INTISARI

Steganografi merupakan teknik untuk mengamankan pesan rahasia yang dilakukan dengan cara menyembunyikan pesan di dalam pesan lainnya tanpa mengubah bentuk pesan yang ditumpanginya. Steganografi dapat digunakan pada citra. Citra yang dihasilkan setelah proses steganografi tidak berbeda dengan citra aslinya.

Metode yang digunakan untuk aplikasi steganografi citra ini adalah *Discrete Cosine Transformation* (DCT). Citra yang terdiri dari piksel berbasis ruang ditransformasikan ke dalam basis frekuensi sehingga diperoleh koefisien DCT untuk setiap blok matriks 8x8. Nilai setiap blok 8x8 koefisien DCT dilakukan kuantisasi. Nilai kuantisasi yang dihasilkan digunakan untuk menyembunyikan bit pesan dengan menggunakan metode JSteg. Pesan rahasia diubah ke dalam bilangan 8 bit. LSB (*Least Significant Bit*) nilai kuantisasi yang tidak 0, tidak 1, dan tidak negatif selanjutnya diganti dengan satu bit pesan. Penggantian bit pesan dilakukan secara berurutan mulai dari MSB (*Most Significant Bit*) sampai dengan LSB.

Untuk menguji penerapan metode DCT pada steganografi citra, maka dibuat sebuah program aplikasi. Program aplikasi steganografi citra dengan metode DCT ini digunakan untuk menyembunyikan pesan rahasia dalam bentuk *file text document* atau *file* txt ke dalam citra JPG atau JPEG. Program aplikasi ini juga digunakan untuk mengekstraksi pesan yang disembunyikan di dalam citra JPEG. Pengujian dilakukan pada empat puluh citra bertipe JPEG dan dua puluh pesan bertipe txt. Hasil pengujian menunjukkan bahwa waktu yang dibutuhkan untuk proses penyembunyian dan ekstraksi pesan tergantung dari ukuran citra yang digunakan dan banyaknya pesan yang disembunyikan, serta citra berwarna abu-abu dapat digunakan untuk menyembunyikan karakter pesan lebih banyak daripada citra berwarna. Selain itu, hasil pengujian menunjukkan bahwa program aplikasi steganografi citra yang dibuat memenuhi kriteria *fidelity* dan *recovery* tetapi tidak tahan atau tidak *robust* terhadap operasi manipulasi citra.

ABSTRACT

Steganography was a technique to protect secret messages by hiding the protect messages within another message without change the form of those message. Steganography can be applied into the image. The result image after steganography process is not different with this original image.

The method used in this image steganography application was discrete Cosine Transformation (DCT). The image consist of space-based pixel that transformed into frequency-based, hence the DCT coefficient was derived for each 8x8-matrix block. The value of each 8x8 block of DCT coefficient was noted with quantization. The resulted quantization values used to hide the message bit using JSteg method. The secret messages convert into eight bit numbers. LSB's (Least Significant Bit) quantization value which not equal to 0, not equal to 1 and not equal to negative was then transformed into one bit message. The one bit message transformation performed in sequence from MSB (Most Significant Bit) to LSB (Least Significant Bit).

To testing the apply of the DCT method in the image steganography, then was made an application program. This application of image steganography program using DCT method was used to hide the secret messages in the form of file text document or file txt into JPG Image or JPEG Image. This application also used to extract the hidden message into JPEG Image. The tested was done into the fourty images in the JPEG format and twenty messages in the txt format. The created image steganography was tested to knowing the ability of the system. Results of the test suggesting that the duration required for hiding process and messages extraction were depend on the size of image that used and depend on the total messages hidden in the image, and moreover, the colour gray image can be used to hide the more message character than other colour images. In addition, result of the test demonstrating that created image steganography complies with fidelity and recovery criteria, however, it was weak or not robust to image manipulation operation.