Uji Ketahanan (Robustness Test) Algoritma Steganografi Pada Aplikasi Media Sosial Berbasis Android

Danang Jaya
Lembaga Sandi Negara
Jl. Harsono RM no 70, Ragunan, Pasar Minggu Jakarta Selatan, 0217805814
e-mail: danang.jaya@lemsaneg.go.id

Abstrak

Algoritma dasar steganografi yang umum digunakan antara lain adalah LSB dan DCT. Masing-masing algoritma dasar steganografi ini mempunyai tingkat ketahanan yang berbeda-beda pada suatu perubahan atau serangan.Beberapaaplikasi media sosialdalam aplikasi smartphone antara lain adalah whatsapp, Blackberry, Facebook dan Telegram. Masing-masing aplikasi memiliki cara tersendiri dalam melakukan layanan pengiriman pesan berbentuk citra. Beberapa layanan media sosial terbukti merusak isi pesan dalam steganografi. Percobaan dengan menggunakan aplikasi steganography yang dikirimkan melalui media sosial menunjukkan bahwa pesan tidak dapat dibuka untuk beberapa media sosial dan utuh pada BBM dengan permintaan HD dan pengiriman file pada Telegram.

Kata kunci: *Steganografi, media sosial*

1. Pendahuluan

Perkembangan teknologi sarana komunikasi dan elektronik memudahkan seseorang untuk melakukan pengiriman informasi dengan mudah dan cepat. Informasi dalam bentuk citra sangat mudah dilakukan penggandaan, modifikasi dan penyebaran dengan memanfaatkan sarana komunikasi. Pada sekitar tahun 2005 banyak digunakan MMS atau email untuk alternatif sarana mengirimkan citra. Beberapa tahun terakhir sosial media menjadi sarana favorit dalam pengiriman citra. Hal ini dimanfaatkan oleh pengembang sosial media untuk memberikan layanan-layanan pengubahan dan pengiriman pesan citra yang cepat dan murah.

Beberapa aplikasi sosial media yang banyak digunakan adalah whatsapp dan facebook. Media sosial ini menempati urutan atas dalam penggunaannya di dunia khususnya Indonesia[1]. Meskipun banyak terdapat sosial media lainnya masih menggunakan aplikasi *messenger* lain seperti BBM, Line, Instagram dan Twitter[2]. Meskipun BBM sudah tidak primadona lagi karena banyaknya aplikasi serupa, tetapi dengan adanya BBM versi android maka aplikasi ini masih tetap bersaing dalam penggunaan media sosial di Indonesia. Aplikasi-aplikasi tersebut banyak dikembangkan dalam *smartphone*.

Aplikasi media sosial pada *smartphone*seperti Facebook, Whatsapp dan BBM merupakan aplikasi yang memberikan fasilitas pengiriman citra.Dalam penggunaannya, pengiriman citra dalam media sosial dapat bertujuan untuk komunikasi rahasia atau bersifat bisnis citra digital. Pengiriman citra dalam usaha komunikasi rahasia umumnya dikenal sebagai steganografi sedangkan yang bersifat bisnis umumnya berkaitan dengan *watermarking*. Steganografi dan *watermarking* mempunya hubungan yang erat dalam kesamaan algoritma dasarnya.

Permasalahan yang muncul adalah bahwa tidak ada satupun media sosial yang menyediakan fitur steganografi atau watermarking. Aplikasi steganografi yang tersedia berbasis android dalam google play sangatlah terbatas dan tidak ada yang dikembangkan oleh suatu perusahaan. Aplikasi steganografi berbasis android yang ada saat ini terpisah dengan aplikasi media sosial dan dikembangkan secara individu. Hal ini tentu membutuhkan suatu kecocokan antara aplikasi media sosial dan aplikasi steganografi yang ada tergantung kepentingannya.[3]

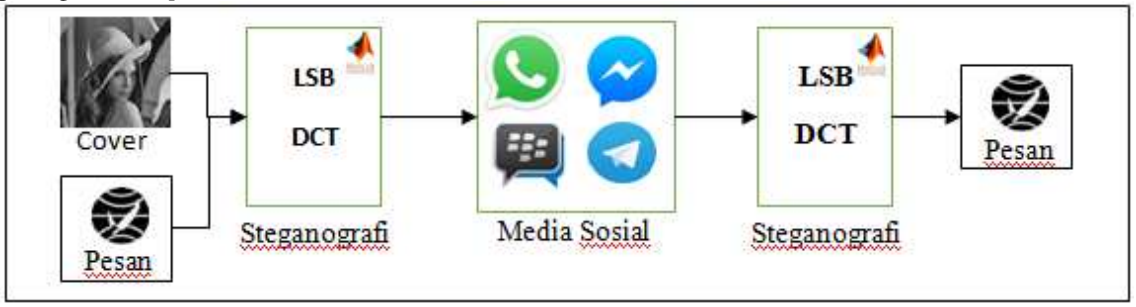
Algoritma-algoritma steganografi yang berkembang saat ini memiliki daya tahan berbeda terhadap perubahan media pembawanya. Permasalahan yang muncul adalah bahwa masing-masing aplikasi steganografi yang ada di Googe Play tidak menyebutkan algoritma yang digunakannya. Dengan mengetahui algoritma atau kemampuan dari aplikasi, diharapkan akan dapat mempermudah penggunaan steganografi atau *watermarking* yang disesuaikan dengan tujuan pengguna media sosial.

Dalam makalah ini penulis akan menjelaskan mengenai uji terhadap suatu ketahanan algoritma dasar steganografi terhadap perlakukan media *cover* dalam proses pengiriman dalam sosial media. Algoritma steganografi yang dipilih adalah algoritma dasar steganografi seperti LSB, DCT dan SVD. Sedangkan media sosial yang dipilih adalah yang penulis anggap paling banyak digunakan seperti whatsapp, Facebook Messsenger dan BBM yang berjalan di *smartphone*.

2. Metode Penelitian

2.1 Mekanisme I

Mekanisme pertama yang ditawarkan menggunakan algoritma standar steganografi yang diprogram menggunakan Matlab. Percobaan dengan menggunakan program matlab untuk memastikan bahwa algoritma dasar steganografi berjalan sesuai harapan. Secara umum mekanisme tersebut dapat dilihat pada Gambar 4. Hasil penyembunyian pesan dalam citra cover selanjutnya dikirimkan melalui aplikasi media sosial. Dalam proses ini tentu ada pemindahan file stego citra dari komputer ke dalam perangkat *smartphone*.



Gambar 4. Mekanisme pengiriman steganografi pada citra

Pengiriman stego citra melalui media sosial dengan memanfaatkan layanan kirim citra atau attach file jika memungkinkan . Untuk aplikasi whatsapp dan facebook messenger hanya memiliki layanan pengiriman citra tetapi tidak memiliki layanan pengiriman file. Sedangkan aplikasi BBM dan Telegrm memiliki saranan layanan pengiriman file. Citra pada BBM dan Telegram akan dilakukan pengiriman melalui dua layanan tersebut.

Penerima stego citra dari media sosial selanjutnya melakukan proses ekstraksi untuk mendapatkan pesanyang dimaksud. Mekanisme ekstraksi disesuaikan dengan algoritma kriptografi yang digunakan. Hasil pesan yang didapat selanjutnya dibandingkan dengan pesan yang dikirim untuk dilakukan perbandingan. Perbandingan dimaksudkan untuk mengetahui adanya perubahan dalam pesan tersbut karena adanya perlakuan dari media sosial. Perbandingan pesan asli dengan pesan hasil ekstraksi menggunakan perhitungan standar jarak untuk suatu titik, yaitu norm.

2.2 Mekanisme II

Mekanisme kedua yang ditawarkan adalah dengan memanfaatkan aplikasi yang tersedia di google play store. Aplikasi bernama Steganography ini merupakan aplikasi untuk melakukan penyembunyian pesan yang dapat berupa teks atau citra ke dalamsuatu citra. Konsep ini tentu sama dengan konsep steganography pada umumnya. Mekanisme kedua secara umum dapat dilihat pada Gambar 5.Mekanisme ini lebih ditujukan untuk mengetahui algoritma steganografi yang digunakan dalam aplikasi steganography.

Gambar 5. Mekanisme pengiriman dengan memanfaatkan aplikasi Steganography

3. Hasil dan Pembahasan

Untuk melakukan implementasi dari mekanisme yang ditawarkan pada bagian III maka dalam melakukan percobaan digunakan peralatan dan data sebagai berikut:

1. Smartphone, akan digunakan smartphone Galaxy Tab 2.0 dengan sistem operasi android 4.2.
2. Laptop Sony Vaio dengan procesor i7 ram 8 GB dan hardisik 256 GB SSD.
3. Matlab 7.
4. Citra Lena.bmp *grayscale* ukuran 512 x 512 *pixel* sebagai citra *cover*dengan ukuran 258 kb dan citra logo.bmp *grayscale* 64 x 64 *pixel* sebagai citra pesan dengan ukuran 6 kb.

Hasil dari percobaan dengan menggunakan aplikasi media sosial didapat perbedaan output jenis file dan ukuran dari file citra yang dikirim. Perubahan ukuran file dan jenis file citra hasil pengiriman dengan media sosial tersebut dapat dilihat pada Tabel 2. Dari tabel tersebut dapat disimpulkan bahwa masing-masing media sosial melakukan proses kompresi terhadap citra yang dikirimkan. Pada pengiriman citra melalui BBM didapat pilihan dalam permintaan HD request, artinya selain citra terkompresi, pengguna dapat meminta citra dalam ukuran asli tetapi tetap dalam jenis file jpg. Sedangkan untuk pengiriman file citra dalam Telegram tetap diterima dalam bentuk file bmp.Pada aplikasi steganography digunakan data cover dan pesan menghasilkan file citra png dengan ukutan 270 kb.

Tabel 2. Ukuran citra output

Media Sosial	Ouput	
	Citra	File
WhatsApp	36 kb jpg	-
Facebook Messenger	31 kb jpg	-
Blackberry Messenger	31 kb jpg	258 kb jpg (HD)
Telegram	36 kb jpg	258 kb bmp
Steganography	270 kb png	-

Percobaan ektraksi terhadap hasil pengiriman citra melalui media sosial dapat dilihat pada Tabel 3. Keberhasilan dari ektraksi tersebut hanya diukur dengan menggunakan persepsi visual. Hal ini karena adanya perbedaan yang signifikan antara hasil yang ektraksi dengan kategori berhasil dan tidak. Untuk pesan yang tidak berhasil diektraksi pada program matlab yang dibuat memberikan hasil bahwa output ektraksi sebagian besar tidak bisa ditampilkan sebagai citra. Hal ini terutama berlaku untuk algoritma LSB dan aplikasi steganography.

Pada hasil pengiriman citra menggunakan algoritma DCT berhasil diektraksi pada BBM dengan permintaan HD dan pengiriman citra melalui *attach file* pada telegram. Hasil yang didapat dalam kondisi berhasil diektraksi sangat jelas sedangkan jika tidak memunculkan informasi tidak dapat ditampilkan dalam bentuk citra atau citra hitam.

Tabel 3. Hasil ekstraksi

Media Sosial	LSB		DCT		Steganography	
	Citra	File	Citra	File	Citra	File
WhatsApp	×	-	×	-	×	-
Facebook Messenger	×	-	×	-	×	-
Blackberry Messenger	×	√	×	√	×	√
Telegram	×	×	×	√	×	√

4. Simpulan

Dari uraian bagian-bagian penjelasan dari bagian pendahuluan sampai dengan implementasi maka dapat diambil kesimpulan adalah sebagai berikut:

1. Semua media sosial yang dicoba melakukan kompresi pada pengiriman pesan berbentuk citra.
2. Sifat kompresi citra pada media sosial bersifat merusak steganografi yang disisipkan.

3. BBM dengan pengiriman permintaan HD tetap menjaga keaslian citra meskipun dalam format citra yang berbeda.
4. Aplikasi steganography (versi android) mampu bertahan pada pengiriman citra dengan permintaan HD dari BBM dan pengiriman file dari Telegram.

Daftar Pustaka

[1] Steven Millward, *Statistik pengguna internet di dunia dan Indonesia*, https://id.techinasia.com/statistik-pengguna-internet-di-dunia-dan-indonesia-slideshow/, 10 Januari 2014.
[2] Ahmad Fauzi, *Data pengguna Smartphone dan Social Media 2015*, http://lembing.com/data-pengguna-smartphone-dan-social-media-2015/, Agustus 2015.
[3] Danang Jaya, *Bermain intelijen sinyal dengan aplikasi gratis dari android*, Seminar Pengembangan Profersi Fungsional Sandiman 2015, Jakarta, 2015
[4] Eric Cole, *Hiding in Plain Sight: Steganography and the Art of Covert Communication*, Wiley Publishing Inc, 2003
[5] Juergen Seitz, *Digital Watermarking: An Introduction*, Information Science Publishing, 2005
[6] Tri Prasetyo Utomo, *Steganografi Gambar dengan Metode Least Significant Bit untuk proteksi komunikasi pada media online*, UIN Sunang Gunung Djati Bandung
[7] Nisheh Baksi, *Steganography*, Syracus University, 2007
[8] Nova HadiL, *Steganografi: Implementasi menggunakan matlab*, Diktat pelatihan Steganografi, 2014
[9] Cox, I., Miller, M., & Bloom, J., *Digital Watermarking*, Morgan Kaufman, 2001
[10] Cahyana, T. Basaruddin & Danang Jaya, *Tehnik Watermarking Citra Berbasis SVD*, NACSIT 2007.
[11] Wikipedia, Media Sosial, https://id.wikipedia.org/wiki/Media_sosial, diakses Agustus 2015