IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.134191

Review on Different Image Forgery Detection Techniques & Methods

Aryan Humnabadkar[1], Bhargav Shivbhakta[2], Prof. Dr. Mrs. A. J. Vyavahare[3]

Dept. of Electronics And Computer Engineering, PES Modern College Of Engineering, Pune, India[1,2]

HOD, Dept. of Electronics And Computer Engineering, PES Modern College Of Engineering, Pune, India[3]

Abstract: The pervasive emergence of deepfake technology presents unprecedented challenges to the authenticity of digital imagery, prompting the need for advanced methods in detection and mitigation. This review synthesizes insights from multiple pivotal papers, spanning diverse approaches to image forgery detection. It begins with an exploration of the intricacies and societal ramifications of deepfake technology. Navigating through methodologies like CNN-based passive tamper detection, block-based copy-move forgery detection, and ensemble approaches using advanced neural network architectures such as Inception Resnet V2, the review scrutinizes each method's distinctive strengths and limitations, providing a nuanced understanding of their efficacy against digital image manipulations. A comparative analysis reveals the variances and trade-offs inherent in these detection methodologies, offering a valuable resource for researchers and practitioners in image forensics. The abstract concludes by outlining persisting challenges in image forgery detection and suggesting prospective avenues for future research. By distilling a comprehensive overview of contemporary image forensics, this review equips stakeholders with essential insights to navigate the evolving landscape of digital image authenticity and fortify defenses against the escalating threat of deepfake manipulations.

Keywords: deepfake, image forensics, CNN, forgery detection, challenges in image forensics.

I. INTRODUCTION

The emergence of advanced technologies in the digital transformation age has not only enabled the smooth access, processing, and sharing of information, but has also introduced substantial security issues. With the introduction of sophisticated image modification programs like Photoshop and Corel Draw, the distinctions between real and modified pictures have blurred, giving birth to the difficult challenge of image forgery [4].

Deepfake technology, which uses artificial intelligence, primarily machine learning, to modify pictures and videos with unparalleled realism, is one particularly troubling aspect of this dilemma [7]. Deepfakes, a combination of "deep learning" and "fake," have emerged as a powerful method of creating synthetic information that is visually indistinguishable from actual graphics [7]. Deepfake methods are rapidly evolving, posing serious dangers, particularly in social media situations where compressed and resized films undergo modifications that might disguise manipulations [6].

Deepfakes pose a threat to science, the media, forensics, and societal stability, among other fields. Examples of photoshopped photographs used for political purposes highlight the need for developing robust techniques for detecting image forgeries [4] [1]. The difficulties are exacerbated by the ease with which digital photos may be modified, which can misrepresent important information and have an impact on judgments made using these pictures [2].

Deepfakes are created using complex algorithms and technologies such as convolutional neural networks (CNN) and other deep learning techniques [5]. Common picture fraud techniques include copy-move, seam carving, re-compress, and retouching; each poses unique difficulties for forensic identification [6]. Conventional picture modification detection methods rely on hand-crafted features, but recent advances in deep learning, particularly with CNNs, have shown promising results [5].

To address the challenges posed by deepfake and traditional forgery techniques, the field of image forgery detection has developed a plethora of methodologies. Passive forensics, for example, analyzes raw image data based on various statistical and semantic features [2]. Furthermore, to prevent tampering, active approaches employ preprocessing techniques such as watermarking and signature embedding [1]. The variety of these techniques reflects the complexities of the image forgery landscape, which necessitates continuous innovation to keep up with malicious advancements.

This review paper aims to provide a comprehensive understanding of image forgery detection techniques, with a focus on countering the challenges posed by deepfake technology, as we navigate through this landscape of evolving threats and technologies. We delve into the active and passive approaches used in image forensics, investigate the complexities of various forgery types, and discuss advancements in deep learning-based detection methods using insights from a review of relevant literature. We hope that by conducting this investigation, we can contribute to the ongoing efforts to improve the reliability and security of digital images in an era dominated by sophisticated image manipulation tools.

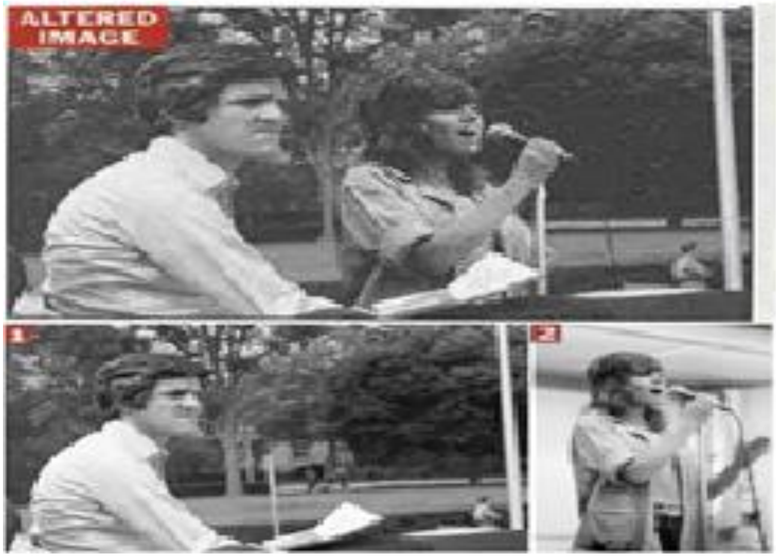

Figure 1: Jan Fonda (right) speaks to a crowd of Vietnam veterans with John Kerry (left) next to her [15]

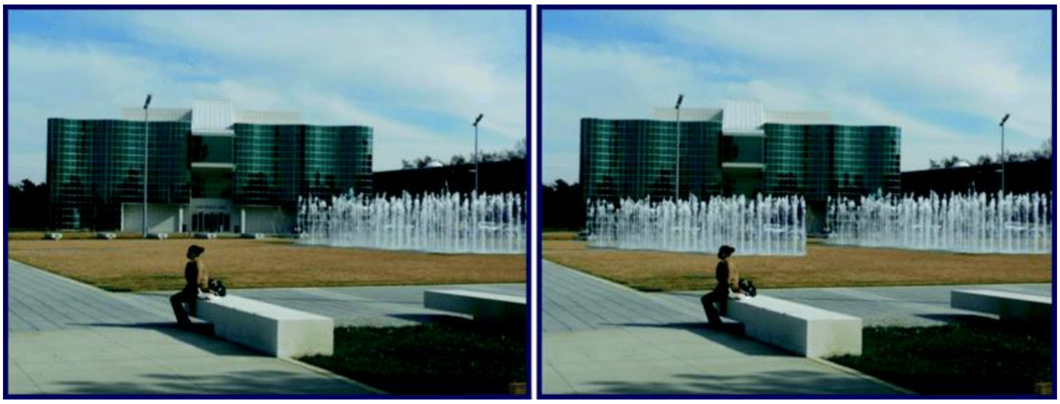

Figure 2 :Authentic image (Left); Forged image (Right) [16]

II. LITRATURE REVIEW

Image forgery has become a widespread problem in the digital age, prompting the development of numerous methods and techniques for detecting it. This review divides these techniques into two categories: active and passive approaches, each with its own subtype. Methods such as digital watermarking and digital signatures, which embed additional information into the image to verify authenticity, fall under the active approach. The passive approach, on the other hand, is further subdivided into forgery-dependent and forgery-independent methods.

Forgery-independent approaches concentrate on intrinsic picture features, with image retouching and lighting inconsistency detection being important subcategories. Image retouching detection techniques use factors such as color variations and structural irregularities to identify changes made to the content. The detection of lighting inconsistency focuses on differences in lighting conditions within a picture, finding disparities that may suggest manipulation. These techniques give useful insights into the subtle modifications that are frequently used in picture fraud.

DOI: 10.17148/IJARCCE.2024.134191

Two prominent examples of methods that rely on outside information and are forgery-dependent are image splicing and copy-move forgery. Image splicing is the process of combining material from many sources, which makes it difficult to keep the visual look consistent.

Copy-move forgery involves copying and positioning specified parts inside the same image, which is frequently used to conceal or emphasize specific aspects. The reliance on external information in forgery-dependent algorithms emphasizes the need of taking context and reference data into account throughout the detection process.

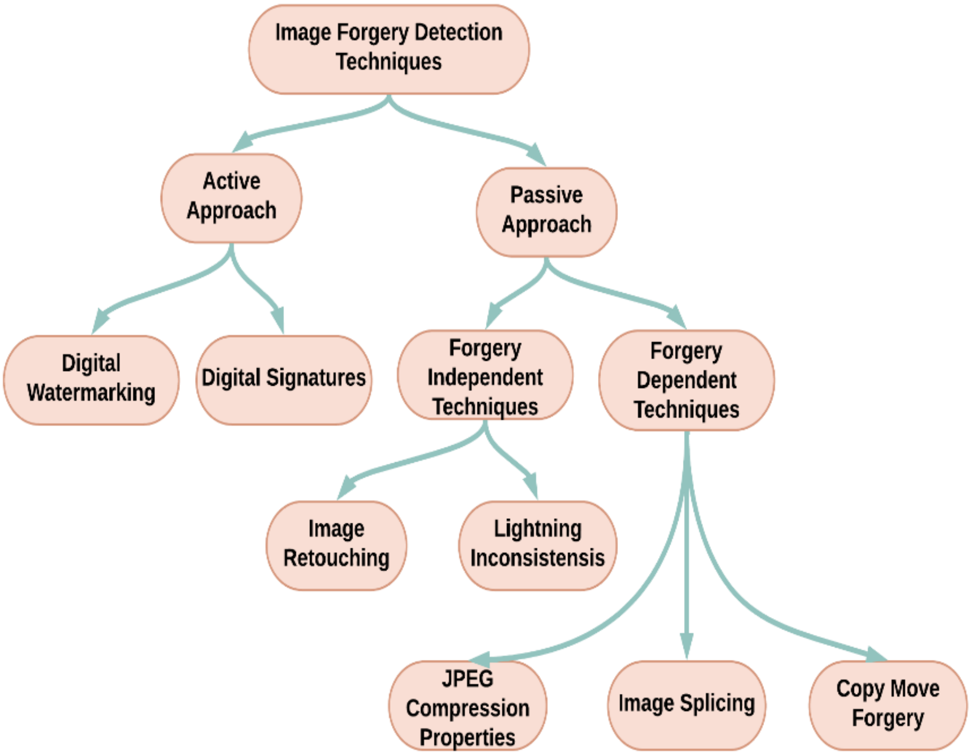

Figure 3 : Categorization of Image Forgery Detection

Deep learning algorithms for deepfake development and detection study investigates not just the technological aspects of deepfake production, but also the ethical implications and potential societal consequences [1]. To detect deepfakes, many methods such as picture preprocessing, bag of words, and deep recurrent network models are used, underscoring the multifaceted nature of solving the issues given by this type of visual fraud.

The authors also highlight the limitations of current detection approaches and propose future research areas, advocating for a more resilient and adaptive strategy to keep up with advancing deepfake techniques. The ethical implications are expanded upon, providing emphasis on the need of responsible AI activities and policymakers' roles in preventing the potential exploitation of deepfake technology.

The passive picture tamper detection using deep learning offers a CNN-based approach for detecting digital image forgeries, utilizing datasets such as MICC, CASIA, and UCID for validation [2]. The research gives a comprehensive knowledge of the difficulties in identifying passive picture tampering, highlighting the need for robust models capable of distinguishing subtle changes. The discussion of future work and problems deepens our grasp of the changing landscape of picture forensics. Furthermore, the authors analyze the computational efficiency of their suggested CNN-based strategy, as well as the trade-offs between accuracy and processing speed. They emphasize the significance of meeting real-time detection needs in a variety of applications, ranging from social networking platforms to forensic investigations. The incorporation of transfer learning techniques is suggested as a potential avenue for enhancing model generalization across diverse datasets.

DOI: 10.17148/IJARCCE.2024.134191

One well-known approach to copy-move forgery detection is to use block-based or key point-based processes in conjunction with preprocessing techniques such as color channel conversion and block division [3].The study not only shows the approaches, but it also discusses the basic ideas of feature extraction and matching. This in-depth examination adds to a better understanding of the advantages and disadvantages of various block-based techniques.

Furthermore, to explore how block-based approaches can be applied to various sorts of copy-move forgeries, such as those involving rotation and scaling. The importance of employing robust feature extraction algorithms is underlined, particularly in circumstances where the copied regions undergo slight changes. For increased forgery detection accuracy, the article argues for a holistic strategy that blends block-based approaches with machine learning strategies.

The negative impact of downsizing on high-frequency features is one of the main shortcomings of current deep learning algorithms for identifying image forgeries [4]. Due to computational constraints, many modern models must be resized, which causes the loss of important data. The suggested framework offers a CNN-based technique that does not require scaling and operates directly on full-resolution photos. The system achieves end-to-end trainability with low memory requirements and little supervision by utilizing gradient checkpointing. The framework combines elements for extraction, aggregation, and classification, which makes it easier to optimize parameters all at once. Experimental results demonstrate the framework's superior performance, surpassing baselines and reference methods in various image forensics datasets. The incorporation of memory-efficient implementations during both forward and backward passes enhances the model's ability to discern discriminant information for accurate whole-image classification.

The proposed end-to-end-trainable structure places special emphasis on the steps involved in extraction, aggregation, and classification. The model examines the entire high-resolution image in the forward pass, and all of the framework's components are simultaneously optimized in the backward pass. To improve accurate whole-image classification, training involves learning to extract and aggregate the most discriminative data. The authors present a detailed formulation for gradient calculation during backpropagation, emphasizing the selective contribution of 'active' patches based on the pooling method employed. The versatility of the proposed approach lies in its ability to outperform existing methods while operating on full-resolution images, preserving high-frequency details crucial for effective image forgery detection. In an image block-matching approach for copy-move fraud detection based on improved singular value decomposition assess the method on a patch dataset and describe the benefits of applying singular value decomposition for feature extraction and dimension reduction [5]. The full discussion of the method's components and their ramifications brings clarity to the proposed approach's understanding.

Furthermore, comparison of the suggested method to traditional block-matching techniques, demonstrates the advantages in accuracy and computing efficiency. The report advocates for more research into sophisticated dimensionality reduction techniques in order to improve the method's scalability and applicability to large-scale image datasets.

The boundary-based image forgery detection system based on a fast shallow CNN, Patch extraction, SCNN architecture modification, and the introduction of Fast SCNN for efficient sliding window detection are all part of the method [6]. The paper discusses the processing time and redundancy limits of deep neural networks.

The authors contribute to the continuing discussion about enhancing the efficiency of forgery detection algorithms by suggesting Fast SCNN as a solution to these difficulties. Furthermore, the authors discuss the practical aspects of implementing their suggested fast shallow CNN in resource-constrained contexts. The trade-offs between detecting accuracy and processing economy are examined, as are potential real-time applications. The paper emphasizes the need for tailored solutions to address specific challenges in image forgery detection, paving the way for future research in the domain of fast and efficient algorithms for real-world scenarios.

Detecting manipulated regions in JPEG images using CNN is a method for extracting DCT coefficients, generating a binary image, and classifying it using a CNN [7]. The research outlines changes to the CNN structure and investigates the effect of filter size on detection accuracy. The study improves the reader's knowledge of the suggested method's mechanics by providing insights into the considerations behind structural changes and their effects.

Furthermore, the authors analyze the CNN-based method's generalization capabilities across different forms of tampering, emphasizing the significance of strong feature extraction techniques. The investigation of ideal filter sizes for various tampering scenarios is expanded, with an emphasis on attaining a balance between sensitivity and specificity [16]. The paper advocates for continuous refinement and adaptation of CNN architectures to address emerging challenges in image forgery detection, underscoring the dynamic nature of the field.

DOI: 10.17148/IJARCCE.2024.134191

Presenting a novel method of detecting image counterfeiting [8] by using a Convolutional Neural Network (CNN) with a nine-layer architecture that includes fully connected layers for logical inference, convolutional layers for feature extraction, and a Softmax classifier for image classification. The RGB images with dimensions of 227x227x3 can be accommodated by the input layer. To add non-linearity, the convolutional layers use the ReLU activation function. Feature fusion is accomplished using max-pooling, and the fully-connected layers are in charge of logical inference, with dropout to prevent overfitting. Based on conditional probabilities, the Softmax classifier in the output layer classifies images as authentic or forged.

Using paired learning with a DenseNet-based two-streamed network, a multimedia forgery detection system [9] combines deep learning techniques, such as Convolutional Neural Networks (CNNs) with contrastive loss. This approach, which is based on contrastive loss, outperforms existing image detectors in terms of distinguishing real images from fakes. The results show that scenarios with a little dataset and significant changes to the original image perform particularly well. Various phases are involved in the proposed methodology, including transforming RGB-colored images to YCrCb, using discrete cosine transform (DCT), quantization based on JPEG quantized tables, and Huffman encoding. The CNN model, featuring a 64-layer filter of size 3x3 with ReLU activation and max pooling, addresses challenges faced by previous methods in detecting forgeries within compressed areas.

A deep learning-based multimedia forgery detection algorithm uses an ensemble technique that makes use of Inception Resnet V2 [10], a fusion of Inception and residual networks that has been trained on datasets such as the Kaggle Deepfake detection challenge and Fake Face Detection. When trained on a dataset predominantly comprised of deepfakes, the model achieves an amazing accuracy of 92%. Notably, the proposed methodology foregoes costly preprocessing such as Error Level Analysis (ELA), instead relying on reshaping images to the desired format. Inception Resnet V2's residual nature reduces feature loss during training, resulting in enhanced accuracy.

Furthermore, the consequences of deploying an ensemble of networks, focusing on the synergy and complementarity of various topologies in increasing overall detection performance are observed. The study emphasizes the suggested model's flexibility to varied datasets, implying its potential in real-world applications with evolving modification techniques. The trade-offs between model complexity and interpretability are investigated, adding to the continuing discussion about developing efficient and effective multimedia forgery detection models for practical deployment.

In summary, the papers evaluated show the wide range of methodologies used in detecting image forgeries, including deep learning, block-based methods, and CNN-based approaches. The comparison of various methodologies reveals useful information about their advantages, disadvantages, and prospective applications in real-world circumstances.

SR. NO.	PAPER TITLE	METHOD USED	TAMPERING DETECTION TYPE	PROS	CONS
1	B. F. Nasar, S. T and E. R. Lason, "Deepfake Detection in Media Files - Audios, Images and Videos," 2020 IEEE Recent Advances in Intelligent Computational Systems (RAICS)	Deep learning techniques, image preprocessing, bag of words, deep recurrent network models	Deepfake creation and detection	Comprehensive exploration of technical and ethical aspects, multi-faceted approach	Lack of specific focus on a single detection method
2	Nguyen, Thanh & Nguyen, Cuong M. & Nguyen, Tien & Nguyen, Duc & Nahavandi, Saeid & Pham, Viet & Huynh-The, Thien. (2019). Deep Learning for Deepfakes Creation and Detection: A Survey.	CNN-based approach	Passive image tamper detection	Robust model, validation using MICC, CASIA, and UCID datasets	Lack of detailed exploration on ethical implications
3	S. Manjunatha. and M. M. Patil, "Deep learning-based Technique for Image Tamper Detection," 2021 Third International Conference on Intelligent Communication	Block or key point-based approaches, color channel conversion, block division	Copy-move forgery detection	In-depth analysis of methodologies, principles of feature extraction	Limited exploration of deep learning techniques

DOI: 10.17148/IJARCCE.2024.134191

SR. NO.	PAPER TITLE	METHOD USED	TAMPERING DETECTION TYPE	PROS	CONS
	Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 1278-1285				
4	F. Marra, D. Gragnaniello, L. Verdoliva and G. Poggi, "A Full-Image Full-Resolution End-to-End-Trainable CNN Framework for Image Forgery Detection," in IEEE Access, vol. 8, pp. 133488-133502, 2020.	CNN-based framework with end-to-end training, gradient checkpointing	Spliced Image Tampering Detection	Utilizes full resolution information for whole-image analysis, Trainable end-to-end with limited memory resources.	Requires weak (image-level) supervision. No mention of real-time processing capabilities.
5	L. Kang and X. -p. Cheng, "Copy-move forgery detection in digital image," 2010 3rd International Congress on Image and Signal Processing, Yantai, China, 2010, pp. 2419-2421	Image block-matching method based on improved singular value decomposition	Copy-move forgery detection	Evaluation using a patch dataset, advantages of singular value decomposition	Limited discussion on real-world application
6	Z. Zhang, Y. Zhang, Z. Zhou and J. Luo, "Boundary-based Image Forgery Detection by Fast Shallow CNN," 2018 24th International Conference on Pattern Recognition (ICPR), Beijing, China, 2018, pp. 2658-2663	Fast shallow CNN, patch extraction, SCNN architecture modification, Fast SCNN	Boundary-based image forgery detection	Proposes a solution to challenges in processing time and redundancy	Limited exploration of deep learning methods
7	K. Taya, N. Kuroki, N. Takeda, T. Hirose and M. Numa, "Detecting tampered regions in JPEG images via CNN," 2020 18th IEEE International New Circuits and Systems Conference (NEWCAS), Montreal, QC, Canada, 2020, pp. 202-205	CNN-based method, extraction of DCT coefficients, binary image creation	Detecting tampered regions in JPEG images	Highlights modifications in CNN structure, explores impact of filter size	Lack of discussion on real-world deployment
8	N. Huang, J. He and N. Zhu, "A Novel Method for Detecting Image Forgery Based on Convolutional Neural Network," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 2018, pp. 1702-1705	Convolutional Neural Network (CNN), nine-layer architecture, RGB images of size 227x227x3	Image forgery detection	Emphasis on training neural networks with appropriate optimizers	Limited discussion on the computational cost of the proposed method
9	Benhamza, H., Djeffal, A., Cheddad, A. (2021),Image forgery detection review In:	CNNs, contrastive loss, pairwise learning approach,	Multimedia forgery detection	Effective in distinguishing imposter images,	Limited discussion on

SR. NO.	PAPER TITLE	METHOD USED	TAMPERING DETECTION TYPE	PROS	CONS
	Proceedings - 2021 International Conference on Information Systems and Advanced Technologies, ICISAT 2021 Institute of Electrical and Electronics Engineers Inc.	Dense Net architecture		successful with small datasets	real-world applicability
10	Y. Shah, P. Shah, M. Patel, C. Khamkar and P. Kanani, "Deep Learning model-based Multimedia forgery detection," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2020, pp. 564-572	Inception Resnet V2, ensemble approach, trained on Kaggle Deepfake detection challenge and Fake face Detection	Multimedia forgery detection	Impressive accuracy of 92%, eliminates extensive preprocessing	Not suitable for all forgery types, limited discussion on ethical considerations

Figure 3 : Comparison Chart on Various Deepfake Image Forgery Detection Papers

III. CHALLENGES

Several pressing difficulties demand attention in the dynamic terrain of multimedia forgery detection in order to move the discipline forward. For starters, the constant advancement of deepfake technology is a constant challenge for researchers in building detection algorithms. As content providers adapt and perfect their strategies, there is an urgent need for detection tools that can effectively detect and fight growing dangers. Understanding the complexities of growing deepfake generating algorithms requires a proactive and flexible strategy.

Another critical difficulty is ensuring that forgery detection methods are generalizable across varied datasets. Because many existing models are trained and assessed on specialized datasets, it is critical to improve their applicability to a wider range of scenarios. To achieve robust generalization, changes in image quality, resolution, and processing techniques must be addressed. The creation of universally applicable models capable of detecting forgeries across varied multimedia datasets is an important route for future research.

In the realm of real-world applications, the deployment of forgery detection systems in real-time scenarios, such as social media platforms or video streaming services, demands a delicate balance between efficiency and accuracy. Researchers need to focus on the development of algorithms that can process multimedia content swiftly without compromising the precision of forgery detection. Striking this balance is essential for the seamless integration of forgery detection mechanisms into applications where timely identification of manipulated content is paramount. Addressing these challenges collectively will contribute to the advancement of multimedia forgery detection and its effective application in real-world contexts.

IV. CONCLUSION & FUTURE SCOPE

Finally, the examined literature gives a thorough overview of the many methodologies used in multimedia forgery detection, spanning from traditional approaches to advanced deep learning approaches. Each method has advantages and disadvantages, emphasizing the importance of a comprehensive understanding of their applicability in various settings. The comparison analysis gives light on the developing environment of picture forensics, with advances in deep learning demonstrating promising results in detecting complex forgeries such as deepfakes.

The future field of study in multimedia forgery detection is broad and diverse. For starters, there is an urgent need for more robust and adaptive deepfake detection methods. As approaches for creating deepfakes advance, researchers must concentrate on enhancing the robustness of detection algorithms in order to stay ahead of more dangerous situations. Efforts should also be made to improve the generalization of forgery detection models across varied datasets, assuring their usefulness in real-world scenarios with varying image qualities and alteration approaches.

DOI: 10.17148/IJARCCE.2024.134191

Furthermore, deploying forgery detection systems in actual applications such as social media platforms needs a precise balance between efficiency and accuracy. Future study should look toward optimizing algorithms for real-time processing while maintaining precision. Furthermore, future research should take into account the ethical implications of forgery detection and build frameworks for responsible use. Interdisciplinary cooperation involving computer vision scientists, ethicists, and legal scholars will be critical in building a complete and ethically sound future for multimedia forgery detection as the area evolves.

REFERENCES

[1]. B. F. Nasar, S. T and E. R. Lason, "Deepfake Detection in Media Files - Audios, Images and Videos," 2020 IEEE Recent Advances in Intelligent Computational Systems (RAICS), Thiruvananthapuram, India, 2020, pp. 74-79, doi: 10.1109/RAICS51191.2020.9332516.

[2]. Nguyen, Thanh & Nguyen, Cuong M. & Nguyen, Tien & Nguyen, Duc & Nahavandi, Saeid & Pham, Viet & Huynh-The, Thien. (2019). Deep Learning for Deepfakes Creation and Detection: A Survey.

[3]. S. Manjunatha. and M. M. Patil, "Deep learning-based Technique for Image Tamper Detection," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 1278-1285, doi: 10.1109/ICICV50876.2021.9388471.

[4]. F. Marra, D. Gragnaniello, L. Verdoliva and G. Poggi, "A Full-Image Full-Resolution End-to-End-Trainable CNN Framework for Image Forgery Detection," in IEEE Access, vol. 8, pp. 133488-133502, 2020, doi: 10.1109/ACCESS.2020.3009877.

[5]. L. Kang and X. -p. Cheng, "Copy-move forgery detection in digital image," 2010 3rd International Congress on Image and Signal Processing, Yantai, China, 2010, pp. 2419-2421, doi: 10.1109/CISP.2010.5648249.

[6]. Z. Zhang, Y. Zhang, Z. Zhou and J. Luo, "Boundary-based Image Forgery Detection by Fast Shallow CNN," 2018 24th International Conference on Pattern Recognition (ICPR), Beijing, China, 2018, pp. 2658-2663, doi: 10.1109/ICPR.2018.8545074.

[7]. K. Taya, N. Kuroki, N. Takeda, T. Hirose and M. Numa, "Detecting tampered regions in JPEG images via CNN," 2020 18th IEEE International New Circuits and Systems Conference (NEWCAS), Montreal, QC, Canada, 2020, pp. 202-205, doi: 10.1109/NEWCAS49341.2020.9159761.

[8]. N. Huang, J. He and N. Zhu, "A Novel Method for Detecting Image Forgery Based on Convolutional Neural Network," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 2018, pp. 1702-1705, doi: 10.1109/TrustCom/BigDataSE.2018.00255.

[9]. Benhamza, H., Djeffal, A., Cheddad, A. (2021),Image forgery detection review In: Proceedings - 2021 International Conference on Information Systems and Advanced Technologies, ICISAT 2021 Institute of Electrical and Electronics Engineers Inc., https://doi.org/10.1109/ICISAT54145.2021.9678207

[10]. Y. Shah, P. Shah, M. Patel, C. Khamkar and P. Kanani, "Deep Learning model-based Multimedia forgery detection," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2020, pp. 564-572, doi: 10.1109/I-SMAC49090.2020.9243530.

[11]. Vyavahare, A.J. & Thool, R.C.. (2012). Segmentation using region growing algorithm based on CLAHE for medical images. IET Conference Publications. 2012. 182-185. 10.1049/cp.2012.2522.

[12]. Bismi Fathima Nasar, Sajini. T, Elizabeth Rose Lalson, ”A Survey on Deepfake Detection Techniques”, International Journal of Computer Engineering in Research Trends, pp:49-55 ,August-2020.

[13]. M. Ali Qureshi and M. Deriche, "A review on copy move image forgery detection techniques," 2014 IEEE 11th International Multi-Conference on Systems, Signals & Devices (SSD14), Barcelona, 2014, pp. 1-5, doi: 10.1109/SSD.2014.6808907.

[14]. Gill, Navpreet & Garg, Ruhi & Doegar, Amit. (2017). A review paper on digital image forgery detection techniques. 1-7. 10.1109/ICCCNT.2017.8203904.

[15]. Gade, Akshada A., and Arati J. Vyavahare. "Feature extraction using glcm for dietary assessment application." International Journal Multimedia and Image Processing (IJMIP) 8.2 (2018): 409-413.

[16]. K. L. Fonda,Kerry,and P. Fakery.,"The washington post," p. A21,Feb.2004.

[17]. Mohammed, Manaf & Taherinia, Amir. (2022). A passive image forensic scheme based on an adaptive and hybrid techniques. Multimedia Tools and Applications. 81. 1-19. 10.1007/s11042-022-12374-5.

[18]. P. Zhou, X. Han, V. I. Morariu and L. S. Davis, "Two-Stream Neural Networks for Tampered Face Detection," 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Honolulu, HI, USA, 2017, pp. 1831-1839, doi: 10.1109/CVPRW.2017.229.