COMPUTATIONAL INTELLIGENCE AND MACHINE LEARNING
e-ISSN: 2582-7464

Computational Intelligence and Machine Learning
Vol-4, Issue-1, April 2023

Liveness Identity Verification for Face Anti-Spoofing in Biometric Validation using Recurrent Neural Network

P.Maragathavalli [1*], J.Sharmila [2], Syed Abdul Kareem [3], Nekkanti Bhavitha [4]

[1] Assistant Professor, Information Technology, Puducherry Technological University, Puducherry, India
[2, 3, 4] B.Tech Student, Information Technology, Puducherry Technological University, Puducherry, India
*Corresponding Author Email: marapriya@ptuniv.edu.in

Abstract

Face anti-spoofing is the task of preventing false facial verification by using a photo, video, mask or a different substitute for an authorized person's face. It has become an increasingly important and critical security feature for authentication systems, due to rampant and easily launchable presentation attacks. However, most previous approaches still suffer from diverse types of spoofing attacks, which are hardly covered by the limited number of training datasets, and thus they often show the poor accuracy when unseen samples are given for the test. To address this problem, a novel method is proposed based on liveness identity verification for face anti-spoofing in biometric validation using the Recurrent Neural Network (RNN).

Keywords

Biometric Validation, Face Anti-Spoofing Identification, Face Liveness Detection, Face Recognition, Lightweight CNN, Machine Learning, RNN.

INTRODUCTION

Faces can be captured conveniently by digital cameras, web cameras, smart phones, etc. The convenience is a double edged sword. It makes faces become not only the most widely used but also the most untrustable biometric modality. With the fast development of face recognition, the modern face recognition algorithms, especially deep networks trained on large scale datasets, can surpass human performance, but they may be easily fooled by face spoofing attacks which can be easily launched by inexperienced attackers. It is noteworthy that the proposed method only requires live facial images for training the model by using Recurrent Neural Network (RNN), which are easier to obtain than fake ones, and thus the generality power for resolving the problem of face anti-spoofing can be expected to be improved. Experimental results on various benchmark datasets demonstrate the efficiency and robustness of the proposed method.

MOTIVATION

Face recognition on our mobile phones facilitates - Unlocking the device, Conducting financial transactions , Access to privileged content stored on the device. Failure to detect spoof attacks on smartphones could compromise confidential information such as emails, banking records, social media content, and personal photos. Biometric verification is a crucial activity in bank locker security system where the spoofing attack cannot be tolerated. Face-Anti Spoofing is used to minimize the fraudulent activities in the virtual interviews, online classes, online examinations where some unauthorized persons indulge in the activity of doing mal-practices.

LITERATURE SURVEY

S.No	NAME OF THE JOURNAL, YEAR	PAPER TITLE	JOURNAL DETAILS	TECHNIQUES USED	DEMERITS
1.	IEEE Transactions on Information Forensics and Security,2021	DRL-FAS: A Novel Framework Based on Deep Reinforcement Learning for Face Anti-Spoofing	R. Cai, H. Li, S. Wang, C. Chen and A. C. Kot, "DRL-FAS: A Novel Framework Based on Deep Reinforcement Learning for Face Anti-Spoofing," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 937 951,2021,doi:10.1109/TIFS.2020.3026553.	Face anti-spoofing, deep learning, reinforcement learning.	Live video identification is not done
2.	IEEE Journal ,2020	A Face Spoofing Detection Method Based on Domain Adaptation and Lossless Size Adaptation	W. Sun, Y. Song, H. Zhao and Z. Jin, "A Face Spoofing Detection Method Based on Domain Adaptation and Lossless Size Adaptation," in IEEE Access, vol. 8, pp. 66553-66563, 2020,doi:10.1109/ACCESS.2020.2985453.	Domain adaptation, face anti-spoofing, face liveness detection, face presentation attack detection, face spoofing detection, forensics, machine learning, pattern recognition.	This kind of attacks is less prevalent as compared to the photo attacks and the video attacks since it is relatively difficult to make a mask.3D mask attacks are usually not included in common face spoofing detection datasets.
3.	IEEE Journal ,2020	One-Class Learning Method Based on Live Correlation Loss for Face Anti-Spoofing	S. Lim, Y. Gwak, W. Kim, J. -H. Roh and S. Cho, "One-Class Learning Method Based on Live Correlation Loss for Face Anti-Spoofing,"in IEEE Access, vol. 8, pp. 201635-201648, 2020, doi: 10.1109/ACCESS.2020.3035747.	Biometric authentication systems, face anti-spoofing, one-class learning, live correlation loss, feature correlation network.	Complexity level is high
4.	IEEE Transactions on Information Forensics and Security,2021	Camera Invariant Feature Learning for Generalized Face Anti-Spoofing	B. Chen, W. Yang, H. Li, S. Wang and S. Kwong, "Camera Invariant Feature Learning for Generalized Face Anti-Spoofing," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 2477-2492, 2021, doi: 10.1109/TIFS.2021.3055018.	Face anti-spoofing, camera invariant, deep learning, generalization capability.	Image attacks are only identified and 3D mask attacks are usually not included in common face spoofing detection datasets.

Table 1. Literature Survey of the Existing Work

LIMITATIONS IN THE EXISTING SYSTEM

Generalizability

Since the exact type of spoof attack may not be known beforehand, how to generalize well to unknown 2D attacks is of utmost importance. A majority of the prevailing

state-of-the-art face anti-spoofing techniques focus only on detecting 2D printed paper and video replay attacks, and are vulnerable to spoofs crafted from materials not seen.

Lack of Interpretability

Given a face image, face anti-spoofing approaches typically output a holistic face "spoons score" which depicts the likelihood that the input image is live or spoof. Without an ability to visualize which regions of the face contribute to the overall decision made be the network, the global spoons score alone is not sufficient for a human operator to interpret the network's decision.

PROPOSED SYSTEM

Input

In this system, image acquisition is done and the 2C images is converted to 3D format. It helps us to collect more details about the affected region in the image. Pickle Dataset is used in this Proposed system Liveness Identity Verification For Face Anti-Spoofing. Pickle in Python is primarily used in serializing and deserializing a Python object structure. It is the process of converting a Python object into a byte stream to store it in a file or database, maintain program state across sessions, or transport data over the network. At first Python pickle serialize the object and then converts the object into a character stream so that this character stream contains all the information necessary to reconstruct the object in another python script. Liveness Detection is carried out here by capturing the face of the person using integrated camera and with that dataset the various frames are generated and stored.

Process

A novel framework based on RNN for the FAS problem is proposed here. While many of the previous works used RNN to leverage temporal information from video frame. We use the advantage of RNN to memory information to reinforce extracted local features gradually. The collected data is then reduced by using 3D Discrete Cosine Transformation (DCT).Extraction of the facial characteristics is done by stemmer based feature extraction method. Feature extracted are reduced with the XGBoost Feature Reduction Technique by using the frames already generated which have the sequence of images of the person.

Output

The classifier that is used in the system is Recurrent Neural Network. The approach expected to provides the best-estimated accuracy of around 97% which identifies whether the person is authorized genuine person or the unauthorized spoof person.

FEATURES

Human Face is detected and characteristics are identified. Biometric validation of human traits with the Dataset. Stemmer Feature Extraction to reduce the dimensionality of the image.

XGBoost Feature Reduction for determining the results. 97% of accuracy in identification of spoofing attack.

DESIGN DIAGRAM

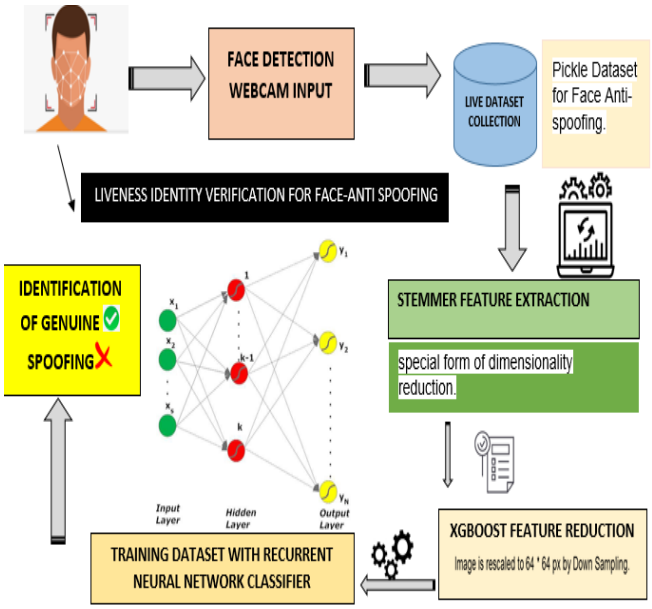


Figure 1. Detailed Design Diagram

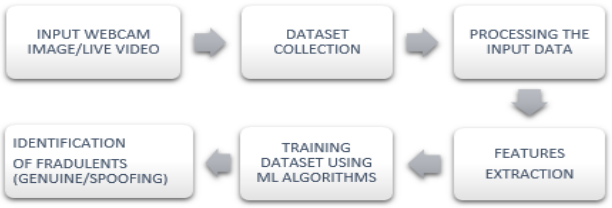


Figure 2. Process Flow Diagram

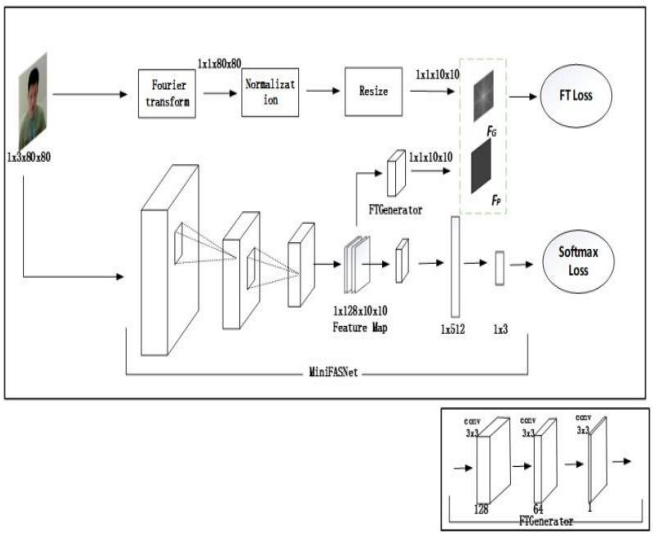


Figure 3. Recurrent Neural Network Architecture

RESULT ANALYSIS

Generating Frames

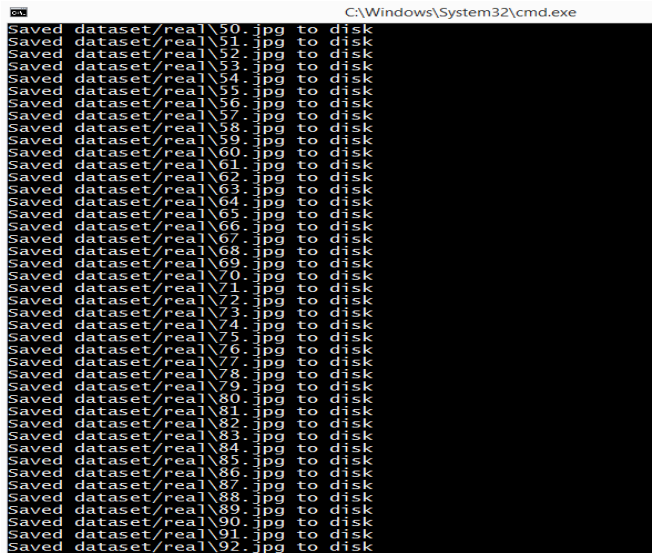


Figure 4. Frames Generation Results for Real and Fake Video Dataset

Training Model

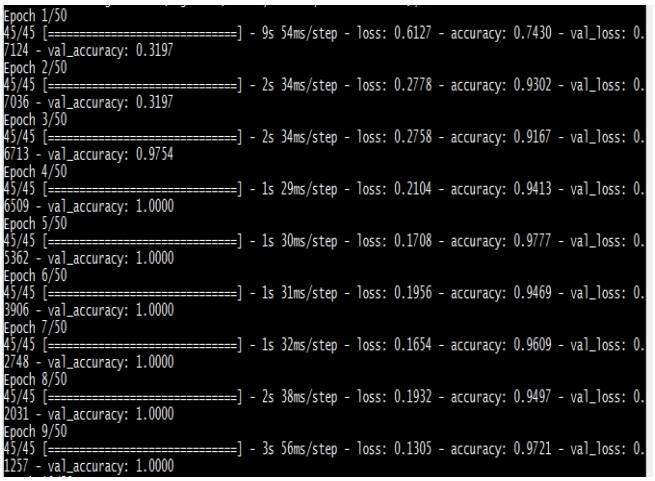


Figure 5. Training Results of FAS Identification Model

Training Loss & Accuracy on Dataset

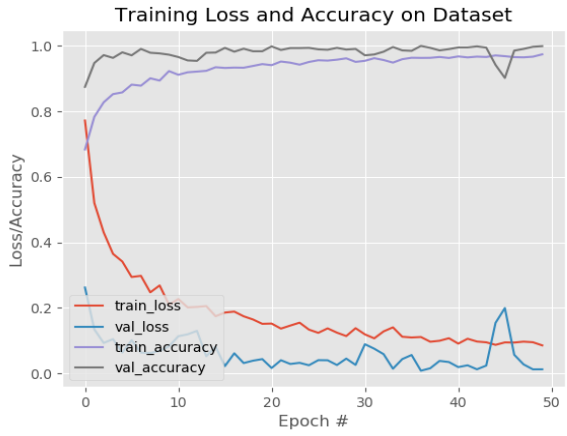
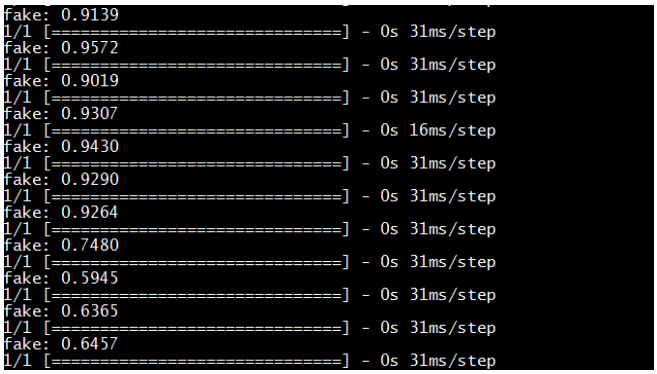


Figure 6. Validation and Testing Accuracy of FAS Model

Identification of Face Anti-Spoofing



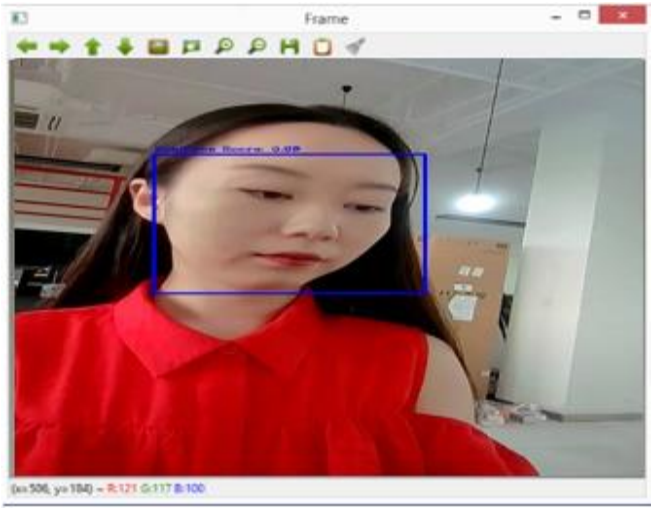
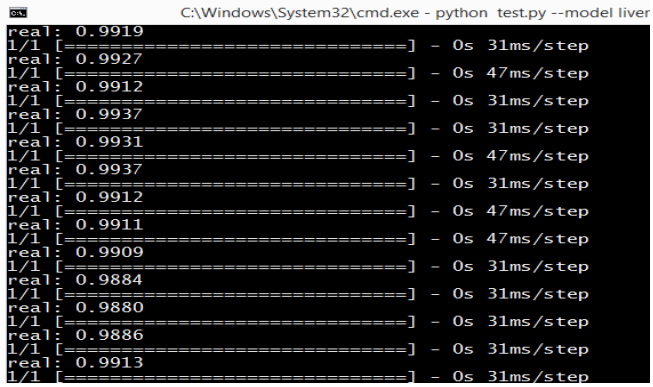


Figure 7. Result for Identification of Real/Genuine Face



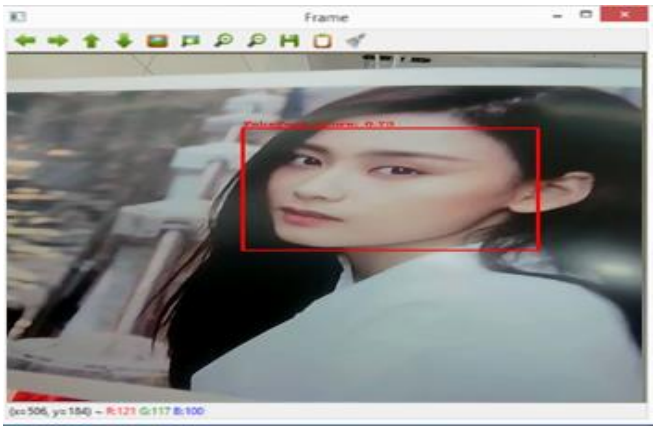


Figure 8. Result for Identification of Fake/Spoof Face

CONCLUSION

Under this face recognition approach, a user is required to take a special action called a challenge for liveness detection. The system ensures that required action was taken. Usually, a group of actions is required to make the model reliable. These actions can include smiles, expressions of emotions such as sadness, surprise or head movements. These interactions require significant time and are inconvenient for users. Face presentation attack detection is often considered as a binary classification task which results in over-fitting to the known attacks leading to poor generalization against unseen attacks. This system employs strengthen techniques enhance reputation price and execution time by using 3D DCT Descriptor for face recognition and stemmer feature extraction and XGBoost feature reduction techniques with the help of Recurrent Neural Network classifier to detect the person indulge in the fraudulent activities. The experimental results show that the proposed anti-spoofing framework can prevent diversity of face attacking forms, such as dim light, realistic face camouflage, static or motion pattern in the most effective way. This system serves for various domains such as it helps to identify the spoofing attack in bank locker security system, Virtual Interviews, Online classes, Online examinations and in the highly-secured authentication systems.

ACKNOWLEDGMENT

We are deeply indebted to Dr. P. Maragathavalli, Assistant Professor, Department of Information Technology, Puducherry Technological University, Puducherry, for her valuable guidance throughout the project work.

REFERENCES

[1] R. Cai, H. Li, S. Wang, C. Chen and A. C. Kot, "DRL-FAS: A Novel Framework Based on Deep Reinforcement Learning for Face Anti-Spoofing," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 937-951, 2021, doi: 10.1109/TIFS.2020.3026553.

[2] A Face Spoofing Detection Method Based on Domain Adaptation and Lossless Size Adaptation W. Sun, Y. Song, H. Zhao and Z. Jin, "A Face Spoofing Detection Method Based on Domain Adaptation and Lossless Size Adaptation," in IEEE Access, vol. 8, pp. 66553-66563, 2020, doi: 10.1109/ACCESS.2020.2985453.

[3] One-Class Learning Method Based on Live Correlation Loss for Face Anti-Spoofing S. Lim, Y. Gwak, W. Kim, J. -H. Roh and S. Cho, "One-Class Learning Method Based on Live Correlation Loss for Face Anti-Spoofing,"in IEEE Access, vol. 8, pp. 201635-201648, 2020, doi: 10.1109/ACCESS.2020.3035747.

[4] B. Chen, W. Yang, H. Li, S. Wang and S. Kwong, "Camera Invariant Feature Learning for Generalized Face Anti-Spoofing," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 2477-2492, 2021, doi: 10.1109/TIFS.2021.3055018.

[5] D. Deb and A. K. Jain, "Look Locally Infer Globally: A Generalizable Face Anti-Spoofing Approach," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1143-1157, 2021, doi: 10.1109/TIFS.2020.3029879.

[6] A. George and S. Marcel, "Learning One Class Representations for Face Presentation Attack Detection Using Multi-Channel Convolutional Neural Networks," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 361-375, 2021, doi: 10.1109/TIFS.2020.3013214.

[7] Data-Fusion-Based Two-Stage Cascade Framework for Multimodality Face Anti-Spoofing W. Liu, X. Wei, T. Lei, X. Wang, H. Meng and A. K. Nandi, "Data-Fusion-Based Two-Stage Cascade Framework for Multimodality Face Anti-Spoofing," in IEEE Transactions on Cognitive and Developmental Systems, vol. 14, no. 2, pp. 672-683, June 2022, doi:10.1109/TCDS.2021.3064679.

[8] Datasets:
https://www.kaggle.com/code/rspadim/reading-pickle-files
https://www.kaggle.com/datasets?search=face+anti+spoofing