

Implementasi Steganografi Menggunakan Variasi Metode DCT (*Discrete Cosine Transform*) Pada Data Citra

Nurmeishy Febriani 14116127

Pembimbing 1 : Angga Wijaya, S.Si., M.Si.

Pembimbing 2 : Ahmad Luky Ramdani, S.Komp., M.Kom.

ABSTRAK

Berkembangnya teknologi telah banyak mempengaruhi proses pengiriman informasi secara digital. Salah satunya sangat berisiko pada keamanan informasi dan data yang dikirim. Ada beberapa cara mengamankan data atau pesan, salah satunya dengan menggunakan teknik penyembunyian data (steganografi). Pada penelitian ini penulis membuat sebuah sistem pengamanan data menggunakan Matlab. Sistem ini menggunakan algoritma *Discrete Cosine Transform* (DCT). Pada penelitian ini pesan yang digunakan berformat txt, lalu pesan disimpan ke dalam sebuah citra gambar berformat BMP, JPG, PNG dan TIF sehingga tidak diketahui lagi keberadaannya. Didapatkan nilai *Peak Signal to Noise Ratio* (PSNR) tertinggi sebesar 54.414 dB dengan nilai *Mean Square Error* (MSE) terkecil 0.23532, dan nilai rata-rata *Mean Opinion Score* (MOS) terbesar 4.2. Untuk pengujian dilakukan beberapa serangan pada *stego image* antara lain *brightness* +30, +50, +70, +90, +110, +130, +150 dan *resize* 94%, 87% dan 77%.

Kata kunci: Steganografi, Citra, Discrete Cosine Transform, Peak Signal to Noise Ratio, Mean Opinion Score.

Steganography Implementation Uses Variations of the DCT (*Discrete Cosine Transforms*) Method on Image Data

Nurmeishy Febriani 14116127

Advisor 1: Angga Wijaya, S.Si., M.Si.

Advisor 2 : Ahmad Luky Ramdani, S.Komp., M.Kom

ABSTRACT

The development of technology has greatly influenced the process of sending information digitally. One of them is very risky to the security of the information and data sent. There are several ways to secure data or messages, one of which is by using data hiding techniques (steganography). In this study, the authors created a data security system using Matlab. This system uses the Discrete Cosine Transform (DCT) algorithm. In this study, the messages used were in txt format, then the message were saved into an image with BMP, JPG, PNG and TIF formats so that their whereabouts were no longer known. Obtained the highest Peak Signal to Noise Ratio (PSNR) value of 54,414 dB with the smallest Mean Square Error (MSE) value of 0.23532, and the largest average *Mean Opinion Score* (MOS) value of 4.2. For testing, several attacks were carried out on the stego image, including brightness +30, +50, +70, +90, +110, +130, +150 and resize to 94%, 87% and 77%.

Keywords: Steganography, Image, Discrete Cosine Transform, Peak Signal to Noise Ratio, Mean Opinion Score.