# ABSTRAK

Kerahasiaan suatu informasi adalah penting dan menjadi suatu perhatian tersendiri. Zaman sekarang informasi tidak hanya dapat disandikan, tetapi dapat juga disisipkan ke dalam media digital. Teknik menyisipkan pesan dikenal dengan nama steganografi. Steganografi sebagai ilmu dan seni untuk menyembunyikan informasi sehingga informasi yang bersifat rahasia tidak dapat diketahui oleh orang lain, kecuali pengirim dan penerima. Beberapa penelitian telah dilakukan berkaitan dengan pengamanan data dengan menerapkan beberapa algoritma.

Pada penelitian ini dibangun aplikasi dengan menerapkan metode steganografi *Least Significant Bit* (LSB), *Discrete Cosine Transform* (DCT), dan *Discrete Haar Wavelet Transform* (DWT) untuk dilakukan analisis faktor *robustness* dan *fidelity*, sedangkan pembuatan aplikasi menggunakan bahasa pemrograman Python dengan micro-framework Flask. Dalam penerapannya, pesan akan disisipkan pada citra digital dengan metode LSB, DCT, DWT, dan kombinasi ketiga metode tersebut. Hasil penyisipan akan diuji dari aspek *robustness* dan *fidelity* dan kemudian akan dianalisis dan disimpulkan manakah metode penyisipan yang paling baik untuk diimplementasikan. Metodologi yang digunakan dalam penelitian ini menggunakan pendekatan metode *prototyping*.

Hasil penelitian menunjukan berdasarkan pengujian robustness dengan pendekatan Stirmark berbasis *geo transform attack,* metode LSB mendapat rata-rata persentase keberhasilan ekstraksi pesan tertinggi sebesar 24,3% dan berdasarkan serangkaian pengujian *fidelity*, metode LSB mendapat hasil dengan rata-rata terbaik yaitu tidak nampak perbedaan visual, rata-rata selisih ukuran *file* terendah sebesar 3,2 MB, nilai PSNR tertinggi sebesar 68,2 dB, dan rata-rata nilai perbedaan RGB dengan jarak *Euclidean* sebesar 339,14.



**Kata kunci**: Steganografi, *Least Significant Bit* (LSB), *Discrete Cosine Transform* (DCT), Discrete *Haar Wavelet Transform* (DWT), *Robustness*, *Fidelity*