

KEAMANAN PESAN MENGGUNAKAN KOMBINASI KRIPTOGRAFI HILL CIPHER DAN LEAST SIGNIFICANT BIT PADA CITRA DIGITAL

MUHAMMAD HUSNUL ARIF

*Program Studi Teknik Informatika - S1, Fakultas Ilmu
Komputer, Universitas Dian Nuswantoro Semarang*

URL : <http://dinus.ac.id/>

Email : 111201106357@mhs.dinus.ac.id

ABSTRAK

Pertukaran informasi melalui dunia maya memiliki berbagai manfaat sebagai contoh estimasi waktu yang cepat, jarak fisik dan batas ruang tidak terbatas dan lain sebagainya. Namun dalam kegiatan tersebut juga dapat menimbulkan resiko keamanan dalam informasi yang bersifat rahasia. Untuk itu diperlukan pengaman yang dapat digunakan untuk melindungi data yang ditransmisikan melalui jaringan internet. Algoritma penyandian yang digunakan dengan menyandikan pesan yang akan dikirim (plaintext) tersebut menjadi pesan yang sudah teracak (ciphertext) adalah algoritma kriptografi dan steganografi. Dalam penerapannya teknik kriptografi yang akan digunakan adalah Hill Cipher. Teknik tersebut dikombinasikan dengan steganografi dengan teknik Least Significant Bit. Hasil yang didapat dari penggabungan teknik dapat menjaga kerahasiaan pesan karena orang yang tidak mengetahui kunci rahasia yang digunakan akan kesulitan untuk mendapatkan pesan yang terdapat pada stego-image ditambah lagi gambar yang sudah pernah disisipi tidak dapat digunakan sebagai cover image. Pesan berhasil disisipkan dan diekstraksi kembali pada semua sample citra baik dengan format *bmp , *png , *jpg pada resolusi 512 x 512 piksel, 256 x 256 piksel. Hasil MSE dan PSNR tidak dipengaruhi format file ataupun ukuran file. Akan tetapi, dipengaruhi pada dimensi citra. Semakin besar dimensi citra, maka MSE semakin kecil artinya kerusakan citra semakin kecil. Sedangkan nilai PSNR-nya semakin besar.

Kata Kunci : Keamanan, Kriptografi, Steganografi, HillCipher, Least Significant Bit

MESSAGE SECURITY USING COMBINATION OF HILL CIPHER CRYPTHOGRAPHY AND LEAST SIGNIFICANT BIT ON DIGITAL IMAGE

MUHAMMAD HUSNUL ARIF

*Program Studi Teknik Informatika - S1, Fakultas Ilmu
Komputer, Universitas Dian Nuswantoro Semarang*

URL : <http://dinus.ac.id/>

Email : 111201106357@mhs.dinus.ac.id

ABSTRACT

Exchange of information through cyberspace has many benefits as an example estimated time fast, unlimited physical distance and space limits, etc. But in these activities can also pose a security risk for confidential information . It is necessary for the safety that can be used to protect data transmitted through the Internet . Encryption algorithm that used to encrypt message to be sent (plaintext) into messages that have been randomized (ciphertext) is cryptography and steganography algorithms . In application of cryptographic techniques that will be used is Hill Cipher. The technique is combined with steganography techniques Least Significant Bit. The result of merging techniques can maintain the confidentiality of messages because people who do not know the secret key used will be difficult to get the message contained in the stego-image and the image that has been inserted can not be used as a cover image. Message successfully inserted and extracted back on all samples with a good image formats * .bmp , * .png , * .jpg at a resolution of 512 x 512 pixels , 256 x 256 pixels. MSE and PSNR results are not influenced file format or file size. However, influenced by dimensions of image. The larger dimensions of the image , then the smaller MSE means to damage the image gets smaller. While PSNR its value increases.

Keyword : Security, Cryptography, Steganography, HillCipher, Least Significant Bit