ISSN: 2583-7346
DOI: https://doi-ds.org/doilink/05.2024-34964487/IJAEAST.2024.02.0003, February 2024, Volume-2, Issue-2, pp.65-68
International Journal of Advances in Engineering Architecture Science and Technology

Deepfake Face Image Detection Using Deep Learning

K. Anjani[1], K. Sahithi[2], V. Sri Vyshnavi[3], B. Sarath[4], K. Divya Kalyani[5]

[1,2,3,4]Student, Department of Computer Science & Engineering, Dadi Institute of Engineering and Technology (Autonomous), Andhra Pradesh, India

[5]Assistant Professor, Department of Computer Science & Engineering, Dadi Institute of Engineering and Technology (Autonomous), Andhra Pradesh, India

sahithikorukonda123@gmail.com[2]

Received: 23-01-2024 **Accepted:** 23-02-2024 **Published:** 26-02-2024

Abstract

Background: An AI-based free programming device has made it simple to make trustworthy face trades in images that leave not many hints of control, in what is known as "deepfake" images.
Objectives: These sensible phony recordings are utilized to make political trouble, coerce somebody or phony psychological warfare occasions, are effortlessly imagined.
Statistical Analysis: Convolutional. In this project we are designing LBP Based deep learning Convolution Neural Network called LBPNET to detect fake face images.
Findings: **E***xt*ract LBP from images and then train LBP descriptor images with Convolution Neural Network to generate training model.
Applications and Improvements: The 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.

Keywords: Deepfake, Face Image Detection, Deep Learning.

1. Introduction

Detecting fake faces can be a challenging task, as fake technology has become increasingly sophisticated. However, there are several methods and techniques that researchers and technology companies have developed to help identify fake faces. Here are some common approaches to detecting fake faces:

Inconsistencies in Facial Features

Fake faces often exhibit subtle inconsistencies that may not be present in real faces. These can include unusual lighting and shading, misaligned facial features, or artifacts around the eyes, mouth, or hairline. Deep learning models can be trained to spot these irregularities.

Blinking and Facial Expressions

Fake videos may lack natural blinking patterns and facial expressions. Some fake algorithms struggle to generate convincing eye movements and subtle facial changes, which can be detected through careful analysis of the video frames.

Lack of Emotional Expression

ISSN: 2583-7346
DOI: https://doi-ds.org/doilink/05.2024-34964487/IJAEAST.2024.02.0003, February 2024, Volume-2, Issue-2, pp.65-68
International Journal of Advances in Engineering Architecture Science and Technology

Fake faces may not exhibit appropriate emotional responses to the content of the video or audio. For example, the facial expressions and emotions displayed may not align with the context of the conversation or situation.

Analysis of Metadata

Examining the metadata of a video file can provide clues. For instance, checking the creation date, editing history, and the source of the video can help determine its authenticity.

2. Literature Survey

The broad adoption of Deep Fakes is attributable to the high quality of the faked movies and the ease with which their programmes may be used by a wide variety of users, from professionals to novices with varied degrees of programming ability. The creation of these apps typically involves the use of deep learning methods. It is well-established that deep learning can successfully represent complex and high-dimensional data. For dimensionality reduction, a specific type of deep network called deep autoencoders has been frequently used and image compression. The first effort at deep-fake creation was Fake App, developed by an Internet user utilizing the auto encoder-decoder pairing structure. However, created a stunning Deep Fake data set that is made up completely of 620 videos. They used the GAN model and the Deep Fake data set. Deep Fake film was created using low and high-quality Face swap-GAN Open-Source Code Videos from the publicly available VidTIMIT website, which can faithfully mimic facial gestures, lip movements, and eye blinking. These films were also used to test several deep false detection techniques. When used to identify Deep Fake films from this freshly created data set, different approaches, such as lip-syncing methods and support vector machine (SVM) picture quality metrics, produce exceptionally high mistake rates. Deep Fake is another technique cybercriminals use to get past authentication or identity checks and get unauthorized access. (CNN) and (GAN) are two examples of deep learning tools that have made preserving facial characteristics and posture more challenging for forensic models in switched-face images. as well as the photographs' lighting. Zhang et al. employed the bag of words method to extract a group of condensed traits, which they then fed into classification algorithms, including SVM, random forest, and multi-layer perceptron's (MLP) to distinguish from the real swapped face photographs. Since GAN models can learn how to disperse detailed input data, their synthesized images are accurate and high-quality, possibly, the most challenging deep learning-generated images to categorize. Recently conducted a study and pointed out Artificial neural networks (ANNs) as it takes some of their fundamental ideas from how the human brain operates. This section comprises the study related to techniques of Fake image/ video detection. Philip S.Yuet al., (2018) aimed to use TI-CNN. TI-CNN is trained with both text and picture input at the same time by projecting explicit and latent characteristics into a unified feature space. Aswini Thota et al., (2018) described a method for fake news detection to obtain an accuracy of 94.21 percent on test data, a precisely calibrated Tiff-IDF - Dense neural network (DNN) model used in it. Research fraternity has been using Deep learning Methods as well as Artificial Intelligence Techniques for identifying forgery contents. Connor Shorten et al., (2019) When the models are assessed on supplemented test data, they achieve 50.99 percent accuracy on the CIFAR-10 dataset against 70.06 percent accuracy on the CIFAR-10 dataset. Krithi Dinesh et al., (2019) [proposed an approach of fake news detection with the use of SVM, Naive Bays and Logistic Regression dataset. Andreas Rossleret al., (2019) focused on the impact of compression on the detestability of state-of-the-art manipulation algorithms in this project, and a standardized baseline for future research is proposed.

ISSN: 2583-7346
DOI: https://doi-ds.org/doilink/05.2024-34964487/IJAEAST.2024.02.0003, February 2024, Volume-2, Issue-2, pp.65-68
International Journal of Advances in Engineering Architecture Science and Technology

3. Methodology

The Deepfake images based on fake and real human faces are utilized for building employed neural network techniques. The fake and real faces are structured with the target label into a dataset. The structured deepfake dataset is split into train, validation, and test data portions. The 90% train portion of the dataset is utilized for training employed neural network techniques. The outperformed LBP (Local binary pattern) approach is fully hyper-parametrized to give the best accuracy score in deepfake detection. The performance evaluation of neural network techniques on unseen test data is determined by 10% of the test portion. The LBP proposed approach makes predictions on unseen data with high accuracy results. An advanced proposed deep learning-based approach is in a generalized form and ready to detect the fake and real faces in deployment.

4. Proposed System

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

1. Divide the examined window into cells (e.g. 16x16 pixels for each cell).
2. 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.
3. 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).
4. 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.
5. Optionally normalize the histogram.
6. Concatenate (normalized) histograms of all cells. This gives a feature vector for the entire window.
7. 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.

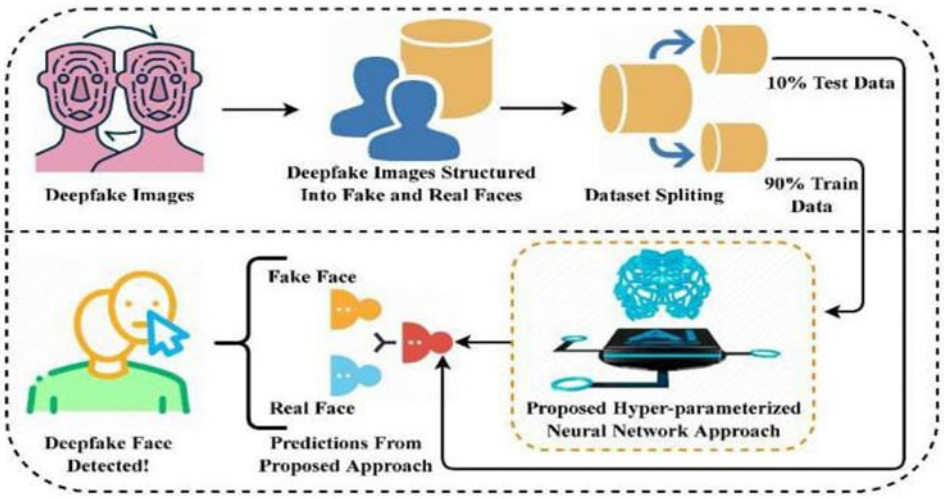

Figure 1. Fake Face Image Detection Architecture

5. Conclusion

In this project, 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 out performs 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 depth wise separable convolutions. Proc. of the IEEE conference on 276 Computer Vision and Pattern Recognition 2017, pp. 1610–02357.