# Steganografi Menggunakan Blok Permutasi dan Algoritma Genetika

Andrian Yoga Pratama [#1], Danang Triantoro M., S.Si., M.T [#2], Jondri Nasri, S.Si, M.Si. [#3]

*#Prodi Ilmu Komputasi, Fakultas Informatika*
*Telkom University, Bandung*
[1] andrianyoga@students.telkomuniversity.ac.id
[2] danang.triantoro@gmail.com
[3] jondri@telkomuniversity.ac.id

**Abstract**

In this final task do the process combination of steganography using Block Permutation Image Steganography (BPIS) and genetic algorithms. Steganography is the art and science of writing hidden messages or techniques to hide messages, so except the sender and receiver no one knows or realizes that there is a secret message. One technique that can be used in this process is the Block Permutation Image Steganography (BPIS). BPIS is an algorithm that serves to change the message or confidential information in the form of a set of binary sequences, then of the binary sequence that is encrypted using a permutation vector. In the end the result of the algorithm BPIS will be reprocessed using genetic algorithms and approaches Least Significant Bit (LSB). The initial hypothesis of this final task is Block Permutation Image Steganography (BPIS) and genetic algorithms with spatial domain techniques can be used in the optimization process of message insertion text on a digital image bitmap format (.bmp), so it will have a level higher security and quality of digital imagery remains good. From the research and trials that have been done show that the combination of the block permutation methods and genetic algorithms can be used in steganography. So the secret message can be inserted in the media cover image and extracted back from stego image. By applying the method of block permutation, the system has a higher security level, as well as genetic algorithm the insertion location messages can be optimized and the quality of the image will remains good.

**Keyword:** *Steganography, Block Permutation Image Steganography, Genetic Algorithm, spatial domain, Least Significant Bit, stego image, BMP*

**Abstrak**

Dalam tugas akhir ini dilakukan proses steganografi dengan kombinasi antara Block Permutation Image Steganography (BPIS) dan algoritma genetika. Steganografi merupakan seni dan ilmu menulis pesan secara tersembunyi atau teknik untuk menyembunyikan sebuah pesan sehingga selain pengirim dan penerima tidak ada yang mengetahui atau menyadari bahwa terdapat suatu pesan rahasia. Salah satu teknik yang dapat digunakan dalam proses ini adalah Block Permutation Image Steganography (BPIS). BPIS adalah algoritma yang berfungsi merubah pesan atau informasi rahasia ke dalam bentuk urutan sekumpulan biner, kemudian dari urutan biner yang ada diacak dengan menggunakan vektor permutasi. Pada akhirnya hasil dari algoritma BPIS akan diolah kembali dengan menggunakan algoritma genetika serta pendekatan Least Significant Bit (LSB). Hipotesis awal tugas akhir ini adalah Block Permutation Image Steganography (BPIS) dan algoritma genetika dengan teknik spatial domain dapat digunakan dalam proses optimasi penyisipan pesan text pada citra digital dengan format bitmap (.bmp) sehingga akan memiliki tingkat keamanan yang lebih tinggi dan kualitas citra digital tetap baik. Dari hasil penelitian dan uji coba yang telah dilakukan menunjukkan bahwa, kombinasi metode blok permutasi dan algoritma genetika dapat digunakan pada steganografi. Sehingga pesan rahasia dapat disisipkan pada media cover image dan diekstraksi kembali dari stego image. Dengan menerapkan metode blok permutasi maka sistem memiliki tingkat keamanan yang lebih tinggi, serta dengan algoritma genetika maka letak penyisipan pesan dapat dioptimasi dan kualitas citra akan tetap terjaga.

**Kata kunci:** *Steganografi, Block Permutation Image Steganography, Algoritma Genetika, spatial domain, Least Significant Bit, stego image, BMP*

# I. PENDAHULUAN

Dalam kehidupan ini kita tidak terlepas dari pesan atau informasi. Dari pesan tersebut kita bisa mendapatkan dan bertukar informasi, serta menemukan hal baru yang bisa dipelajari. Namun karena banyaknya jenis pesan yang dapat dikirim, keamanan pesan tersebut juga menjadi bahan pertimbangan. Ada pesan yang hanya sekedar dikirim sebagai konsumsi publik, ada pula pesan yang dikirim secara tersembunyi tanpa harus diketahui oleh orang lain secara kasat mata. Dengan menggunakan teknik steganografi maka kita dapat menyisipkan pesan di dalam media lain seperti citra, audio, video tanpa diketahui oleh orang yang tidak diinginkan. Steganografi menjadi salah satu teknik yang sangat bermanfaat untuk mengirim sebuah pesan yang memiliki nilai informasi sangat penting, sehingga pesan tersebut sampai hanya pada orang yang memang mempunyai akses penuh terhadap pesan itu. Dalam hal ini, algoritma genetika digunakan untuk mencari matriks penyesuaian terbaik. Algoritma genetika dan blok permutasi digunakan sebagai suatu cara dalam meningkatkan pengamanan dan pengiriman pesan. Penyadap (eavesdropper) dalam hal ini menjadi faktor pendorong diterapkannya metode pengamanan dalam pengiriman pesan. Penyadap merupakan orang yang mencoba menangkap pesan selama ditransmisikan. Tujuan penyadap adalah untuk mendapatkan informasi sebanyak - banyaknya dalam sistem tersebut. Oleh karena itu dibutuhkannya sebuah sistem yang optimal untuk menyisipkan pesan dalam suatu media, sehingga pesan tersebut dapat dikirim dengan tingkat keamanan yang tinggi dan terhindar dari serangan Penyadap (eavesdropper). Serta dibutuhkan sebuah sistem yang dapat menyembunyikan pesan tersebut dengan algoritma yang memiliki tingkat akurasi yang tinggi dalam pengiriman pada pesan rahasia tersebut.

# II. DASAR TEORI

## *A. Steganografi*

Steganografi merupakan seni menyembunyikan informasi ke dalam beberapa file media dengan cara menjaga informasi yang tersembunyi di dalamnya [1]. Dengan demikian, dapat digunakan sebagai pendekatan keamanan informasi untuk mengamankan data yang tersimpan atau pertukaran data melalui jenis komunikasi yang tidak aman. Steganografi menyimpan informasi rahasia dengan menyembunyikan informasi dalam beberapa file media seperti gambar, audio, video, atau file text. Informasi yang akan disembunyikan disebut pesan rahasia, media yang digunakan untuk menanamkan informasi disebut media cover dan media yang telah berisi pesan rahasia disebut media stego.

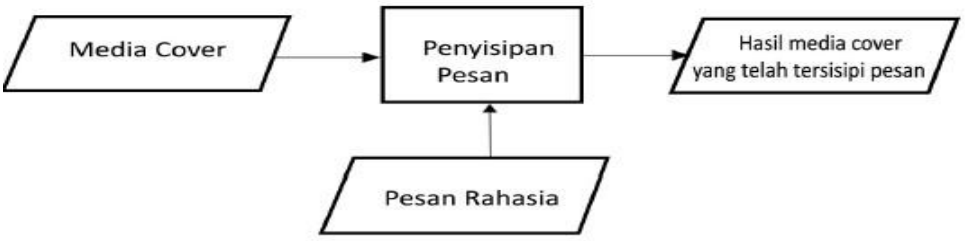


Fig. 1. Ilustrasi Steganografi

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 berlebihan dengan bit informasi yang akan di sembunyikan.

## *B. Blok Permutasi*

Algoritma ini mengubah pesan atau informasi rahasia ke urutan biner, membagi urutan biner ke dalam blok menggunakan permutasi secara acak, membuat blok permutasi membentuk urutan biner permutasi dan menggunakan LSB (Least Significant Bit) untuk menggabungkan urutan biner permutasi ke dalam gambar bitmap (.bmp). Proses Block Permutation Image Steganography (BPIS) dilakukan pada proses pra-steganografi, artinya algoritma ini merupakan algoritma sebelum proses steganografi atau sebelum embedding informasi ke dalam stego cover.

## *C. Algoritma Genetika*

Inisialisasi populasi awal dilakukan untuk mendapatkan hasil berupa solusi awal dari suatu permasalahan algoritma genetika. Inisialisasi ini dilakukan secara acak sebanyak jumlah kromosom/populasi yang diinginkan. Tahap berikutnya masuk pada perhitungan nilai fitness, kemudian dilakukan seleksi dengan menggunakan metode roda roullete. Selanjutnya dilakukan perkawinan silang (crossover) dan juga mutasi. Setelah melalui beberapa generasi maka algoritma ini akan berhenti sebanyak generasi yang diinginkan.

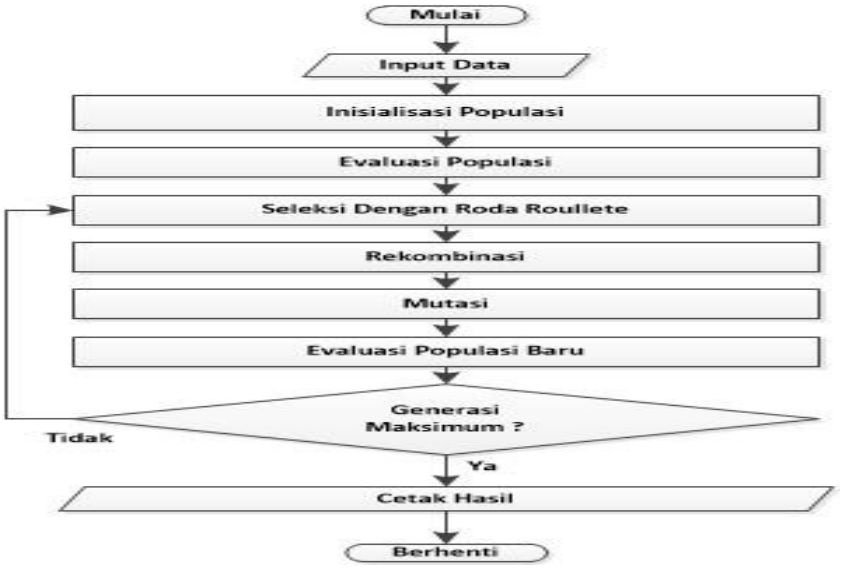


Fig. 2. Flowchart Algoritma Genetika

Algoritma AG dalam steganografi digunakan untuk menjamin keamanan pesan rahasia dari RS Analysis, sehingga keberadaan pesan rahasia sulit untuk dideteksi oleh RS Analysis. Selain itu, dalam algoritma steganalisis juga terdapat RS Attack, ini merupakan bagian dari RS Analysis yang akan mendeteksi stego - pesan dengan analisis statistik dan nilai - nilai pixel. Pada [2], Setelah pesan rahasia ditanamkan secara LSB (Least Significant Bit) pada gambar cover, nilai - nilai pixel dari stego-image dirubah atau dimodifikasi dengan algoritma AG untuk menjaga karakter statistiknya. Pada percobaan sebelumnya, dengan menggunakan algoritma AG maka lebih efektif dalam hal perlawanan terhadap steganalisis dengan kualitas visual yang lebih baik.

*D. Least Significant Bit (LSB)*

Least Significant Bit (LSB) merupakan salah satu metode dalam steganografi. LSB dilakukan dengan mengambil bit - bit terakhir warna pada citra dan menggantinya dengan bit - bit data [5]. Pada [3], dijelaskan bahwa setiap pixel pada file gambar BMP 24 bit terdiri dari susunan tiga warna yaitu merah, hijau, biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (1 byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Tujuan utama dari LSB adalah memanipulasi nilai suatu titik warna (pixel) sehingga data dapat disembunyikan ke dalam titik warna tersebut namun perubahan yang terjadi berusaha diminimalisasi sehingga perubahannya tidak dapat dideteksi oleh mata manusia [5].

*E. Kualitas Citra*

1) *Mean Square Error (MSE)* adalah kesalahan kuadrat kumulatif antara stego dan stego cover yang dinyatakan kedalam logaritmik (dB) skala dengan bentuk persamaan:

$$— \sum \sum \quad (\quad) \quad (\quad) \qquad (\ )$$

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 Ration* (PSNR) adalah ukuran variansi kualitas antara biner terakhir dan cover stego, dan biasanya dinyatakan kedalam logaritmik (dB) skala sebagai berikut:

$$(\frac{\quad}{\sqrt{\quad}}) \qquad (\ )$$

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

3) *Structural Similarity Index Metric* (SSIM): Structural Similarity Index SSIM digunakan untuk mengukur kesamaan antara dua gambar. Nilai dari SSIM yaitu antara 0 dan 1, dimana semakin nilai mendekati 1 maka semakin bagus pula kualitas suatu citra. Nilai SSIM dapat di hitung menggunakan rumus:

( ) ( )( ) ( )
( )( )

Dimana dan adalah average dari cover image dan stego image, dan adalah variance dari cover image dan stego image, adalah covariance dari cover image dan stego image serta dan adalah konstanta.

## III. PERANCANGAN SISTEM

### A. *Proses Embedded*

*1) Proses pra-steganografi :* Dalam proses pra-steganografi menggunakan algoritma *Block Permutation Image Steganography* (BPIS). Pesan rahasia yang akan disisipkan diubah terlebih dahulu ke dalam bentuk biner, kemudian kumpulan biner tersebut diurutkan dan dibagi perblok. Blok kemudian diacak dengan permutasi sehingga hasil dari proses ini adalah gabungan blok permutasi. Berikut merupakan flowchart prosedur pra-steganografi.

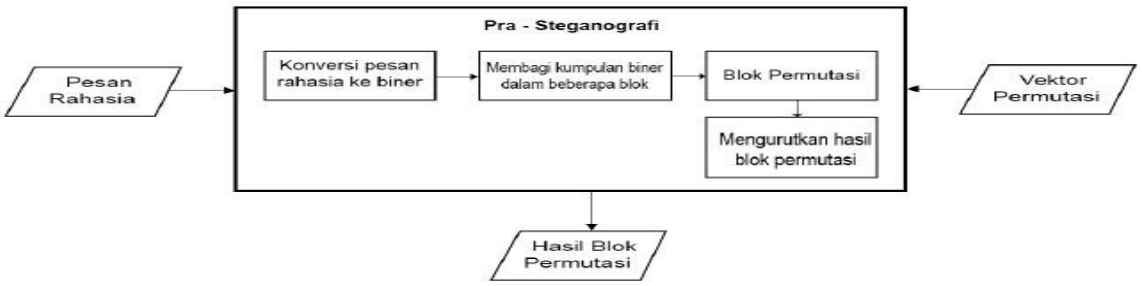


Fig. 3. Proses Pra-steganografi

Pesan rahasia yang disisipkan bertipe teks (.txt), teks tersebut berisi sekumpulan informasi dalam bentuk string. Tipe data string adalah tipe data yang digunakan untuk menyimpan barisan karakter. Kemudian pesan rahasia (file teks) diproses dengan cara melakukan konversi ke dalam bentuk biner (ASCII). Sebelum dilakukan konversi, pesan string akan diubah ke dalam bentuk char. Kemudian dari bentuk char tersebut dikonversi ke dalam bentuk biner 8-bit. Kemudian dilakukan proses permutasi untuk menunjang keamanan data ketika dilakukan proses ekstraksi.

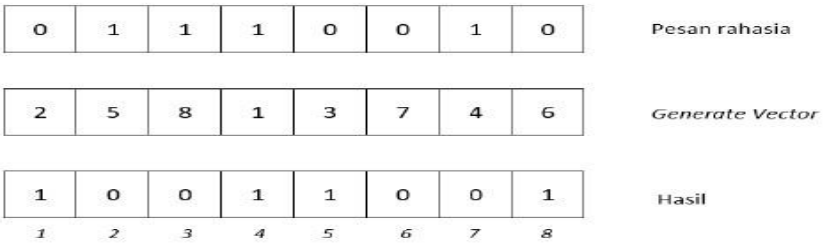


Fig. 4. Proses permutasi

*2) Proses Steganografi:* setelah proses pra-steganografi yang menerapkan algoritma *Blok Permutation Image Steganography* (BPIS) selesai, maka akan dihasilkan gabungan blok permutasi. Pada tahapan selanjutnya blok permutasi akan diproses dengan menggunakan algoritma genetika. Algoritma genetika pada sistem ini digunakan untuk mencari matriks dengan penyesuaian terbaik [2]. Operator pada algoritma genetika akan bekerja dengan melakukan manipulasi pada kromosom. Maka langkah utama yang dilakukan adalah melakukan pengkodean solusi ke dalam bentuk kromosom [9]. Pemilihan representasi yang digunakan perlu dilakukan untuk memudahkan dalam segi implementasi. Dalam satu gen terdiri dari beberapa bilangan integer antara [0-3], sedangkan jumlah gen dalam satu kromosom sebesar jumlah gen pada *cover image* yaitu 512x512 piksel (262.144). Setiap satu gen merupakan representasi dimensi pada *cover image.*


Fig. 5. Representasi Kromosom pada algoritma genetika

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

*B. Proses Ekstraksi*

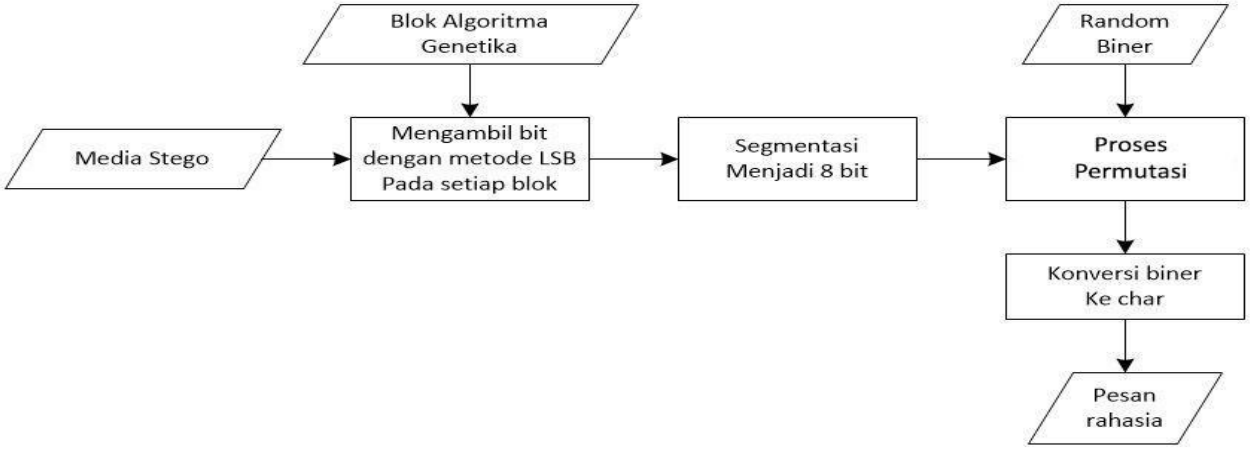


Fig. 6. Proses Ekstraksi

Dalam proses ekstraksi pesan rahasia pada media stego dibutuhkan hasil dari blok algoritma genetika dan random biner yang digunakan pada proses pra-steganografi. Sehingga tahap pertama yang perlu dilakukan adalah mengambil jumlah bit yang disisipkan pada setiap blok berdasarkan informasi dari hasil blok algoritma genetika. Selanjutnya bit-bit tersebut disusun ke dalam urutan biner 8 bit. Selanjutnya, melakukan proses *generate random vector permutation* dan melakukan proses permutasi pada setiap blok. kemudian masuk pada proses konversi urutan bit tersebut ke dalam bentuk *chararcter*. *Character* (char) tersebut merupakan pesan rahasia yang berhasil di ekstraksi dari media stego.

## IV. PEMBAHASAN

*A. Hasil dan Analisis*

*1) (Skenario 1) Analisis pengaruh fungsi fitness terhadap kualitas citra:* tujuan dibuatnya skenario satu adalah untuk melihat perbandingan antara nilai fitness SSIM dan PSNR. Ketika menggunakan fungsi fitness SSIM maka nilai SSIM akan lebih besar jika dibandingkan dengan nilai SSIM yang nilai fitness-nya PSNR. Sebaliknya, jika yang digunakan adalah fungsi fitness PSNR, maka nilai PSNR-nya lebih besar dari nilai PSNR dengan fungsi fitness SSIM. Dari tabel 1 terlihat jika pengujian setiap ukuran populasi menghasilkan nilai PSNR yang selalu lebih tinggi jika menggunakan fitness PSNR. Perbedaan terlihat jelas pada perbandingan dengan nilai PSNR yang menggunakan nilai fitness SSIM. Hal ini terjadi karena besarnya nilai yang dihasilkan dipengaruhi oleh fungsi atau nilai yang akan dioptimasi.

TABEL 1
HASIL PENGUJIAN SKENARIO 1

| *Cover Image* | Ukuran Populasi | *Fitness* PSNR | | | *Fitness* SSIM | | |
|---|---|---|---|---|---|---|---|
| | | SSIM | PSNR | MSE | SSIM | PSNR | MSE |
| lena.bmp | 10 | 0.9999 | 60.5179 | 0.0577 | 1.0000 | 60.3976 | 0.0593 |
| | 20 | 0.9999 | 60.5354 | 0.0575 | 1.0000 | 60.3924 | 0.0594 |
| | 30 | 0.9999 | 60.5588 | 0.0572 | 1.0000 | 60.4368 | 0.0570 |
| | **40** | **0.9999** | **60.5710** | **0.0570** | 1.0000 | 60.4098 | 0.0571 |
| | 50 | 0.9999 | 60.5594 | 0.0572 | 1.0000 | 60.4187 | 0.0571 |
| | **60** | 0.9999 | 60.5698 | 0.0570 | **1.0000** | **60.4369** | **0.0572** |

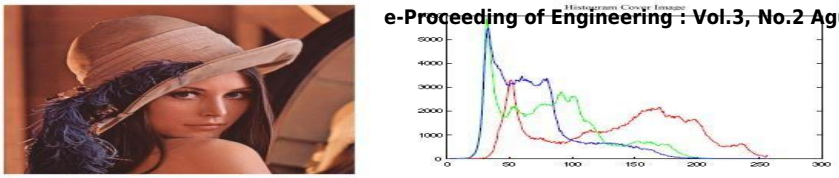

Fig. 7. Cover Image

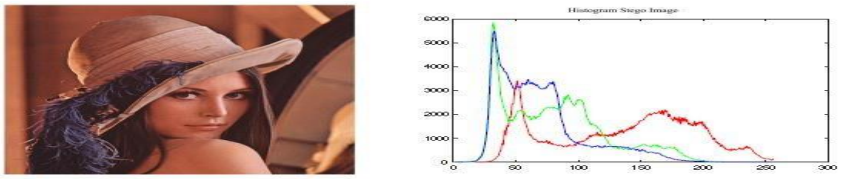

Fig. 8. Stego Image

*2) (Skenario 2) Pengaruh Permutasi terhadap performansi citra:* Dalam skenario yang kedua akan dilakukan pengujian pada steganografi dengan kombinasi antara permutasi dan algoritma genetika (AG), serta algoritma genetika (AG) tanpa menggunakan permutasi. Hasil dari skenario yang kedua dapat dilihat pada tabel 2 dibawah ini

TABEL 2
HASIL PENGUJIAN SKENARIO 2

| *Cover Image* | Ukuran Populasi | MSE | | PSNR | |
|---|---|---|---|---|---|
| | | Permutasi AG | AG Tanpa Permutasi | Permutasi AG | AG Tanpa Permutasi |
| lena.bmp | 30 | 0.0572 | 0.0573 | 60.5588 | 60.5476 |
| | 40 | 0.0570 | 0.0573 | 60.5710 | 60.5528 |
| | 50 | 0.0572 | 0.0571 | 60.5594 | 60.5666 |
| | 60 | 0.0570 | 0.0571 | 60.5698 | 60.5655 |

Dari hasil pengujian terlihat bahwa kombinasi antara permutasi dan algoritma genetika, dengan algoritma genetika tanpa menggunakan permutasi menghasilkan nilai yang tidak jauh berbeda pada nilai PSNR. Umumnya permutasi digunakan untuk meningkatkan keamanan data pada saat dilakukan proses ekstraksi. Sehingga untuk nilai PSNR kedua pengujian pada skenario ini tidak terlalu jauh berbeda. Berikut merupakan perbandingan hasil histogram pada skenario 2.

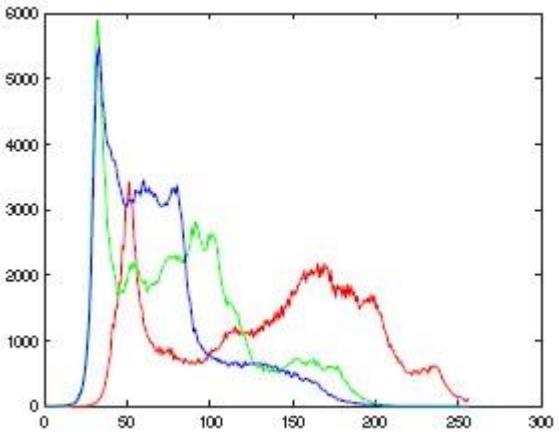


Fig 9. Histogram Permutasi AG

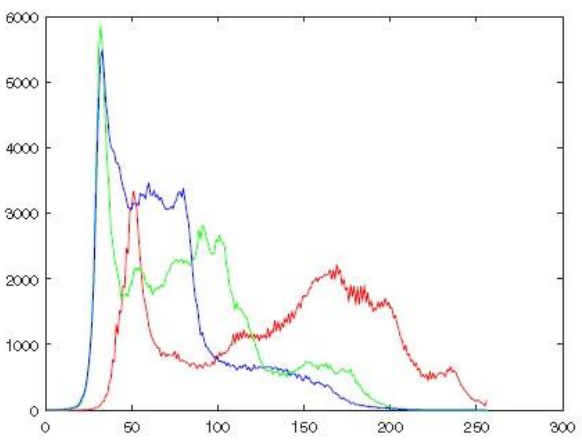


Fig 10. Histogram AG Tanpa Permutasi

Jika dilihat dari perbedaan histogram, tidak jauh berbeda dengan skenario satu, pada grafik bagian *red* mengalami fase kenaikan dan penurunan jumlah piksel. Sedangkan pada grafik bagian *green* dan *blue* tidak terlalu mengalami perubahan. Pada grafik bagian *red* sangat terlihat adanya perubahan, hal ini disebabkan karena proses penyisipan selalu mencari titik optimum yang dimulai dari bagian *red plane*, *green plane*, hingga masuk pada *blue plane*. Apabila ada seorang penyadap (*eavesdropper*) yang ingin mengambil pesan dan menemukan koordinat piksel yang telah disisipkan, maka dapat dihitung peluangnya. Pesan disisipkan dengan menggunakan teknik *Least Significant Bit* (LSB).

Untuk mengambil pesan pada citra digital dengan menggunakan teknik *Brute-force attack* maka diperlukan percobaan sebanyak $(2x2x2)^{512x512}$ kali. Dimana peluang dengan besar (2x2x2) merupakan bagian *plane* dalam RGB. Setiap *plane* hanya memiliki 2 peluang yaitu 0 (tidak disisipi) dan 1 (disisipi). Sedangkan (512x512) merupakan jumlah dimensi yang digunakan pada citra digital. Jika hal tersebut dilakukan maka memerlukan waktu yang lama dan memiliki jumlah iterasi besar. Kemudian, jika seorang penyadap (*eavesdropper*) telah berhasil memecahkan masalah tersebut, seorang penyadap (*eavesdropper*) akan dihadapkan pada blok permutasi yang harus dipecahkan dari banyaknya iterasi tersebut. Dengan besar vektor permutasi yang digunakan adalah 8 bit. Sehingga, jika seorang penyadap (*eavesdropper*) ingin memecahkan persoalan ini secara *Brute-force attack*, maka dibutuhkan 8! kali percobaan.

*3)* (Skenario 3) Pengaruh algoritma genetika terhadap performansi citra: Dalam skenario yang ketiga dilakukan pegujian terhadap permutasi dengan algoritma genetika, dengan permutasi tanpa menggunakan algoritma genetika. Hasil dari skenario ini dapat dilihat pada tabel 3 dibawah ini.

TABEL 3
HASIL PENGUJIAN SKENARIO 3

| *Cover Image* | Ukuran Populasi | MSE | | PSNR | |
|---|---|---|---|---|---|
| | | Permutasi AG | Permutasi Tanpa AG | Permutasi AG | Permutasi Tanpa AG |
| lena.bmp | 30 | 0.0572 | | 60.5588 | |
| | **40** | 0.0570 | | **60.5710** | |
| | 50 | 0.0572 | **0.2103** | 60.5594 | **54.9364** |
| | 60 | 0.0570 | | 60.5698 | |

Pada tabel 3 dapat dilihat bahwa setiap percobaan dengan algoritma genetika dilakukan dengan ukuran populasi berbeda. Nilai PSNR dan MSE yang dihasilkan menggunakan algoritma genetika selalu lebih baik apabila dibandingkan pada proses permutasi tanpa menggunakan algoritma genetika. Hal ini disebabkan karena pada proses yang tidak menggunakan algoritma genetika hanya menggunakan algoritma LSB saja tanpa mempertimbangkan nilai PSNR, SSIM, dan MSE. Berikut perbandingan histogram yang dihasilkan dari *stego image* pada skenario 3.

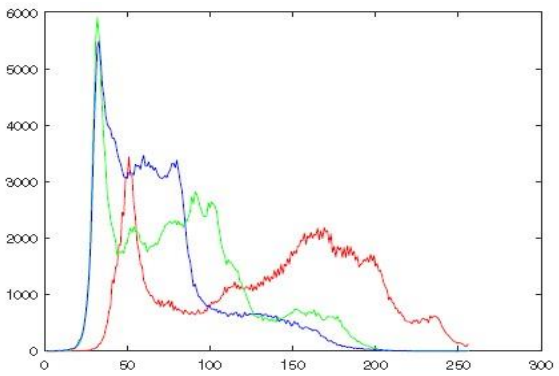


Fig 11. Histogram Permutasi AG

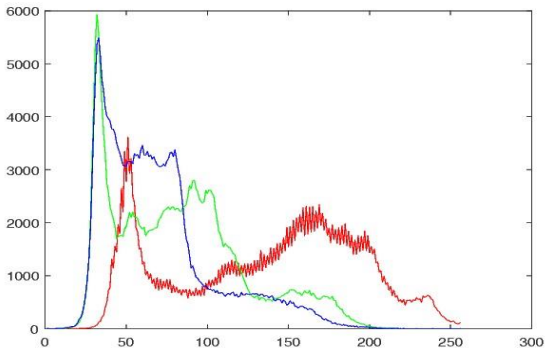


Fig 12. Histogram Permutasi Tanpa AG

Nilai PSNR terbaik yang diperoleh pada pengujian dengan algoritma genetika, yaitu sebesar 60.5710 pada ukuran populasi 40. Sedangkan pada pengujian yang tidak menggunakan algoritma genetika diperoleh nilai fitness PSNR 54.9364.

## V. KESIMPULAN

Berdasarkan penelitian dan uji coba yang telah dilakukan, maka dapat disimpulkan sebagai berikut:

1. Metode permutasi dan algoritma genetika dapat digunakan pada steganografi, sehingga pesan rahasia berhasil disisipkan pada cover image dan diekstraksi kembali dari stego image.
2. Berdasarkan hasil uji coba sistem untuk performansi citra, maka fungsi fitness harus disesuaikan dengan fungsi yang dioptimasi. Jika ingin mendapatkan nilai dengan kualitas citra PSNR terbaik maka dapat menggunakan fungsi fitness PSNR. Jika ingin mendapatkan nilai kualitas citra SSIM terbaik maka dapat menggunakan fungsi fitness SSIM.
3. Pada fungsi fitness PSNR, peformansi kualitas citra terbaik yaitu sebesar 60.5710 dB. Sedangkan Pada fungsi fitness SSIM, peformansi kualitas citra nterbaik yaitu sebesar 1.0000.
4. Dari hasil uji coba sistem pada skenario kedua, terbukti bahwa permutasi tidak berpengaruh terhadap performansi kualitas gambar, Dengan demikian kualitas citra stego yang dihasilkan tetap baik. Dengan menggunakan permutasi maka tingkat keamanan pesan lebih tinggi.
5. Dengan meggunakan algoritma genetika, nilai performansi kualitas gambar yang dihasilkan lebih baik. Sehingga error yang dihasilkan pada MSE lebih kecil dibanding tidak menggunakan algoritma genetika.

## REFERENCES

[1] Al-Bahadili, Hussein. (2013). A Secure Block Permutation Image Steganography Algorithm. Faculty of Information Technology, University of Petra.
[2] Wang, Shen, Bian Yang, dan Xiamu Niu. (2010).A Secure Steganography Method based on Genetic Algorithm. School of Computer Science and Technology, Harbin Institute of Technology.
[3] Utomo, Tri Prasetyo. (2012). Steganografi Gambar Dengan Metode Least Significant Bit Untuk Proteksi Komunikasi Pada Media Online.Fakultas Sains dan Teknologi, UIN Sunan Gunung Djati Bandung.
[4] Shihab, Adnan M., Raghad K. Mohammed, dan Woud M. Abed. (2013). Evaluating The Performance Of The Secure Block Permutation Image Steganography Algorithm. University of Baghdad.
[5] M, Vikranth.B., Muzammil Hasan Momin, Sayed Muneer Mohsin, Saurav Rimal, dan Saswat Raj Pandey. (2015). A Survey Of Image Steganography. Department Of Computer Science and Engineering, BMSCE.
[6] Suyanto.(2007).Artificial Intelligence. Bandung: Informatika Bandung.
[7] Text Corpora. http://corpus.canterbury.ac.nz/descriptions/calgary diakses pada 28 Oktober 2015.
[8] Cantu-Paz, Erick. (2012). On Random Numbers and the Performance of Genetic Algorithms. Center for Applied Scientific Computing, Lawrence Livermore National Laboratory.
[9] Zukhri, Zainudin. (2014). Metode Komputasi Evolusioner untuk Menyelesaikan Masalah Optimasi. Yogyakarta: Andi Offset.
[10] Reese, Andrea. (2009). Random number generators in genetic algorithms for unconstrained and constrained optimization. Daytona State College.
[11] Putra, Darma. (2010). Pengolahan Citra Digital. Yogyakarta: Andi Offset.
[12] Herry, M., Purnomo, Arif Muntasa.(2010).Konsep pengolahan citra digital dan ekstraksi fitur. Yogyakarta: Graha Ilmu.
[13] Prabowo, Anton., Hidayatno, Achmad., Christiyono, Yuli.(2011). Penyembunyian Data Rahasia pada Citra Digital Berbasis Chaos dan Discrete Cosine Transform. Universitas Diponegoro.
[14] Sandika Putra, Satya., Sidik Sasongko, Priyo., Bahtiar, Nurdin. (2011). Verifikasi Kepemilikan Citra Medis dengan Kriptografi RSA dan LSB Watermarking. Universitas Diponegoro.
[15] Chalekar, MS. K.T., Yengntiwar, T.S. (2014). Image Contrast Enhancement By Using Optimal Contrast - tone Mapping Method. University India.