EFFICIENT AND RECENT ADVANCES FOR FACE SPOOFING DETECTION USING CONVOLUTIONAL NEURAL NETWORK BASED FEATURE EXTRACTION

[1]M.Suganthi, [2]Dr. C. Akila

[1]Research Scholar, AP / CSE Department, Thamirabharani Engineering College,
Tirunelveli, Tamilnadu, India, sugi.mp@gmail.com
[2]AP / CSE, Anna University Regional Campus, Tirunelveli, akilavp@gmail.com

Abstract

Feature extraction plays an important role in the area of pattern recognition, machine learning and computer vision. The performance of visible light face recognition is limited by varying illumination conditions. Major factors affecting the recognition accuracy of the visible light in the face recognition system. So the face spoofing can easily occurred in the face recognition. Even though many face anti-spoofing methods have been proposed, they cannot generalize well on unforced attacks. In this proposed system, in order to recognize the face spoofing by Convolution Neural Network (CNN) based feature extraction is used to detect the fake faces.

Index Terms— Feature extraction, Convolution Neural Network (CNN).

I. Introduction

Traditional biometric identification is based on the chemical features of a person, such as hair, DNA and so on. Nowadays, more and more biometric intelligent recognition systems are used for security targets, such as face recognition, iris recognition, fingerprint recognition and so on. Compared with traditional biometric identification methods, intelligent biometric methods are more user-friendly and convenient. However, these systems can be easily spoofed without special anti-spoofing detections. Some sophisticated methods, such as video and mask, can be used to spoof face recognition systems. One of the most challenging problems in biometric systems is the identity of theft. These barriers hinder the popularity of biometric authentication systems, which means there is a strong need for reliable anti- spoofing systems. A huge number of methods have been carried out to solve this problem. These methods can be divided into two classes: hardware-based methods and software-based methods. Software-based methods have two mainstreams: intrusive and non-intrusive methods. Among these methods, face is a commonly used biometric feature as face images are easily accessible and there is much textural and color information in a face image. Face liveliness detection, a direct and convenient method, has a rapid development in recent years. Face liveliness detection is based on face detection system. After a face image is detected and preprocessed, different kinds of features in face image will be extracted and merged for judgment. Only real faces are accepted and sent for further authentication and processing. Photo attack is a main threat to face liveliness detection, since photos can be obtained easily and they look almost the same with live faces from a specific point of view. Other powerful attacks include video attack, mask attack, model attack and soon.

A spoofing attack occurs when a person tries to masquerade as someone else by falsifying data and thereby gaining illegitimate access and advantages. For instance, one can spoof a face recognition system by presenting a photograph, a video, a mask or a 3D model of a targeted person in front of the camera. While one can also use make-up or plastic surgery as other means of spoofing, photographs are probably the most common sources of spoofing attacks because one can easily download and capture facial images. Furthermore, the number of publications in the field is growing steadily and some publicly available databases have been released. Still, the field of non-intrusive anti-spoofing methods is rather immature, since there exist no consensus on the best spoofing detection practices and techniques and not that many standard databases to develop and test the algorithms for objective comparison. Typical countermeasure against spoofing is liveness detection that aims at detecting physiological signs of life such as eye blinking, facial expression changes, mouth movements, etc. Another existing countermeasure to spoofing attacks consists of combining face recognition with other biometric modalities such as gait and speech. Indeed, multi-modal systems are intrinsically more difficult to spoof than uni-modal systems. Some other attempts to counter face spoofing are basedon structure from motion to calculate the depth information.

While there is a significant number of works addressing e.g. pose and illumination variation problems in face recognition[1], the vulnerabilities to spoofing attacks were mostly unexplored until very recently when an increasing attention is started to be paid to this threat. A spoofing attack occurs when a person tries to masquerade as someone else e.g. by wearing a mask to gain illegitimate access and advantages. This work provides the first investigation in research literature on the use of dynamic texture for face spoofing detection. Unlike masks and 3D head models, real faces are indeed non-rigid objects with contractions of facial muscles which result in temporally deformed facial features such as eye lids and lips. Our key idea is to learn the structure and the dynamics of the facial micro-textures that characterize only real faces but not fake ones. Hence, we introduce a novel and appealing approach to face spoofing detection using the spatiotemporal (dynamic texture) extensions of the highly popular Convolutional Neural Network approach. We experiment with two publicly available databases consisting of several fake face attacks of different natures under varying conditions and imaging qualities. The experiments show excellent results beyond thestate-of-the-art.

II. Existing System

Biometrics offers a secure and convenient way for access control. Face biometrics is one of the most convenient modalities for biometric authentication due to itsnon-intrusive nature. Even though face recognition systems are reaching human performance in identifying persons in many challenging datasets, most face recognition systems are still vulnerable to presentation attacks (PA), also known as spoofing attacks. Merely presenting a printed a printed photo to print and replay attacks from different PAD databases. As per the ISO standard [3], presentation attack is defined as "a presentation attacks are defined as" a presentation to the biometric data captures subsystem with the goal of interfering with the operation of the biometric system". Presentation attacks include both ' impersonation' refers to attacks in which the attacker wants to be recognized as a different person, whereas in 'obfuscation' attacks, the objective is to hide the identity of the attacker. The biometric characteristic or object used in a presentation attack is known as presentation attack instrument (PAI).

Nowadays, face recognition has been used in many security occasions, but few of them have ability to distinguish real and fake faces. Besides, many researches on face liveliness detection mainly focused on intrusive methods, which are not user-friendly in practice. This paper proposes a novel non-intrusive face liveliness detection method based on the analysis of texture and color features. More specifically, this method adopts an improved local ternary pattern (LTP) [4] to classify the nearby pixels. Based on the face pixel analysis, the infinity norm of pixel matrices is added as new features. The effectiveness of feature selection has been validated by different kinds experiments on three challenging face anti- spoofing databases (NUAA, CASIA FASD and Replay-attack) [4]. This method reaches a compromise between number of features and accuracy, which means it also, works on embeddedsystems.

III. Proposed System

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation[3] and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining theprivacy.

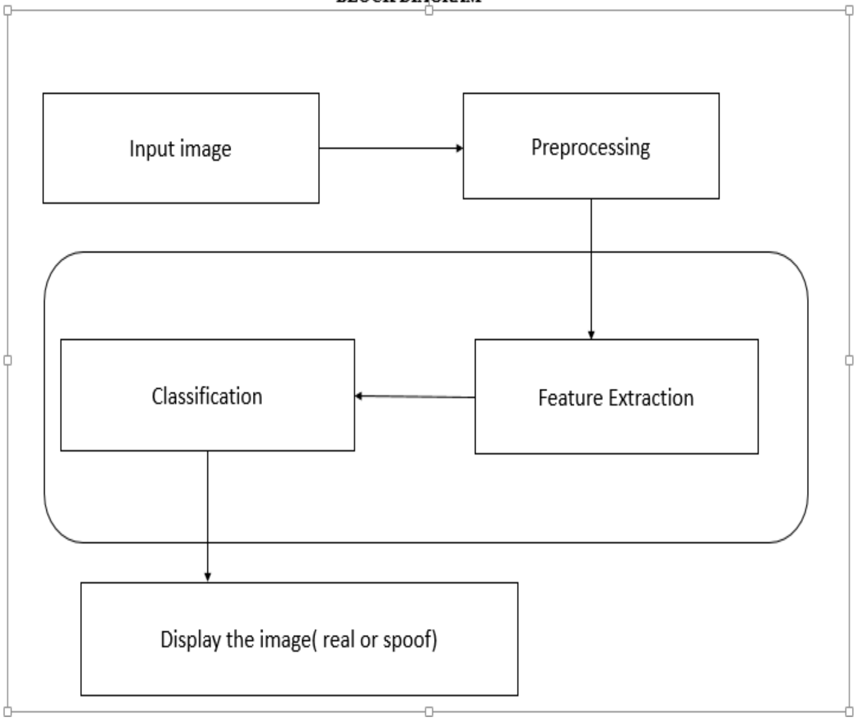
A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing [10] are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user.

Efficient and intelligent output design improves the system's relationship to help user decision-making.

Fig. 1 System Architecture

CNN (Convolutional Neural Network):

BLOCK DIAGRAM



Today, we will make an Image dehazingof our own utilization, which can recognize whether a given picture is of influenced or something different relying on your took care of information. To accomplish our objective, we will utilize one of the well known AI calculations out there which is utilized for Image Classification for example Convolutional Neural Network (or CNN) [1]. As we probably are aware it's an AI calculation for machines [11] to comprehend the highlights of the picture with foreknowledge and recall the highlights[9] to figure whether the name of the new picture took care of to the machine. The actual dataset (100 percentages) is classified into two types, train dataset (75 percentages), test dataset (25 percentages).

Presently subsequent to getting the informational collection, we need to pre-measure the information a piece and give results to every one of the picture given there during preparing the informational collection. A CNN have some layers, they are Convolutional layers, Activation or ReLU layers, Pooling layers, a fully connected layer. The convolutional layer is used to filter or resize into small size of the images. ReLU (Rectified Linear Unit), in this layer it takes only positive values only other non positive values are changed into 0.

IV Output Images

For Normal or Real Image:

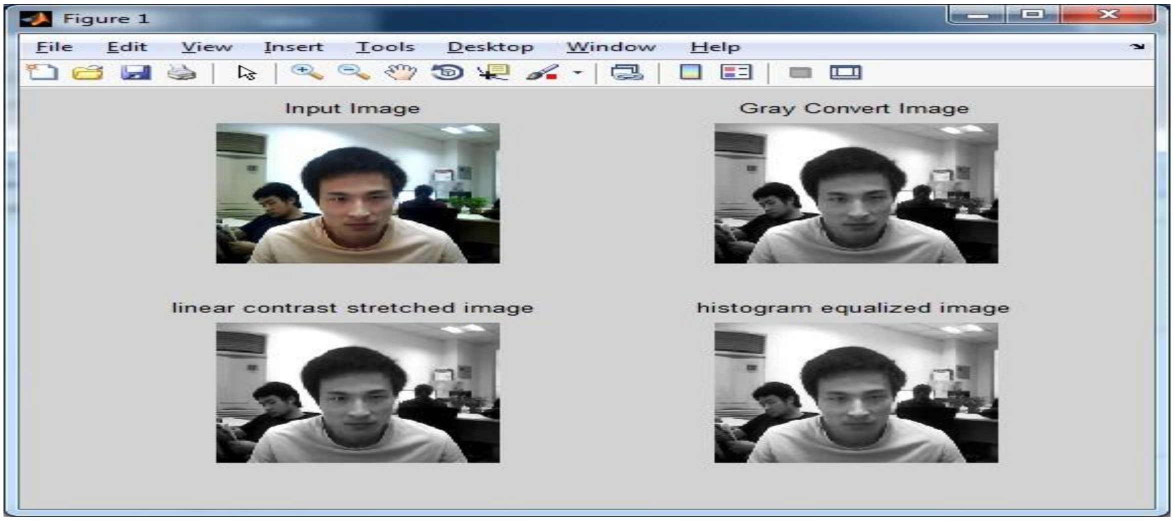


Figure 1
File Edit View Insert Tools Desktop Window Help
Input Image
Gray Convert Image
linear contrast stretched image
histogram equalized image

Fig. 2 Input (Real) Image, Gray Convert Image, Linear Contrast Stretched Image, Histogram Equalized Image

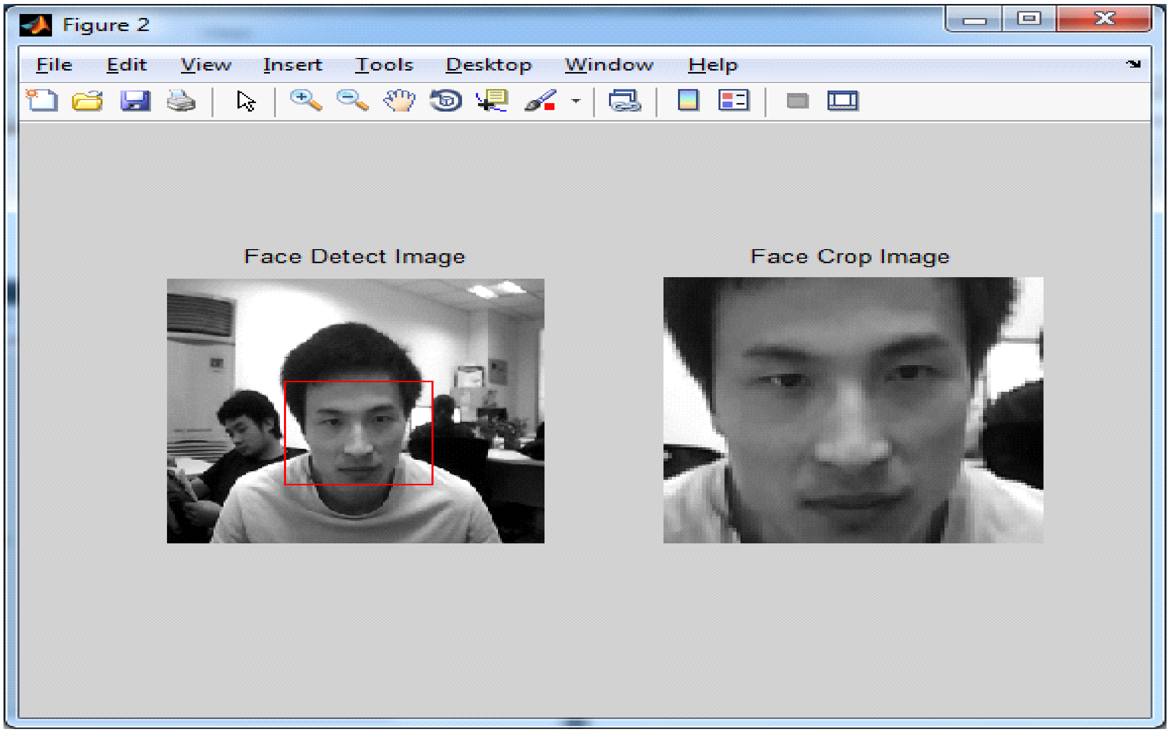


Fig. 3 Face Detect Image, Face Crop Image

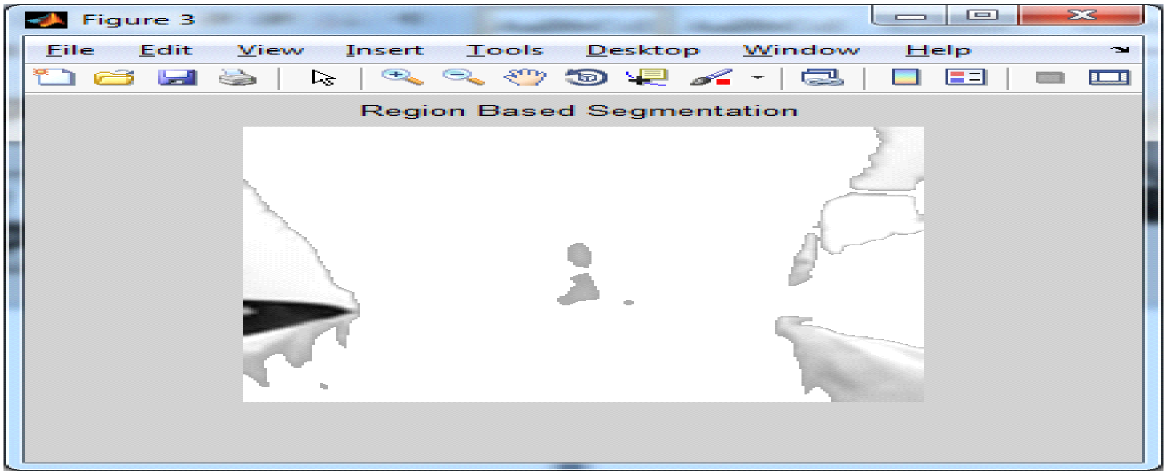


Figure 3
File Edit View Insert Tools Desktop Window Help
Region Based Segmentation

Fig. 4 Region Based Segmentation

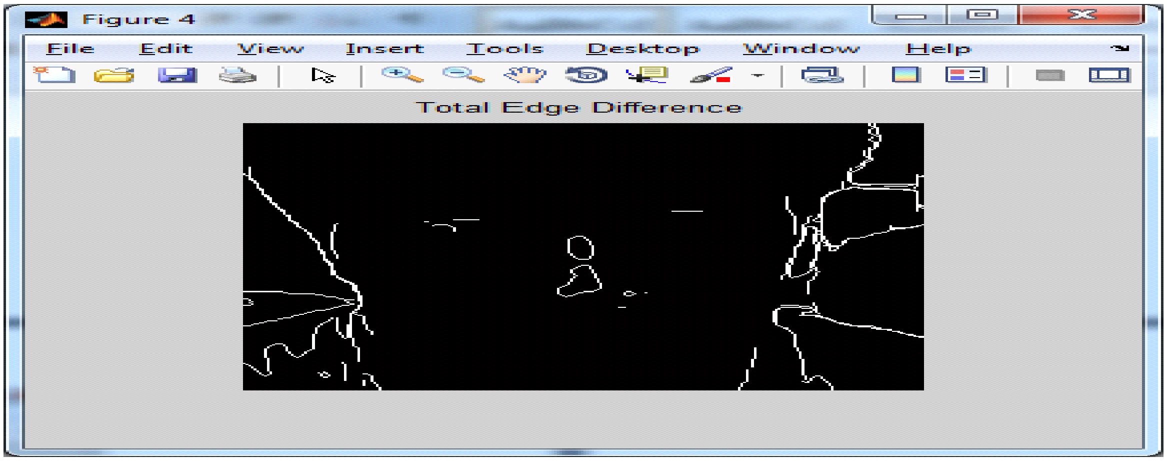


Fig. 5 Total Edge Difference

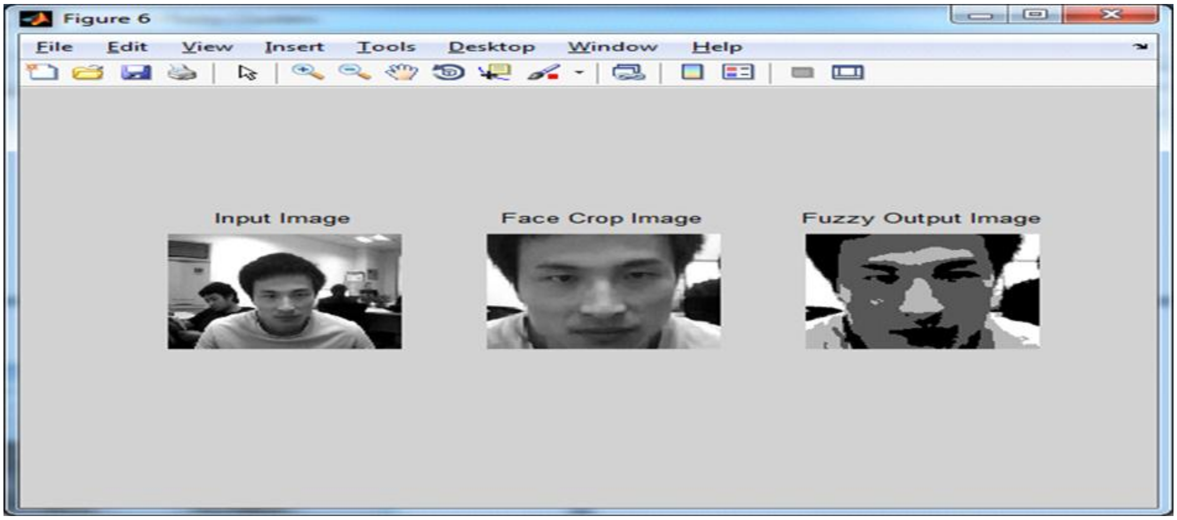


Fig. 6 Fuzzy Output Image

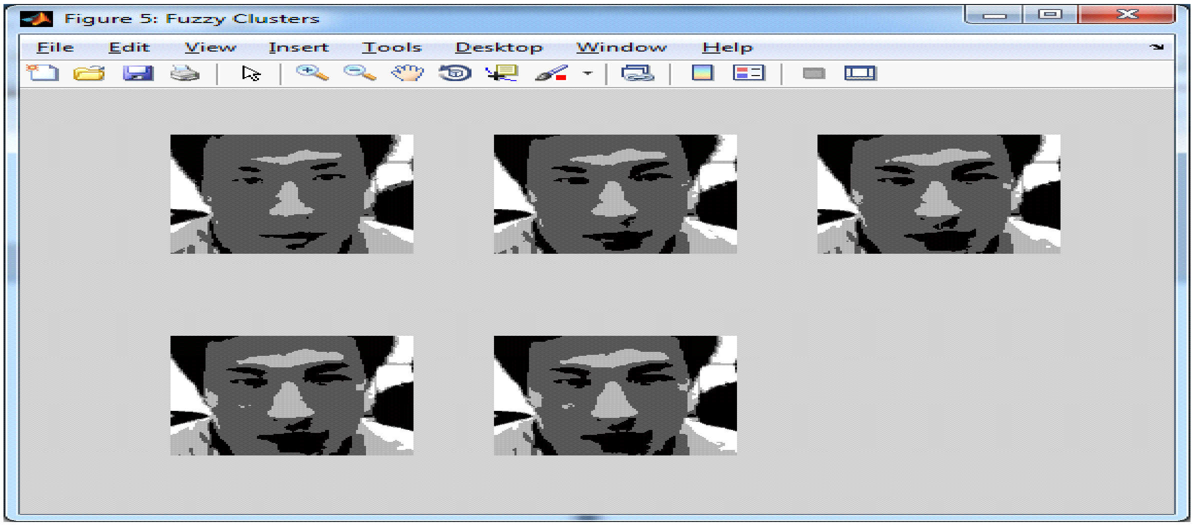
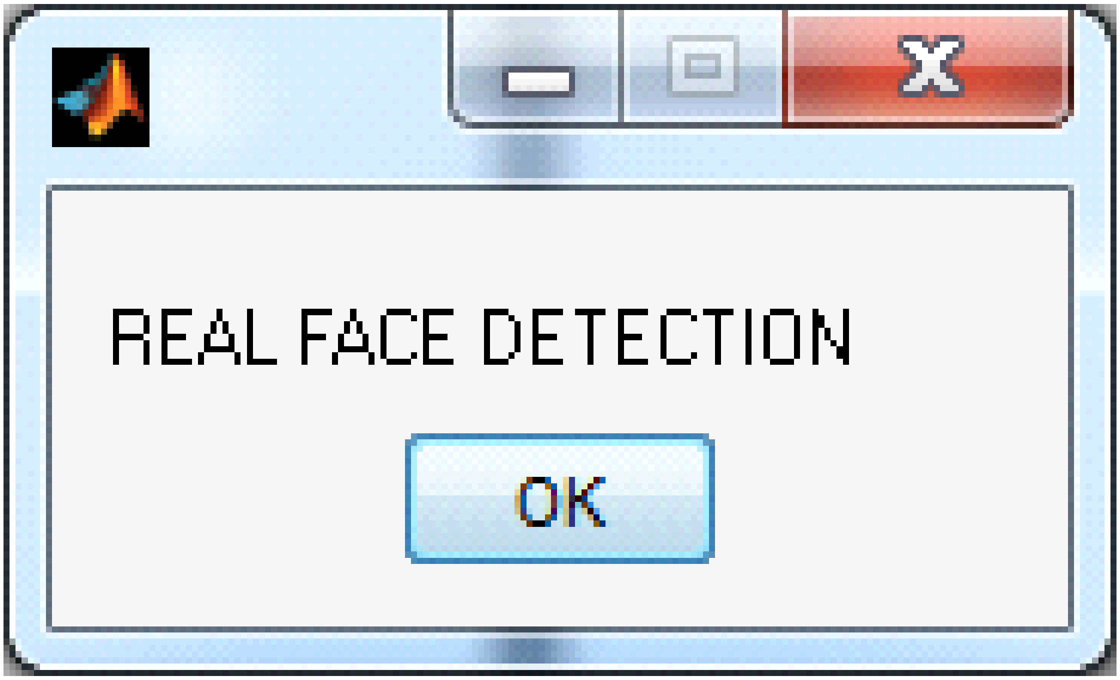


Fig. 7 Fuzzy Clusters



REAL FACE DETECTION

Fig. 8 Final Output for Real Image

For Spoofing Image:

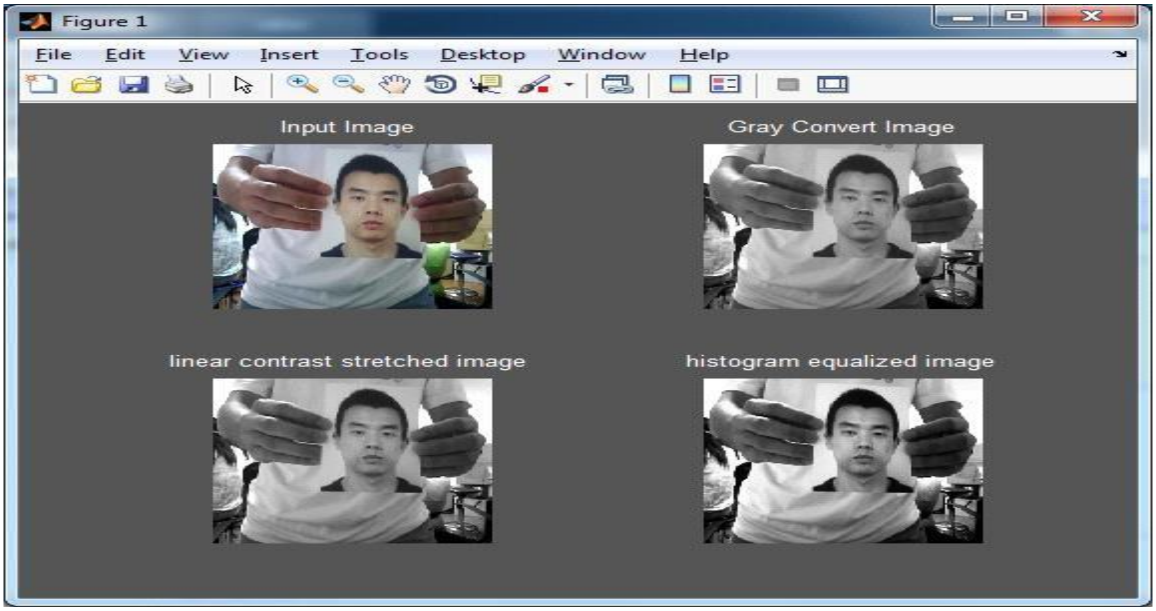


Figure 1
File Edit View Insert Tools Desktop Window Help
Input Image
Gray Convert Image
linear contrast stretched image
histogram equalized image

Fig. 9 Input (Spoof) Image, Gray Convert Image, Linear Contrast Stretched Image, Histogram Equalized Image

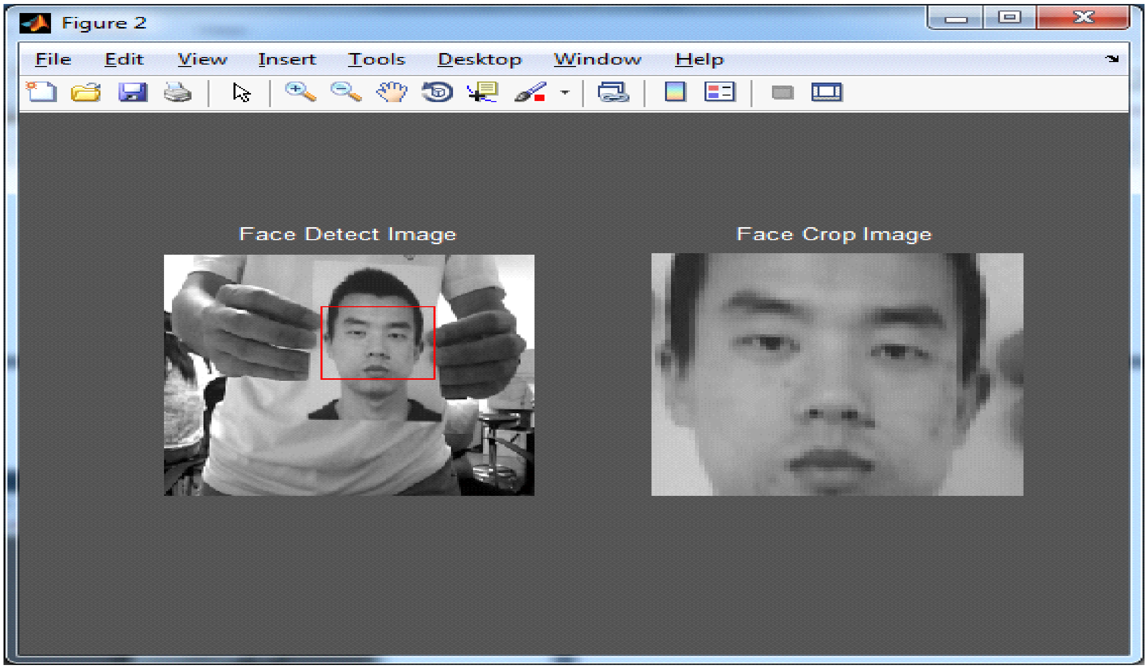


Fig. 10 Face Detect Image, Face Crop Image

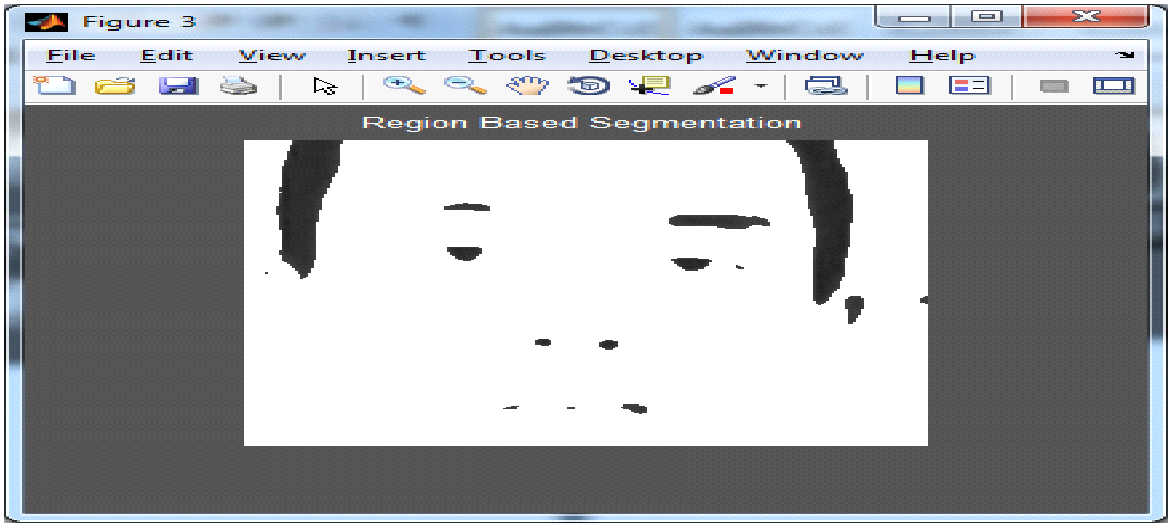


Figure 3
File Edit View Insert Tools Desktop Window Help
Region Based Segmentation

Fig. 11 Region Based Segmentation

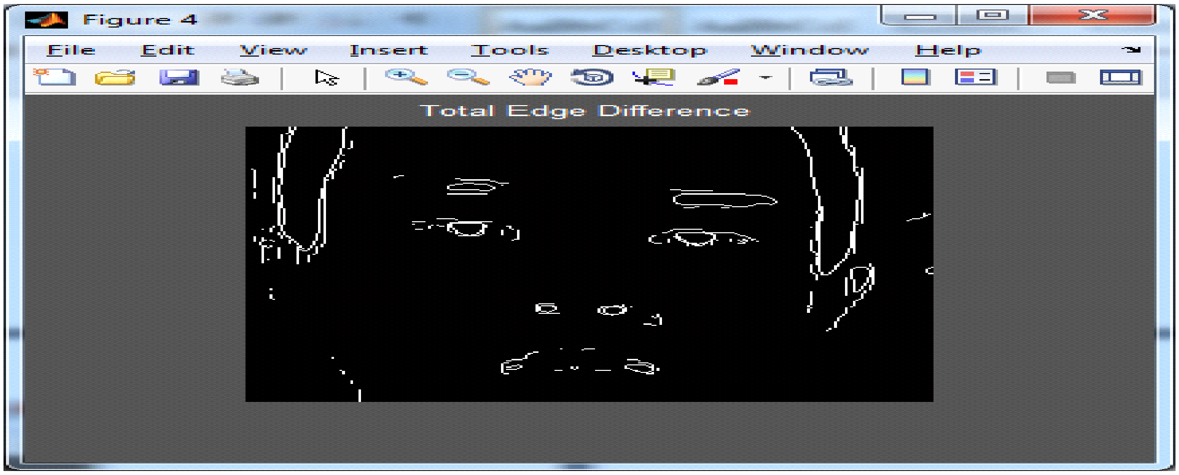


Fig. 12 Total Edge Difference

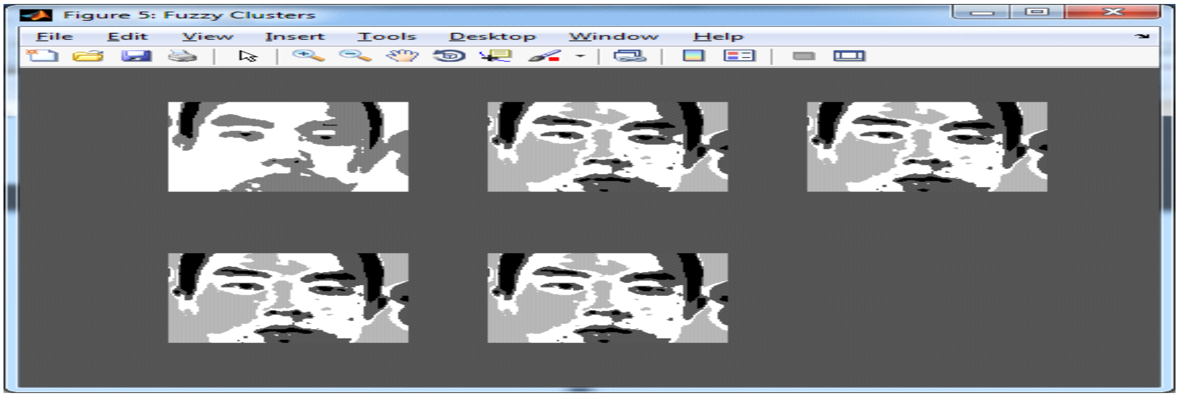


Fig. 13 FuzzyClusters

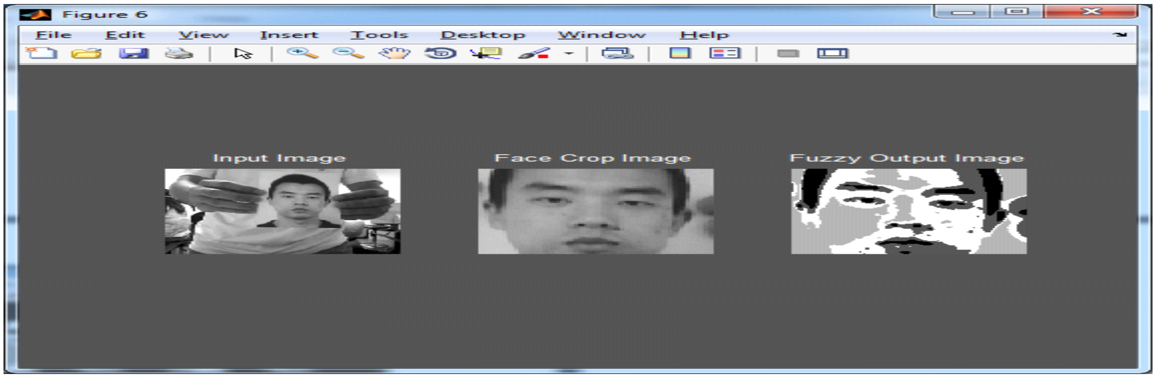


Fig. 14 Fuzzy Output Image

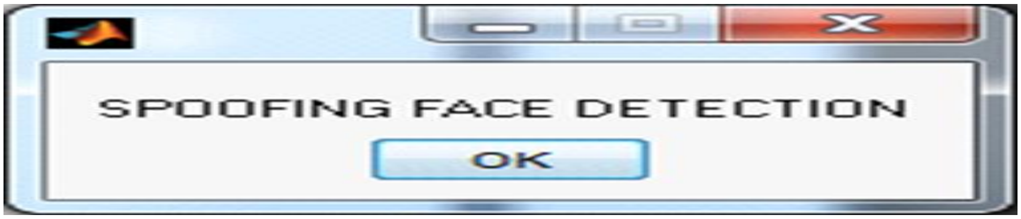

SPOOFING FACE DETECTION

Fig. 15 Final Output for Spoof Image

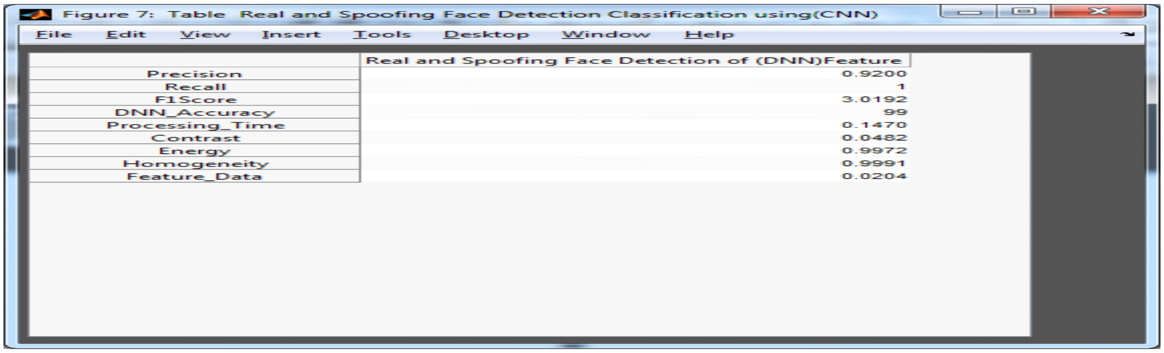


Figure 7: Table Real and Spoofing Face Detection Classification using(CNN)
File
Edit
View
Insert
Tools
Desktop
Window
Help

	Real and Spoofing Face Detection of (DNN)Feature
Precision	0.9200
Recall	1
F1Score	3.0192
DNN_Accuracy	99
Processing_Time	0.1470
Contrast	0.0482
Energy	0.9972
Homogeneity	0.9991
Feature_Data	0.0204

Fig. 16 Real and Spoofing Face Detection Classification Using (CNN)

IV. Conclusion

Current face biometric systems are very vulnerable to spoofing attacks and photographs are probably the most common sources of spoofing attacks. Even though many anti-spoofing attacks are available for detecting real and spoofing faces. But most of them fail to detect sophisticated attacks so, we apply the Convolutional Neural Network (CNN) for improving the accuracy of face spoofing detection.

VI Future Enhancement

The excellent results suggest also that more complex databases with various types of high- quality spoofing attacks and proper protocol are needed for future development, since the current publicly available databases have their limitations, thus are not generalizing the problem well enough. We believe that our approach can also be extended to detect spoofing attacks using masks or 3D models of the face because skin has a very particular texture with, for example, pores whereas fake faces have seldom such a level of detail.

References

[1] G. Heusch and S. Marcel, “Pulse-based features for face presentation attack detection,” Biometrics Theory, Applications and Systems (BTAS), 2018 IEEE 9th International Conference on, Special Session On Image And Video Forensics In Biometrics (IVFIB).,2018.

[2] J. Gan, S. Li, Y. Zhai, and C. Liu, “3d convolutional neural network based on face anti- spoofing,” in Multimedia and Image Processing (ICMIP), 2017 2nd International Conference on. IEEE, 2017, pp.1–5.

[3] H. Li, P. He, S. Wang, A. Rocha, X. Jiang, and A. C. Kot, “Learning generalized deep feature representation for face antispoofing,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2639–2652,2018.

[4] Y. Liu, A. Jourabloo, and X. Liu, “Learning deep models for face anti-spoofing: Binary or auxiliary supervision,” in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2018, pp.389–398.

[5] Y. Atoum, Y. Liu, A. Jourabloo, and X. Liu, “Face anti-spoofing using patch and depth- based cnns,” in *Biometrics (IJCB), 2017IEEE International Joint Conference on*. IEEE, 2017, pp. 319–328.

[6] X. Wu, R. He, Z. Sun, and T. Tan.(2018) A light cnn for deep face representation with noisy labels.[Online]. Available:https://github.com/AlfredXiangWu/LightCNN

[7] “IARPA ODIN,”https://www.iarpa.gov/index.php/research-programs/odin, accessed: 2018-10-20.

[8] R. Raghavendra, K. B. Raja, S. Venkatesh, F. A. Cheikh, and C. Busch, “On the vulnerability of extended multispectral face recognition systems towards presentation attacks,” in *Identity, Security and Behavior Analysis (ISBA), 2017 IEEE International Conference on*. IEEE, 2017, pp. 1–8.

[9] A. Agarwal, D. Yadav, N. Kohli, R. Singh, M. Vatsa, and A. Noore, “Face presentation attack with latex masks in multispectral videos,” in *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, July 2017,pp.275–283.

[10] T. de Freitas Pereira, A. Anjos, and S. Marcel, “Heterogeneousface recognition using domain specific units,” *IEEE Transactionson Information Forensics and Security*,2018.

[11] X. Wu, R. He, Z. Sun, and T. Tan, “A light cnn for deepface representation with oisy labels,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2884– 2896, 2018.