FAKE IMAGE IDENTIFICATION USING CNN

Dr.K.V.Subbaiah, Chebrolu Bhanu sri, Kancharla Venkata Sesi Kumar, Amarapu Siddardha sri ram

[1]Professor in Department of CSE VISVODAYA ENGINEERING COLLEGE, KAVALI.

[2,3,4]B.Tech with CSE in VISVODAYA ENGINEERING COLLEGE, KAVALI.

Abstract_ Image forensics aims to detect the manipulation of digital images. Currently, splice detection, copy-move detection and image-retouching detection are attracting significant attention from researchers. However, image editing techniques develop over time. An emerging image editing technique is colourization, in which greyscale images are coloured with realistic colours. Regrettably, certain images may intentionally apply this technique to confuse object recognition algorithms. Nowadays, biometric systems are useful for recognising a person's identity, but criminals change their appearance, behaviour, and psychology to deceive the recognition systems. We are using a new technique called deep texture feature extraction from images to build and train a machine learning model using the CNN (Convolutional Neural Networks) algorithm. We refer to this technique as LBPNet or NLBPNet because it heavily relies on the LBP algorithm for feature extraction. Experimental results demonstrate that both proposed methods exhibit decent performances against multiple state-of-the-art colourization approaches.

1.INTRODUCTION

Now-a-days biometric systems are useful in recognizing person's identity but criminal change their appearance in behaviour and psychological to deceive recognition system. To overcome from this problem we are using new technique called Deep Texture Features extraction from images and then building train machine learning model using CNN (Convolution Neural Networks) algorithm. This technique refer as LBPNet or NLBPNet as this technique heavily dependent on features extraction using LBP (Local Binary Pattern) algorithm.

In this project we are designing LBP Based machine learning Convolution Neural Network called LBPNET to detect fake face images. Here first we will extract LBP from images and then train LBP descriptor images with Convolution Neural Network to generate training model. Whenever we upload new test image then that test image will be applied on training model to detect whether test image contains fake image or non-fake image. Below we can see some details on LBP.

Local binary patterns (LBP) is a type of visual descriptor used for classification in computer vision and is a simple yet very efficient texture operator which labels the pixels of an image by thresholding the neighborhood of each pixel and considers the result as a binary number. Due to its discriminative power and computational simplicity, LBP texture operator has become a popular approach in various applications. It can be seen as a unifying approach to the traditionally divergent statistical and structural models of texture analysis. Perhaps the most important property of the LBP operator in real-world applications is its robustness to monotonic gray-scale changes caused, for example, by illumination variations. Another important property is its computational simplicity, which makes it possible to analyze images in challenging real-time settings.

The LBP feature vector, in its simplest form, is created in the following manner:

ivide the examined window into cells (e.g. 16x16 pixels for each cell).

For each pixel in a cell, compare the pixel to each of its 8 neighbors (on its left-top, left-middle, left-bottom, right-top, etc.). Follow the pixels along a circle, i.e. clockwise or counter-clockwise.Where the center pixel's value is greater than the neighbor's value, write "0". Otherwise, write "1". This gives an 8-digit binary number (which is usually converted to decimal for convenience).

Compute the histogram, over the cell, of the frequency of each "number" occurring (i.e., each combination of which pixels are smaller and which are greater than the center). This histogram can be seen as a 256-dimensional feature vector.

Optionally normalize the histogram.

Concatenate (normalized) histograms of all cells. This gives a feature vector for the entire window.The feature vector can now be processed using the Support vector machine, extreme learning machines, or some other machine learning algorithm to classify images. Such classifiers can be used for face recognition or texture analysis

2.LITERATURE SURVEY

Hsu, C ; Lee C et al. [1] have proposed a novel deep forgery discriminator(DeepFD) to detect fake images generated by state of the art GANS based on contrastive loss.To address the existing shortcomings they had adopted contrastive loss in extracting the typical features of fake/generated images generated by different GANS.Their results have shown that their proposed system DeepFD had detected 94.7% fake images which are generated by several state of the art GANS.

Hsuan T. Chang, Chih-Chung Hsu et al. [2] have introduced a blind watermarking theme to perform image authentication and change of state localization within the receiver.So based on the extracted watermark, they had determined whether the received image is tampered or not.so to detect whether the image is tampered or not, they have proposed methods like Sequential watermark alignment based on coefficient stamping(SWACS) and morphological region growing and subband duplication(MRGSD) which determine the positions of modified pixels in the misreported watermark and to identify the tampered region. Chih-Chung

Hsu,Tzu-Yi Hung et al. [3] have proposed a new system for detecting forged regions in video in which they have got used correlation of noise residue.They modeled the system as GMM(Gaussian mixture model),where they have got proposed two-step scheme to estimate model parameters and they have extensively utilized Bayesian classifer to find best threshold value.In their experiments, two video inpainting schemes are used to simulate two unique sorts of tampering procees.Their experimental outcomes have shown that their proposed system had achieved higher accuracy for the videos.

Zheng et al. [5] found that it is particularly challenging to spot fake news and photographs since it is impossible to verify content on a pure basis and there aren't many models for doing so. can be utilised to fix the issue. It has been suggested that the issue of "detecting bogus news" be studied. Many useful characteristics of the language, words, and images utilised in fake news are discovered through a thorough analysis. A collection of hidden attributes produced from this model across several layers can be used to identify some hidden traits in the words and visuals used in fake news. The TICNN pattern has been suggested. By presenting distinct and integrated features in a same area, TICNN is trained simultaneously using text and image data. To detect fake accounts on social networks, particularly Facebook,

Raturi's 2018 design [6] was developed. Based on the posts and their location on social networking walls, a machine learning feature was utilised in this study to more accurately forecast bogus accounts. In order to validate content based on text classification and data analysis, Support Vector Machine (SVM) and Complement Nave Bayes (CNB) were utilised. The gathering of derogatory words and their frequency of occurrence were the main topics of the data analysis. For Facebook, SVM displays a 97% resolution, whilst CNB displays a 95% accuracy in Bag of Words recognition (BOW) counterfeit accounts with a basis. The study's findings demonstrated that the primary issue was safety of The problem with social networks is that published data is not thoroughly verified.

Two approaches were suggested in a 2017 study by Bunk et al [7] to detect and pinpoint fraudulent photos using a combination of resampling attributes and deep learning. In the original system, overlapping picture adjustments are used to estimate the Radon conversion of resampling parameters. A heat map is then created using deep learning classifiers and a Gaussian conditional domain pattern. Total areas are used in a Random Walker segmentation technique. Software resampling attributes are passed on overlapping object patches over an LSTM-based network in the following system for identification and localization. The effectiveness of both systems' detection and localization capabilities was also contrasted. The outcomes demonstrated the effectiveness of both systems in identifying and resolving digital picture fraud.

3.PROPOSED SYSTEM

This project aims to create LBP Based machine learning Convolution Neural Network known as LBPNET to identify phoney face pictures. Here first we will extract LBP from images and then train LBP descriptor images using Convolution Neural Network to produce training model. Whenever we upload fresh test image, that test image will be applied on training model to detect whether test image contains false image or non-fake image.

3.1 MODULES

In this project we are designing LBP Based machine learning Convolution Neural Network called LBPNET to detect fake face images.

Here first we will extract LBP from images and then train LBP descriptor images with Convolution Neural Network to generate training model.

Whenever we upload new test image then that test image will be applied on training model to detect whether test image contains fake image or non-fake image. Below we can see some details on LBP.

3.2 CNN

A Convolutional Neural Network (CNN) is a deep learning model primarily used for analyzing visual and time-series data. It automatically extracts features from raw input through layers that perform convolution operations, followed by activation functions like ReLU and pooling layers that reduce dimensionality while preserving important information. CNNs are highly effective in recognizing patterns and making predictions without requiring manual feature extraction, making them ideal for applications such as image classification, medical imaging, and ECG signal analysis. Their ability to learn complex features from data enables accurate and efficient decision-making in various fields.

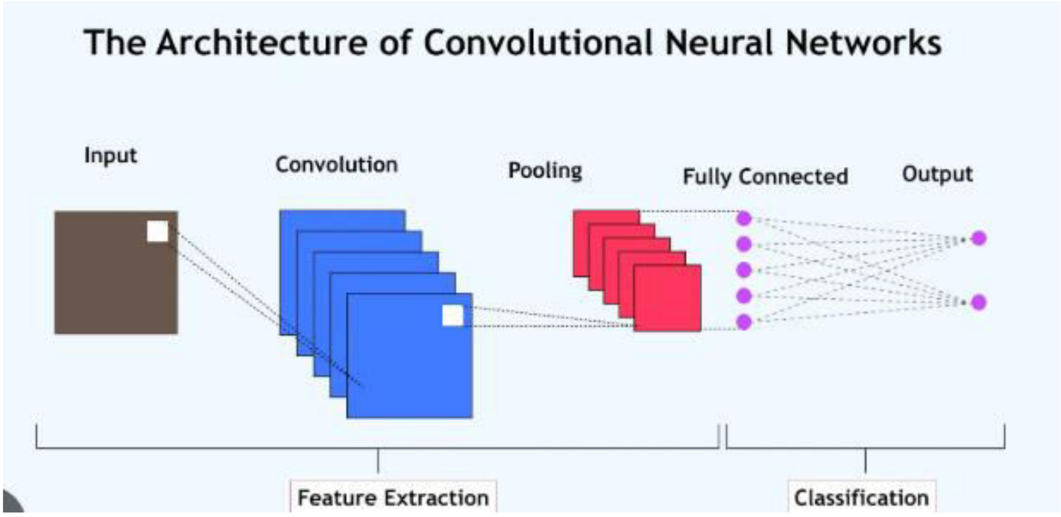


Fig 1:Architecture

4.RESULTS AND DISCUSSION

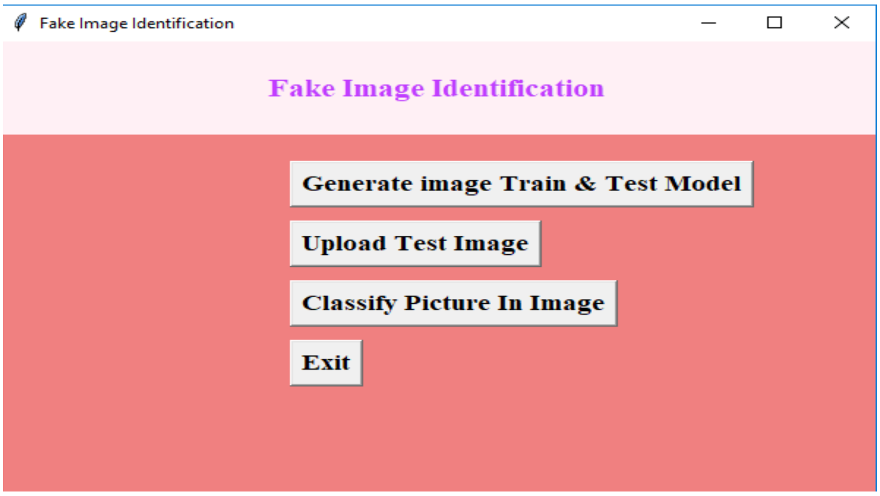
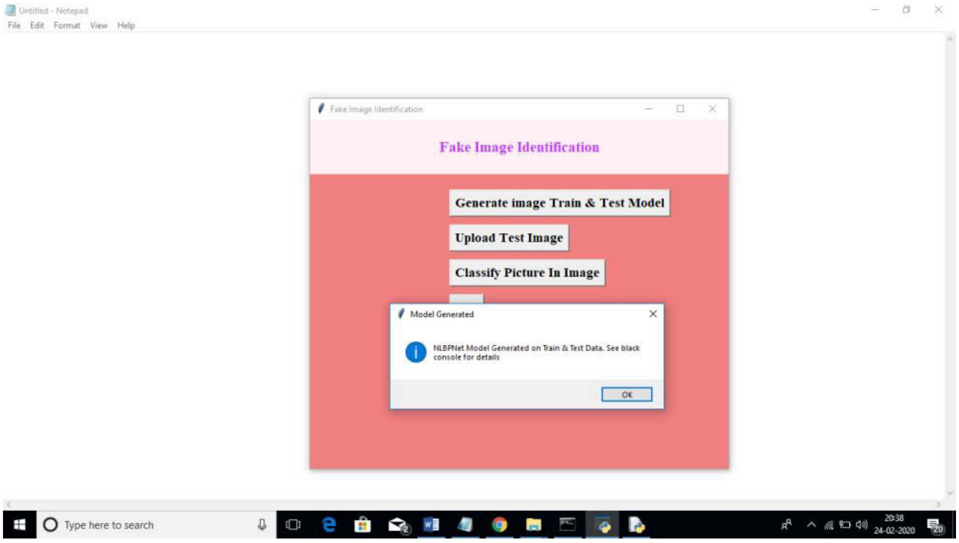

Fake Image Identification
Fake Image Identification
Generate image Train & Test Model
Upload Test Image
Classify Picture In Image
Exit

Fig 2:In above screen click on ‘Generate Image Train & Test Model’ button to generate CNN model using LBP images contains inside LBP folder.


Untitled - Notepad
File Edit Format View Help
Fake Image Identification
Fake Image Identification
Generate image Train & Test Model
Upload Test Image
Classify Picture In Image
Model Generated
OK
Type here to search
20:38
24-02-2020

NLBPNet Model Generated on Train & Test Data. See black console for details

Fig 3:In above screen we can see CNN LBPNET model generated. Now click on 'Upload Test Image' button to upload test image

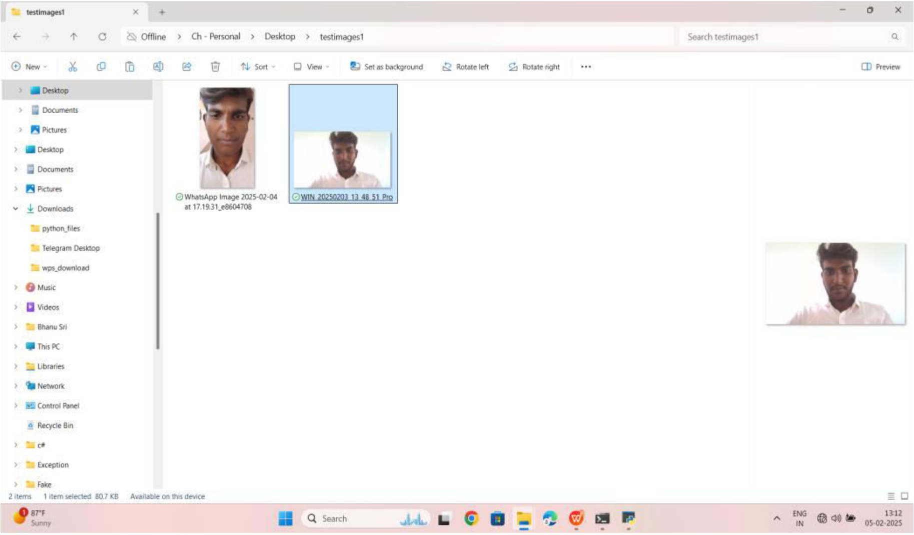


Fig 4:In above screen we can see two faces are there from same person but in different appearances. For simplicity I gave image name as fake and real to test whether application can detect it or not. In above screen I am uploading fake image and then click on 'Classify Picture In Image' button to get below result

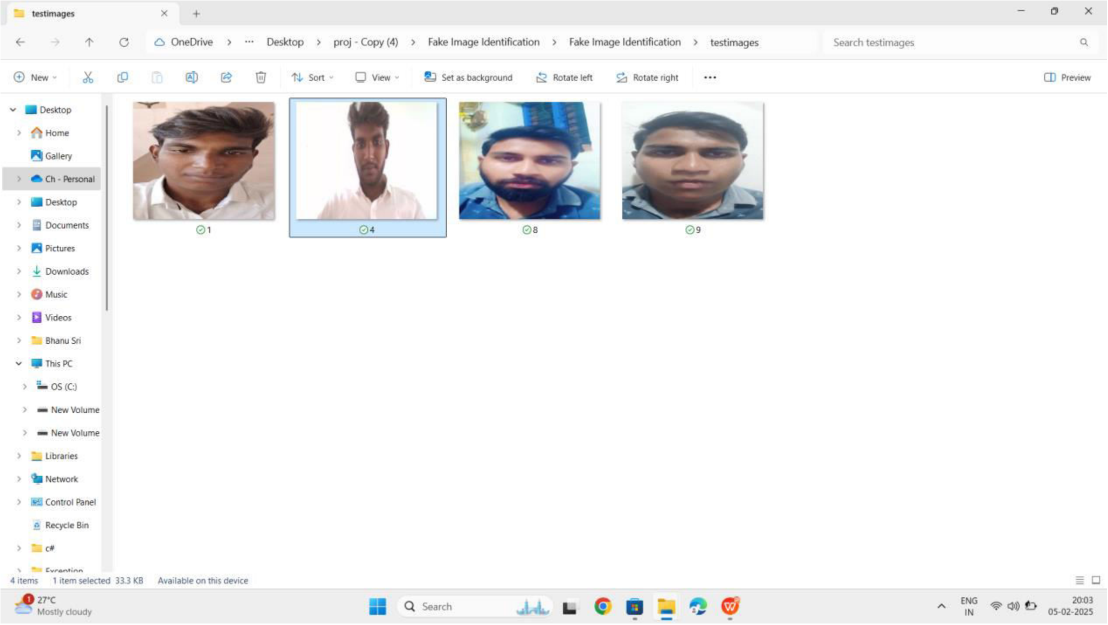


Fig 5:In above screen we can see all real face will have normal light and in fake faces peoples will try some editing to avoid detection but this application will detect whether face is real or fake

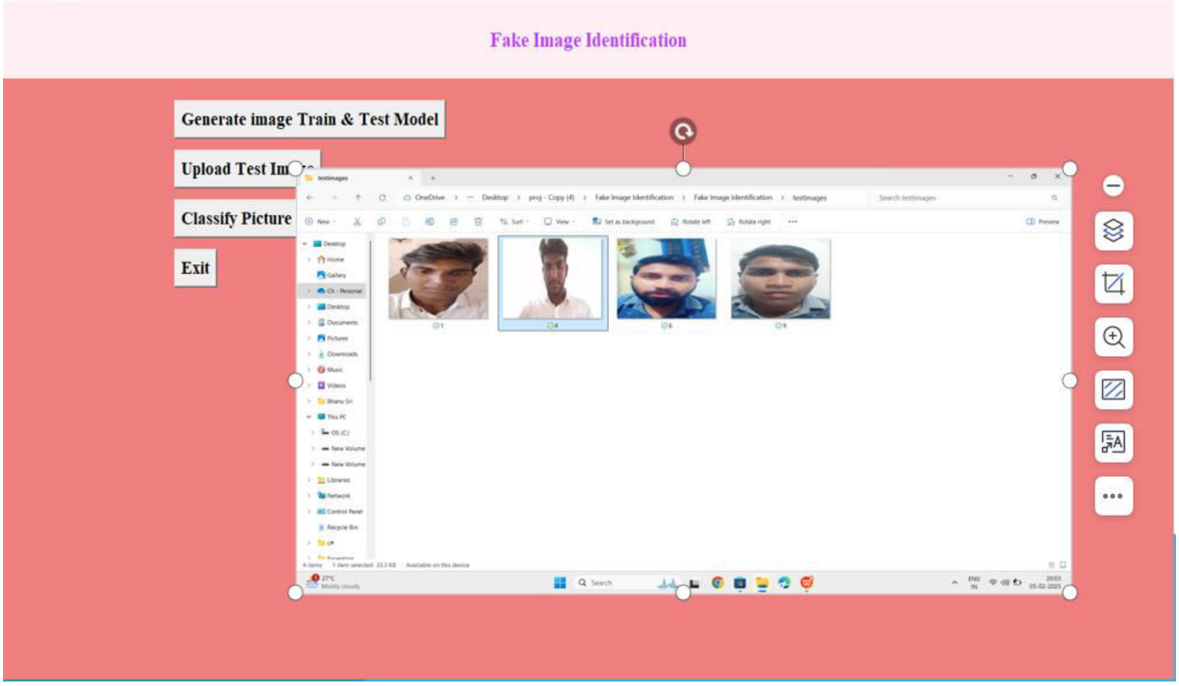


Fig 6:In above screen I am uploading 1.jpg and after upload click on open button to get below screen

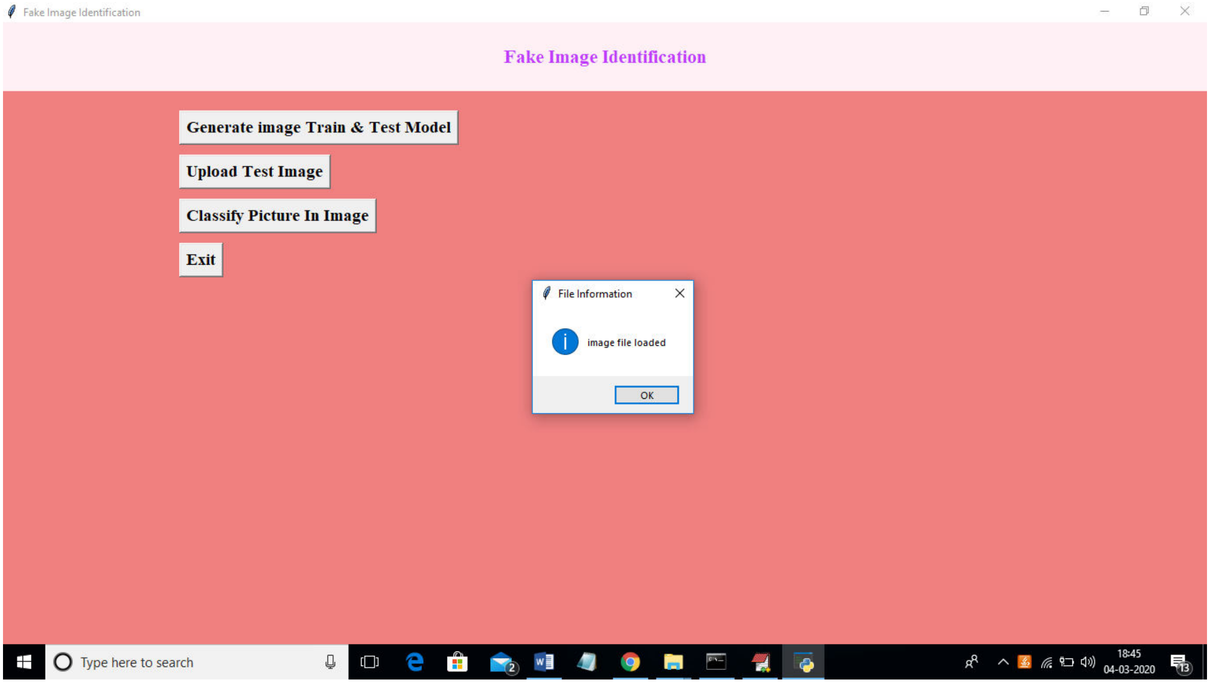

Fake Image Identification
Fake Image Identification
Generate image Train & Test Model
Upload Test Image
Classify Picture In Image
Exit
File Information
OK
Type here to search
18:45
04-03-2020

image file loaded

Fig 7:And now click on 'classify Picture in Image' to get below details

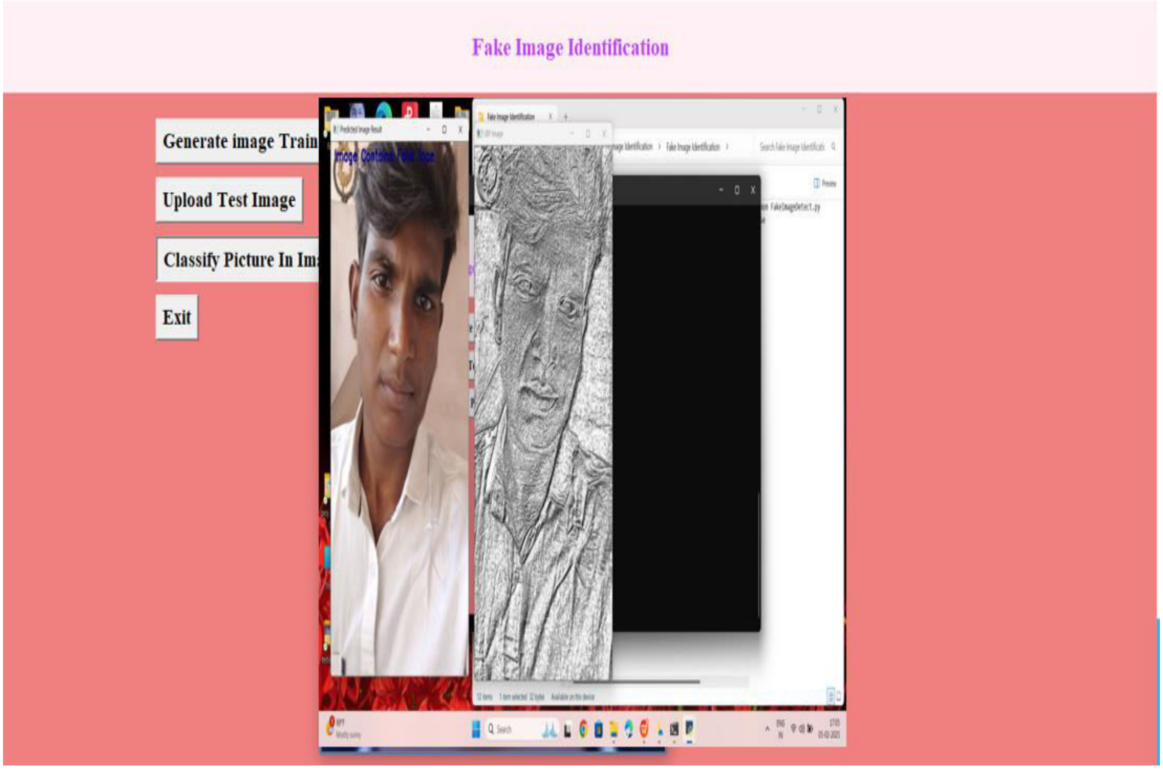


Fig 8: In above screen we are getting result as image contains Fake face. Similarly u can try other images also. If u want to try new images then u need to send those new images to us so we will make CNN model to familiar with new images so it can detect those images also.

5.CONCLUSION

This research presents a new common fake feature network based on pairwise learning designed to effectively identify the fake face/general images produced by state-of-the-art GANs. By combining the crosslayer feature representations into the last fully connected layers, the suggested CNN can be utilised to learn the middle- and high-level and discriminative fake feature. The suggested paired learning can be applied to increase the efficacy of false picture identification even more. The suggested paired learning should enable the suggested fake image detector to identify the false image produced by a fresh GAN. Our experimental findings showed that the suggested approach beats existing state-of-the-art approaches in terms of accuracy and recall rate.

REFERENCES

1. Karras, T.; Aila, T.; Laine, S.; Lehtinen, J. Progressive growing of gans for improved quality, stability, and variation. arXiv Preprint, arXiv:1710.10196 2017. 256

2. Brock, A.; Donahue, J.; Simonyan, K. Large scale gan training for high fidelity natural image synthesis. arXiv Preprint, arXiv:1809.11096 2018.

3. Zhu, J.Y.; Park, T.; Isola, P.; Efros, A.A. Unpaired image-to-image translation using cycle-consistent 259 adversarial networks. arXiv Preprint, 2017.

4. AI can now create fake porn, making revenge porn even more complicated,. http://theconversation.com/ai-can-now-create-fake-porn-making-revenge-porn-even-more-complicated-92267, 262 2018.

5. Hsu, C.; Lee, C.; Zhuang, Y. Learning to detect fake face images in the Wild. 2018 International Symposium 264 on Computer, Consumer and Control (IS3C), 2018, pp. 388–391. doi:10.1109/IS3C.2018.00104.

6. H.T. Chang, C.C. Hsu, C.Y.a.D.S. Image authentication with tampering localization based on watermark 266 embedding in wavelet domain. Optical Engineering 2009, 48, 057002.

7. Hsu, C.C.; Hung, T.Y.; Lin, C.W.; Hsu, C.T. Video forgery detection using correlation of noise residue. Proc. of the IEEE Workshop on Multimedia Signal Processing. IEEE, 2008, pp. 170–174.

8. Farid, H. Image forgery detection. IEEE Signal Processing Magazine 2009, 26, 16–25.

9. Huaxiao Mo, B.C.; Luo, W. Fake Faces Identification via Convolutional Neural Network. Proc. of the ACM Workshop on Information Hiding and Multimedia Security. ACM, 2018, pp. 43–47.

10. Marra, F.; Gragnaniello, D.; Cozzolino, D.; Verdoliva, L. Detection of GAN-Generated Fake Images over Social Networks. Proc. of the IEEE Conference on Multimedia Information Processing and Retrieval, 2018, 274 pp. 384–389. doi:10.1109/MIPR.2018.00084.

11. Chollet, F. Xception: Deep learning with depthwise separable convolutions. Proc. of the IEEE conference on 276 Computer Vision and Pattern Recognition 2017, pp. 1610–02357.

Author’s profile

Dr.K.V.Subbaiah is currently working as a Professor in the Department of Computer Science and Engineering in Visvodaya Engineering College , kavali , spsr Nellore , Andhra Pradesh,India.

I am Bhanu sri Chebrolu,currently pursuing a B.Tech in Computer Science and Engineering in Visvodaya Engineering College,kavali,spsr Nellore,Andhra pradesh,India.My areas of intrest include python,java,HTML,sql.I have earned certifictions such as ,DotNet full Stack from Wipro, I got successfully completed python training from Besant Technologies.I have also completed Java programming Internship at Intern certify.

I am siddardha sri ram Amarapu,currently pursuing a B.Tech in Computer Science and Engineering in Visvodaya Engineering College, Kavali ,spsrNellore ,AndhraPradesh,India.My areas of Intrest include java,python . I have Earned Certifications such as completed internship on java full stack at skill Spire Techologies and I have also completed Dotnet Internship at Intern certify.

I am sasikumar kancharla,currently pursuing a B.Tech in Computer Science and Engineering at Visvodaya Engineering College,Kavali,spsr Nellore ,Andhra Pradesh,India.My areas of Intrest include java,python .I have Earned Certifications such as completed internship on python full stack at excelr ,i have also completed Data science internship at Intern certify .