Video Spoofing Attack Detection Using Convolutional Neural Networks and Ensemble Learning Voting Classifier Methods

1st Siti Vanesa Rahma
School of Computing
Telkom University
Bandung, Indonesia
sitivanesarahma@student.telkomuniversity.ac.id

2nd Vera Suryani
School of Computing
Telkom University
Bandung, Indonesia
verasuryani@telkomuniversity.ac.id

***Abstract*—Facial recognition technology is increasingly being used in various applications, but this has resulted in the emergence of new threats such as spoofing. Existing detection systems still face several shortcomings, such as low accuracy or limited variety of training data, making them vulnerable to spoofing attacks. This research develops a spoofing detection system based on Convolutional Neural Networks (CNN) and ensemble learning methods that combine several models, such as Support Vector Machines (SVM), Random Forests, and Logistic Regression with Voting Classifier techniques tested on the iBeta Level 1 - Liveness Detection Dataset. This approach is done by utilizing a combination of models to improve detection accuracy and reduce the weakness of individual models. The proposed system is tested using validation and test datasets to ensure no overfitting/underfitting occurs. The experimental results in the test data in this study show that the method achieves 97% accuracy on tests and 98% on validation for ensemble learning, as well as 100% on test and validation for CNN-based models. These findings prove the effectiveness of deep learning and ensemble learning approaches in detecting spoofing, thus potentially improving the security of face recognition systems.**

Keywords—spoofing, deep learning, ensemble learning, overfitting, underfitting, accuracy

I. Introduction

Facial recognition technology is currently a very important component for the process of identifying or authenticating identities in life, ranging from public security, finance, military, to everyday life [1]. At the same time, the security threats of these facial recognition systems are growing, especially with Spoofing attacks. Spoofing refers to impersonating a legitimate user through the use of images, videos, or face masks to fool a facial recognition system. Due to the fact that the incidence of this crime continues to grow, it is imperative that crime detection and prevention mechanisms be researched.

Several studies have been conducted in an attempt to find a solution to this problem. However, each of these studies has limitations that need to be addressed. One example is the research conducted by [2], which resulted in accuracy rates between 88 to 90 percent on the validation dataset. On the other hand, the model was unable to account for variations in lighting conditions, which are often experienced in real-world applications. Research conducted by [3] revealed that the Sequential CNN algorithm produced a relatively low accuracy of 87%, while the Naïve Bayes method only managed to get an accuracy of 81.2%. This shows that the architecture and techniques used are not the most effective. When compared to this study, other studies, such as [4] only achieved 77.41% accuracy using the SVM technique because the selected features were limited to RGB average, variance, and luminance. In addition, most of these methods are unable to handle real-world conditions, such as illumination variations, or more complex types of spoofing attacks, such as the use of 3D masks. This emphasizes the need for more sophisticated approaches to detect these attacks. Previous studies using machine learning tend to have performance limitations in lower accuracy than those using deep learning. Therefore, in this study, ensemble learning is used to see if this algorithm can be better when compared to deep learning.

This research aims to overcome the limitations of previous methods by developing a face spoofing detection system that is more accurate and resistant to various attack conditions. This research utilizes Convolutional Neural Networks or commonly called CNN with Xception architecture that excels in detecting complex patterns. In addition, to increase the generalization capacity of the model, a Voting classifier-based ensemble learning strategy that integrates Support Vector Machine or commonly called SVM, Random Forest, and Logistic Regression is used. With the use of these models, this research can handle challenges such as illumination differences, frame variations, as well as detect advanced Spoofing attacks, while improving accuracy over previous methods.

II. Relate Work

Spoofing [5] is the current state of deception of facial recognition technology to disrupt the biometric validation process so that the system cannot correctly recognize real and fake faces. This situation has become a widespread concern in the field of digital media and cybersecurity because there have been various negative impacts from the development of these threats. Research related to Spoofing detection has shown progress to eradicate the negative impact of Spoofing.

Several studies have introduced methods to detect Spoofing using one of the fields of Artificial Intelligent (AI), namely machine learning and deep learning. The machine learning and deep learning approaches used also vary, one of which is in research [6] detecting with CNN, Naive Bayes, KNN, SVM, Random Forest, and Decision Tree algorithms giving an average maximum accuracy of around 87.5%. Another study [7] using the Video Vision Transformer (ViViT) deep learning algorithm found that on the Rose-Youtu Dataset the training set accuracy was obtained at 98.34% but dropped in the validation set and test set by 86.47% and 86.78%. The research [8] shows high accuracy for the use of internal datasets with training accuracy of 95%,