ABSTRACT

IMPLEMENTATION OF AES CRYPTOGRAPHY AND IMAGE STEGANOGRAPHY USING THE SPREAD SPECTRUM METHOD FOR SECURING TEXT DATA

By

Diva Zahra Berliani

21102103

Data security has become one of the most important aspects in the digital age, particularly in protecting sensitive information from hacking and data theft threats. One of the main challenges is how to maintain the confidentiality and integrity of data when transmitted through networks vulnerable to attacks. To address this issue, this research proposes a solution by combining the Advanced Encryption Standard (AES) 128-bit algorithm as a method of data encryption and the Spread Spectrum steganography technique to embed ciphertext into images. Embedding ciphertext into images using the Spread Spectrum technique helps maintain the confidentiality and integrity of the data because the encrypted message is hidden within the image, which appears to be a regular image, thus reducing the risk of detection by unauthorized parties. This enhances the security of the transmitted data as the ciphertext is spread across the image. The aim of this research is to implement the AES (Advanced Encryption Standard) method for encryption and Spread Spectrum steganography for embedding ciphertext into images, as well as to test its effectiveness in preserving image quality and data security. The test results show that this method effectively maintains data confidentiality and integrity, with the Mean Square Error (MSE) value remaining low and the Peak Signal-to-Noise Ratio (PSNR) above 30 dB, indicating that the

image quality remains good after the message embedding. Thus, the combination of AES and Spread Spectrum can serve as a potential solution for data protection in various information security applications.

Key Words : AES, Spread Spectrum, Steganography, Data Security, MSE, PSNR