ABSTRAK

Keamanan data tersembunyi dalam citra digital masih menghadapi tantangan, terutama pada metode steganografi LSB yang rentan terhadap deteksi dan manipulasi struktural. Penelitian ini mengusulkan kombinasi algoritma AES-GCM 256-bit (untuk kerahasiaan dan integritas) dengan RSA 4096-bit (untuk keamanan kunci) pada proses penyisipan pesan. Metode ini mengenkripsi pesan rahasia dengan AES-GCM, mengenkripsi kunci AES dengan RSA, lalu menyisipkan data terenkripsi ke dalam citra PNG 24-bit menggunakan LSB steganografi. Pengujian melibatkan metrik kualitas citra (PSNR), deteksi tersembunyi (StegExpose), serta analisis keamanan (entropi *ciphertext*, integritas hash, dan ketahanan manipulasi *ciphertext*). Hasil penelitian menunjukkan entropi *ciphertext* mencapai ~96–99,99%, kualitas citra stego tetap tinggi (PSNR sekitar 66 dB pada file *plaintext* 137 Byte dan sekitar 46 dB pada *plaintext* ukuran 2857 KB) dan tidak terdeteksi oleh StegExpose. Verifikasi integritas menggunakan SHA-256 membuktikan pesan diekstrak tanpa perubahan bit, sedangkan setiap modifikasi satu byte *ciphertext* menyebabkan dekripsi gagal (deteksi manipulasi 100%). Dengan demikian, kombinasi AES-GCM + RSA dapat meningkatkan keamanan steganografi LSB tanpa menurunkan kualitas visual citra.

Kata Kunci: AES, Enkripsi, LSB, RSA, Steganografi

ABSTRACT

The security of hidden data in digital images still faces challenges, particularly in LSB steganography methods that are vulnerable to detection and structural manipulation. This study proposes a combination of the AES-GCM 256-bit algorithm (for confidentiality and integrity) with RSA 4096-bit (for key security) in the message embedding process. The method encrypts the secret message using AES-GCM, encrypts the AES key with RSA, and then embeds the encrypted data into a 24-bit PNG image using LSB steganography. Testing involved image quality metrics (PSNR), hidden data detection (StegExpose), and security analysis (ciphertext entropy, hash integrity, and resistance to ciphertext manipulation). The results show that the ciphertext entropy reaches approximately 96–99.99%, stego image quality remains high (PSNR around 66 dB for a 137-byte plaintext and around 46 dB for a 2857 KB plaintext), and hidden data is not detected by StegExpose. Integrity verification using SHA-256 confirms the extracted message matches the original with no bit changes, while any one-byte modification to the ciphertext results in decryption failure (100% tamper detection). Thus, the AES-GCM + RSA combination can enhance the security of LSB steganography without degrading the visual quality of the image.

Keywords: AES, Encryption, LSB, RSA, Steganography