Abstract

Image forgery detection is a critical field in digital forensics, aiming to verify the authenticity of images in an era where digital manipulation tools are widely accessible. The surge in doctored images across media platforms necessitates robust methods to discern genuine imagery from altered ones. Recent advancements in deep learning have significantly enhanced the ability to detect sophisticated forgeries, including those involving copy-move and splicing techniques. These methods leverage neural networks to analyze visual data for inconsistencies that may indicate tampering. Moreover, the detection of Deep-fake content, which can generate highly realistic image alterations, has become a focal point in forgery detection research. As technology evolves, so does the complexity of forgeries, making ongoing research and development in this area both challenging and essential for maintaining the integrity of digital content..

Contents

List Of Figures

CHAPTER 1

INTRODUCTION

Image forgery detection is a critical field in digital forensics, addressing the challenge of identifying manipulated or altered images. With the advent of sophisticated image editing software, the authenticity of digital images has become a significant concern, especially in contexts where visual evidence is paramount. The process involves analyzing an image's characteristics to detect inconsistencies that may suggest tampering. Techniques in this field have evolved from simple, manual inspection to advanced computational methods, including machine learning and deep learning approaches. These technologies can examine various aspects of an image, such as pixel consistency, metadata, and compression artifacts, to determine its integrity. As the field progresses, the development of more robust and efficient detection tools continues to be a vital area of research, with applications ranging from security and law enforcement to media and academic integrity. The goal is not only to identify forgeries but also to maintain trust in digital media as a reliable source of information. Image forgery detection stands as a guardian against misinformation, ensuring that the digital representations we see and share are true to reality.[8]

1.1 Background and Related Work

Image forgery detection has become a critical field of study as the ease of manipulating digital images has grown with advances in technology. The proliferation of sophisticated image editing tools has led to a significant increase in the creation and distribution of forged images, necessitating the development of reliable detection methods. Recent research has focused on deep learning approaches, which have shown promise in identifying manipulations such as copy-move and splicing attacks, as well as more complex forgeries like DeepFake generated content. These methods leverage the power of neural networks to learn and detect inconsistencies and artifacts that may indicate tampering. Studies have also explored the use of multi-modal fusion techniques, which combine various forms of data to improve detection accuracy. Furthermore, the field has

seen the introduction of unsupervised learning methods, such as contrastive learning and clustering, to enhance the ability to detect forgeries without the need for labeled datasets. As the field evolves, it is expected that image forgery detection methods will become more sophisticated, incorporating a wider range of forensic features and adapting to new forms of digital manipulation.

1.2 Objective of the Project

The objective of a face forgery detection project is to develop algorithms and systems capable of identifying and detecting manipulated or forged facial images and videos. With the rise of sophisticated image and video editing tools, such as deep learning-based generative models like GANs (Generative Adversarial Networks), it has become increasingly challenging to discern real from fake content, especially in the context of facial images and videos.

1.3 Objective of the Project

The objective of a face forgery detection project is to develop algorithms and techniques capable of identifying manipulated or forged facial images and videos. With the rise of deep learning and artificial intelligence, creating convincing fake images and videos, commonly referred to as deep-fakes, has become increasingly accessible. These deep-fakes can be used for malicious purposes, such as spreading misinformation, defamation, or identity theft [9].

Therefore, the aim of face forgery detection projects is to create robust systems that can distinguish between authentic and manipulated facial content. This typically involves developing machine learning models trained on datasets of both real and fake facial images and videos. These models can then be used to analyze new content and determine it.

1.4 Purpose and Significance

Image forgery detection is a critical field in digital forensics, addressing the growing concern over the authenticity of images in various sectors such as journalism, law enforcement, and online media. With the widespread availability of sophisticated image editing tools, the manipulation of images has become more prevalent, leading to the spread of misinformation and potential legal issues. The purpose of image forgery

detection is to verify the integrity of images, ensuring that they have not been altered in a deceptive manner. This is significant as it helps maintain public trust in digital media, supports the credibility of journalistic sources, and upholds the evidentiary value of images in legal contexts. Advanced techniques, including deep learning approaches, have been developed to detect subtle manipulations that are not visible to the naked eye, thereby combating the spread of fake images and protecting individuals and organizations from the consequences of image-based fraud.

1.5 Technological landscape

The technological landscape of face forgery detection encompasses a variety of techniques and approaches, drawing from fields such as computer vision, machine learning, deep learning, image processing, and forensic analysis. Here are some key technologies and methods commonly used in face forgery detection[10]

- **Deep Learning Models**: Deep learning has revolutionized face forgery detection, with conventional neural networks (CNNs) being widely used. These models can automatically learn features from raw image data, enabling them to detect subtle manipulations in facial images and videos.
- **Generative Adversarial Networks (GANs)**: GANs are used both for creating deep-fakes and for detecting them. In the context of forgery detection, GAN-based approaches train discriminative models to distinguish between real and fake images.
- **Capsule Networks**: Capsule networks offer an alternative to traditional CNN architectures and have shown promise in detecting manipulated images by capturing hierarchical relationships between image features.
- **Forensic Analysis Techniques:** These techniques involve analyzing various aspects of an image or video, such as inconsistencies in lighting, shadows, reflections, and facial geometry, to detect signs of manipulation.[7]

1.6 Scope

The scope of face forgery detection encompasses various techniques and methodologies aimed at identifying and preventing the manipulation of facial images or videos. Here's a breakdown of the scope:

Image Manipulation Detection: This involves developing algorithms to detect whether facial images have been digitally altered or manipulated. Techniques may include analyzing inconsistencies in pixel patterns, identifying artifacts left by editing software, or comparing the image to a database of known authentic images.

Deep fake Detection: Deep fakes are highly realistic forgeries created using deep learning algorithms. Detecting deep fakes involves training models to recognize patterns specific to deep fake generation, such as unnatural facial movements, inconsistent lighting or shadows, and discrepancies in facial features.

Video Analysis: In addition to static images, detecting face forgeries in videos is crucial. This includes identifying manipulated facial expressions, detecting inconsistencies in facial movements, and assessing the overall coherence of the video sequence.

CHAPTER 2

LITERATURE REVIEW

2.1 Literature Review

Recent developments of image forensic techniques have led to the emergence of state-of-the-art techniques with which we can detect manipulations that have been made in digital images. Previously, some research studies .have proposed approaches that rely on the observations that are made during each phase of the image history, from its acquisition phase to saving it in a compressed format. The processing of the image leaves a trace on the image for the verification of digital authenticity. It is then determined as authentic or inauthentic by the verification of a digital signature.[6]

Yerushalmy et al. suggested a new approach for the detection of image forgery. This technique is not adding digital watermarking in the images and does not compare the images for training and testing. The authors proposed that image features extracted during the acquisition phase are themselves proof of authenticity of the image. These features are often visible to the naked eye. Specifically, it uses image artifacts caused by various irregularities as markers to determine image validity. Ahmet et al. proposed a technique for detecting image tampering using a color filter array. It computes a single feature and a simple threshold-based classifier. The authors tested their approach with authentic, computer-generated, and tampered images. The experimental analysis showed low error rates.[11]

Barad et al. performed a research survey that was based on deep learning techniques for the task of image forgery detection, and they presented an analysis of the approaches used to detect the authenticity of images on publicly available datasets. Yue et al. introduced a deep learning-based architecture for copy/move image forgery detection using Buster-net, which is an end-to-end trainable approach. Buster-net uses two-branch architecture. The goal of the first branch is to identify manipulation areas using visual artifacts, whereas the second branch identifies copy/move areas using visual similarities. For effective Buster-Net training, they proposed simple techniques for out-of-domain datasets and a stepwise approach. Their extensive research study demonstrated that Buster-net outperformed traditional copy/move algorithms by a large margin. The proposed architecture was evaluated with the CASIA and CoMoFoD datasets.

Manhattan ET AL. discussed the importance of detecting tampering in images using deep learning-based techniques on publicly available datasets such as CASIA, UCID, MICC , and so forth. They covered passive image forensic analysis methodology and highlighted future challenges in developing a mechanism for the detection of tampered images. In another study, Belhassen et al. proposed a unique IDF technique based on a CNN. The goal of this technique is to automatically learn how image modification could be done. The proposed IDF technique takes image-altering features as input generated after destroying the contents of an image. Since tampering alters some resident associations, this technique focused on examining the local operational association among pixels rather than focusing on the look and feel of the image; it then detects forgery in an image. In another study, Rao et al. proposed a CNN-based architecture for the detection of digital image forgery. They proposed that the first layer of the CNN model is directly involved in the prepossessing stage. It searches for the issues that occur after tampering. They trained the CNN model on trial images, whereas SVM was used for the detection of manipulations. Bi et al. proposed a ringed residual U-Net (RRU-Net) for forgery detection in image slicing. They proposed an architecture where forgery detection is employed using an end-to-end image segmentation network. The goal of the RRU-Net study was to use human brain mechanisms to develop an approach using RRU-Nets, which can detect manipulations without pre- and post-processing. Generally, the human brain works on recall and consolidation mechanisms. Therefore, the purpose of this technique is to optimize the learning capacity of a CNN, which is inspired by human brain attributes. They solved the gradient degradation problem, as residual propagation is used to recall the input feature information in a CNN. Finally, it differentiates between the original and fake regions, as the remaining response is merged with the response feature. The experimental results showed that the proposed technique gave better results compared to the state-of-the-art traditional methods.

In another study, Zhan et al. proposed a transfer learning-based methodology that has the benefit of gaining prior knowledge using the steganalysis model. With this approach, they were able to obtain an average accuracy of 97.36% on the BOSSBase and BOW datasets. Amit et al. proposed a transfer learning-based mechanism that utilizes the pre-trained weights of the AlexNet model, which saves training time. This approach uses SVM as a classifier. The overall performance of the model was satisfactory.

CHAPTER 3

PROBLEM STATEMENT

3.1 Problem Statement

In the digital age, the authenticity of images has become a topic of increasing concern. With the advent of sophisticated image editing software, the ability to manipulate images has never been easier, leading to a rise in the phenomenon known as image forgery. This has significant implications for various sectors, including media, legal evidence, academic research, and more, where the integrity of visual data is paramount.

Image forgery detection is a field that addresses these concerns by developing methods to identify altered images. The problem statement of image forgery detection revolves around the need to discern authentic images from those that have been manipulated, a task that is becoming increasingly complex with the advancement of editing tools. The challenge lies not only in detecting the presence of forgery but also in localizing and characterizing the nature of the alterations.

Recent research has focused on leveraging deep learning techniques to improve the accuracy and efficiency of forgery detection. Convolutional neural networks (CNNs), for instance, have shown promise in identifying subtle inconsistencies within an image that may indicate tampering. These methods analyze various aspects of an image, such as pixel-level details, compression artifacts, and noise patterns, to detect signs of manipulation.

The development of comprehensive datasets and benchmarks is crucial for advancing this field. These datasets provide a diverse range of forged images, allowing researchers to train and test their detection models effectively. As the technology evolves, so does the sophistication of forgeries, making it a continuous race between forgers and forensic analysts.

The implications of image forgery are far-reaching. In the realm of journalism, for instance, the integrity of photographic evidence is essential for credible reporting. In legal scenarios, tampered images can lead to wrongful convictions or acquittals. Therefore, the

development of robust image forgery detection systems is not just a technical challenge but also a societal necessity.[12]

3.2 Existing System

Image forgery detection using deep learning by recompressing images

Capturing images has been increasingly popular in recent years, owing to the widespread availability of cameras. Images are essential in our daily lives because they contain a wealth of information, and it is often required to enhance images to obtain additional information. A variety of tools are available to improve image quality; nevertheless, they are also frequently used to falsify images, resulting in the spread of misinformation. This increases the severity and frequency of image forgeries, which is now a major source of concern. Numerous traditional techniques have been developed over time to detect image forgeries. In recent years, convolutional neural networks (CNNs) have received much attention, and CNN has also influenced the field of image forgery detection. However, most image forgery techniques based on CNN that exist in the literature are limited to detecting a specific type of forgery (either image splicing or copy-move). As a result, a technique capable of efficiently and accurately detecting the presence of unseen forgeries in an image is required. In this paper, we introduce a robust deep learning based system for identifying image forgeries in the context of double image compression. The difference between an image's original and recompressed versions is used to train our model. The proposed model is lightweight, and its performance demonstrates that it is faster than state-of-the-art approaches. The experiment results are encouraging, with an overall validation accuracy of 92.23%.

Disadvantages Of forgery detection system

1. **Resource Intensive:** Some forgery detection methods require significant computational resources, making them impractical for real-time applications or large-scale image datasets. This can limit their usability, especially for organizations with limited resources.

2. **False Positives and Negatives:** Like any detection system, image forgery detection algorithms can produce false positives (identifying authentic images as forgeries) or false negatives (failing to detect actual forgeries). Balancing the trade-off between these two types of errors can be challenging.

Dependency on Training Data: Many forgery detection algorithms rely on machine learning techniques and require large amounts of labeled training data. If the training data is biased or incomplete, the algorithm's performance may suffer, leading to inaccuracies in detection.

Limited to Known Techniques: Detection algorithms are typically designed to identify specific types of image manipulations or forgeries. They may struggle to detect novel or previously unseen techniques, especially if they deviate significantly from known patterns.

Privacy Concerns: Some forgery detection methods may involve analyzing sensitive or private information contained within images, raising concerns about privacy and data security. This is particularly relevant in cases where images contain personally identifiable information or sensitive content.

Ethical Considerations: The use of forgery detection technologies raises ethical questions regarding privacy, consent, and the potential for misuse. For example, there may be concerns about the use of detection algorithms to infringe on individuals' rights or to perpetrate surveillance without their knowledge.

Cost: Implementing effective forgery detection systems can be costly, particularly for organizations that require specialized expertise or custom solutions. This cost may be prohibitive for some users, especially smaller businesses or individuals.

CHAPTER 4

Proposed System

4.1 Introduction and Purpose

In the digital age, the authenticity of visual content has become a paramount concern. With the proliferation of image editing software and the ease with which digital images can be altered, the need for reliable image forgery detection methods has never been more critical. Image forgery detection is a field within digital forensics that seeks to determine the integrity of images and identify any manipulations that may have been made . The purpose of image forgery detection is multifaceted. It serves to protect individuals from defamation, businesses from false advertising claims, and the general public from misinformation. In legal contexts, ensuring the authenticity of digital evidence is crucial. Similarly, in journalism, the credibility of media outlets hinges on the veracity of the images they publish. In academic and scientific research, the integrity of visual data can significantly impact the validity of findings.

Recent advancements in deep learning have revolutionized the field of image forgery detection. Techniques such as conventional neural networks (CNNs) have been employed to detect subtle inconsistencies in images that may indicate tampering. These methods can identify common forms of image manipulation, including copy-move and splicing attacks, as well as more sophisticated Deep-fake content.[4]

The challenges in image forgery detection are significant, given the continuous evolution of image manipulation tools and techniques. Researchers are engaged in a constant arms race, developing more advanced detection methods to counter increasingly sophisticated forgeries. The goal is not only to identify forgeries but also to do so in a manner that is efficient and reliable, minimizing false positives and negatives.

The implications of image forgery detection extend beyond the immediate identification of altered images. They touch on broader societal issues such as trust in digital media, the spread of misinformation, and the ethical use of technology. As such, the field is not just about developing better algorithms; it's about fostering a digital environment where truth and authenticity are valued and preserved.

For those interested in the technical aspects of image forgery detection, recent surveys provide comprehensive overviews of the state-of-the-art methods and discuss potential future research directions. These resources are invaluable for anyone looking to understand the current landscape of image forgery detection and its importance in maintaining the integrity of digital media.

4.2 Digital Image Forgery Detection Methods

Typically, the methodologies used for forgery detection are classified into two types such as active forensics and passive forensics, in which digital watermarking and digital signature are the types of active techniques. Then, the splicing, image retouching, image cloning, and copy-move techniques are the categories of the passive technique. The description of these techniques are investigated in the following sub-sections

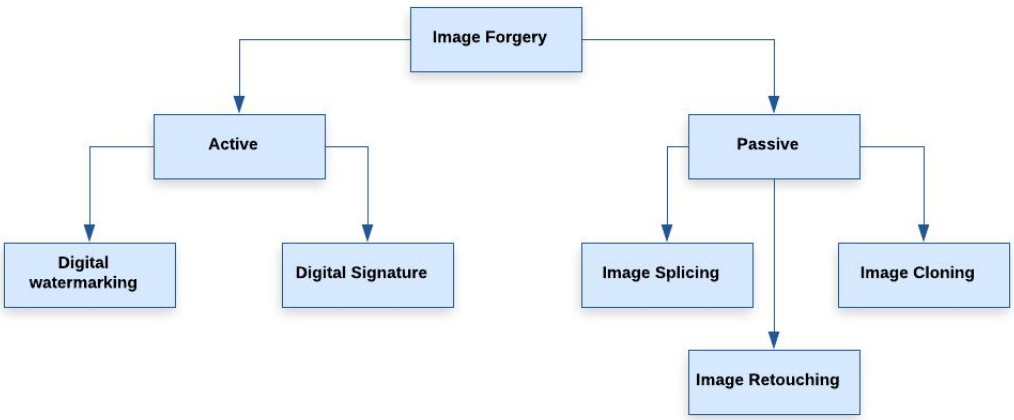


figure 4.1. Categories of image forgeries[14]

4.3 Digital Watermarking

In this type of image forgery, a digital watermark is added on the photo, which is more or less visible. Then, the appended information is more or less transparent, so it is very difficult to notice the watermark. Ferrara, et al. suggested a new forensic tool for analyzing the original image and forged regions based on the interpolation process. The image splicing can be detected by the use of the conditional Co-occurrence Probability Matrix (CCPM) , which uses the third-order statistical features during the forgery detection. Normally, the watermarking schemes are categorized as reversible and irreversible. In which, the image irreversible distortions are avoided based on the original features of the image by using the reversible watermarking techniques. The watermarking can be mainly used to indicate the source or authorized consumer of the image. It is a pattern of bits that is inserted into a digital media for identifying the creator. The watermarking techniques are semi-fragile, fragile, and content based, which are mainly used for image authentication application. Li, et al. implemented a new method for detecting the copy move forgery, where the Local Binary Pattern (LBP) was utilized to extract the circular blocks. The stages involved in this system are preprocessing, feature extraction, feature matching, and post processing. Here, it is stated that when the region is rotated at different angles, it is highly difficult to detect the forgeries. Hussain, et al.suggested a multiresolution Weber Local Descriptors (WLD) for detecting the image forgeries based on the features obtained from the chrominance components.[2] Here, the WLD histogram components are calculated and the Support Vector Machine (SVM) classifier is utilized to detect the forgery. In this paper, two different types of forgeries such as splice and copy-move are detected by using the multi-resolution WLD approach.

Applications of Image forgery detection

Media Integrity Verification: News agencies, social media platforms, and online content providers can use forgery detection to verify the authenticity of images before publishing them. This helps prevent the spread of misinformation and fake news.

Intellectual Property Protection: Companies and individuals can use forgery detection to protect their intellectual property, such as copyrighted images or logos, from unauthorized alteration or misuse.

Authentication Systems: Forgery detection algorithms can be integrated into authentication systems to verify the authenticity of identity documents, passports, or other forms of official documentation.

Art and Photography Authentication: In the art world, forgery detection can help authenticate paintings, photographs, and other works of art to prevent fraud and ensure the integrity of art collections.

Digital Rights Management (DRM): Forgery detection can be used in DRM systems to protect digital content, such as movies, music, and ebooks, from unauthorized manipulation or distribution.

Biometric Authentication: In biometric systems, forgery detection can help ensure the authenticity of biometric data, such as fingerprints or facial images, used for identity verification purposes.

E-commerce and Online Marketplace: Online retailers can use forgery detection to verify the authenticity of product images submitted by sellers, helping to build trust with customers and prevent the sale of counterfeit goods.

Medical Imaging: In healthcare, forgery detection can be applied to medical images, such as X-rays and MRI scans, to ensure their integrity and authenticity for diagnostic purposes.

Document Verification: Forgery detection can assist in verifying the authenticity of digital documents, such as contracts, financial records, and legal agreements, to prevent fraud and tampering

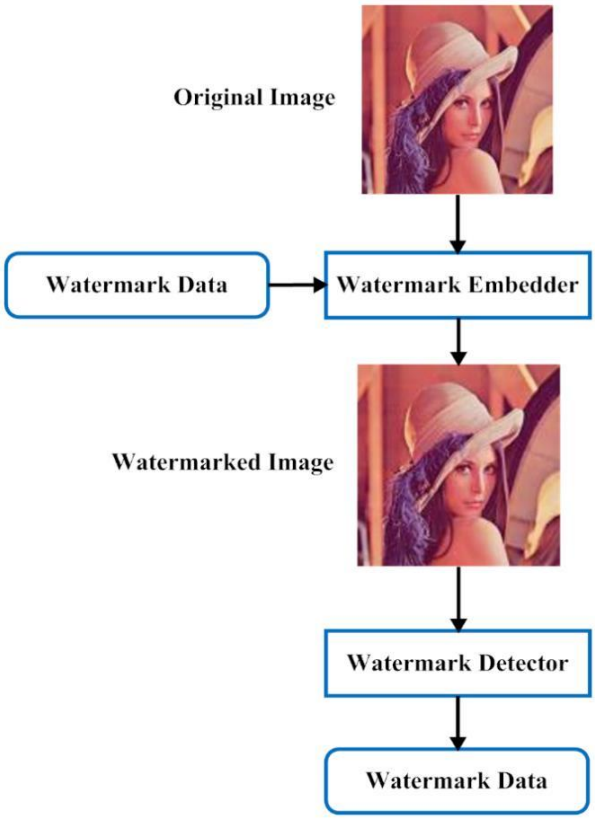


Figure 4.2. Digital watermarking[15]

4.4 Splicing Method

Image splicing is a kind of forgery detection method, in which a single image is created based on the combination of two or more images. It is also termed as image composition, in which various image manipulation operations are performed. Typically, many inconsistencies may be created in the image features due to the splicing operation. In this technique, the composition between the two images is estimated and incorporated for creating a fake image. Based on the image block content, the difference between the illumination and reference illuminate color is estimated. In this digital image forgery, it is very difficult to extract the exact shape of the image. Typically, the image splicing method is categorized into two types such as boundary-based and regionbased. Alahmadi, et al suggested a passive splicing forgery detection mechanism for verifying the authenticity of digital images. Here, the features are extracted from the chromatic channel for capturing the tampering artifacts. Kakar, et al utilized a forgery detection approach for detecting the splicing in the digital images. Here, the small inconsistencies in the motion blur are detected by analyzing the special characteristics of image gradients . The stages involved in this detection are image subdivision, motion blur estimation, smoothing, blur computation, interpolation and segmentation.[3]

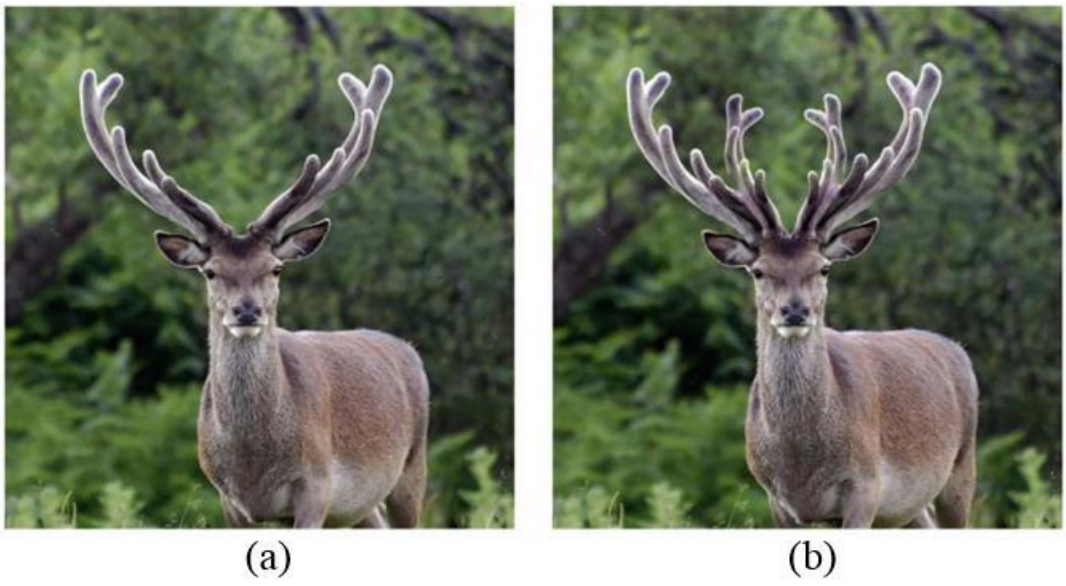


figure 4.3 (a). Original image and (b). Duplicated image[16]

4.5 Image Retouching

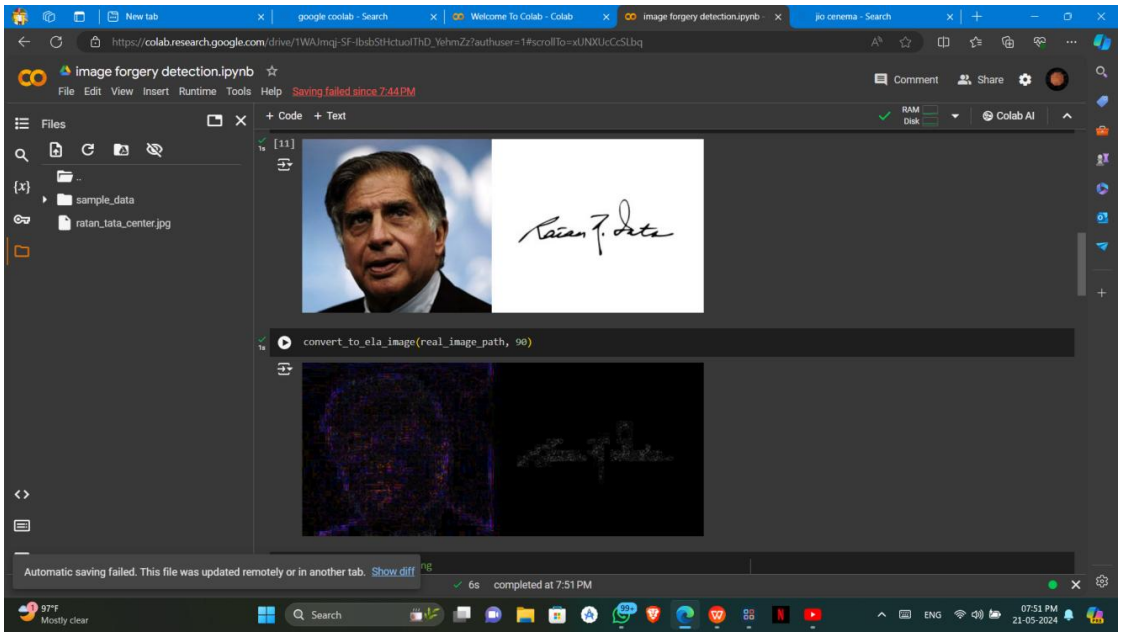
Among the other image forgeries, image retouching is considered as the less harmful forgery technique, in which some enhancement can be performed on the image. Also, it is popular in photo editing applications and magazines. Muhammad, et al suggested an un-decimated dyadic wavelet transformation technique for detecting the copy-move forgery. Typically, more sophisticated tools are available for making this type of forgery by applying the soft touch on the edges. So, it is very difficult to differentiate the color and texture of the stimulated part with the unoriginal part. Moreover, it makes the forgery detection as highly complicated, because of two or more identical objects in the same image. So, the authors of this paper utilized similarity measurements for detecting this forgery, in which the noisy inconsistency is analyzed between the copied and moved parts. Here, it is stated that the transformation methods such as FMT, Scale Invariant Feature Transform (SIFT), and Discrete Wavelet Transform (DWT) can detect the forgery in a highly compressed image. Ghorbani, et al recommended a Discrete Cosine Transform Quantization Coefficients Decomposition (DCT-QCD) for detecting the copy-move forgery.The integrity and authenticity verification of digital images is a very difficult process, specifically the images used for news items, medical records, and court law. Because the copy-move forgery may be created for those types of images.[1]

figure 4.4 (a). Forged image and (b). Real image[17]

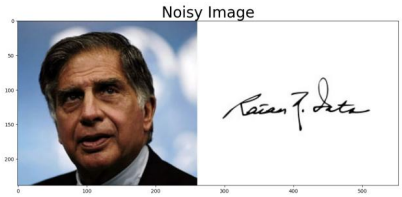
CHAPTER 5

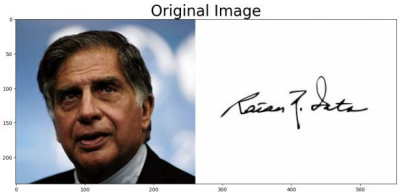
Output

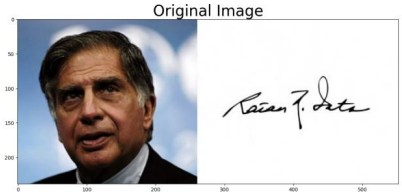
5.1 Output



5.2 Output 2







CHAPTER 6

CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

Image forgery detection has become a critical field of study as the prevalence of digital images grows in our daily lives. With the advancement of technology, the ability to manipulate images has become more accessible, leading to a surge in doctored images across various media. This has necessitated the development of sophisticated methods to detect and prevent image forgery. Recent research has focused on deep learning techniques, which have shown great promise in identifying alterations in images, such as copy-move and splicing attacks. These methods leverage the power of neural networks to learn and detect patterns that are indicative of forgery, often with a high degree of accuracy.

The field is evolving rapidly, with new datasets being created to train and test these deep learning models, ensuring they can handle a wide array of forgery scenarios. Researchers are also exploring the use of error level analysis, noise residuals, and other statistical methods to complement deep learning approaches. The goal is to create a robust system that can not only detect but also localize the forged areas within an image, providing comprehensive tools for forensic analysis.

As we look to the future, the integration of machine learning techniques with traditional digital forensics approaches appears to be a promising direction. This could lead to the development of more generalized models that can adapt to the ever-changing landscape of digital forgery. Moreover, there is a growing emphasis on open access to research, allowing for greater collaboration and advancement in the field. The battle against image forgery is not just a technical challenge but also a societal one, as it involves maintaining the integrity of visual information in a world increasingly reliant on digital media.

In conclusion, the fight against image forgery is ongoing, with deep learning at the forefront of current research efforts. The continuous improvement of detection methods, coupled with the development of new datasets and collaborative research, will be vital in preserving the authenticity of digital imagery. As the technology advances, so too must our vigilance and our tools, ensuring that we can trust the images that inform, entertain, and impact our lives.

6.2 Future Scope

- Advancements in Deep Learning: The future of image forgery detection is likely to be dominated by deep learning techniques, which have shown promising results in identifying sophisticated manipulations like copy-move and splicing attacks.

- Combating DeepFakes: As DeepFake technology evolves, image forgery detection methods will need to adapt to effectively distinguish between real and AI-generated images.

- Dataset Development: Building comprehensive datasets will be crucial for training and validating image forgery detection algorithms, ensuring they can handle a wide range of forgery scenarios.

- Legal and Ethical Considerations: With the increasing prevalence of image forgeries, there will be a growing need for legal frameworks to address the ethical implications of digital image manipulation.

- Cross-Media Solutions: Research is moving towards developing forgery detection methods that are not just limited to images but can be generalized across different media forms, including video.

- Environmental Awareness: Future research may involve enhancing the environmental awareness of forgery detection systems, allowing them to consider the context in which an image was taken.

- Protection Against Hostile Attacks: As image forgery techniques become more sophisticated, detection methods will need to improve to protect against adversarial attacks that aim to fool these systems.

- Comprehensive Analyses: There will be an emphasis on in-depth reviews and comparative studies of forgery detection methods, providing clear directions for new research in the field.

References

[1] B. Mahdian and S. Saic, "A bibliography on blind methods for identifying image forgery," Signal Processing: Image Communication, vol. 25, pp. 389-399, 2010.

[2] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy-move forgery detection scheme," IEEE Transactions on Information Forensics and Security, vol. 10, pp. 507-518, 2015.

[3] H.-D. Yuan, "Blind forensics of median filtering in digital images," IEEE Transactions on Information Forensics and Security, vol. 6, pp. 1335- 1345, 2011.

[4] C. Chen, J. Ni, and J. Huang, "Blind detection of median filtering in digital images: A difference domain based approach," IEEE Transactions on Image Processing, vol. 22, pp. 4699-4710, 2013.

[5] X. Lin, J.-H. Li, S.-L. Wang, A.-W.-C. Liew, F. Cheng, and X.-S. Huang, "Recent Advances in Passive Digital Image Security Forensics: A Brief Review," Engineering, 2018/02/17/ 2018.

[6] M. D. Ansari, S. P. Ghrera, and V. Tyagi, "Pixel-based image forgery detection: A review," IETE journal of education, vol. 55, pp. 40-46, 2014.

[7] C.-M. Pun, X.-C. Yuan, and X.-L. Bi, "Image forgery detection using adaptive oversegmentation and feature point matching," IEEE

[8] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "Geometric tampering estimation by means of a SIFT-based forensic analysis," in Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on, 2010, pp. 1702-1705.

[9] W. Li and N. Yu, "Rotation robust detection of copy-move forgery," in Image Processing (ICIP), 2010 17th IEEE International Conference on, 2010, pp. 2113-2116.

[10] M. C. Stamm, S. K. Tjoa, W. S. Lin, and K. R. Liu, "Undetectable image tampering through JPEG compression anti-forensics," in Image Processing (ICIP), 2010 17th IEEE International Conference on, 2010, pp. 2109-2112.

[11] V. Christlein, C. Riess, and E. Angelopoulou, "On rotation invariance in copy-move forgery detection," in Information Forensics and Security (WIFS), 2010 IEEE International Workshop on, 2010, pp. 1-6.

[12] E. Kee and H. Farid, "Exposing digital forgeries from 3-D lighting environments," in Information Forensics and Security (WIFS), 2010 IEEE International Workshop on, 2010, pp. 1-6.

[13] M. Kobayashi, T. Okabe, and Y. Sato, "Detecting forgery from staticscene video based on inconsistency in noise level functions," IEEE Transactions on Information Forensics and Security, vol. 5, pp. 883-892, 2010.

[14] Z. He, W. Sun, W. Lu, and H. Lu, "Digital image splicing detection based on approximate run length," Pattern Recognition Letters, vol. 32, pp. 1591-1597, 2011.

[15] M. Jaberi, G. Bebis, M. Hussain, and G. Muhammad, "Accurate and robust localization of duplicated region in copy–move image forgery," Machine vision and applications, vol. 25, pp. 451-475, 2014