ABSTRACT

Data security is a critical challenge in digital transmission due to the risk of unauthorized access. This research develops a data security system integrating double encryption using the AES-256 algorithm in Cipher Block Chaining (CBC) mode and RSA-2048 with Least Significant Bit (LSB) steganography on color PNG images. The system is built using Python with a Tkinter interface, encompassing encryption/embedding, extraction/decryption, and performance measurement functions. Testing was conducted on five PNG images (resolutions from 100x100 to 500x500 pixels) with text messages varying from 100 to 2667 characters. Results demonstrate that the system successfully encrypts and embeds data with an average Mean Squared Error (MSE) of 0.0263730426 and Peak Signal-to-Noise Ratio (PSNR) of 64.3427895234 dB, indicating excellent stego image quality with no significant visual differences. The extraction and decryption processes fully recover the original message without data loss. System efficiency is evidenced by an average execution time of 92.376 ms for encryption/embedding and 370.392 ms for extraction/decryption, along with memory usage of 0.682 MB and 0.528 MB. Steganographic capacity approaches the theoretical limit (93,354 practical characters vs. 93,746 theoretical characters at 500x500 pixels), with a capacity gap of 295–395 characters at lower resolutions due to metadata overhead. The use of compress_level=0 ensures the stego file size increases in accordance with embedded data (average increase of 90.944%). The system proves effective in securing text data with high security, visual imperceptibility, adequate efficiency, and optimal capacity, achieving all research objectives. Recommendations for further development include optimizing decryption time, enhancing steganographic capacity, and testing resilience against steganalysis attacks.

Keywords: *Cryptography, Encryption, AES, RSA, Steganography*