# KOMBINASI ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) DAN METODE PERTUKARAN KUNCI DIFFIE-HELLMAN PADA PENGAMANAN CITRA DIGITAL MEDIS

**Yugo Bayu Prastyo**

## ABSTRAK

Data rekam medis merupakan data sensitif yang perlu dijaga tingkat keamanan dan kerahasiaannya. Salah satu bentuk data rekam medis adalah citra medis. Di dalam citra medis terdapat berbagai informasi pribadi mengenai pasien. Dalam melakukan pertukaran informasi citra medis, sering kali data citra tersebut mengalami kebocoran sehingga pihak yang tidak berwenang dapat mengetahui isi citra tersebut. Penelitian ini bertujuan untuk mengembangkan suatu pengamanan citra digital medis yang menggunakan kombinasi algoritma AES pada proses enkripsi-dekripsi data dan algoritma Diffie-Hellman pada proses pertukaran kunci untuk menjaga keamanan dan kerahasiaan citra medis. Algoritma AES digunakan pada proses enkripsi dan dekripsi citra, sedangkan algoritma Diffie-Hellman digunakan untuk mengamankan kunci dari algoritma AES tersebut. Dari hasil penelitian ini, di dapatkan hasil bahwa kombinasi algoritma AES dan Diffie-Hellman berhasil mengamankan citra medis. Algoritma Diffie-Hellman akan menghasilkan kunci yang berbeda – beda yang selanjutnya digunakan sebagai kunci AES. Sedangkan algoritma AES mampu mengenkripsi dan mendekripsi citra medis tanpa merubah isi dari citra tersebut.

**Kata kunci:** Kriptografi, Citra Medis, Algoritma *Advanced Encryption Standard* (AES), Algoritma Diffie-Hellman, Enkripsi, Dekripsi

***COMBINATION OF ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM AND DIFFIE-HELLMAN KEY EXCHANGE METHODS ON MEDICAL DIGITAL IMAGE PACIFIER***

**Yugo Bayu Prastyo**

## *ABSTRACT*

*The medical record data is sensitive data that needs to be maintained at the level of security and confidentiality. One of medical record data is a medical image. In the medical image there are various personal information about the patient. In exchanging medical image information, often the image data is leaked so that unauthorized parties can find out the contents of the image. This study aims to develop a medical digital image security that uses a combination of AES algorithms in the process of data encryption and decryption and the Diffie-Hellman algorithm in key exchange processes to maintain the security and confidentiality of medical images. The AES algorithm is used in the process of image encryption and decryption, while the Diffie-Hellman algorithm is used to secure the keys of the AES algorithm. From the results of this study, the results obtained that the combination of AES and Diffie-Hellman algorithms succeeded in securing medical images. The Diffie-Hellman algorithm will produce different keys which are then used as AES keys. While the AES algorithm is able to encrypt and decrypt medical images without changing the contents of the image.*

***Keyword:*** *Cryptography, Medical Image, Advanced Encryption Standard (AES) Algorithm, Diffie-Hellman Algorithm*