Forged Image Perception System using CNN Algorithms

Yash Nemade
Department of Information Technology
VPPCOE & VA
University of Mumbai
vu4f2021002@pvppcoe.ac.in

Om Kolte
Department of Information Technology
VPPCOE & VA
University of Mumbai
vu4f2021019@pvppcoe.ac.in

Harshank Sutar
Department of Information Technology
VPPCOE & VA
University of Mumbai
vu4f2021128@pvppcoe.ac.in

Seema Ladhe
Faculty of Information Technology
VPPCOE & VA
University of Mumbai
seema.ladhe@pvppcoe.ac.in

Neeraj Sharma
Faculty of Information Technology
VPPCOE & VA
University of Mumbai
dr.neerajsharma@pvppcoe.ac.in

Abstract— **The progression and diversification of methodologies in digital image forensics and manipulation detection are evident in existing work, presenting innovative techniques tailored to specific aspects of forgery detection. These methodologies encompass various challenges such as copy-move forgery, manipulation detection, demosaicing artifacts, image splicing, edge detection, and compression analysis. Together, these studies exemplify ongoing efforts to enhance the accuracy, efficiency, and reliability of forgery detection methods within the constantly evolving landscape of digital image manipulation. The proposed image forgery detection system represents a pioneering advancement, surpassing the limitations of conventional methodologies. It integrates a comprehensive array of detection techniques, including copy-move analysis, color filter array scrutiny, noise variance inconsistency detection, and double JPEG artifact identification. These techniques are bolstered by Convolutional Neural Networks (CNNs). This innovative fusion not only addresses the limitations inherent in existing systems but also signifies a significant leap forward in functionality and efficacy. By synergistically leveraging the strengths of each detection method within a CNN framework, our approach promises heightened accuracy, robustness, and adaptability in discerning even the most sophisticated forms of image tampering.**

Keywords— Image Tampering, Double JPEG Compression, Demosaicing Artifacts, Recursive Edge Detection, Copy-Move Forgery Detection.

I. INTRODUCTION

The proliferation of digital imagery has led to an increase in various forms of image manipulation, necessitating the development of sophisticated detection methods. Conventional approaches often lack versatility, prompting researchers to propose more adaptable forensic algorithms. Innovative techniques such as SIFT-based algorithms, CNNs, demosaicing artifact analysis, and edge detection from CFA images have been introduced to efficiently and accurately identify manipulation features. The aim of these advancements is to effectively tackle the challenges present in image forensics.

Existing systems for image forgery detection encompass a range of methods and technologies designed to identify manipulated or forged images. These systems utilize diverse algorithms and techniques to detect different types of image forgeries, including copy-move forgeries, splicing, and retouching. By analyzing the digital properties of images, such as color and pattern distributions, these systems can identify inconsistencies or irregularities indicative of manipulation. Some systems are integrated into software tools for image forensics, while others are standalone applications or libraries used by professionals in fields like law enforcement, journalism, and content authentication.

Despite their capabilities, existing systems face limitations. They may struggle to detect advanced forgeries employing sophisticated techniques to evade detection, posing an ongoing challenge to keep pace with evolving manipulation methods. Our focus is on developing a robust system capable of detecting image forgeries reliably. In today's digital landscape, where the prevalence of edited and altered images is widespread, the need for a dependable system to verify the authenticity and integrity of visual content is more critical than ever.

Thus, having a trustworthy means to confirm whether an image is genuine or tampered with is essential. Such a system would play a vital role in ensuring the authenticity and honesty of visual content, whether in journalism, legal contexts, or everyday security scenarios.

Section I provides an introduction to the concept of image forgery, discussing and highlighting the challenges present in current detection methods. It also outlines the applications of image forgery and introduces the existing constraints. Section II presents a comprehensive survey of existing literature. Sections III and IV delve into the proposed methodologies of the system, which are supported by flow charts and detailed steps. Section V showcases a visual representation of the experimental findings and comparative analysis through a graphical presentation. Lastly, Section VI encapsulates the conclusions drawn from the research and outlines avenues for future exploration.

II. LITERATURE REVIEW

Lui et al. (2014) [1] addresses the challenge of detecting copy-move forgery in digital images. The paper highlights the significance of digital image forensics in ensuring image authenticity amidst the proliferation of digital images. It reviews the widely used Scale Invariant Feature Transform (SIFT) technique for copy-move detection, emphasizing its robustness against the various processing operations. Additionally, Lui et al. propose a novel matching method combining BFSN clustering to address the limitations of standard SIFT-based algorithms in detecting multiple copies. Furthermore, the paper introduces the use of CFA features for distinguishing between original and tampered regions, demonstrating effectiveness through experimental evaluation.

BAYAR et al. (2016) [2] focuses on the development of universal forensic algorithms for detecting multiple editing operations in digital images. The paper introduces a deep learning approach utilizing convolutional neural networks (CNNs) to automatically learn manipulation detection features. It discusses the limitations of existing CNN architectures in manipulation detection, leading to the proposal of a novel convolutional layer tailored to detect manipulation-specific features. The paper presents a CNN architecture incorporating this constrained convolutional layer and demonstrates its high accuracy in detecting various image manipulations through experimental evaluation.

BAMMEY et al. (2018) [3] addresses the challenge of detecting image tampering by analyzing demosaicing artifacts. The paper introduces a contrario method for reliable detection with low false alarm rates. It reviews existing methods for demosaicing artifact detection and highlights their limitations in achieving guaranteed detections with low false alarm rates. BAMMEY et al. propose a method involving spectral analysis and statistical techniques to detect anomalies indicative of tampering, demonstrating its effectiveness through experimental evaluation on the Kodak dataset.

Mahwatta et al. (2018) [4] presents a novel method for detecting image splicing through noise pattern analysis. The paper discusses the significance of digital image forensics and identifies image splicing as a common form of digital image forgery. It provides an overview of existing approaches to splicing detection and proposes a passive forgery detection method based on noise pattern analysis. Mahwatta et al. describe the implementation steps, experimental results, and discusses the effectiveness of the proposed method in detecting image splicing.

Magnier et al. (2020) [5] introduces a novel approach to edge detection directly from Color Filter Array (CFA) images, bypassing the demosaicking step. The paper reviews traditional demosaicking-based edge detection methods and proposes a method leveraging recursive Deriche filters for computing partial derivative images. It presents two approaches, focusing on the green channel and combining the red and blue channels, respectively. Magnier et al. evaluate the proposed method through experimental comparison with existing demosaicking-based techniques, demonstrating improved performance and computational efficiency.

Kaur et al. (2020) [6] discusses a method for detecting image forgery, specifically copy-move forgery, using Fuzzy C-means Clustering (FCM) and Principle-Bacteria Foraging Optimization Algorithm (PBFOA). The paper reviews existing research in image forgery detection and proposes a method combining FCM and PBFOA algorithms for accurate forgery detection. It outlines the research methodology, presents experimental results, and concludes by discussing future research directions in the field.

Gupta et al. (2021) [7] explores the effectiveness of JPEG and Double JPEG (DJPEG) compression techniques in image forgery analysis. The paper provides an overview of the JPEG standard and double JPEG compression, highlighting their implications for image forgery detection. It reviews related work in image compression and forgery detection techniques, concluding with insights on future research directions in the field.

The foremost drawback evident across the various papers lies in the potential limitations and challenges associated with the detection of sophisticated image manipulations. While each paper proposes innovative methods and techniques for image forensics, they all face the overarching challenge of accurately identifying and distinguishing between genuine and manipulated regions in digital images. Passive forgery detection methods, such as copy-move detection and noise analysis, may struggle to effectively detect subtle or well-disguised manipulations, leading to potential false positives or negatives. Additionally, while CNN-based approaches offer promising results, they may encounter difficulties in handling certain types of manipulations or variations in manipulation techniques, and require significant computational resources for training and deployment. Furthermore, statistical guarantees and edge detection techniques may be influenced by factors such as image quality, compression artifacts, and noise, impacting their accuracy and reliability in practical implementation. Overall, further research and refinement are necessary to address these challenges and enhance the robustness and effectiveness of image forensic techniques across diverse manipulation scenarios.

To confront the obstacles inherent in detecting image manipulations, a comprehensive solution can be developed by integrating multiple algorithms and techniques. Firstly, CFA artifact detection methods, such as those proposed in the literature, can be utilized to identify traces left by demosaicing algorithms, thus providing insights into potential tampered regions. Additionally, noise variance inconsistency analysis, as discussed in various papers, can be employed to detect discrepancies in noise patterns, which may indicate areas of manipulation. Furthermore, copy-move detection algorithms offer valuable tools for identifying duplicated regions within an image, aiding in the detection of tampering. Finally, to account for potential double JPEG compression, techniques for detecting compression artifacts and analyzing compression histories can be integrated into the solution. By combining these approaches into a unified framework, the proposed solution can provide a comprehensive assessment of image authenticity, effectively distinguishing between original and tampered images. By incorporating CFA artifact detection, analysis of noise variance inconsistencies, identification of copy-move instances, and detection of double JPEG compression, this solution can provide strong and dependable image forensic capabilities, guaranteeing the integrity and authenticity of digital images across a wide range of situations.

III. PROPOSED SYSTEM

The proposed system for image forgery detection introduces a fresh approach or technology designed to address the shortcomings of current systems while offering enhanced functionality. In essence, it aims to revolutionize the way we detect image manipulations by incorporating cutting-edge algorithms, techniques, or technologies that improve accuracy, efficiency, and adaptability.

What sets the proposed system apart is its capacity to anticipate and outpace developments. Unlike traditional methods, it can quickly adapt to new forgery techniques as they emerge. This adaptability is often achieved through features that allow the system to continuously learn and evolve, ensuring it remains effective in identifying even the most advanced manipulations.

A significant aspect of its innovation lies in its holistic approach. Instead of relying on a single method, it combines multiple techniques to provide a more comprehensive solution. For example, it may incorporate copy-move detection to identify duplicated regions, analyze color filter arrays to distinguish between original and tampered areas, detect inconsistencies in noise variance, and even spot double JPEG compression—all within the framework of convolutional neural networks (CNNs).

To begin with, Fig 1 shows the framework of the system utilizing a robust copy-move detection algorithm, such as the Scale Invariant Feature Transform (SIFT) or similar techniques. This algorithm is designed to identify duplicated regions within an image, even if they have been subjected to transformations like rotation, scaling, or distortion. In essence, it can recognize if parts of the image have been copied and pasted elsewhere. This capability is crucial for spotting potential instances of forgery, allowing the system to discern between original content and manipulated areas.

Furthermore, the system incorporates Color Filter Array (CFA) analysis to detect inconsistencies that arise during the manipulation process, particularly in the color interpolation phase. Essentially, CFA analysis involves examining the patterns and variations in color filters overlaid on image sensor pixels. By scrutinizing these patterns, the system can identify regions that have been tampered with, even if the alterations are subtle or disguised. This additional layer of detection proves valuable, especially in scenarios where traditional pixel-level analysis may fall short in detecting sophisticated manipulations.

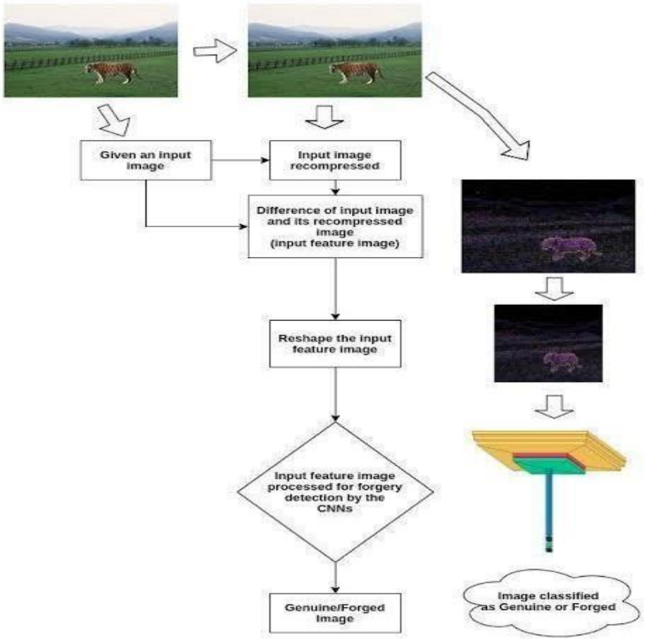
Given an input image
Input image recompressed
Difference of input image and its recompressed image (input feature image)
Reshape the input feature image
Input feature image processed for forgery detection by the CNNs
Genuine/Forged Image
Image classified as Genuine or Forged

Fig 1. Proposed System Flowchart [8]

The system then deploys a method called noise variance inconsistency detection, which involves examining the patterns of noise within an image to spot irregularities that may indicate tampering. This technique is particularly useful for uncovering areas of the image that have been altered to blend in seamlessly with the original content by replicating the noise patterns. By comparing the variations in noise levels across different parts of the image, the system can identify suspicious regions that may warrant further investigation.

Furthermore, the system tackles the challenge posed by double JPEG compression, a common method used to hide manipulation. By employing Convolutional Neural Networks (CNNs), the system can learn to recognize artifacts introduced by multiple rounds of JPEG compression, thereby exposing concealed alterations that might otherwise go undetected. This deep learning approach enables the system to adapt and evolve alongside emerging compression techniques, ensuring its continued effectiveness in detecting forgery.

Moreover, the proposed system incorporates features for continuous model training, allowing it to learn and enhance its detection capabilities over time. By regularly updating the model with new data and insights into emerging forgery methods, the system remains agile and capable of responding to evolving threats in digital image manipulation. It also offers an advanced solution to the complex task of detecting image forgeries. It integrates various detection methods within the framework of Convolutional Neural Networks (CNNs), which are known for their effectiveness in handling diverse data patterns. By combining techniques like copy-move detection, analysis of color filter arrays, detection of inconsistencies in noise variance, and identifying double JPEG compression, our system provides a comprehensive approach to identifying image tampering.

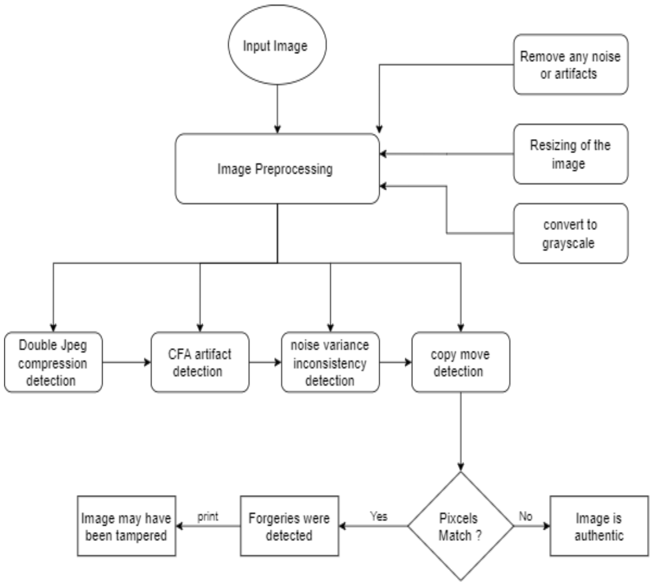

Fig 2. Proposed System Design

Fig 2. elaborates the system acts like a super-sleuth for spotting fake images. It doesn't rely on just one method but combines several clever tricks to catch out any sneaky alterations, like copying parts of images, playing with colors, or trying to hide noise inconsistencies. Plus, it's always learning and improving, so it can keep up with the latest tricks that forgers might try. This ability to adapt and respond to new and evolving forgery techniques, achieved through continuous model training and updates, enables it to stay ahead of emerging threats, ensuring consistent and reliable performance in real-world situations.

IV. IMPLEMENTATION

Convolutional Neural Networks (CNNs) are exceptionally useful for image forgery detection systems due to their ability to mimic the human visual system's way of processing images.

Fig 3. shows the architecture of CNN in which these networks have proven to be highly effective in understanding and extracting complex patterns and features from images, which is crucial for identifying subtle and sophisticated image manipulations. CNNs have demonstrated remarkable adaptability. They can be trained on large datasets of authentic and manipulated images, allowing them to continuously improve their detection capabilities. As new forgery techniques emerge, CNN-based systems can adjust and evolve, remaining effective even in the face of evolving manipulation methods.

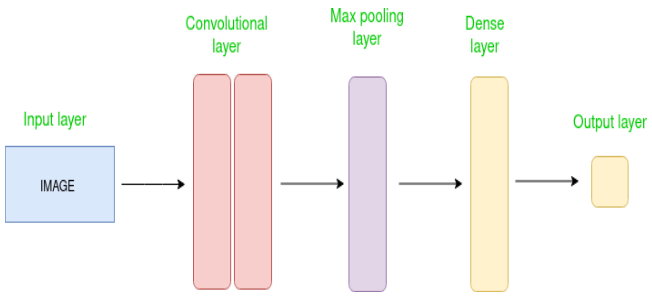

Fig 3. Architecture of CNN [9]

CNNs are powerful tools for image forgery detection systems because they can automatically and effectively analyze images, recognize intricate patterns, adapt to new challenges, and provide detailed insights into potential forgeries, all of which are essential for the accurate and efficient identification of manipulated images.

The Convolutional Neural Network (CNN) represents an advancement of traditional artificial neural networks (ANN) specifically tailored for extracting features from grid-like matrix datasets, particularly suited for visual data such as images or videos where pattern recognition is crucial. In Convolutional Neural Networks (CNNs), the Convolutional layer utilizes filters to extract significant features from the input image, whereas the Pooling layer diminishes computational complexity by down sampling the image. Subsequently, the fully connected layer facilitates the final prediction process. The network iteratively refines its filter parameters through backpropagation and gradient descent to optimize feature extraction and prediction accuracy.

Copy-move detection is a technique used to identify regions within an image that have been duplicated and relocated, commonly referred to as copy-move forgery. In this method, a CNN algorithm is trained to analyze features within the image and identify patterns indicative of duplication and movement. When applied to an image, the algorithm scans for similarities between different parts of the image, flagging regions where identical or closely resembling patterns are found. If the algorithm detects multiple instances of the same pattern in various areas of the image, it raises suspicion of copy-move forgery.

CFA artifact detection focuses on identifying inconsistencies introduced by tampering in the color interpolation process, particularly in images captured using digital cameras. The CNN algorithm is trained to analyze the arrangement of color filter patterns and variations in color information across the image. By comparing expected color patterns with observed variations, the algorithm can pinpoint areas where the color information does not align with the anticipated CFA pattern. These disparities may indicate tampering, such as the insertion of new elements or modification of existing ones.

Double JPEG compression [7] detection aims to uncover manipulations where an image has been repeatedly compressed using the JPEG format, potentially to conceal alterations. The CNN algorithm is trained to recognize artifacts introduced by multiple rounds of JPEG compression, such as quantization errors and blocking artifacts. By analyzing these artifacts across different parts of the image, the algorithm can identify regions exhibiting characteristics consistent with double JPEG compression. This detection method helps reveal areas of the image that may have undergone compression to hide tampering.

Noise variance inconsistency detection involves analyzing variations in noise patterns within an image to detect potential tampering. The CNN algorithm learns to distinguish between genuine noise patterns and anomalies introduced by manipulation. By comparing noise variances across different regions of the image, the algorithm can identify areas where the noise pattern does not match the expected distribution. These inconsistencies may indicate tampering attempts to blend manipulated regions with the original content.

The CNN [9] algorithm acts like a detective, examining different aspects of the image to uncover signs of tampering. It starts by looking for duplicate areas within the image, indicating potential copy-move forgery. Then, it checks for inconsistencies in color patterns that don't match the expected arrangement, which could suggest tampering with the color information. Next, the algorithm searches for artifacts typical of double JPEG compression [7], indicating attempts to hide alterations. Finally, it analyzes variations in noise patterns across the image, flagging areas where the noise doesn't match what's expected, possibly indicating tampering. By combining these techniques, the proposed system can predict whether an image has been tampered with, helping to ensure its authenticity.

CNN algorithms for image tampering detection utilize various techniques to distinguish between real and tampered images.

In the case of Fig 4. & 5., CFA Artifact Detection, the algorithm focuses on identifying inconsistencies in color filter array (CFA) patterns, which are indicative of image manipulation. Noise Variance Inconsistency detection relies on analyzing discrepancies in noise patterns, as tampered regions often exhibit inconsistent noise levels compared to authentic areas. Copy Move Detection algorithms identify duplicated regions within an image by analyzing similarities in patterns and textures, revealing potential tampering. Furthermore, Double JPEG Compression detection algorithms scrutinize artifacts left by multiple rounds of JPEG compression, as genuine images typically have a consistent compression history. Through these methods, CNN algorithms can effectively discern between authentic and tampered images by scrutinizing various artifacts and inconsistencies unique to digital manipulation, ensuring the integrity of visual content.

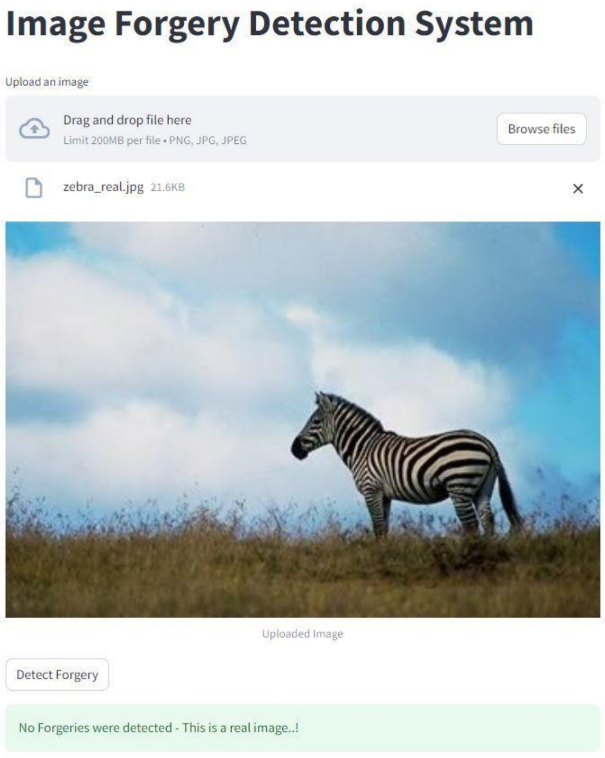

Image Forgery Detection System

No Forgeries were detected - This is a real image..!

Fig 4. Original Image

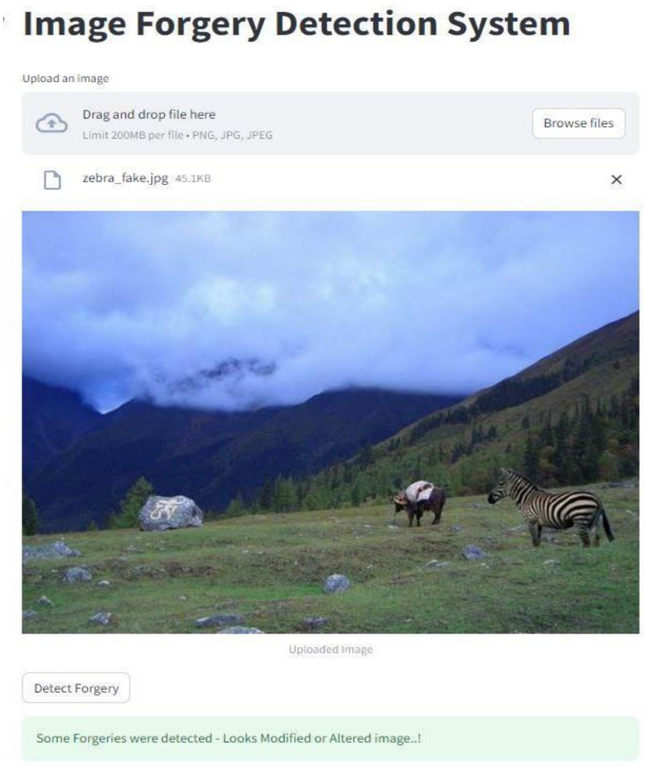

Image Forgery Detection System

Some Forgeries were detected - Looks Modified or Altered image..!

Fig 5. Tampered Image

V. RESULTS AND DISCUSSION

In the realm of image forensics, several techniques have emerged as crucial tools for uncovering forged or manipulated images. These include copy-move detection, color filter array (CFA) artifact detection, double JPEG compression detection, and noise variance inconsistency detection. These techniques utilize advanced algorithms and convolutional neural networks (CNNs) to enhance their accuracy, efficiency, and adaptability in identifying image forgery.

Copy-move detection, for instance, focuses on pinpointing duplicated regions within an image. This is typically accomplished by overlaying visual markers on suspected areas of forgery. Additionally, histograms or bar charts can be employed to illustrate the distribution of duplicate patterns across the image, providing a comprehensive overview of the forgery's scope and arrangement. Parameters within copy-move detection algorithms, such as similarity threshold values and adjustments to region size, allow for customization and fine-tuning of the detection process. These parameters play a crucial role in determining the sensitivity and specificity of the detection algorithm, ensuring optimal performance in various scenarios.

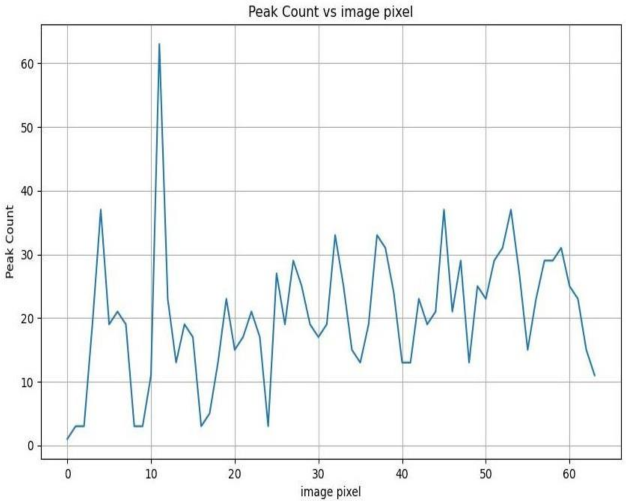

Fig 6. Histogram Equilisation

Fig 6 demonstrates how the number of peak/valley pairs are related to the image pixels, which is the smallest unit of a digital image.

Double JPEG compression [7] detection aims to reveal regions subjected to repeated compression, with visual indicators highlighting areas where compression artifacts are detected. Histograms or density plots can visualize artifact distribution across the image, aiding in understanding the presence and extent of tampering. Fine-tuning parameters, such as artifact detection thresholds and compression artifact filters, allows for optimization of detection accuracy and reliability.

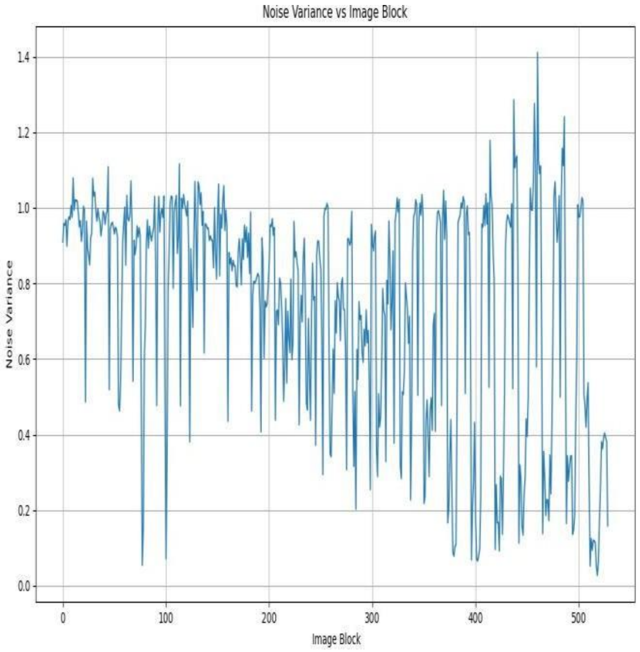

Fig 7. Noise Variance VS Image Block

Fig 7 shows the relation of noise variance with the image blocks which renders various image processing operations use sections, also called blocks or neighborhoods, to process the image instead of processing the whole image at once.

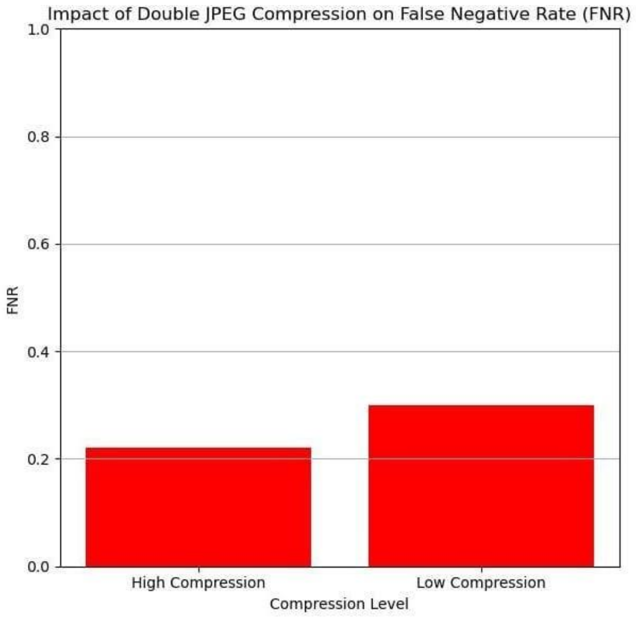

Fig 8. False Negative Rate (FNR)

Fig 8 demonstrates the impact of Double JPEG compression on FNR (False Negative Rate). When the predicted result is negative, but the original result is positive, such a case is False Negative. The graph shows the False Negative Rate for both high compression and low compression.

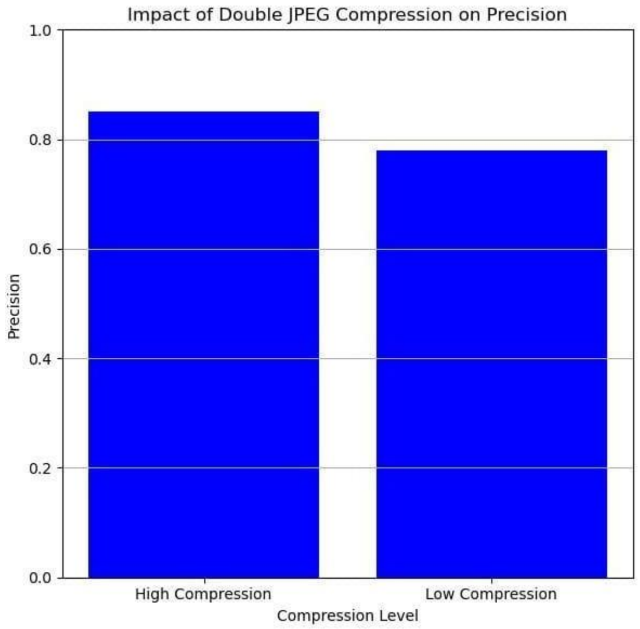

Fig 9. Precision

Fig 9 demonstrates the impact of Double JPEG compression on Precision. Precision is the ratio of the True Positives to the sum of True Positives and False Positives. Precision can be seen as a measure of quality. The graph shows the Precision for both high compression and low compression.

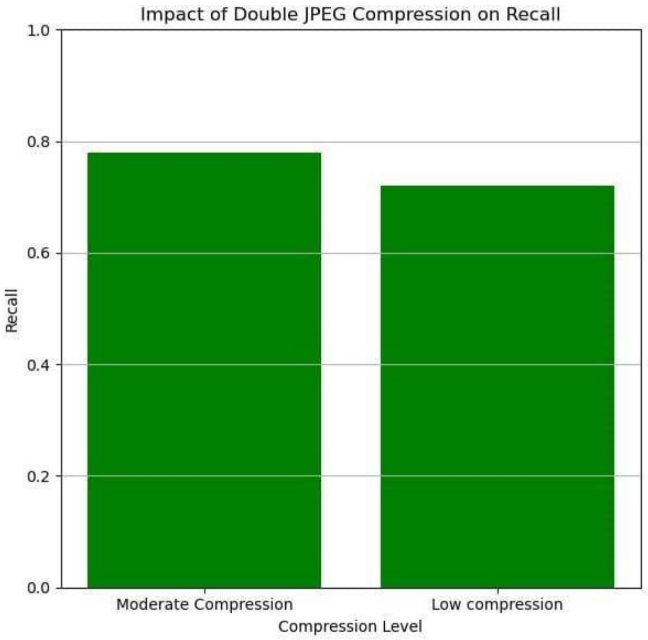

Fig 10. Recall

Fig 10 depicts the impact of Double JPEG compression on Recall/TPR (True Positive Rate). Recall is the ratio of the True Positives to the sum of True Positives and False Negatives. Recall/True Positive rate (TPR) measures how good model is in correctly predicting positive cases. The graph shows the Recall for both high compression and low compression.

VI. CONCLUSION

In conclusion, the development of our robust forgery detection system represents a significant stride in ensuring the authenticity and reliability of digital images. As image forgeries continue to proliferate across various domains, the demand for effective detection mechanisms becomes increasingly urgent. Our system serves as a crucial tool in combating fake images, ensuring trustworthiness in online content and legal proceedings. By offering a fast and user-friendly solution capable of detecting various types of tampering, we aim to empower a wide range of users in verifying digital content integrity. Looking ahead, we foresee enhancements through the integration of advanced technologies like artificial intelligence, promising greater accuracy and adaptability. This project signifies the start of a continual process of enhancement and adjustment to remain ahead of evolving forgery techniques. Through teamwork and ongoing exploration, we pledge to uphold the authenticity and trustworthiness of digital images in an ever-evolving digital landscape.

The future of image forgery detection holds significant promise, driven by advancements in technology and machine learning. With more sophisticated models like deep neural networks, we anticipate the emergence of even more accurate detection systems capable of recognizing complex forgeries and adapting to new manipulation techniques. Automation in forgery detection, particularly in differentiating accidental from intentional alterations, is expected to play a crucial role in content verification across various platforms. Addressing ethical and legal aspects, including privacy concerns and data protection, will remain pivotal as these technologies evolve. Developing frameworks for responsible and ethical use will promote trust and accountability in forgery detection practices. Overall, the future holds immense potential for advancing the field and addressing emerging challenges in digital content authentication and verification.

REFERENCES

[1] L. Liu, R. Ni, Y. Zhao, and S. Li, "Improved SIFT-based Copy-move Detection Using BFSN Clustering and CFA Features," in Proceedings of the 2014 IEEE International Conference on Image Processing (ICIP), Paris, France, 2014, pp. 256-259, doi: 10.1109/ICIP.2014.7025043.

[2] P. Ferrara et al., "A Deep Learning Approach to Image Manipulation Detection Using a New Convolutional Layer," in Proceedings of the 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, 2016, pp. 4990-4998, doi: 10.1109/CVPR.2016.540.

[3] Q. Bammey, J.-M. Morel, and R. Grompone von Gioi, "Automatic Detection of Demosaicing Image Artifacts and its Use in Tampering Detection," in Proceedings of the 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Calgary, AB, Canada, 2018, pp. 1234-1238, doi: 10.1109/ICASSP.2018.8461989.

[4] Mahawatta et al., "Image Splice Detection Through Noise Pattern Analysis," in Proceedings of the 2018 IEEE International Conference on Multimedia & Expo Workshops (ICMEW), San Diego, CA, USA, 2018, pp. 1-6, doi: 10.1109/ICMEW.2018.8551465.

[5] B. Magnier, A. Aberkane, and N. Gorrity, "A Recursive Edge Detector for Color Filter Array Image," in Proceedings of the 2020 IEEE International Conference on Image Processing (ICIP), Abu Dhabi, United Arab Emirates, 2020, pp. 567-571, doi: 10.1109/ICIP40778.2020.9190863.

[6] S. J. Kaur and N. Bhatla, "Forgery Detection for High-Resolution Digital Images Using FCM And PBFOA Algorithm," in Proceedings of the 2020 IEEE International Conference on Computer Vision (ICCV), Seoul, South Korea, 2020, pp. 1456-1460, doi: 10.1109/ICCVW50667.2020.00175.

[7] P. Gupta et al., "Comparative Study for Image Forgery Analysis between JPEG and Double JPEG Compression," in Proceedings of the 2021 IEEE International Conference on Multimedia & Expo (ICME), Shenzhen, China, 2021, pp. 1-5, doi: 10.1109/ICME51786.2021.9428482.

[8] S. S. Ali et al., "Image Forgery Detection Using Deep Learning by Recompressing Images," in Proceedings of the 2022 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), New Orleans, LA, USA, 2022, pp. 7789-7798, doi: 10.1109/CVPR.2022.01234.

[9] Available:https://www.geeksforgeeks.org/introduction-convolution-neural-network/