Fake face detection algorithm using rPPG and LSTM

Yu Jin Shin[1], Min Cheol Kim [1], Chae Lin Seok [1], Su Min Jeon [1], Eui Chul Lee*[1]

[1]Department of Human-Centered Artificial Intelligence, Sangmyung University, Hongjimun 2-Gil 20, Jongno-Gu, Seoul 03016, South Korea
Corresponding author* : eclee@smu.ac.kr

Abstract

Biometric recognition technology has been widely used in the field of security systems in recent years, and face recognition is gaining attention for its high accuracy and real-time processing capability. However, there is a problem that a person's face is exposed and can be easily forged with facial images, etc., making forged face detection an important issue. In this paper, we propose a fake face discrimination technique between the real face image and the face photo image by extracting the biological signal from the time series image extracted from the face image using rPPG (remote-photoplethysmogram) signal and LSTM. As a result, it can be confirmed that the biometric signal data filtered in the LSTM model shows a high accuracy of 96.67%.

Keywords: Face recognition, biometric signal detection, counterfeit face detection, rPPG, LSTM, YCbCr

1. Introduction

Recently, personal authentication technology using biometric information has been actively researched. Since the biometric method uses different biometric characteristics of each person, there is no need to carry additional tools such as keys or cards, and there is no fear of sharing, loss, or theft. In addition, it is recognized as an important authentication technology due to the advantage that there is little possibility of fraudulent activity because the person is physically in the field at all times when authentication is required. However, the importance of detecting forged biometric information is increasing as there have recently been cases of forgery of such biometric information to deceive the biometric security system. Therefore, studies are being conducted to detect the “liveness” of biometric information in order to determine whether such a forged face is present. In this paper, we propose a method to detect a fake face using photographs based on physiological signals obtained from time series images. The key is to take advantage of the characteristic that the frequency band of the signal, which is considered to be heartbeat, appears prominent in the real face, but this band does not appear in still images or still objects.

In Suh's “Physiological signal extraction based liveness detection method for face recognition system” study, the YCbCr color model captured minute changes through an image-based skin color amplification method. After that, he proposed a method to determine whether a person in front of the current face recognition system is alive or not by extracting biometric signals [1].

In Liu's "3D Mask Face Anti-spoofing with Remote Photoplethysmography" study, bio-signals are extracted using local rPPG signals to prevent noise. Here, the rPPG signal performs a cross-correlation operation with the estimated value “ground truth”, which is a periodic signal, using a characteristic that has consistency only in the real face. In order to perform the above operation, a process of estimating the "ground truth" value is required, and performance is influenced by this estimated value.
Therefore, in this paper, we propose a method of detecting fake faces using photographs using only biometric signals obtained from time series images.

2. Proposed Work

In this paper, the LSTM model is trained on the basis of the biometric signals extracted from the human face image to discriminate the real face image and the forged image. The following figure is a flowchart of the proposed method.

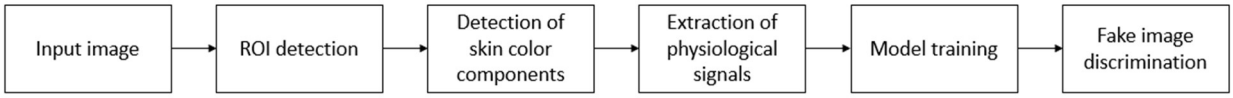

Figure 1. Flow chart of the method of detecting fake images

First, a time series image is input as input data. Since the movement of the face or the change of the facial expression can act as a noise component irrelevant to the biometric signal, a static face image is used. In order to identify the forged images, an experiment was conducted using face images with an average length of 8 to 10 seconds.

Afterwards, the face area is detected by applying Viola's method to the input image [3]. We applied the YCbCr color model to extract bio-signals based on the detected face area. In the YCbCr model, Y represents the lighting component, and Cb and Cr represent the blue and red components, respectively, and a minute change in skin color was extracted through the average of the Cb and Cr values in the image. By applying the YCbCr color model, it is possible to extract a bio-signal by capturing the color change due to blood flow from the viewpoint of the color difference component excluding the change in lighting [1].

In order to remove the noise component included in the image from the obtained bio-signal, bandpass filtering was applied to extract a signal in a frequency domain similar to that of the bio-signal. After that, a furrier transform was applied to the filtered signal to extract a signal(Frequency) transformed into the frequency domain.

Long Short-Term Memory (LSTM), a type of Recurrent Neural Networks (RNN), was used to detect forged face images through biometric signals [4]. Using LSTM, it is possible to effectively detect a counterfeit face by effectively estimating the time series relationship of biometric signals. LSTM model consists of 4 layers, LeakyReLU and Sigmoid activation functions, and batch normalization and early termination methods to prevent overfitting, and the overall model structure is shown in the figure.

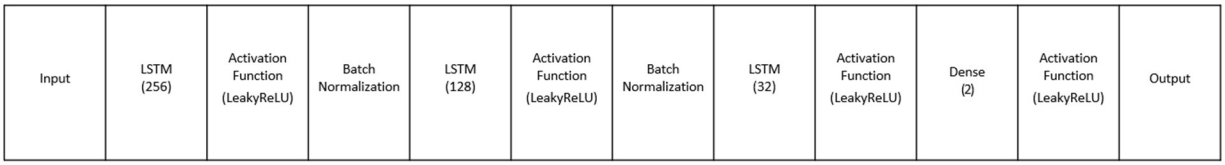

Figure 2. LSTM model structure

In order to apply the above algorithm, a video-type image of at least 10 seconds or longer taken from a close range that can capture subtle changes in skin color is required. Public face datasets does not meet the condition, so it is not possible to prove the validity of the fake face detection algorithm. Therefore, in this experiment, we conducted experiments based on images taken directly from separate subjects, not on public datasets.

As a result of deriving the accuracy by applying the test dataset to the LSTM model, 0.97 was obtained, and as a result of deriving the F1 score, 0.97, the above algorithm shows good performance in detecting fake faces.

3. Conclusion

This paper proposes a fake face detection algorithm using rPPG and LSTM methods. The purpose of this task is to discriminate fake biometric signal only through video without any other devices other than a webcam. For this, a biometric signal is extracted from an image and a frequency signal is obtained through a furrier transform. LSTM is used as an algorithm to discriminate fake biometric signal, and it has been proven that it shows good performance.

Currently, only two types of real faces and printed faces have been classified. In future studies, data

and algorithms will be expanded to distinguish replay faces. In addition, we will shorten the time required for detection so that this system can be used not only in the enrollment, but also in the verification and recognition.

4. References

[1] Suh, Kun-Ha, Eui-Chul Lee, "Physiological signal extraction based liveness detection method for face recognition system", Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology 6.3, 2016, pp. 51-59.

[2] Liu, Siqi, et al., "3D mask face anti-spoofing with remote photoplethysmography", European Conference on Computer Vision. Springer, Cham, 2016.

[3] Viola, Paul, and Michael J. Jones, "Robust real-time face detection." *International journal of computer vision* 57.2, 2004, pp. 137-154.

[4] Nishizaki, Hiromitsu, Koji Makino, "Signal classification using deep learning", IEEE International Conference on Sensors and Nanotechnology. IEEE, 2019.