

ABSTRACT

Currently, security of data especially on the image file is a very important thing to be kept confidential. This has to do with copyright. For that developed a method that aims to randomize the image file, so it can not be manipulated and falsified by others unauthorized persons.

Encryption Data Algorithm Standard (DES), an encryption algorithm with a symmetric key, one of the cryptography method introduced by WL Tuchman in 1972 at the IBM lab. DES algorithm, processed at 64 bit plain. DES algorithm using external keys up to 8 characters or 64 bits. The external keys are processed to produce 16 pieces of internal key with each key length 48 bits. The internal lock is a part in the process of encryption and decryption. In addition the DES algorithm also uses the s-box predefined eight pieces, which will be used in the Feistel system. DES algorithm is quite good with the loop 16 times on the stages of encryption and decryption. This makes plain file encryption function optimally. DES Algorithm felt able to be applied to the cryptographic process in image files, especially bitmap image file formats.

From testing research on the application of the DES algorithm on the bitmap file obtained some results. First, the greater the capacity of the processed bitmap file, the longer it takes. Because, the larger the file size, then the process pengacakan of the contents of the file will also be longer. Second, the keys used in the encryption and decryption must be the same or symmetry. Third, the capacity of the file before and after the change are not encrypted.

Keywords: Cryptography, DES algorithm, the image bitmap format