DETECTION OF IMAGE FORGERY USING DEEP LEARNING THROUGH CONVOLUTIONAL NEURAL NETWORKS

B. Aruna Sri[1], B. Kritika[2], M. Harini[2], Nusrat Begum[2], N. Sree Sai Harshitha[2]

[1]Assistant Professor, [2]UG Scholar, [1,2]Department of Computer Science and Engineering

[1,2]Malla Reddy Engineering College for Women (A), Maisammaguda, Medchal, Telangana.

kribha226@gmail.com, nusratbegum1283@gmail.com, harshithananjyala2003@gmail.com, mupparapuharini@gmail.com

ABSTRACT

Now-a-days biometric systems are useful in recognizing person's identity but criminals 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 refers 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.

Keywords: Local binary patterns, Machine learning, Image forgery.

1. INTRODUCTION

Recently, the generative model based on deep learning such as the generative adversarial net (GAN) is widely used to synthesize the photo-realistic partial or whole content of the image and video. Furthermore, recent research of GANs such as progressive growth of GANs (PGGAN)[1] and BigGAN could be used to synthesize a highly photo-realistic image or video so that the human cannot 20 recognize whether the image is fake or not in the limited time. In general, the generative applications can be used to perform the image translation tasks [3]. However, it may lead to a serious problem once the fake or synthesized image is improperly used on social network or platform. For instance, cycleGAN is used to synthesize the fake face image in a pornography video [4]. Furthermore, GANs may be used to create a speech video with the synthesized facial content of any famous politician, causing severe problems on the society, political, and commercial activities. Therefore, an effective fake face image detection technique is desired. In this paper, we have extended our previous study associated with paper ID #1062 to

effectively and efficiently address these issues.

In traditional image forgery detection approach, two types of forensics scheme are widely used: active schemes and passive schemes. With the active schemes, the externally additive signal (i.e., watermark) will be embedded in the source image without visual artifacts. In order to identify whether the image has tampered or not, the watermark extraction process will be performed on the target image to restore the watermark[6]. The extracted watermark image can be used to localize or detect the tampered regions in the target image. However, there is no "source image" for the generated images by GANs such that the active image forgery detector cannot be used to extract the watermark image. The second one-passive image forgery detector–uses the statistical information in the source image that will be highly consistency between different images. With this property, the intrinsic statistical information can be used to detect the fake region in the image[7][8]. However, the passive image forgery detector cannot be used to identify the fake image generated by GANs since they are synthesized from the low-dimensional random vector. Nothing change in the generated image by GANs because the fake image is not modified from its original image

Intuitively, we can adopt the deep neural network to detect the fake image generated by GAN. Recently, there are some studies that investigate a deep learning-based approach for fake image detection in a supervised way. In other words, fake image detection can be treated as a binary classification problem (i.e., fake or real image). For example, the convolution neural network (CNN) network is used to learn the fake image detector [9]. In [10], the performance of the fake face image detection can be further improved by adopting the most advanced CNN–Xception network [11]. However, there are many GANs proposed year by year. For example, recently proposed GANs such as [1][12][13][14][15][16][3][2] can be used to produce the photo-realistic images. It is hard and very time-consuming to collect all training samples of all GANs. In addition, such a supervised learning strategy will tend to learn the discriminative features for a fake image generated by each GANs. In this situation, the learned detector may not be effective for the fake image generated by another new GAN excluded in the training phase.

In order to meet the massive requirement of the fake image detection for GANs-based generator, we propose novel network architecture with a pairwise learning approach, called common fake feature network (CFFN). Based on our previous approach [5], it is clear that the pairwise learning approach can overcome the shortcomings of the supervised learning-based CNN such as methods in [9][10]. In this paper, we further introduce a novel network architecture combining with pairwise learning to improve the performance of the fake image detection. To verify the effectiveness of the proposed method, we apply the proposed deep fake detector (DeepFD) to identify both fake face and generic image. The primary contributions of the proposed method are two-fold:

- We propose a fake face image detector based on the novel CFFN consisting of several dense blocks to improve the representative power of the fake image.

- The pairwise learning approach is first introduced to improve the generalization property of the proposed DeepFD.

2. LITERATURE SURVEY

2.1. TITLE: Remote Sensing and Image Interpretation.

Author: Lillesand, T.M. and Kiefer, R.W. and Chipman, J.W.,

Remote Sensing and Image Interpretation, 7th Edition is designed to be primarily used in two ways: as a textbook in the introductory courses in remote sensing and image interpretation, and as a reference for the burgeoning number of practitioners who use geospatial information and analysis in their work. Because of the wide range of academic and professional settings in which this book might be used, we have made the discussion "discipline neutral." In short, anyone involved in geospatial data acquisition and analysis should find this book to be a valuable text and reference.

2.2 Title: Deep Learning: methods and applications.

Author: Li Deng and Dong Yu.

This monograph provides an over view of general deep learning methodology and its applications to a variety of signal and information processing tasks. The application areas are chosen with the following three criteria in mind: (1) expertise or knowledge of the authors; (2) the application areas that have already been transformed by the successful use of deep learning technology, such as speech recognition and computer vision; and (3) the application areas that have the potential to be impacted significantly by deep learning and that have been experiencing research growth, including natural language and text processing, information retrieval, and multimodal information processing empowered by multi-task deep learning.

2.3 Title: A Logical Calculus of Ideas Immanent in Nervous Activity.

Author: McCulloch, Warren; Walter Pitts.

Because of the "all-or-none" character of nervous activity, neural events and the relations among them can be treated by means of propositional logic. It is found that the behavior of every net can be described in these terms, with the addition of more complicated logical means for nets containing circles; and that for any logical expression satisfying certain conditions, one can find a net behaving in the fashion it describes. It is shown that many particular choices among possible neurophysiological assumptions are equivalent, in the sense that for every net behaving under one assumption, there exists another net which behaves under the other and gives the same results, although perhaps not in the same time. Various applications of the calculus are discussed.

2.4 Title: An introduction to convolutional neural networks.

A Convolutional neural network (CNN) is a neural network that has one or more convolutional layers and is used mainly for image processing, classification, segmentation and also for other auto correlated data. A convolution is essentially sliding a filter over the input. One helpful way to think about convolutions is this quote from Dr Prasad Samarakoon: "A convolution can be thought as "looking at a function's surroundings to make better/accurate predictions of its outcome."Rather than looking at an entire image at once to find certain features it can be more effective to look at smaller portions of the image.

2.5 Title: Receptive fields and functional architecture of monkey striate cortex.

Author: Hubel, D. and Wiesel, T.

The striate cortex was studied in lightly anaesthetized macaque and spider monkeys by recording extracellularly from single units and stimulating the retinas with spots or patterns of light. Most cells can be categorized as simple, complex, or hypercomplex, with response properties very similar to those previously described in the cat. On the average, however, receptive fields are smaller, and there is a greater sensitivity to changes in stimulus orientation. A small proportion of the cells are colour coded.2. Evidence is presented for at least two independent systems of columns extending vertically from surface to white matter. Columns of the first type contain cells with common receptive-field orientations. They are similar to the orientation columns described in the cat, but are probably smaller in cross-sectional area. In the second system cells are aggregated into columns according to eye preference. The ocular dominance columns are larger than the orientation columns, and the two sets of boundaries seem to be independent.3. There is a tendency for cells to be grouped according to symmetry of responses to movement; in some regions the cells respond equally well to the two opposite directions of movement of a line, but other regions contain a mixture of cells favouring one direction and cells favouring the other.4. A horizontal organization corresponding to the cortical layering can also be discerned. The upper layers (II and the upper two-thirds of III) contain complex and hypercomplex cells, but simple cells are virtually absent. The cells are mostly binocularly driven. Simple cells are found deep in layer III, and in IV A and IV B. In layer IV B they form a large proportion of the population, whereas complex cells are rare. In layers IV A and IV B one finds units lacking orientation specificity; it is not clear whether these are cell bodies or axons of geniculate cells. In layer IV most cells are driven by one eye only; this layer consists of a mosaic with cells of some regions responding to one eye only, those of other regions responding to the other eye. Layers V and VI contain mostly complex and hypercomplex cells, binocularly driven.5. The cortex is seen as a system organized vertically and horizontally in entirely different ways. In the vertical system (in which cells lying along a vertical line in the cortex have common features) stimulus dimensions such as retinal position, line orientation, ocular dominance, and perhaps directionality of movement, are mapped in sets of superimposed but independent mosaics. The horizontal system segregates cells in layers by hierarchical orders, the lowest orders (simple cells monocularly driven) located in and near layer IV, the higher orders in the upper and lower layers.

3 PROPOSED SYSTEM

We propose a strategy for consolidating highlights from different layers in given CNN models. In addition, effectively learned CNN models with preparing pictures are reused to separate highlights from numerous layers. The proposed combination strategy is assessed by picture classification benchmark informational indexes, CIFAR-10, NORB, and SVHN. In all cases, we show that the proposed strategy improves the detailed exhibitions of the current models by 0.38%, 3.22% and 0.13%, separately.

4. RESULTS

Image Classification Using CNN (Convolution Neural Networks) Algorithm

In this project we are using python KERAS and Google TENSORFLOW CNN algorithm to classify images, CNN algorithm can predict images correctly up to 90% which is better prediction accuracy compare to all other algorithms such as SVM, KNN etc. To classify images using CNN we need to train CNN network with all possible images and when new images uploaded then CNN train model will be

applied on this new image to predict or identify image.

CNN working procedure

To demonstrate how to build a convolutional neural network based image classifier, we shall build a 6 layer neural network that will identify and separate one image from other. This network that we shall build is a very small network that we can run on a CPU as well. Traditional neural networks that are very good at doing image classification have many more parameters and take a lot of time if trained on normal CPU. However, our objective is to show how to build a real-world convolutional neural network using TENSORFLOW.

Neural Networks are essentially mathematical models to solve an optimization problem. They are made of neurons, the basic computation unit of neural networks. A neuron takes an input (say x), do some computation on it (say: multiply it with a variable w and adds another variable b) to produce a value (say; $z = wx+b$). This value is passed to a non-linear function called activation function (f) to produce the final output(activation) of a neuron. There are many kinds of activation functions. One of the popular activation function is Sigmoid. The neuron which uses sigmoid function as an activation function will be called sigmoid neuron. Depending on the activation functions, neurons are named and there are many kinds of them like RELU, TanH.

If you stack neurons in a single line, it's called a layer; which is the next building block of neural networks. See below image with layers
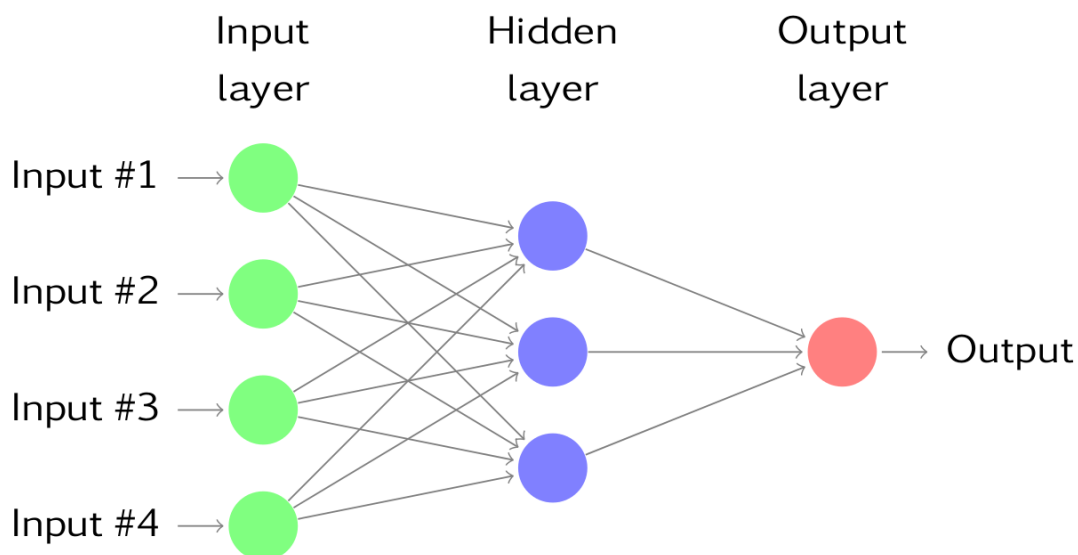

To predict image class multiple layers operate on each other to get best match layer and this process continues till no more improvement left.

Screen shots

Double click on 'run.bat' file to get below screen

In this paper author has used NUAA Photograph Imposter (fake) Database with images obtained from real and fake faces. We also used images and convert that image into LBP format. Below are some images from LBP folder
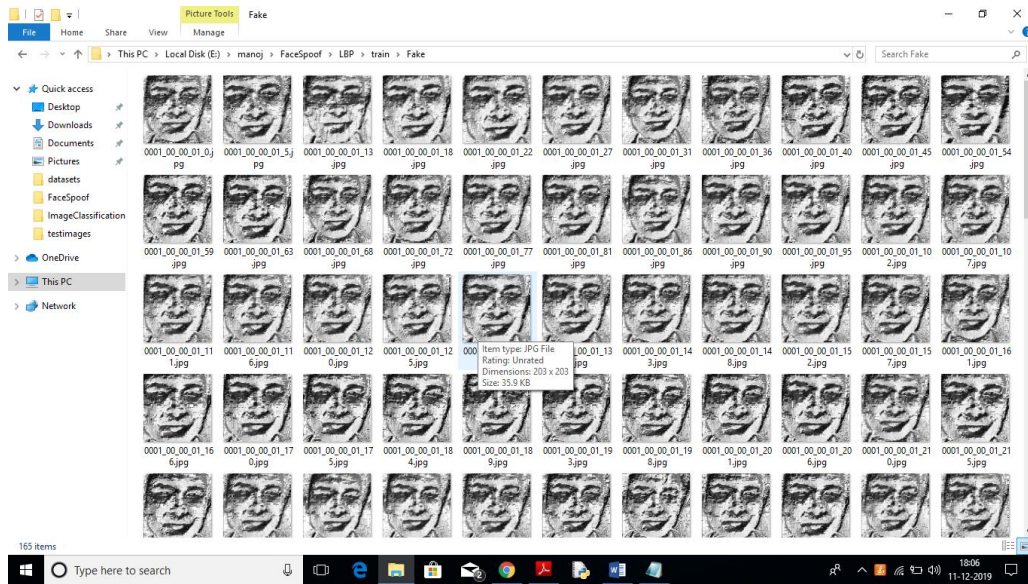
All this fake and real images you can see inside 'LBP/train' folder.

This project consists of following modules:

1. Generate NLBPNet Train & Test Model: in this module we will read all LBP images from LBP folder and then train CNN model with all those images.

2. Upload Test Image: In this module we will upload test image from 'testimages' folder. Application will read this image and then extract Deep Textures Features from this image using LBP algorithm.

3. Classify Picture In Image: This module apply test image on CNN train model to predict whether test image contains spoof or non-spoof face.
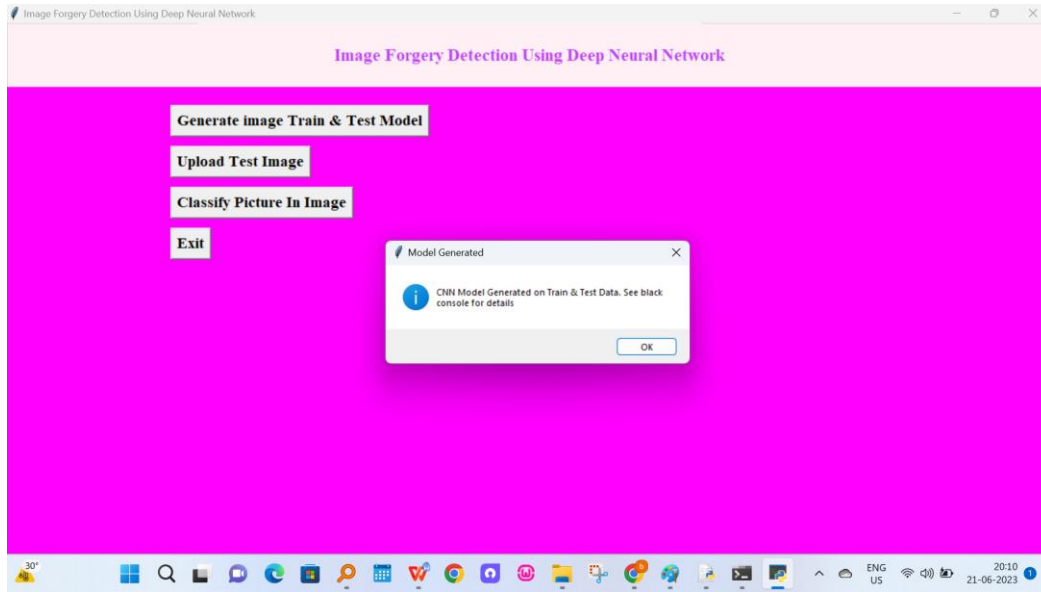
Screen shots

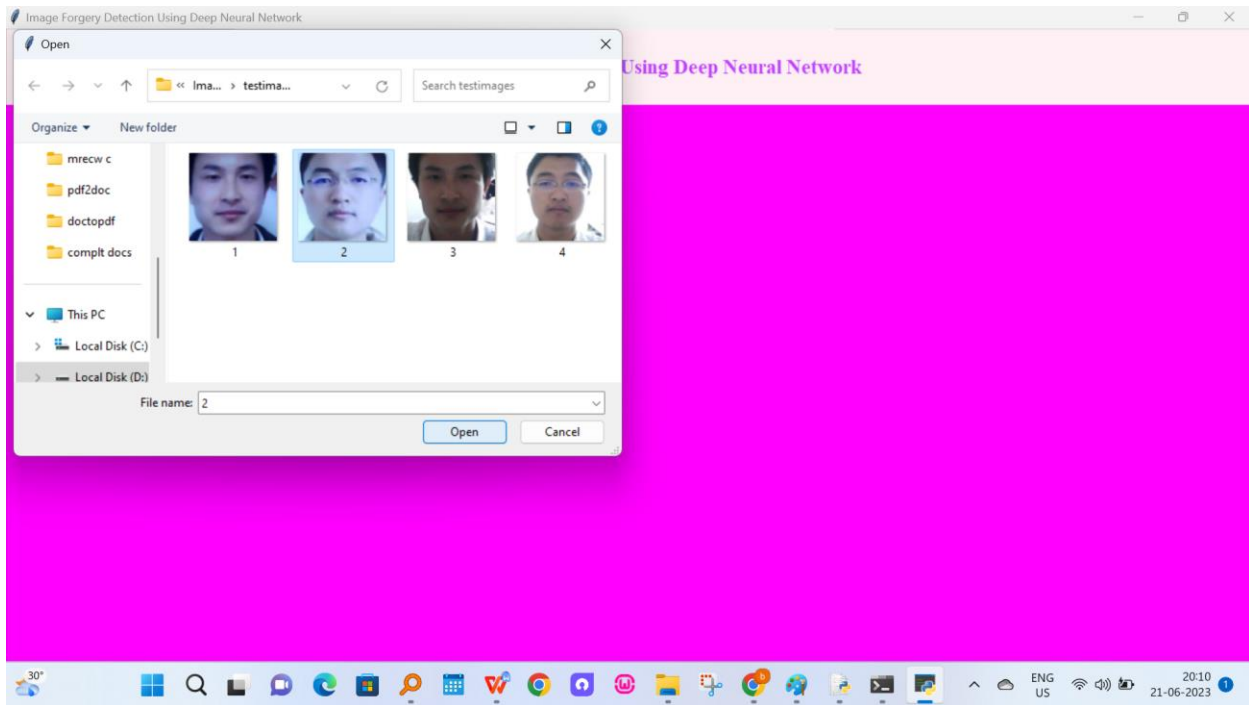To run this project double click on 'run.bat' file to get below screen
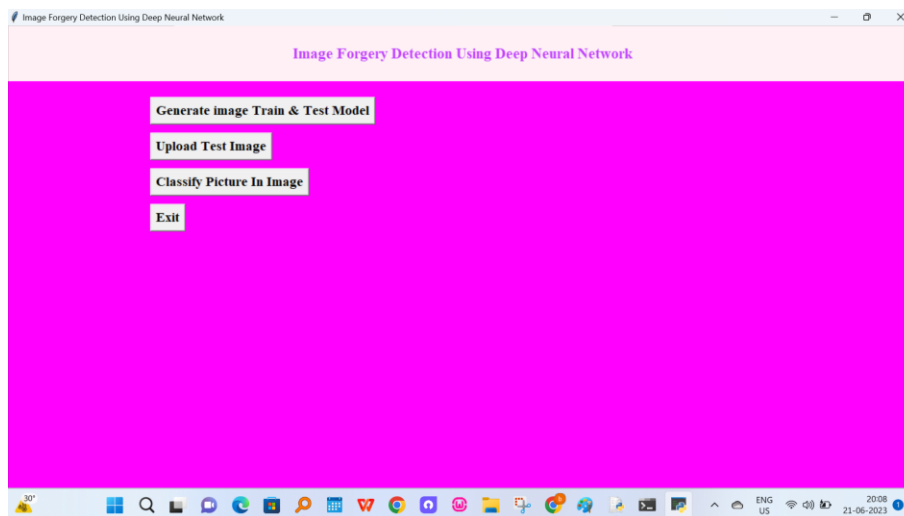
In above screen click on 'Generate Image Train & Test Model' button to generate CNN model using LBP

images contains inside LBP folder.

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


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.
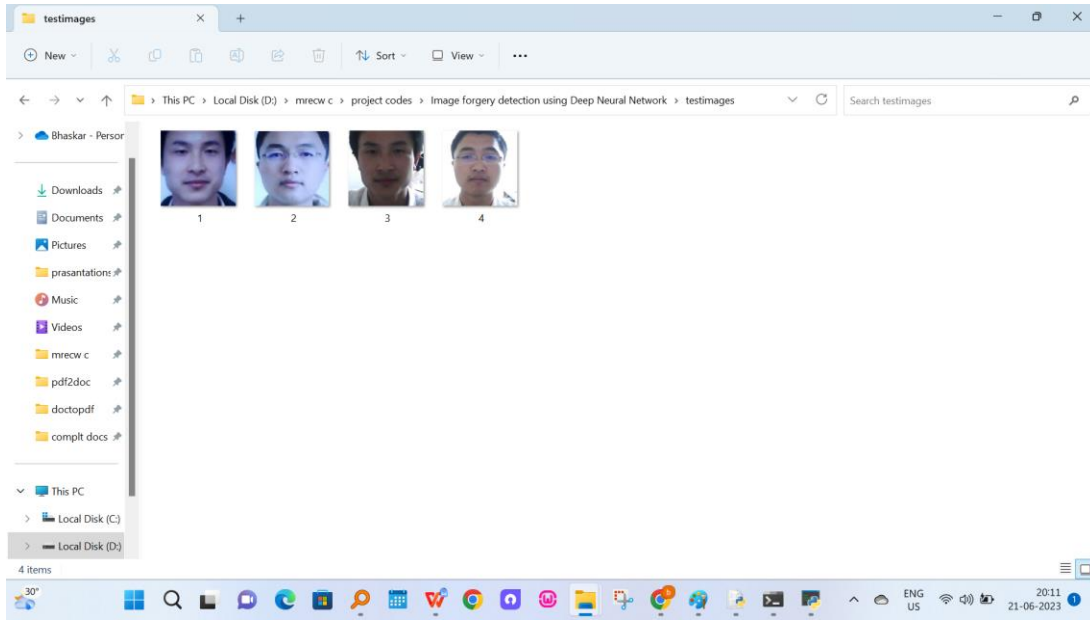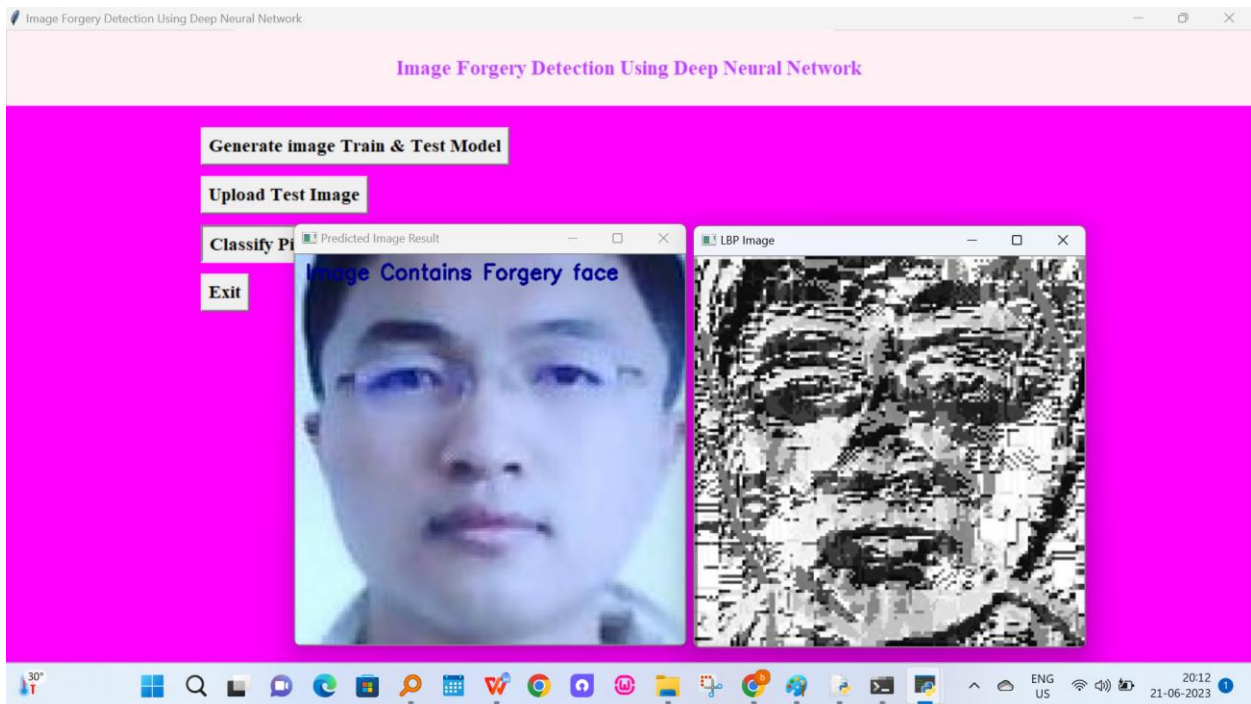
In above screen we can see all real face will have normal light and in fake faces peoples will try some editing to avoid detection but this application will detect whether face is real or fake
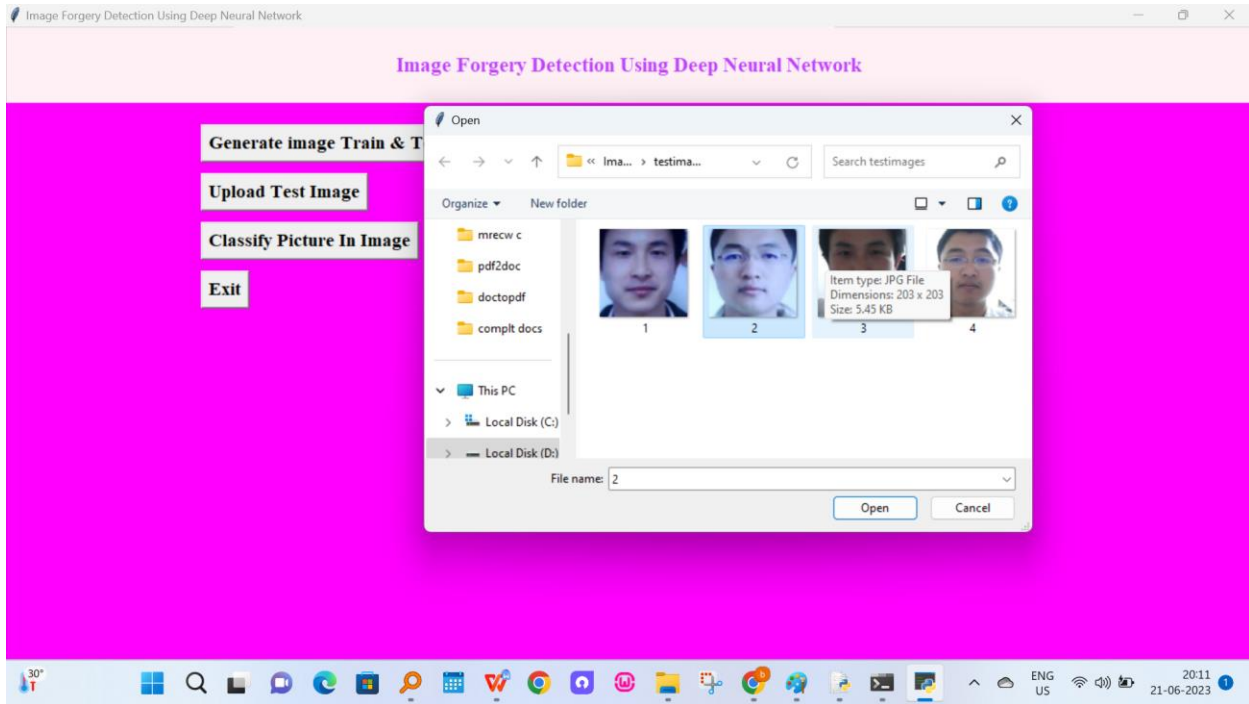
In above screen I am uploading 1.jpg and after upload click on open button to get below screen
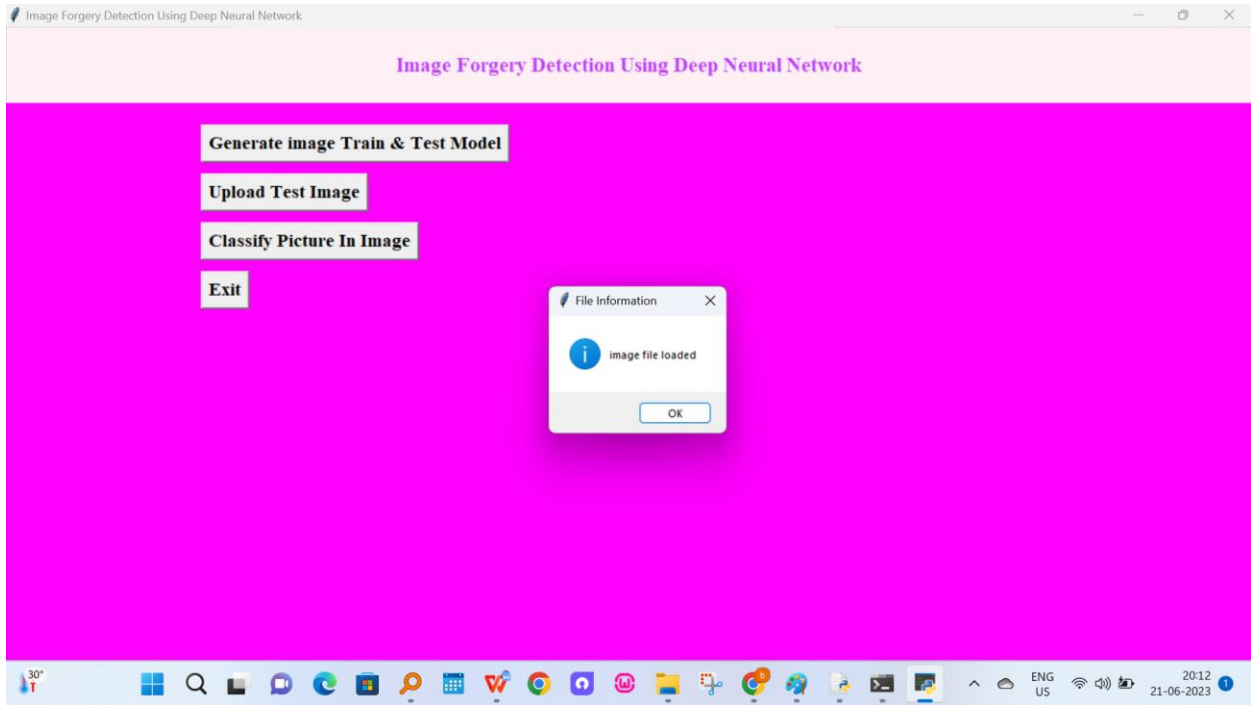
And now click on 'classify Picture in Image' to get below details

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

In this paper, we have proposed a novel common fake feature network based the pairwise learning, to detect the fake face/general images generated by state-of-the-art GANs successfully. The proposed CFFN can be used to learn the middle- and high-level and discriminative fake feature by aggregating the cross-layer feature representations into the last fully connected layers. The proposed pairwise learning can be used to improve the performance of fake image detection further. With the proposed pairwise learning, the proposed fake image detector should be able to have the ability to identify the fake image generated by a new GAN. Our experimental results demonstrated that the proposed method outperforms other state-of-the-art schemes in terms of precision and recall rate

REFERENCES

[1] Available online: http://www.greencarreports.com/news/1093560_1-2-billion-vehicles-on-worlds-roads-now-2-billion-by-2035-report (accessed on 5 June 2021).

[2] Available online: https://www.weforum.org/agenda/2016/04/the-number-of-cars-worldwide-is-set-to-double-by-2040 (accessed on 5 June 2021).

[3] Available online: https://commons.wikimedia.org/wiki/File:China_cross-border_Guangdong-Macau_ registration_plate_%E7%B2%A4Z_D100%E6%BE%B3.jpg (accessed on 14 April 2019). (licensed under CC BY-SA 4.0).

[4] Available online: https://commons.wikimedia.org/wiki/File:Damaged_Ontario_DCDM236.JPG (accessed on 14 April 2019). (licensed under CC BY-SA 4.0).

[5] Manzoor, M.A.; Morgan, Y. Vehicle Make and Model classification system using bag of SIFT features. In Proceedings of the 2017 IEEE 7th Annual IEEE Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 9–11 January 2020.

[6] Huang, B.-J.; Hsieh, J.-W.; Tsai, C.-M. Vehicle Detection in Hsuehshan Tunnel Using Background Subtraction and Deep Belief Network. In Asian Conference on Intelligent Information and Database Systems; Springer: Cham, Switzerland, 2020.

[7] Lu, Xiaofeng; Izumi, Takashi; Takahashi, Tomoaki; Wang, Lei. Moving vehicle detection based on fuzzy background subtraction. In Proceedings of the 2014 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), Beijing, China, 6–11 July 2019.

[8] Faro, A.; Giordano, D.; Spampinato, C. Adaptive background modeling integrated with luminosity sensors and occlusion processing for reliable vehicle detection. IEEE Trans. Intell. Transp. Syst. **2018**, 12, 1398–1412. [CrossRef]

[9] Chen, Li-Chih; Hsieh, Jun-Wei; Yan, Yilin; Chen, Duan-Yu. Vehicle make and model recognition using sparse representation and symmetrical SURFs. Pattern Recognit. **2017**, 48, 1979–1998. [CrossRef]

[10] Sivaraman, S.; Trivedi, M.M. Looking at vehicles on the road: A survey of vision-based vehicle detection, tracking, and behavior analysis. IEEE Trans. Intell. Transp. Syst. **2016**, 14, 1773–1795. [CrossRef]

[11] Wang, Rui; Zhang, Lei; Xiao, Kejiang; Sun, Rongli; Cui, Li. EasiSee: Real-time vehicle classification and counting via low-cost collaborative sensing. IEEE Trans. Intell. Transp. Syst. **2015**, 15, 414–424. [CrossRef]

[12] Dong, Zhen; Wu, Yuwei; Pei, Mingtao; Jia, Yunde. Vehicle type classification using a semisupervised convolutional neural network. IEEE Trans. Intell. Transp. Syst. **2015**, 16, 2247–2256. [CrossRef]

[13] Fu, Huiyuan; Ma, Huadong; Liu, Yinxin; Lu, Dawei. A vehicle classification system based on hierarchical multi-SVMs in crowded traffic scenes. Neurocomputing **2016**, 211, 182–190. [CrossRef]

[14] Irhebhude, M.E.; Amin, N.; Edirisinghe, E.A. View invariant vehicle type recognition and counting system using multiple features. Int. J. Comput. Vis. Signal Process. **2016**, 6, 20–32.

[15] Lowe, D.G. Object recognition from local scale-invariant features. In Proceedings of the Seventh IEEE International Conference on Computer Vision; IEEE: New York, NY, USA, 1999; Volume 2.

[16] Bay, Herbert; Ess, Andreas; Tuytelaars, Tinne; Van Gool, Luc. Speeded-up robust features (SURF). Comput. Vis. Image Underst. **2008**, 110, 346–359. [CrossRef]

[17] Dalal, N.; Triggs, B. Histograms of oriented gradients for human detection. In Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, CVPR 2005, San Diego, CA, USA, 20–25 June 2005; Volume 1.

[18] Siddiqui, A.J.; Mammeri, A.; Boukerche, A. Real-time vehicle make and model recognition based on a bag of SURF features. IEEE Trans. Intell. Transp. Syst. **2016**, 17, 3205–3219. [CrossRef]

[19] Boonsim, N.; Prakoonwit, S. Car make and model recognition under limited lighting conditions at night. Pattern Anal. Appl. **2017**, 20, 1195–1207. [CrossRef]

[20] Petrovic, V.S.; Cootes, T.F. Analysis of Features for Rigid Structure Vehicle Type Recognition. BMVC **2004**, 2. [CrossRef]

[21] Pearce, G.; Pears, N. Automatic make and model recognition from frontal images of cars. In Proceedings of the 2011 8th IEEE International Conference on Advanced Video and Signal-Based Surveillance (AVSS), Klagenfurt, Austria, 30 August–2 September 2011.

[22] Varjas, V.; Tanács, A. Car recognition from frontal images in mobile environment. In Proceedings of the 2013 8th International Symposium on Image and Signal Processing and Analysis (ISPA), Trieste, Italy, 4–6 September 2013.

[23] Clady, Xavier; Negri, Pablo; Milgram, Maurice; Poulenard, Raphael. Multi-class vehicle type recognition system. Lect. Notes Comput. Sci. **2008**, 5064, 228–239.

[24] Munroe, D.T.; Madden, M.G. Multi-class and single-class classification approaches to vehicle model recognition from images. In Proceedings of the 16th Irish Conference on Artificial Intelligence and Cognitive Science (AICS 2005), Portstewart, Northern Ireland, September 2005.

[25] Dlagnekov, L.; Belongie, S.J. Recognizing Cars; Department of Computer Science and Engineering, University of California: San Diego, CA, USA, 2005.

[26] Baran, R.; Glowacz, A.; Matiolanski, A. The efficient real-and non-real-time make and model recognition of cars. Multimedia Tools Appl. **2015**, 74, 4269–4288. [CrossRef]

[27] Fraz, M.; Edirisinghe, E.A.; Sarfraz, M.S. Mid-level-representation based lexicon for Vehicle Make and Model Recognition. In Proceedings of the 2014 22nd International Conference on Pattern Recognition (ICPR), Stockholm, Sweden, 24–28 August 2014.

[28] Psyllos, A.; Anagnostopoulos, C.-N.; Kayafas, E. Vehicle model recognition from frontal view image measurements. Comput. Stand. Interfaces **2011**, 33, 142–151. [CrossRef]

[29] Jang, D.M.; Turk, M. Car-Rec: A real time car recognition system. In Proceedings of the 2011 IEEE Workshop on Applications of Computer Vision (WACV), Kona, Hawaii, 5–7 January 2011.

[30] Hsieh, J.-W.; Chen, L.-C.; Chen, D.-Y. Symmetrical SURF and its applications to vehicle detection and vehicle make and model recognition. IEEE Trans. Intell. Transp. Syst. **2014**, 15, 6–20. [CrossRef]

[31] Boyle, J.; Ferryman, J. Vehicle subtype, make and model classification from side profile video. In Proceedings of the 2015 12th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Karlsruhe, Germany, 25–28 August 2015.

[32] Available online: http://vbie.eic.nctu.edu.tw/en/introduction (accessed on 05 January 2017).

[33] Available online: http://mmplab.cs.ntou.edu.tw/MMR/ (accessed on 23 July 2016).

[34] Manzoor, M.A.; Morgan, Y. Vehicle make and model recognition using random forest classification for intelligent transportation systems. In Proceedings of the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–10 January 2018.

[35] Oliva, A. Gist of the scene. Neurobiol. Atten. **2005**, 696, 251–258.

[36] Oliva, A.; Torralba, A. Modeling the shape of the scene: A holistic representation of the spatial envelope. Int. J. Comput. Vis. **2001**, 42, 145–175. [CrossRef]

[37] Wolpert, D.H. The lack of a priori distinctions between learning algorithms. Neural Comput. **1996**, 8, 1341–1390. [CrossRef]

[38] Burges, C.J.C. A tutorial on support vector machines for pattern recognition. Data Min. Knowl. Discov. **1998**, 2, 121–167. [CrossRef]

[39] Vapnik, V. The Nature of Statistical Learning Theory; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2013.

[40] Devroye, L.; Györfi, L.; Lugosi, G. A Probabilistic Theory Of Pattern Recognition; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2013; Volume 31.

[41] Weston, J. Support Vector Machine (And Statistical Learning Theory) Tutorial; NEC Labs America: Princeton, NJ, USA, 1998.

[42] Vapnik, V.N.; Vapnik, V. Statistical Learning Theory; Wiley: New York, NY, USA, 1998; Volume 1.