

## INTISARI

Kejahatan dunia maya semakin menyerang privasi seseorang, organisasi, dan pemerintah. Data diri yang penting semakin tidak aman karena pengambilan data secara ilegal oleh orang yang tidak memiliki kepentingan di dalamnya. Penelitian ini bertujuan untuk mengembangkan suatu teknik penyisipan data pada citra gambar yang diuji ketahanan datanya saat diserang oleh gaussian blur.

Pengembangan teknik ini menggunakan bahasa pemrograman Python dan metode LSB (*Least Significant Bit*). Dengan pengujian terhadap serangan gaussian blur menggunakan pengujian *imperceptibility*, *fidelity*, dan *robustness*. Hasil pengujian yang telah dilakukan untuk pengujian *imperceptibility* menggunakan 25 responden dengan 10 citra gambar dan didapatkan persentase 80%. Hasil pengujian *fidelity* menggunakan 10 citra gambar dengan mengukur nilai MSE dan nilai PSNR didapatkan bahwa 10 citra mendapat nilai MSE mendekati 0 atau kurang dari 1 dan 10 citra mendapat nilai PSNR >40dB yang dapat dikatakan sangat baik. Hasil pengujian *robustness* menggunakan radius blur 0 sampai 1 pada 10 citra gambar mendapatkan hasil 8 dari 10 citra gambar dapat diekstraksi pesannya, sehingga secara keseluruhan penelitian ini dikatakan “Berhasil dan Sangat Baik”.

**Kata Kunci :** Steganografi, Dunia Maya, LSB, Python *Programming*, Gaussian Blur

## **ABSTRAK**

Cybercrimes are increasingly invading the privacy of individuals, organizations and governments. Important personal data is increasingly insecure because of illegal data collection by people who have no interest in it. This study aims to develop a data embedding technique in images whose data robustness is tested when attacked by Gaussian Blur.

The development of this technique uses the Python programming language and the LSB (Least Significant Bit) method. By testing the gaussian blur attack using imperceptibility, fidelity, and robustness tests. The test results that have been carried out for imperceptibility testing use 25 respondents with 10 images and get a percentage of 80%. The results of the fidelity test using 10 images by measuring the MSE value and PSNR value found that 10 images got an MSE value close to 0 or less than 1 and 10 images got a PSNR value of  $>40\text{dB}$  which can be said to be very good. The results of the robustness test using a blur radius of 0 to 1 on 10 images obtained the message that 8 out of 10 images could be extracted, so that overall this study was said to be "Successful and Very Good".

**Keywords** : Steganography, Cybercrimes, LSB, Python Programming, Gaussian Blur