INTISARI

Perkembangan teknologi saat ini sudah sangat pesat, hampir semua bidang dalam kehidupan tidak luput dari yang Namanya teknologi dan internet. Hal ini karena dengan adanya teknologi dan internet dapat mempermudah dalam mencari informasi dan pertukaran data. Namun tidak semua pengguna internet dapat menggunakannya dengan bijak. Selain dapat mempermudah internet juga dapat menjadi sarana kejahatan digital seperti pencurian data. Maka dari itu diperlukan Solusi dalam pengamanan data untuk memastikan data-data penting yang bersifat pribadi tidak dapat diketahui oleh orang tidak bertanggung jawab. Salah satu yang dapat digunakan dalam pengamanan ada adalah Teknik steganografi. Teknik steganografi membutuhkan adanya citra sebagai wadah penyimpan pesan yang akan disembunyikan. Metode steganografi seperti Least Significant Bit dan Bit-Plane Complexity Segmentation dapat digunakan dengan bahasa pemrograman python pada platform pemrograman Visual Studio Code Tujuan dari penelitian kali ini adalah untuk membandingkan metode steganografi LSB dan BPCS dalam menyembunyikan pesan. Pengujian yang digunakan dalam perbandingan ini berupa Pengujian kualitas citra (fidelity), pengujian manipulasi (robustness), percobaan pengembalian pesan (recovery), dan perbandingan kualitas visual citra (imperceptibility). Lalu perbandingan kemiripan citra diuji melalui hasil nilai MSE dan PSNR. Hasil dari perbandingan didapatkan bahwa metode LSB lebih baik dalam mempertahankan kualitas citra, sedangkan metode BPCS lebih baik dalam hal mempertahankan pesan didalam citra.

Kata Kunci : Steganografi, LSB, BPCS, Citra Digital, Analisis, Python

ABSTRACT

The current technological advancement is rapidly growing, and almost every aspect of life is influenced by technology and the internet. This is because technology and the internet facilitate easy access to information and data exchange. However, not all internet users can use it wisely. Besides providing convenience, the internet can also be a platform for digital crimes such as data theft. Therefore, a solution is needed for data security to ensure that sensitive personal data remains unknown to irresponsible individuals. One solution for data security is the use of steganography techniques. Steganography requires an image as a container for hiding messages. Steganographic methods like Least Significant Bit (LSB) and Bit-Plane Complexity Segmentation (BPCS) can be implemented using the Python programming language on the Visual Studio Code platform. The objective of this research is to compare the LSB and BPCS steganography methods in concealing messages. The evaluation criteria for this comparison include image quality testing (fidelity), manipulation testing (robustness), message recovery experiments, and visual image quality comparison (imperceptibility). Additionally, the similarity of images is tested through the results of MSE (Mean Squared Error) and PSNR (Peak Signal-to-Noise Ratio) values. The comparison results indicate that the LSB method is better at maintaining image quality, while the BPCS method excels in preserving messages within the image.

Keywords: Steganography, LSB, BPCS, Digital Image, Analysis, Python