dengan stego image. Pada stego image akan dilakukan pengujian hasil sebagaimana akan dijelaskan nanti.
5. Untuk mengambil data plaintext kembali maka dilakukan ekstrak data pada stego image dengan teknik steganografi Heksa. Keluarannya berupa file cover image dan cypertext.
6. Cypertext didekripsi dengan kriptografi Blowfish, keluarannya berupa plaintext.

7. Penerima mendapatkan 2 file yaitu plaintext/pesan sebenarnya yang dikirimkan oleh pengirim dan file cover image.
8. Hasil outputnya dari aplikasi ini berupa file stego image yang kemudian dilakukan pengujian hasil metode, yang akan dijelaskan pada pembahasan berikutnya.

4. IMPLEMENTASI DAN PEMBAHASAN

4.1 Implementasi

Dalam tahap ini akan dilakukan implementasi sistem, yakni penerapan program integrasi Kriptografi Blowfish dengan Steganografi Heksa menggunakan bahasa pemrograman Visual Basic 6.0. Program yang dibuat disebut dengan nama BlenBlow.

4.2 Sampel Gambar dan Plaintext

Sampel teks yang digunakan untuk penyisipan ke cover image pada penelitian ini adalah file bertipe TXT yang berukuran 5.656 bytes

Adapun sampel image diambil dari database laboratorium SIPI-USC (Signal and Image Processing Institute – University of Southern California). Database gambar SIPI-USC adalah kumpulan gambar standar yang dapat digunakan untuk penelitian gambar dan analisis citra. Sampel gambar yang diambil adalah gambar yang berkarakteristik foto udara dari luar angkasa dengan ukuran gambar 512x512 pixel, kedalaman warna 24 bit per pixel, serta ukuran file sebesar 786.572 bytes dengan format file TIFF, dan nama filenya "2.1.02.tiff" yang bisa didownload di (http://sipi.usc.edu/database/database.php).

Sedangkan untuk melakukan pengujian gambar format file diubah menjadi tipe Bitmap (BMP), dikarenakan format BMP adalah format standar yang biasa digunakan untuk menampilkan gambar dan belum mengalami perubahan kompresi warna. Oleh karena itu file sampel gambar akan dikonversi dahulu dari format TIFF menjadi BMP dengan program Microsoft Paint. Gambar 4 menampilkan file yang sebagai sampel gambar pada penelitian ini.

Gambar 4 Sampel gambar yang digunakan

4.3 Tampilan GUI BlenBlow

Aplikasi yang dirancang pada penelitian ini disebut dengan nama BlenBlow yang dapat dilihat pada gambar 5.

Gambar 5 Tampilan GUI BlenBlow

4.4 Hasil dan Analisis

4.4.1 Hasil Pengujian Ketahanan

Pada tahap ini akan dilakukan pengujian untuk membuktikan pencapaian keamanan implementasi steganografi Heksa. Adapun teknik pengujian ini menggunakan uji ketahanan (*rebustness*), yaitu hasil gambar dari proses steganografi akan dimanipulasi dengan menggunakan beberapa teknik olahan atau pengeditan gambar untuk membuktikan bahwa data yang disisipkan mampu diekstrak atau diambil kembali atau data sisipan rusak (Wijaya, 2014).

Paramater keamanan yang digunakan pada pengujian ketahanan ini adalah mengukur seberapa banyak jumlah olahan gambar yang bisa/mampu diekstrak oleh steganografi DCS dan Heksa. Semakin banyak jumlah olahan gambar yang bisa diekstrak maka semakin tinggi tingkat dalam mengamankan atau mempertahankan data sisipan. Sebaliknya semakin sedikit jumlah olahan gambar yang bisa diekstrak maka semakin lemah teknik steganografinya (Poornima & Iswarya, 2013).

Proses pengujian ketahanan ini dilakukan dengan mengolah/mengedit satu file sampel gambar menjadi 30 olahan gambar. Dalam mengolah gambar penelitian ini menggunakan program *AutoImager* (Autoimager, 2015). Pada setiap hasil olahan gambar diekstrak dengan steganografi DCS dan Heksa. Kemudian dibandingkan jumlah yang mampu diekstrak oleh DCS dan Heksa. Tabel 1 menampilkan 30 olahan gambar dan hasil ekstrak steganografi DCS dan Heksa.

Tabel 1 Hasil pengujian ketahanan steganografi DCS dan Heksa

No	Uji olahan gambar	Stegano DCS		Stegano Heksa	
		Hasil ekstrak	Nilai	Hasil ekstrak	Nilai
1.	Add noise	Bisa	Level 300	Bisa	Level 300
2.	Anti alias	Bisa	Threshold 150	Bisa	Threshold 150
3.	Brightness	Bisa	150 %	Bisa	
4.	Color resolution	Bisa	8 bit	Bisa	8 bit
5.	Contras	Bisa	150 %	Bisa	150 %
6.	Crop	Gagal		Gagal	
7.	Deskew	Gagal		Gagal	
8.	Despeckle	Bisa		Bisa	
9.	Dpi	Bisa	96 dpi	Bisa	96 dpi
10	Max filter	Gagal		Gagal	
11	Median	Bisa	Size 3	Bisa	Size 3
12	Min filter	Gagal		Gagal	
13	Mosaic	Gagal		Gagal	
14	Motion blur	Gagal		Gagal	
15	Multiply	Gagal		Gagal	
16	Oilify	Gagal		Gagal	
17	Old photo	Gagal		Gagal	

18	Pixelate	Gagal		Gagal	
19	Polar	Gagal		Gagal	
20	Posterize	Gagal		Gagal	
21	Zoom wave	Bisa		Bisa	
22	Resample	Gagal		Gagal	
23	Resize	gagal		Gagal	
24	Rotate	Bisa	180^0	Bisa	180^0
25	Saturation	Gagal		Gagal	
26	Sharpen	Bisa	100 %	Bisa	100 %
27	Unsharp mask	Bisa	Amount 100	Bisa	Amount 100
28	Waggle	Gagal		Gagal	
29	Wave shear	Gagal		Bisa	Horizontal 100
30	Convert tipe	Bisa	JPG MAX	Bisa	JPG MAX
Jumlah		**10**		**11**	

Dari hasil file stego image yang diolah gambar sebanyak 30 olahan, bahwa ada 11 olahan gambar yang mampu diekstrak oleh Heksa dan 19 olahan gambar yang lainnya tidak bisa diekstrak data teksnya, sedangkan DCS mampu mengekstrak 10 gambar olahan.

Melihat hasil dari uji ketahanan di atas bisa disimpulkan bahwa tingkat keamanan Heksa dalam mempertahankan data sisipan lebih kuat dari pada steganografi DCS, sehingga bisa dikatakan Heksa lebih aman digunakan untuk penyampaian pesan teks.

4.4.2 Hasil Analisis PNSR

Peak Signal to Noise Ratio (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya noise yang berpengaruh pada sinyal tersebut (Ansari, 2015). PSNR merupakan parameter standar untuk menilai kualitas suatu citra secara obyektif dengan membandingkan noise cover image dan stego image terhadap sinyal puncak dalam satuan desibel (dB) (Ansari, 2015). PSNR sering digunakan untuk mengukur kualitas file gambar asli (cover image) dengan file gambar sisipan (stego image). Untuk menghitung nilai PSNR, terlebih dahulu harus menghitung nilai MSE (*Mean* Squared Error) dengan menggunakan persamaan:

$$\text{MSE} = \frac{1}{M.N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \left(f(x,y) - g(x,y) \right)^2$$

Keterangan :

f(x,y) = nilai piksel cover image

g(x,y) = nilai piksel stego image

M, N = merupakan dimensi citra

Kemudian menghitung nilai PSNR menggunakan persamaan berikut :

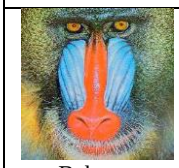
$$\text{PSNR} = 20.\log 10 \left(\frac{255}{\sqrt{MSE}} \right)$$

Pada penelitian ini PSNR digunakan untuk menentukan tingkat noise cover image dan stego image. Semakin tinggi nilai PNSR maka semakin sedikit perubahan yang terjadi pada cover image dan stego image, artinya steganografi akan semakin tidak terdeteksi. Nilai MSE yang tinggi menandakan kualitas penyisipan data kurang baik dan sebaliknya nilai yang tinggi PSNR menandakan kualitas penyisipan data sangat baik. Stego image yang baik harus memiliki nilai PSNR diatas 35dB (Cheddad, 2010).

Paramater keamanan yang digunakan pada analisis PNSR adalah mengukur nilai PNSR pada stego image steganografi DCS dan Heksa. Semakin tinggi nilai PNSR maka semakin tidak terdeteksi stego image, artinya semakin baik dalam meningkatkan penyampaian pesan teks dan semakin rendah nilai MSE maka semakin baik dalam meningkatkan penyampaian pesan teks.

Proses analisis PNSR pada penelitian ini menggunakan 4 sampel gambar (cover image). Pada setiap sampel gambar disisipi pesan teks dengan teknik DCS dan Heksa. Kemudian pada masing-masing stego image ditentukan nilai PNSR. Kemudian dibandingkan nilai PNSR stego image DCS dengan Heksa. Tabel 2 menampilkan perbandingan hasil analisis PNSR stego image DCS dan Heksa.

Tabel 2 Perbandingan analisis PNSR stego image DCS dan Heksa

Sampel gambar	Stego image DCS		Stego image Heksa	
	MSE	PNSR	MSE	PNSR
 Sky	0,1523	40,4943	0,0694	58,2938
 Temple	0,1938	40,2948	0,0657	58,4256
 Lena	0,1203	41,3384	0,0746	59,4059
 Baboon	0,1637	41,3984	0,0785	59,3419

Pada tabel 2 bisa dilihat bahwa nilai PNSR gambar Sky dengan penyisipan data steganografi DCS bernilai 40,4943 dan nilai MSE 0,1523, sedangkan pada steganografi Heksa nilai PNSR 58,2938 dan nilai MSE 0,0694. Nilai PNSR Heksa

lebih tinggi dari pada PNSR DCS dan nilai MSE Heksa lebih rendah dari MSE DCS, maka hasil stego image pada gambar Sky Heksa lebih baik dari DCS. Pada gambar Temple nilai PNSR steganografi DCS bernilai 40,2948 dan nilai MSE 0,1938, sedangkan pada steganografi Heksa nilai PNSR 58,4256 dan nilai MSE 0,0657. Nilai PNSR Heksa lebih tinggi dari pada PNSR DCS dan nilai MSE Heksa lebih rendah dari MSE DCS, maka hasil stego image pada gambar Temple Heksa lebih baik dari DCS. Pada gambar Lena nilai PNSR steganografi DCS bernilai 41,3384 dan nilai MSE 0,1203, sedangkan pada steganografi Heksa nilai PNSR 59,4059 dan nilai MSE 0,0746. Nilai PNSR Heksa lebih tinggi dari pada PNSR DCS dan nilai MSE Heksa lebih rendah dari MSE DCS, maka hasil stego image pada gambar Lena Heksa lebih baik dari DCS. Pada gambar Baboon nilai PNSR steganografi DCS bernilai 41,3984 dan nilai MSE 0,1637, sedangkan pada steganografi Heksa nilai PNSR 59,3419 dan nilai MSE 0,0785. Nilai PNSR Heksa lebih tinggi dari pada PNSR DCS dan nilai MSE Heksa lebih rendah dari MSE DCS, maka hasil stego image pada gambar Baboon Heksa lebih baik dari DCS.

Pada 4 gambar sampel tersebut semua nilai PNSR Heksa lebih tinggi dari pada nilai PNSR DCS dan nilai MSE Heksa lebih rendah dari MSE DCS, maka dengan parameter analisis PNSR dapat disimpulkan bahwa steganografi Heksa lebih baik dari pada steganografi DCS. Tabel 3 menampilkan ringkasan selisih nilai perbedaan PNSR DCS dengan Heksa.

Tabel 3 selisih nilai MSE PNSR DCS dengan Heksa

Sampel gambar	Selisih MSE DCS terhadap Heksa	Selisih PNSR DCS terhadap Heksa
Sky	-0,0829	17,7995
Temple	-0,1281	18,1308
Lena	-0,0457	18,0675
Baboon	-0,0852	17,9435

Pada tabel 3 nilai PNSR Heksa lebih tinggi dari pada nilai PNSR DCS dan nilai MSE Heksa lebih rendah dari MSE DCS, maka dapat disimpulkan bahwa steganografi Heksa lebih baik dari pada steganografi DCS.

Berdasarkan hasil dari pengujian ketahanan dan analisis dengan PNSR, maka bisa dibuat tabel kesimpulan yang bisa dilihat pada tabel 4.

Tabel 4 Kesimpulan analisis DCS dan Heksa

Pengujian	Parameter keamanan	Hasil DCS	Hasil Heksa
Uji ketahanan	Semakin banyak olahan gambar yang bisa diekstrak maka semakin kuat steganografi dalam mempertahankan data teks sisipan	Mampu mengektrak 10 dari 30 olahan gambar	Mampu mengektrak 11 dari 29 olahan gambar
Analisis PNRS	Semakin tinggi nilai PNSR maka semakin tinggi tidak terdeteksi stego image	Nilai 4 gambar PNSR DCS lebih rendah dari Heksa	Nilai 4 gambar PNSR DCS lebih tinggi dari Heksa

Melihat dari tabel 4 maka dapat disimpulkan bahwa steganografi Heksa lebih baik dari DCS dalam segi uji ketahanan dengan selisih satu olahan gambar dan lebih baik dari segi analisis PNRS dengan nilai 4 gambar PNRS Heksa lebih tinggi dari DCS. Dari kesimpulan tersebut maka steganografi Heksa layak untuk digunakan sebagai keamanan penyampaian pesan teks.

5. KESIMPULAN

Berdasarkan hasil yang didapat dari proses implementasi dan pembahasan maka penelitian Implementasi Metode Kriptografi Blowfish Menggunakan Steganografi Heksa dapat ditarik kesimpulan:

1. Peningkatan Keamanan ganda pada penyampaian teks digital bisa mengimplemetasikan integrasi kriptografi Blowfish dengan steganografi Heksa dengan menggunakan aplikasi yang bernama BlenBlow.
2. Berdasarkan hasil pada tabel 4 dapat membuktikan bahwa implementasi dari program BlenBlow layak untuk digunakan penyampaian pesan teks yang lebih aman.

6. DAFTAR PUSTAKA

1. Autoimager. http://www.autoimager.com/download.asp. Diakses pada 1 September 2015
2. Ansari, Munawir. (2015). Komparasi Metode Hybrid Image Watermarking DWT-SVD Dengan RDWT-SVD Untuk Proteksi Pada Citra Digital. Yogyakarta, fakultas Teknologi Industri, Universitas Islam Indonesia.
3. Boora & Gambhir. (2013). Arnold Transform Based Steganography. International Journal of Soft Computing and Engineering (IJSCE). ISSN: 2231-2307, Volume-3, Issue-4.
4. Cheddad, A., Condell, J., Curran, K., Kevitt, P.Mc., 2010. Digital Image Steganography : Survey and Analysis of Current Methods. Signal Processing, Elsevier. Northern Ireland, UK.
5. Gutte, Chincholkar and Lahane. (2013). Steganography For Two And Three Lsbs Using Extended Using Extended Substitution Algorithm. Ictact Journal On Communication Technology, March 2013, volume: 04, issue: 01.
6. Haldankar & Kuwelkar. (2014). Implementation Of Aes And Blowfish Algorithm. International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308.
7. Padmaa. & Venkataramani. (2014). Encypted Secret Heksa With Image Steganography For Enhanced Imperceptibility Dan Capacity. Tamilnadu India.
8. Poornima & Iswarya. (2013). AN OVERVIEW OF DIGITAL IMAGE STEGANOGRAPHY. International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1,February 2013.
9. SIPI, The USC-SIPI Image Database, website pada http://sipi.usc.edu, diakses pada 24 Agustus 2015.
10. Wijaya, Wijaya Satriya. (2014). Integrasi Metode Steganografi DCS Pada Image Dengan Kriptografi Blowfish. Yogyakarta, fakultas Teknologi Industri, Universitas Islam Indonesia.
11. Wijaya, Satriya. & Prayudi, Yudi. (2014). Konsep hidden message menggunakan teknik steganografi dynamic cell spreading. Jurnal media informatika, ISSN: 0854-4743, Volume 2. NO. 1, PP 23-38.
12. Yadav. (2011). Information Security Using Heksa of Steganography and Cryptography. Int. J. Comp. Tech. Appl., Vol 2 (6), 2023-2036. ISSN:2229-6093
13. Kumar and Karthikeyan. 2012. Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms. I. J. Computer Network and Information Security, 2012, 2, 22-28. DOI: 10.5815/ijcnis.2012.02.04