



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 4, April 2024

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.423

9940 572 462

6381 907 438

ijirset@gmail.com

www.ijirset.com

Deep Learning-Based Gender Classification by Training with Fake Data

Dr.V.K.Buvenesvari, G.Barath, M.Dinesh, S.Arulkumar, S.Dinesh

Associate Professor, Department of MCA, Muthayammal Engineering College, Namakkal, Tamilnadu, India

Final Year Student, Department of MCA, Muthayammal Engineering College, Namakkal, Tamilnadu, India

ABSTRACT: Recently, the dangers associated with face generation technology have been attracting much attention in image processing and forensic science. The current face anti-spoofing methods based on Generative Adversarial Networks (GANs) suffer from defects such as overfitting and generalization problems. This paper proposes a new generation method using a one-class classification model to judge the authenticity of facial images for the purpose of realizing a method to generate a model that is as compatible as possible with other datasets and new data, rather than strongly depending on the dataset used for training. The method proposed in this paper has the following features: (a) we adopted various filter enhancement methods as basic pseudo-image generation methods for data enhancement; (b) an improved Multi-Channel Convolutional Neural Network (MCCNN) was adopted as the main network, making it possible to accept multiple preprocessed data individually, obtain feature maps, and extract attention maps; (c) as a first ingenuity in training the main network, we augmented the data using weakly supervised learning methods to add attention cropping and dropping to the data; (d) as a second ingenuity in training the main network, we trained it in two steps. In the first step, we used a binary classification loss function to ensure that known fake facial features generated by known GAN networks were filtered out. In the second step, we used a one-class classification loss function to deal with the various types of GAN networks or unknown fake face generation methods. We compared our proposed method with four recent methods. Our experiments demonstrate that the proposed method improves cross-domain detection efficiency while maintaining source-domain accuracy. These studies show one possible direction for improving the correct answer rate in judging facial image authenticity, thereby making a great contribution both academically and practically.

KEYWORDS: Multi-Channel Convolutional Neural Network (MCCNN), GAN network, Deep Learning, Deepfakes, Ensemble, Machine

Learning Classifiers

I. INTRODUCTION

Gender and age play a significant role in interpersonal interactions among people who live in communities. The use of smart gadgets has expanded as technology has progressed, and social media has begun to draw everyone's attention. Daily studies on gender and age prediction have grown in prominence, it increases the number of apps that use such techniques. In these applications, facial photographs are commonly employed since they contain useful information that may be used to extract human interaction. For gender detection and age prediction, Image processing, feature extraction, and classification steps are usually used. These steps may change based on the objective of the study and the characteristics to be used. The face images were processed using a variety of approaches, and calculations were performed based on the results of the investigations. For image processing, there are two basic and typical which we need to follow. Image enhancement is the process of improving an image so that the resultant image is of higher quality and can be used by other applications. The most popular technique for extracting information from an image is the other technique. The image is divided into a specified number of parts or objects in order to solve the challenge and this procedure is called Segmentation. Due to the accuracy of its classification technique, deep learning techniques are a variety of tasks such as classification, feature extraction, object recognition, and so on, it helps in gender and age prediction.

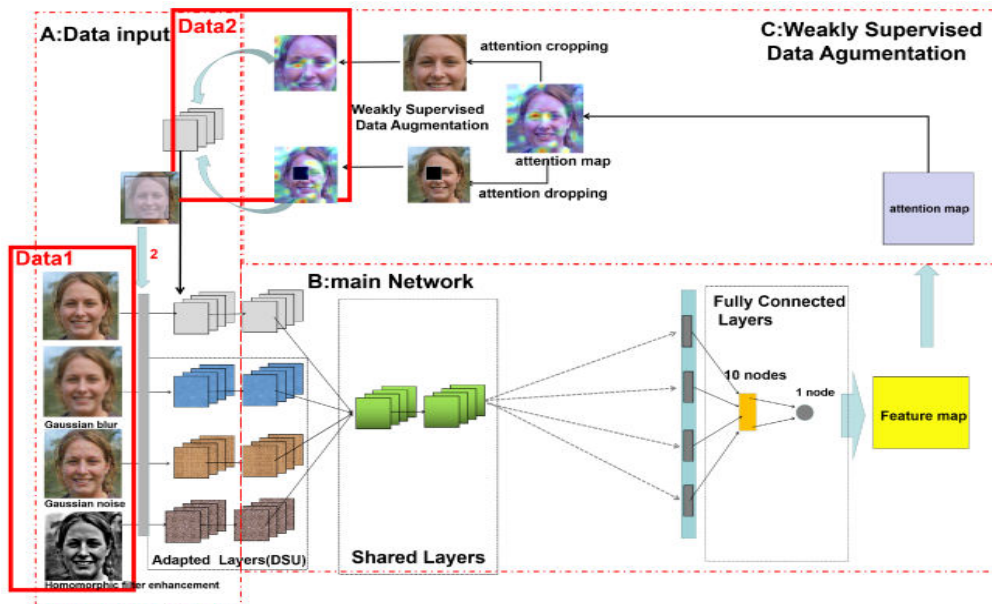


Fig 1: Deep Learning Based One-Class Detection System

The previous system’s machine learning algorithms were not utilized to improve classification skills for a vast number of images and data available via the internet. In this paper, Deep Learning techniques are used to reliably estimate a person's gender and age from a single facial capture. 'Male' or 'Female' will be the predicted gender. We might use age categories based on the experiment to forecast a person's age. The eyes are one of the most essential aspects of face images in various applications such as facial recognition and emotional expression. Human Facial Image Processing gives numerous hints and signs that can be applied to a variety of businesses, security, entertainment, and others. The expression on a person's face can reveal a lot of information about them, such as their emotional condition, the slightest agreement or disagreement, irony or fury, and so on. Faces have become an important subject of study in psychology for this reason. Gender detection can provide a wealth of information to firms' recruitment teams, for example. Verification of ID cards, such as voter ID cards, which are used by millions of people to vote in elections, and so on. Finding ineligible or fraudulent individuals is made easier with human facial image analysis.

II. RELATED WORK

Before the rise of deep learning techniques, image manipulation techniques could create realistic fake images. Nonetheless, this procedure required extremely expert image editing and, as a result, a significant amount of time. Deepfake Indiscernible replicas are produced by several deepfake generation models, however, these fakes can still be found using either deep learning methods or specialist scientific approaches. The convolution techniques used by almost all deepfake generators are visible in the image. Even though these traces can be found with a thorough investigation, the volume of data being published to social media sites today calls for quick and automated techniques. Deepfake images’ convolutional traces can be easily found using supervised deep-learning techniques if the user supplies adequate training data. presented a deep learning approach based on a relatively tiny network called MesoNet to detect whether a video is false. In their research, the authors analyze each frame individually to find deepfakes.

Additionally, classifies the frames based on their optical flow. The gradient between neighboring video frames was used to train a CNN(Convolutional Neural Network) to detect sudden changes in the video. These rapid transitions demonstrate how frame-by-frame deepfake films are generated. The representation of the training dataset affects a wide range of deep learning-based deepfake detection techniques, as mentioned. If a detector was not trained with data

generated by a specific deepfake approach, it would almost certainly perform poorly when confronted with such a method after deployment.

By estimating the 3D head position from 2D facial area information, a different method for identifying changes was introduced in [28]. The estimated variance between head orientations was used as the vector of a key point in SVM training to distinguish between authentic and fake visual input. The methodology in [28] yields improved deepfake detection results; nevertheless, its effectiveness diminishes for blurred data. An approach to distinguishing the generated faces from suspicious samples was put out by [29]. With the help of the SVM and random forest, multimedia stream descriptors [30] were used to estimate key points and classify the real from the false images. The method demonstrates a low-cost method for detecting deep fakes, however for video re-encoding attacks, the detection precision decreases. The use of biological signals, such as heart rate, computed from the input video sample’s facial region, as a deepfakes detection approach was first described in [7]. The computed characteristics were utilized to locate the actual and changed data using SVM and CNN-based classifiers. Although the technique is effective at detecting tampering, it is vulnerable to attacks including video post-processing.

III. METHODOLOGY

DEEP LEARNING Deep learning is an artificial intelligence (AI) technique that seeks to learn from experience to resemble the human brain. Through a training procedure, these representations are learned. To teach the software how to detect an object, we must first train it with a large number of object images that we categorise according to different classes. Deep learning-based algorithms, on average, require a large amount of training data and take longer to train than traditional machine learning methods. Finding unique attributes when trying to recognise any object or character on an image is time-consuming and complex. Unlike traditional machine learning, where features are manually retrieved, problems can be solved using deep learning approaches, which extract important characteristics from data automatically. A neural network with multiple hidden layers is known as deep learning. They may build complicated notions from simple concepts after an image has been taught over the network. By integrating simple elements such as shape, edges, and corners, an image can be trained in the network to learn items such as characters, faces, and so on. As the image travels through the layers, each one gets a simple property while moving on to the next. As the layers grow larger, the network may learn more complex features and eventually merge them to identify the image. In the field of computer vision, deep learning has discovered a bunch of use. The domains that work with facial data were among the most important computer vision applications.

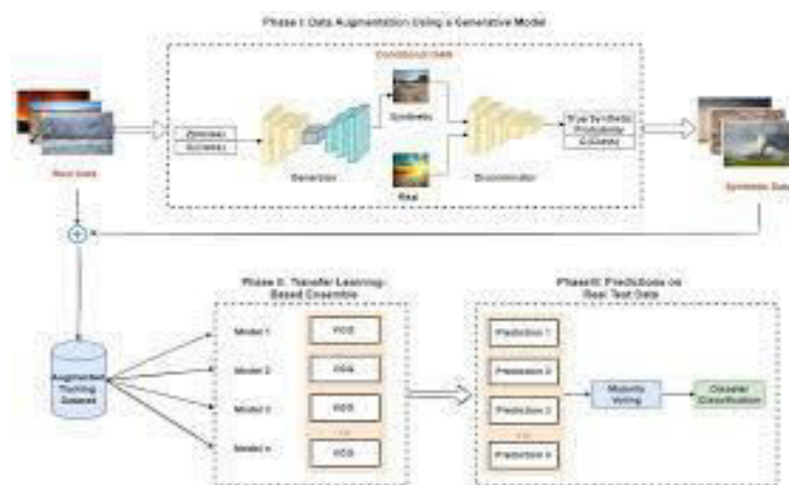


Fig 2: Work Flow



CONVOLUTIONAL NEURAL NETWORK (CNN) A CNN (convolutional neural network) is a kind of artificial neural network that is commonly used for image or object identification and categorization. Using a CNN, Deep Learning recognises items in an image. An input layer, hidden layers, and an output layer are all part of a standard neural network. The anatomy of the brain inspired CNNs. Artificial neurons or nodes in CNNs collect inputs, process them, and deliver the result as output, rather like a neuron inside the brain functions and transmits signals between cells. The images are used as a source of data. Multiple hidden layers may exist in CNNs, each of which performs feature extraction from the image by performing calculations. The very first layer that extracts feature out of an input image is convolution. The object is classified and identified in the output layer by the fully connected layer. The convolutional layer is the most important constituent of CNN. The mathematical procedure of convolution is used to combine two sources of data. Gender estimation from social image collection, images that do not require access to private details of the subject areas that are not displayed in the images, such as their birth date, and the usual approach that includes the collection of other information about an individual and on the basis about which we discover gender on manually handled annotated data for gender recognition. That is why we use D-CNN, which works directly on images and aids in precise gender estimation. Overfitting is usually a minor issue. Comes into play if deep learning or machine learning-based approaches are used on a dataset with such a small number of face images.

CNN MODEL We must first extract the face from a webcam image before proceeding with the implementation. The OpenCV library in Python is used to accomplish this. An effective object detection method is face detection utilising Haar feature-based cascade classifiers, which is a machine learning-based approach. There will be a large number of positive and negative photos, on which the classifier will be trained. It's then utilised to find faces in other pictures. Figure 2 shows a schematic illustration of the CNN model.

IV. RESULT ANALYSIS

ALGORITHM FOR GENDER AND AGE PREDICTION

A face recognition system is a bit of software that can match a human face in a video or digital image frame to a database of faces. Woody Bledsoe, Helen Chan Wolf, and Charles Bisson were among the first to develop facial recognition technology. Bledsoe, Wolf, and Bisson began working with computers to recognise human faces in 1964 and 1965. When detecting a face in a frame, some natural (lighting, posing angles, facial labeling) and digital (noise, interference) alterations are applied. Two properties of a human face as a template contribute to the difficulty of recognising a human face: (1) The number of templates, or faces to be categorized, is enormous and almost certainly limitless. (2) Almost every pattern looks the same. We can use several sorts of audience records to fix this problem and keep the algorithm more efficient. In neural networks, the audience set also acts as a standard for gender detection categorization.

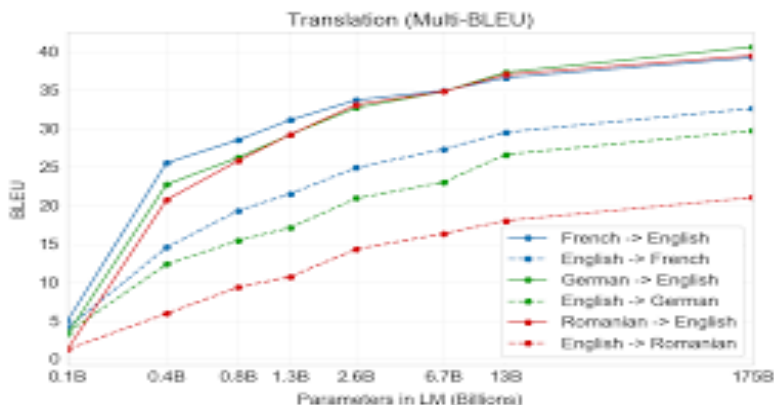


Fig 3: Result Analysis

We use Python Deep Learning in this study to detect specific gender and age of provided facial data. Deep Learning is part of the machine learning category. Deep Learning is an Artificial Intelligence technology that mimics the functioning of human cognitive processing. From unstructured data collections, it can identify objects, people, talks, and characters. Input, Face Detection, Face Processing (Gender and Age classification), and Output are the four key sections of the algorithm

V. CONCLUSION

Age and Gender Classification are two of the most essential resources for getting information from an individual. Human faces contain enough information to be useful for a variety of purposes. Human age and gender classification are critical for reaching the right audience. We attempted to replicate the process using standard equipment. The algorithm's efficiency is determined by a number of factors, but the major goal of this study is to make it as simple and quick as possible while maintaining the highest level of accuracy. Work is being done to improve the algorithm's efficiency. Future enhancements include discarding faces for nonhuman objects, adding more datasets for people of other ethnic groups, and giving the computer more granular control over its workflow. Deep learning and CNN could be used to improve this prototype's ability to reliably identify a person's gender and age range out of a single image of their face. From this study, we can conclude with two important conclusions. First, despite the limited availability of age and gender-tagged photos, CNN can be used to improve age and gender detection outcomes. Second, by employing additional training data and more complex systems, the system's performance can be slightly increased.

REFERENCES

1. Mo, H.; Chen, B.; Luo, W. Fake faces identification via convolutional neural network. In Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security, Innsbruck, Austria, 20–22 June 2018; pp. 43–47. [[Google Scholar](#)]
2. Cozzolino, D.; Thies, J.; Rössler, A.; Riess, C.; Nießner, M.; Verdoliva, L. Forensictransfer: Weakly-supervised domain adaptation for forgery detection. *arXiv* **2018**, arXiv:1812.02510. [[Google Scholar](#)]
3. Quan, W.; Wang, K.; Yan, D.M.; Zhang, X. Distinguishing between natural and computer-generated images using convolutional neural networks. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2772–2787. [[Google Scholar](#)] [[CrossRef](#)]
4. Goodfellow, I.; Pouget-Abadie, J.; Mirza, M.; Xu, B.; Warde-Farley, D.; Ozair, S.; Courville, A.; Bengio, Y. Generative adversarial nets. In Proceedings of the 27th International Conference on Neural Information Processing Systems, Montreal, QC, Canada, 8–13 December 2014; 2014; Volume 2, pp. 2672–2680. [[Google Scholar](#)]
5. Radford, A.; Metz, L.; Chintala, S. Unsupervised representation learning with deep convolutional generative adversarial networks. *arXiv* **2015**, arXiv:1511.06434. [[Google Scholar](#)]
6. Isola, P.; Zhu, J.Y.; Zhou, T.; Efros, A.A. Image-to-image translation with conditional adversarial networks. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Honolulu, HI, USA, 21–26 July 2017; pp. 1125–1134. [[Google Scholar](#)]
7. Zhu, J.Y.; Park, T.; Isola, P.; Efros, A.A. Unpaired image-to-image translation using cycle-consistent adversarial networks. In Proceedings of the IEEE International Conference on Computer Vision, Venice, Italy, 22–29 October 2017; pp. 2223–2232. [[Google Scholar](#)]
8. Zhang, H.; Goodfellow, I.; Metaxas, D.; Odena, A. Self-attention generative adversarial networks. In Proceedings of the International Conference on Machine Learning, Long Beach, CA, USA, 10–15 June 2019; pp. 7354–7363. [[Google Scholar](#)]
9. Brock, A.; Donahue, J.; Simonyan, K. Large scale GAN training for high fidelity natural image synthesis. *arXiv* **2018**, arXiv:1809.11096. [[Google Scholar](#)]
10. Daras, G.; Odena, A.; Zhang, H.; Dimakis, A.G. Your local GAN: Designing two dimensional local attention mechanisms for generative models. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Seattle, WA, USA, 13 June 2020; pp. 14531–14539. [[Google Scholar](#)]
11. Gao, H.; Pei, J.; Huang, H. Progan: Network embedding via proximity generative adversarial network. In Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, Anchorage, AK, USA, 4–8 August 2019; pp. 1308–1316. [[Google Scholar](#)]

12. Karras, T.; Laine, S.; Aila, T. A style-based generator architecture for generative adversarial networks. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Long Beach, CA, USA, 15–20 June 2019; pp. 4401–4410. [[Google Scholar](#)]
13. Karnewar, A.; Wang, O. MSG-GAN: Multi-Scale Gradient GAN for Stable Image Synthesis. In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Seattle, WA, USA, 13–19 June 2020; pp. 7796–7805. [[Google Scholar](#)]
14. Karras, T.; Laine, S.; Aittala, M.; Hellsten, J.; Lehtinen, J.; Aila, T. Analyzing and improving the image quality of stylegan. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Seattle, WA, USA, 13–19 June 2020; pp. 8110–8119. [[Google Scholar](#)]
15. Neethirajan, S. Is Seeing Still Believing? Leveraging Deepfake Technology for Livestock Farming. *Front. Vet. Sci.* **2021**, *8*, 740253. [[Google Scholar](#)] [[CrossRef](#)] [[PubMed](#)]
16. Greengard, S. Will deepfakes do deep damage? *Commun. ACM* **2019**, *63*, 17–19. [[Google Scholar](#)] [[CrossRef](#)] [[Green Version](#)]
17. Marra, F.; Gragnaniello, D.; Verdoliva, L.; Poggi, G. Do gans leave artificial fingerprints? In Proceedings of the 2019 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), San Jose, CA, USA, 28–30 March 2019; pp. 506–511. [[Google Scholar](#)]
18. Marra, F.; Saltori, C.; Boato, G.; Verdoliva, L. Incremental learning for the detection and classification of gan-generated images. In Proceedings of the 2019 IEEE International Workshop on Information Forensics and Security (WIFS), San Jose, CA, USA, 28–30 March 2019; pp. 1–6. [[Google Scholar](#)]
19. Chawla, N.V.; Bowyer, K.W.; Hall, L.O.; Kegelmeyer, W.P. SMOTE: Synthetic minority over-sampling technique. *J. Artif. Intell. Res.* **2002**, *16*, 321–357. [[Google Scholar](#)] [[CrossRef](#)]
20. Inoue, H. Data augmentation by pairing samples for images classification. *arXiv* **2018**, arXiv:1801.02929. [[Google Scholar](#)]



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details