

IMPLEMENTASI STEGANOGRAPHY PLUS MINUS 1 (PM1) DENGAN BINARY PARTICLE SWARM OPTIMIZATION (BPSO)

Erianov¹, Tjokorda Agung Budi Wirayuda², Bedy Purnama³

¹Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Privacy merupakan hak setiap orang untuk menjaga informasi yang ia punya untuk tidak diberitahukan kepada public atau hanya orang tertentu saja yang mengetahuinya. Steganografi merupakan salah satu teknik data hiding yang menunjang aspek privacy. Steganografi dapat didefinisikan teknik penyisipan data pada sebuah citra cover dimana diharapkan tidak akan merusak struktur maupun visual dari citra cover sebagai medium penyisipan. Dengan adanya Steganografi maka sebuah medium terlihat seperti aslinya ketika sebuah pesan disisipkan yang tidak lain salah satu karakteristik steganografi yaitu fidelity. Pada tugas akhir ini akan dilakukan optimasi pada steganografi. Adapun metode steganografi yang digunakan adalah Plus Minus 1 (PM1) dengan Binary Particle Swarm Optimization (BPSO). BPSO digunakan untuk melakukan optimasi kualitas citra sehingga ketika pesan disisipkan maka medium penyisipan mirip dengan medium aslinya. Parameter kualitas citra yang akan dilihat pada optimasi ini adalah PSNR, MSE dan BER.

Kata Kunci : Steganography, Binary Particle Swarm Optimization, Plus Minus 1

Abstract

Privacy is the right of everyone to keep the information which had to not be notified to the public or only certain people know about it. Steganography is a technique of data hiding to support aspects of privacy. Steganography can be defined as technique of data hiding on a cover image of which is expected it will not make the structure of the visual image of the cover as well as embedding medium cover broken down . Here implemented steganography which would be optimized . The steganographic method used was Plus Minus 1 (PM1) with Binary Particle Swarm Optimization (BPSO). BPSO used to perform optimization of image quality so that when embedding message in the medium cover, medium cover will be similar to the original one. Image quality parameters that would be use in this optimization process is PSNR, MSE and BER.

Keywords : Steganography, Binary Particle Swarm Optimization, Plus Minus 1

Telkom
University

BAB 1

PENDAHULUAN

1.1 LATAR BELAKANG

Privacy dapat dikatakan sebagai hak seseorang untuk menjaga informasi yang ia punya untuk tidak diberitahukan pada public atau hanya orang tertentu saja yang dapat mengetahui informasi tersebut. Seiring dengan perkembangan teknologi dimana setiap orang dapat saling membagikan informasi yang ia punya, Informasi yang ada dapat menjadi ancaman yang membahayakan sehingga keamanan sebuah informasi menjadi sangat penting. Misalnya data history pasien , informasi data intelijen , dll.

Dilihat dari sisi kewanitaan sebuah Informasi maka sebuah sistem teknologi informasi hendaknya mendukung aspek Confidentiality (Privacy), Integrity, Availability, Authentication, Acces Control dan Non-Repudition ^[3]. Salah satu metode untuk menjamin adanya keamanan informasi adalah steganography ^[3]. Secara harfiah, Steganografi berasal dari bahasa Yunani yang mempunyai arti "menulis terselubung" (steganos = terselubung, graphein = menulis)¹. Steganografi adalah teknik untuk menyembunyikan data pada data lain sebagai medium, tanpa merusak medium baik secara struktur dan visual.

Penelitian mengenai metode steganografi telah banyak diteliti dan disimulasikan ^[1]. Algoritma Particle Swarm Optimization (PSO) merupakan salah satu metode metaheuristik yang pernah ada dan biasanya diimplementasikan untuk permasalahan optimasi ^[12]. Salah satu varian dari PSO adalah Binary Particle Swarm Optimization (BPSO). Yang membedakan BPSO dan PSO adalah representasi solusinya dimana BPSO memakai representasi solusi biner.

Dalam tugas akhir ini, penulis merancang dan menganalisis steganografi plus minus 1 (PM1) dengan menggunakan Binary Particle Swarm Optimization (BPSO) pada citra. Pemakaian varian ini dikarenakan untuk studi kasus PM1 representasi solusi biner sehingga dapat dioptimasi dengan BPSO. BPSO digunakan untuk mengoptimalkan performansi steganografi dengan mencari solusi PM1 yang tepat. Diharapkan dengan metode tersebut dapat dicapai performansi steganografi yang optimal. Adapun performansi steganografi yang menjadi tolok ukur adalah confidentiality, recovery dan robustness.

1.2 PERUMUSAN MASALAH

Berdasarkan latar belakang pada tugas akhir ini maka yang menjadi rumusan masalahnya adalah :

1. Bagaimana mengimplementasikan steganografi PM1 dengan BPSO ?
2. Bagaimana efek penggunaan BPSO untuk optimasi steganografi PM1 dilihat dari MSE, PSNR dan BER
3. Bagaimana pengaruh Parameter BPSO (Jumlah iterasi, Jumlah Partikel) terhadap optimasi steganografi PSNR dan MSE

BATASAN MASALAH :

1. Simulasi dilakukan dengan menggunakan tool Matlab 7.10.0.499 (R2010a)
2. Citra pembawa berukuran $N \times N$ yang kemudian selanjutnya dibagi dan diproses didalam blok 8×8 , dan N merupakan kelipatan dari 8.
3. Pesan rahasia yang digunakan adalah citra biner dengan format Bitmap (.bmp)
4. Gangguan yang digunakan adalah White Noise Gaussian (AWGN)
5. Steganografi yang diimplementasikan adalah Non-Blind

1.3 TUJUAN

Berdasarkan rumusan masalah diatas maka tugas akhir ini mempunyai tujuan sebagai berikut :

1. Mengimplementasikan steganografi PM1 dengan BPSO
2. Mengetahui efek penggunaan BPSO untuk steganografi PM1
3. Membandingkan dan menganalisis performansi metoda steganografi PM1 dengan algoritma BPSO dan metoda steganografi tanpa algoritma BPSO
4. Mengukur dan menganalisa nilai parameter BPSO (jumlah iterasi, jumlah partikel) dalam peningkatan kualitas citra (MSE, PSNR & BER)

1.4 METODE PENYELESAIAN MASALAH

Metode yang akan digunakan dalam penyelesaian masalah ini adalah sebagai berikut :

1. Studi literatur

Mempelajari konsep dasar dan pemilihan algoritma yang digunakan, sehingga penulis dapat menentukan dan merancang sistem yang lebih jelas dan rinci.

2. Perancangan

Merancang dan mendesain sistem pada software Matlab yang akan digunakan untuk mengimplementasikan sistem steganografi.

3. Realisasi dan Simulasi

Membuat program untuk proses steganografi menggunakan metode Plus Minus 1 dengan algoritma BPSO pada citra digital meliputi program penyisipan pesan, dan program ekstraksi pesan. Tidak hanya itu akan ditambah feature pengujian ketahanan system dengan memberikan noise AWGN.

4. Pengujian

Pengujian sistem dilakukan untuk mengetahui apakah sistem yang dibangun sudah mencapai tujuan yang diinginkan.

5. Analisa Hasil

Analisa dilakukan pada hasil-hasil yang telah diperoleh dari pengujian sistem dan berdasarkan rumusan masalah yang telah ditentukan.

6. Penyusunan Laporan Tugas Akhir

Pada tahap ini dilakukan penyusunan laporan hasil penelitian yang telah dilakukan kemudian membuat analisa dan kesimpulan dari hasil penelitian tersebut.

1.5 SISTEMATIKA PENULISAN

Tugas akhir ini disusun dengan sistematika pembahasan sebagai berikut :

BAB 1 PENDAHULUAN

Bab ini terdiri dari latar belakang, tujuan, rumusan masalah, batasan masalah, metode penyelesaian masalah dan sistematika penulisan.

BAB 2 LANDASAN TEORI

Bab ini berisi tentang landasan teori yang mendukung dan mendasari penulisan tugas akhir. Dasar teori yang dibahas dalam bab ini adalah dasar teori mengenai representasi

citra digital, pengertian dan karakteristik sistem steganografi, Discrete Cosine Transform (DCT), metode plus minus 1, algoritma BPSO, dan parameter kualitas citra.

BAB 3 PERANCANGAN DAN IMPLEMENTASI

Bab ini menguraikan tentang proses pembuatan sistem secara mendetail

BAB 4 ANALISIS DAN HASIL PENGUJIAN

Bab ini berisi analisa dari hasil yang diperoleh dari tahap perancangan sistem dan implementasi

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran yang berguna untuk pengembangan tugas akhir berikutnya.



BAB 5

KESIMPULAN DAN SARAN

5.1 KESIMPULAN

1. Faktor skala sebagai pengali tabel kuantisasi pada proses kuantisasi mempengaruhi jumlah koefisien DCT terkuantisasi non zero AC yang secara tidak langsung representasi kapasitas penyisipan citra secret. Semakin kecil faktor penskalaan, semakin besar kapasitas penyisipan begitu juga sebaliknya.
2. Besarnya jumlah iterasi mempengaruhi kualitas PSNR/MSE yang dihasilkan walaupun nilai pergerakannya juga tidak signifikan. Namun jumlah iterasi bisa saja tidak terlalu mempengaruhi jika nilai optimum telah didapatkan pada iterasi awal sehingga nilai PSNR/MSE terbaik cenderung tetap.
3. BPSO rentan terhadap masalah terperangkapnya pada local optimum. Hal tersebut pada terlihat pada pengujian jumlah iterasi. hal ini terlihat untuk pengujian citra cover lena sudah menyentuh iterasi 100 nilai lastbest untuk partikel tidak berubah (55.6339) padahal kita bisa melihat bahwa nilai PSNR maksimum untuk ketika percobaan (citra girl) adalah 55.6873. hal ini dikarenakan parameter BPSO yang sensitive ^[2] misalnya pemilihan inertia weight^[2]
4. Besarnya jumlah iterasi mempengaruhi kualitas PSNR/MSE yang dihasilkan walaupun nilai pergerakannya juga tidak signifikan. Namun jumlah iterasi bisa saja tidak terlalu mempengaruhi jika nilai optimum telah didapatkan pada iterasi awal sehingga nilai PSNR/MSE terbaik cenderung tetap.
5. BPSO melakukan optimasi terhadap kualitas MSE dan PSNR dengan nilai optimasi yang sangat kecil dengan ratio optimasi $< 1\%$.
6. BPSO cenderung melakukan optimasi terhadap kualitas BER terlihat dari pengujian untuk noising. Terlihat bahwa hasil output citra stego BPSO cenderung memberikan

optimasi pula terhadap hasil ekstraksi kualitas citra secret (BER) walaupun nilai optimasinya juga sangat kecil/tidak signifikan.

7. Untuk steganografi non blind diperlukan citra cover original dan citra stego dalam melakukan proses ekstrak. Noise mempengaruhi kualitas citra secret yang diekstrak. Dari ketiga skema kualitas citra secret terburuk saat diekstrak adalah skema ke-3 dimana kedua citra tersebut diberikan noise. Hal tersebut dapat terjadi karena peran dari kedua citra tersebut dalam proses ekstrak. Citra cover original merepresentasikan nilai encode citra secret yang akan diembed (kebalikan logika dengan nilai encode citra original) dan citra stego yang akan merepresentasikan letak blok citra secret. Sehingga dengan adanya noise akan mempengaruhi pemilihan nilai encode original dan letak blok secret .dengan adanya noise nilai encode citra original dan letak blok secret dapat mengalami kesalahan

5.2 SARAN

1. Digunakan pesan rahasia berupa citra grayscale atau citra warna RGB, sehingga dapat merepresentasikan pesan lebih luas
2. Diimplementasikan Steganography dengan non blind sehingga steganography makin terlihat *secret*.
3. Perlu adanya *improvement* terhadap BPSO mengingat metode tersebut rentan terhadap permasalahan terperangkap pada local optimum.
4. Mengingat ruang solusi yang sempit, Oleh karenanya ruang solusi nya ditambah seperti pemilihan skala kuantisasi mengingat parameter tersebut penentu kualitas BER maupun PSNR.

REFERENSI

- [1] Aditya Yogie, Andhika Pratama dan Alfian Nurlifa. Studi Pustaka untuk Steganografi dengan beberapa Metode. Laboratorium Komputasi dan Sistem Cerdas. Jurusan Teknik Informatika, FTI, UII
- [2] Ahmadih Motjaba Khanesar, Mohammad Teshnehlab and Mahdi Aliyari Shoorehdeli. A Novel Binary Particle Swarm Optimization. Electric Engineering Faculty. K.N. Toosi University of Technology
- [3] Arif, Fazmah Yulianto. Teori Keamanan Informasi. Bandung
- [4] Bajaj Ruchika, Punam dan S.K. Pal. Best Hiding Capacity Scheme for Variable Length Messages Using Particle Swarm Optimization. Department of Computer Science, University of Delhi, India.
- [5] Bertalya. Representasi Citra. Universitas Gunadarma 2005
- [6] Ensiklopedia Citra Digital. Institut Teknologi Telkom
- [7] Heriniaina, Feno Rabevohitra dan Jun Sang. Using PSO Algorithm for Simple LSB Substitution based Steganography scheme in DCT Transformation Domain
- [8] Hidayati, Amriane. Desain dan Analisis Steganografi Plus Minus 1 Menggunakan Algoritma Genetika Untuk Citra Digital. Institut Teknologi Telkom. Bandung
- [9] Mochammad, Adel. Steganography-Based Secret and Reliable Communications : Improving Steganographic Capacity and Imperceptibility. Department of Information Systems and Computing. Brunel University

- [10] PM1 Yu Lifang, Yao Zhao, Rongrong Ni dan Zhenfeng Zhu. PM1 Steganography in JPEG images using genetic algorithm
- [11] Ruid. Steganography Primer. Computer Academic Underground 2004
- [12] X.H.Shi, Y.C.Liang, H.P Lee, C.Lu dan Q.X Wang. Particle Swarm Optimization based Algorithm for TSP and Generalized TSP. Institute of High Performance Computing, Singapore
- [13] Wohlogemuth, Sven. Steganography and watermarking. IG Telematics

