ABSTRAK

ANALISIS DAN PENGEMBANGAN METODE PADA TEKNIK STEGANOGRAFI UNTUK MENGATASI PERMASALAHAN MANIPULASI *ROBUSTNESS*

Oleh

DEDI DARWIS

Pemanfaatan steganografi saat ini telah banyak diterapkan pada pertukaran data melalui internet, pesan singkat, media sosial serta penyembunyian data di dalam *personal computer (PC). Robustness* merupakan hal yang penting pada keamanan steganografi. Pada umumnya, citra yang disisipi pesan tidak memiliki ketahanan terhadap serangan, sehingga pesan akan rusak ketika dilakukan ekstraksi setelah manipulasi *robustness* diterapkan. Beberapa jenis dari serangan *robustness* adalah manipulasi *cropping, rotate, resize*, dan pemberian efek warna pada gambar. Hal ini akan menjadi masalah terhadap keamanan Steganografi gambar karena *stego-image* yang dilakukan manipulasi akan mengalami kerusakan pada pesan rahasia ketika dilakukan proses ekstraksi karena piksel pada *stego-image* mengalami perubahan nilai.

Pada penelitian ini dikembangkan pendekatan baru untuk mengatasi permasalahan *robustness* dengan mengembangkan metode *LSB*, pemanfaatan domain spasial, *exif metadata image* dan kriptografi *fernet*. Penelitian ini menghasilkan tiga pendekatan baru dalam hal mengatasi permasalahan *robustness* namun tetap memperhatikan kualitas citra hasil steganografi. Metode yang dikembangkan diberi nama : *Center Sequential Technique (CST), Center Embedded Pixel Positioning (CEPP)* dan *Steganography on Image Metadata (SIM)*.

Berdasarkan hasil uji yang dilakukan, metode *CST, CEPP* dan *SIM* dapat mengatasi manipulasi *cropping* lebih dari 50% secara simetri dan asimetri. Namun, metode *CST* dan *CEPP* tidak dapat menahan operasi untuk *rotate, resize* dan pemberian efek warna pada gambar. Sedangkan untuk operasi *rotate, resize* dan pemberian efek warna pada gambar hanya dapat ditangani oleh metode SIM. Berdasarkan pengujian yang dilakukan, metode *CST* dapat menghasilkan rata-rata nilai *PSNR* sebesar 51,14776 db, dan pada metode *CEPP* menghasilkan rata-rata nilai *PSNR* 51,96582 db, sedangkan untuk metode *SIM*, nilai *PSNR* mencapai 100 db. Hal ini membuktikan bahwa metode yang dikembangkan terutama pada metode *SIM* dapat menghasilkan kualitas citra *stego image* yang baik berdasarkan perhitungan nilai *PSNR*.

Kata Kunci : *Center Embedded Pixel Positioning, Center Sequential Technique, Fidelity, LSB, Steganography on Image Metadata, Robustness*

ABSTRACT

ANALYSIS AND DEVELOPMENT OF METHODS IN STEGANOGRAPHIC TECHNIQUES TO OVERCOME ROBUSTNESS MANIPULATION PROBLEMS

By

DEDI DARWIS

The use of steganography has now been widely applied to data exchange via the internet, short messages, social media and data hiding in personal computers (PCs). Robustness is important in steganographic security. In general, image which is embedded with the message have not resistance to attack, so the message will be damaged when it was extracted after robustness manipulation. Several types of robustness attacks are cropping, rotating, resizing, and applying color effects to the images. This will be a problem for the security of image Steganography because the Stego image that is manipulated will experience damage to the secret message when the extraction process is carried out because the pixels on the Stego image change in value.

In this study, a new approach was developed to overcome the robustness problem by developing the LSB method, utilizing spatial domains, exif metadata images and fernet cryptography. This study proposed three new approaches in terms of overcoming the problem of robustness, but still retain the quality of the steganographic image. The methods developed were named: Center Sequential Technique (CST), Center Embedded Pixel Positioning (CEPP) and Steganography on Image Metadata (SIM).

Based on the results of tests carried out by the CST, CEPP and SIM those methods can overcome the cropping manipulation for more than 50% symmetrically and asymmetrically. However, the CST and CEPP methods cannot withstand manipulations to rotate, resize and apply color effects to images. Meanwhile, the manipulation of rotate, resize and color effects on the image can only be handled by the SMI method. Based on the tests carried out, the CST method can produce an average PSNR value of 51,14776 db and the CEPP method produces an average PSNR value of 51,96582 db, and for the SIM method, the PSNR value reaches 100 db. This proves that the method developed especially on the SIM method can produce a good stego image quality based on the calculation of the PSNR value.

Keywords: *Center Embedded Pixel Positioning, Center Sequential Technique, Fidelity, LSB, Steganography on Image Metadata, Robustness*