ICSSR Sponsored - International Conference on Need of Digital Transition and CSR For Innovative Sustenance in the 2023 Economy
© 2023 IJSRST | Volume 10 | Issue 11 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
International Journal of Scientific Research in Science and Technology

Image Forgery Detection Using Deep Learning Techniques - A Review

Maneesa Nasreen T[1], Leena C Sekhar[2], Ibrahim Salim M[3]
[1]Student, [2]Associate Professor, [3]Assistant Professor
Department of Computer Applications, MES College, Marampally, Kerala, India

ABSTRACT

Image forgery detection refers to the process of identifying any manipulation or alteration on a digital image with the intention of misrepresenting reality. In recent years, deep learning methods have emerged as an effective approach for this task due to from images. In this paper , we present an overview of the current state-of-the-art techniques for image forgery detection using deep learning techniques. With the increasing use of digital images, the problem of image forgery has become more prevalent, and traditional techniques are not always effective in detecting these forgeries. A detailed description of the key steps involved in building a deep learning-based image forgery detection model, including data collection and pre-processing, model design and training, and evaluation are explained here. The paper also highlights some of the key considerations and challenges in this field, such as selecting appropriate architectures, loss functions, and optimization techniques. The significant potential of deep learning techniques for addressing the problem of image forgery, and highlights the importance of continued research in this field to develop more effective and robust detection methods are also presented in this paper.

Keywords—Image forgery, Deep learning, Copy-move forgery, Image slicing, image retouching, CNN, SIFT, SURF, Support Vector Machine(SVM)

I. INTRODUCTION

Images are powerful communication devices. Digital images has become highly pervasive in our day-to-day lives.Image has remarkable role in various areas such as forensic investigation, criminal investigation, surveillance systems etc.But due to the availability of sophisticated tools and softwares for image manipulation, it is very easy to tamper the image by anyone.With the advancement of image editing techniques, authenticity and reliability of digital image has become very challenging.Image forgery detection refers to the process of identifying any manipulation or alteration on a digital image with the intention of misrepresenting reality.

Image forgery detection has become an increasingly important area of research in recent years, as the widespread availability of powerful image editing tools has made it easier than ever to create convincing forgeries. Image forgery can take many forms, such as copy-move, splicing, and retouching, and can have serious implications in fields such as journalism, law enforcement, and digital forensics.

Traditional methods for image forgery detection, such as statistical analysis and pattern recognition, have limitations in terms of accuracy and robustness. In recent years, deep learning techniques have emerged as a promising approach to image forgery detection, as they can automatically learn features from the image data and have shown impressive performance in various image-related tasks.

This review paper aims to provide a comprehensive survey of recent research on image forgery detection using deep learning techniques. We will first discuss the various types of image forgeries and the challenges associated with detecting them. We will then review the traditional methods for image forgery detection and their limitations.Through this survey, we hope to provide a better understanding of the current state-of-the-art in image forgery detection using deep learning, as well as the challenges and opportunities for future research in this field.

II. CLASSIFICATION OF IMAGE FORGERY

Image manipulation detection approaches can be broadly categorized as active and passive techniques. In the active approach, additional information is added to the image during the acquisition or later stage by authorized personnel, such as a digital watermark,digital signature. This embedded information is then used for detecting any potential manipulation or forgery in the image. On the other hand, passive approaches are also known as "blind approaches" because they do not rely on any additional information for forgery detection. Instead, these approaches extract features from the image and use these features to identify any signs of manipulation or forgery. In other words, passive approaches do not require any prior knowledge or information about the image to detect any potential tampering.

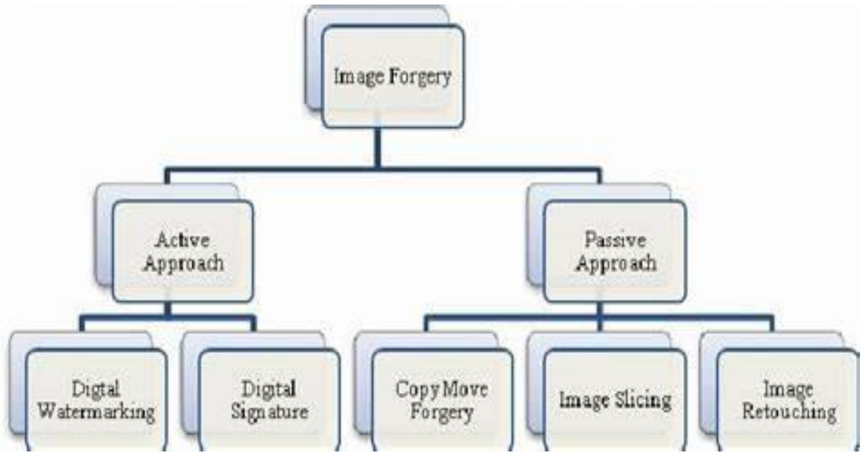

Fig.1: different type of image forgery detection classification.

A. DIGITAL WATERMARKING AND DIGITAL SIGNATURE

Digital Watermarking is a technique that involves adding an invisible or semi-visible mark to an image to detect if the image has been tampered with or copied.Digital signatures involve adding a digital signature to an image, which can be verified to ensure the authenticity of the image.

B. COPY-MOVE FORGERY DETECTION

Copy-move forgery detection is a type of image forgery detection technique that focuses on identifying tampering in images where a portion of the image has been copied and pasted onto another part of the same image. This technique is commonly used in forensic investigations where it is suspected that an image has been altered to misrepresent or hide certain information.

Copy-move forgery detection techniques typically involve dividing the image into small overlapping blocks and then comparing these blocks to identify any areas that have been copied and pasted. These techniques can use various features such as color, texture, and shape to identify similarities between different parts of the image. Once the copied and pasted areas are identified, the forgeries can be located and analyzed further to determine the extent of the tampering and the techniques used to create the forgery.

Copy-move forgery detection can be a challenging task as the forgeries can be created with various degrees of complexity, such as scaling, rotation, and flipping. However, various techniques have been developed to address these challenges, such as feature extraction, matching, clustering, and post-processing.

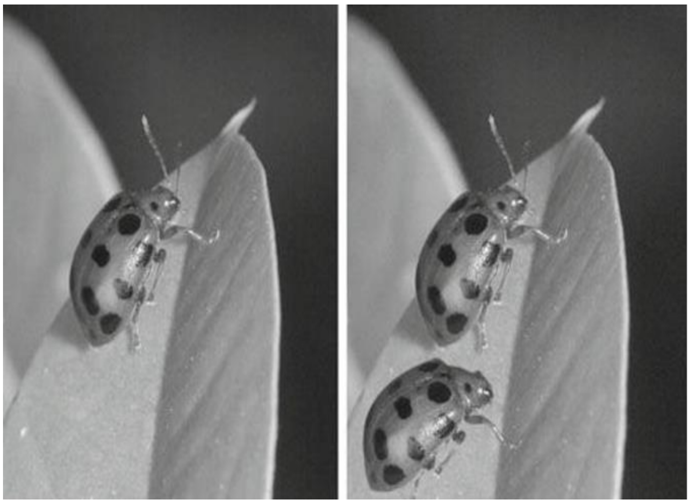

Fig.2:example for copy-move image forgery

C. IMAGE SLICING

Image slicing can also be used in image forgery detection to identify copy-move forgeries. In this case, the large image is divided into smaller overlapping blocks or tiles, and these tiles are compared to identify any regions that have been copied and pasted within the same image. By analyzing the features of these tiles, such as color, texture, and shape, it is possible to identify similarities between different parts of the image and locate the areas that have been tampered with. Once the forgeries are identified, further analysis can be conducted to determine the extent of the tampering and the techniques used to create the forgery.

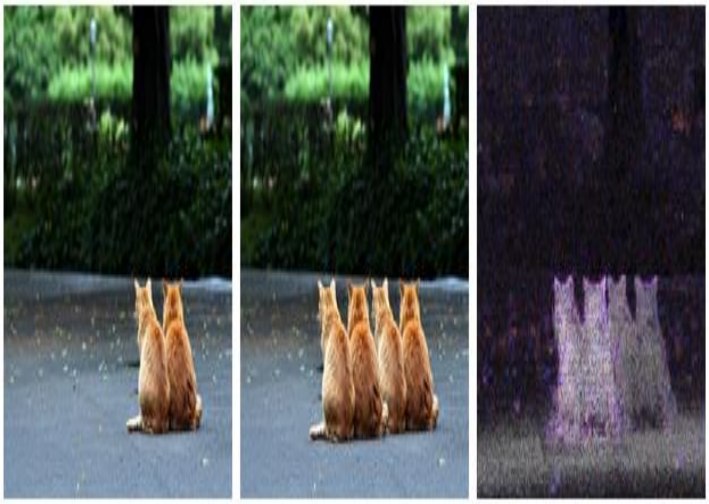

Fig.3.example for image slicing forgery

D. IMAGE RETOUCHING

Image retouching is a common technique used in image forgery to manipulate or alter the appearance of an image for various purposes. In some cases, image retouching may be used to create more complex forgeries such as fabricating evidence or manipulating news images. These forgeries can be challenging to detect, but there are various techniques available to analyze the image's color distribution, edges, and boundaries to identify inconsistencies in the image metadata. To prevent image retouching forgeries, it is essential to establish strict guidelines and protocols for image processing and authentication and educate individuals and organizations about the potential risks and consequences of image retouching forgeries, especially in sensitive or high-stakes situations.

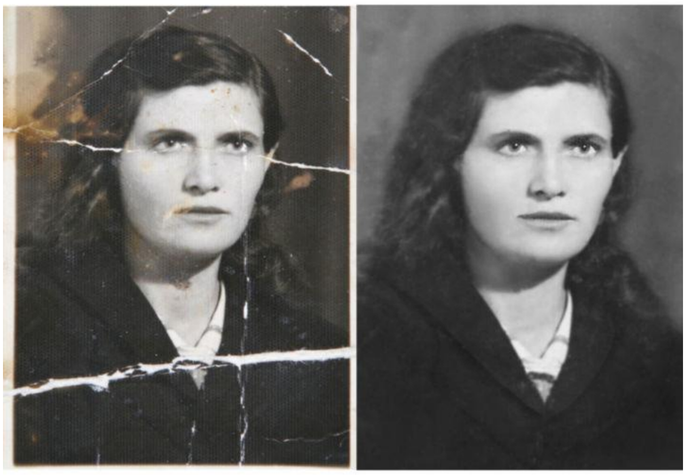

Fig.4:example for retouching old photograph

E. IMAGE MORPHING

Image morphing is a technique used to create a new image by blending two or more images together. This technique can be used to create caricatures, animations, or even to create fake images. Image morphing forgery is when this technique is used maliciously to create a fake image that appears realistic. Detecting image morphing forgery can be difficult, but there are various techniques available to identify inconsistencies in the image's color distribution, texture, and edges. To prevent image morphing forgery, it is essential to establish strict guidelines for image processing and authentication and educate people about the potential risks and consequences of creating and sharing fake images.

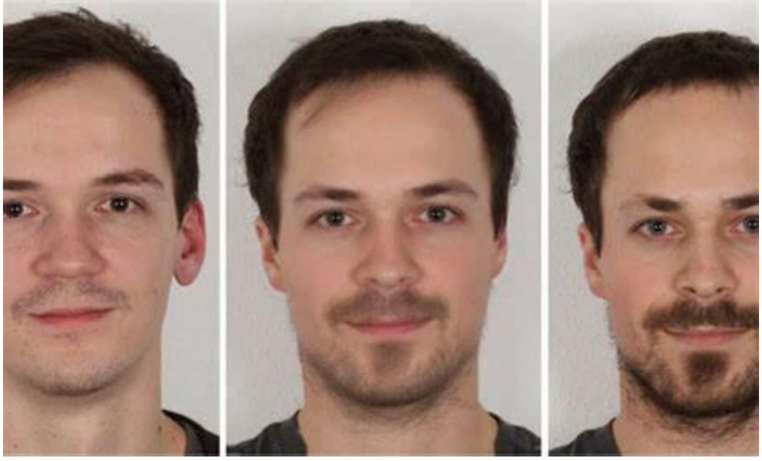

Fig.5:Example for image morphing

III. IMAGE FORGERY DETECTION

Image forgery detection is the process of identifying whether an image has been manipulated or not. This can be achieved by analyzing various features such as pixel values, color spaces, and image textures. However, with the increasing use of sophisticated image editing tools, it has become challenging to detect image forgeries using traditional techniques. Deep learning techniques, on the other hand, have shown promising results in image forgery detection due to their ability to learn high-level features from raw data.

Convolutional Neural Networks (CNNs) are the most commonly used deep learning techniques for image forgery detection. CNNs are designed to identify features in images by applying filters to different parts of the image. CNNs can learn the features that are most relevant to image forgery detection, such as color variations, edges, and textures.

Recurrent Neural Networks (RNNs) have also been used for image forgery detection. RNNs are particularly useful for detecting temporal changes in videos or image sequences. They can identify patterns in the sequence of images that are indicative of image forgeries.

Generative Adversarial Networks (GANs) have also shown promising results in image forgery detection. GANs are designed to generate new images that are similar to the original images. They can also be used to detect image forgeries by comparing the generated images to the original images.

IV. RELATED WORKS

Youssef William, et al.[1] proposes a technique for detecting image forgery by analyzing point features. The technique involves extracting SIFT keypoints , clustering them, and analyzing the distribution of clusters. Experimental results show that the proposed technique is effective in detecting different types of image forgeries, including copy-move, splicing, and removal. Ze Yang ,et al.[2] proposes a method for detecting colorized image forgeries using VLAD encoding and SVM. The proposed method extracts feature descriptors from colorized images, applies VLAD encoding to cluster the descriptors, and trains an SVM classifier to identify forgeries. Experimental results demonstrate the effectiveness of the proposed method in detecting colorized forgeries.

Chi-Man Pun, et al.[3] proposes a forgery detection method by segmenting images using adaptive over-segmentation and matching feature points between regions. The method is effective in detecting various types of forgeries, including copy-move and splicing, and outperforms state-of-the-art methods. Muhammad Naveed Abbas, et al.[4] proposes a deep learning model for detecting copy-move forgeries, which can be applied to post-processed images. The proposed model achieves high detection accuracy and outperforms other state-of-the-art methods.

Gul Muzaffer and Guzin Ulutas [5] proposes a deep learning-based approach to detecting copy-move forgery in digital images. The proposed method uses a convolutional neural network (CNN) to learn discriminative features and achieve high accuracy in detecting copy-move forgeries. Md. Taksir Hasan Majumder and A. B. M. Alim Al Islam [6] presents a comprehensive survey of deep learning-based approaches to image forgery detection. The survey covers various deep learning models, techniques, and datasets used in the field of image forgery detection. Jason Bunk, et al.[7] observed that uses deep learning techniques such as convolutional neural networks (CNNs) to learn discriminative features from resampling-based features and detect image forgeries. The proposed method also incorporates localization modules to accurately locate forged regions. H M Shahriar Parvez, et al.[8] observed

that proposes a method for detecting copy-move forgeries using Gabor descriptors and K-means clustering. The proposed method achieves high accuracy in detecting copy-move forgeries and is computationally efficient.
Ms. Jayshri Charpe and Ms. Antara Bhattacharya [9] proposes a method for detecting image manipulation by analysing the statistical properties of the image. Arfa Binti Zainal Abidin [10] presends a comprehensive survey of deep learning-based approaches for detecting copy-move forgeries. The survey covers various deep learning techniques such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and generative adversarial networks (GANs) used in the field of copy-move forgery detection.

V. SUMMARY OF LITERATURE REVIEW

The literature review papers discussed various techniques for detecting image forgeries, with some focusing on deep learning-based methods and others on traditional methods. Many papers proposed segmentation-based approaches, such as adaptive over-segmentation and feature point matching, while others used resampling features, Gabor descriptors, or statistical properties of the image. The deep learning-based approaches included CNNs, RNNs, and GANs, and were shown to achieve high detection accuracy. Some papers also addressed the issue of detecting forgeries in post-processed images. Overall, the papers demonstrated a wide range of effective techniques for detecting image forgeries, with the most effective approach depending on the specific type of forgery and the characteristics of the image.

VI. FUTURE SCOPE

Image forgery detection using deep learning has a promising future as it has shown significant improvements in detecting image forgeries in recent years. Advanced deep learning models such as attention mechanisms, transformer networks, and graph neural networks, can improve the accuracy and efficiency of image forgery detection. Multi-model forgery detection: The combination of different modalities, such as text, audio, and video, with image forgery detection can provide a more comprehensive and robust forgery detection system. Real-time forgery detection using deep learning can enable quick and efficient detection of image forgeries in real-world scenarios, such as social media platforms and live news broadcasts. Application-specific detection can help in identifying and preventing specific types of forgeries in these domains.

VII. CONCLUSION

The paper provided a comprehensive overview of image forgery detection and its importance in computer vision. The review highlighted that deep learning techniques, including CNNs, RNNs, and GANs, have been widely used for image forgery detection. The review paper evaluated the effectiveness of deep learning techniques in detecting various types of image forgeries, such as copy-move, splicing, and retouching. The current limitations of deep learning techniques were identified, including the need for standardized datasets, the vulnerability of models to adversarial attacks, and the lack of standardization in benchmarking protocols. Future research directions were proposed, such as developing more robust and efficient models for image forgery detection, improving the availability of standardized datasets, and developing standardized benchmarking protocols.In conclusion, the review paper highlights the potential of deep learning techniques in detecting image forgeries and identifies the current challenges and limitations that need to be addressed in future research.

VIII. REFERENCES

[1]. William, Y., Safwat, S. and Sal em, M.A.M., 2019, September. Robust image forgery detection using point feature analysis. In 2019 Federated Conference on Computer Science and Information Systems (FedCSIS) (pp. 373-380). IEEE.

[2]. Yang, Z., Yu, Z., Liang, Y., Guo, R. and Xiang, Z., 2020, December. Computer Generated Colorized Image Forgery Detection using VLAD Encoding and SVM. In 2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC) (Vol. 9, pp. 272-279). IEEE.

[3]. Pun, C.M., Yuan, X.C. and Bi, X.L., 2015. Image forgery detection using adaptive oversegmentation and feature point matching. ieee transactions on information forensics and security, 10(8), pp.1705-1716.

[4]. Abbas, M.N., Ansari, M.S., Asghar, M.N., Kanwal, N., O'Neill, T. and Lee, B., 2021, January. Lightweight deep learning model for detection of copy-move image forgery with post-processed attacks. In 2021 IEEE 19th World Symposium on Applied Machine Intelligence and Informatics (SAMI) (pp. 000125-000130). IEEE.

[5]. Muzaffer, G. and Ulutas, G., 2019, April. A new deep learning-based method to detection of copy-move forgery in digital images. In 2019 scientific meeting on Electrical-Electronics & Biomedical Engineering and computer science (EBBT) (pp. 1-4). IEEE.

[6]. Majumder, M.T.H. and Al Islam, A.A., 2018, December. A tale of a deep learning approach to image forgery detection. In 2018 5th international conference on networking, systems and security (NSysS) (pp. 1-9). IEEE.

[7]. Bunk, J., Bappy, J.H., Mohammed, T.M., Nataraj, L., Flenner, A., Manjunath, B.S., Chandrasekaran, S., Roy-Chowdhury, A.K. and Peterson, L., 2017, July. Detection and localization of image forgeries using resampling features and deep learning. In 2017 IEEE conference on computer vision and pattern recognition workshops (CVPRW) (pp. 1881-1889). IEEE.

[8]. Parvez, H.S., Jalab, H.A., Ala'a, R., Sadeghi, S. and Uliyan, D.M., 2018, July. Copy-move Image Forgery Detection Based on Gabor Descriptors and K-Means Clustering. In 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (pp. 1-6). IEEE.

[9]. Charpe, J. and Bhattacharya, A., 2015, April. Revealing image forgery through image manipulation detection. In 2015 Global Conference on Communication Technologies (GCCT) (pp. 723-727). IEEE.

[10]. Abidin, A.B.Z., Majid, H.B.A., Samah, A.B.A. and Hashim, H.B., 2019, December. Copy-move image forgery detection using deep learning methods: a review. In 2019 6th international conference on research and innovation in information systems (ICRIIS) (pp. 1-6). IEEE.