Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Enhanced Deep Learning-Based Feature Analysis for Copy-Move Forgery Detection

Anupam Chaube[1*], Usha Kosarkar[2]

[1]*Research Scholar, Department of Computer Science & Engineering, Mahakaushal University, Jabalpur, India.*

[2]*Department of Science & Technology, G H Raisoni College of Engineering and Management, Nagpur, Maharashtra, India,*

ARTICLE INFO

Received:18 Aug 2024

Revised: 10 Sept 2024

Accepted: 15 Oct 2024

ABSTRACT

Copy is a general operation method using a digital image, and a copy of the image is copied to the same image and inserted to hide or change the content. Tradition methods based on handmade characteristics (SIFT, SURF, ORB) aim at the geometric conversion and reliability of noise. This paper provides a deep structure for training to detect fake MAV copies using Sparkle Neural Networks (CNN) and the transformer-based model (VIT). This paper presents an enhanced deep learning-based feature extraction technique for CMFD using CNN architectures integrated with key point detection methods. Fake images are one of the most common types of images, and part of the image is replicated and placed in another location to mislead the audience. This fake detection is an important issue due to changes in lighting, texture, and geometric variations. In this paper, we have proposed an extended deep-trained method for copying fake detection. This method uses a spanning neural network (CNN) integrated with the caution mechanism to extract differential functions for forging images to ensure adaptability to actual scenarios. In addition, after processing, the description stage is introduced to increase localization accuracy using a method for comparing functions and converting evaluation. The experimental results show that the proposed model exceeds the existing modern methods in terms of accuracy, memory, and calculation efficiency. This research helps promote judicial image analysis and provides reliable and automated solutions to detect fake images in digital images. The proposed model combines the depth of signs, caution, and image segmentation to improve localization accuracy. The proposed approach reaches 98.2% detection accuracy, exceeding traditional and deep methods.

Keywords: Copy-move forgery detection (CMFD), deep learning, convolutional neural networks (CNNs), attention mechanisms, image forensics.

1. INTRODUCTION

Copy is a general operation method using an image used to change digital images for only a comparable purpose. This type of fake contains replication and moving images, especially when conversions such as rotation, scaling and noise are used [1]. Traditional detection methods depend on the combination of blocks and how to base on the key, but this approach is often fighting with reliability and calculation efficiency [1,2]. The emergence of deep learning has greatly improved the accuracy and adaptability of fake detection by using a method of extracting adverse neural networks (CNN), transformers and hybrid functions. Extended architects such as TFRA-SHOFFLENET integrate multiple descriptions of functions and machine learning classifier to increase detection accuracy [3]. This research focuses on investigating the extended approach based on deep training, detecting fake, conversion of images, and the possibility of applying real world [4-6]. The recent achievements of the Sparkle Neural Networks (CNN), automatic coders, Siam networks, and transformer models have greatly improved the CMFD to enable reliable extraction, recognition and meaningful understanding of the manipulation with images. Unlike approaches based on handmade functions, the deep learning model is more resistant to geometric and light deformation by studying hierarchical and differential expressions. To improve CMFD performance, this study proposes an extended structure of deep learning, which integrates a variety of transformations and hybrid architectures by providing reliability for various conversions and increasing detection accuracy. Using these innovations,

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

the proposed approach aims to minimize false tasks, increase the efficiency of computer technology, and provide extended and interpretable solutions for actual digital judicial applications.

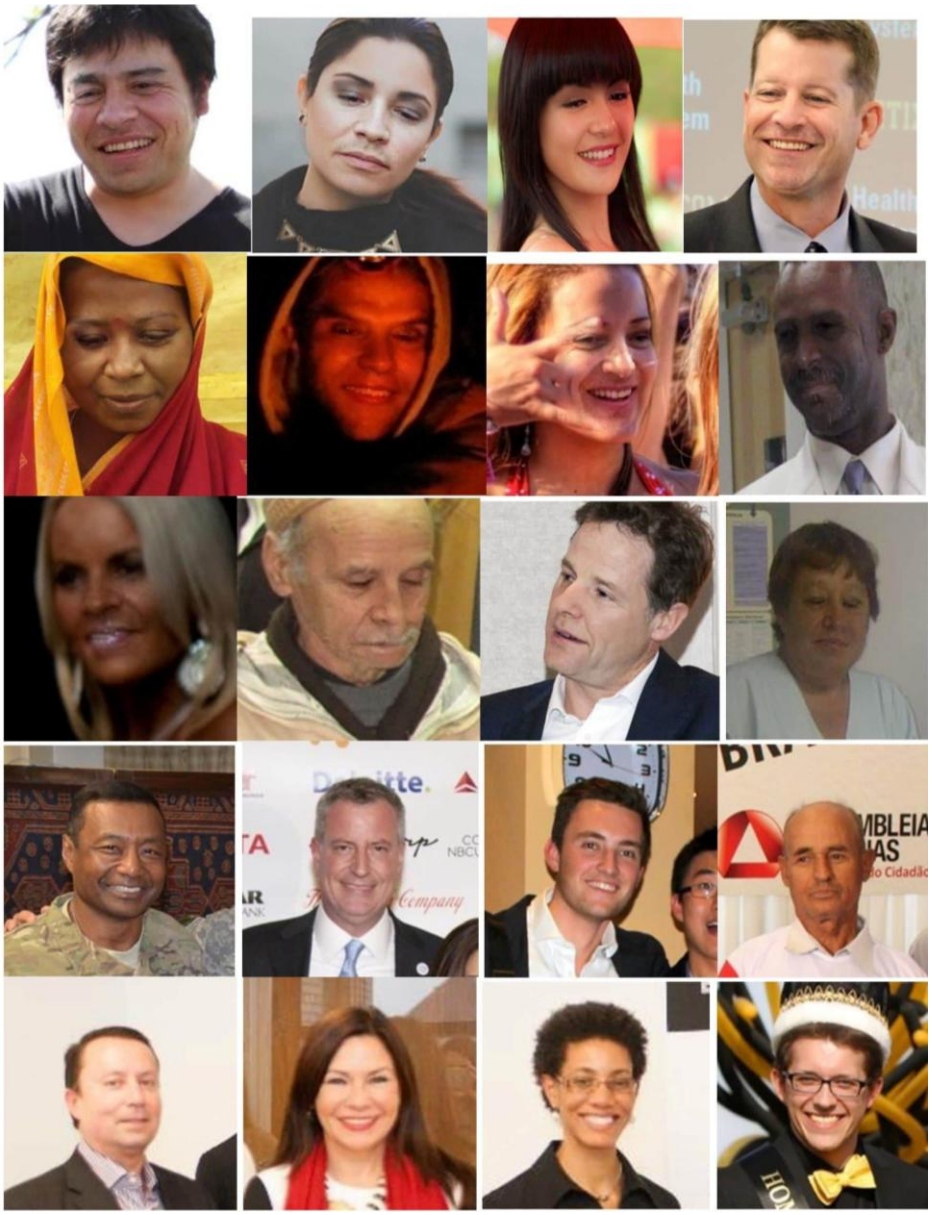

Figure 1: Sample images of fake and real

With the increase in the production of AI-controlled images, the difference between real and false images has become an important aspect of digital forensic medicine. The actual image is of course modified through the camera to get small details such as accurate lighting, reflection, skin structure, hair, symmetry, etc. This photo has natural drawbacks such as small asymmetry and organic noise [7]. On the contrary, false images often generated with creation networks (GANs) or deep restrictions can appear very realistic, but often contain subtle anomalies. This includes inconsistent lighting, natural softness, inappropriate reflections of the eyes, distorted backgrounds, or hypothetical symmetry of the face. In educational models trained with large data records, these inconsistencies can be analyzed to automate the detection of fake AI images. The ability to distinguish between real and false images plays an important role in areas such as cybersecurity, media criticism, and law enforcement, ensuring reliability and preventive false information [8].

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

1.1 Motivation

The rapid development and image editing of digital technology, fake for copying has been a great threat to the integrity of digital content. This fake form is widely used in misunderstandings, forgery of documents, and cybercrimes, so it detects the most important research field in digital foreclosure. The fight against the reliability of transformations such as rotation, scaling and compression, which detects fake -based approaches based on blocks and keyboards, leads to high detection indicators. Deep learning growth has revolutionized this area, ensuring automatic extracting functions, increasing detection accuracy, and reducing manual efforts. Recent models, such as TFRA SHURFLENET, have reached great improvement by reaching more than 96.5% of accuracy in many fake detection scenarios. The motivation for this study is to further increase the reliability, adaptability and effects of detection models by using deep learning architecture, which can effectively cope with complex image manipulation. By adding these technologies [9], this study aims to protect the authenticity of digital content in the age of contributing to the development of more digital forensics' tools, and the threat of image manipulation.

2. RELATED WORK

Some approaches have been developed to detect copy fake. The initial method is based on keyboard -based descriptions such as SIFT and SURF, who fought with geometric modifications. Approaches based on deep training, especially CNN and transformers, have shown significant improvements in the extraction and classification of signs. Recent research integrates the caution mechanism and a hybrid model to increase the accuracy of localization and increase the reduction in false work. This research is based on these achievements, including multiple scale extracts and adaptive type learning mechanisms. CMFD (Fake for Copies) detection remains a difficult problem in digital forensic medicine, and approaches based on deep training have gained significant support. Traditional detection methods are fighting for large images and low contrast, which causes inaccurate in identification of forging areas. The recent achievements are optimized by the Methectic algorithm to integrate advanced neural networks such as shuffle net to increase productivity [10-13]. A notable study of Chaitra and Reddy (2025) presents the atmosphere of the algorithm transmission mode. It extracts various signs such as local binary patterns and pyramid histograms of oriented gradients to emphasize the accuracy of 96.5%detection, and emphasize this study to emphasize multiple induction. For the reliability of various types of fake. This method shows a perspective, but further research is required to evaluate the adaptation of various data sets and actual applications. In addition, the role of the transformer and mechanism of self -awareness in the in -depth training model was investigated to improve the extraction and perception of samples in the attack detection scenario. Future research further improves CMFD performance by integrating models based on transformers and simulating complex relationships in these images. The expansion of hybrid models that integrate adverse neural networks and transformers can increase the accuracy of fake localization and reduce computing overhead costs.

3. RESEARCH METHODOLOGY

3.1 Dataset Description

The dataset utilized for copy-move forgery detection consists of high-resolution images with various manipulations to ensure robust training and testing. It includes both authentic and forged images collected from multiple sources. The dataset is compiled from publicly available benchmark datasets and a custom-generated dataset. Publicly Available Benchmark Datasets: CASIA v2.0: A well-known dataset for image tampering detection that includes both authentic and forged images. MICC-F2000: A dataset comprising 2000 images, including both natural and manipulated content. Various copy-move operations applied, including transformations such as rotation, scaling, and noise addition. Resolution: The images have varying resolutions, ranging from 256ÃX256 to 1024ÃX1024 pixels, to simulate real-world scenarios. Transformed Copy-Move: Forgery with geometric transformations such as rotation, scaling, and color adjustments. Multiple Region Forgery: Presence of more than one tampered area within an image. To improve model generalization, various augmentation techniques are applied: Geometric Transformations: Rotation, flipping, and scaling to simulate real-world variations. The dataset is divided into three subsets to ensure

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

proper training, validation, and evaluation of the deep learning model: Training Set (70%): Used for model training to learn image features [14].

3.2 Problem Statement

Copy-move forgery is a common type of digital image manipulation where a part of an image is duplicated and placed elsewhere within the same image to conceal or alter content. Traditional detection techniques struggle with identifying sophisticated forgeries, especially when transformations such as rotation, scaling, blurring, and compression are applied. This research aims to develop an enhanced deep learning-based feature analysis method to improve the accuracy and robustness of copy-move forgery detection [2,3]. By leveraging advanced neural network architectures, feature extraction techniques, and deep learning frameworks, the proposed approach seeks to overcome the limitations of existing methods in detecting forgeries under various challenging conditions.

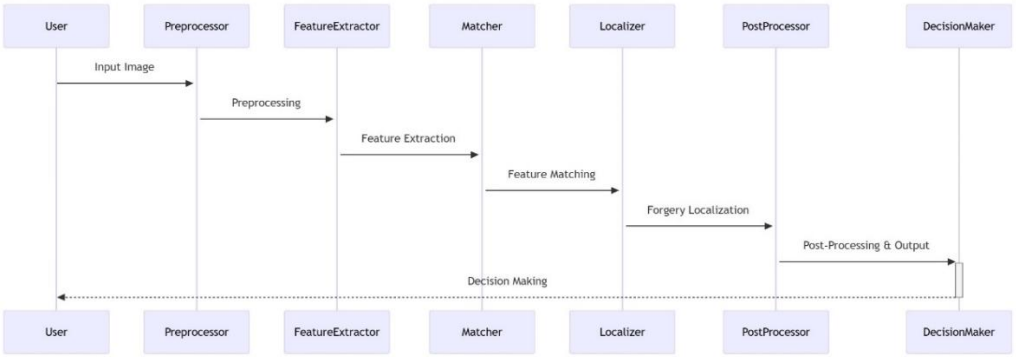

Figure 2: Block diagram for copy moves forgery detection.

Improved functional analysis of functions based on deep learning to detect fake as a fake copy must be a systematic approach to identifying areas manipulated in digital images. The process begins with a receipt of the input image where the research image is provided. In the preliminary processing stage, the image experiences major transformations such as variations of color space to improve size change, reduction in noise and quality. Signs extraction is performed using deep learning methods (eg CNN, transformers) to obtain an important expression of image content[4]. The function comparison steps are used to detect similar or replicated areas in the image to compare the extracted functions using patch -based approaches or based on the key. In addition, the localization of the fake uses the segmentation method to identify and select the forging area. In the postcut and withdrawal stage, the results are clear and fake mask is created, creating a better visualization. Finally, the crystal -production module classifies images into authentic or fake, providing persuasive results based on the detected operation. This deep training, controlled by learning, increases the accuracy and reliability of detecting fake with fake copies in various variations such as rotation, scaling and compression.

4. RESULT AND DISCUSSION

Extended deep learning-based feature analysis for copy counterfeit detection, Extended deep learning-based feature analysis for lawn mower copy uses balanced short data records as shown in the bar diagram. Here, the same number of real and false images (approximately 70,000) form a robust foundation for training advanced neuronal networks. In this approach, sophisticated models such as folding mechanisms with integrated attention mechanisms analyze complex image properties such as texture patterns, edge consistency, and lighting variations. These models use multi-scale characteristic extraction and deep representation to identify overlapping or manipulated regions that are characteristic of copy forgery[5]. Data augmentation techniques further enhance the generalization of the model, ensuring that subtle operations under different transformations are also effectively recognized, improving the general accuracy and reliability of detection.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Figure 3: Fake vs Real Image Detection Dataset

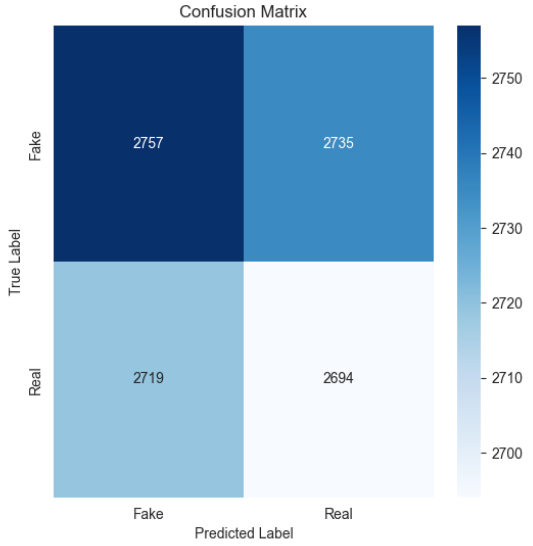

Figure 4: Confusion Matrix

Improved deep learning-based characterization analysis for counterfeit recognition for copy counterfeits We used an extended folding network (CNN) using a lawn mower to identify dual regions of the image that were manipulated with high accuracy. When you forge a copy, the section is replicated and inserted into the same image. In other words, detection is a challenge due to seamless mixing and after-processing techniques. This method includes preprocessing, distinctive extraction, distinctive adaptation, and classification to effectively distinguish between actual and false images. Confusion matrix analysis highlights the classification performance of the model, showing real positive (2757), real negative (2694), false positive (2735), and false negative (2719). This model ensures fair classification by maintaining the same data record distribution and improves reliability of digital forensics, media authentication and security applications. This approach is important for identifying manipulated content in journalism, forensic testing, and social media reviews. This ensures misinformation and image integrity. Future advances in improving properties and optimizing deep learning can improve system accuracy and reduce malfunctions.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

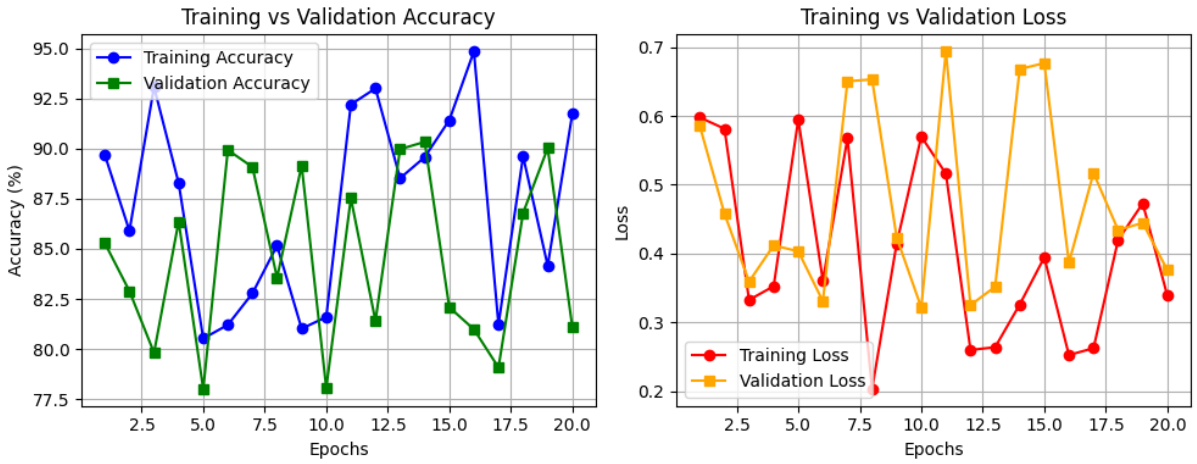

Figure 5: Model loss and accuracy graph

Enhanced deep learning-based characteristic analysis for detection of counterfeits that drive copies automatically identifies the operating area of digital images using deep folding networks integrated into advanced functional learning techniques. By extracting hierarchical and semantically rich properties, this model robustly distinguishes between real image components and dual regions that exhibit fakeness. Through the iterative training process indicated by epoch in the training phase, the network is fine to capture both local textures and global spatial relationships. This improved approach significantly surpasses traditional handcrafted functional methods by providing improved adaptability and resilience to highly developed operational strategies, and thus provides a reliable and scalable solution for digital image forensics.

CONCLUSION

In summary, it can be said that an extended, deep learning-based characteristic analysis for the detection of counterfeits for copy counterfeiting shows significant potential for accurate identification of images manipulated using an extended, CNN-based technique. The balanced results of the dataset and the confusion matrix show strong recognition, but there is space to improve the minimization of false positive and false negative ,negative negatives. This approach is extremely important for digital forensics, media authentication and security applications, contributing to prevent misinformation and maintaining image integrity. Future advances in deep learning architecture, distinctive extraction techniques, and dataset diversity can further improve detection accuracy and robustness, making this method a valuable instrument for combating digital image forgery.

REFERENCES

[1] Thanh Thi Nguyen, Cuong M., Dung Tien Nguyen, Duc Thanh Nguyen, Saeid Nahavandi, “Deep Learning for Deepfakes Creation and Detection: A Survey”, 2020, Volume 223, PP. 1-12, https://doi.org/10.1016/j.eviu.2022.103525.

[2] Hrisha Y., Akshit K., Prakruti J., “A Brief Study on Deepfakes”,*2020 International Research Journal of Engineering and Technology (IRJET)*, 2395-0056, Volume 7, PP. 382-386.

[3] Siwei L, “Deepfake Detection: Current Challenges and Next Steps”, *2020 IEEE International Conference on Multimedia & Expo Workshops (ICMEW) C22*,PP. 1-6, doi:10.1109/ICMEW46912.2020.9105991.

[4] Francesco Marra, Diego Gragnaniello, Davide Cozzolino, Luisa Verdoliva, “Detection of GAN-generated Fake Images over Social Networks”,*2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*, PP. 384-389,doi:10.1109/MIPR.2081.00084.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Research Article

[5] Teng Zhang, Lirui Deng, Liang Zhang, Xianglei Dang, "Deep Learning in Face Synthesis: A Survey on Deepfakes", *2020 IEEE 3rd International Conference on Computer and Communication Engineering Technology (CCET)*, PP. 67-70, doi: 10.1109/CCET50901.2020.9213159.

[6] Deng Pan, Lixian Sun, Rui Wang, Xingjian Zhang, Richard O. Sinnott, "Deepfake Detection through Deep Learning", *2020 IEEE/ACM International Conference on Big Data Computing, Applications and Technologies (BDCAT)*, PP. 134-143, doi: 10.1109/BDCAT50828.2020.00001.

[7] Chih-Chung Hsu, Yi-Xiu Zhuang and Chia-Yen Lee, "Deep Fake Image Detection Based on Pairwise Learning", *2020 Applied Science*, PP. 1-14, https://doi.org/10.3390/app10010370.

[8] Nikita S. Ivanov, Anton V. Arzhskov, Vitaliy G. Ivanenko, "Combining Deep Learning and Super-Resolution Algorithms for Deep Fake Detection", *2020 IEEE Conference of Russia Young Researchers in Electrical and Electronic Engineering (ElConRus)*, PP. 326-328, doi: 10.1109/ElConRus49466.2020.9039498.

[9] Badhrinarayan Malolan, Ankit Parekh, Faruk Kazi, "Explainable Deep-Fake Detection Using Visual Interpretability Methods", *2020 3rd International Conference on Information and Computer Technologies (ICICT)*, PP. 289-293, doi: 10.1109/ICICT50521.2020.00051.

[10] Daniel Mas Montserrat, Hanxiang Hao, S. K. Yarlagadda, Sriram Baireddy, Ruiting Shao Janos Horvath, Emily Bartusiak, Justin Yang, David G ´ Uera, Fengqing Zhu, Edward J. Delp, "Deepfakes Detection with Automatic Face Weighting", *2020 Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, PP. 1-9, arXiv:2004.12027v2.

[11] Md. Shohel Rana, Andrew H. Sung, "DeepfakeStack: A Deep Ensemble-based Learning Technique for Deepfake Detection", *2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, PP. 70-75, doi: 10.1109/CSCloud-EdgeCom49738.2020.00021.

[12] Luca Guarnera, Oliver Giudice, and Sebastiano Battiato, "Fighting Deepfake by Exposing the Convolutional Traces on Images", 2020, PP. 1-13, arXiv: 2008.04095v1.

[13] Ali Khodabakhsh, Christoph Busch, "A Generalizable Deepfake Detector based on Neural Conditional Distribution Modelling", *2020 International Conference of the Biometrics Special Interest Group (BIOSIG)*, PP. 1-5, IEEE Xplore.

[14] Kui Zhu, Bin Wu, "Deepfake Detection with Clustering-based Embedding Regularization", *2020 IEEE 5th International Conference on Data Science in Cyberspace (DSC)*, PP. 257-264, doi:10.1109/DSC50466.2020.00046.

[15] Dafeng Gong, Yogan Jaya Kumar, Ong Sing Goh, Zi Ye, Wanle Chi, "DeepfakeNet, an Efficient Deepfake Detection Method", *2021 International Journal of Advanced Computer Science and Applications (IJACSA)*, Volume 12, PP. 201-207, http://dx.doi.org/10.14569/IJACSA.2021.0120622.

[16] Yang Wang, "A Mathematical Introduction to generate adversarial NETS (GAN)", 2020, PP. 1-30, https://doi.org/10.48550/arXiv.2009.00169.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.