PENYIMPANAN KUNCI KRIPTOGRAFI MENGGUNAKAN STEGANOGRAFI DENGAN ALGORITMA GIFSHUFFLE

Megah Mulya*[1]
[1] Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Sriwijaya; Jl.Raya Palembang–Prabumulih km.32, Ogan Ilir 30662, Telp. (0711) 581077 Fax: 0711 580053 Palembang
e-mail: [*1] **megahmulya@yahoo.com**

Abstrak

Kriptografi saat ini telah berkembang menjadi Steganografi yang penyembunyian informasi tanpa memerlukan komputasi algoritma tertentu dalam encode dan decodenya. Salah satu teknik Steganografi untuk menyisipkan pesan pada citra berformat GIF adalah algoritma gifshuflle. Algoritma Steganografi Gifsuffle menarik untuk diteliti karakteristiknya karena pada awalnya algoritma ini lazim digunakan untuk teknik watermark. Pada penelitian ini digunakan untuk teknik steganografi terhadap karakter berupa kunci kriptografi. Persoalan yang akan diselesaiakan dalam penelitian ini adalah bagaimana karakteristik steganografi yang menggunakan gidshuffle. Metode untuk membuktikan karakteristin tersebut adalah dengan tiga langkah saitu langkah pertama mengengbangkan perangkat lunak stegarografi dengan menerapkan algoritma Gifshufle, langkah kedua menganalisa bagaimana kualitas stegoimagenya terhadap karakter dengan PSNR dan berbagai perubahan citra , dan langkah ketiga bagaimana daya tampung terhadap karakter yang mampu disimpan. Penelitian ini menghasilkan kesimpulan perangkat lunak untuk mengetah krakterstik Gifsuffle dan Stegarograi telah berhasil dikembangkan. Penelitian juga menghasilkan kesimpulan Gifshulle mempunyai kapasitas penyisipan sampai 210 karakter yang cukup untuk penyembunyian kunci-kunci kriptografi. Sampai batas karakter yang mampu disimpan kualitas steganografinya adalah bagus ditangai dengan PSNR yang bagus. Sedangkan ketahanan serangan dari perubahan gambar adalah sangat lemah.

Kata kunci: *steganografi, gifshulle, PSNR*

1. PENDAHULUAN

Jaringan komputer memberikan manfaat yang besar bagi manusia terutama sejak hadirnya internet yang telah banyak diakses oleh masyarakat secara luas. Jaringan komputer khususnya internet telah memberikan kemudahan dan berbagai fasilitas yang ditawarkan. Akan tetapi disisi lain membawa ancaman terhadap kepentingan pengguna. Sudah tidak asing lagi terdengar terjadinya kejahatan di internet maupun teknologi jaringan lainnya yang mengakibatkan kerugian.

Untuk tujuan keamanan data pada umumnya digunakan teknik kriptografi yang melibatkan algoritma simetri ataupun asimetri. Kekuatan kedua teknik tersebut bertumpu pada kerahasiaan kunci enkripsi seperti halnya *password* pada beberapa sistem yang menerapkan pengamanan data. Seperti halnya *password* karenai kunci kriptografi menjadi tumpuan kekuatan system keamanan data maka haruslah dijaga sedemikian rupa agar aman dan praktis dalam

pengelolaannya. Sebuah penelitian mengungkapkan adanya kebiasaan ceroboh bahwa masyarakat Indonesia tergolong memiliki password yang paling mudah ditebak. Penyebabnya diantaranya adalah password dibuat hanya berupa kombinasi angka semata, terlalu pendek dan password berupa frasa data pribadi atau password sengaja disimpan(ditulis) dengan ceroboh [1].

Timbulnya ancaman kejahatan dalam jaringan komputer khususnya internet maka memaksa berbagai pihak untuk mencari cara mengamankan sumberdaya yang sedang berada dalam jaringan komputer ataupun sumberdaya yang tersimpan dalam komputer pengguna. Teknologi keamanan data (*data scurity*) telah berkembang pesat karena sudah menjadi kebutuhan pokok di hampir setiap orang/organissai/perusahaan. Sehingga banyak pihak tidak segan mengeluarkan dana yang besar untuk mewujudkan sistem keamanan data yang dinilai handal untuk menunjang bisnisnya.

Sampai saat ini terdapat banyak metode pengmanan data yang dikembangkan termasuk Kriptografi. Kriptografi telah berkembang kearah penyembunyian informasi di dalam suatu media tanpa melibatkan kunci penyandian yang dikenal sebaga Steganografi.Salah satu algoritma Steganografi untuk menyisipkan pesan pada citra berformat GIF adalah algoritma *gifshuflle*. Algoritma *gifshuffle* berbasis pada citra berformat GIF dengan cara memposisikan ulang atau mengacak (shuffle) susunan dari ke-256 palet warna. Penukaran posisi memungkinkan diperolehnya sebuah informasi berkaitan dengan perbedaan posisi awal dan posisi akhir [2]. Algoritma Steganografi Gifsuffle menarik untuk diteliti karakteristiknya karena pada awalnya algoritma ini lazim digunakan untuk teknik watermark. Steganografi dan watermark pada prinsipnya mirip yaitu menyisipkan pesan kedalam suatu media namun berbeda dalam tujuannya. Steganografi dan watermark merupakan sub kajian didalam matakuliah Kriptografi.

Penelitian ini menjawab permasalahan yang akan dikaji diantaranya adalah bagaimana mengembangkan perangkat lunak yang mengimplementasikan metode Gifshuffle untuk meyisipkan pesan rahasia berupa karakter kunci Kriptografi, bagaimanakah kualitas stegoimage setelah dilakukan penyisipan dibanding dengan icitra aslinya? , dan bagaimanakah daya tampung citra terhadap pesan rahasia berupa karakter kunci Kriptografi jika penyisipan dilakukan dengan Gifshuffle.[3]. Sedangkan batasan yang melingkupi penelitian adalah perangkat lunak yang dikembangkan hanya untuk mengukur citra gif terhadap kualitas dan kecepatan, pesan rahasia yang disisipkan dalam Gifshufle diartikan sebagai kunci simetri dalam sekala bit, dan diasumsikan dengan karakter penyisipan ukuran kecil sebagai pesan berupa kunci simetri.

2. METODE PENELITIAN

Penelitianini bertujuan untuk mengetahui karakteristik metode GifShuffle untuk penyisipan kunci kriptografi berkaitan dengan kemampuan menyembunyikan informasi dan ketangguhan penyimpanan informasi tersebut. Dengan diketahuinya karakteristik tersebut maka dengan batasan-batasan yang tepat metode GifShuffle dapat digunakan dalam steganografi dengan optimal sehingga dapat menyembunyikan kunci dengan aman. Secara spesifik permasalahan yang akan dijawab adalah : adanya kebutuhan media penyembunyi pesan berupa kunci kriptografi, karakteristik penyembunyian GifShuffle belum diketahui terhadap variasi panjang kunci dan editing, diperlukan perangkat lunak untuk melihat karakteristik GifShuffle.

Untuk menjawab permasalahan pada penelitian maka dilakukan dengan tigalangkah. Langkah pertama adalah pengembangkan perangkat lunak steganografi GifShuffle dan langkah kedua adalah penentuan karakteristik GifShuffle dengan percobaan perangkat lunak steganografi GifShuffle. Pada langkah pertama penelitian terdapat dua kegiatan taitu menentukan ekuiremen dari konsep GifShuffle. Dari hasil pengambilan *rekuiremen* tersebut selanjutnya dilakukan kegiatan berikutnya yaitu analisis, perancangan , implementasi dan pengujian perangkat lunak.

Langkah berikutnya yaitu melakukan percobaan guna mendapatkan karakteristik GifShuffle dengan alat percobaan perangkat lunak steganografi. Langkah kedua ini berupa kegiatan percobaan. yaitu percobaan untuk mengamati karakteristik terhadap efek pengeditan. Pada langkah ini akan dilihat kualitas citra yang telah disisipi pesan dibandingkan dengan citra aslinya yang belum disisipi pesan.

Langkah berikutnya yaitu melakukan percobaan guna mendapatkan karakteristik GifShuffle dengan alat percobaan perangkat lunak steganografiuntuk mengamati karakteristik terhadap daya tampung pesan stringdidalam citra.

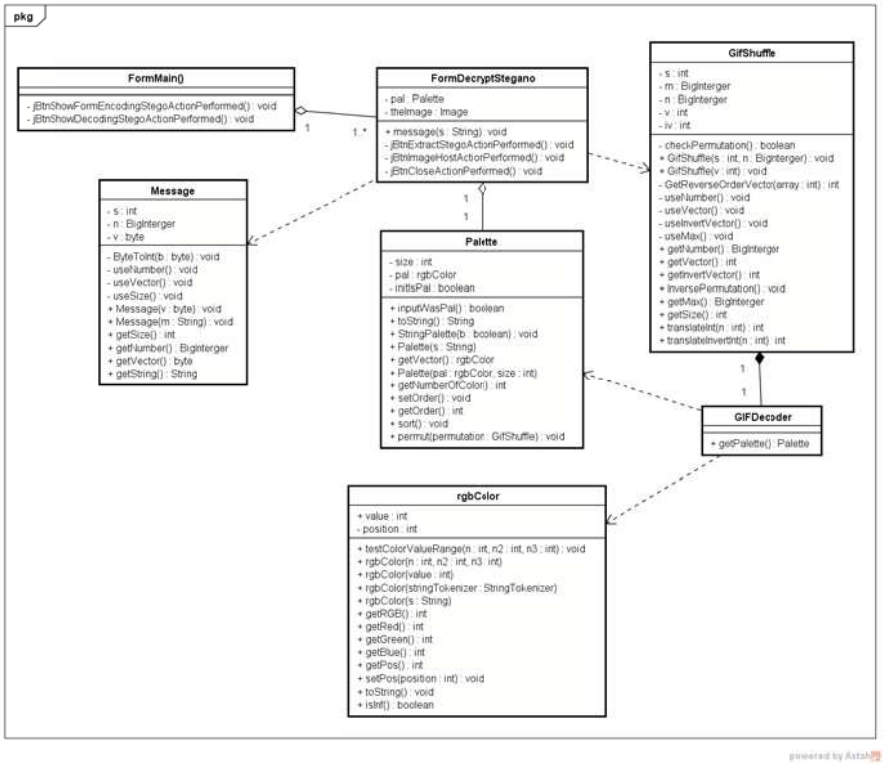
Ketiga langkah dalam penelitian ini diharapkan akan menghasilkan luaran berupa perangkat lunak untuk mengetahui karakteristik GifShuffle dan karakeristik GifShuffle terhadap variasi panjang string (daya tampung) dan variasi editing serta kehandalan GifShuffle untuk penyembunyian kunci simetri dan berbagai batasannya (kualitas). Variabel yang diukur adalah Peak Signal to Noise Ratio (PSNR) untuk mengetahui perbandingan kualitas citra sebelum dan sesudah disisipkan pesan [4].

3. HASIL DAN PEMBAHASAN

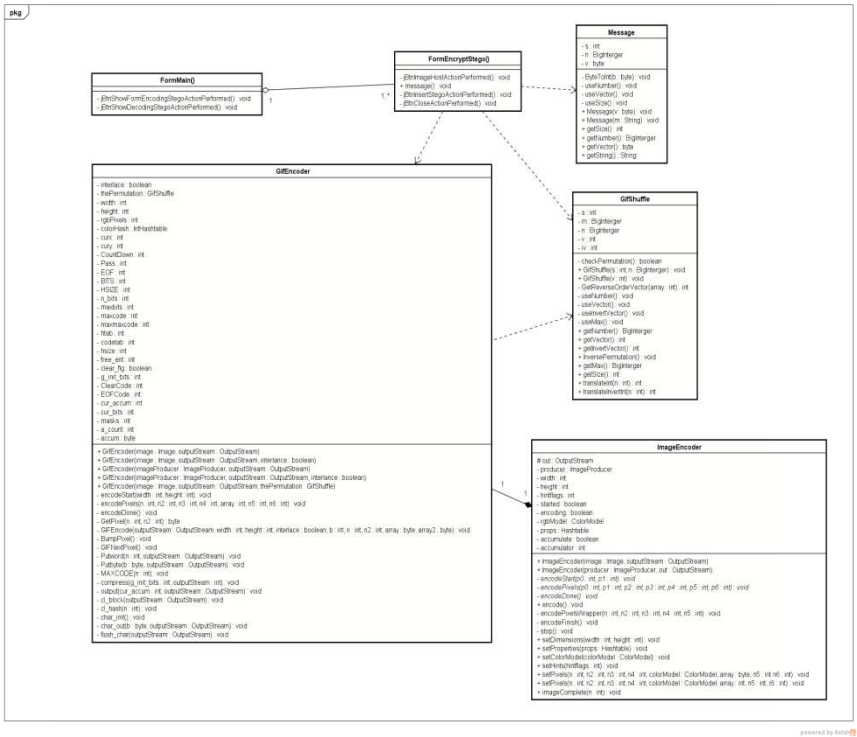
Penelitian ini menghasilkan perangkat lunak steganografi yang menerapkan algoritma Gishuffle untuk penyisipan pesan, telah digunakan untuk percobaan analisa daya tampung terhadap karakter, kualitas citra steganografi setelah disisipi pesan , dan ketahanan citra gif yang telah disisipi terhadap serangan pengeditan.

Perangkat lunak yang dihasilkan dari penelitian dapat dilihat pada gambar 1, gambar 2, dan gambar 3 berupa tampiran antarmuka, kelas diagram decoding dan kelas diagram encoding.

Gambar 1 Tampilan perangkat lunak Steganografi dengan algoritma Gifsuffle



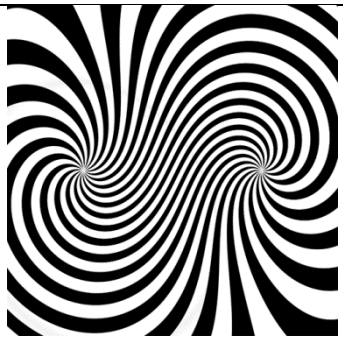
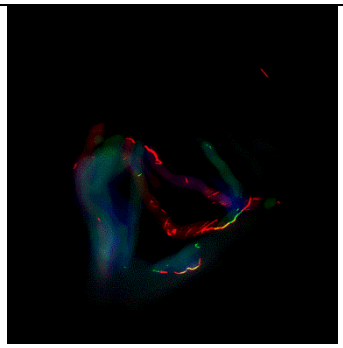
Gambar 2 Kelas diagram encode perangkat lunak Steganografi dengan algoritma Gifsuffle



Gambar 3 Kelas diagram decode perangkat lunak Steganografi dengan algoritma Gifsuffle

Perangkat lunak tersebut digunakan untuk pengujian terhadap data uji yang berupa beberapa citra berformat gif yang dapat dilihat pada table 1. Citra berformat gif tersebut memiliki ukuran 291 kb, 445 kb dan 720 kb.

Tabel 1 Citra Uji dalam penelitian

No	**Citra Uji**	**Ukuran (kb)**
1		291
2		445
3		720

Selanjutnya citra berformat gif tersebut disisipi dengan berbagai panjang karakter dengan panjang 11 karakter, 49 karakter, 129 karakter, 210 karakter dan 211 karakter yang dapat dilihat pada tabel 2. Karakter lebih panjang dari 210 ternyata tidak mampu ditampung oleh citra berformat gif dalam steganografi. Ketidak mampuan citra berformat gif menampung pesan melebihi 210 karakter ditandai dengan gagalnya proses decoding termadap karakter yang semula di encoding. Sedangkan untuk berbagai panjang karakter yang lebih pendek atau sama dengan 210 semua proses encoding dapat dikembalikan dengan decoding seperti semula. Citra berformat gif yang telah tersisipi karakter dengan panjang tidak lebih dari 210 dilakukan uji PSNR. Uji PSNR untuk mengukur tingkat perbedaan antara citra asli tanpa dititipi dengan citra yang telah disisipi karakter. Dari hasil pengujian menunjukkan semuanya bernilai infinity atau

baik. Hasil uji terhadap kapasitas tampung citra terhadap jumlah karakter dan pengukuran PSNR dapat dilihat pada tabel 3.

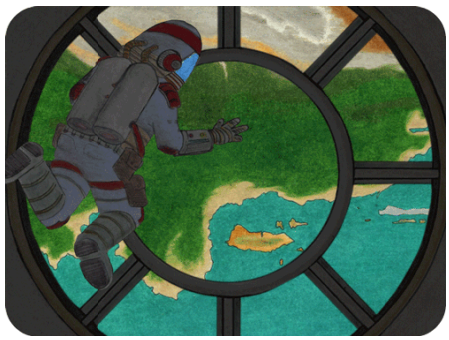
Tebal 2 Pesan yang akan disisipkan

Pesan ke	Isi Pesan	Ukuran Pesan (byte)
1	industrious	11
2	User modelling for a computer coach: a case study	49
3	****The Project Gutenberg Edition of THE WORLD FACTBOOK 1992**** ******This file should be named world92.zip or world92.txt******	129
4	This projected audience is one hundred million readers. If our value per text is nominally estimated at one dollar, then we produce a million dollars per hour; next year we will have to do four text file .....!	210
5	This projected audience is one hundred million readers. If our value per text is nominally estimated at one dollar, then we produce a million dollars per hour; next year we will have to do four text file .....!.	211

Tabel 3. Hasil Uji *Encode-Decode* Pesan dan PSNR Algoritma Gifshuffle

Pesan	Citra Uji 1	Citra uji 2	Citra Uji
1	Sukses: sukses PSNR: infinity	Sukses:sukses PSNR: infinity	Sukses:sukses PSNR: infinity
2	Sukses:sukses PSNR: infinity	Sukses:sukses PSNR: infinity	Sukses:sukses PSNR: infinity
3	Sukses:sukses PSNR: infinity	Sukses:sukses PSNR:infinity	Sukses:sukses PSNR: Infinity
4	Sukses:sukses PSNR: infinity	Sukses:sukses PSNR: infinity	Sukses:sukses PSNR: infinity
5	Sukses:gagal *encode* PSNR: -	Sukses: gagal *encode* PSNR: -	Sukses: gagal *encode* PSNR: -

Pengujian ketahanan citra yang telah dilakukan steganografi terhadap serangan dilakukan dengan melihat apakah pesan yang disisipkan masih dapat diekstraksi meskipun citra mengalami beberapa perubahan. Beberapa pengujian yang dilakukan adalah horizontal flip, rotasi, scaling, blur dan penambahan titik. Ditra berfomat gif yang digunakan untuk pengujian berukuran 273 x 207 piksel dengan kapasitas 131.1 kb yang dapat dilihat pada gambar 4. Percobaan pengujian terhadap dengan berbagai pengubahan citra gif menunjukkan rentan terhadap serangan tersebut seperti yang dapat dilihat pada tabel 5. Pada kelima pengubahan citra kesemuanya berakibat karakter gagal didecode.



Gambar4 Citra uji ketahanan steganografi dengan gifshuffle berukuran 273 x207 piksel dan size 131.1 kb

Tabel 5. Hasil Pengujian Ketahanan Pesan

No	JenisPenyerangan	GambarsetalahdiberikanEfek	Keterangan
1.	*Horizontal Flip*		Ukuran gambar: 273 x 207 piksel Size: 131.1 kb Penjelasan: Melakukan *flip* gambar secara horizontol Status: Gagal*decode*
2.	Rotasi		Ukuran gambar: 273 x 207 piksel Size: 131.1 kb Penjelasan: Merotasi gambar 180° Status: Gagal*decode*
3.	*Scaling*		Ukuran gambar: 336 x 233 piksel Size: 189 kb Penjelasan: Mengubah skala gambar sebersar 120% Status: Gagal*decode*

4	*Blur*		Ukuran gambar: 273 x 207 piksel Size:114,4 kb Penjelasan: Melakukan balur terhadap gambar Status: Gagal*decode*
5	PenambahanTitik		Ukuran gambar: Size: Penjelasan: Status: Gagal*decode*

4. KESIMPULAN

Penalitian ini memberikan kesimpulan :

1. Perangkat lunak Penyimpanan Kunci Kriptografi Menggunakan Steganografi dengan Algoritma Gifshuffle berhasil dikembangkan.
2. Algoritma Gifshuffle dapat digunakan dalam teknik steganografi untuk menyimpan kunci Kriptografi.
3. Penggunaan algoritma gifshuffle mampu menampung karakter kunci Kriptografi yang disisipkan sampai sejumlah 210 karakter dengan kuaitas stegoimage bagus.
4. Penyimpanan kunci Kriptografi menggunakan algoritma gifshuffle tidak tahan terhadap serangan pengeditan citra .

5. SARAN

Karakter yang disisipkan penelitian ini karena untuk kebutuhan penyembunyian kunci kriptografi maka perlu mempertimbangkan faktor kecepatan encoding dan decoding. Oleh karena itu disarankan pada penelitian selanjutnya dilakukan pengukuran waktu kedua proses encoding dan decoding dalam steganografi.

UCAPAN TERIMA KASIH

Penulis mengucapkan terimakasih epada lembaga penelitian Unsri yang telah memberi dukungan financial terhadap penelitian ini.

DAFTAR PUSTAKA

[1] Bonneau J., 2012, The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords, *IEEE Symposium on Security and Privacy*, San Francisco,.

[2] Penalosa, Ronald A. 2005. Steganografi Pada Citra dengan Format GIF Menggunakan Algoritma Gifshuffle., http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2006-2007/Makalah1/Makalah1-053.pdf, diakses tgl 10 November 2014

[3] Kwan, Matthew. 2003. How Gifshuffle Works. http://www.darkside.com.au/gifshuffle/description.html, diakses tgl 5 Agustos 2014

[4] Pooja Kaushik, Yufvraj Sharma, 2012; Comparison Of Different Image Enhancement Techniques Based Upon Psnr & Mse*, International Journal of Applied Engineering Research*, Vol.7 No.11.