APLIKASI METODE STEGANOGRAPHY PADA CITRA DIGITAL DENGAN MENGGUNAKAN METODE LSB (LEAST SIGNIFICANT BIT)

Agustinus Noertjahyana, Samuel Hartono, Kartika Gunadi

Universitas Kristen Petra, Jl. Siwalankerto 121-131 Surabaya

agust@peter.petra.ac.id, sam_har@yahoo.com, kgunadi@peter.petra.ac.id

Abstrak

Saat ini pengiriman data telah banyak dilakukan melalui media digital (Internet, E-mail, dan sebagainya).Data yang dikirim melalui media digital tersebut bisa berupa data yang penting, sehingga muncul permasalahan pada saat pengiriman data yaitu terkait dengan keamanan data.Terlebih lagi apabila data yang dikirimkan merupakan data yang bersifat rahasia.Untuk itulah muncul pemikiran bagaimana data dapat dikirimkan secara aman dalam artian data tidak bisa dibaca secara langsung atau bahkan tidak bisa diganti.

Citra digital adalah salah satu media yang paling umum dikenal oleh masyarakat.*Steganography* adalah suatu metode *cryptography*, yang digunakan untuk menyembunyikan data ke dalam citra digital sehingga data yang dikirimkan tidak dapat diidentifikasi oleh pihak yang tidak bertanggung jawab.Pada penelitian ini akan menggunakan metode LSB (*Least Significant Bit*). Data akan di segmentasikan pada beberapa citra digital sehingga memungkinkan pengiriman data dengan ukuran yang besar.

Dengan mengembangkan metode *steganography* maka pengiriman data yang dilakukan tidak hanya memiliki tingkat keamanan yang baik, namun juga memiliki efisiensi dalam proses penyembunyian data yangcukup tinggi yaitu sekitar 30%.

Kata kunci : *Citra Digital, LSB, Steganography*

1. Pendahuluan

Saat ini, pengiriman data melalui media elektronik semakin meningkat. Bukan hanya data biasa, bahkan data perusahaan yang bersifat rahasia pun saat ini dikirimkan melalui internet. Data bisa terkirim secara langsung atau bahkan melalui bentuk citra digital.

Citra digital merupakan salah satu bentuk media yang banyak dijumpai. Dengan menggunakan metode *Steganography*, maka penyembunyian data di dalam citra digital dapat dilakukan sehingga dapat memungkinkan dilakukannya pengiriman data dengan menggunakan citra digital sebagai pembawa (*carrier*).

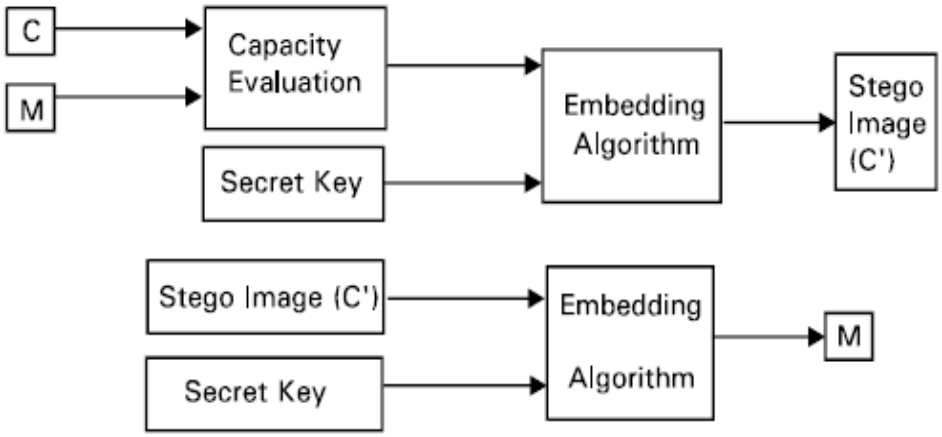
Saat ini metode *Steganography* mengalami banyak perkembangan, salah satu pengembangan yang dapat dilakukan adalah dengan mengembangkan efisiensi daya tampung data yang dapat disembunyikan pada sebuah citra digital.Pada penelitian ini akan membahas mengenai pengembangan metode *Steganography* dengan menggunakan metode LSB (*Least Significant Bit*).

2. Kajian Pustaka

2.1 Metode Steganography

Steganography adalah seni menyembunyikan informasi untuk mencegah pendeteksian pesan yang disembunyikan [2].*Steganography* berasal dari bahasa Yunani yang memiliki arti penulisan terlapis (*covered writing*), termasuk di dalamnya suatu metode komunikasi rahasia dalam jumlah besar yang menyembunyikan pesan dengan sangat baik.*Steganography* dan *Cryptography* memiliki garis besar tujuan yang sama yaitu mengamankan suatu informasi namun terdapat perbedaan mendasar yang terletak pada cara pengamanannya. *Cryptography* mengacak pesan sehingga tidak dapat terbaca, sedangkan *Steganography* bertujuan untuk menyembunyikan informasi sehingga tidak dapat terlihat.Pada *cryptography*, informasi yang tersimpan dalam bentuk *ciphertext* dapat menimbulkan kecurigaan pada penerima sehingga dapat menyebabkan timbulnya usaha untuk melakukan pembobolan (*hacking*), namun hal ini tidak terjadi pada informasi tersembunyi (*hidden* message) yang diolah dengan metode *Steganography*.

Secara garis besar metode Steganography terdiri dari 2 bagian utama [5], yaitu proses penyembunyian data *(hidden message)* dan proses pengembalian data ke bentuk semula *(reveal message)*. Kedua proses ini dilakukan dengan menggunakan sebuah kata kunci rahasia *(secret key)* yang akan digunakan di dalam prosesnya untuk meningkatkan keamanan data. Untuk lebih jelas mengenai konsep steganography dapat dilihat pada gambar 1.

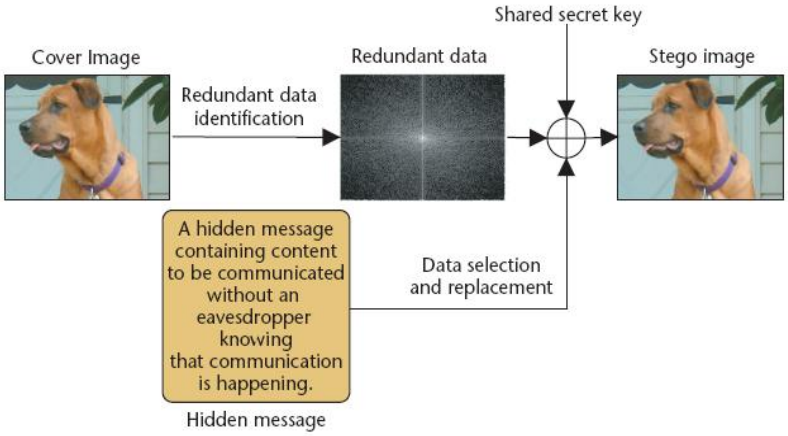


Gambar 1. Bagan Proses Penyembunyian dan Pengembalian Data

Proses penyembunyian data pada metode *steganography* adalah salah satu bagian yang memegang peranan penting di dalam proses secara keseluruhan dimana pada bagian ini, penyembunyian data yang merupakan inti dari metode *steganography* dilakukan. Pada proses penyembunyian data ini diperlukan ketepatan dalam perhitungan bit – bit warna serta bit – bit data karena jika terjadi sedikit kesalahan saja pada perhitungan maka akan berakibat pada rusaknya data yang dikirimkan sehingga data tidak akan dapat dikembalikan ke dalam bentuk semula. Selain itu ukuran keberhasilan pada metode *steganography* juga dipengaruhi oleh proses penyembunyian data dimana hasil dari proses penyembunyian data yang berupa *stego image* haruslah menyerupai gambar asli *(cover image)* sehingga tidak terjadi kecurigaan dari pihak lain yang melihatnya. Selain itu faktor efisiensi data juga perlu dipertimbangkan dalam penyembunyian data sehubungan dengan perbandingan besarnya data yang disembunyikan dengan kualitas *stego image* yang dihasilkan (semakin besar data yang disembunyikan maka kualitas *stego image* yang dihasilkan semakin rendah). Besar data yang dapat dihasilkan oleh metode *steganography* secara umum mencapai sekitar 5 hingga 10 persen dari ukuran file citra digital [6].

Untuk menyembunyikan data dengan menggunakan metode *Steganography* membutuhkan dua buah file[3], pertama adalah sebuah file citra digital yang akan digunakan sebagai untuk menyembunyikan informasi yang disebut sebagai *Cover Image* dan sebuah file

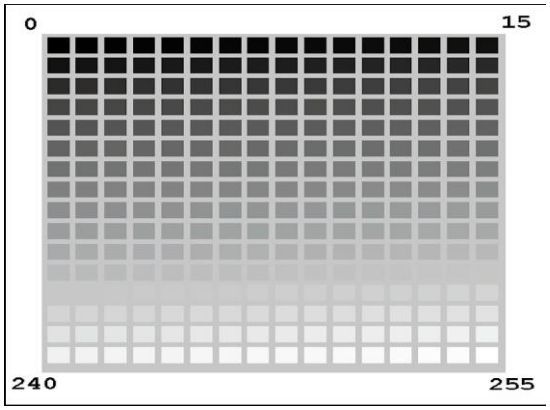
dengan tipe bebas (dapat berupa file gambar, dokumen, text, media dan sebagainya) yang hendak disembunyikan ke dalam citra digital, dengan menggabungkan kedua file tersebut dan memproses dengan suatu algoritma maka akan terbentuk suatu file citra digital yang disebut *Stego Image* sebagai pembawa pesan (*carrier*), selanjutnya pada proses pengiriman data, file *stego image* yang akan dikirimkan, sehingga data secara aman telah tersembunyi di dalam citra. Pada metode s*teganography* tidak diperkenankan menggunakan format citra digital yang termasuk dalam kategori *lossy* (misal : JPEG, 8-bit BMP, dan sebagainya) namun format yang dipakai harus merupakan *losslessimage format* (misal : 24-bit BMP, 32-bit BMP) karena diperlukan suatu media pembawa yang dapat menyimpan bit-bit data tanpa menghilangkan suatu bagian dari bit-bit data tersebut. Contoh metode penyembunyian data dapat dilihat pada gambar 2.



Gambar 2. Penyembunyian data dengan metode *Steganography*

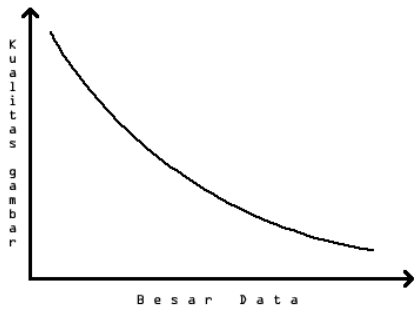
Garis besar dari proses penyembunyian data dengan metode *steganography*adalah terdapat suatu *cover image* dan sebuah *hidden message* yang mengandung suatu data yang akan dikirimkan tanpa ingin diketahui oleh pihak lain [6]. Dengan menggunakan suatu *secret key* maka dilakukan suatu proses penggabungan antara data dengan *cover image* yang akan menghasilkan suatu *stego image* yang siap untuk dikirimkan.

Metode *Steganography* dapat menyembunyikan informasi dengan menggunakan berbagai cara pada citra digital, antara lain dengan *masking and filtering*, *LSB* serta penggunaan algoritma-algoritma citra digital, pada *masking and filtering* dilakukan penyembunyian dengan cara yang hampir sama dengan proses *watermark* pada kertas biasa yaitu dengan mengurangi atau menambah tingkat kecerahan pada area tertentu, namun hal ini jarang digunakan dan dirasa kurang fleksibel karena membatasi jenis data yang akan disembunyikan [4]. Selain itu proses ini hanya dilakukan pada objek *greyscale* dimana hanya terdapat 8 bit data yang memiliki nilai warna 0 hingga 255. Gambar tabel tingkat intensitas dapat dilihat gambar 3.



Gambar 3. Tabel tingkat intensitas warna 8 bit

Cara yang paling umum digunakan pada *steganography* adalah dengan menggunakan LSB *(least significant bit insertion)* yaitu mengganti deretan bit-bit belakang pada pixel gambar dengan deretan bit-bit data [5].Dengan melakukan penggantian pada bit-bit belakang pada warna citra, maka perubahan tingkat intensitas warna tidak dapat terdeteksi oleh mata manusia. Semakin besar bit data yang dimasukan berpengaruh pada semakin besarnya perubahan tingkat intensitas warna pada citra. Penyembunyian data dengan metode *steganography* juga dapat dilakukan dengan menggunakan algoritma pengolahan citra digital lainnya dengan syarat di dalam prosesnya tidak menghilangkan bit-bit data *(lossless)*.Setiap metode memiliki tingkat keberhasilan berbeda yang diukur berdasarkan efisiensi penyimpanan data serta kualitas *stego image* yang dihasilkan. Besar data dan kualitas gambar berbanding terbalik dalam arti semakin besar data yang tersimpan[2], maka kualitas *stego image* yang dihasilkan semakin menurun, hal ini digambarkan pada grafik gambar 4.



Gambar 4. Grafik perbandingan kualitas gambar serta besar data yang disimpan

Untuk mengembalikan data ke dalam bentuk semula maka dilakukan proses pembandingan antara *cover image* dan *stego image* dengan menggunakan suatu *secret key*. Proses pengembalian data secara garis besar hampir sama dengan proses penyembunyian data namun menggunakan urutan proses yang berbeda dimana proses dilakukan secara terbalik.

2.2 Digital Image Processing

Image processing adalah suatu metode yang digunakan untuk memproses atau memanipulasi citra digital dalam bentuk 2 dimensi [1].*Image processing* dapat juga dikatakan segala operasi untuk memperbaiki, menganalisa, atau mengubah suatu citra digital.Konsep dasar pemrosesan suatu objek pada citra digital menggunakan *image processing* diambil dari kemampuan indera penglihatan manusia yang selanjutnya dihubungkan dengan kemampuan otak manusia.

Dalam sejarahnya, *image processing* telah diaplikasikan dalam berbagai bentuk, dengan tingkat kesuksesan cukup besar.Seperti berbagai cabang ilmu lainnya, *image*

processing menyangkut pula berbagai gabungan cabang-cabang ilmu, diantaranya adalah optik, elektronik, matematika, fotografi, dan teknologi komputer.

2.2.1.File Bitmap

Secara umum sebuah citra digital dapat diwakili oleh format warna RGB (*Red-Green-Blue*) untuk setiap titiknya, di mana setiap komponen warna memiliki batasan sebesar 1 *byte*.Jadi untuk masing-masing komponen R, G, dan B mempunyai variasi dari 0 sampai 255 [4]. Total variasi yang dapat dihasilkan untuk sistem dengan format warna RGB adalah 256 x 256 x 256 atau 16.777.216 jenis warna. Karena setiap komponen warna memiliki batasan sebesar 1 *byte* atau 8 *bit*, maka total untuk mempresentasikan warna RGB adalah 8+8+8 = 24 *bit.*

Pada format file bitmap dapat terdiri dari 1, 4, 8, 24, dan 32 bit warna untuk setiap *pixel*-nya. Pada format file bitmat 32 bit, selain menyimpan format warna RGB (*Red-Green-Blue*), juga terdapat 1 byte yang disebut *Alpha* yang menyimpan intensitas warna dari *pixel.*

2.3. LSB *(Least Significant Bit)*

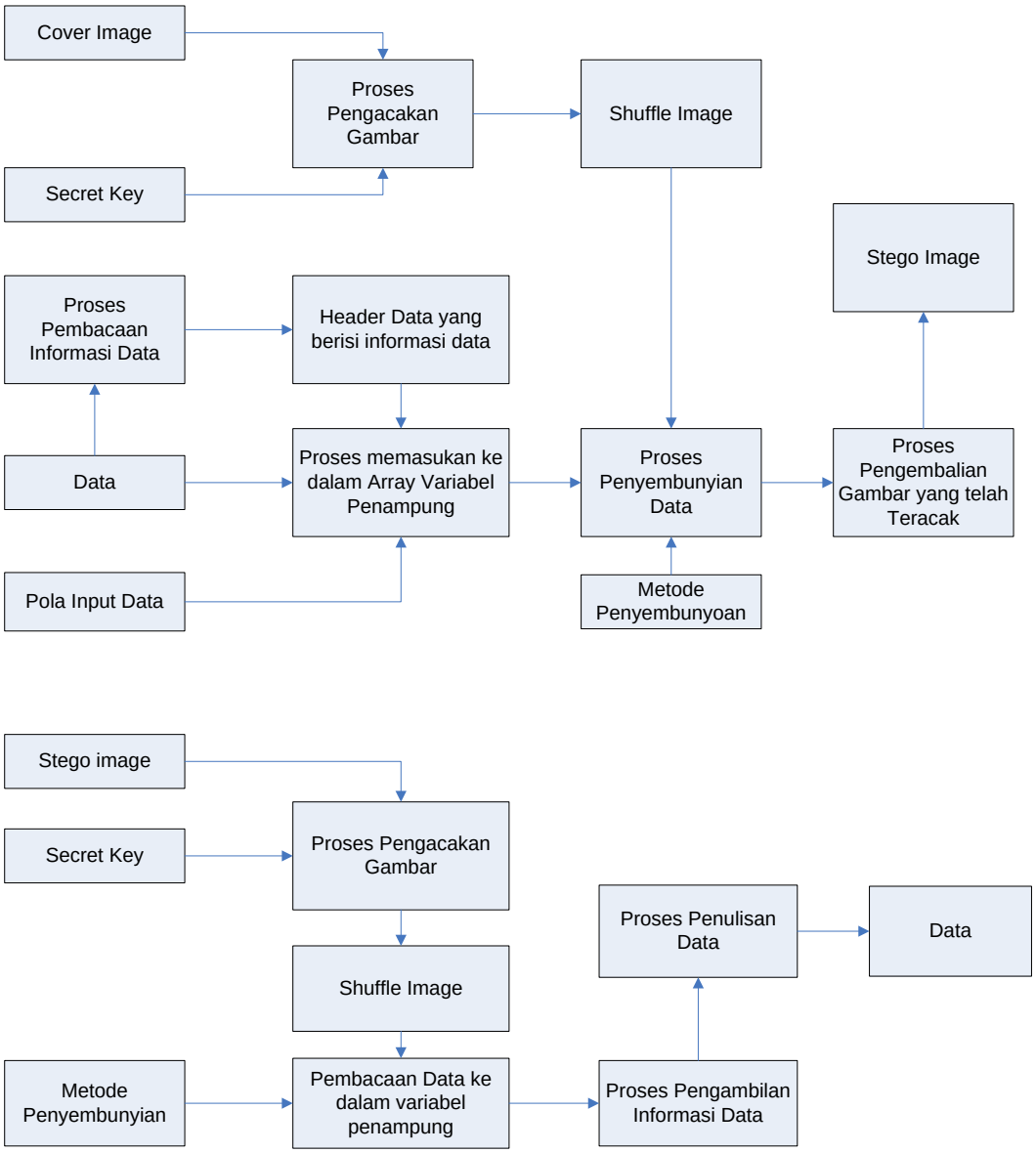
LSB *(Least Significant Bit)* merupakan salah satu metode dalam *steganography*. LSB dilakukan dengan mengambil bit – bit terakhir warna pada citra dan menggantinya dengan bit – bit data. Banyak cara yang dapat dilakukan untuk mengganti bit – bit warna pada citra, antara lain dengan melakukan operasi penambahan atau pengurangan nilai warna pada citra, atau juga dengan cara melakukan operasi AND dan OR antara bit – bit warna dengan bit – bit data. 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 seakan – akan perubahannya tidak dapat dideteksi oleh mata manusia.

3. Metode Penelitian

Gambaran proses secara umum terdiri dari beberapa tahapan yaitu :

- Proses untuk pengacakan gambar dari satu cover image, sehingga akan menghasilkan *shuffle image.*
- Secara bersamaan dilakukan proses pembacaan data dokumen yang akan dimasukkan ke dalam citra digital beserta pola input datanya.
- Melakukan proses penyembunyian data menggunakan metode tertentu.
- Mendapatkan kembali gambar yang sudah diacak pada proses sebelumnya sehingga pada hasil akhir didapatkan stego image.

Sedangkan untuk proses pembacaan data dokumen yang berasal dari suatu stego image didapatkan dengan cara membalik proses seperti yang ada di atas. Untuk lebih jelasnya proses dapat dilihat pada gambar 5.



Gambar 5. Blok Diagram Proses *Steganography*

4. Hasil dan Pembahasan

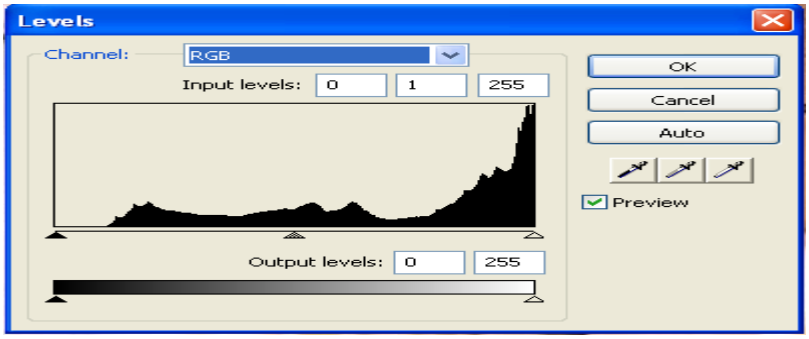
Pengujian yang dilakukan adalah menyembunyikan file dokumen ke dalam file gambar. Proses yang dilakukan adalah dengan melakukan pengacakan pada gambar asli untuk selanjutnya memasukkan data dokumen ke dalam file gambar dengan menggunakan metode LSB. File gambar asli dapat dilihat pada gambar 6, Proses pengacakan gambar dapat dilihat pada gambar 7, serta Hasil dari proses steganografi dapat dilihat pada gambar 8.

Gambar 6. Citra Digital Asli

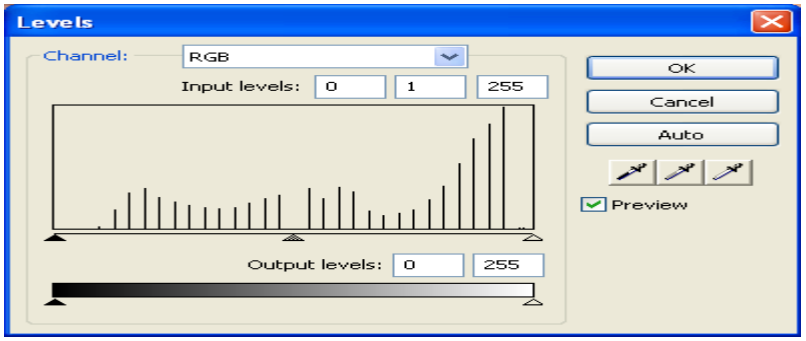
Gambar 7. Pengacakan Citra Digital

Gambar 8. Citra Digital Hasil Steganografi

Untuk mengetahui penurunan kualitas pada citra digital akan digunakan histogram yang tersedia pada aplikasi pengolahan gambar *Macromedia Firework MX 2004.*Hasil histogram dari citra digital pada gambar 9 dan 10.



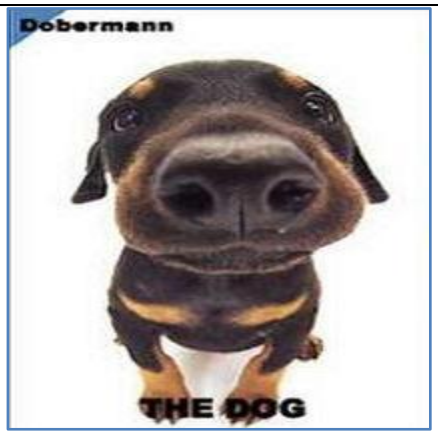
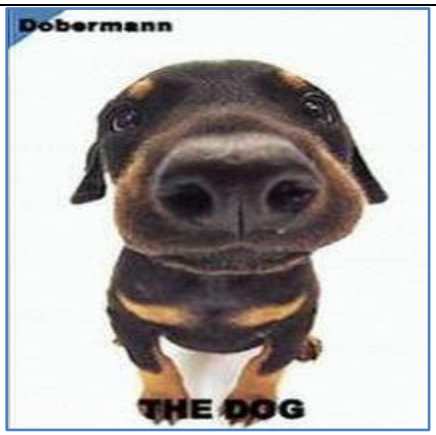
Gambar 9. Histogram Citra Digital Asli



Gambar 10. Citra Digital hasil Stego Image

Dengan melihat pada hasil histogram, hasil stego image dengan menggunakan metode LSB nampak terputus-putusm hal ini disebabkan oleh proses pemotongan 3 bit paling akhir untuk setiap titik warna yang diganti dengan bit data.

Pengujian selanjutnya dilakukan dengan menggunakan data berukuran besar yang akan disembunyikan ke dalam beberapa citra digital. Data yang digunakan di dalam pengujian adalah *file* yang telah dilakukan proses kompresi dengan format *zip*, besar data adalah 458752 *bytes*. Hasil dari Stego image disimpan ke dalam 4 file seperti yang terlihat pada gambar 11.

	
Cover Image ke-1 (210 x 300)	*Stego Image* ke-1 (210 x 300)
	
Cover Image ke-2 (221 x 319)	*Stego Image* ke-2 (221 x 319)
	
Cover Image ke-3 (419 x 404)	*Stego Image* ke-3 (419 x 404)

	
Cover Image ke-4 (800 x 600)	*Stego Image* ke-4 (800 x 600)

Gambar 11. Hasil Stego Image ke dalam beberapa citra digital.

5. Kesimpulan

Berdasarkan hasil pengujian tersebut, maka didapatkan kesimpulan bahwa daya tampung citra digital untuk menampung file sebesar 30% dan semakin banyak warna pada citra digital dapat menampung lebih banyak file. Sehingga untuk pengujian yang lebih optimal sebaiknya menggunakan citra digital dengan semakin banyak ragam warna. Mengacu kepada data histogram dapat terlihat penurunan kualitas citra digital relatif kecil..

Referensi

[1] Abednego, Luciana. dan Nico Saputro. 2004. Implementasi Teknik Feature Morphing Pada Citra Dua Dimensi.

[2] Guillermito. 2004. Steganography: A few tools to discover hidden data.

[3] Johnson., Neil F., and Sushi Jajodia. 1998. Exploring Steganography : Seeing The Unseen.

[4] Kay, David C., John R. Levine.1992, Graphics File Formats, First Edition, United States of America.

[5] Kharrazi, Mehdi., Husrev T. Sencar, and Nasir Memon. 2004. Image Steganography: Concepts and Practice.

[6] Provos, Niels., and Peter Honeyman. 2003. Hide and Seek : Introduction to Steganography.