

ABSTRAK

MUH. DIRHAM RAHIM, 2026. Klasifikasi *Payload Malware* Tersembunyi pada Citra Digital (Steganalisis) Menggunakan Algoritma *Convolutional Neural Network* (CNN) (Dibimbing oleh Muhyiddin A.M Hayat, S.Kom.,M.T dan Rizki Yusliana Bakti, S.T., M.T.).

Ancaman keamanan siber saat ini semakin mengarah pada teknik penetrasi senyap steganografi Steghide pada citra JPEG. Sistem steganalisis biner konvensional memiliki titik buta forensik karena gagal membedakan tingkat keparahan anomali, seperti antara sisipan teks biasa dan malware destruktif. Oleh karena itu, penelitian ini mengusulkan model 1-Dimensional Convolutional Neural Network (CNN 1D) untuk mengklasifikasikan ancaman steganografi ke dalam tiga kelas: Normal, Anomali Ringan (teks 20 KB), dan Anomali Berat (malware .bat 40 KB). Kapasitas payload tersebut dipilih karena mampu merepresentasikan margin perubahan densitas koefisien secara signifikan untuk menguji sensitivitas model. Guna mengatasi overfitting dan bias visual, ekstraksi dilakukan pada domain frekuensi koefisien Discrete Cosine Transform (DCT) menjadi 2.466 fitur statistik, lalu diuji pada 1.500 citra beresolusi 1024x1024 piksel menggunakan skenario Paired Dataset dan Grouped Split. Hasil penelitian menunjukkan model mencapai tingkat akurasi 83,11% dengan F1-Score 82,98%. Meskipun terdapat tumpang tindih prediksi antara kelas malware dan teks yang membatasi nilai Recall Anomali Berat di angka 76,00%, sistem mencatatkan 0 kejadian False Negative pada persilangan menuju kelas Normal. Hal ini mengindikasikan tingginya keandalan instrumen, di mana tidak ada satupun skrip destruktif yang lolos terklasifikasi sebagai citra aman.

Kata kunci: Steganalisis, Steganografi JPEG, Discrete Cosine Transform (DCT), Convolutional Neural Network 1D, Multi-class Payload Classification.