OPEN ACCESS
Indo-JC
Indonesian Journal of Computing
ISSN 2460-9056
socj.telkomuniversity.ac.id/indojc

IND. JOURNAL ON COMPUTING
VOL. 1, ISSUE. 2, SEPT 2016. PP. 57-66
DOI:10.21108/INDOJC.2016.1.2.89

Steganografi Citra Digital Menggunakan Blok Permutasi dan Algoritma *Particle Swarm Optimization* (PSO)

Husna Aydadenta[#1] , Danang Triantoro[#2], Jondri[#3]

[#] *School of Computing, Telkom University*
Jl.Telkomunikasi No.01 Terusan Buah Batu Bandung, JawaBarat

[1]husnaaydadenta@gmail.com
[2]danang.triantoro@gmail.com

Abstract

Todays technology development has increasingly advanced. There are a lot of things that are made conveniently by technology, one of them is in communication. Communication using internet network was already the first choice because the facility and speed. But, the data security rarely noticed by user. So, it takes data safe security techniques to keep data secure while communicating. There are many techniques for protect data security, such as steganography. Steganography is a technique for embed secret information into many media files. In this project steganography using BPIS method or block permutation and PSO algorithm. Digital imagery that been used is bitmap format and used text in embedded information. the message that embedded in digital imagery will be converted to binary sequence, then the next process is pra-steganography process using block permutation method, so the message information will be randomized by the method. Furthermore, PSO algorithm do the optimization process or finding the best solution to embedded message in pixel so that performance of citra keep doing well. Embedded text or information is using Least Significant Bit (LSB) approach. The final results show the value of the best image quality performance is 60.4295 dB which is the digital image flowers with the number of particles is 50 and the maximum iterations is 50. The result of image quality performance using LSB technique is 58.716 dB. This result show image quality performance using PSO algorithm is better than using LSB technique.

Keywords: Steganography, Block Permutation Image Steganography, Particle Swarm Optimization, spatial domain, Least Significant Bit, citra digital, BMP

Abstrak

Pada saat ini perkembangan teknologi sudah semakin maju, banyak hal yang dipermudahkan oleh teknologi, salah satu nya dalam komunikasi. Komunikasi melalui jaringan internet sudah menjadi pilihan utama karena kemudahan dan kecepatannya. Akan tetapi keamanan datanya jarang diperhatikan oleh para users, sehingga dibutuhkan teknik keamanan data yang aman untuk menjaga data ketika melakukan komunikasi. Ada banyak teknik untuk menjaga keamanan data diantara nya seperti steganografi. Steganografi merupakan teknik untuk menyembunyikan informasi rahasia ke dalam beberapa media file. Pada penelitian ini dilakukan proses steganografi menggunakan metode BPIS atau blok permutasi dan algoritma optimasi PSO. Citra digital yang digunakan berformat bitmap dan pesan informasi yang akan disisipkan adalah teks. Pesan yang disisipkan di dalam citra digital akan dikonversi kedalam biner, selanjutnya akan dilakukan proses pra-steganografi dengan metode blok permutasi, sehingga pesan informasi akan teracak oleh metode tersebut. Selanjutnya algoritma PSO akan melakukan proses optimasi atau pencarian solusi terbaik untuk penyisipan pesan tiap piksel, tujuannya agar performansi citra tetap baik. Penyisipan pesan atau informasi dilakukan dengan pendekatan Least Significant Bit (LSB). Hasil akhir yang didapat menunjukan nilai performansi kualitas citra terbaik 60.4295 dB yaitu pada citra digital flowers dengan jumlah partikel 50 dan maksimum iterasi 50. Sedangkan hasil performansi kualitas citra dengan menggunakan teknik LSB biasa yaitu 58.716 dB. Hal ini menunjukan performansi kualitas citra dengan menggunakan metode blok permutasi dan algoritma PSO lebih baik dari pada menggunakan teknik LSB biasa.

Kata Kunci: Steganografi, Block Permutation Image Steganography, Particle Swarm Optimization, spatial domain, Least Significant Bit, citra digital, BMP

RECEIVED ON AUGUST 2016. ACCEPTED ON SEPT 2016

I. PENDAHULUAN

Setiap harinya manusia tidak terlepas dengan yang namanya interaksi, salah satu interaksi yang dilakukan oleh manusia dengan melakukan komunikasi, komunikasi sangat penting didalam kehidupan karena dengan komunikasi banyak ilmu dan wawasan yang diperoleh. Ada banyak cara untuk melakukan komunikasi baik itu dengan lisan, tulisan maupun melalui alat bantu lainnya, seperti media cetak atau gambar. Seiring dengan perkembangan teknologi, komunikasi juga sudah semakin mudah. Pada saat ini komunikasi melalui jaringan internet sudah sangat sering dilakukan baik itu melalui email, web, blog maupun media sosial lainnya. Tetapi cara komunikasi tersebut keamanan data biasanya sering dilupakan, padahal keamanan data sangat penting dalam melakukan komunikasi terutama komunikasi melalui jaringan internet. Selain itu komunikasi melalui jaringan internet sering disalah gunakan oleh beberapa pihak, seperti mengambil karya atau hak cipta seseorang, maka untuk itu dibutuhkan suatu teknik untuk mengamankan data [1].

Ada banyak teknik yang digunakan untuk mengamankan data, seperti steganografi, yaitu teknik keamanan data dengan cara menyembunyi pesan kedalam beberapa media, seperti gambar, video, audio dan lain sebagainya [1]. Tujuannya adalah untuk menyembunyikan pesan atau informasi dibeberapa media hingga sampai ke tangan penerima dan tidak ada seorangpun yang curiga akan keberadaaan isi file tersebut [1]. Sehingga keamanan data didalam media stego (media yang telah disisipi oleh pesan) sangatlah penting. Ada beberapa metode untuk menjaga keamanan data tersebut, seperti dengan menggunakan operasi logika XOR. Kelemahan metode ini adalah jumlah pesan biner 0 dan 1 akan berbeda dengan hasilnya. Adapun metode lain, yaitu dengan menggunakan metode blok permutasi [1]. Dengan blok permutasi pesan rahasia akan dikonversi kedalam biner, kemudian akan dibentuk blok sejumlah N. Fungsi dibentuk perblok untuk mempermudah pada proses ektraksi pesan. Pada penelitian ini, metode yang digunakan adalah metode blok permutasi, karena dengan menggunakan metode blok permutasi bit biner pesan akan diacak tanpa mengubah karakter pesan saat diekstrak. Kemudian, pada penelitian ini jumlah blok permutasi diasumsikan sama seperti jumlah bit setiap karakter, yaitu 8 bit.

Permasalahan optimasi pada steganografi citra digital telah banyak dikaji dan dilakukan penelitian. Optimasi pada steganografi citra digital dapat dilakukan dengan banyak cara, diantara dengan menentukan titik optimum piksel pada citra digital, menentukan banyaknya piksel optimal yang disisipkan pada setiap piksel, dan lain sebagainya [2]. Pada penelitian ini dilakukan optimasi dengan menentukan titik-titik optimum penyisipan pada piksel citra digital. Didalam sebuah citra digital terdiri dari banyak piksel. Maka untuk itu dibutuhkan suatu algoritma untuk mencari titik optimum penyisipan pesan pada citra digital.

Pada penelitian ini digunakan algoritma optimasi PSO (*Particle Swarm Optimization*). Alasan pemilihan algoritma PSO adalah karena algoritma PSO merupakan algoritma optimasi yang sederhana, efektif, dan dapat diadaptasikan untuk berbagai macam permasalahan termasuk optimasi kombinatorik [3]. Performansi hasil steganografi menggunakan blok permutasi dan algoritma PSO ini akan dibandingkan dengan penelitian terdahulu yaitu dengan menggunakan blok permutasi tanpa algoritma optimasi [1]. Hasil dari penelitian ini adalah dengan menerapkan metode blok permutasi untuk keamanan pesan dan algoritma PSO untuk menjaga performasi kualitas citra dengan menyisipkan pesan berupa teks ke dalam file citra digital berformat bitmap dengan pendekatan teknik *Least Significant Bit* (LSB). Tujuannya adalah untuk meningkatkan keamanan pesan atau informasi dan kualitas citra yang tetap terjaga.

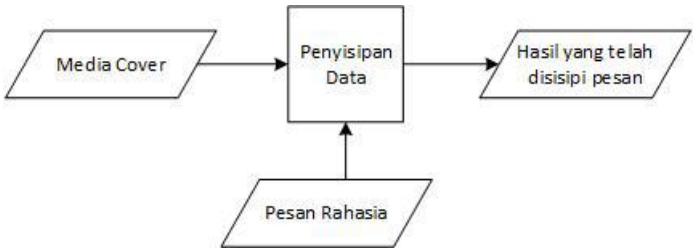
II. PENELITIAN SEBELUMNYA

Pada penelitian sebelumnya permasalahan penentuan titik-titik optimum berhasil dipecahkan dengan menggunakan algoritma PSO. Pada penelitian tersebut menggunakan citra digital *greyscale* dan membagi citra digital menjadi 8x8 blok, sehingga terbentuk 64 blok yang terdiri dari 64x64 piksel untuk setiap blok. Dan media yang digunakan dalam penyisipan adalah citra digital *greyscale* yang dimensinya lebih kecil dari media stego. Performansi PSNR terbaik yang diperoleh pada penelitian ini adalah 44.42 dB.

H. Al-Bahadili [1] melakukan penelitian dengan menggunakan metode blok permutasi, dimana jumlah bloknya adalah N. Tujuan dari metode blok permutasi tersebut untuk mengamankan data atau pesan rahasia, metode blok permutasi akan mengacak bit biner pesan rahasia sebelum disisipkan, sehingga data atau pesan rahasia yang akan disisipkan akan lebih aman.

III. TINJAUAN PUSTAKA

Steganografi adalah sebuah seni dalam komunikasi dengan menyembunyikan informasi dimedia seperti gambar, audio, video dan lain sebagainya sehingga tidak menimbulkan kecurigaan *eavesdropper* [9]. Tujuan dari steganografi yaitu untuk menyembunyi pesan sehingga ketika seseorang melihat file yang di sisipkan pesan tidak mudah curiga kecuali dengan melakukan steganalisis terhadap file tersebut [1].



Gambar. 1. Ilustrasi Steganografi

Pada dasarnya, proses menyembunyikan informasi pada sistem steganografi dimulai dengan mengidentifikasi bit pada media cover, kemudian proses *embedding* sehingga menghasilkan media stego yaitu media cover yang telah berisikan informasi dengan menggantikan bit-bit yang *redundant* dengan bit informasi yang akan di sembunyikan [9]. Informasi yang akan disembunyikan disebut pesan rahasia, media yang digunakan untuk menyimpan pesan disebut media cover atau *cover image*, sedangkan file yang telah di sisipkan pesan rahasia disebut media stego atau *stego image* [1].

Blok Permutasi

Metode ini mengubah pesan atau informasi rahasia ke urutan biner (ASCII), kemudian membagi urutan biner ke dalam beberapa blok, kemudian meng-*generate vector* permutasi secara acak untuk dilakukan proses *permute* setiap bit. Metode ini berfungsi untuk mengamankan data yang akan disisipkan karena pada proses *permute* bit-bit informasi akan diacak terlebih dahulu. Sehingga, pesan tidak akan mudah untuk diekstrak kecuali dengan menggunakan hasil blok permutasi yang sama seperti blok permutasi awal.

Particle Swarm Optimization

PSO dimulai dengan sekumpulan partikel (solusi) yang dibangkitkan secara acak. Setiap partikel kemudian dievaluasi kualitasnya menggunakan fungsi *fitness*. Selanjutnya, partikel-partikel akan terbang mengikuti partikel yang optimum. Pada saat iterasi, setiap partikel di-*update* mengikuti dua nilai terbaik. Yang pertama adalah *fitness* terbaik yang dicapai oleh satu partikel jauh partikel itu tebaang. Nilai *fitness* terbaik ini dilambangkan dengan p_{best} dan disimpan di memori. Sedangkan nilai terbaik yang kedua adalah *fitness* terbaik yang dicapai oleh semua partikel dalam topologi ketetanggaan. Indeks g_{best} digunakan untuk menunjukan partikel dengan *fitness* terbaik. Setelah menemukan dua nilai terbaik, suatu partikel i pada posisi X_i, meng-update vektor *velocity* dan kemudian meng-update posisinya menggunakan persamaan berikut [7]:

$$v_j(i) = v_j(i-1) + c_1 r_1(p_{best} - x_j(i-1)) + c_2 r_2(g_{best} - x_j(i-1)) \quad (1)$$

$$x_j(i) = x_j(i-1) + v_j(i) \quad (2)$$

Dimana $v_j(i)$ adalah kecepatan partikel j pada iterasi i, $x_j(i)$ adalah posisi partikel j pada iterasi i, $c_1 c_2$ *Learning rate*, p_{best} merupakan nilai *fitness* terbaik yang dihasilkan partikel sejauh ini, g_{best} nilai *fitness* terbaik diantara partikel dan $r_1 r_2$ adalah bilangan acak dalam interval [0,1].

Least Significant Bit (LSB)

Least Significant Bit (LSB) merupakan pendekatan dasar pada steganografi yang digunakan untuk menggabungkan urutan biner permutasi ke dalam stego cover [1]. Pada umumnya *Least Significant Bit* (LSB) menggabungkan informasi rahasia ke dalam stego cover dalam spasial domain [4]. Spasial

domain adalah proses memanipulasi piksel-piksel dari suatu citra sehingga menghasilkan citra yang baru, tujuannya adalah untuk memperbaiki kualitas dari citra [10]. Pada steganografi LSB, pesan rahasia diubah menjadi string biner. Sehingga string biner akan menggantikan LSB-plane [4].

Kualitas Citra

Untuk pengukur kualitas suatu citra dilakukan dengan pendekatan *fidelity*, yaitu pengujian terhadap aspek mutu. Ada beberapa macam metode untuk mengukur aspek mutu suatu citra, seperti:

1) Mean Square Error (MSE): adalah kesalahan kuadrat kumulatif antara stego dan stego cover, kemudian dinyatakan ke dalam bentuk persamaan:

$$MSE = \frac{1}{XY} \sum_{y=1}^{Y} \sum_{x=1}^{X} [I(x,y) - K(x,y)]^2 \tag{3}$$

Dimana $I(x,y)$ dan $K(x,y)$ mewakili nilai piksel pada posisi x, y di cover stego atau mewakili dimensi gambar.

2) Peak Signal Noise Ratio (PSNR): adalah ukuran variansi kualitas antara biner terakhir dan cover stego, dan biasanya dinyatakan kedalam logaritmik (dB) skalasebagai berikut:

$$PSNR = 20 \log_{10}(\frac{MAX_I}{\sqrt{MSE}}) \tag{4}$$

Dimana MAX_I adalah nilai piksel maksimum. Semakin besar nilai PSNR maka semakin sedikit perbedaan antara biner penutup (terakhir) dengan cover stego [18].

3) Structural Similarity Index Metric (SSIM): digunakan untuk mengukur kesamaan antara dua gambar. Nilai SSIM dapat di hitung menggunakan rumus:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{5}$$

Dimana μ_x dan μ_y adalah *average* dari *cover image* dan *stego image*, σ_x^2 dan σ_y^2 adalah *variance* dari *cover image* dan *stego image*, σ_{xy} adalah *covariance* dari *cover image* dan *stego image* serta c_1 dan c_2 adalah konstanta. Nilai dari SSIM yaitu antara 0 dan 1, dimana semakin nilai mendekati 1 maka semakin bagus pula kualitas suatu citra.

IV. METODE PENELITIAN

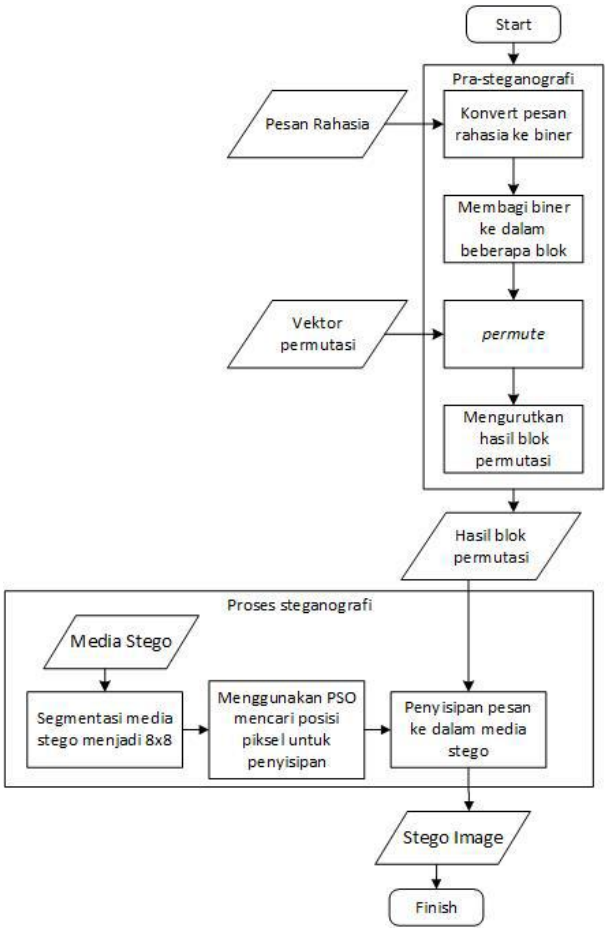
Pada penelitian ini akan dibangun sistem steganografi menggunakan blok permutasi dan algoritma PSO. Pada sistem ini terdiri dari 2 bagian, yaitu proses penyisipan dan proses ekstraksi. Pada proses penyisipan terdiri dari 2 proses yaitu proses pra-steganografi dan proses steganografi. Untuk rancangan sistem dapat dilihat pada Gambar 2

Pada proses penyisipan pesan terdiri dari 2 proses yaitu proses pra-steganografi dan proses steganografi. Pada proses pra-steganografi terjadi proses permutasi yang berfungsi untuk mengacak biner pesan sedangkan proses steganografi terjadi proses penyisipan pesan dengan melakukan optimasi piksel-piksel pada *stego image* menggunakan algoritma PSO. Perhatikan Gambar 2.

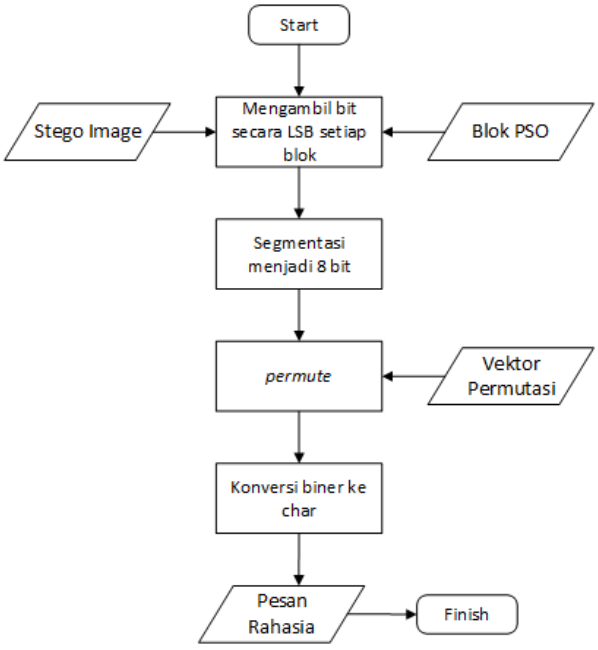
Pada proses pra-steganografi digunakan metode *Block Permutation Image Steganography* (BPIS). Dimana inputan teks rahasianya diubah kedalam bentuk biner, kemudian diurutkan dan disegmentasi kedalam blok. Pada tahap selanjutnya blok diacak menggunakan proses permutasi dengan *generate* blok permutasi sehingga hasil dari proses ini adalah gabungan blok permutasi.

Pesan rahasia yang akan disisipkan merupakan teks, yaitu teks yang berisi pesan berformat string yang mengandung informasi. Dimana pesan rahasia (file teks) akan dikonversi kebiner (ASCII). Setelah itu dilakukan proses *generate vektor* permutasi, yang berfungsi berfungsi untuk keamanan data pada saat proses ekstraksi. Proses permutasi dapat dilihat pada Gambar 2.

Pesan yang akan disisipkan adalah paper5.txt dimana ukuran dari file ini sebesar 11.9KB dan terdiri dari 11.634 karakter dengan 93.072 bit biner. Sedangkan citra digital yang digunakan adalah lena.bmp dengan ukuran 769KB atau dengan dimensi 512x512.



Gambar. 2. Penyisipan Pesan



Gambar. 3. Ekstraksi Pesan

```
.pn 0
.EQ
delim $$
define RR 'bold R'
define SS 'bold S'
define II 'bold I'
define mo '"\(mo"'
define EXIST ?"\z\-\d\z\-\r\-\d\v'0.2m'\(br\v'-0.2m'"?
define NEXIST ?"\z\-\d\z\o'\-\(sl'\r\-\d\v'0.2m'\(br\v'-0.2m'"?
define ALL ?"\o'V-'"?
define subset '\(sb'
define subeq  '\(ib'
define supset '\(sp'
define supeq  '\(ip'
define mo '\(mo'
define nm ?"\o'\(mo\(sl'"?
define li '\& sup ['
define lo '\& sup ('
define hi '\& sup ]'
define ho '\& sup )'
.EN
.ls 1
.ce
A LOGICAL IMPLEMENTATION OF ARITHMETIC
.sp 3
```

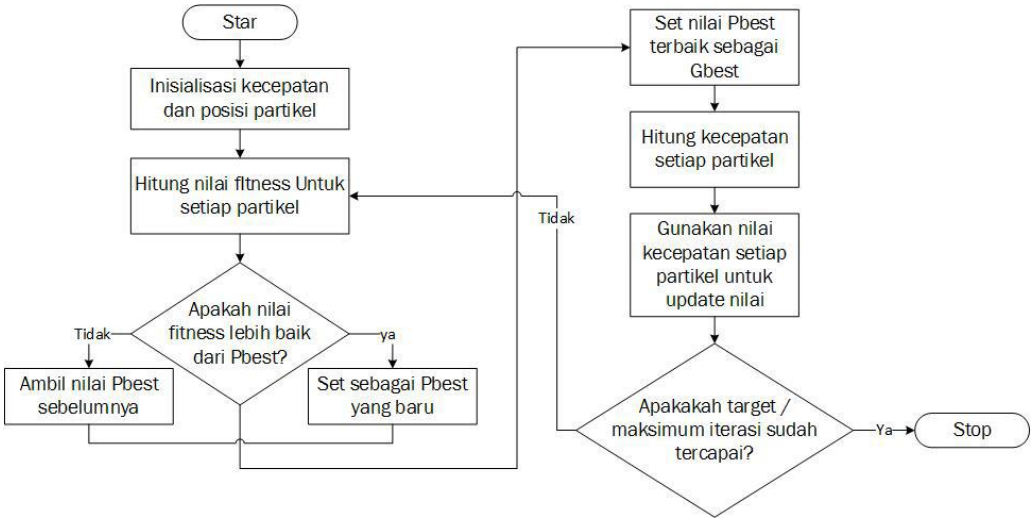
Gambar. 4. Pesan Teks

Gambar. 5. Media Citra Digital

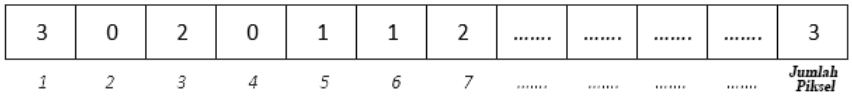
Kemudian, pada proses steganografi (penyisipan pesan) dilakukan dengan pendekatan teknik LSB. Pada proses ini, pertama membagi jumlah dimensi citra digital ke dalam 64 blok. Kemudian, PSO akan melakukan proses pencarian solusi perblok, dengan meng-*update* kecepatan partikel dan posisi partikel, kemudian dihitung nilai *fitness*nya (menggunakan persamaan 4), jika nilai *fitness* lebih baik dari p_{best} maka nilai *fitness* digunakan sebagai nilai p_{best} yang baru, kemudian dari nilai p_{best} dipilih yang terbaik untuk digunakan sebagai g_best, jika nilai *fitness* sudah tercapai atau kriteria untuk berhenti telah terpenuhi maka iterasi akan berhenti. Berikut diagram alir algoritma PSO dan pada Gambar 7 merupakan representasi partikel yang digunakan dalam algoritma PSO.

Dimana 0 berarti tidak ada bit yang disisipkan, jika 1 hanya satu bit yang disisipkan pada *red plane*, jika 2 berarti dua bit yang disisipkan pada *red plane* dan *green plane* dimana 1 *plane* disisipi oleh 1 bit, begitu pula jika 3, menyisipkan 3 bit, yaitu pada *red green* dan *blue plane* setiap *plane* disisipi oleh 1 bit.

Pada proses ekstraksi pesan dari *stego image* maka dibutuhkan hasil dari blok pso dan blok permutasi yang digunakan pada proses pra-steganografi. Pertama mengambil jumlah bit yang disisipkaan pada setiap blok berdasarkan informasi dari hasil blok algoritma PSO Kemudian, segmentasi bit-bit tersebut menjadi urutan biner 8 bit. Selanjutnya, melakukan proses permutasi setiap blok. Hasil dari proses permutasi akan dikonversi kembali sehingga hasil konversi tersebut akan menghasilkan informasi seperti sebelum disisipkan. Untuk diagram alir proses ekstraksi pesan dapat dilihat pada Gambar 3



Gambar. 6. Flowchart Algoritma PSO



Gambar. 7. Representasi Partikel

V. HASIL EKSPERIMEN

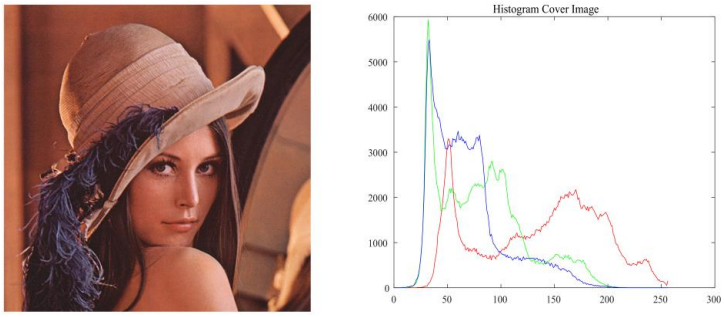
Pada eksperimen ini, digunakan citra digital berdimensi 512x512 yang dibagi menjadi 8x8 segingga diperoleh 64 blok dengan 64x64 piksel perblok. Jumlah partikel PSO yang digunakan adalah 20, 30, 40, dan 50 dengan maksimum iterasi 50, c_1 dan c_2 = 2, dan r_1 dan r_2 = bilangan random [0 1]. Nilai parameter tersebut diambil dari rujukan penelitian tentang algoritma PSO [17]. Pada eksperimen ini, hasilnya akan dibandingkan dengan penelitian terdahulu.

TABEL I
HASIL PENGUJIAN SKENARIO 1

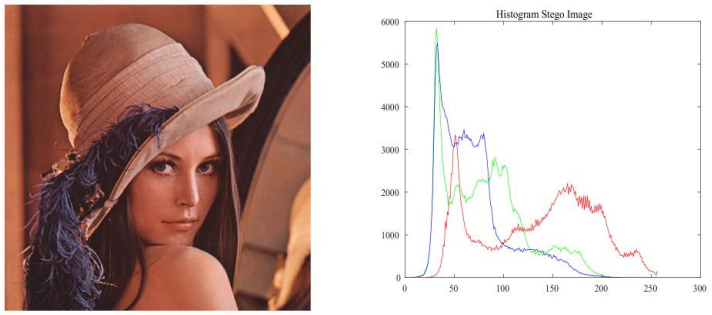
Cover Image	Jumlah Partikel	PSNR Menggunakan Permutasi dan PSO	PSNR Tanpa Menggunakan PSO [1]
lena	20	60.3732	
	30	60.3940	57.771
	40	60.4057	
	50	60.4143	
flowers	20	60.3984	
	30	60.4162	58.716
	40	60.4173	
	50	60.4295	

Dari tabel diatas dapat dilihat hasil eksperimen setiap partikel selalu lebih tinggi dari hasil eksperimen penelitian terdahulu [1]. Hal ini disebabkan karena pada penelitian terdahulu tidak menggunakan algoritma optimasi, hanya menggunakan metode permutasi yang bertujuan untuk mengamankan pesan rahasia.

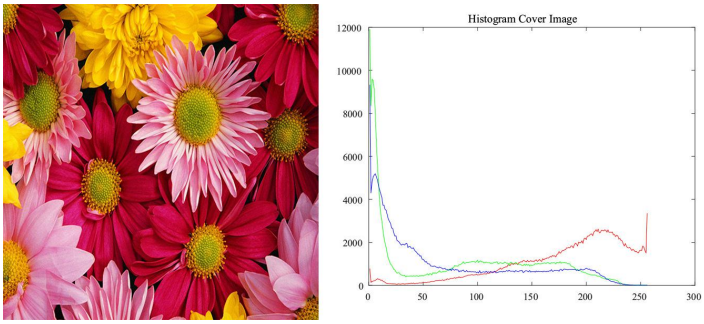
Kemudian untuk perbandingan hasil stego dan cover image dapat dilihat pada gambar 8, 9, 10, dan 11



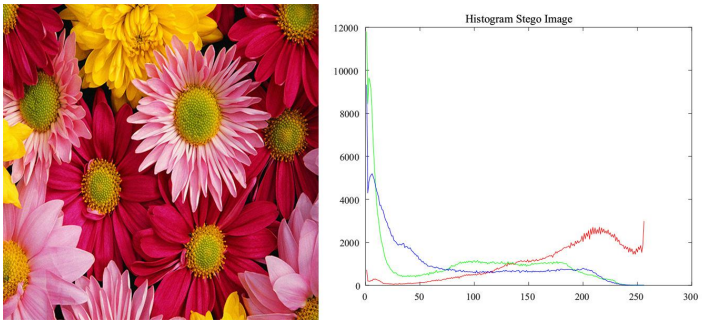
Gambar. 8. Cover Image Lena



Gambar. 9. Stego Image Lena Dengan PSNR 60.4143 db



Gambar. 10. Cover Image Flowers



Gambar. 11. Stego Image Flowers Dengan PSNR 60.4295 db

Dari gambar tersebut dapat dilihat hasil dari stego image tidak terlalu jauh berbeda dari gambar aslinya. Kemudian jika dilihat dari histogram gambarnya, terdapat beberapa perbedaan pada grafik *red*. Hal ini menunjukan ada beberapa bit yang disisipkan pada *red plane*, sehingga mengubah frekuensi (sumbu-y) dan kedalaman warna (sumbu-x) pada plane tersebut.

Kemudian, jika dihitung peluang seorang *eavesdropper* untuk mengambil pesan atau menemukan posisi piksel yang disisipi pesan menggunakan LSB pada citra secara *Brute-force attack* yaitu sebanyak $(2x2x2)^{512x512}$ kali. Dimana $2x2x2$ adalah *plane* pada RGB, setiap *plane* hanya memiliki 2 kemungkinan yaitu 0 (tidak disisipi) dan 1 (disisip), dan $512x512$ adalah jumlah dimensi citra. Puluang menemukan posisi piksel pada *stego image* sangat banyak dan setelah *eavesdropper* berhasil menebak atau memecahkan masalah ini, seorang *eavesdropper* harus memecahkan blok permutasi. Dimana jumlah *vector permutation* ini sebanyak 8 bit jadi jika seorang *eavesdropper* ingin memecahkan persoalan ini secara *Brute-force attack* membutuhkan 8! kali percobaan.

VI. KESIMPULAN

Berdasarkan penelitian yang telah dibuat beserta ujicoba yang telah dilakukan, metode permutasi dan algoritma *Particle Swarm Optimization* dapat digunakan pada steganografi. Dan berdasarkan hasil uji coba sistem untuk peformansi kualitas citra jika ingin mendapatkan nilai kualitas citra PSNR terbaik dapat menggunakan fungsi *fitness* PSNR, fungsi *fitness* berfungsi untuk mengoptimalkan suatu fungsi. Kemudian untuk metode permutasi tidak berpengaruh terhadap performansi atau kualitas gambar, permutasi hanya berpengaruh terhadap keamanan data, sebab permutasi berfungsi untuk mengacak bit-bit pesan. Dan dengan meggunakan algoritma PSO, diperoleh nilai performansi kualitas gambar yang lebih baik dari pada non algoritma PSO. Sebab, dengan menggunakan algoritma PSO kualitas suatu citra akan tetap terjaga. Dari hasil uji coba sistem, nilai performansi terbaik terdapat pada teknik permutasi & algoritma PSO yaitu pada jumlah partikel 50 dan maksimum iterasi 50 dengan nilai performansi kualitas citra digital (PSNR) 60.4295 dB.

REFERENCES

[1] Al-Bahadili, H. (2013). *A Secure Block Permutation Image Steganography Algorithm*. International Journal on Cryptography and Information Security (IJCIS). 3:2 11-22

[2] Bedi, P., Bansal, R., & Sehgal, P. (2013, January 24). *Using PSO in a spatial domain based image hiding scheme with distortion tolerance*. Computers and Electrical Engineering, 39 , 640-654. doi:10.1016

[3] Murdiansyah Danang Triantoro (2016, Maret). *Optimasi Jaringan Sensor Nirkabel Menggunakan Algoritma Two Sub-Swarms PSO Diskrit*. Ind. Journal on Computing, Vol. 1, Issue. 1, 1-10. doi:10.21108/indojc.2016.1.1.36

[4] Wang, S., Yang, B., & Niu, X. (2010). *A Secure Steganograpgy Method based on Genetic Algorithm*. Journal of Information Hiding and Multimedia Signal Processing.

[5] Adiwijaya, Faoziyah P. N., PermanaF. P., Wirayuda T. A. B., & Wisesty U.N. (2013). *Tamper Detection and Recovery of Medical Image Watermarking using Modified LSB and Huffman Compression*. Institute of Electrical and Electronics Engineers (IEEE). 978-1-4673-5256-7/13

[6] Clerc , M. (2005). *Particle Swarm Optimazation*. United Kingdom: British Library Cataloguing.

[7] Suyanto. (2010). *Algoritma Optimasi (Determinastik atau Probabilitas)*. Indonesia: Graha Ilmu.

[8] Wang, S., Yang, B., & Niu, X. (2010). *A Secure Steganograpgy Method based on Genetic Algorithm*. Journal of Information Hiding and Multimedia Signal Processing.

[9] Provos , N., & Honeyman, P. (2013). *Hide and Seek: An Introduction to Steganography*. The IEEE Computer Society.

[10] Putra, D. (2010). *Pengolahan Citra Digital*. Yogyakarta: C.V. ANDI OFFSET.

[11] M, A. F., Fariza, A., & Prasetyaningrum, I. (n.d.). *Aplikasi GIS Berbasis J2ME Pencarian Jalur Terpendek Menggunakan Algoritma Particle Swarm Optimazation (PSO) Di Kabupaten Bangkalan*. Institut Teknologi Sepuluh Nopember Surabaya(ITS).

[12] Zerda, E. R. (2009). *Analisis dan Penerapan Algoritma Particle Swarm Optimization (PSO) pada Optimasi Penjadwalan Sumber Daya Proyek*. Bandung: Departemen Teknik Informatika Institut Teknologi Telkom.

[13] Andika, Y., & Munir, R. (2006). *Pengembangan Random Number Generator dengan Video dan Suara*. Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung.

[14] Purnomo , D. H. (2014). *Cara Mudah Belajar Metode Optimasi Metaheuristik menggunakan Matlab*. Yogyakarta: Gava Media.

[15] Kusumanto, R., & Tompunu, A. N. (2011). *Pengolahan citra digital untuk mendeteksi obyek menggunakan pengolahan warna model noemalisasi RGB*. Seminar Nasional Teknologi Informasi & Komunikasi Terapan.

[16] Erianov (2012). *Implementasi steganography plus minus 1 (PM1) dengan binary particle swarm optimization (BPSO)*. Skripsi Institut Teknologi Telkom Bandung.

[17] Li-ping , Z., Huan-jun, Y., & Shang-xu, H. (2004). *Optimal choice of parameters for particle swarm optimization*. Journal of Zhejiang University SCIENCE(1009-3095), 528-534.

[18] Putra, S. S., Sasongko, P. S., & Bahtiar, N. (2011). *Verifikasi pemilikan citra medis dengan kriptografi RSA dan LSB watermarking*. Sains dan Matematika, 19, 75-81.

[19] Santosa, B. (n.d.). *Tutorial Particle Swarm Optimization*. Sukolilo Surabaya: Kampus ITS.