

**IMPLEMENTASI STEGANOGRAFI ADAPTIF BERBASIS
HYBRID EDGE DETECTION DAN GENERATIVE
ADVERSARIAL NETWORK PADA CITRA DIGITAL**

TUGAS AKHIR

*Karya Ilmiah sebagai salah satu syarat untuk menyelesaikan jenjang strata satu
(S-1) di Jurusan Teknik Elektro, Fakultas Teknik, Universitas Andalas*

Oleh

Rahma Dayandri

NIM. 2110952014

Pembimbing:

Dr. Eng. Rahmadi Kurnia, S.T., M.T.

NIP. 196908201997031002



Program Studi Sarjana
Teknik Elektro Fakultas Teknik
Universitas Andalas

2025

Judul	Implementasi Steganografi Adaptif Berbasis <i>Hybrid Edge Detection</i> Dan <i>Generative Adversarial Network</i> Pada Citra Digital	Rahma Dayandri
Program Studi	Teknik Elektro	2110952014
Fakultas Teknik Universitas Andalas		
Abstrak Pesatnya perkembangan teknologi komunikasi digital menuntut sistem keamanan informasi yang semakin andal. Steganografi merupakan salah satu metode yang digunakan untuk menyisipkan informasi rahasia ke dalam media digital secara tersembunyi. Penelitian ini mengusulkan metode steganografi adaptif dengan deteksi tepi hibrida (<i>Canny</i> dan <i>Kirsch</i>) dengan penyisipan <i>Least Significant Bit</i> (LSB) dan disempurnakan oleh <i>Generative Adversarial Network</i> (GAN). Metode deteksi tepi hibrida (<i>Canny</i> dan <i>Kirsch</i>) digunakan untuk memaksimalkan kapasitas pesan dengan menyisipkannya pada area kompleks citra yang secara visual tidak sensitif terhadap perubahan. Setelah penyisipan awal, GAN merekonstruksi stego image untuk menghilangkan jejak statistik dan meningkatkan keamanan terhadap serangan steganalisis. Model dilatih dengan dataset DIV2K pada kapasitas 1–4 bit per kanal warna. Hasil pengujian menunjukkan bahwa GAN berhasil meningkatkan keamanan secara signifikan; citra yang telah disempurnakan (<i>Stego 2</i>) mampu lolos dari deteksi RS <i>Analysis</i>, sementara citra hasil LSB awal (<i>Stego 1</i>) sangat mudah terdeteksi. Meskipun <i>Stego 1</i> memiliki PSNR lebih tinggi, <i>Stego 2</i> mempertahankan kualitas visual yang baik (PSNR > 30 dB) pada kapasitas rendah. Dengan teknik repetisi bit, sistem menunjukkan ketahanan terhadap noise intensitas rendah, namun gagal menghadapi kompresi <i>lossy</i>. Penelitian ini membuktikan bahwa kombinasi ini terbukti efektif untuk menciptakan sistem steganografi yang aman terhadap analisis statistik dengan kualitas visual yang dapat diterima. Kata Kunci: Steganografi, LSB Adaptif, Deteksi Tepi, <i>Canny</i>, <i>Kirsch</i>, <i>Generative Adversarial Network</i> (GAN), Keamanan Informasi, Steganalisis.		

Title	<i>Implementation of Adaptive Steganography Based on Hybrid Edge Detection and Generative Adversarial Network on Digital Images</i>	Rahma Dayandri
Mayor	Department of Electrical Engineering	2110952014
Faculty of Engineering		
Abstract <i>The rapid development of digital communication technology demands increasingly reliable information security systems. Steganography is one method used to embed secret information into digital media in a hidden manner. This study proposes an adaptive steganography method that integrates hybrid edge detection (Canny and Kirsch) with Least Significant Bit (LSB) embedding, further enhanced by a Generative Adversarial Network (GAN). The hybrid edge detection is utilized to maximize message capacity by embedding data into complex image regions that are visually less sensitive to changes. After the initial embedding, the GAN reconstructs the stego image to eliminate statistical traces and improve security against steganalysis attacks. The model was trained on the DIV2K dataset with embedding capacities ranging from 1 to 4 bits per color channel. Experimental results show that GAN significantly improves security; the refined stego image (Stego 2) successfully evades RS Analysis detection, while the initial LSB stego image (Stego 1) is easily detected. Although Stego 1 achieves a higher PSNR, Stego 2 maintains good visual quality (PSNR > 30 dB) at lower capacities. Using bit-repetition techniques, the system demonstrates robustness against low-intensity noise but remains vulnerable to lossy compression. This research proves that the proposed combination is effective in creating a steganography system that is secure against statistical analysis while maintaining acceptable visual quality.</i> <i>Keywords: Steganography, Adaptive LSB, Edge Detection, Canny, Kirsch, Generative Adversarial Network (GAN), Information Security, Steganalysis.</i>		