ABSTRACT

Along with the development of information technology, data security is a very important aspect in the digital era, Otoritas Jasa Keuangan (OJK) reported that in the period 2020 to 2023 there were more than 20 cases of data theft. From the many cases, an effective data security method is needed by combining cryptography and steganography. This study aims to apply the Advanced Encryption Standard (AES) cryptographic algorithm and the Spread Spectrum steganography method to secure data by inserting PDF files into PNG digital images. The AES algorithm is used to encrypt messages so that they can only be accessed by those who have the key, while the Spread Spectrum steganography method is used to hide messages in digital images without significantly reducing visual quality. This study includes the process of encrypting the contents of the message with AES, then changing it to bit form which is then spread on the object cover with the spread spectrum steganography method, then in the file extraction process despreading is carried out to take the bits contained in the stego image and return it to file form. Furthermore, after testing, an evaluation of the quality of the resulting image is carried out based on the PSNR (Peak Signal to Noise Ratio) and MSE (Mean Squared Error) parameters. The results of the study show that the method used is able to insert and extract data with good image quality (PSNR> 40 dB) and short processing times. Thus, this study shows that the combination of AES and Spread Spectrum Steganography is successful in protecting data, especially in the context of protecting confidential digital documents.

Keywords: Data security, Cryptography, AES, Steganography, Spread Spectrum.