INTISARI

Pengetahuan mengenai keamanan data pada saat ini sangatlah penting. Hal ini dikarenakan adanya jaringan internet yang memberikan kemudahan terhadap pertukaran data sehingga banyak orang yang menggunakannya. Akan tetapi tidak semua orang dapat dengan bijak dalam memanfaatkan internet sebagai sarana pertukaran data. Hal seperti ini justru dapat memicu adanya tindak kejahatan seperti pencurian data. Maka dari itu diperlukan adanya suatu penanganan terhadap keamanan data untuk memastikan jika pesan atau informasi yang bersifat rahasia terjaga dari pihak-pihak yang tidak bertanggung jawab. Salah satu cara untuk mengamankan data adalah dengan menyembunyikannya menggunakan teknik steganografi. Teknik steganografi membutuhkan media yang menjadi wadah untuk pesan yang akan disembunyikan. Metode yang digunakan adalah Least Significant Bit. Tahapan pre-processing dilakukan dengan perangkat lunak Jupyter Notebook dan program steganografi yang dijalankan pada perangkat lunak Visual Studio Code menggunakan bahasa pemrograman Python. Tujuan dari penelitian ini adalah mengetahui performa metode Least Significant Bit terhadap citra RGB, Grayscale, dan HSV. Pengujian yang dilakukan diantarannya adalah dengan melihat perbandingan kualitas citra yang dihasilkan (fidelity) dan pengembalian isi pesan citra (recovery). Pengujian security check dilakukan dengan melihat hasil histogram. Lalu pengujian perbandingan kemiripan citra dilakukan dengan mengetahui nilai MSE dan PSNR. Hasil penelitian ini menunujukan bahwa citra grayscale memiliki tingkat kemiripan antara citra cover dan citra stego lebih tinggi dibandingan RGB dan HSV dengan rata-rata nilai MSE =.0.000702 dan PSNR = 80.33818794. Beriutnya pengujian kapasitas penyisipan dilakukan dengan membandingkan ukuran citra berdasarkan jumlah karakter yang digunakan.

Kata kunci: Steganografi, LSB, Citra Digital, Python.

ABSTRACT

Knowledge of data security at this point is very important. This is because there is an internet network that makes it easy to exchange data so that many people use it. However, not everyone can use the internet wisely as a means of exchanging data. Things like this can actually trigger crimes such as data theft. Therefore it is necessary to have a handling of data security to ensure that confidential messages or information are protected from irresponsible parties. One way to secure data is to hide it using steganography techniques. Steganography techniques require media to be a container for messages to be hidden. The method used is Least Significant Bit. The pre-processing stage was carried out using Jupyter Notebook software and a steganography program that was run on Visual Studio Code software using the Python programming language. The purpose of this study is to determine the performance of the Least Significant Bit method on RGB, Grayscale, and HSV images. The tests carried out include looking at the comparison of the resulting image quality (fidelity) and the return of the contents of the image message (recovery). Security check testing is done by looking at the histogram results. Then testing the comparison of image similarity is done by knowing the MSE and PSNR values. The results of this study indicate that grayscale images have a higher degree of similarity between cover images and stego images than RGB and HSV with an average MSE value = 0.000702 and PSNR = 80.33818794. Next, the insertion capacity test is carried out by comparing the size of the image based on the number of characters used

Keywords: Steganography, LSB, Digital Image, Python.