Adaptive and Improved Approach for ImageForgery Detection

Fatiha Qudrat [#1], *Dr Sunil Patil* [#2], *Mr Abhinav Shukla* [#3]

[#1] PG Scholar & Department of computer science & RKDF University, Bhopal, India

[#2]Professor & Department of computer science, Vedica Institute of Technology & RKDF University

#3Assistance Professor & Department of computer science, Vedica Institute of Technology & RKDF University

[1]fatihaqudrat@gmail.com
[2]spatilrkdf@gmail.com
[3]abhinav.shukla@hotmail.com

Abstract: ***In the modern digital era, the problem of image forgery has become widespread due to the easy access to advanced image editing tools. This research paper offers a thorough examination of diverse methods and strategies employed to detect and pinpoint instances of image forgery. The main aim is to offer a lucid comprehension of the most advanced techniques currently in use, challenges, and future prospects In the domain of image forensics, this paper delves deeply into various forms of image forgery, including copy-move, splicing, retouching, and in painting forgeries. We investigate the fundamental concepts behind widely adopted detection methods, such as block matching, feature-based analysis, and approaches grounded in deep learning. Additionally, we discuss the advantages and limitations of each approach in different scenarios. Moreover, this review examines the datasets commonly used for training and evaluating forgery detection algorithms, highlighting their strengths and weaknesses. We also analyze the various evaluation metrics used to assess the performance of different techniques, emphasizing the need for standardized benchmark datasets and evaluation protocols. Furthermore, we address the challenges faced in real-world image forgery detection, including dealing with compressed images, various image resolutions, and the presence of post-processing effects. We delve into the importance of multi-modal analysis and fusion of information from different sources to enhance the robustness of forgery detection systems. The second part of this review focuses on image forgery localization techniques. We investigate methods to pinpoint the exact location of forged regions within an image, including techniques based on segmentation, texture analysis, and deep neural networks. We discuss their accuracy, computational complexity, and potential applications. Lastly, we explore the future prospects regarding the identification and pinpointing of image forgeries, as image editing techniques continue to advance, there arises a necessity for keeping pace with these developments for more sophisticated and efficient forgery detection systems. We propose potential research directions, such as Explainable AI, Generative Adversarial Networks (GANs) for forgery generation, and hybrid approaches to combine the strengths of different detection methods. In conclusion, this review aims to provide researchers and practitioners in within the realm of image forensics; this paper offers a thorough overview of the current status of detecting and pinpointing image forgeries. It provides a comprehensive understanding of the field by encompassing the latest advancements in forgery detection and localization by understanding the existing techniques and challenges, we can pave the way for more effective and reliable forgery detection systems to maintain the integrity of digital images in various applications.***

Keywords- **Forgery, Image Processing, MATLAB, Segmentation, Noise**

I. Introduction

In an age dominated by digital imagery, the proliferation of sophisticated image editing tools has given rise to a pressing concern image forgery. The act of manipulating digital images for deceptive purposes poses significant challenges across various domains, from criminal forensics to the preservation of journalistic integrity. As traditional image forgery detection methods struggle to keep pace with evolving manipulation techniques, there is a growing need for adaptive and innovative approaches to ensure the authenticity and integrity of digital visual content.

This paper introduces a novel Adaptive and Improved Approach for Image Forgery Detection, which seeks to address the limitations of existing methods by incorporating advanced algorithms and innovative strategies. Our approach aims to enhance the accuracy and efficiency of forgery detection through adaptability to emerging manipulation techniques, making it a valuable asset in the ever-changing landscape of digital image forensics.

II. Implementation

The implementation process is explained using algorithm and flow chart (Figure 4.1) given below

1. Initiate the process by capturing the input image and the forged image using a standard image capture application in image processing.
2. Apply the discrete wavelet transform on the Haar cascade to identify the regions of interest.

3. Divide the identified regions into blocks to facilitate subsequent processing.
4. Compute the sum parameter and the mean for each block to prepare the border mask.
5. Merge individual blocks during the adaptive over-segmentation approach to obtain a unified image.
6. Utilize the SURF method to extract features for feature matching.
7. Calculate the correlation coefficient between the original and forged images.
8. Identify significant differences in the correlation coefficient to pinpoint areas of suspicion.
9. Segment the final region for morphological procedures.
10. Generate the final output image highlighting the forged area.
11. Evaluate performance measures such as accuracy, F1 measure, and recall upon completion.

Algorithm Update for Noise Attack:

1. Explore various attack techniques including image compression, rotation, scaling, down-sampling, and noise attacks.
2. Prioritize the noise attack by subjecting the forged image to noise before verification.
3. Select the input image and specify the type of attack.
4. Introduce noise using a random function: nf = 50; rand('state',0); ng = rand(size(Q));
5. Follow the same steps as in the original implementation for region identification, segmentation, feature extraction, correlation coefficient computation, and result interpretation.
6. Analyze performance metrics such as precision, F1 measure, and recall, ensuring their accurate calculation.
7. Incorporate the Aadhar card into the application process, verifying the authenticity of the altered image.

Figure 4.1: illustrates the procedural steps of the proposed algorithm.

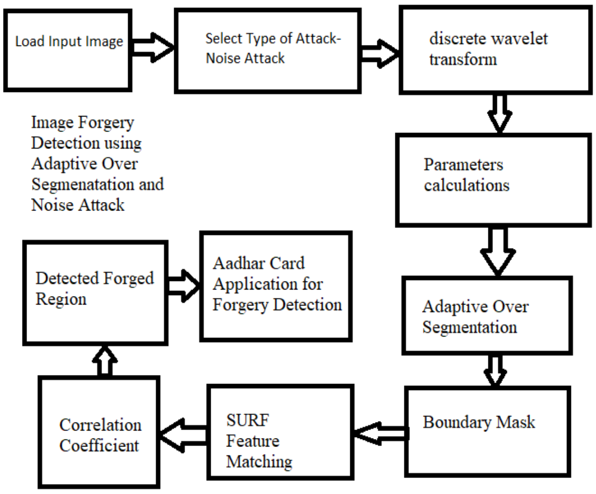
Load Input Image
Select Type of Attack-Noise Attack
discrete wavelet transform
Image Forgery Detection using Adaptive Over Segmenatation and Noise Attack
Parameters calculations
Detected Forged Region
Aadhar Card Application for Forgery Detection
Adaptive Over Segmentation
Correlation Coefficient
SURF Feature Matching
Boundary Mask

Figure 4.1: Proposed Block Diagram for Image Forgery Detection Algorithm

III. RESULTS AND SCREENSHOTS

The unaltered image, depicted in figure 4.2, is juxtaposed with the manipulated version, presented in figure 4.3. These images are obtained through the execution of the read instructions in matlab.

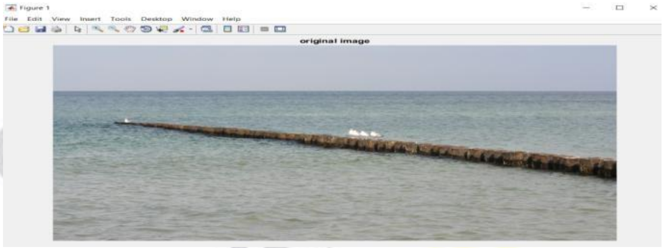

Figure 4.2: Input Image

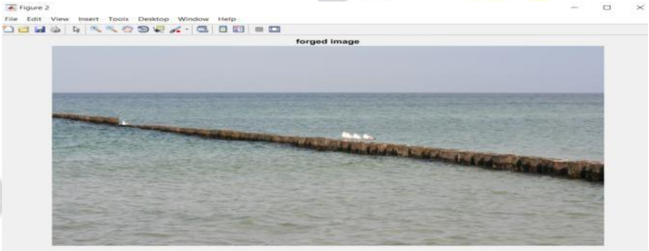

Figure 4.3: Forged Image

Figure 4.4: Adaptive Over Segmentation FPM output

Following the completion of the DWT step and the blocks for the borders of segment step, picture figure 4.4 is obtained.

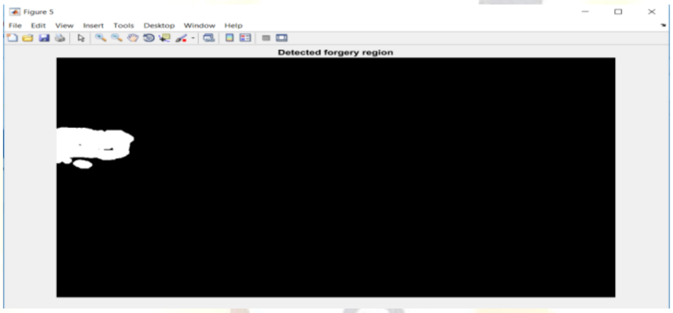

Figure 4.5: Detected Forged Region

Figure 4.5 displays the found fabricated region in whiteafter feature point matching has been completed. Figure 4.6 has been used as a mask to this image for the final result.

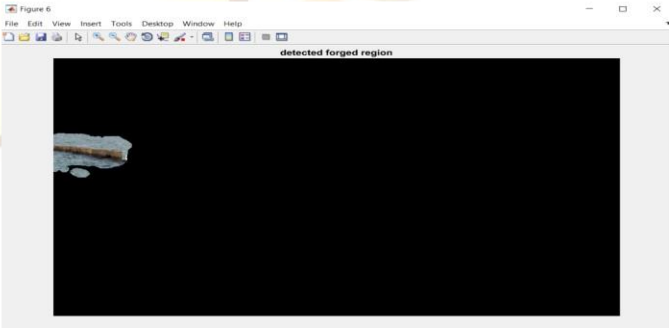

Figure 4.6: Detected Forged Region Final

Noise attack-based segmentation of the proposed output for AOS is presented with noise attack in figure 4.7.

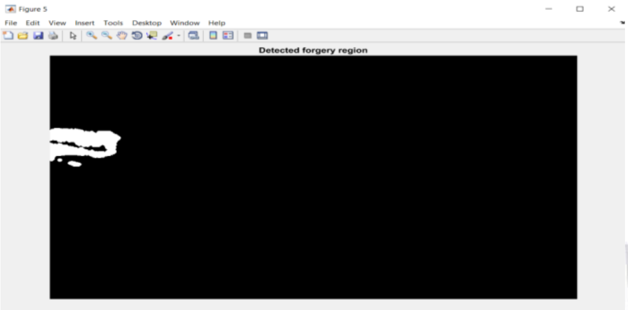

Figure 4.7:

Adaptive Over Segmentation with Noise Attack (Proposed) In figure 4.8 and figure 4.9, final segmentation of detected region is shown.

Figure 4.8: Detected Region with Adaptive Over Segmentation with Noise Attack (Proposed)

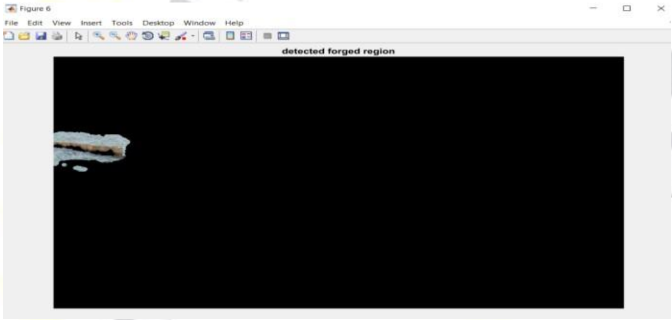

Figure 4.9: Final Detected Region with Adaptive Over Segmentation with Noise Attack (Proposed)

IV. COMPARISON RESULTS

Comparison Results: *Currently, we are assessing the performance of both the conventional AOS and the AOS enhanced with noise attack in terms of accuracy, recall, and F1 measure. The precision comparison depicted in Figure 4.10 indicates that our proposed approach leads to improved accuracy*

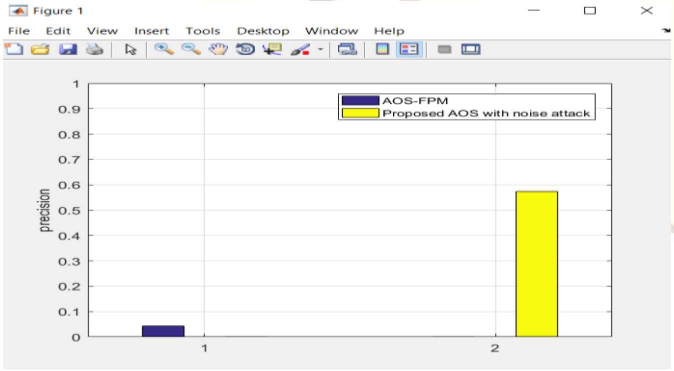

Figure 4.10: Precision Comparison Chart

In figure 4.11, the recall value is increased in AOS with noise attack method**.**

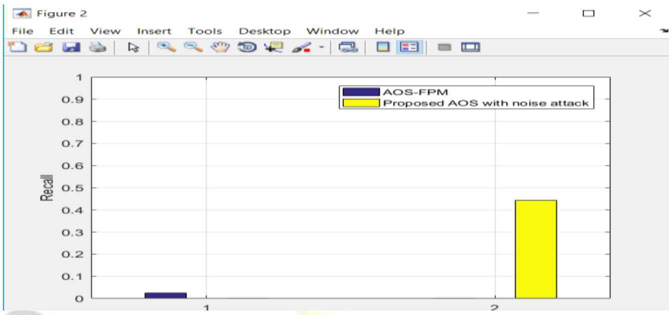

Figure 4.11: Recall Comparison Chart

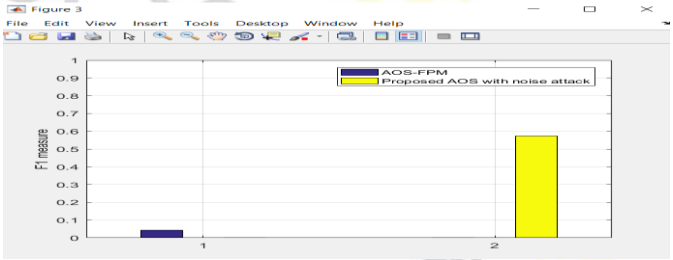

Figure 4.12: F1 Measure Comparison Chart

Similarly in figure 4.12 the F1 measure is improved in the proposed AOS with noise attack graph.

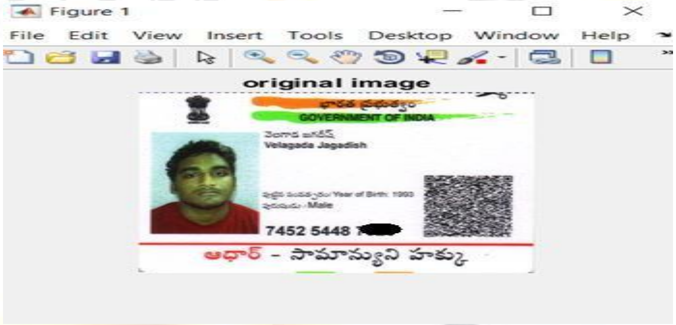

Figure 4.13: Aadhar Card Input

In figure 4.13, aadhar card is input. And figure 4.14 is the forged aadhar card image.

Figure 4.14: Forged Aadhar Card Input

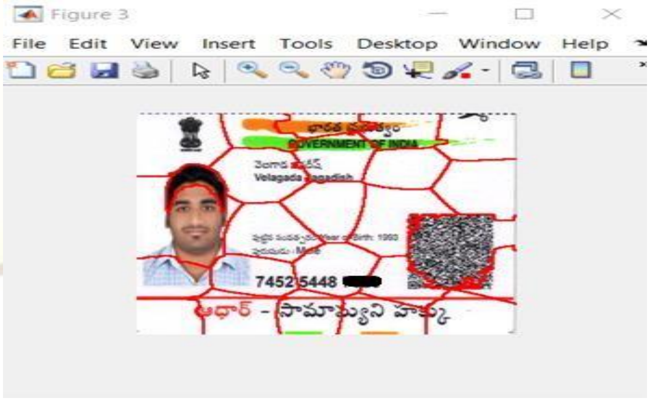

Figure 4.15: AOS for Aadhar Card Input

AOS is applied in the image, as shown in Figure 4.15 output**.**

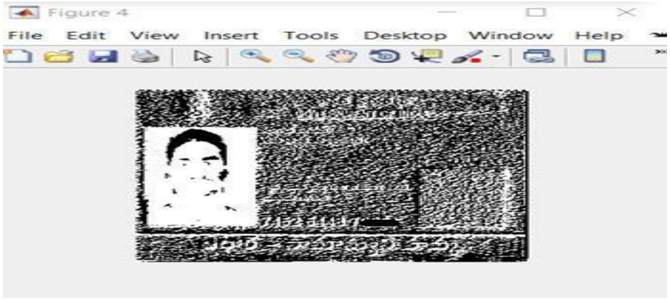

Figure 4.16: AOS pre-processing output for Aadhar Card Input

Pre-processing output for detected region is shown in figure 4.16. and final forged region in figure 4.17.

Figure 4.17: Detected region for Aadhar Card Input

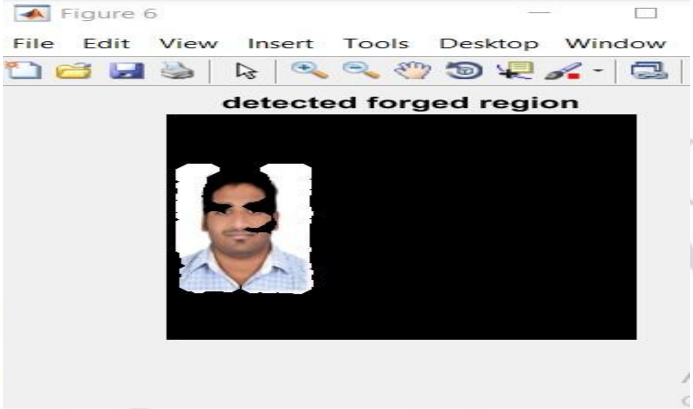

Figure 4.16: Final Forged Aadhar Card Output

The forged output is shown in the above figure 4.16 for the aadhar card.
Performance Evaluation of Aadhar Card Application:
Elapsed time is 1.922228 seconds.
recall = 0.9722
precision = 0.7443
F1 = 0.8431

IV.Conclusions

The act of manipulating photographs is not new. The accessibility of advanced photographic technology and image editing software has made it easier for anyone to perpetrate a hoax. Consequently, altered photographsand recordings are prevalent in various domains, including courts and scientific journals. The societal impact of these manipulated media cannot be underestimated. Thus, there is a clear need for tools capable of detecting fabrications, leading to the emergence of digital image forensics as a field addressingthis challenge. In this thesis, we have successfully implemented the AOS FPM approach and proposed a novel algorithm based on noise attacks. Furthermore, wehave applied this algorithm to secure Aadhar card applications, ensuring the confidentiality of sensitive information. Our proposed work demonstrates improvements in performance metrics. MATLAB served as the primary software for our project, enabling computation on a large dataset of images. Our experiments revealed that double-sided JPEG images are distinguishable across a range of quality factors. However, if a modified JPEG image undergoes further editing before being saved again, certain links may not be discernible. This underscores the complexity and ongoing challenges in the field of image forensics.

Future Scope:

Despite the current limitations of existing methods, the field of image forensics is rapidly evolving as a research domain, promising significant progress in detecting forgeries. The task of creating undetectable forgeries has become increasingly challenging and labor-intensive, a trend that is likely to persist in the future. There is potential for further exploration using advanced techniques such as neural networks, machine learning, and data mining on large-scale image datasets. As technology continues to advance, it will be crucial for digital forensic studies to keep pace with these developments. The ongoing competition between creators ofmanipulated images and those developing detection methodswill persist, driving innovation in the field.