

## Image Forgery Detection using Modified Adaptive Over-Segmentation and Feature Matching

Dr. Prashant Giridhar Shambharkar<sup>1</sup>, Manim Tirkey<sup>2</sup>, Sayan Sarkar<sup>3</sup>, Pankaj Kumar<sup>4</sup>

<sup>#</sup>Department of Computer Science and Engineering, Delhi Technological University, Delhi - 110042, India

<sup>1</sup>prashant.shambharkar@dtu.ac.in

<sup>2</sup>manimtirkey2000@gmail.com

<sup>3</sup>sayan.sarkar56537@gmail.com

<sup>4</sup>shahpankaj213@gmail.com

### Abstract

*With the emergence of digitisation of Visual Graphics it has been a constant need to extract typical features of Images. Forgery, on the other hand, is not something new to the world of Computer Graphics. In the past it was restricted to craftsmanship and writing and it didn't affect human civilisation rather it was seen as an art for a few centuries. But, with the advent of the technology it has been noticed that by the use of computerised picture handling softwares and altering devices a picture can be easily changed and controlled. It is notably done nowadays to falsify and spread certain narratives through the Media and on the Internet. These alterations show that even graphical information is as vulnerable as any other information, questioning the credibility of digital images. This work is an improvement of an already existing Adaptive Over-Segmentation technique which has recently been used to detect forgery of a digital image by introducing a new feature of detection of forgery even if noise was introduced to the forged copy of the original image.*

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

### I. INTRODUCTION

Recently, Image Processing Analysts have shifted their focus on the topic of advanced image forgery. A well known change that forgers do is a copy move fraud[1] in a digital image. Fraudsters who make such imagery have been seen to add certain transformations on the forged image to make it more different from the original image with methods like scaling, straining, clouding and prolongation. Other than these, adding noise has been seen as a stronger alternative to avoid being detected by today's algorithms. In previous decades we have discovered two main types of estimates to detect forgery: Square counts [1-13] and the central problem based estimates [14-19].

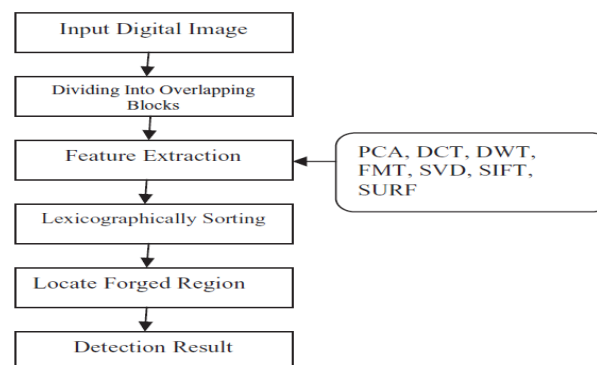


Fig. 1 Flow Chart for Image Forgery Detection

Figure 1 depicts the primary flow for the process of duplicating and transferring a picture forgery recognition system. The very first step is to recognise an image as its information, and that image must be of advanced kind. The picture must be separated into certain covering squares before it can be further prepared in the system. The following stage is to distinguish the major and main highlights of the picture by using different techniques, for example, PCA, DCT, DWT, FMT, SVD, SIFT, SURF. Following the extraction of an image's highlights, the image is organised with the assistance of lexicographical technique. Now, the framework will look for the manufactured location in the picture. Furthermore, the final step is to separate and take all of the consequences from the system.

The computerised grafting of at least two photographs into a single composite is a common form of photographic control. When done carefully, the outskirts between the joined districts may be indistinguishable from the outside. However, the researchers demonstrate that grafting disrupts higher-request Fourier measurements, which can thus be used to recognise joining. The majority of cameras encode images in the JPEG format. This lossy pressure plot accounts for some adaptability in the amount of pressure achieved. Manufacturers typically produce their products in a variety of ways in order to tailor pressure and cost to their specific demands and preferences. As seen, this distinction can be used to identify the source (camera make/model) of a picture. We duplicate a move forgery recognition plot in this proposed project by utilising versatile over-division and highlight point coordinating. The editor used for tampering with the AADHAR card image was Adobe Photoshop.

## II. IMAGE FORGERY DETECTION

Image forgery has been a problem since the advent of conventional photography in the nineteenth century, but it is a substantially more prevalent concern in the advanced era. The only problem is that photographs are often used as firm evidence of an event and are often regarded as truthful and dependable by the general public. Images that are created, thereby betraying this confidence, may have far-reaching social consequences. CCTV videos, for example, are often used in a trial to provide strong evidence, either by the defence or by the arraignment. If the jury's trust in these images is called into question, and they are unable to place their full trust in them, the preliminary is declared a failure. Recognising influence and forgery within these pictures is also important. In addition, fashioned photographs are widely used in the mainstream, either deliberately or accidentally. Newspapers, websites, and showcasing efforts regularly alter photographs of models or celebrated figures to make them seem more stylishly appealing to the viewer. This may be as simple as adding a channel or adjusting the image's separation, but it is often considerably more extraordinary; increased muscle definition, more conditioned body parts, and wrinkle expulsion are examples of often achieved outcomes.

The issue has become so prevalent and well-known that the action word "photoshopped," which refers to the well-known image editing software Adobe Photoshop, has become a neologism for controlling and changing advanced images. One of the most significant issues that must be resolved is the fact that there are many techniques for modifying an image, and due to the perplexing existence of computerised images, it is impossible to devise a measurement that distinguishes each type of image forgery. As a result, image forgery recognition isn't widely used in the professional community. The secret concept can be extremely useful in most expert fields that handle photographs on a daily basis, where the unwavering accuracy and authenticity of these images is critical. Furthermore, with the massive increase in the use of online life, people will greatly benefit from having the ability to recognise phonies within photographs. Convincingly managed images are typically flowed through web-based networking media stages [17] and can be easily distributed within networks that trust them to be valid.

To discern these image fabrications, we must see certain commonplace methods used to control photographs. There are few examples:

- Duplicate glue Cloning - This is the process of cloning established territory within a picture, allowing regions to be protected or objects to be copied. This is a commonly used tactic since the frauds which seem convincing due to the fact that they have come from the source picture regardless.
- Photo Splicing - The process of joining objects from another image to the source image, including objects that were not present in the first image.

There are various mixing strategies available, such as obscuring edges, reducing separation, and using cloning to help camouflage the new article in with the surrounding territory.

- Modification in existing regions - This is similar to duplicate glue copying, except instead of being a precise replica, existing districts are modified to meet the requirements of the forgery. This may include simply resizing the post, representing or slanting it, or connecting two existing objects. In any case, the copied locale has been resampled, meaning that it has modified enough not to be detected by any clone discovery measurement. Although existing tasks have chipped away at the correlation of image forgery detection methods, they are often limited in complexity and only investigate variants of a similar calculation on images that are specifically created for that type of strategy. JPEG Analysis and Edge Detection, for example, have been investigated; however, little clarification is provided as to why these specific applications were chosen over others, as these would in principle detect comparative types of fraud.

Furthermore, no information about the images used in the investigation is provided; for example, it is unclear if they are normal library images or images customised for this type of forgery detection measurement. Similarly, prior image forgery detection applications are often of a scholarly type (confirmation of concept or model quality) or extremely simple. Looking for forgery recognition increases academic papers on the topic, but the most downloaded results on the popular open-source website SourceForge return truly insignificant applications that only identify metadata labels built within photos [2][3][4]. While this is a useful metric, and something that will be attempted regardless of the fundamental calculations within our execution, metadata labels are largely evacuated or monitored, and it is therefore not a precise proportion of whether a picture has been made or not. Despite the fact that the usage of this project is mostly a proof of concept and is mainly used for research purposes, it is a starting point that could be developed into a full-fledged programme. Making a tidy, simple GUI for the chosen measurement is then truly minor, bringing the kind of forgery position to the mass market.

We used the same database as used in [31] for the proposed method. The dataset is made up of 48 images which are high-resolution, uncompressed PNG true colour images with average sizes of 1500×1500. The dataset contains smooth and high texture images and there are varied copied regions from a categorisation of living, nature, man-made and mixed. Copy move forgeries are commonly made from rotating or scaling connotatively meaningful regions of the image making very life-like image forgeries. So, we objectively chose this dataset for evaluation.

In this Copy Move Forgery Detection Algorithm, we first suggest the AOS calculation, which is nearly the same as square-based forgery detection algorithm which divides the original input into squares. Many square-based forgery identification equations have been proposed in previous years. The host picture was usually divided into covering regular squares in the new square-based forgery recognition conspires, with the square size previously characterised and set. The forgery areas were identified at that time by coordinating such squares. As a result, the known areas are only made of ordinary squares, which can't speak to the exact forgery locale well; as a result, the review rate of the square-based techniques is always exceedingly limited. Furthermore, as the scale of the input image or host image grows, the measurement of the covering squares becomes considerably cost ineffective. To

resolve these problems, we suggested the AOD (Adaptive Over-Division) technique, which fragments the input image into non-covering areas of periodic square images; subsequently the forged areas can be separated by organising certain non-covering and volatile locales.

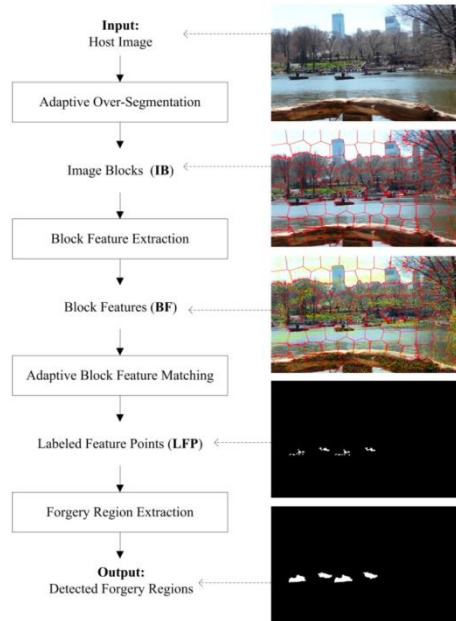


Fig. 2. Flowchart explaining the Copy Move Forgery Detection Algorithm

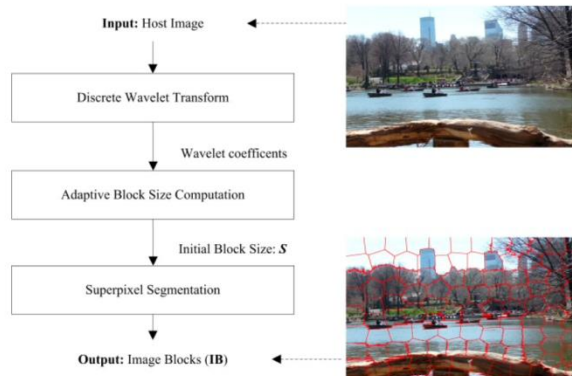


Fig. 3. Flowchart explaining Adaptive Over-Segmentation Algorithm

We used the straightforward direct iterative sorting (SLIC) calculation [23] to segment the host image into significant sporadic super pixels, as individual squares, because we needed to partition the host image into non-covering districts of erratic form and because the super pixels are perceptually significant nuclear locales that can be obtained by over-division. The SLIC computation employs a k-means grouping method to proficiently generate the super pixels, and it adheres to the constraints very well. Figure 3 depicts various blocking/division tactics, including (a) covering and rectangular blocking, (b) covering and circular blocking, and (c) non-covering and intermittent blocking with the newer division technique. The newer SLIC division technique reduces the computational costs as compared to covering blocking; additionally, the volatile and important locales can generally speak to the forgery district better than the ordinary squares. Regardless, the underlying scale of the super pixels in SLIC is difficult to choose.

TABLE I  
BRIEF COMPARISON OF KEYPOINT AND BLOCK BASED DESCRIPTORS

| S.No. | Keypoint based Descriptors  | Block based Descriptors  |
|-------|---|--|
| 1     | Uses local image gradients to describe each keypoint region   | Uses partitioning of an image into overlapping or non-overlapping blocks                 |
| 2     | A feature vector is created around the keypoint   | Following the partitioning a feature extraction is done in each block or pairs of blocks |
| 3     | These descriptors have less computational cost as compared to block based descriptors   | Due to robust extraction processes it has higher computational cost                      |
| 4     | It is useful for partitioning an image into corner or isolated focuses to provide nearby highlights representation of the image | The adjacent block features based on their similarities are used to detect forgery       |

### III. IMPLEMENTATION

Firstly, the feature point matching technique is used to apply adaptive over segmentation. Following that, as suggested in the work, a noise attack is applied to the adaptive over segmentation strategy. Aadhar card image forgery identification is applied as an extension to this work. The results are compared based on the F1 scale, recall, and precision.

The implementation method is explained using algorithm and flow chart (Figure 4) given below:

- Initially, the input image to be checked and forged image is obtained using basic image acquisition software in image processing.
- Using the discrete wavelet transform on the haar cascade to determine the field of interest
- Using red colouring, the areas are divided into blocks for segmentation.
- For the preparation of the boundary mask, the sum parameter and mean are determined.
- At this point, the adaptive over segmentation technique is used to merge and display the blocks into a single image.
- The SURF process is used to calculate characteristics for the feature matching technique.
- The correlation coefficient between the original and the forged image is computed.
- The area or location where the correlation coefficient demonstrates a disparity.
- The morphological operations (i.e. erosion) remove the final area through the segmentation process.
- The detected forged area is seen in the final output picture.
- Quality measures such as accuracy, F1 measure, and recall have been measured.

Work-proposed algorithm modification for noise attack

- Some threats, such as image compression, rotation, noise, scaling, and down sampling, can be investigated. The most common of these is the noise attack, in which a forged image is subjected to noise and then observed.
- After selecting the input image, the method of attack is selected.
- Noise generation with the random function below; `nf=50; rand('state',0); ng=rand(size(Q));`
- Using the discrete wavelet transform on the haar cascade to determine the field of interest
- Using red colouring, the areas are divided into blocks for segmentation.
- For the preparation of the boundary mask, the sum parameter and mean are determined.

- At this point, the adaptive over segmentation technique is used to merge and display the blocks into a single image.
- The SURF process is used to calculate characteristics for the feature matching technique.
- The correlation coefficient between the original and the forged image is computed.
- The area or location where the correlation coefficient demonstrates a disparity.
- The morphological operations (i.e. erosion) remove the final area through the segmentation process.
- The detected forged area is seen in the final output picture.
- Quality measures such as accuracy, F1 measure, and recall have been measured.
- The aadhar card is taken as an application, forged by changing the photograph, and then checked using software.

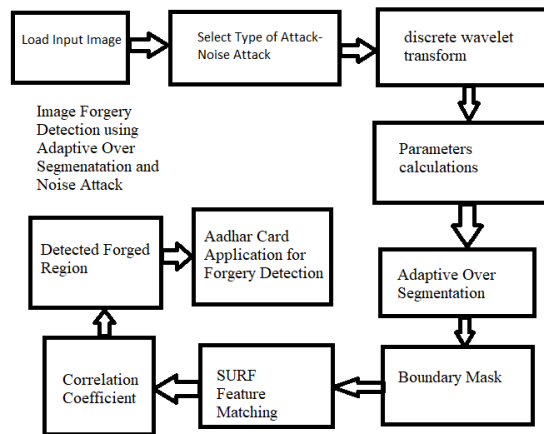


Fig. 4. Proposed Block Diagram for Image Forgery Detection Algorithm

Wavelet transformations are performed on the image to extract distinct features and represent a digital image in a reduced amount of data; our purpose is fulfilled by the former usage. DWT is used over DCT (discrete cosine transform), which is also a common image compression transform, so as to perform better in case of high pass bands for providing fewer sub-bands and superior spatial resolution. Also, in DCT the reconstructed image has lower edge quality. So, DWT is preferred over DCT. SURF is used to calculate the characteristics of feature matching techniques as mentioned in the algorithm. It is used over a commonly used algorithm called the Scale Invariant Feature Transform (SIFT). The most basic reason for following a SURF based transformation is that the descriptor vector for a  $4 \times 4$  region has a length of 64 whereas it is the double in case of SIFT which proves that SURF is faster than SIFT. The combination of both DWT and SURF thus results in superior spatial resolution and a faster transform for feature matching.

#### IV. EXPERIMENTAL RESULT

Figure 5 and 6, are the input image and forged image. This is input from MATLAB read commands. After performing the steps of DWT and blocks for boundaries of segment, image figure 7 is achieved. After feature point matching figure 8 has the detected forged region in white. This image is masked to figure 9 for final output. In figure 10, noise attack based segmentation of proposed output for AOS is shown with noise attack. In figure 11 and figure 12, final segmentation of the detected region is shown.

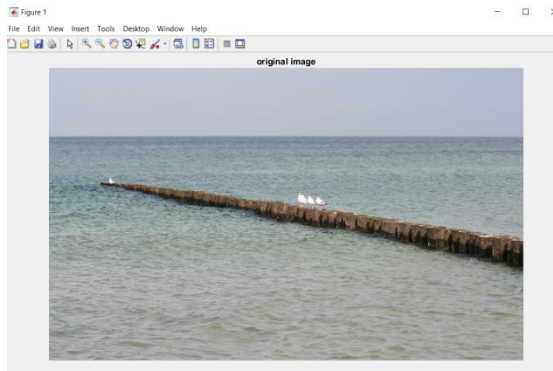


Fig. 5. Input Image

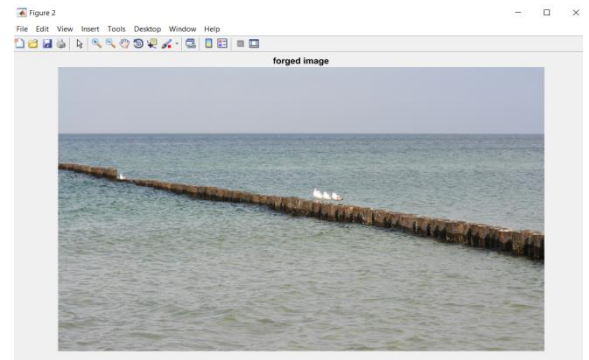


Fig. 6. Forged Image

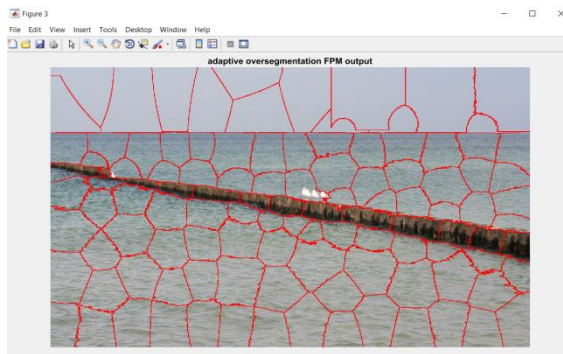


Fig. 7. Adaptive Over Segmentation FPM Output

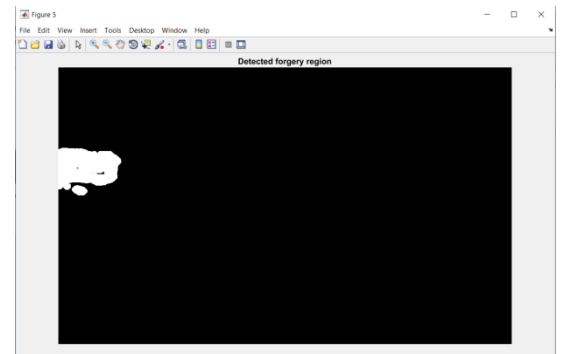


Fig. 8. Detected Forged Region

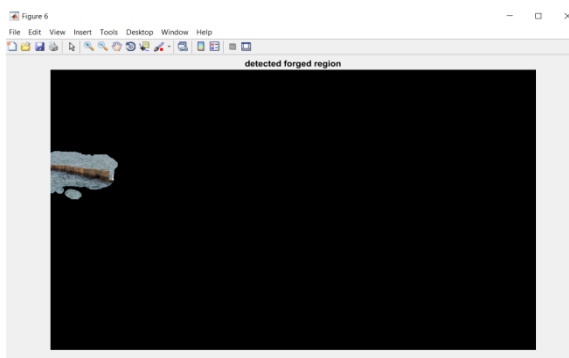


Fig. 9. Detected Forged Region Final

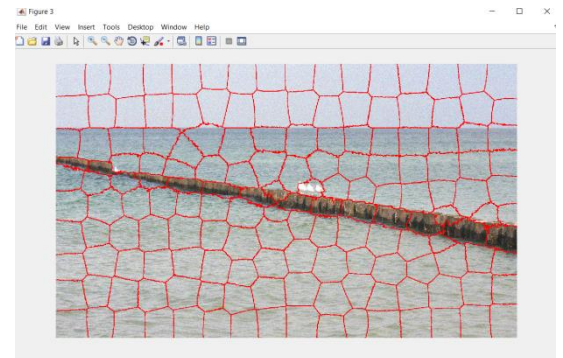


Fig. 10. Adaptive Over Segmentation with Noise Attack  
(Proposed)

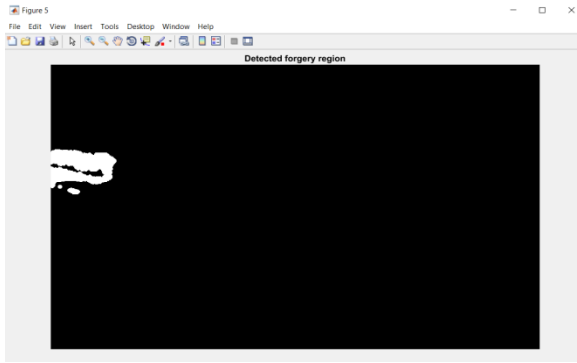


Fig. 11. Detected Region with Adaptive Over Segmentation with Noise Attack (Proposed)

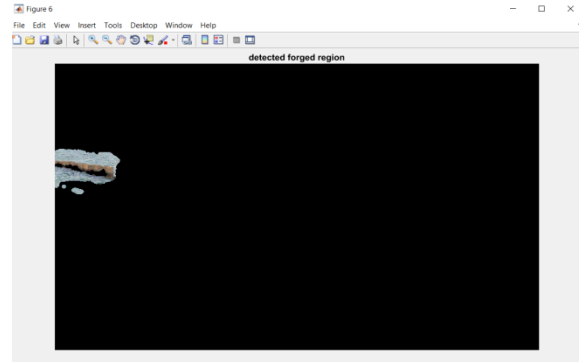


Fig. 12. Final Detected Region with Adaptive Over Segmentation with Noise Attack (Proposed)

#### V. COMPARISON RESULTS AND PRACTICAL APPLICATION OF PROPOSED WORK

Now, the simple AOS and noise attack based AOS is compared on the basis of precision, recall and F1 measure. In figure 13, precision comparison shows that for proposed work precision is increased. In figure 14, the recall value is increased in AOS with noise attack method. Similarly in figure 15 the F1 measure is improved in the proposed AOS with noise attack graph. In figure 16, aadhar card is input. And figure 17 is the forged aadhar card image. AOS is applied in the image, as shown in Figure 18 output. Pre-processing output for the detected region is shown in figure 19. and final forged region in figure 20. The forged output is shown in the figure 21 for the aadhar card.

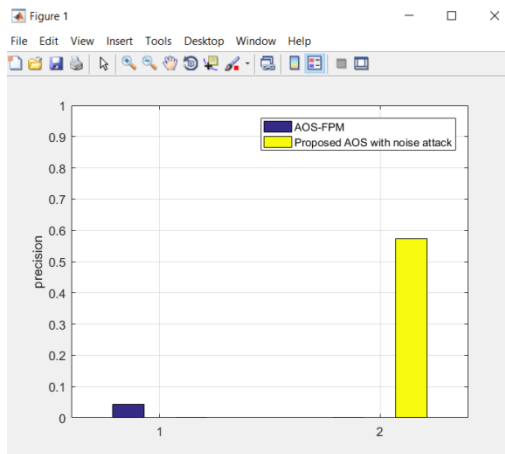


Fig. 13. Precision Comparison Chart

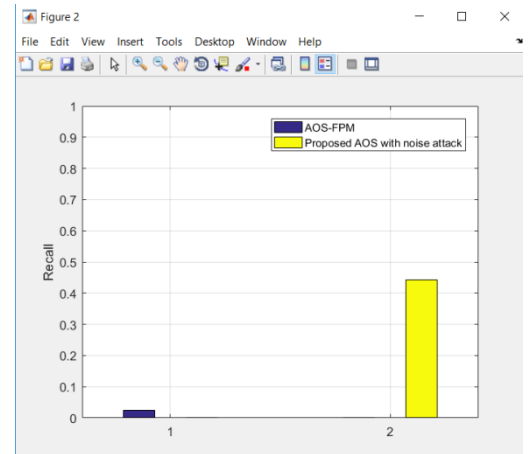


Fig. 14. Recall Comparison Chart

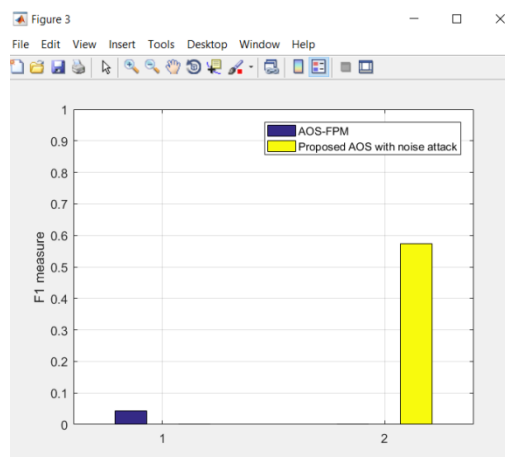


Fig. 15. F1 Measure Comparison Chart

TABLE II  
COMPARISON WITH EXISTING AND PROPOSED WORK

| S. No. | Comparison Parameters                       | Percentage |
|--------|---|------------|
| 1      | Precision in AOS-FPM                        | 5.6 %      |
| 2      | Precision in proposed AOS with noise attack | 57 %       |
| 3      | Recall in AOS-FPM                           | 4.1 %      |
| 4      | Recall in proposed AOS with noise attack    | 44 %       |
| 5      | F1 measure in AOS-FPM                       | 5.2 %      |

|   |  |      |
|---|--|------|
| 6 | F1 measure in proposed AOS with noise attack | 58 % |
|---|--|------|



Fig. 16. Aadhar Card Input

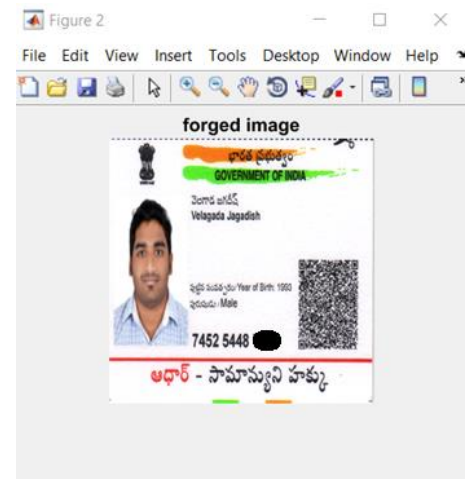


Fig. 17. Forged Aadhar Card Input

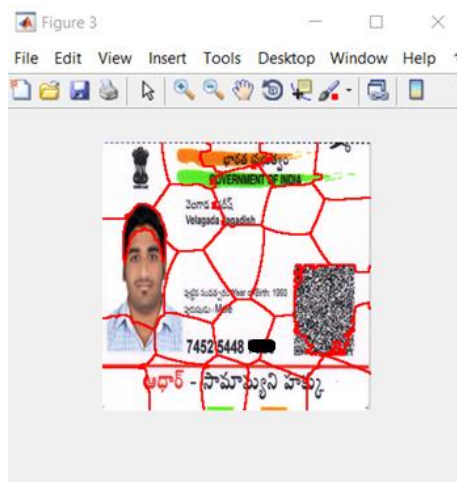


Fig. 18. AOS for Aadhar Card Input

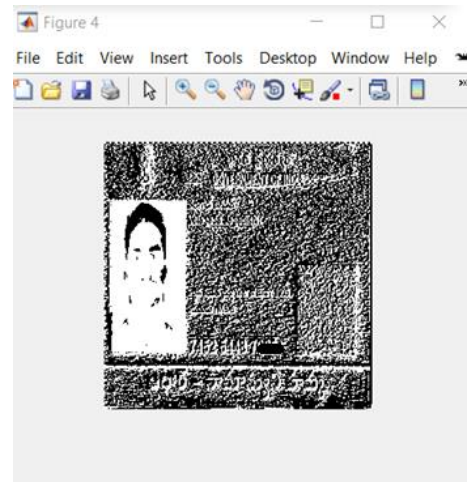


Fig. 19. AOS pre-processing output for Aadhar Card Input

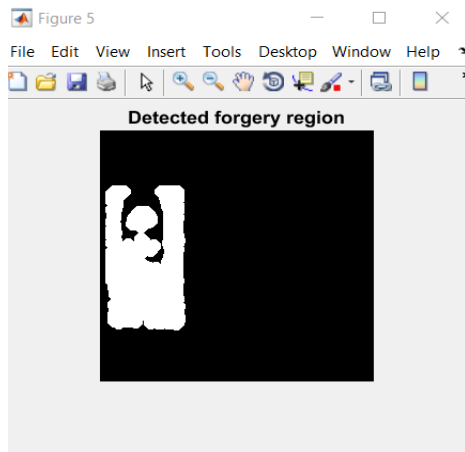


Fig. 20. Detected Region for Aadhar Card Input

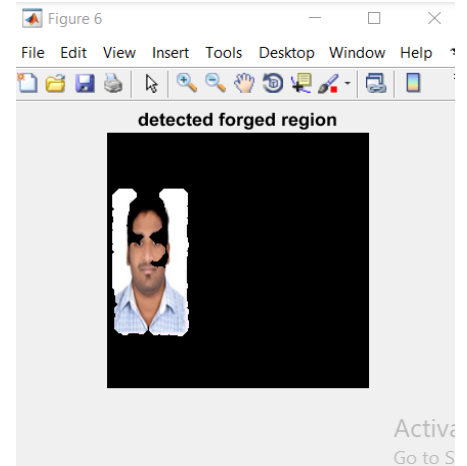


Fig. 21. Final forged Aadhar Card Output

#### Performance Evaluation of Aadhar Card Application:

Elapsed time is 1.922228 seconds.

recall=0.9722

precision=0.7443

F1 = 0.8431

## VI. CONCLUSION AND FUTURE SCOPE

### A. Conclusion

Changing images isn't a novel concept. The availability of advanced photo engineering and picture preparing software makes it possible for someone to commit a scam. As one would imagine, distorted images and videos are appearing everywhere, from trials to newspapers, and these images have the potential to deeply influence culture. There is an undeniable need for instruments that can detect forgeries, and the field of computerised picture crime scene investigation has risen to address this issue with no prerequisites. This thesis successfully implements the AOS FPM technique and proposes a noise attack based algorithm, which is also applied to the Aadhar card framework for information security. In addition, the proposed study improves the output metrics. The programme used for this work is MATLAB. The only kind of input that the programme currently takes is in JPEG format. The calculation was tested on a large number of images and discovered that a twofold JPEG image is recognisable for a wide range of value factors. However, if a modified JPEG image is changed before re-sparing, the links depicted are not shown.

### B. Future Scope

Picture criminology is a flourishing research area that, despite the limitations of current methods, promises significant advancement in fake venues. It has made and will continue to make it more difficult and time- consuming to create an untraceable falsification. More methods, such as neural networks, artificial learning, and data mining techniques, will be used for large-scale image processing in the future. If creativity advances, it will become increasingly important for the study of computerised legal sciences to keep up, and the never- ending competition between picture fabrication makers and picture fake finders will continue.

REFERENCES

- [1] Chi-Man Pun, Xiao-Chen Yuan, Xiu-Li Bi, “*Image Forgery Detection Using Adaptive Over-Segmentation and Feature Point Matching*” 1556-6013 (c) 2015 IEEE.
- [2] Mohd Dilshad Ansari, S. P. Ghrera & Vipin Tyagi, “*Pixel-Based Image Forgery Detection*” IETE JOURNAL OF EDUCATION | VOL 55 | NO 1 | JAN\_JUN 2014.
- [3] Payal Srivastava, Manoj Kumar, Vikas Deep, Purushottam Sharma, “*A Technique to Detect Copy-Move Forgery using Enhanced SURF*” International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8, Issue-6S August 2019
- [4] Tajuddin Manhar Mohammed, Jason Bunk, Lakshmanan Nataraj, Jawadul H. Bappy, Arjuna Flenner<sup>3</sup>, B.S. Manjunath, Shivkumar Chandrasekaran, Amit K. Roy-Chowdhury, and Lawrence A. Peterson, “*Boosting Image Forgery Detection using Resampling Features and Copy-move Analysis*” IS&T International Symposium on Electronic Imaging 2018 Media Watermarking, Security, and Forensics 2018
- [5] Yue Wu, Wael Abd-Almageed, and Prem Natarajan, “*Detecting Copy-Move Image Forgery with Source/Target Localization*” EECV 2018
- [6] Hany Farid, “*Image Forgery Detection*” 1053-5888/09/\$25.00©2009IEEE
- [7] Ankit Kumar Jaiswal, Rajeev Srivastava, “*A technique for image splicing detection using hybrid feature set*” # Springer Science+Business Media, LLC, part of Springer Nature 2020
- [8] Tulsi Thakur, Kavita Singh, Arun Yadav, “*Blind Approach for Digital Image Forgery Detection*” International Journal of Computer Applications (0975 – 8887) Volume 179 – No.10, January 2018
- [9] Abhishek Kashyap, Rajesh Singh Parmar, Megha Agarwal, Hariom Gupta, arXiv:1703.09968v2 [cs.MM] 30 Mar 2017
- [10] Bo Liu, Chi-Man Pun, and Xiao-Chen Yuan, “*Digital Image Forgery Detection Using JPEG Features and Local Noise Discrepancies*” Hindawi Publishing Corporation Scientific World Journal Volume 2014, Article ID 230425
- [11] Parul Sharma, Harpreet Kaur, “*Copy-Move Forgery Detection with GLCM and Euclidian Distance Technique in Image Processing*” International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue- 1C2, May 2019
- [12] Navneet Kaur, Navdeep Kanwal, “*Image Forgery Detection Technique for Digital Images*” International Journal of Advanced Research in Computer Science May – June 2017
- [13] Johan Hagelbäck, “*Hybrid Pathfinding in StarCraft*” IEEE TRANSACTIONS ON COMPUTATIONAL INTELLIGENCE AND AI IN GAMES, VOL. 8, NO. 4, DECEMBER 2016
- [14] Owen Mayer, Matthew C. Stamm, “*Accurate and Efficient Image Forgery Detection Using Lateral Chromatic Aberration*” 1556-6013 (c) 2018 IEEE
- [15] M. Ali Qureshi, M.Deriche, “*Copy Move Image Forgery Detection Technique*” 978-1-4799-3866-7/14/\$31.00 ©2014 IEEE

- [16] Chunhe Song, Peng Zeng, Zhongfeng Wang, Tong Li, Lin Qiao, Li Shen, “*Image Forgery Detection Based on Motion Blur Estimated Using Convolutional Neural Network*” 1558-1748 (c) 2019 IEEE
- [17] Kanagavalli.N, Latha.L, “*Copy-Move Image Forgery Detection Techniques*” International Conference on Inventive Systems and Control (ICISC-2017)
- [18] Mohanad Fadhil Jwaid, Prof. Trupti N. Baraskar, “*Study and Analysis of Copy-Move & Splicing Image Forgery Detection Techniques*” International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2017)
- [19] Viktor Tuba, Raka Jovanovic, Milan Tuba, “*Digital Image Forgery Detection Based on Shadow HSV Inconsistency*” 978-1-5090-5835-8/17/\$31.00 c 2017 IEEE
- [20] Ms. Jayshri Charpe, Ms. Antara Bhattacharya, “*Revealing Image Forgery through Image Manipulation Detection*” Proceedings of 2015 Global Conference on Communication Technologies (GCCT 2015)
- [21] Youssef William, Sherine Safwat, Mohammed A.-M. Salem, “*Robust Image Forgery Detection Using Point Feature Analysis*” Proceedings of the Federated Conference on Computer Science and Information Systems pp. 373–380 DOI: 10.15439/2019F227 ISSN 2300-5963 ACSIS, Vol. 18 IEEE Catalog
- [22] Mohammed N. Nazli, “*COMPARISON BETWEEN IMAGE FORGERY DETECTION ALGORITHMS*” 2017 8th International Conference on Information Technology (ICIT)
- [23] Beste Üstübioğlu, Vasif Nabiyev, Guzin Ulutas, and Mustafa Ulutas, “*Image Forgery Detection Using Colour Moments*” 978-1-4799-8498-5/15/\$31.00 ©2015 IEEE
- [24] Yong Yew Yeap, U. U. Sheikh, Ab Al-Hadi Ab Rahman, “*Image Forensic for Digital Image Copy Move Forgery Detection*” 2018 IEEE 14th International Colloquium on Signal Processing & its Applications (CSPA 2018)
- [25] Charmil Nitin Bharti, Purvi Tandel, “*A Survey of Image Forgery Detection Techniques*” IEEE WiSPNET 2016 conference.
- [26] Tu K.Huynh, Thuong Le-Tien, Khoa V.Huynh, Sy C.Nguyen, “*A Survey on Image Forgery Detection Techniques*” 2015 IEEE RIVF
- [27] H.B.Kekre, Dharendra Mishra, Pallavi N. Halarnkar, Prajakta Shende, and Sukriti Gupta, “*Digital Image Forgery Detection using Image Hashing*” Manuscript received September 25, 2012
- [28] Mr.Arun Anoop M, “*Image forgery and its detection*” IEEE Sponsored 2J/d International Conference on Innovations in Information, Embedded and Communication systems (ICIIECS)2015
- [29] Navpreet Kaur Gill, Ruhi Garg, Er.Amit Doegar, “*A Review Paper on Digital Image Forgery Detection Techniques*” 8th ICCCNT 2017 July 3-5, 2017, IIT Delhi, India
- [30] Payal Srivastava, Manoj Kumar, Vikas Deep, Purushottam Sharma, “*A Technique to Detect Copy-Move Forgery using Enhanced SURF*” International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8, Issue-6S August 2019

- [31] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "*An Evaluation of Popular Copy-Move Forgery Detection Approaches*," Ieee Transactions on Information Forensics and Security, vol. 7, pp. 1841-1854, Dec 2012.