ABSTRAK

IMPLEMENTASI PENGAMANAN *TEXT FILE* PADA *HYBRID SYSTEM* MENGGUNAKAN ALGORITMA *VIGENÈRE* DAN ALGORITMA *ADAPTIVE MINIMUM ERROR LEAST SIGNIFICANT BIT REPLACEMENT(*AMELSBR*)*

Oleh

Tryo Romadhoni Pujakusuma

Perkembangan teknologi jaringan dan internet memungkinkan setiap orang untuk saling bertukar data dan informasi. Masalah yang muncul ketika informasi tersebut bersifat rahasia, terutama bagi suatu perusahaan, institusi dan juga individu yang mempunyai dokumen dan data yang penting, sehingga perlu dijaga keamanan dari data tersebut. Keamanan merupakan hal yang terpenting dalam pengiriman suatu pesan rahasia. Dalam hal ini kriptografi yang berperan menyandikan pesan rahasia kedalam bentuk pesan yang tidak beraturan dan steganografi yang menyembunyikan pesan tidak beraturan tersebut ke dalam media gambar, sehingga menghasilkan keamanan ganda dalam pengiriman pesan rahasia. Dalam penelitian ini peneliti membangun sistem hibrid kriptografi dan steganografi menggunakan *Vigenere* dan AMELSBR berbasis *web* dengan media penampung berupa gambar dengan *format file* (.jpg) sebagai *input (cover),* gambar dengan jenis file (.png) sebagai *output (stegoimage)* serta data yang dapat disisipkan berupa berkas dengan *format file* (.txt). Kesimpulan yang didapat dari penelitian ini adalah Sistem *hybrid* dengan menggabungkan algoritma *Vigenere* dan metode AMELSBR ini dapat digunakan dengan baik untuk menyandikan pesan rahasia serta menyembunyikannya ke dalam media penampung gambar sehingga memperoleh keamanan ganda dalam pengiriman data. Tidak terlihat perbedaan yang signifikan antara *stegoimage* dengan gambar aslinya setelah dilakukan penyisipan. Oleh sebab itu penggunaan metode AMELSBR baik digunakan dalam steganografi. *Stegoimage* dapat tahan terhadap proses manipulasi *brightness* dan *contrast* dengan catatan gambar harus mempunyai nilai warna dominan hitam (rgb(0,0,0)) atau putih (rgb(255,255,255)) dan tidak banyak varian warna, dengan kata lain gambar yang dapat mengembalikan berkas tanpa mengalami pengurangan makna secara berlebihan setelah dilakukannya manipulasi *brightness* dan *contrast* adalah gambar dengan kualitas citra *biner* dan citra *grayscale*.

Kata Kunci: *hybrid*, kriptografi, steganografi, Vigenere, AMELSBR.

ABSTRACT

IMPLEMENTATION OF TEXT FILE SECURITY ON HYBRID SYSTEM USING VIGENÈRE ALGORITHM AND AMELSBR (ADAPTIVE MINIMUM ERROR LEAST SIGNIFICANT BIT REPLACEMENT) ALGORITHM

By

Tryo Romadhoni Pujakusuma

The development of technology and the internet allows everyone to exchange data and information. Problems arise when the information is confidential, especially for a company, institution and also individuals who have important documents and data. Therefore, the security of the data is a must. In this case cryptography plays a role of encrypting secret messages into the form of unreadable messages and steganography that hides the irregular messages into the image media, resulting in double security in the delivery of secret messages. In this research we develop a hybrid system using Vigenere and AMELSBR with cover media in the form of (.jpg) format as input (cover), file type (.png) as output (stegoimage) and data be inserted as a file with text format. The conclusion of this research is that the hybrid system can be used to encrypt the secret message and hide it into the cover media to make it more secure in data transmission. Therefore, the use of AMELSBR method is good used in steganography. Stegoimage can withstand the process of manipulating the brightness and contrast with the image record must have the dominant black color value (rgb (0,0,0)) or white (rgb (255,255,255)) and not many color variants, in other words the image can restore the file without experiencing excessive reduction of meaning after the manipulation of brightness and contrast is an image with binary image quality and grayscale image.

Key word: Hybrid, Cryptography, Steganography, Vigenere, AMELSBR.