ABSTRACT

A biometric system is a security process that uses information based on certain characteristics of a living person to verify or recognize the identity. One example is the face recognition system that is able to distinguish different people through facial features. Face biometric systems implemented in real-world applications are mainly used for access control and surveillance. With the capability to recognize a person the systems still suffer problems such as attacks using fake faces or so-called spoofing.

Addressing this challenge requires a security system that has the task of preventing fake authorizations that violate the facial recognition system using photos, videos, masks, or other attacks using the faces of authorized persons. The Deep Learning approach with the CNN architecture is chosen based on the parameter values of each layer that can be measured and modified. As for CASIA-SURF dataset is used because it has not only quantity but also provides more types of image and diversity to achieve better results.

In this research, a study aims to maintain accuracy and reduce the number of parameters used by the CNN architecture in the spoof classification system. The original model named SqueezeNext is used and modified further by reducing the depth or number of filters in the architecture and categorizes the classification system between real faces and spoof attacks. The results of the experiment achieve accuracy up to 99% and 0.1% loss which maintain the good performance with the number of parameters used in the model around 0.30 M resulting in 4.4 MB model size which is less than SqueezeNext and FeatherNetB.

Keywords: Image Processing, Biometric System, Convolutional Neural Network, Face Spoof.

INTISARI

Sistem biometrika adalah proses keamanan yang menggunakan informasi berdasarkan karakteristik tertentu dari seorang manusia untuk diverifikasi atau dikenali identitasnya. Salah satu contohnya adalah sistem pengenalan wajah yang mampu membedakan setiap orang melalui ciri wajah. Sistem biometrika wajah yang diimplementasikan dalam aplikasi dunia nyata umumnya digunakan untuk kontrol akses dan pengawasan. Dengan kemampuan untuk mengenali seseorang, sistem ini masih mengalami masalah seperti serangan menggunakan tiruan wajah atau biasa disebut dengan *spoofing*.

Untuk mengatasi tantangan ini diperlukan sistem keamanan yang memiliki tugas untuk mencegah otorisasi palsu yang melanggar sistem pengenalan wajah menggunakan foto, video, topeng, atau serangan lain menggunakan wajah orang yang berwenang. Pendekatan *Deep Learning* dengan arsitektur CNN dipilih berdasarkan nilai parameter setiap lapisan yang dapat diukur dan dimodifikasi. Adapun *CASIA-SURF dataset* yang digunakan tidak hanya memiliki kuantitas yang banyak tapi menyediakan lebih banyak tipe citra serangan dan keragaman untuk mencapai hasil yang lebih baik.

Penelitian ini dilakukan dengan tujuan untuk mempertahan akurasi yang sudah baik dan mengurangi jumlah parameter yang digunakan oleh arsitektur CNN pada sistem klasifikasi untuk serangan wajah. Model dasar yang digunakan adalah *SqueezeNext* yang dimodifikasi lebih lanjut dengan mengurangi kedalaman atau jumlah filter dalam arsitektur lalu mengategorikannya menjadi sistem klasifikasi citra antara wajah asli dan serangan tiruan. Hasil percobaan yang mencapai rata-rata akurasi hingga 99% dengan kerugian 0,1% memperlihatkan model yang diusulkan tetap memiliki performa yang baik dengan jumlah parameter lebih kecil sekitar 0,30 M dan menghasilkan model berukuran sekitar 4,4 MB yang lebih kecil dari model *SqueezeNext* dan *FeatherNetB*.

Kata kunci -- *Image Processing, Biometric System, Convolutional Neural Network, Face Spoof.*