International Journal of Gender, Science and
..ISSN: 2040-0748

UGC Care Group I Journal
Vol-13 Issue-01 June 2024

The Use of Deep Learning Algorithms for the Determination of Authentic Images

Mrs. MOUNIKA.S [1], Ms. PRAVEENA.P. [2]

#1 Assistant professor in the department of IT at DVR & DR. HS MIC College of Technology (Autonomous), Kanchikacherla, NTR District.

#2 MCA student in the Department of Computer Applications (DCA) at DVR & DR.HS MIC COLLEGE OF TECHNOLOGY, Kanchikacherla, NTR District

ABSTRACT— Criminals alter their physical appearance, demeanor, and mental state in order to fool modern biometric identification systems. We are constructing a trainable machine learning model with the help of the CNN (Convolution Neural Networks) method, which is a novel approach to extracting deep texture features from photos, in order to circumvent this issue. Because it relies so much on the LBP (Local Binary Pattern) algorithm for feature extraction, this method goes by the names LBP Net and NLBP Net.
Our goal in developing LBPNET, a convolutional neural network based on learning biases, is to identify photos of people's faces that are not real. In order to create a training model, we will first use Convolution Neural Networks to extract LBP from photos, and then we will train these images to be LBP descriptors. In order to determine whether a newly uploaded test picture comprises a fake or non-fake image, we apply it to the training model. You may find more information about LBP below. A simple and extremely fast texture operator, local binary patterns (LBP) label picture pixels by thresholding the neighborhood of each pixel and considering the result as a binary integer. These patterns are employed as visual descriptors for classification in computer vision. The LBP texture operator is a popular method in many applications because of its computing simplicity and discriminative capability. In this way, it bridges the gap between the structural and statistical models of texture analysis, which have hitherto been somewhat different. The LBP operator's resistance to monotonic gray-scale fluctuations, such as those generated by variations in light, is one of its most valuable properties in practical applications. One

further crucial quality is that it can handle complex real-time picture analysis because to its computational simplicity.

INTRODUCTION

The ability to tell altered photos apart from the original has grown in tandem with the use of digital editing tools. But have no fear! Help is on the way from deep learning algorithms. These algorithms can detect the genuineness of a picture by analyzing its visual patterns and clues. These algorithms can determine the likelihood of picture manipulation by comparing it to a database of known authentic and altered photos. Deep learning techniques are complex, and this project will go into their details as well as their training and application to the problem of identifying false photos.
project, you will be investigating the potential of AI to detect instances of image manipulation via the use of deep learning algorithms for the purpose of recognizing false photos. A class of machine learning algorithms known as "deep learning" attempts to simulate the way the human brain uses neural networks. To identify whether a picture has been edited, they may examine its textures, colors, edges, and patterns, among other visual aspects.

Real and fake photos must be included in the dataset for these algorithms to be trained. The authentic photos will be used as a reference point, while the altered ones will have several kinds of editing done to them, such retouching, picture splicing, or cloning. Using this dataset as a teaching tool, the deep learning algorithm will discover patterns and characteristics that distinguish between authentic and false photos.

While training, the system will pick up on some visual clues that suggest manipulation, such skewed lighting, artificial shadows, or pixel patterns that don't seem right. The program can calculate the probability of an image's falsity by examining these indicators.

You may use the trained algorithm to detect altered or real photos even when you haven't seen them before. You can tell whether a picture is false or not by entering it into an algorithm, which will then evaluate its visual characteristics and provide a probability score. You may use this score to find out whether the picture is real or if someone messed with it.

Remember that deep learning algorithms aren't infallible, even if they're great tools for detecting bogus photos. Due to their reliance on the patterns and signals gained from the

training data, they could miss more complex or unique modification approaches on occasion. Keeping up with the ever-changing manipulation techniques requires constant updates and improvements to the algorithm. Here is the easiest way to construct the LBP feature vector:
Take a look at the eight pixels on each side of each pixel in a given cell and see how they stack up against each other. Move in a clockwise or counterclockwise circle following the pixels.

Put "0" when the value of the central pixel is higher than that of its neighbor. Indicate "1" in its place if not. A binary number, which is often translated to decimal for convenience, with 8 digits, is obtained from this.

Find the distribution of the occurrences of each "number" (i.e., every combination of pixel sizes relative to the center) and plot it across the cell as a histogram. Imagine this histogram as a feature vector with 256 dimensions.

It is optional to standardize the histogram. Join all of the cells' normalized histograms. A feature vector covering the whole window is produced by this.
Now we may process the feature vector using a machine learning method to categorize photos, such as a support vector machine, an extreme learning machine, or another option. Applications for these classifiers include texture analysis and face recognition.

Related works:

Convolutional Neural Network:

CNN is the deep neural network architecture most commonly used. It has an input layer, an output layer, and one or more hidden layers, just like other neural networks. In CNN [3], the hidden layers first read the inputs from the first layer and then execute a convolution mathematical operation on the input values. In addition to matrix multiplication, CNN employs non-linearity activation methods such as Rectified Linear Units (RELU) and extra convolutional approaches such as pooling layers. To minimize the complexity of the data, pooling layers provide outputs using methods such as average pooling.

Recurrent Neural Network:

It is another artificial neural network application that can learn characteristics from sequence data [2]. Basically, RNN is built from a variety of hidden layers, each with its own bias and weight. The connection

between the nodes in an RNN-based direct cycle graph runs sequentially. By offering a recurrent hidden state that encapsulates time-scale dependencies, it can handle a temporal sequence.

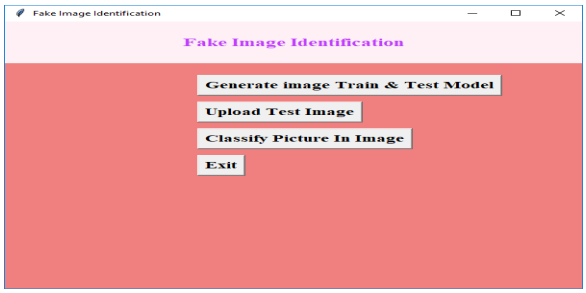
Long Short-Term Memory:

It is a sort of artificial RNN that manages long-term dependencies. The full data sequence may be learned using the feedback connections in LSTM. The input gate, forget gate and output gate make up the basic LSTM architecture. The cell state remembers the values from prior intervals and stores them. The input gate first selects the values that ought to be written into the cell state. The forget gate may logically select which information has to be forgotten by employing a sigmoid function. In which the information from the present moment should be taken into account in the following phase is decided by the output gate.

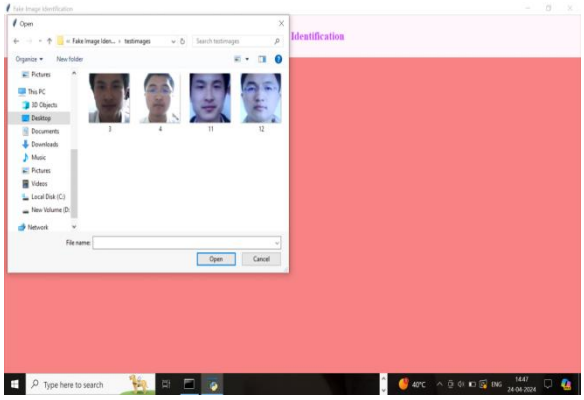
METHODOLOGY

1) **Generate Image Train & Test Model:** Using this module, generating CNN model using LBP images contains inside LBP folder.
2) **Upload Test Image:** Using this module, uploading test image
3) **Classify Picture In Image:** Using this module, detecting whether face is real or fake

RESULT AND DISCUSSION

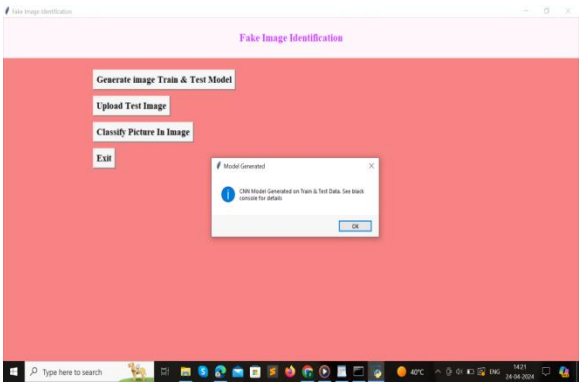


In above screen click on 'Generate Image Train & Test Model' button to generate CNN model using LBP images contains inside LBP folder.

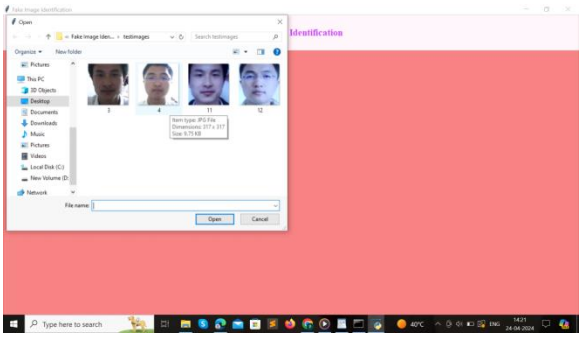


In above screen we can see two faces are there from same person but in different appearances. For simplicity I gave image name as fake and real to test whether application can detect it or not. In above screen I am uploading fake image and then

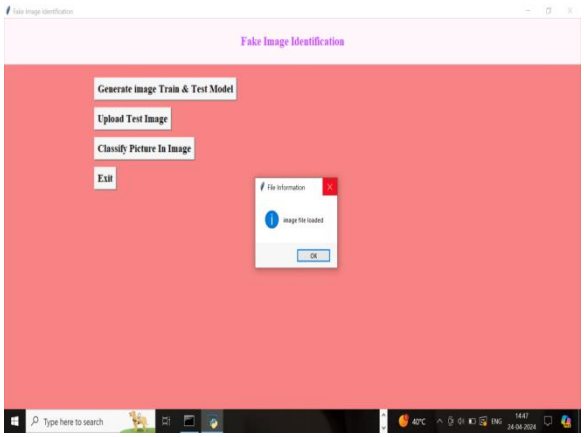
click on 'Classify Picture In Image' button to get below result



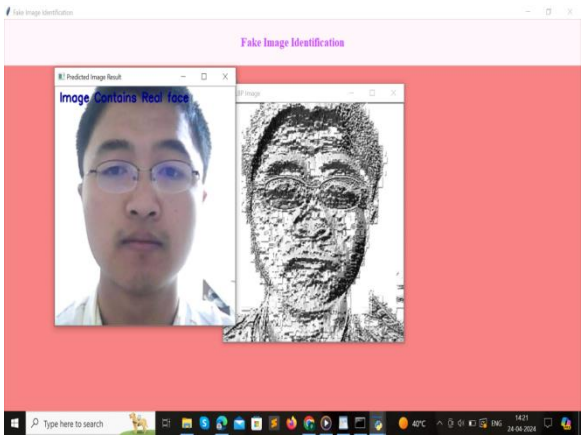
In above screen we can see all real face will have normal light and in fake faces peoples will try some editing to avoid detection but this application will detect whether face is real or fake



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.

CONCLUSION

This research presents a new approach to common false feature networks based on pairwise learning. It effectively detects fake

face/general pictures produced by state-of-the-art GANs. Accumulating the cross-layer feature representations into the final fully connected layers, the suggested CNN may be used to train middle- and high-level, discriminative false features. Further enhancement of the performance of false picture detection may be achieved by the use of the suggested paired learning. The suggested paired learning should allow the proposed false image detector to detect the new GAN's phony images. The suggested strategy beats existing state-of-the-art systems in recall rate and accuracy, according to our testing data.

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.

AUTHOR PROFILES:

Mrs. MOUNIKA.S completed her Bachelor of Technology in Computer Science and Engineering. She completed her Masters of Technology in Computer Science and Engineering from JNTU KAKINADA UNIVERSITY. Currently working as an Assistant Professor in the department of IT at DVR & DR HS MIC COLLEGE OF TECHNOLOGY(Autonomous), Kanchikacherla, NTR(Dist), AP. Her areas of interest are Data Mining, Cloud Computing and Machine Learning & Networks.

Ms. PRAVEENA.P as MCA Student in the Department of DCA at DVR &DR.HS MIC COLLEGE OF TECHNOLOGY, Kanchikcherla, NTR(DT).She completed her BSC(Computers) in Sri Kota Raghavaiah Degree College. Her areas of interests are C, Java, Python.