IMPLEMENTASI STEGANOGRAFI *PIXEL INDICATOR TECHNIQUE* (PIT) DAN KRIPTOGRAFI ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) PADA CITRA GAMBAR

YUGO ALFATTAH

11051100599

Jurusan Teknik Informatika

Fakultas Sains dan Teknologi

Universitas Islam Negeri Sultan Syarif Kasim Riau

ABSTRAK

Masalah keamanan informasi pada saat ini adalah hal yang sangat diperhatikan untuk menghindari terjadinya pencurian data, pembobolan sistem, atau penyadapan. Pada penelitian sebelumnya terdapat beberapa kelemahan, pertama, pesan asli disisipkan langsung ke dalam gambar tanpa dienkripsi terlebih dahulu. Kedua, semua pesan *stego image* dengan format JPG rusak saat diekstraksi. Oleh karena itu, pada penelitian ini dilakukan kombinasi antara steganografi PIT dan kriptografi AES. Dari pengujian yang telah dilakukan, pada aspek kapasitas, format PNG mengalami penambahan ukuran file paling sedikit antara 50-100 KB, format JPG bertambah antara 300-500 KB, sedangkan format BMP mengalami pengurangan ukuran rata-rata 100 KB. Semua *stego image* tidak tahan pada manipulasi *cropping* di sisi atas, kiri, dan kanan. Pada manipulasi *cropping* di sisi bawah, hanya *stego image* dengan pesan berukuran 157 KB yang mengalami kerusakan. *Stego image* yang mengandung pesan 15 *bytes* dan 13 KB saja yang berhasil di-*retrieve* dan didekripsi menjadi pesan asli kembali. Pada aspek keamanan dengan menggunakan *tools* steganalysis, 3 *stego image* dari format PNG terdeteksi adanya pesan rahasia, 1 *stego image* terdeteksi dari format JPG, dan 1 *stego image* terdeteksi dari format BMP. Kanal *Red* dan *Blue* menjadi kanal terbaik dalam penyisipan, karena tidak mengalami banyak perubahan dibandingkan kanal *Green*.

Kata Kunci: ***Advanced Encryption Standard*, BMP, JPG, Kriptografi, *Pixel Indicator Technique*, PNG, Steganografi**

IMPLEMENTATION OF PIXEL INDICATOR TECHNIQUE (PIT) STEGANOGRAPHY AND ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM'S CRYPTOGRAPHY ON PICTURE IMAGES

YUGO ALFATTAH

11051100599

Informatics Engineering Department

Faculty of Science and Technology

Islamic State University of Sultan Syarif Kasim Riau

ABSTRACT

Today, information security issue is the most concern thing to prevent data stealing, system breaking, or tapping. There are some lack in the previous research, first, original message was embedded straight to carrier image without encryption. Second, all original message that embedded into JPG file format was damaged. Therefore, in this research is done combination between PIT steganography and AES cryptography. Based on the result, on the capacity aspect test, PNG experienced least increasing file size around 50 to 100 KB, JPG experienced most increasing file size around 300 to 500 KB, and BMP experienced decreasing file size around 100 KB. All of stego images can't hold on cropping manipulation from top side, left side, and right side of the image. When it comes to crop on bottom side, only images contained message of 157 KB that have damaged. Only stego images that contained message of 15 bytes and 13 KB survive retrieving and decrypting to plaintext. From the security aspect test using steganalysis tools, there are 3 stego images of PNG detected secret message in them, and 1 stego image of JPG and 1 stego image of BMP. Red channel and Blue channel is the best channel to embedding hidden message because there is not much changing on them, comparing with Green channel.

Keyword: **Advanced Encryption Standard, BMP, Cryptography, JPG, Pixel Indicator Technique, PNG, Steganography**