Visual Attack dan *Statistical Attack* pada Aplikasi Steganography

Danang Jaya
Direktorat Analisis Sinyal Deputi Pengamanan Persandian Lembaga Sandi Negara
Jl. Harsono RM no 70, Ragunan, Pasar Minggu, Jakarta Selatan
danang.jaya@lemsaneg.go.id

Abstrak

Aplikasi Steganography merupakan apliasi penyembunyian informasi berupa teks atau citra pada citra. Aplikasi ini berjalan di sistem operasi Android versi 4.0 atau diatasnya dan dapat diunduh secara gratis dari google play. Aplikasi ini dikembangkan oleh Jan Meznik secara perorangan. Steganography versi 1.0 memiliki ukuran sebesar 672 kb yang terakhir kali di *update* pada tanggal 25 April 2014. Aplikasi ini dilengkapi pilihan masukan *password* sebagai tambahan pengamanan informasi yang disembunyikan.

Visual Attack merupakan cara pengujian adanya penyisipan nilai bit pada *pixel* citra secara sekuensial. Beberapa tehnik *visual attack* adalah metode Bitplane LSB dan *Enhanced* LSB. *Statistical attack* dapat digunakan untuk menentukan apakah fenomena adanya penyembunyian data acak dalam suatu citra. Beberapa tehnik *Statistical attack* antara lain adalah Chi-Square *Attack* dan *histogram analysis attack*.

Hasil pengujian dengan menggunakan *visual attack* tidak ditemukan informasi atau petunjuk letak penempatan informasi. Berdasarkan hasil pengujian Bitplane LSB dan *Enhanced* LSB tidak bisa menemukan adanya indikasi penyimpanan informasi secara sekuensial. Sedangkan hasil *Statistical Attack* juga tidak bisa menunjukkan adanya rangkaian terenkripsi pada lokasi sekuensial tertentu. Dari hasil pengujian berdasarkan *visual attack* dan *statistical attack* dapat diindikasikan bahwa aplikasi Steganography menyembunyikan informasi pada lokasi yang acak. Sehingga perlu dikaji lebih lanjut mengenai algoritma pengacakan lokasi dan atau sheet pembangkit lokasi acak tersebut.

Kata Kunci -- Steganography, Android, *Visual Attack*, *Statitical Attack*

A. Pendahuluan

Steganografi merupakan seni atau ilmu yang banyak digunakan untuk menyembunyikan suatu pesan rahasia dalam suatu media[1]. Algoritma steganografi yang paling umum diimplementasikan adalah *least siginificant bit* (LSB). Selain cepat dalam proses embedding juga mudah implementasinya dalam citra audio bahkan video tak terkecuali pada aplikasi berbasis Android[2-4]. Hal ini pula yang memicu banyaknya teknik-teknik yang digunakan untuk melakukan deteksi terhadap penerapan algoritma LSB tersebut.

Beberapa teknik yang digunakan untuk melakukan teknik deteksi keberadaan pesan tersembunyi berdasarkan suatu algoritma LSB antara lain adalah *visual attack* dan *statistic attack*. *Visual attack* digunakan untuk mendeteksi adanya suatu pesan tersembunyi secara LSB yang disisipkan pada citra secara sekuensial. Sedangkan *statistic attack* digunakan untuk mengetahui fenomena penyembunyian data acak/terenkrisi pada suatu media [5].

Aplikasi Steganography merupakan apliasi penyembunyian informasi berupa teks atau citra pada citra. Aplikasi ini berjalan di sistem operasi Android versi 4.0 atau diatasnya dan dapat diunduh secara gratis dari google play. Aplikasi ini dikembangkan oleh Jan Meznik secara perorangan. Steganography versi 1.0 memiliki ukuran sebesar 672 kb yang terakhir kali di update pada tanggal 25 April 2014. Aplikasi ini dilengkapi pilihan masukan password sebagai tambahan pengamanan informasi yang disembunyikan[6].

Pengujian terhadap aplikasi Steganography telah dilakukan dengan menguji ketahanan dari stego citra. Dengan melakukan pengiriman hasil embedding citra logo pada media citra maka didapat hasil bahwa citra stego tidak tahan terhadap kompresi dari media sosial whatsapp, facebook dan

BBM[6]. Tetapi dalam penelitian ini tidak disimpulkan mengenai algoritma penyisipan dari aplikasi Steganography tersebut.

Tujuan melakukan kajian tersebut adalah untuk mengetahui algoritma penyisipan yang ditawarkan oleh aplikasi Steganograhy. Hal ini penting dilakukan agar para pengguna merasa nyaman dalam menggunakan aplikasi tersebut mengingat sangat terbatasnya aplikasi-aplikasi tentang penyembunyian informasi yang disediakan Google Play.

Penulisan makalah hasil kajian ini secara umum akan dibagi menjadi beberapa bagian yaitu pendahuluan, pembahasan dan simpulan. Pada bagian pedahuluan akan dijelaskan mengenai latar belakang kajian tersebut dilakukan, perkembangan penggunaan metode dan tujuan dilakukannya kajian. Bagian kedua akan menjelaskan mengenai pembahasan percobaan-percobaan yang dilakukan untuk mendapatkan hasil yang diharapkan.

B. Pembahasan

1. Data yang digunakan

Untuk melakukan kajian terhadap penggunaan algoritma penyisipan pada aplikasi Steganography maka akan digunakan data-data sebagai berikut:

a. Laptop Sony Vaio dengan processor i7 ram 8 GB dan hardisk 256 GB SSD
b. Matlab 2010
c. Smartphone Galaxy Tab 2.0 dengan sistem operasi android 4.2
d. Citra Lena.bmp *grayscale* dengan ukuran 512 x 512 *pixel* sebagai citra *cover* dengan ukuran 258 kb
e. Citra logo.bmp *grayscale* dengan ukuran 32 x 32 pixel, 64 x 64 *pixel*dan 128 x 128 *pixel* dan 256 x 256 *pixel* dengan ukuran berturut-turut adalah3 kb, 6 kb dan 18 kb.
f. Teks input dengan rincian sebagai berikut
   - Karakter huruf ‘AAAAAAAAAA’ (10 huruf A)
   - Karakter huruf ‘AA ..AA’ (100 huruf A)

Adapun citra Lena.bmp dan citra logo.bmp dapat dilihat seperti pada Gambar 1a dan 1b (dengan ukuran disesuaikan).

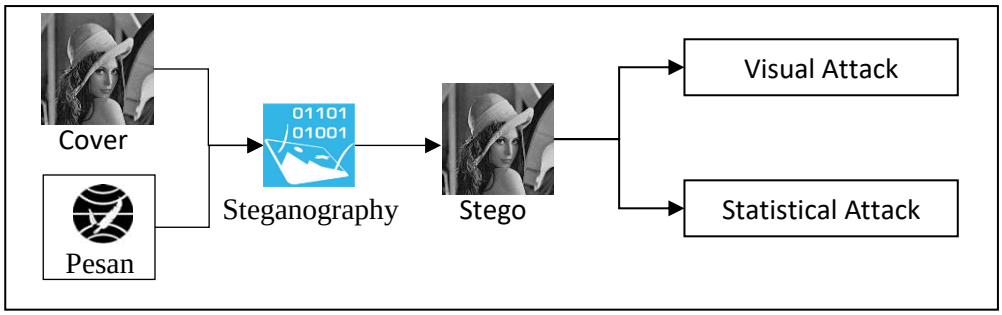
a

b

Gambar 1. Data yang digunakan

2. Mekanisme percobaan

Dalam melakukan percobaan kali ini, mekanisme yang digunakan adalah seperti terlihat pada Gambar 2. Pada gambar tersebut dijelaskan bahwa Pesan yang merupakan citra logo.bmp atau teks disisipkan ke citra cover Lena.bmp dengan menggunakan aplikasi Steganography. Hasil dari masing-masing citra stego per pesan dilakukan *visual attack* dan *statistical attack*.



Gambar 2. Mekanisme percobaan

3. Hasil Implementasi Data Uji

Dari data pesan yang disisipkan ke dalam citra cover, didapat hasil implementasi seperti terlihat pada Tabel 1. Keseluruhan file output dari aplikasi Steganography berbentuk file png. Citra png memiliki3 layer, sedangkan citra cover yang digunakan hanya memiliki 1 layer. Dari tabel tersebut pula dapat dilihat perbandingan *peak signal noise to ratio* (PSNR) dari citra cover dengan masing-masing layer hasil aplikasi Steganography. Secara umum citra hasil implementasi aplikasi steganography dapat dilihat pada Gambar 3.

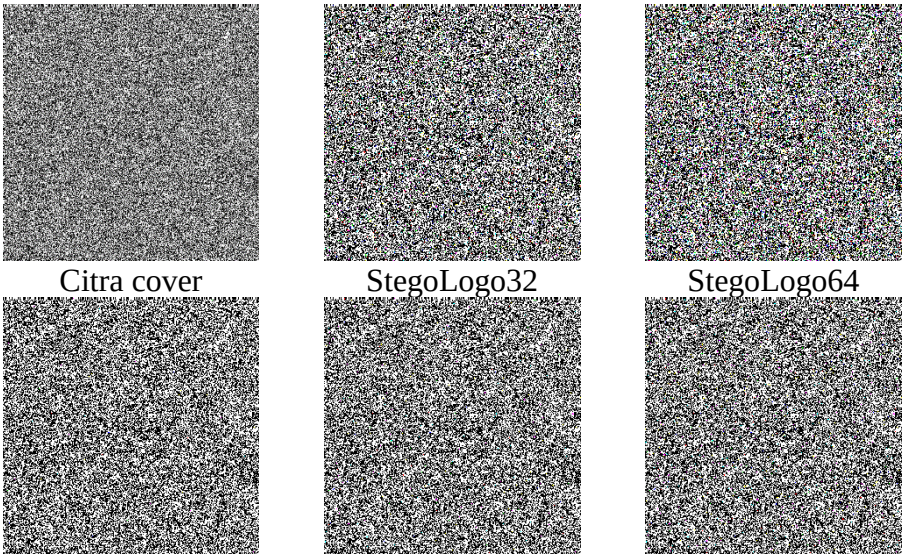
Tabel 1. Hasil implementasi Data Uji

No	Pesan	Citra Stego			
		Ukuran file	PSNR (1)	PSNR (2)	PSNR (2)
1	Logo32.bmp	252 kb	118,7385	118,3785	118,7386
2	Logo64.bmp	269 kb	114,9754	114,9754	115,0113
3	Logo128.bmp	Pesan “Destination Image is not big enough ...”			
4	Huruf A sebanyak 10	239 kb	126,5025	126,5025	126,3987
5	Huruf A sebanyak 100	241 kb	124,6492	124,6492	124,6721
6	Huruf A Sebanyak 320	244 kb	121,9836	121,9836	122,0272

Gambar 2. Citra hasil penyisipan pesan

4. *Visual Attack*

Beberapa tehnik visual attack yang umum digunakan adalah enhanced LSB dan bitplane LSB. Kedua tehnik tersebut mirip yaitu dengan menampilkan urutan bit tertentu saja. Ide dasar dari teknik *enhanced* LSB adalah dengan mengambil atau menampilkan *bit-bit* LSB saja. Metode ini seringkali juga dikelompokkan dalam kategori penapisan (*filtering*). Jika citra yang dikenakan *enhanced* LSB mengandung pesan maka secara kasat mata dapat diamati adanya kejanggalan pada gambar yang sudah ditapis. Hasil implementasi *enhanced* LSB pada citra hasil penyisipan pesan dapat dilihat pada Gambar 3.



Gambar 2. Citra hasil penyisipan pesan

Secara visual dari Gambar 2 dapat dilihat bahwa tidak terdapat kejanggalan (artefak) pada masing-masing citra hasil *enhanced* LSB. Mulai dari citra cover sampai dengan citra berpesan secara keseluruh tidak terdapat perbedaan secara visual. Hal ini dapat disimpulkan bahwa kemungkinan besar algoritma penyisipan pada aplikasi steganography tidak dilakukan secara sekuensial.

5. *StatisticalAttack*

Statistical attack untuk keperluan steganoanalisis menggunakan *chi square*. Konsep dibalik *chi square attack* adalah bahwa bit-bit LSB didalam citra tidak sepenuhnya acak seperti yang dipikirkan orang. Jika bit-bit tersebut diubah secara sederhana (misalnya dengan menggantinya dengan bit-bit pesan) maka penyerang dapat mengetahuinya dengan menggunakan pendekatan statistik. *Chi square attack* merupakan serangan berbasis statistik yang menganalisis histogram dari PoV (*pairs of value*).

Dalam prakteknya, chi square attack dilakukan secara progresif dengan persentase sampel yang meningkat. Pada mulanya 1% sampel diuji lalu 2% dan seterusnya hingga 100%. Citra yang diduga terdapat pesan dipindai mulai dari sudut kiri atas terus kekanan hingga seluruh pixel dievaluasi (100%).

Dengan menggunakan *statistical attack* terhadap seluruh citra yang diuji maka didapat seperti terlihat pada Tabel 2. Dengan persentase sampling mulai dari 10 sampai dengan 100 didapat nilai 0 (nol) untuk keseluruhan uji. Hal ini berarti tidak ditemukan pesan dalam mode acak atau terenkripsi pada citra uji. Hal yang sama berlaku untuk nilai ambang 0.5 dan 0.7.

Tabel 2. Statistical attack dengan nilai ambang 0.9

No	Nama File	Persentase sampling									
		10	20	30	40	50	60	70	80	90	100
1	Citra Cover	0	0	0	0	0	0	0	0	0	0
2	StegoLogo32	0	0	0	0	0	0	0	0	0	0
3	StegoLogo64	0	0	0	0	0	0	0	0	0	0
4	StegoHurufA10	0	0	0	0	0	0	0	0	0	0
5	StegoHurufA100	0	0	0	0	0	0	0	0	0	0
6	StegoHurufA320	0	0	0	0	0	0	0	0	0	0

C. Simpulan dan Saran

Dari penjelasan bagian A dan B maka dapat diambil kesimpulan bahwa dengan menggunakan *visual attack* dan *statistical attack* tidak menunjukkan pentunjuk penggunaan algoritma LSB pada aplikasi Steganography. Hasil percobaan yang dapat ditindaklanjuti adalah mengetahui pola penyisipan pesan ke dalam media citra tersebut dilihat dari ukuran besar file yang akan bertambah seiring dengan bertambahnya ukuran file pesan yang disisipkan.

D. Daftar Pustaka

[1] Eric Cole, 2003, *Hiding in Plain Sight: Steganography and the Art of Covert Communication*, Wiley Publishing Inc

[2] Alexandre Miguel Ferreira, 2015. *An Overview on Hiding an Detecting Stego-Data in Video Stream*. System & Network Engineering Research Project II, University of Amsterdam, Belanda

[3] Purba, J. V., Situmorang, M., & Arisandi, D. 2012, Implementasi Steganografi Pesan Text ke Dalam File Sound (.wav) dengan modifikasi jarak byte pada algoritma least significant bit (LSB). *Jurnal Dunia Teknologi Informasi* 1(1), 20-55.

[4] Azis Ardiansyah Wahyudi. 2014. *Implementasi Steganografi Berkas File MP3 Menggunakan Metodde LSB (Least Significant Bit) pada Perangkat Mobile Android*. Skripsi. Program Studi Teknik Informastika. Universitas Islam Negeri Sunan Kalijaga.

[5] Westfeld, A. and Pfitzmann, A. 2000. Attack on Steganographic systems. 3rd International Workshop. *Lecture Note in Computer Science*, Springer Verlag Berlin, 1768

[6] Jan Meznik. 2014, Steganography, (online). https://play.google.com/store/apps/details?id=com.meznik.Steganography, diakses 11 November 2015

[7] Danang Jaya, 2015, Bermain intelijen Sinyal dengan

[8] Danang Jaya, 2015, *Uji Ketahanan (Robustness Test) Algoritma Steganografi pada Aplikasi Media Sosial Berbasis Smartphone*, KNS&I 2015 STIKOM Bali, 9 Oktober 2015, Bali