ABSTRAK

Identifikasi gambar yang dihasilkan oleh kecerdasan buatan (AI) dan sulit dibedakan dari citra asli memiliki implikasi penting di bidang keamanan. Penggunaan deep learning, khususnya Convolutional Neural Network (CNN), sebagai solusi efektif untuk tantangan ini sangat relevan. CNN memainkan peran krusial dalam mengekstraksi fitur dari gambar, memungkinkan identifikasi pola-pola penting yang tidak mudah terlihat. Penelitian ini menerapkan arsitektur CNN dalam membedakan gambar buatan AI dan gambar asli untuk mendukung deteksi gambar palsu. Proses pelatihan dan pengujian model dilakukan menggunakan library TensorFlow, dengan parameter yang dioptimalkan melalui callback EarlyStopping. Penelitian ini menggunakan dataset CIFAKE, yang terdiri dari 60.000 gambar hasil sintesis dan 60.000 gambar asli, dengan total 120.000 gambar berukuran 32x32 piksel dalam format RGB. Data uji yang digunakan adalah data yang berasal dari luar dataset pelatihan. Model dilatih selama 100 epoch dengan optimizer Adam dan learning rate sebesar 0.001. Hasil penelitian menunjukkan bahwa model dengan 4 lapisan konvolusi dan 2 lapisan fully connected mencapai akurasi 94% pada data pelatihan. Namun, terjadi penurunan akurasi hingga sekitar 80% saat diuji dengan data baru yang sebelumnya belum pernah dilihat. Nilai F1-score yang dicapai adalah 94% dan nilai mAP sebesar 98%. Penelitian ini memberikan kontribusi penting dalam bidang deteksi gambar palsu dengan menunjukkan efektivitas arsitektur CNN dalam mengklasifikasikan gambar buatan AI dan gambar asli. Meskipun model menunjukkan kinerja tinggi pada data pelatihan, tantangan dalam mengklasifikasikan data baru yang berbeda dari data latih masih memerlukan perhatian lebih lanjut untuk peningkatan lebih lanjut di masa depan.

Kata Kunci: Kecerdasan Buatan, *Convolutional Neural Network (CNN)*, CIFAKE, Keamanan, Deteksi Gambar Palsu

ABSTRACK

Identifying images generated by artificial intelligence (AI) that are difficult to distinguish from real images has significant implications in the field of security. The use of deep learning, particularly Convolutional Neural Network (CNN), as an effective solution to this challenge is highly relevant. CNN plays a crucial role in extracting features from images, enabling the identification of important patterns that are not easily visible. This research applies CNN architecture to differentiate between AI-generated images and real images to support fake image detection. The model's training and testing processes were conducted using the TensorFlow library, with parameters optimized through the EarlyStopping callback. This study uses the CIFAKE dataset, consisting of 60,000 synthetic images and 60,000 real images, totaling 120,000 images of 32x32 pixels in RGB format. The test data used are from outside the training dataset. The model was trained for 100 epochs using the Adam optimizer with a learning rate of 0.001. The results show that the model with 4 convolutional layers and 2 fully connected layers achieved an accuracy of 94% on the training data. However, there was a drop in accuracy to around 80% when tested with new, previously unseen data. The F1-score achieved was 94%, and the mAP value was 98%. This research makes a significant contribution to the field of fake image detection by demonstrating the effectiveness of CNN architecture in classifying AI-generated images and real images. Although the model shows high performance on the training data, the challenge of classifying new data different from the training data requires further attention for future improvements.

Keywords: Artificial Intelligence, Convolutional Neural Network (CNN), CIFAKE, Security, Fake Image Detection