Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Tugas Besar I IF4020 Kriptografi
Sem. II Tahun 2014/2015

Perbandingan Tiga Metode Steganografi pada Citra Digital Berbasis Metode Modifikasi LSB

Selain dengan enkripsi, keamanan pesan juga dapat dilakukan dengan metode steganografi. Pesan disimpan di dalam media digital seperti citra sedemikian sehingga keberadaan tidak dapat dideteksi. Penyembunyian pesan di dalam citra dilakukan sedemikian sehingga tidak merusak kualitas citra (Gambar 1). Algoritma steganografi sederhana pada citra digital adalah dengan algoritma modifikasi LSB. Nilai bit LSB pada *pixel-pixel* citra diganti dengan bit-bit pesan. Untuk meningkatkan keamanan, maka penyisipan pesan ke dalam *pixel-pixel* citra tidak dilakukan secara sekuensial, tetapi secara acak. Oleh karena itu, pembangkit bilangan acak dibutuhkan untuk membangkitkan posisi *pixel*. Pembangkit bilangan acak ini tergantung pada kunci (yang akan menjadi *seed* atau nilai awal untuk memulai pembangkitan). Pada proses ekstraksi pesan, kunci ini dibutuhkan kembali untuk membangkitkan bilangan acak yang sama (lihat Gambar 1).

Pada praktekmya, sebelum disisipkan, pesan dienkripsi terlebih dahulu dengan sebuah algoritma enkripsi. Karena anda baru belajar algoritma kriptografi klasik, maka algoritma enkripsi yang digunakan adalah *Vigenere Cipher* (*extended* untuk alfabet 256 karakter) seperti yang pernah dikerjakan pada Tucil 1.

Sudah banyak riset yang telah dilakukan untuk mengembangkan metode modifikasi LSB. Tujuan riset tersebut adalah bagaimana meningkatkan kapasistas data yang disisipkan namun tidak mengurangi fifelity citra. Dua paper terlampir (format pdf) memaparkan pengembangan metode modifikasi LSB untuk mencapai tujuan tersebut:

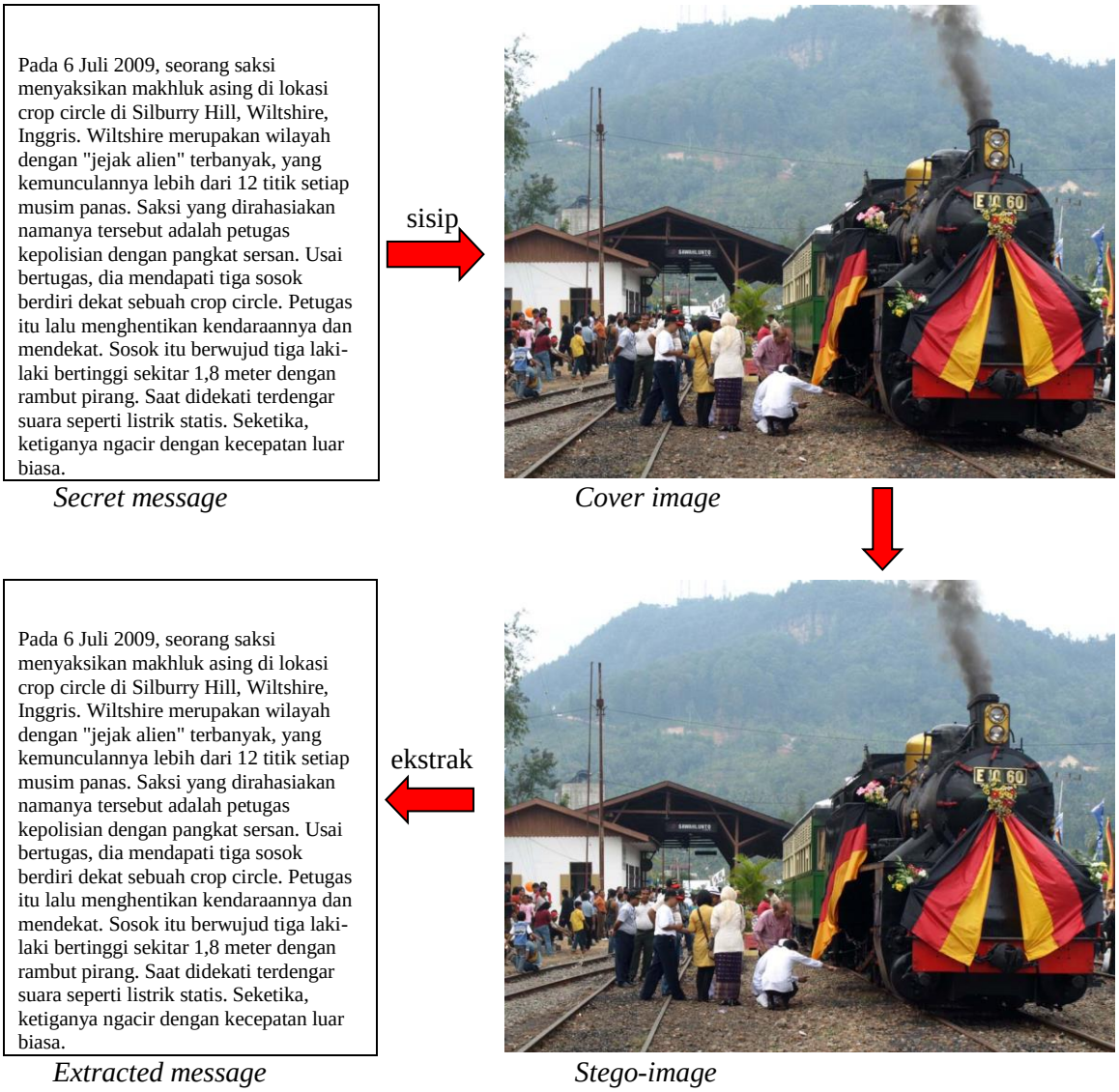
1. *A steganographic method for digital images with four-pixel differencing and modified LSB substitution*, oleh Xin Liao,, Qiao-yan Wena, Jie Zhang.
2. *Digital Image Steganography using Nine-Pixel Differencing and Modified LSB Substitution*, oleh Gandharba Swain

Dalam tugas besar ini, anda diminta membuat program steganografi pada citra *bitmap* (*berwarna* dan *grayscale*) dengan tiga buah metode modifikasi LSB:

1. Metode modifikasi LSB standard (seperti yang telah dijelaskan di dalam kuliah)
2. Metode modifikasi LSB yang dikembangkan oleh Xin Liao dkk
3. Metode modifikasi LSB yang dikembangkan oleh Gandharba Swain.

Selanjutnya anda membandingkan kinerja ketiga buah metode tersebut dari aspek PSNR dan kapasitas data yang dapat disisipkan.

Format citra yang digunakan adalah citra *bitmap* yang tidak terkompresi meskipun ukurannya lebih besar dibandingkan format yang terkompresi (misalnay JPEG). Anda harus memahami format *file* citra *bitmap* agar tahu cara memanipulasi bit LSB-nya. Pesan yang disisipkan adalah sembarang *file* dengan ukuran yang tidak melebihi kapasitas penyisipan (*payload*). Kapasitas penyisipan dihitung sebelum proses penyisipan.



Gambar 1. Penyisipan dan ekstraksi pesan rahasia pada citra *bitmap*

Spesifkasi program:

1. Program menerima masukan berupa citra digital, nama file pesan, dan kunci steganografi.
2. Pesan harus dienkripsi dengan *Vigenere Cipher* sebelum disisipkan ke dalam citra.
3. Pengguna memasukkan sebuah kata kunci yang berfungsi dua: sebagai kunci enkripsi pada *Vigenere Cipher* dan sebagai kunci (*seed*) pembangkitan bilangan acak.
   Contoh: Kunci = 'STEGANO', kunci ini langsung dijadikan sebagai kunci enkripsi.
   Untuk *seed* berupa bilangan acak (yang umumnya berupa integer/real), maka nilai-nilai integer dari string 'STEGANO' dijumlahkan, yaitu Int('S') + Int('T') + Int('E') + Int('G') + Int('A') + Int('N') + Int('O') = ...
   Atau, hanya mengambil sebagian huruf dari STEGANO, misalnya karakter pada posisi ganjil saja, yaitu Int('S') + Int('E') + Int('A') + Int('O') = ..., atau terserah cara yang anda gunakan.
4. Jangan menyisipkan kunci di dalam file citra.
5. Program menolak menyisipkan pesan jika ukuran file pesan melebihi kapasitas maksimal yang dapat disisipkan.
6. Program dapat menyimpan *stego-image* (citra yang sudah disisipi pesan)..

7. Program dapat mengekstraksi pesan utuh seperti sediakala dan menyimpannya sebagai file dengan nama lain (*save as*).
8. Agar format file hasil ekstraksi diketahui, maka properti file seperti ekstensi (.exe, .doc, .pdf, dll), sebaiknya juga disimpan (atau nama file asli juga disimpan.agar diketahui formatnya, sehingga ketika di-*save a*s yang muncul adalah nama file asli tersebut, lalu pengguna dapat menggantinya dengan nama lain). Penyimpanan nama file (dan properti lainnya) tentu akan mengurangi kapasitas pesan yang dapat disimpan.
9. Program dapat menampilkan (*view*) citra asli dan citra stegano dalam dua jendela berbeda.
10. Program dapat menampilkan ukuran kualitas citra hasil steganografi dengan *PSNR* (*Peak Signal- to-Noise Ratio*). *PSNR* adalah metrik yang umum digunakan untuk mengukur kualitas citra. *PSNR* dihitung dengan rumus:

$$PSNR = 20 \times \log_{10}\left(\frac{256}{rms}\right) \quad (1)$$

yang dalam hal ini 256 adalah nilai sinyal terbesar (pada citra dengan 256 derajat keabuan), dan *rms* (*root mean square*) adalah akar pangkat dua dari kuadrat selisih dua buah citra I dan $\hat{I}$ yang berukuran $M \times N$:

$$rms = \sqrt{\frac{1}{MN}\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{ij} - \hat{I}_{ij})^2} \quad (2)$$

Satuan *PSNR* adalah desibel (dB). *PSNR* menyatakan visibilitas derau di dalam citra. *PSNR* yang besar mengindikasikan nilai *rms* yang kecil; *rms* kecil berarti dua buah citra mempunyai sedikit perbedaan. Dari praktek pengolahan citra, citra dengan PSNR > 30 masih dapat dianggap kualitasnya bagus, tetapi jika PSNR < 30 dikatakan kualitas citra sudah terdegradasi secara signifikan.
11. Citra uji yang digunakan adalah beberapa citra uji standard (Lenna, peppers, cameraman, boat, dll) dan citra natural lainnya.
12. Untuk mengukur kinerja masing-masing metode (kapasitas data versus PSNR), maka lakukan pengujian dengan mengalirkan bit-bit data sebanyak kapasitas maksimal, sembunyikan dengan metode LSB yang diuji, lalu hitung PSNR. Rangkumlah hasil pengujian anda seperti contoh tabel berikut (tapi anda ganti kolomnya dengan Metode LSB standard, Metode LSB 2 (Liao dkk), Metode LSB 3 (Swain))

Table 3
Comparisons of the results between Wu et al.'s and ours.

Covers	Wu et al.[11]		Ours	
	Capacity	PSNR	Capacity	PSNR
Elaine	760182	37.28	821640	38.98
Lena	768612	37.35	810564	39.57
Baboon	729526	36.36	903580	36.90
Peppers	774985	37.48	805492	39.79
Toys	772678	37.18	816852	39.36
Girl	771137	37.48	808584	39.61
Gold	768850	37.42	816892	39.27
Barb	738908	35.43	871184	37.67
Zelda	778303	37.70	797268	40.16
Tiffany	772946	37.35	805760	39.77
Average	763613	37.10	825782	39.11

13. Fitur-fitur lainnya dipersilakan dibuat.

Prosedur Pengerjaan

1. Tugas dikerjakan secara berkelompok (1 kelompok @ 3 orang), dilarang *gabut*, dilarang menggunakan kode program orang lain. Cantumkan pembagian tugas dengan jelas antara anggota kelompok.
2. Waktu pengumpulan tugas: paling lambat 27 Februari 2015 sebelum pukul 17.00 di Lab IRK). Terlambat menyerahkan tugas, nilai = 0.
3. Kakas pengembangan program bebas (Java, .NET, Delphi, Visual C, dll)
4. Yang diserahkan pada saat pengumpulan antara lain:
    a. Disket atau CD yang berisi program sumber (*source code*), arsip siap eksekusi (*executable file*) (termasuk semua *.dll* jika ada), dan arsip-arsip uji (citra, file pesan).
    b. Laporan yang memiliki sistematika sebagai berikut :
        i. Teori singkat (steganografi, metode modifikasi LSB standard, metode modifikasi LSB dari Liao dkk, Metode modifikasi LSB dari Swain.
        ii. Implementasi program, termasuk : rancangan program.
        iii. Pengujian program dan analisis hasil. Uji program dengan bermacam-macam citra *bitmap* dan bermacam-macam file pesan.
        iv. Pengujian kinerja seperti yang dijelaskan pada butir 12 pada spesifikasi program.
        v. Kesimpulan dari hasil implementasi.
        vi. Tampilkan foto anda bertiga di *cover* laporan sebagai pengganti logo gajah.

    Laporan dikumpulkan dalam bentuk *hard copy* dan *soft copy* dengan format *.pdf .

4. Penilaian tugas dilakukan pada saat demo.