



INTISARI

Sistem keamanan berbasis pengenalan wajah (*face recognition*) semakin meningkat karena kemudahan, ketepatan, dan keakuratan yang diberikan. Secara bersamaan, terdapat usaha untuk mengeksploitasi kelemahan pada sistem dengan teknologi *face recognition* melalui *face presentation attack*. Pendekatan *face liveness detection* atau *face anti-spoofing* digunakan untuk mengatasi *face presentation attack*. Penelitian ini bertujuan untuk menentukan *pre-trained model* terbaik untuk *face liveness detection* atau *face anti-spoofing*. Selain itu, akan ditentukan pengaruh *background* terhadap performa *pre-trained model*. Metode yang diimplementasikan adalah CNN berbasis *transfer learning*. Percobaan dilakukan pada dua *dataset* untuk *face liveness detection* atau *face anti-spoofing*, yaitu NUAA Imposter Database dan Replay-Attack Database. Untuk setiap *dataset*, terdapat versi yang mengandung detail *background* (format 1) dan versi yang hanya mengandung area wajah (format 2). Pada NUAA Imposter Database, VGG-19 yang dilatih dengan *dataset* format 1 dan *learning rate* sebesar 10^{-3} memiliki performa terbaik dengan HTER sebesar 1,37%, F1 score sebesar 98,63%, *binary accuracy* sebesar 98,29%, dan *loss* sebesar 0,0417. Pada Replay-Attack Database, VGG-16 yang dilatih dengan *dataset* format 1 dan *learning rate* sebesar 10^{-4} memiliki performa terbaik dengan HTER sebesar 2,65%, F1 score sebesar 99,12%, *binary accuracy* sebesar 98,65%, dan *loss* sebesar 0,0539. Pada NUAA Imposter Database dan Replay-Attack Database, *background* berpengaruh terhadap performa *pre-trained model*, baik itu berpengaruh positif maupun negatif. Pada VGGNet (VGG-16 dan VGG-19), Inception-v3, dan Xception, *background* dapat menurunkan nilai HTER. Pada ResNet-101, *background* dapat menaikkan nilai HTER.

Kata kunci: *face liveness detection*, *face anti-spoofing*, *convolutional neural network*, *transfer learning*, *pre-trained model*

ABSTRACT

The security system based on face recognition is increasingly improving due to the convenience, accuracy, and reliability it provides. Simultaneously, there are efforts to exploit weaknesses in the system through face presentation attacks using face recognition technology. The approach of face liveness detection or face anti-spoofing is used to address face presentation attacks. This research aims to determine the best pre-trained model for face liveness detection or face anti-spoofing. Additionally, the influence of the background on the performance of the pre-trained model will be determined. The implemented method is transfer learning-based CNN. Experiments were conducted on two datasets for face liveness detection or face anti-spoofing, namely the NUAA Imposter Database and the Replay-Attack Database. For each dataset, there are versions that contain detailed backgrounds (format 1) and versions that only contain the face area (format 2). In the NUAA Imposter Database, VGG-19 trained with format 1 dataset and a learning rate of 10^{-3} showed the best performance with an HTER of 1.37%, F1 score of 98.63%, binary accuracy of 98.29% and a loss of 0.0417. In the Replay-Attack Database, VGG-16 trained with format 1 dataset and a learning rate of 10^{-4} demonstrated the best performance with an HTER of 2.65%, F1 score of 99.12%, binary accuracy of 98.65% and a loss of 0.0539. In both the NUAA Imposter Database and the Replay-Attack Database, the background had an impact on the performance of the pre-trained models, whether it was positive or negative. In VGGNet (VGG-16 and VGG-19), Inception-v3 and Xception, the background could decrease the HTER value. However, in ResNet-101, the background could increase the HTER value.

Keywords: face liveness detection, face anti-spoofing, convolutional neural network, transfer learning, pre-trained model