ANALISIS DAN IMPLEMENTASI IMAGE WATERMARKING MENGGUNAKAN METODE MULTIPLE SCANNING DIFFERENCE VALUE HISTOGRAM

Analysis and Implementation of Image Watermarking Using Multiple Scanning Difference Value Histogram

Daniel Gilbert Bismark **Gelar Budiman,ST., MT.** **I Nyoman Apraz Ramatryana,ST., MT.**

Prodi S1 Teknik Telekomunikasi, Fakultas Teknik, Universitas Telkom

Jl. Telekomunikasi, Dayeuh Kolot Bandung 40257 Indonesia

danielgilbetr@gmail.com

Abstrak

Saat ini adalah era dimana semua orang menggunakan internet untuk kebutuhan sehari-hari. Ada yang melakukan transaksi secara online, melakukan pembayaran dengan Internet banking, bermain game online , dan lain-lain. Oleh karena itu diperlukan teknik Digital Watermarking, yaitu untuk menanamkan data digital dalam file secara rahasia kedalam suatu data lainnya, tetapi tidak diketahui keberadaannya oleh indera manusia.

Dalam perancangan ini diharapkan berkas *watermark* dapat diekstraksi dari berkas citra dengan tetap menjaga kualitas. Parameter performansi yang diuji dalam tugas akhir ini adalah PSNR dan seberapa besar kapasitas bit yang bisa disisipi. Kapasitas bit yang bisa disisipi di citra host akan berbeda satu host dengan host yang lain. Metode ini menggunakan dua teknik *scanning*, yaitu horizontal dan vertical. Masing-masing teknik akan membandingkan besar kapasitas bit yang bisa disisipi, kemudian memilih teknik yang akan digunakan.

Kata kunci : *image watermarking, histogram, reversible data hiding, Multiple Scanning Difference Value Histogram, PSNR,horizontal,vertical*

Abstract

This is the era in which all people use the Internet for their daily needs. There conducting online transactions, make payments with Internet banking, online gaming, and others. Therefore we need a Digital Watermarking technique, which is to embed digital data in a secret file into an other data, but it is not known to exist by human senses.

In this scheme is expected to file a watermark can be extracted from the image file while maintaining quality. Performance parameters tested in this thesis is PSNR and how much capacity of bits that can be inserted. Capacity of bits that can be inserted in the image of the host will be different from one host to another host. This method uses two scanning techniques, ie horizontal and vertical. Each of these techniques will compare the large capacity of bits that can be inserted, then choose the techniques to be used.

1.Pendahuluan

1.1 Latar Belakang

Saat ini adalah era dimana semua orang menggunakan internet untuk kebutuhan sehari-hari. Ada yang melakukan transaksi secara online, melakukan pembayaran dengan Internet banking, bermain game online , dan lain-lain. Semua orang pasti melakukan satu kegiatan di dunia maya, yaitu download (mengunduh) file seperti audio, video, *image*. Di dunia maya pasti ada orang yang mengklaim file audio , video, *image* sebagai hak miliknya, padahal file tersebut kepunyaan orang lain atau malah suatu perusahaan. Karena kurang perlidungan dan pencegahan pada file multimedia tersebut adalah salah satu penyebab terjadinya klaim atas kepunyaan orang, penyebaran dan penggandaan sampai saat ini. Oleh karena itu untuk menjaga file multimedia beserta hak cipta atas penggandaan dan penyebarannya, dikembangkan teknik *Digital Watermarking*.

Teknik *Digital Watermarking* adalah teknik untuk menanamkan data digital dalam *file* secara rahasia kedalam suatu data lainnya, tetapi tidak diketahui keberadaannya oleh indera manusia (indera penglihatan atau indera pendengaran), dan mampu menghadapi pengolahan sinyal digital sampai pada tahap tertentu.Teknik watermarking ini menggunakan metode *Single Scanning Histogram Modification*. Dengan metode tersebut, kita dapat menyisipkan atau menanam data informasi rahasia sebesar yang sedikit. Oleh karena keterbatasan kapasitas saat menanamkan informasi, dibutuhkan metode baru.

Maka dari itu diperlukan suatu metode baru, yaitu metode *multiple scanning difference value histogram*. Dengan menggunakan metode *Multiple scanning difference value histogram*, maka yang pada mulanya kita menanamkan data rahasia, kemudian kita membandingkan kapasitas yang paling besar antara teknik *scanning horizontal atau scanning vertical.* Hal ini bergantung kepada *Host* atau citra gambar yang digunakan.

1.2 Perumusan Masalah

1. Bagaimana merancang dan mengimplementasi *image watermarking* dengan metode *Multiple Scanning Difference Value Histogram*.
2. Kualitas *host image* sebelum dan sesudah disisipkan *watermark*
3. Kualitas pesan sebelum dan sesudah diekstrasi dari *host image*
4. Menghitung kapasitas data *watermark* yang dapat disisipkan pada *host image.*

1.3 Asumsi dan Batasan Masalah

1. Sistem yang dirancang hanya menangani tentang proses penyisipan data ke dalam *image* dan mengekstraknya kembali.
2. Hanya menggunakan teknik *Multiple Scanning* dengan horizontal dan vertikal
3. Tidak dilakukan perbandingan dengan metode *image watermark* lainnya.
4. Mengukur PSNR, MSE, kemudian mengukur BER pada saat melakukan proses pengujian/serangan.
5. Menggunakan *host image* dengan *grayscale*, berukuran 512×512
6. Menggunakan citra *watermark* dengan ukuran 64×64, dan citra *watermark* tersebut terdiri dari bit biner.

1.4 Tujuan Penelitian

Adapun Tujuan penelitian pada tugas akhir ini adalah sebagai berikut:

1. Merancang *image watermarking* dengan metode *Multiple Scanning Diffrence Value Histogram* menggunakan MATLAB.
2. Menganalisa kualitas *host image* sebelum dan sesudah penyisipan. Menganalisa kualitas *watermark* sebelum dan sesudah ekstrasi.
3. Mengetahui kapasitas penyisipan pada setiap *host image.*

1.5 Metode Penelitian

1. Studi Literatur

   Mempelajari teori dan konsep yang berhubungan dengan tugas akhir ini. Melalui pustaka-pustaka yang berkaitan dengan penelitian, baik berupa buku maupun jurnal ilmiah.
2. Perancangan Sistem

   Perancangan aplikasi berdasarkan masalah yang telah diidentifikasi dan dirumuskan
3. Implementasi Sistem

   Aplikasi yang telah dirancang akan diimplementasikan pada MATLAB
4. Pengujian Sistem

   Aplikasi yang telah dirancang akan diuji apakah telah berjalan atau tidak.
5. Analisa Hasil Pengujian

   Data-data hasil pengujian akan dianalisa mengenai kesesuaian hasil pengujian tersebut dengan hasil yang diharapkan.
6. Penulisan Laporan

   Tahap ini dilakukan penulisan laporan tentang hasil yang telah diujikan dan analisa dari data-data hasil pengujian yang telah dilakukan.

2. Dasar Teori

2.1 Steganography

Steganografi digital bertujuan menyembunyikan informasi digital ke dalam saluran rahasia sehingga satu dapat menyembunyikan informasi dan mencegah deteksi pesan tersembunyi [1]. *Steganalysis* adalah seni menemukan adanya informasi yang tersembunyi; seperti sistem steganalytic digunakan untuk mendeteksi apakah sebuah gambar mengandung pesan tersembunyi. Dengan menganalisis berbagai fitur gambar antara stego-gambar (gambar yang mengandung pesan tersembunyi) dan gambar cover (gambar yang tidak mengandung pesan tersembunyi), sebuah Sistem steganalytic mampu mendeteksi stego-gambar. Kriptografi adalah praktek berebut pesan ke bentuk dikaburkan untuk mencegah orang lain dari pemahaman itu, sementara steganografi adalah praktek mengaburkan pesan sehingga tidak bisa ditemukan.

Untuk sistem steganografi, persyaratan mendasar adalah bahwa stego-image menjadi perseptual dibedakan ke tingkat yang tidak menimbulkan kecurigaan. Di Dengan kata lain, informasi yang tersembunyi memperkenalkan hanya sedikit modifikasi penutup objek. Kebanyakan sipir pasif mendeteksi stego-gambar dengan menganalisis fitur statistik mereka.

2.2 *Digital Watermarking*

Watermarking bukan fenomena baru. Selama hampir seribu tahun, *watermark* di atas kertas telah digunakan untuk terlihat menunjukkan penerbit tertentu dan untuk mencegah pemalsuan mata uang. Sebuah *watermark* desain terkesan pada selembar kertas selama produksi dan digunakan untuk identifikasi hak cipta . Desain mungkin pola, logo, atau beberapa gambar lainnya. Di era modern, seperti kebanyakan data dan informasi disimpan dan dikomunikasikan dalam bentuk digital, membuktikan keaslian memainkan peran yang semakin penting [1].

Akibatnya, *watermarking digital* adalah proses dimana informasi yang sewenang-wenang dikodekan ke dalam gambar dengan cara seperti menjadi tak terlihat untuk pengamat gambar.

2.3 *Single Scanning Histogram Modification*

Proses *embedding* dilakukan dengan tahapan sebagai berikut [3]:

1. Melakukan pembagian blok-blok di dalam gambar, dalam kasus ini gambar dibagi menjadi blok 4x4 .
2. Setelah melakukan pembagian blok-blok gambar, Memilih teknik scanning yang akan digunakan.
3. Setelah memilih teknik *scanning*, maka langkah selanjutnya adalah menjabarkan nilai pixel sesuai dengan teknik *scanning*.
4. Langkah selanjutnya adalah melakukan komputasi pengurangan, yakni dengan cara mengurangi nilai pixel dengan nilai pixel yang sebelumnya. Untuk nilai pixel yang paling pertama nilainya tidak berubah karena nilai pixel yang paling pertama dijadikan nilai pixel acuan.
5. Lakukanlah pergeseran histogram, yakni nilai pixel yang nilai positif akan ditambahkan 1, sedangkan yang nilai pixel yang nilainya 0 atau nilai pixelnya negatif maka nilainya tidak berubah.
6. Lakukan proses *embedding*. Proses *embedding* dilakukan dengan cara melakukan penambahan nilai pixel di tempat dimana ada nilai pixel yang 0.
7. Setelah Proses embedding, maka lakukanlah proses pengurangan dengan acuan dari nilai pixel sebelum komputasi pengurangan (nilai pixel asli, yakni nilai pixel yang ada langkah ke-3).
8. Kembalikan susunan nilai pixel dengan menggunakan teknik scanning yang dipakai.

Persamaan pergeseran histogram adalah[3]:

$$\text{[illegible]} = \begin{cases} \text{[illegible]} \le 0{,}2 \le i \le \text{[illegible]} \\ \text{[illegible]} + 1 \quad \text{[illegible]} > 0{,}2 \le i \le \text{[illegible]} \end{cases}$$

Proses pengembalian image pixel dengan persamaan berikut[3]:

$$\text{[illegible]} = \begin{cases} \text{[illegible]} \quad \text{[illegible]} - \text{[illegible]} \le 0{,}2 \le i \le \text{[illegible]} \\ \text{[illegible]} + 1 \quad \text{[illegible]} - \text{[illegible]} \ge 0{,}2 \le i \le \text{[illegible]} \end{cases}$$

Dan, Persamaan matematis embedding adalah[3] :

$$\text{[illegible]}' = \begin{cases} \text{[illegible]} + w \quad \text{[illegible]} = 0{,}2 \le i \le \text{[illegible]} \\ \text{[illegible]} \quad \text{[illegible]} \ne 0{,}2 \le i \le \text{[illegible]} \end{cases}$$

Proses ekstrasi bit sisip dengan persamaan[3]:

$$w = \begin{cases} 0 \quad \text{[illegible]} - \text{[illegible]} = 0{,}2 \le i \le \text{[illegible]} \\ 1 \quad \text{[illegible]} - \text{[illegible]} = 1{,}2 \le i \le \text{[illegible]} \end{cases}$$

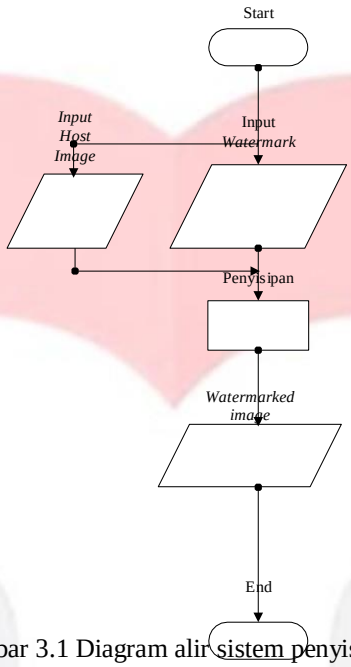
2.4 Multiple Scanning Histogram Modification

Teknik yang aktif pertama kali akan dijadikan acuan untuk menjadi muatan maksimal. Kemudian akan dilakukan algoritma iterasi sebagai berikut :

1. Menjalankan Program Teknik *scanning Horizontal* dan *vertical* secara bersamaan.
2. Memilih Kapasitas yang paling besar dari salah satu teknik *sccanning* diatas.
3. Bila sudah memilih Kapasitas Penyisipan yang paling besar, maka lakukanlah teknik scanning tersebut untuk melakukan penyisipan.
4. Setelah berhasil melakukan penyisipan Watermark di dalam *host* citra, melakukan perhitungan MSE dan PSNR.

3. Sistem

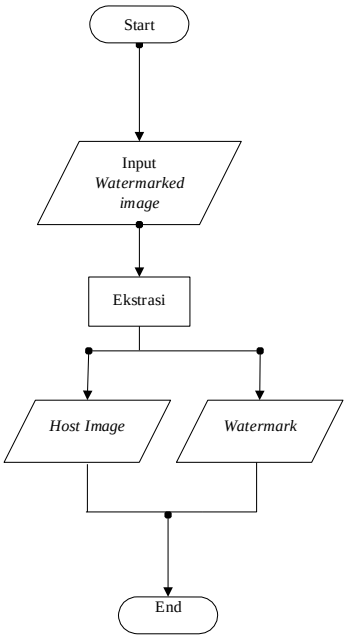
3.1 Diagram Alir Sistem



Gambar 3.1 Diagram alir sistem penyisipan

Gambar 3.1 adalah alur kerja dari sistem *image watermarking* untuk penyisipan ini dapat dijabarkan dalam penjelasan berikut :

1. Ketika pertama kali aplikasi dijalankan, sistem akan masuk ke *menu* dimana *user* memilih *host image* dan *image watermark.*
2. Setelah memilih, maka sistem akan melakukan penyisipan, sehingga didapatkan *image* yang telah disisipkan
3. Setelah proses penyisipan, dapat diketahui juga nilai PSNR dan MSE dari gambar hasil penyisipan.



Gambar 3.2 Diagram Alir sistem ekstrasi

Gambar 3.2 adalah alur kerja dari sistem *image watermarking* untuk Ekstrasi ini dapat dijabarkan dalam penjelasan berikut :

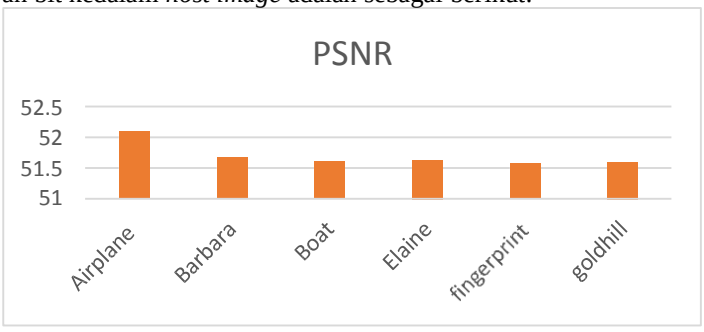
1. Ketika sistem ekstrasi dijalankan, *user* akan memilih *image* yang sebelumnya sudah disisipkan dan disimpan.
2. Setelah *user* memilih *image*, maka dapat dilakukan proses ekstrasi. Hasil *output* dari proses ekstrasi adalah *host image* dan *image watermark*.
3. Proses ekstrasi dikatakan berhasil bila tidak ditemukan kerusakan pada *host image* dan *image watermark* nya.

4. Pengujian dan Analisis

Untuk megetahui performansi system yang telah dirancang, maka perlu dilakukan pengujian terhadap system yang telah dikembangkan. Pada tahap pengujian dilakukan beberapa langkah pengujian terhadap beberapa sampel gambar. Tingkat keberhasilan sistem ditunjukkan dengan membandingkan besar kapasitas penyisipan.

4.1 Analisis uji penyisipan bit

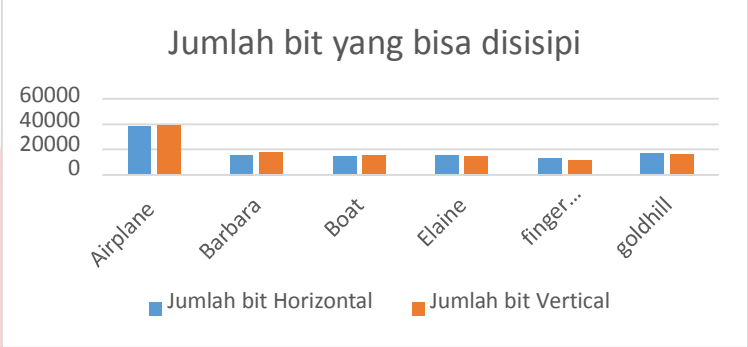
Untuk pengujian penyisipan bit kedalam *host image* adalah sebagai berikut:



Gambar 4.1 PSNR

Dari gambar 4.1, diperoleh hasil bahwa sampel Gambar Airplane memiliki nilai PSNR yang lebih tinggi dari sampel gambar yang lain yaitu, 52.089 db. Sedangkan untuk nilai PSNR yang terendah adalah sampel gambar fingerprint dengan nilai 51.5739 db. Untuk PSNR yang baik adalah yang nilainya berada diatas 30 db, karena diatas 30 db gambar hasil penyisipan tidak terlihat perbedaannya dengan kasat mata [2]. Pada saat proses ekstrasi selesai, kualitas citra watermark tidak mengalami gangguan, hal ini dibuktikan dengan nilai BER 0.

4.2 Pengujian Jumlah bit yang bisa disisipi

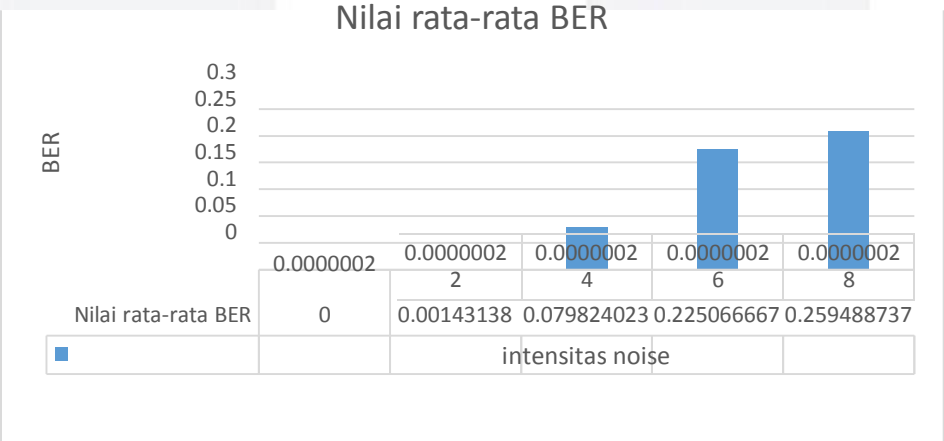


Gambar 4.2 Kapasitas penyisipan

Berdasarkan gambar 4.2 dapat diperoleh bahwa jumlah bit sisip yang paling terbesar adalah sampel gambar airplane dengan menggunakan teknik vertikal, yakni 38927 bit. Untuk tiap sampel gambar akan berbeda-beda dalam penggunaan teknik *scanning*. Gambar Airplane memiliki kapasitas penyisipan yang besar karena memiliki banyak nilai pixel yang sama, sehingga mengakibatkan saat terjadi proses *histogram shifting* pada proses *embedding*, maka didapatkan jumlah nilai *pixel* 0 yang banyak. Hal tersebut mengakibatkan nilai *pixel* 0 menjadi tempat untuk menyisipkan informasi rahasia berupa bit.

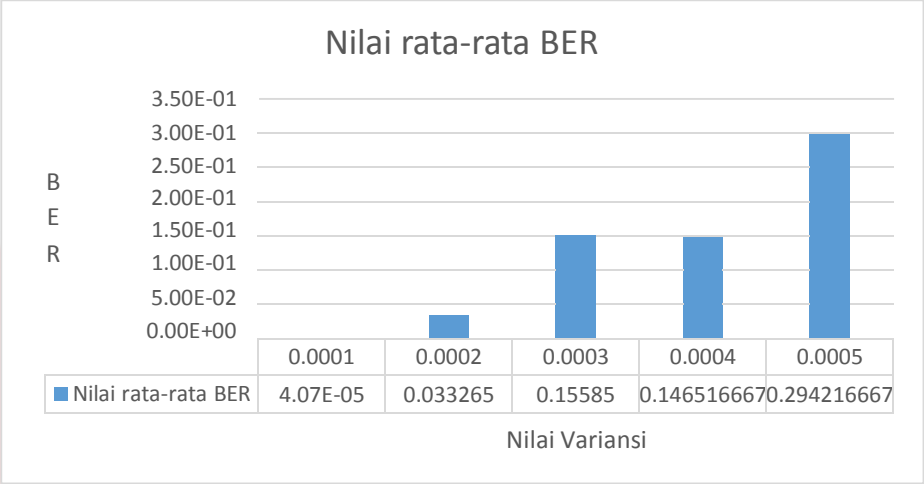
4.3 Pengujian dengan memberikan noise

Pada pengujian kali ini, *image* yang sudah diberi *watermark* akan diberikan *noise Gaussian*. Setelah diberi noise , akan dilakukan proses ekstrasi untuk melihat nilai BER nya. Intensitas noise yang diberikan ada di 0.0000002, 0.00000022, 0.00000024, 0,00000026, 0.00000028.



Gambar 4.3 Nilai rata-rata BER di noise *Gaussian*

Berdasarkan grafik gambar 4.3 , yakni Nilai rata-rata BER diambil dari nilai tiap sampel kemudian diambil nilai rata-rata BER yang diklasifikasikan berdasarkan intensitas noisenya. Semakin tinggi nilai intensitas, maka semakin besar nilai BER nya. Pada intensitas 0.00000026, nilai BER sudah mencapai 0.2, dimana sudah terlihat kerusakan pada citra *watermark* saat proses ekstrasi. Nilai BER semakin tinggi karena tingkat penyebaran noise juga semakin tinggi mengakibatkan noise merubah beberapa nilai pixel,sehingga saat melakukan ekstrasi nilai pixel tidak bisa kembali ke nilai pixel yang awal.



Gambar 4.4 Nilai rata-rata BER di noise *salt&pepper*

Berdasarkan Data grafik pada gambar 4.7, nilai rata-rata BER dari tiap intensitas noise, dimana setiap sampel gambar diambil data nilai BER, kemudian dihitung nilai rata-rata BER nya berdasarkan intensitas noise nya. Semakin nilai intensitas *noise* ditingkatkan, maka semakin meningkat juga nilai BER nya, sehingga mengakibatkan kualitas citra *watermark* terganggu. Hal ini diakibatkan karena saat memberikan noise pada hasil setelah *embedding*, beberapa nilai pixel setelah proses *embedding* dan nilai pixel setelah pemberian noise berbeda,sehingga saat melakukan proses ekstrasi, nilai pixel tidak kembali ke nilai pixel semula. Semakin tinggi nilai intensitas noise, mengakibatkan banyak nilai pixel berubah saat setelah diberikan noise.

.

5. Kesimpulan

Berdasarkan hasil pengujian dan analisis yang telah dilakukan pada implementasi *image watermarking* menggunakan metode *Multiple scanning difference value histogram*, maka dapat diambil kesimpulan sebagai berikut :

1. Kualitas *host image* sebelum penyisipan dan setelah ekstrasi tanpa adanya proses pengujian tetaplah sama, tidak terjadi perubahan atau kerusakan pada *host image*. Hal ini dapat dilihat dari kualitas gambar hasil *embedding*, yakni PSNR nya yang rata-rata diatas 50 db. Sedangkan gambar hasil *embedding* yang baik memiliki PSNR diatas 30 db.
2. Kualitas *watermark* sebelum penyisipan dan setelah ekstrasi tanpa adanya proses pengujian tetaplah sama, tidak terjadi perubahan atau kerusakan pada *watermark*. Hal ini dapat kita lihat saat proses ekstrasi selesai, nilai BER menunjukkan 0.
3. Setiap *host image* yang digunakan saat melakukan proses penyisipan menggunakan teknik *scanning* yang berbeda satu sama lain. *Host image airplane* mempunyai kapasitas bit penyisipan yang paling besar,yakni 38.927 bit dengan menggunakan teknik *scanning* vertical.

.

Daftar Pustaka

[1]F. Y. Shih, Digital watermarking and steganography : Fundamentals and Teqniques, USA: Taylor & Francis, 2008.

[2]I. J. Cox, M. L. Miller, J. A. Bloom, Fridrich, J. and T. Kalker, Digital Watermarking and Steganography Second Edition, San Francisco: Morgan Kaufmann, 2008.

[3]b. H. L. Z.-M. L. J.-S. P. Zhenfei Zhaoa, "Reversible data hiding based on multilevel histogram modification and," International Journal of Electronics and Communications (AEÜ), 2011.