IDENTIFICATION OF FAKE IMAGES THROUGH CONVOLUTIONAL NEURAL NETWORKS

[1]A.Jyoshna, [2]Akavaram Tejaswini, [3]Sirandasu Sairaj,[4] V. Sampath Kumar

Assistant Professor in department Of IT Teegala Krishna Reddy Engineering College

allenkijyoshna@gmail.com

UG Scholars In Department of IT Teegala Krishna Reddy Engineering College

[2]tejaswiniakavaram@gmail.com ,[3] sairajsirandasu@gmail.com ,[4] sampathkumar.vaspari@gmail.com

Abstract

Now-a-days biometric systems are useful in recognizing person's identity but criminals change their appearance in behavior 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.

I 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) 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 . However, it may lead to a serious problem once the fake or synthesized image is improperly used on social network or platform. For instance, cycle GAN is used to synthesize the fake face image in a pornography video. 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 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. 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 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 . In, the performance fake face image 2 detection can be further improved by adopting the most advanced CNN–Xception network. 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, 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.

II LITERATURE SURVEY

Remote Sensing and Image Interpretation.

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.

Deep Learning: methods and applications

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: expertise or knowledge of the authors; the application areas that have already been transformed by the successful use of deep learning technology, such as speech recognition and computer vision; and 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.

III EXISTING SYSTEM

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.

Disadvantages

- **Data bias:** The accuracy of the neural network model depends on the quality and

quantity of data used for training. If the training data is biased, the model may not perform accurately.

- **False positives:** The neural network model may sometimes identify legitimate profiles as fake, leading to false positives.
- **Resource-intensive:** Training a neural network model requires significant computing power and resources, which can be costly.
- **Complexity:** Building and training a neural network model requires specialized knowledge and expertise, making it difficult for non-experts to replicate the project.
- **Privacy concerns:** The use of neural networks to identify fake profiles may raise privacy concerns, as personal data is used to train the model. It is essential to ensure that user data is handled securely and with consent.

IV PROPOSED SYSTEM

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.

Advantages:

- ***Increased accuracy***: Neural networks can identify patterns in large amounts of data, making them effective at identifying fake profiles across multiple online social networks with a high level of accuracy.
- ***Scalability:*** The neural network model can be trained on a large dataset, making it possible to scale up the project as the number of social networks grows.
- ***Real-time detection:*** The neural network can process data in real-time, making it possible to identify fake profiles as they are created and take action immediately.

- Automation: Once the model is trained, the process of identifying fake profiles can be automated, saving time and resources.

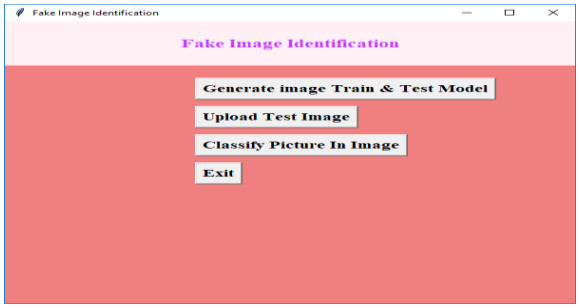
V IMPLEMENTATION

Data Collection **:** In the context of CNN (Convolutional Neural Networks), data collection involves gathering and preparing a dataset that consists of images and their corresponding labels.

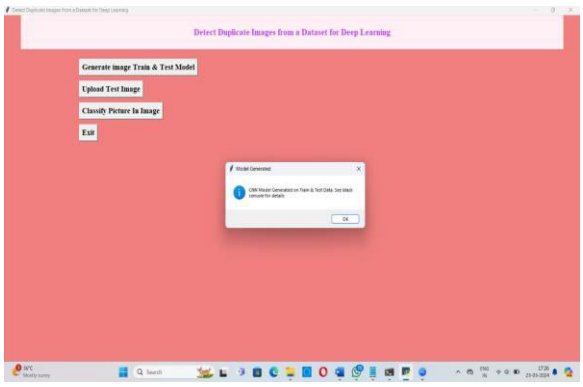
- ***Data Pre-Processing*****:** Data preprocessing in CNN involves standardizing input images, normalizing pixel values, and augmenting the dataset to enhance model performance and generalization.
- ***Feature Extraction*****:** In CNN, feature extraction involves using convolutional layers to automatically learn and extract relevant features from input images, such as edges, textures, and shapes, which are then used for classification or other tasks.

• ***Evaluation Model*:** In CNN, model evaluation involves assessing the performance of the trained neural network using metrics such as accuracy, precision, recall, F1-score, and confusion matrices on a separate test dataset to determine its effectiveness in making predictions on unseen data.

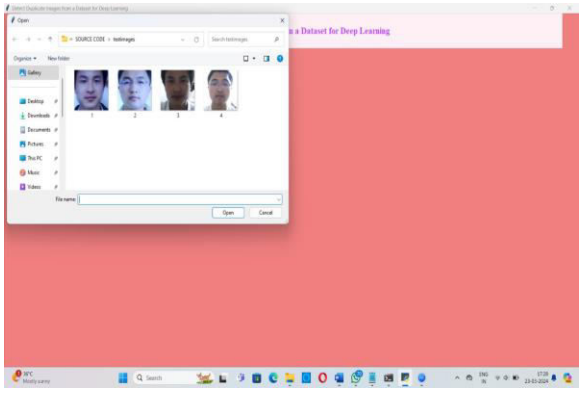
VI RESULTS



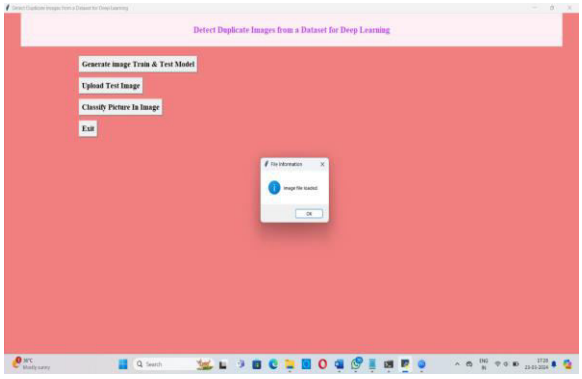
Generate Image Train & Test Model



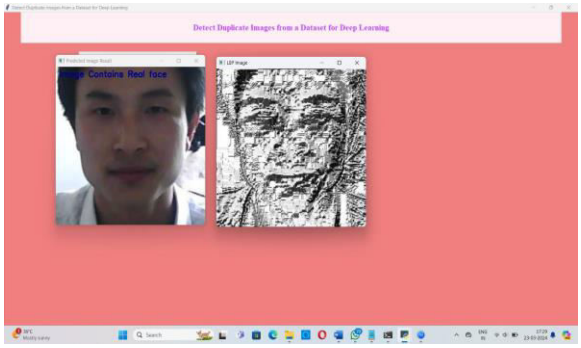
CNN Lbpnet Model

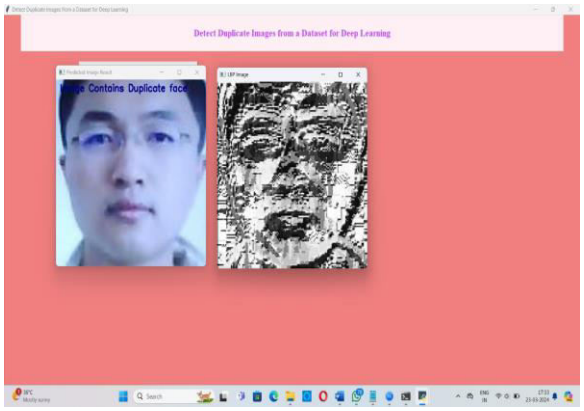


Upload image



Classify Picture in Image





Result

VII CONCLUSION

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. 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. 1610–023

12. H. Farid, “Image forgery detection,” IEEE Signal Processing Magazine, Vol. 26, no. 2, pp. 16–25, 2009

13. S. Bayram, I. Avcibas, B. Sankur, and N. Memon, “Image manipulation de taction with binary similarity
measures,” in Proc. European Signal Processing Conf., Turkey, 2005