ISSN: 2096-3246

Volume 55, Issue 02, July, 2023

FACE SPOOFING DETECTION BASED ON MULTI-SCALE COLOR INVERSION DUAL-STREAM CONVOLUTIONAL NEURAL NETWORK

DR.T.S. GHOUSE BASHA[1], BOGGAVARAPU KAVYA SUDHA[2], C NIKITHA[3], CHEPYALA VAISHNAVI[4], CHETTUPALLI SUSHMITHA[5]

PROFESSOR1, DEPARTMENT OF ECE, MALLA REDDY ENGINEERING COLLEGE FOR WOMEN, HYDERABAD

UGSCHOLAR2,3,4&5, DEPARTMENT OF ECE, MALLA REDDY ENGINEERING COLLEGE FOR WOMEN, HYDERABAD

ABSTRACT:

Currently, face recognition technology (FRT) has been applied ubiquitously. However, due to the abuse of personal face photos on social media, FRT has encountered unprecedented challenges which promote the development of face spoofing detection (also called face liveness detection or face anti-spoofing) technology. Traditional face spoofing detection methods usually extract features manually and distinguish real and fake faces through a single cue, which may make these methods have problems with low accuracy and generality. In addition, the effectiveness of existing methods is affected by illumination variations. To address the above issues, we propose a multi-scale color inversion dual-stream convolutional neural network, termed MSCI-DSCNN. One stream of the proposed model converts the input RGB images into grayscale ones and conducts multi-scale color inversion to obtain the MSCI images, which are then put into the improved MobileNet to extract face reflection features. The other stream of the network directly feeds RGB images into the improved MobileNet to extract face color features. Finally, the features extracted separately from the two branches are fused and then used for face spoofing detection. We evaluate the proposed framework on three publicly available databases, CASIA-FASD, REPLAY-ATTACK, and OULU-NPU, and achieve promising results. To further measure the generalization capability of the proposed approach, extensive cross-database experiments are performed and the results exhibit great effectiveness of our MSCI-DSCNN method.

INTRODUCTION

Nowadays, electronic device systems usually use different biometrics such as fingerprints, iris, face, etc. for personal identity verification, among which face recognition technology is the most common method. The ubiquitous face recognition applications in daily life also

provide opportunities for criminals to steal the personal information of legitimate users (Birla & Gupta, 2022). Criminals can obtain personal photos posted by users through social networks and show them to face capture devices, thus achieving the purpose of passing the face recognition systems. Therefore, face spoofing detection technology has become a hot research topic in both academia and industry (Chang and Yeh, 2022, Rehman et al., 2020). There are three main ways for illegal users to attack face recognition systems: print attack, replay attack, and mask attack (Yan et al., 2022). Print attack refers to printing the photos of legitimate users and presenting them to face recognition systems for committing face fraud. Replay attack denotes attackers exhibiting personal videos through mobile devices to deceive the face certification system. Mask attack means that attackers wear 3D masks to spoof the face recognition system. Due to low cost and easy implementation, print and replay attacks are the most common attack methods and the main research objects of this paper. Face spoofing detection, also known as face liveness detection, is usually used as a pre-processing step of a face recognition system to determine whether the acquired face image is from a real face or a fake one. Therefore, face spoofing detection is generally regarded as a binary classification problem. Traditional face spoofing detection mainly includes texture-based methods and physiological information-based methods. Texture-based methods consider that the texture features of the secondary imaging medium are different from those of the real face. These methods typically use LBP (Chen et al., 2019, Chingovska et al., 2012, Shu et al., 2021, Shu et al., 2022), HOG (Komulainen et al., 2012, Yang et al., 2013), and DOG (Zhang et al., 2012) to extract hand-crafted features for face spoofing detection, but generally suffer from poor generalization capability in cross-datasets. The methods based on physiological information primarily leverage motion features such as eye blink (Pan et al., 2007) and mouth movement (Kollreider et al., 2007) as significant cues to distinguish real and fake faces, but these methods are largely computationally intensive.

Unlike the low-level representation of hand-crafted features extracted by traditional methods, deep learning-based approaches can extract high-level semantic feature expressions which are mostly divided into two kinds: single disparity cue-based methods and multiple disparity cues-based methods. The various cues include image quality, rPPG, spatial–temporal information, etc. Image quality-based methods are proposed because secondary imaging of fake faces can bring about problems such as distortion of color distribution (Li, Feng, Boulkenafet, Xia, & Li, 2016), vagueness, Moire effect, etc. This kind of method is weak in discriminating different classes of fake faces across datasets and usually requires high-quality images as input. The rPPG-based methods improve the detection effect by combining the rPPG signals and the features extracted by neural networks (Hernandez-Ortega et al., 2018), but this type of method is susceptible to interference from illumination and requires good constant lighting conditions. Spatial-temporal information-based methods are used for face spoofing detection by fusing temporal and spatial information (Asim et al., 2017), and this type of method can improve the resistance ability for print and replay attacks. However, since two different features are utilized in this type of method, the number of parameters and computation costs are increased heavily.

Although a variety of methods have been proposed for face spoofing detection, there are still problems such as poor generality across datasets, a large number of parameters, and the effectiveness susceptible to illumination conditions. The problem of illumination conditions is inspired by the study of Retinex theory. To address the above issues, we propose a multi-scale color inversion dual-stream convolutional neural network (MSCI-DSCNN) which consists of an MSCI stream and an RGB stream. The MSCI stream is used to extract the face reflection features and the RGB stream is applied to extract the face color features. Finally, these two kinds of features are integrated adaptively for face anti-spoofing. The main contributions of this paper are as follows:

(1) A multi-scale color inversion algorithm is proposed to reduce the sensitivity to illumination variation and increase the difference between real and fake faces;
(2) Improving the MobileNet to make it more suitable for face spoofing detection;
(3) Designing and introducing a paralleled convolutional block attention module (PCBAM) into the improved MobileNet to promote the integration of spatial attention and channel attention;
(4) The proposed method has been extensively evaluated in three publicly available databases, and the experimental results show the effectiveness of MSCI-DSCNN. In addition, we also conduct cross-database tests and obtain satisfactory results, indicating that the proposed MSCI-DSCNN has strong generality.

Traditional machine learning-based methods

Traditional methods usually use hand-crafted features for face spoofing detection, mainly including texture-based methods and physiological information-based methods.
Firstly, in terms of texture feature-based methods, Chingovska et al. (Chingovska et al., 2012) studied texture features based on local binary pattern (LBP) and its effects on three types of attacks. Zhang et al. (Zhang & Xiang, 2020) proposed to horizontally connect the LBP histograms of the discrete wavelet transform (DWT) blocks

METHODOLOGY

Although deep learning methods are capable of extracting high-level semantic features, the detection performance is greatly affected by illumination variations because most of the existing face spoofing detection methods are for visible light images. In practical applications, the illumination conditions are not constant, and according to the Retinex theory, we propose a new solution for the changing illuminations, which consists of a dual-stream deep convolutional neural network. Firstly, the

EXPERIMENTS

The proposed MSCI-DSCNN is trained and tested on a PC with a GTX 1080 Ti GPU using the Tensorflow toolbox. First, we briefly introduce the three publicly available benchmark databases, including OULU-NPU (Boulkenafet, Komulainen, Li, & Feng, 2017), REPLAY-ATTACK (Chingovska et al., 2012), and CASIA-FASD (Zhang et al., 2012). Next, we describe the evaluation metrics. Finally, we present our experimental results on the three datasets, including intra-dataset results and cross-dataset results.

CONCLUSION

In this paper, we propose a dual-stream convolutional neural network termed multi-scale color inversion dual-stream convolutional neural network (MSCI-DSCNN) for face spoofing detection under changing illumination conditions. To enable the network to extract more discriminative reflection features, we propose the multi-scale color inversion (MSCI) method and embed it into one stream of the model.

REFERENCES

- L. Birla *et al.* **PATRON: Exploring respiratory signal derived from non-contact face videos for face anti-spoofing** **Expert Systems with Applications** (2022)
- H.-H. Chang *et al.* **Face anti-spoofing detection based on multi-scale image quality assessment** **Image and Vision Computing** (2022)
- V.L. da Silva *et al.* **Residual spatiotemporal convolutional networks for face anti-spoofing** **Journal of Visual Communication and Image Representation** (2023)
- R. Huang *et al.* **Face anti-spoofing using feature distilling and global attention learning** **Pattern Recognition** (2023)

- Y.A.U. Rehman *et al.* **SLNet: Stereo face liveness detection via dynamic disparity-maps and convolutional neural network** **Expert Systems with Applications** (2020)
- C. Wang *et al.* **A Learnable Gradient operator for face presentation attack detection** **Pattern Recognition** (2023)
- C. Wang *et al.* **An adaptive index smoothing loss for face anti-spoofing** **Pattern Recognition Letters** (2022)
- W. Zhang *et al.* **Face anti-spoofing detection based on DWT-LBP-DCT features** **Signal Processing: Image Communication** (2020)
- A. Alotaibi *et al.* **Deep face liveness detection based on nonlinear diffusion using convolution neural network** **Signal, Image and Video Processing** (2017)