

PROPOSAL TUGAS AKHIR
Keamanan System Lanjut - EC7010
Dosen : Dr. Ir. Budi Rahardjo

Oleh:
Irianto
23203014
Option Sistem Cerdas dan Kendali
Program Pasca Sarjana Teknik Elektrro
Institut Teknologi Bandung
2004

Judul : Embeding Pesan Rahasia Dalam Gambar

Abstrak

Dalam paper ini akan diuraikan tentang “Embeding Pesan Rahasia Dalam Gambar” dengan menggunakan teknik steganography, yang mana Embeding Pesan Rahasia Dalam Gambar adalah merupakan penyembunyian suatu pesan rahasia dengan cara mengembedkan (menyatukan) pesan tersebut dalam suatu gambar JPEG khususnya dan gambar lainnya secara umum.

Pesan Rahasia yang diembedkan dalam gambar disini dilakukan dengan menggunakan teknik steganografi yang kami batasi untuk gambar diam dan dalam format JPEG, walaupun proses tersebut juga dapat diterapkan untuk format lainnya. Steganografi adalah suatu seni dan sains untuk menyembunyikan informasi atau pesan yang bersifat rahasia dengan menyembunyikan pesan tersebut pada media cover yang lain misalnya gambar, sedemikian rupa sehingga tidak menimbulkan kecurigaan bagi pihak lawan. Pada masa lalu, orang menggunakan tattoo tersembunyi atau tinta tak tampak untuk menyampaikan isi pesan steganografi, sekarang ini dengan teknologi komputer dan jaringan telah tersedia sehingga mudah menggunakan saluran komunikasi, maka berkembang pula teknik-teknik steganografi. Pertumbuhan akhir-akhir ini dalam teknologi komputasional tersebut mendorong perkembangan steganografi untuk menyembunyikan pesan rahasia diterapkan dalam teknik-teknik keamanan system, dimana embedding pesan rahasia dalam gambar telah menjadi suatu aplikasi bidang-bidang yang penting, seperti penyembunyian catatan copyright atau nomor serial dan juga pencegahan pencopian secara langsung dari orang-orang yang tidak berhak.

Proses embedding pesan rahasia dalam system steganorafi pada dasarnya dilakukan dengan mengidentifikasi media covernya yaitu redundant bit yang mana dapat dimodifikasi tanpa merusak integritas dari medium itu sendiri. Proses embedding akan menghasilkan suatu medium stego dengan penggantian bit-bit redundant dengan data dari pesan rahasia tersebut. Teknik steganografi dapat digunakan untuk menyembunyikan data dalam gambar digital dengan sedikit atau tanpa terasa adanya perubahan yang tampak pada gambar tersebut dan dapat dieksploitasi untuk mengekspor pesan rahasia. Karena gambar sering dikompres dalam penyimpanan atau pengirimannya, maka steganografi yang efektif harus menggunakan teknik coding untuk mencegah terjadinya error akibat algoritma kompresi yang lossy. Kompresi JPEG (Joint Photographic Expert Group), walaupun menghasilkan distorsi visual sedikit, tetapi tetap saja menghasilkan error yang cukup besar dalam data bitmap. Hal ini menunjukkan bahwa, disamping error yang disebabkan proses kompresi, pesan dapat diencode secara steganografi kedalam data pixel sedemikian rupa sehingga dapat di kembalikan lagi setelah proses JPEG, meskipun dengan hasil yang tidak terlalu akurat sekali.

Dalam penyajian makalah, uraian dibagi dalam beberapa bab seperti berikut:

1. Pendahuluan
2. Embedding Pesan Rahasia Dalam Gambar
3. Deteksi Pesan Rahasia Dalam Gambar
4. Hasil Percobaan
5. Kesimpulan
6. Lampiran : Algoritma

(Note : bab-bab akan diubah sesuai bahan yang sedang kami pelajari)

Referensi:

1. Christian Cachin, "Digital Steganography", Switzerland, 2004.
2. Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn "Information Hiding: A Survey".
3. Prof. Gene Tsudik, "ImageDowngrading: A steganographic technique to hide secret messages".
4. A. Westfeld and A. Pfitzmann, "Attack on Steganography Systems", Springer-Verlag, 1998.
5. T. Zhang and X. Ping, "A Fast and Effective Steganalytic Technique Against JSteg-like Algorithms," Proc. 8th ACM Symp. Applied Computing, ACM Press, 2003.
6. S. Lyu and H. Farid, "Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines," Springer-Verlag, 2002.
7. Derek Upham: Jsteg, 1997, e. g. <http://www.tiac.net/users/korejwa/jsteg.htm>.
8. Andreas Westfeld: The Steganographic Algorithm F5, 1999. <http://wwwrn.inf.tu-dresden.de/~westfeld/f5.html>