Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 9, Issue. 7, July 2020, pg.33 – 42

Image Forgery Detection with Modified Adaptive Over Segmentation Technique and Noise Attacks

Sadia Zahra[1]; Mohd. Sadim[2]
[1]Department of Computer Science & AFU, India
[2]Department of Computer Science & AFU, India
[1] zahrasadiasonu@gmail.com; [2] sadim4u@gmail.com

Abstract— With the advancement of PC innovation and picture preparing programming, computerized picture imitation has been progressively simple to perform. In any case, advanced pictures are a well-known wellspring of data, and the dependability of computerized pictures is in this manner turning into a significant issue. Image forgery is current research trends as forgery may lead to bad consequences like misuse of someone's information and cheating frauds. It is important to prevent any kind of forgery of bank documents, pictures or any certificates. In this paper, study and implementation of a new image forgery detection technique is done. The technique proposed is inspired from the existing feature matching and adaptive over segmentation technique, under which noise attack is performed and also improved the performance parameters such as precision, recall and F1 measure values are much near 1 than the existing one technique. Further, a new application of this technique is tested on real Aadhar card for image forgery detection which will be useful for the detection any forgery in the Aadhar card of a person.

Keywords— Forgery, Image Processing, MATLAB, Segmentation, Noise

I. INTRODUCTION

As of late, an ever-increasing number of analysts have started to concentrate on the issue of advanced image altering. Of the current sorts of image altering, a typical control of a computerized image is duplicate move forgery [1], which is to glue one or a few replicated region(s) of an image into different part(s) of a similar image. During the duplicate and move activities, some image preparing strategies, for example, revolution, scaling, obscuring, pressure, and commotion expansion are infrequently applied to make persuading phonies. [2] Since the duplicate and move parts are replicated from a similar image, the CLAMOUR segment, shading character and other significant properties are perfect with the rest of the image; a portion of the forgery recognition techniques that depend on the related image properties are not pertinent for this situation. [3] In earlier years, numerous forgery discovery strategies have been proposed for duplicate move forgery location. As indicated by the current strategies, the duplicate move forgery location techniques can be sorted into two primary classifications. square based calculations [4] and include key point-based calculations [5-7].

There are numerous sorts of image frauds, for example, grafting objects starting with one image then onto the next, expelling items or districts from images, making duplicates of articles in a similar image, and the sky is the limit from there. To identify these frauds, specialists have proposed strategies dependent on a few procedures, for example, JPEG pressure antiques, resampling location, lighting ancient rarities, clamor irregularities, camera sensor commotion, and some more. Nonetheless, most procedures in writing center around a particular kind of control or a gathering of comparable alter tasks. In sensible situations, a large group of tasks are applied when making altered images. For instance, when an article is joined onto an image, it is frequently joined by different tasks, for example, scaling, pivot, smoothing, differentiate upgrade, and that's only the tip of the iceberg. The need for image forgery detection implementation is important which motivates to work on this platform in MATLAB.

This paper is organized as follows. Introduction to image forgery and its need in research in first section. In second section, related work shows literature in brief. The next section shows implementation in brief and finally results for image forgery proposed work is presented and concluded.

II. RELATED WORK

In [1] proposed a forgery discovery technique in which the information image was isolated into over-lapping rectangular squares, from which the quantized Discrete Cosine Transform (DCT) coefficients of the squares were coordinated to discover the altered locales. [2] applied Principal Component Analysis (PCA) to diminish the element measurements. [3] utilized the RGB shading parts and heading data as square highlights. [4] utilized Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to extricate the image highlights. [5] determined the 24 Blur-invariant minutes as highlights. [6] determined the solitary estimations of a decreased position guess in each square. [7] utilized the Fourier-Mellin Transform (FMT) to acquire highlights. [8, 9] utilized the mean powers of circles with various radii around the square community to speak to the square highlights. [10] utilized the dim normal consequences of each square and its sub-obstructs as the square highlights. [11, 12] utilized Zernike minutes as square highlights. [13] utilized data entropy as square highlights. As an option in contrast to the square based techniques, key point-based forgery discovery strategies were proposed, where image key focuses are separated and coordinated over the entire image to oppose some image changes while distinguishing copied locales. In [14-16, 18], the Scale-Invariant Feature Transform (SIFT) [20] was applied to the host images to remove include focuses, which were then coordinated to each other. At the point when the estimation of the move vector surpassed the edge, the arrangements of relating SIFT highlight focuses were characterized as the forgery district. In [17, 19], the Speeded Up Robust Features (SURF) [20] were applied to extricate includes rather than SIFT.

III.IMPLEMENTATION

In this section, implementation and results are discussed. Firstly, adaptive over segmentation is implemented with feature point matching technique. After which, noise attack is introduced to the adaptive over segmentation technique as proposed work. As an application to this work, aadhar card image forgery detection is implemented. The results are compared on the basis of F1 measure, recall and precision.

The implementation process is explained using algorithm and flow chart (Fig. 1) given below. Several attacks can be studied such as image compression attack, rotation attack, noise attack, scaling attack and down sampling attack. Out of these main is noise attack, in which forged image comes under noise influence and then the forged image is detected. After selecting the input image, the type of attack is selected. Noise introduction using random function below:

```
nf=50;
rand('state',0);
 ng=rand(size(Q));
```

Application of discrete wavelet transform on the haar cascade to see area of consideration. The areas are defined into blocks for segmentation using red marking. Sum parameter, mean is calculated for the boundary mask preparation. This stage is for adaptive over segmentation technique the blocks are combined and displayed into one image. Using SURF method features are calculated for feature matching technique. Correlation coefficient

between original and forged image is calculated. The region or location where correlation coefficient shows difference is located. The final region is extracted through the segmentation method by the morphological operations. Final output image shows the detected forged region. Evaluation of performance metrics is completed such as precision, F1 measure and recall are calculated. As an application, the aadhar card is taken, it is forged by changing the image and then tested under the software.

The block diagram of this process is shown in Fig. 1. figure shows the process of the proposed algorithm step by step.

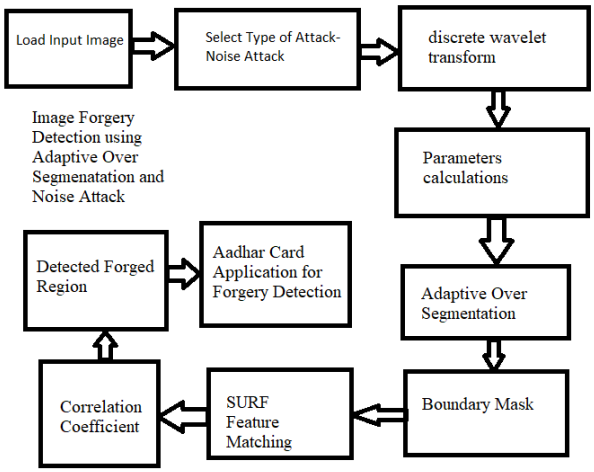

Fig. 1. Proposed Block Diagram for Image Forgery Detection Algorithm

IV. RESULTS

In this section, results are displayed. Fig. 2 and 3 are the input image and forged image. This is input from MATLAB read commands.

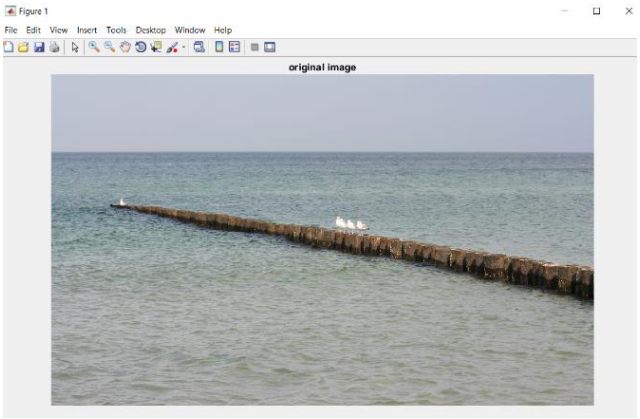

Fig. 2. Input Image

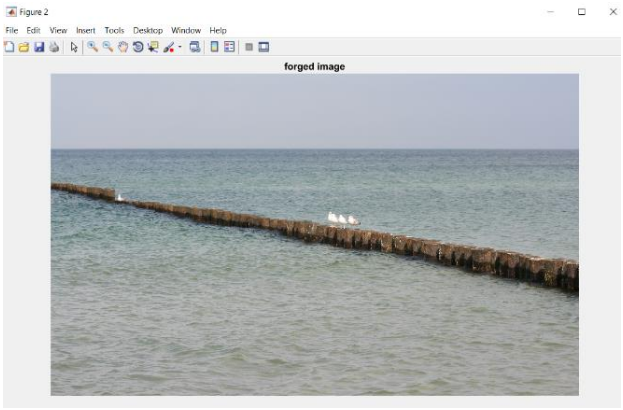

Fig. 3. Forged Image

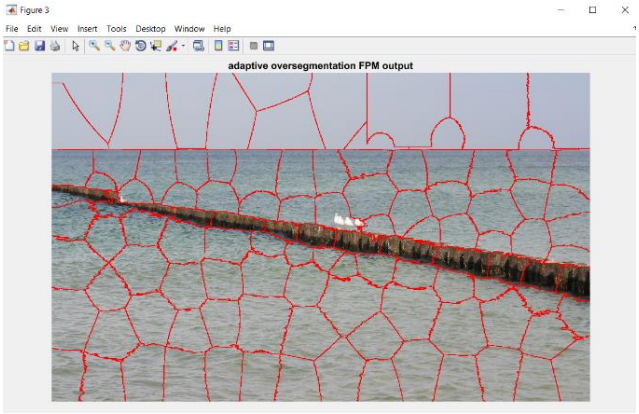

Fig. 4. Adaptive Over Segmentation FPM output

After performing the steps of DWT and blocks for boundaries of segment, image Fig. 4 is achieved.

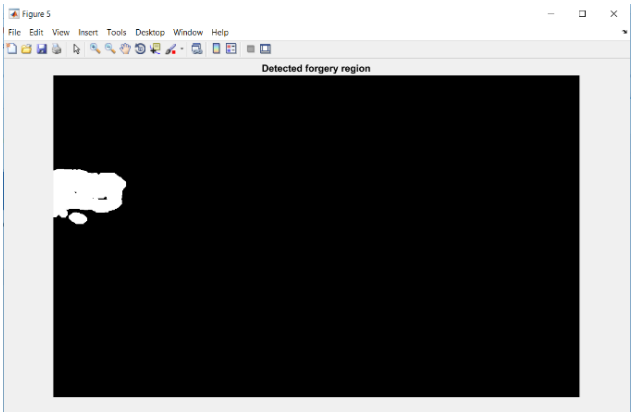

Fig. 5. Detected Forged Region

After feature point matching Fig. 5 has the detected forged region in white. This image is masked to Fig. 6 for final output.

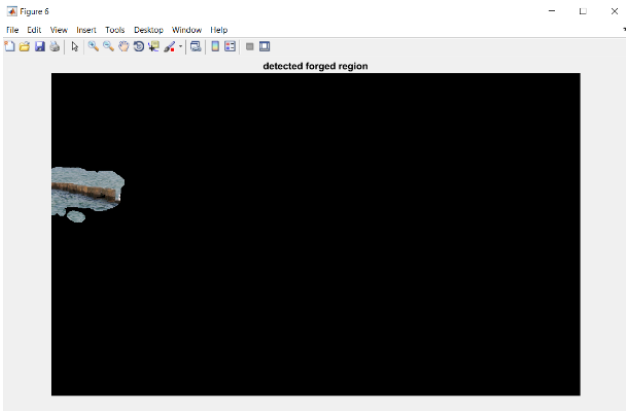

Fig. 6. Detected Forged Region Final

In Fig. 7, noise attack based segmentation of proposed output for AOS is shown with noise attack.

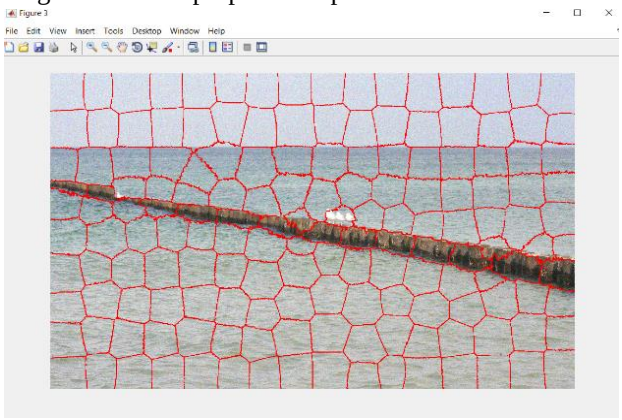

Fig. 7. Adaptive Over Segmentation with Noise Attack (Proposed)

In Fig. 8 and Fig. 9, final segmentation of detected region is shown.

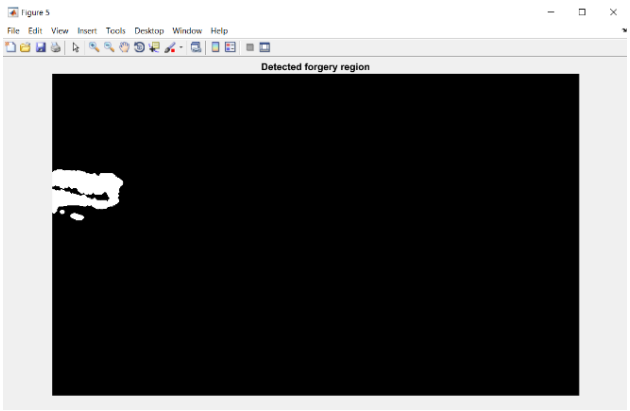

Fig. 8. Detected Region with Adaptive Over Segmentation with Noise Attack (Proposed)

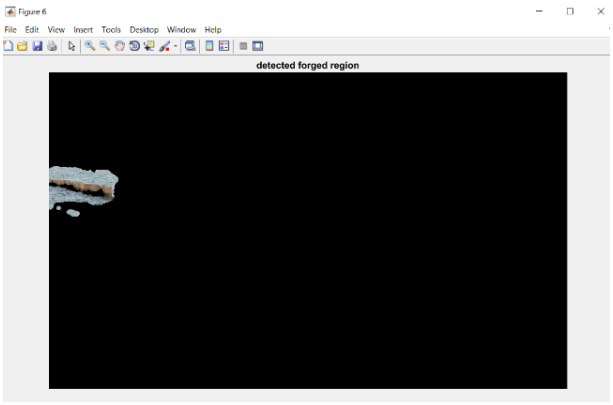

Fig. 9. Final Detected Region with Adaptive Over Segmentation with Noise Attack (Proposed)

Now, the simple AOS and noise attack based AOS is compared on the basis of precision, recall and F1 measure. In Fig. 10, precision comparison shows that for proposed work precision is increased.

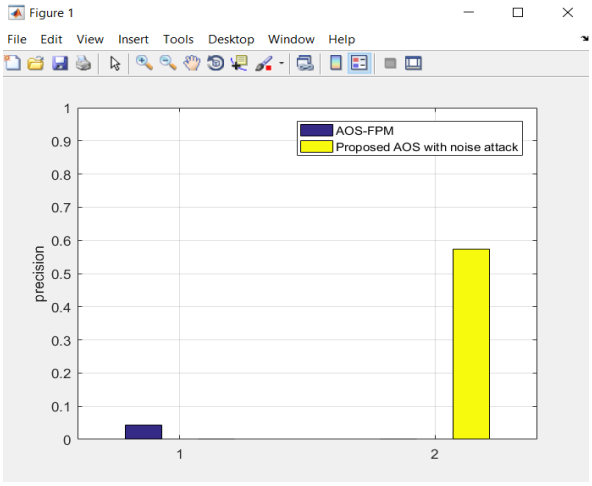

Fig. 10. Precision Comparison Chart

In Fig. 11, the recall value is increased in AOS with noise attack method.

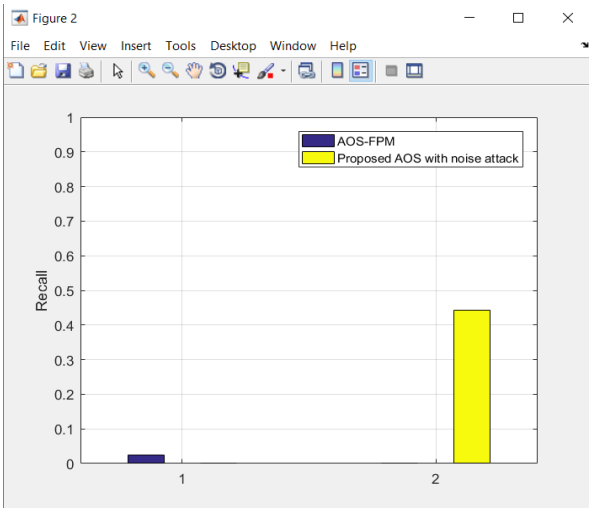

Fig. 11. Recall Comparison Chart

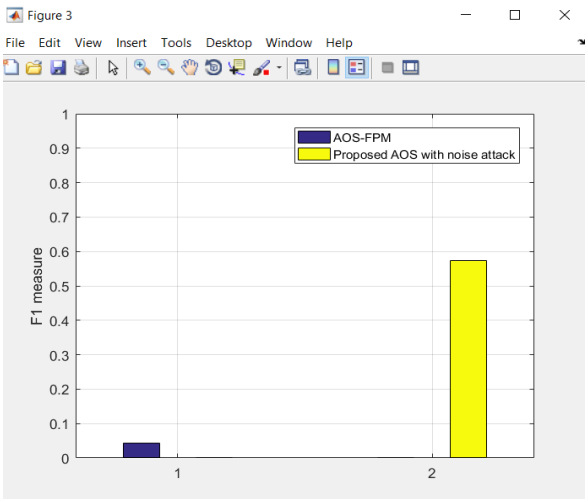

Fig. 12. F1 Measure Comparison Chart

Similarly, in Fig. 12 the F1 measure is improved in the proposed AOS with noise attack graph.

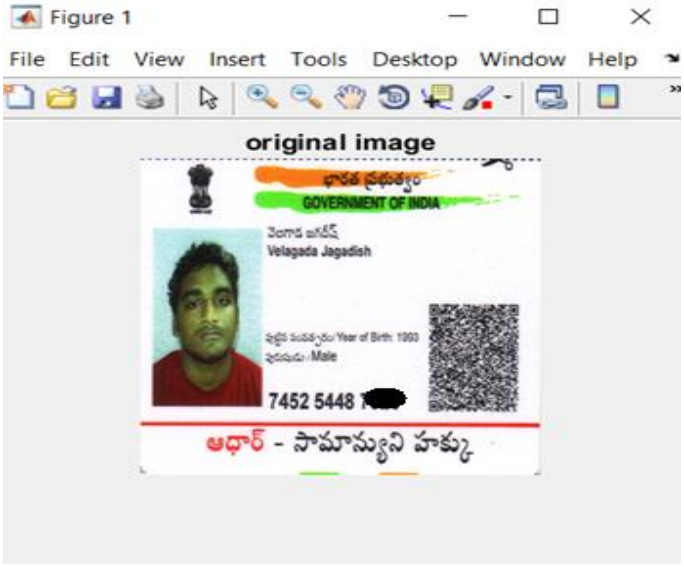

Fig. 13. Aadhar Card Input

In Fig. 13, aadhar card is input. And Fig. 14 is the forged aadhar card image.

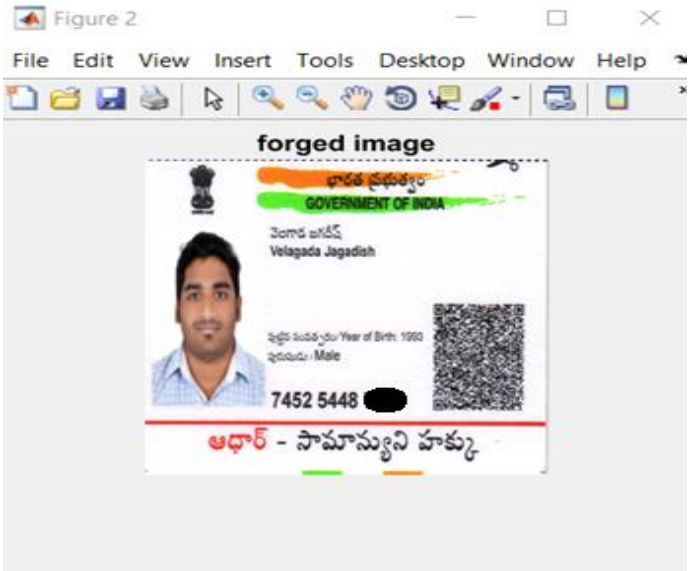

Fig. 14. Forged Aadhar Card Input

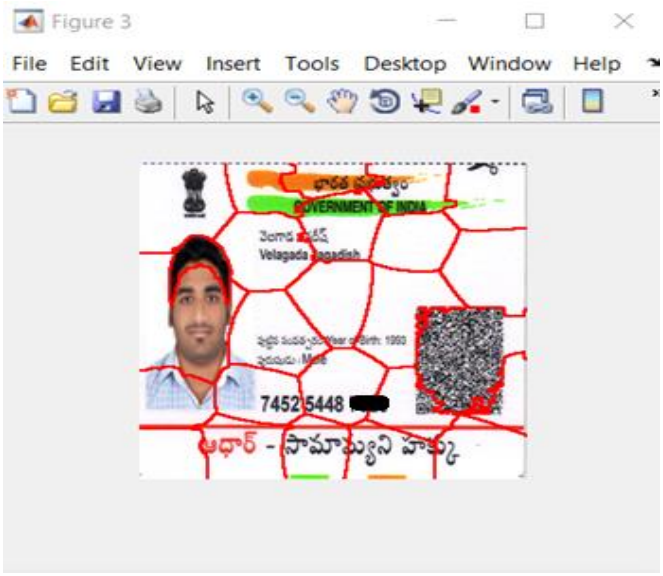

Fig. 15. AOS for Aadhar Card Input

AOS is applied in the image, as shown in Fig. 15 output.

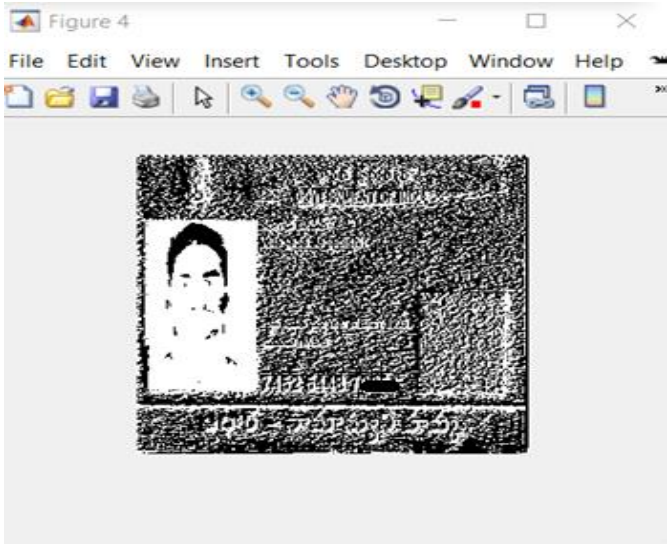

Fig. 16. AOS pre-processing output for Aadhar Card Input

Pre-processing output for detected region is shown in Fig. 16. and final forged region in Fig. 17.

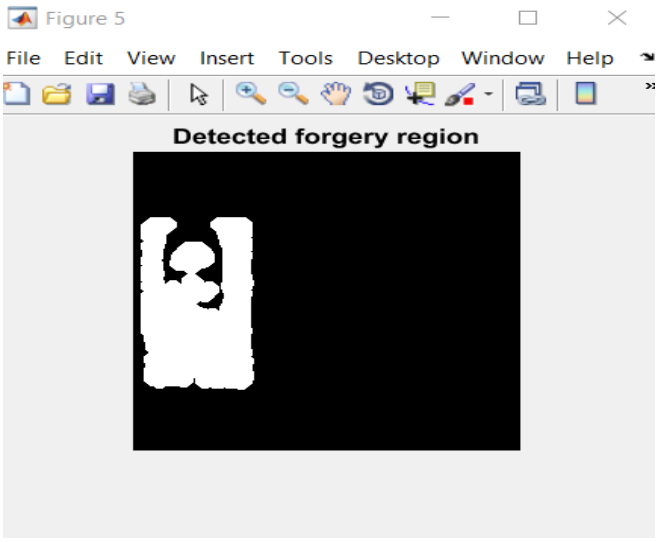

Fig. 17. Detected region for Aadhar Card Input

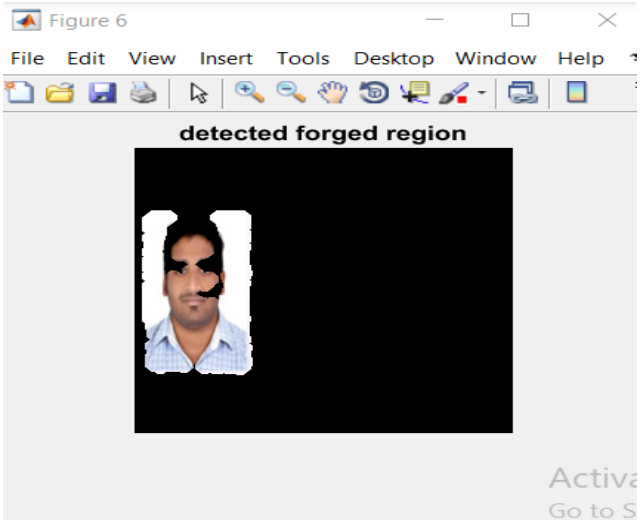

Fig. 17. Final Forged Aadhar Card Output

The forged output is shown in the above Fig. 17 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

V. CONCLUSION

Altering pictures isn't new. Accessibility of advanced picture innovation and picture preparing programming makes it simple for anybody to make a fraud. As anyone might expect, altered pictures and recordings are showing up all over the place, from courts to logical diaries, and these pictures can profoundly affect society. There is an unmistakable requirement for instruments to identify fabrications, and the field of computerized picture crime scene investigation has risen to address this issue with no pre-necessities. In this paper, successfully implementation is done for AOS FPM technique and proposed a noise attack based algorithm, also applied on Aadhar card application for safety of information. Also, the performance metrics are improved in proposed work. The software used for this work is MATLAB. The calculation has been tried on countless pictures and discovered that twofold JPEG image is recognizable for a scope of value factors. Yet, on the off chance that an altered JPEG picture is edited preceding re-sparing, the connections depicted are not presented.

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 Flenner3, 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).

