

Face Spoof Detection Using Dual Stream Convolutional Neural Network

Amoolya M¹, Amrutha B P², Ambika Y N³, Alok R Patil⁴, Thirumagal E⁵

⁵Professor

^{1,2,3,4,5}School of C&IT, Reva University, Bengaluru, India

¹amoolyam1999@gmail.com, ²amruthapradeep738@gmail.com, ³ambikanagaraj32@gmail.com,

⁴alokpatil676@gmail.com, ⁵thirumagal.e@reva.edu.in

Article Info

Volume 83

Page Number: 4667-4672

Publication Issue:

May-June 2020

Abstract

Face recognition is an acknowledgement strategy used to distinguish countenances of people whose pictures spared in information index. Face acknowledgement has consistently stayed a huge focal point of research due to its non-intruding nature. Face discovery is utilized in biometrics, regularly as a piece of a facial acknowledgement framework. This imaginative innovation has defects. This is the place the requirement for against parodying arrangements becomes possibly the most important factor. Most of the faces caricaturing assaults utilize 2D and 3D to trick facial acknowledgement programming. In spite of the fact that numerous compelling strategies have been proposed for against parodying we find that the presentation of many existing techniques is corrupted by illumination. It spurs us to create light invariant strategies for hostile to satirizing. In our paper we propose a double stream convolutional neural system. It fundamentally chips away at two spaces: to be specific RGB and MSR. The two spaces are similarly significant on the grounds that the previous contains high recurrence facial highlights yet delicate to brightening. Both these highlights are taken care of the system and we use attention based combination strategy to intertwine both the features. The outcome, whether the picture is genuine or parody is built up utilizing softmax.

Article History

Article Received: 19 November 2019

Revised: 27 January 2020

Accepted: 24 February 2020

Publication: 12 May 2020

Keywords: Face spoofing, convolutional neural networks, attention-based fusion, softmax.

1. Introduction

To viably secure the protection of an individual, it is basic to construct a face authentication framework. Over the most recent couple of years, face acknowledgment frameworks have picked up enthusiasm because of face rich highlights that offer a solid biometric signal to perceive people for a wide assortment of utilization. Face biometrics additionally these days being utilized universally as an option in contrast to passwords on cell phones. Regardless of the extraordinary arrangement of progress in facial acknowledgment framework, the multifaceted nature of spoofing attacks additionally emerges subsequently increasingly complex counter methodologies are manufactured which is powerful, productive and minimized.

Face spoofing:

A face spoofing is an undertaking to get someone else's advantages or access rights by using a photo, video or a substitute for an affirmed person's face. There are for the most part four sorts of face parodying attacks: photo ambush, covering ambush, video attack and 3D ambush. Photo attack and video answer ambush, are the most generally perceived attacks.

Photo ambush: the aggressor uses someone's photo. The image is appeared on a propelled contraption. This is the most generally perceived kind of ambush since by far most have facial pictures open on the web (on the web), photos could be gotten successfully without approval.

The video attack: this procedure requires a circled video of a casualty's face, ensures conduct and facial

improvements to look progressively standard diverged from holding someone's photo. Covering attack and 3D attacks are dynamically modern ambushes and besides huge cost including ambushes.

Face spoofing is moreover called face liveness acknowledgment, planned to counter different sorts of ridiculing attacks. Face parody distinguishing proof is really a parallel grouping issue, since face caricaturing recognizable proof normally functions as pre-preparing venture of face acknowledgment framework to choose whether the face is gotten from authentic individual or not.

Two stream convolutional neural system:

In profound learning, a convolutional neural framework is a class of profound neural framework. This is ordinarily applied to breaking down visual symbolism. They have applications in picture and video acknowledgment, recommender framework, picture order, clinical picture assessment, characteristic language handling and cash related time course of action.

Convolutional neural system comprises of numerous layers and it likewise contains shrouded layers. The concealed layer of CNNs comprises of a progression of convolutional layers with an augmentation dab item. The convolutional layers incorporate pooling layer, completely associated layer and standardization layer. These layers are alluded to as shrouded layers on the grounds that their information and yields are set apart by the actuation work. The initiation layer is regularly a RELU layer.

Pooling layer: pooling layer diminishes the component of the data by merging the yield of neuron packs at one layer into a neuron in the accompanying layer. Pooling may enlist a greatest worth or normal worth. Max pooling uses the best an incentive from all of a gathering of neurons at the previous layer. While normal pooling uses the typical incentive from all of a lot of neurons at the previous layer.

Completely associated layer: completely associated layer interface each neuron in one layer to each neuron in another layer. Right now neuron gets contribution from each component of the past layer. The availability design between neurons is like that of creature visual cortex and convolutional systems are by natural procedure. CNN's utilization generally like pre-handling contrasted with other picture characterization calculation.

2. Related Works

A. Face caricaturing location:

A mocking assault is an endeavor to obtain another person's benefits or access rights by utilizing a photograph, video or an alternate substitute for an approved individual's face. Recorded underneath are some of face satirizing assaults.

(I) .Motion Analysis Based Methods

These techniques exhaustively endeavor to perceive unconstrained improvement snippets of data made when

two dimensional fakes are acquainted with the camera of the system, for instance, photographs or accounts. Right now, et al. abused the way that human squint happens once every 2-4 seconds and proposed eye-flash based liveness disclosure for photo caricaturizing using (unconstrained) eye-glints. This procedure uses an undirected prohibitive subjective field framework to show the eye-squinting, which relaxes up the opportunity doubt of generative exhibiting and states dependence constraints from covered Markov illustrating. Obviously real human faces (which are 3D objects) will move out and out remarkably rather than planar articles, and such mutilation models can be used for liveness area.

(ii). Texture Analysis Based Methods

This kind of system takes a gander at the skin properties, for instance, skin surface and skin reflectance, under the assumption that surface properties of veritable faces and prints, for example, hues, are uncommon. Occasions of recognizable surface models in view of relics are printing dissatisfactions or clouding. Diverged from various frameworks, surface examination based counts are generally faster to portray a joke ambush.

(iii). Feature-Based Methods

At the present time features, for instance, eyes, nose and mouth are above all removed and their regions and neighborhood estimations (geometric as well as appearance) are dealt with into a classifier. A significant test for feature extraction procedures is including recovery; this is where the structure endeavors to recuperate features that are imperceptible in view of huge assortments.

(iv). Equipment Based Methods

Very few interesting hardware based face against scoring frameworks has been proposed so for reliant on imaging development outside the visual range, for instance, 3D significance, proportional infrared, or near infrared pictures by taking a gander at the reflectance information of certified appearances and parody materials using a specific set-up of LEDs and photo diodes at two exceptional frequencies.

B. Convolutional Neural Network

Convolutional neural network consists of series of network layer. These layers helps in dividing the input layer into pixels and compare it with the data. They have applications in picture and video acknowledgment, suggested frameworks, picture arrangement, clinical picture examination, normal language preparing, and budgetary time arrangement.

C. Multi Scale Retinex

Multiscale retinex was at first used to give steadiness in shading pictures; anyway it is likewise capable to be utilized in dark scale pictures. Gentility and shading consistency allude to wide scope of force and ghastrly enlightenment varieties. Multiscale retinex is framed from the retinex hypothesis by Edwin Land. Land

proposed the possibility of retinex as a model of daintiness to quantify the delicacy reaction in a picture.

3. Existing Works

The prior face parody discovery primarily centers around movement, texture, recurrence and quality parameters to distinguish genuine and Non genuine or parody face.

Writing overview

J. Yang, Stan Z li [1] proposed a strategy to identify whether a picture is genuine or counterfeit by thinking about the info picture. From the information picture or video caught from multiple perspectives, facial tourist spots are identified and key casings are chosen. At that point the picture is taken care of into help vector machine (SVM) classifier which is prepared to recognize phony or genuine face.

Andre Anjos [2] proposed a strategy called LBP-TOP based Counter measure against face ridiculing assaults. This strategy check faces by counter estimates dependent on movement and surface.

Surface of the picture is dissected utilizing lower twofold example (LBP) and movement is broke down utilizing amendment technique. The info picture is isolated into N casings and afterward they are broke down dependent on the small scale surface and movement.

Javier Galabally [3] proposed a strategy dependent on general picture quality appraisal. In this strategy, right off the bat the info picture is changed over into grayscale picture. The grayscale picture is then separated utilizing a low pass Gaussian channel for producing the misshaped form of the picture. At that point by looking at the quality between the grayscale picture and mutilated adaptation of the picture utilizing picture quality evaluation.

D. Wen [4] proposed a technique utilizing Image Distortion Analysis (IDA). The features Considered are concealing arranged assortment, reflection, fogginess and Chromatic moment. Here the features are arranged and Classified using Support Vector Machine (SVM) to perceive the face to be either certified or spoof face.

K Patel [5] this technique utilizes More examples. In this we break down the more example associating that ordinarily shows up during the recovery of video or photograph replays on a screen in various channels (R , G , B and Grayscale) and districts. The more examples can be identified utilizing MLBP and DSIFT highlights.

J. Komulainen [6] proposed a strategy to distinguish non genuine faces utilizing Histogram of Oriented Gradient (HOG) descriptors. The strategy of the face is poor down utilizing the chest region marker. The locator is utilized to see the nearness of the show off medium. On the off chance that the upper piece of a face picture isn't found, by then it results that the information picture is non-confirmed (parody); else the information picture is given as duty to the ridiculing medium locator to discover whether the information picture is trick or authentic picture.

L. Ashoke Kumar [7] proposed a methodology utilizing customary neural systems. The convolutional organize design is built to capture the ridiculed faces from getting to for the sake of veritable clients. Own datasets of genuine and phony pictures are made to prepare the neural system. The two datasets are prepared independently to determine the outright result.

Haonan Chen, Zhen Lei [8] proposed a methodology utilizing two stream convolutional neural system. The info picture is changed over into two spaces that is RGB and MSR. The RGB space contains the itemized facial surfaces, yet it is delicate to light. What's more the MSR pictures can successfully catch the high recurrence data, which is discriminative for face caricaturing discovery. Both the highlights are intertwined to get the ideal yield.

4. Proposed Works

Computers see pictures utilizing pixels. Pixels in pictures are normally related. For instance, a specific gathering of pixels may connote an edge in a picture or some other example. Convolutions utilize this to help distinguish pictures. Convolution neural systems can be constructed utilizing keras library in python. We have made a liveness identifier fit for spotting counterfeit faces and performing hostile to confront mocking in face acknowledgment frameworks.

Consider what might occur if an accursed client attempted to deliberately go around your face acknowledgment framework.

Such a client could attempt to hold up a photograph of someone else. Perhaps they even have a photograph or video on their cell phone that they could consider up to the camera answerable for performing face acknowledgment.

In those circumstances it's altogether feasible for the face held up to the camera to be effectively perceived at the end of the day prompting an unapproved client bypassing your face acknowledgment framework!

How might you approach recognizing these counterfeit versus genuine/real faces? How might you apply hostile to confront ridiculing calculations into your facial acknowledgment applications?

The appropriate response is to apply liveness identification with OpenCV which is actually what we'll be doing in our undertaking

Steps included:

Step:1: Build the picture dataset

Step:2: Implement a CNN equipped for performing liveness identifier (LivenessNet)

Step:3: Train the liveness finder organize.

Step:4: Create a Python + OpenCV content equipped for taking our prepared liveness identifier

Objectives:

1. To counter the face spoofing attacks using dual stream convolutional neural networks

2. To adaptively and effectively use two features generated by two stream convolutional neural network (TSCNN).
3. Here we have program which can build the image dataset of real and fake images using open cv
4. Implement a CNN capable of performing liveness detector
5. Train the liveness detector network
6. Make a python + open cv content equipped for our prepared liveness indicator display and apply it to constant video.

Block diagram:

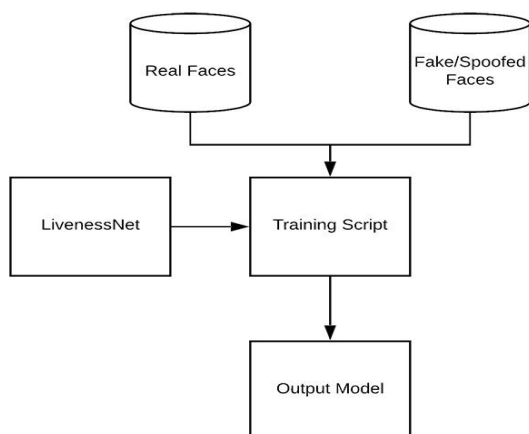


Figure 1: Block diagram

Algorithm:

We referred algorithms like:

1. Texture assessment, including figuring Local Binary Patterns (LBPs) over faces zones and using a SVM to arrange the faces as authentic or parody.
2. Frequency assessment, for instance, taking a gander at the Fourier space of the face.
3. Variable focusing assessment, for instance, taking a gander at the assortment of pixel regards between two successive edges.
4. Heuristic-based counts, including eye advancement, lip improvement, and squint disclosure. These course of action of counts attempt to follow eye advancement and squints to ensure the customer isn't holding up a photo of another person (since a photo won't gleam or move its lips).
5. Optical Flow figuring, to be explicit investigating the differentiations and properties of optical stream created from 3D things and 2D planes.
6. 3D face shape, similar to what is used on Apple's iPhone face affirmation structure, enabling the face affirmation system to perceive real faces and printouts/photos/pictures of another person.

Blend of above strategies can help in face liveness location and further it can utilized dependent on the necessary application

5. System Requirements

Hardware Requirements: Windows 10(i3 processor),
8 GB RAM

Software Requirements : Python
Pycharm
Anaconda 3

Modules: Open CV (cv2) and Numpy

6. Experimental Results and Analysis

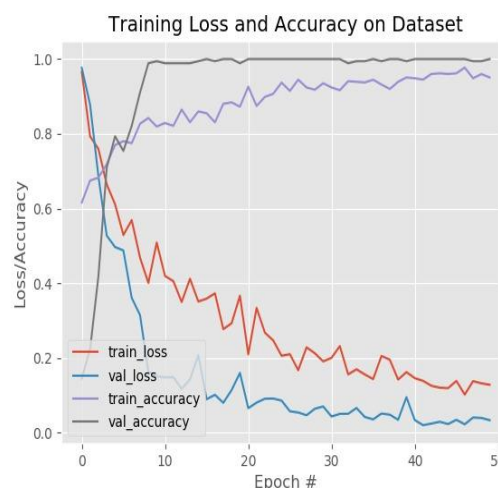


Figure 2: Loss graph

The above graph shows the accuracy of training in four ways.

Screen shots of data sets: We have two datasets namely real images and fake images.

Real: Real video is given as input and the program is written to prepare the data set like this where the images are cropped and stored in the same size.

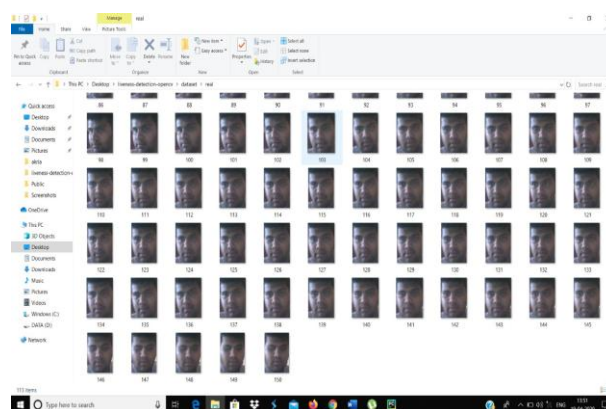


Figure 3: Real images dataset

Fake: Fake video is given as input and the program is written to prepare the data set like this where the images are cropped and stored in the same size.

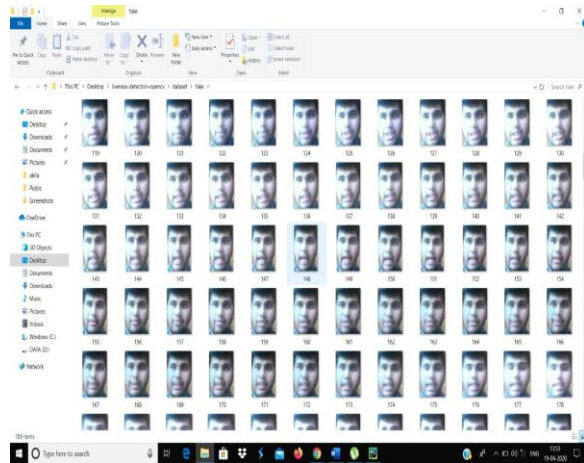


Figure 4: Fake images dataset

Analysis:
(To analyze whether the images are real or spoof)
For real image:

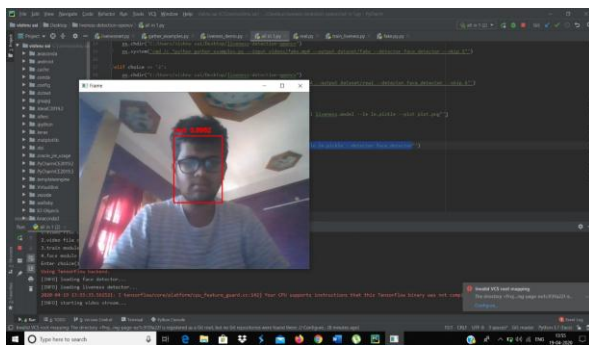


Figure 5: Detection of real image

As you can see in the figure a real face is detected.

For spoof image:

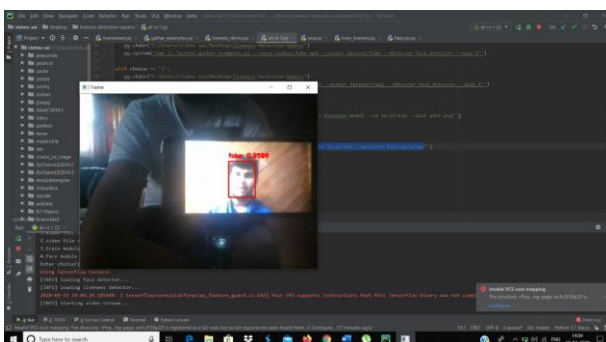


Figure 6: Detection of fake image

If the person tries to spoof using photo masking or video masking techniques then the result will be shown as fake, as you see in the figure 6.

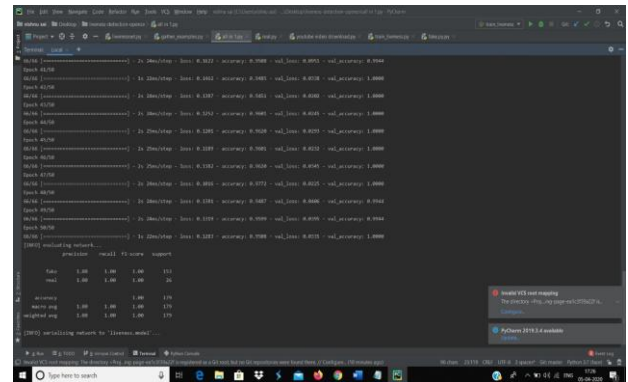


Figure 7: Analysis results

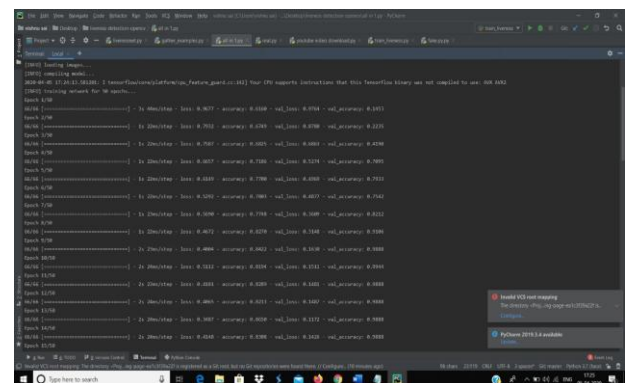


Figure 8: Analysis results

We have trained the model repeatedly with data set to system using module like keras and sklearn. This is the graph showing for 50 cycles of epoch. As you can see validation loss is less than training loss, we have overcome the problem of over fitting.

LivenessNet

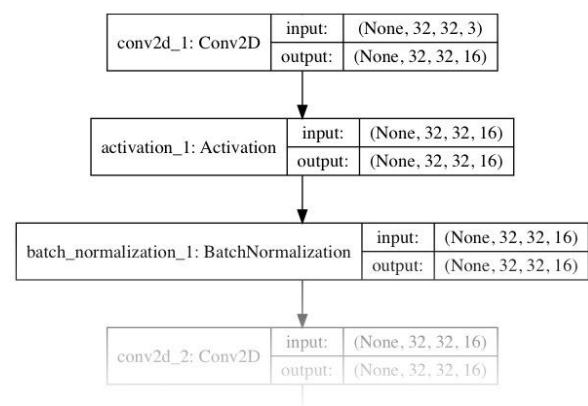


Figure 9: Accurate values of training model

The above figure represents the accuracy values of the training model.

7. Conclusion

Right now, we have proposed an attention based double stream convolutional neural system for face spoof detection to recognize genuine and counterfeit countenances. This strategy essentially includes two spaces, RGB and MSR. The two spaces contain high facial highlights. The RGB space contains point by point facial surfaces, yet it is delicate to light, though MSR picture can catch the high recurrence data. These highlights are fed into the system (CNN) and afterward the highlights are intertwined to know whether the picture is genuine or fake utilizing the softmax function.

This strategy shows the adequacy of the combination of RGB and MSR data.

8. Acknowledgement

Our appreciation goes to Prof.Thirumangal E, Professor of computer Sciences, the University of Reva for her strong ongoing support for the research, so that, amid a maze of possibilities and shortcomings, we can achieve a planned objective.

References

- [1] Face hostile to satirizing through half breed convolutional neural system by Lei li and Zhaoqiang Xia distributed on 2017 in the International Conference on the Frontiers and Advances in Data Science (FADS).
- [2] Face Spoofing Detection Using Color Texture Analysis by Jukka Komulainen and Abdenour Hadid distributed in IEEE Transactions on Information Forensics and Security
- [3] Attention-Based double-Stream Convolutional Networks for Face parody Detection by Haonam Chen and Guosheng hu conveyed in 2019 IEEE Transactions on Information Forensics and Security
- [4] Face spoof detection with image distortion analysis by Di Wen, Hu Han and Anil K jain published in 2015 IEEE Transactions on Information Forensics and security