JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

FACE ANTI-SPOOFING BY COMBINING HIGH- AND LOW-FREQUENCY CHARACTERISTICS FOR SUPERIOR GENERALISATION POWER

[1]G.V.Vinod,[2]V.Rakesh,[3]D.PavanKumar,[4]V.Mahesh,[5]V.VarunDev
[1]**AssistantProfessor,** Dept of ECE, Godavari Institute of Engineering and Technology(A),Rajahmundry,AP
[2,3,4,5]**Students,** Dept of ECE, Godavari Institute of Engineering and Technology (A),Rajahmundry,AP

Abstract-In this work, In order to solve the face anti-spoofing problem, we propose a novel framework based on the Convolutional Neural Network (CNN) and the Recurrent Neural Network (RNN), which is motivated by the way humans decide whether a given face example is real or fake: by quickly scanning the entire face to get a sense of its overall appearance and then examining its local features in detail to pick out subtle differences (RNN). To be more precise, we apply deep reinforcement learning to characterise the action of exploring face-spoofing-related information in image sub-patches. We also create a recurrent approach to gradually train RNN representations of local information from the investigated sub-patches. In the end, we use a convolutional neural network (CNN) to learn both the local and global features of the input image, and then combine them to make a classification decision. We also conduct extensive experiments on a variety of open-source datasets, including an ablation study and a visualisation analysis, to further evaluate our suggested technique.

The results of our experiments reveal that our method is superior to the state-of-the-art since it achieves state-of-the-art performance in every scenario tested.

Keywords: FACE ANTI-SPOOFING CNN, rPPG, RNN, SVM.

1. INTRODUCTION

Improvements have been made in recent years on the FAS front. In the past, a Support Vector Machine (SVM) was taught to tell the difference between real and fake samples by using features collected from images using a number of methods that either worked in Spatial or Fourier space and relied on picture descriptors as representations. Nevertheless, the descriptors used to identify these features (such as Local Binary Pattern) were not created with the FAS problem in mind, hence they are not sufficiently discriminative. Recent studies have shown that deep learning-based solutions, which aim to construct discriminative representations in an end-to-end fashion, are superior to traditional countermeasures for spoofing assaults. Convolutional neural networks (CNNs) are initially introduced by Yang et al. addressing the FAS issue. They use features collected from the last layer of the Alex Net-based model to train a support vector machine (SVM) to categorise occurrences into one of two groups ('genuine' or'spoofing') [8]. To augment traditional binary labels, Liu et al. [9] search for additional supervisory signals. The use of supplementary approaches, such as the creation of pseudo depth maps and the transmission of supervision signals through remote Photo Plethysmo Graphy (rPPG) from the underlying RGB images, greatly aids in their training. Anti-spoofing

methods that use the Recurrent Neural Network (RNN) have been shown [10, 11], and these methods make use of temporal information from subsequent frames. Whereas these approaches offer numerous benefits, there is a potential drawback: the learned feature representations may overfit to the features of a certain database. Whereas depth information may help with face anti-spoofing when the suspicious input is in 2D format (such a printed photo or a screen display), it is not likely to be helpful against mask attacks, which need 3D information. There has been significant progress in the field of FAS in recent years. Generally, features are retrieved using one of many well-established approaches, either in the Spatial or Fourier space, and then a Support Vector Machine (SVM) is trained to differentiate between real and faked instances. Local Binary Pattern and other similar descriptors were not designed with the FAS problem in mind, hence they cannot be depended upon to offer enough discrimination. New studies have shown that deep-learning-based solutions are more effective than traditional methods in protecting against spoofing attacks because they train discriminative representations in an end-to-end fashion. Convolutional neural networks (CNNs) are initially introduced by Yang et al. addressing the FAS issue. They use features collected from the last layer of the Alex Net-based model to train a support vector machine (SVM) to categorise occurrences into one of two groups ('genuine' or'spoofing') [8]. To augment traditional binary labels, Liu et al. [9] search for additional supervisory signals. The use of supplementary approaches, such as the creation of pseudo depth maps and the transmission of supervision signals through remote Photo Plethysmo Graphy (rPPG) from the underlying RGB images, greatly aids in their training. Although these approaches have several benefits, including the ability to use temporal information from consecutive frames for face anti-spoofing [10, 11], there is one drawback: the trained feature representations may overfit to the properties of a particular database. Although depth information may help with face anti-spoofing when the suspicious input is in a 2D format (such a printed photo or a screen display), it is not likely to be helpful against mask attacks, which need 3D information.

2. LITERATURE REVIEW

Anil K. Jain, Arun Ross and Salil Prabhakar In this article, we will provide an introduction to the study of biometrics and briefly discuss its potential benefits, drawbacks, strengths, limits, and associated privacy issues. Biometric systems are basically pattern recognition systems that work by collecting biometric data from a person, analysing that data to generate a feature set, and then comparing that feature set to a stored template set. Since they depend on fictitious tokens or representations of the person's identity, the standard knowledge-based and token-based techniques do not give genuine personal recognition. Hence, it is clear that a biometric component is required in any system that guarantees accurate personal recognition. Security and privacy may require a reasonable compromise. The market, the technology, and the applications of biometrics will all become more intertwined as the field develops[1].

Fessi B A, Ben Abdallah, S, Hamdi Mand BoudrigaBoth AI and cybersecurity are addressed in this study. Introduces a novel genetic algorithm-based decision model for intrusion response systems (NGAA-IRS). Brief histories of IDRS (intrusion detection and response system) and GA (and its use in IDRS) are described. The parameters of the intrusion response system and the evolution process for the GA are then detailed in depth, along with the novel genetic algorithm technique. The model is distinguished by its cost-benefit-based fitness function and a novel implementation of individual structure based on a matrix of response-resource elements. The NGAA-IRS model is the only one that can make use of these capabilities; they have not been employed in any other systems so far[2].

Qinghan XiaoThe fast progress of wireless technology has led to the creation of several mobile gadgets with both military and civilian uses. Because of the need for mobility, ad hoc networks are attracting more attention in the defence industry's R&D sector. In coalition operations, peer-to-peer architecture is useful for mobile communication. With no need for a central server, users may send data anywhere in the world over the Internet. A unique

difficulty arises with ad hoc networks, however, since user authentication is often handled by an authentication server. To address the issue of insufficient data protection in ad hoc networks, we provide a biometric authentication approach. In this framework, a peer's biometric information is used to verify their identity before they are allowed to join an existing group, and this occurs even in the absence of an authentication server[3].

B Ananda Krishna, S Radha and K Chenna Kesava Reddy Ad hoc networks are a novel kind of wireless networking for hosts that are themselves mobile. While there is a trend towards adopting ad hoc networks for commercial usage owing to their unique qualities, the primary applications of ad hoc networks remain in the military for tactical and other security-sensitive activities. How to practically identify and fight against the key assaults on data, impersonation, and unauthorized data change is one of the biggest challenges in designing these networks. There might be malevolent nodes in the network, whose only purpose is to slow things down for everyone else. With our proposed security model, packets are encrypted and decrypted using a variety of techniques, with the key being chosen at random. By careful analysis of the suggested model's performance, we find that it incurs no additional control overhead but does experience a little delay as a result of the encryption procedure. We conclude that the suggested security model is effective for highly mobile, extensively used networks, and may be extended to accommodate other cryptographic methods[4].

A. Jagadeesan, T. Thillaikkarasi, Dr. K. DuraiswamyIncreasing recognition accuracy by combining data from many biometric modalities, multimodal biometrics fusion approaches have attracted a lot of attention. Bringing together cryptography and biometrics is a win-win situation, capitalising on the best features of both. Effective method for producing a safe cryptographic key that relies on multimodal biometrics (Iris and fingerprint) and the difficulty of factoring huge integers. At first, fingerprint and iris pictures are parsed for characteristics; next, points of interest and textural qualities are retrieved. The multi-biometric template is constructed by first fusing the retrieved features at the feature level. In the end, a 256-bit cryptographic key is generated using a multi-biometric template. The produced 256-bit cypher key may improve security and user authentication[5].

3.EXISTING SYSTEM

Existing systems use a plethora of algorithms and approaches for recognition; nevertheless, the new solution was about 5 times quicker than the quickest traditional Face matching algorithms.It may also be used as a rapid matching approach to speed up the process in identification jobs by removing numerous templates with low scores by establishing a threshold based on the matching scores.

4. PROPOSED SYSTEM

There were a plethora of recognition algorithms and techniques employed in the proposed system, but LSTM face matching algorithms made up the bulk of the work.

Furthermore, by adjusting the threshold based on the matching scores, it may be used as a speedy matching technique to expedite the identification process by eliminating a large number of templates that have low scores.Enhancing Performance Analysis.

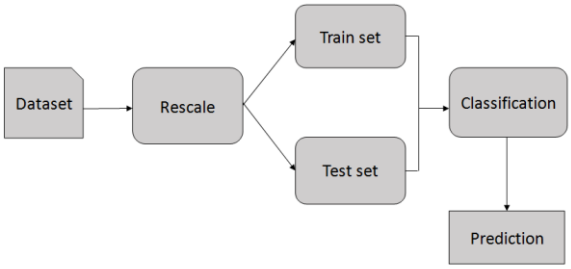
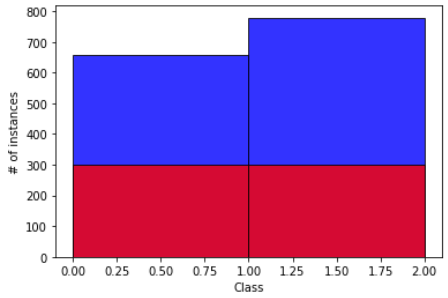
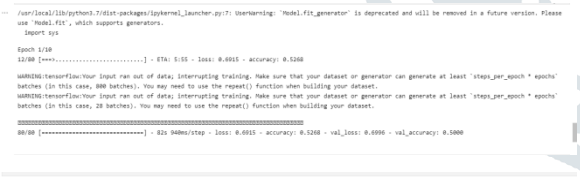


Fig1: Block Diagram of Proposed Method

5. RESULTS



Layer (type)	Output Shape	Param #
conv2d (Conv2D)	(None, 126, 126, 32)	896
max_pooling2d (MaxPooling2D)	(None, 63, 63, 32)	0
conv2d_1 (Conv2D)	(None, 61, 61, 64)	18496
max_pooling2d_1 (MaxPooling2D)	(None, 30, 30, 64)	0
conv2d_2 (Conv2D)	(None, 28, 28, 128)	73856
max_pooling2d_2 (MaxPooling2D)	(None, 14, 14, 128)	0
flatten (Flatten)	(None, 25088)	0
dense (Dense)	(None, 256)	6422784
dense_1 (Dense)	(None, 1)	257



6. CONCLUSION

We provide an innovative two-pronged methodology for investigating face anti-spoofing evidence. Our work is innovative in two ways: 1) we offer the first effort at applying deep reinforcement learning to optimise the FAS issue, and 2) we suggest the use of convolutional and recurrent neural networks to extract both global and local information for the FAS task from a single frame. We conduct extensive tests on six separate data sets to evaluate the performance of our suggested method. It has been shown experimentally, both inside and across domains, that our proposed framework can achieve state-of-the-art performance when compared to a variety of state-of-the-art baselines.

REFERENCES

[1] Maltoni D, Maio D, Jain AK, Prabhakar S (2009) Handbook of fingerprint recognition. Springer, London

[2] Hong L, Wan Y, Jain AK (1998) Fingerprint image enhancement: algorithm and performance evaluation. IEEE Trans Pattern Anal Mach Intell 20(8):777–789

[3] Jain AK, Hong L, Bolle R (1997) On-line fingerprint verification. IEEE Trans Pattern Anal Mach Intell 19(4):302–314

[4] Feng J, Jain AK (2011) Fingerprint reconstruction: from minutiae to phase. IEEE Trans Pattern Anal Mach Intell 33(2):209–223

[5] Bazen AM, Verwaaijen GTB, Gerez SH, Veelenturf LPJ, Van der Zwaag BJ (2000) A correlation-based fingerprint verification system. In: Proceedings of the ProRISC2000 workshop on circuits, systems and signal processing, pp 205–213

[6] Bazen AM, Gerez SH, Veelenturf L, Zwaag BV, Verwaaijen G (2000) A correlation-based fingerprint verification system. Stw Technology Foundation 31(5):652–655

[7] Ross A, Reisman J, Jain AK (2002) Fingerprint matching using feature space correlation. International Workshop Copenhagen on Biometric Authentication 2359:48–57

[8] Cavusoglu A, Gorgunoglu S (2007) A robust correlation based fingerprint matching algorithm for verification. J Appl Sci 7(21):3286–3291