International Journal of Engineering &Technology, 7 (3.12) (2018) 505-511

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An Integrated Technique for Image Forgery Detection using Block and Keypoint Based Feature Techniques

Leela Apurupa[1*], J.D.Dorathi Jayaseeli[2], D. Malathi[3]

[1, 2, 3]Department of Computer Science and Engineering
SRM Institute of Science and Technology, Chennai, Tamilnadu, India
**Corresponding Author E-mail: [1]apurupa_ch@srmuniv.edu.in, [2]dorathijayaseeli.jd@ktr.srmuniv.ac.in*
[3]malathi.d@ktr.srmuniv.ac.in

Abstract

The invention of the net has introduced the unthinkable growth and developments within the illustrious analysis fields like drugs, satellite imaging, image process, security, biometrics, and genetic science. The algorithms enforced within the twenty first century has created the human life more leisurely and secure, however the protection to the first documents belongs to the genuine person is remained as involved within the digital image process domain. a replacement study is planned during this analysis paper to discover. The key plan in the deliberate take a look at and therefore the detection of the suspected regions are detected via the adaptive non-overlapping and abnormal blocks and this method is allotted exploitation the adaptive over-segmentation algorithmic rule. The extraction of the feature points is performed by playacting the matching between every block and its options. The feature points are step by step replaced by exploitation the super pixels within the planned Forgery Region Extraction algorithm then merge the neighboring obstructs that have comparative local shading decisions into the element squares to encourage the brought together districts; at last, it applies the morphological activity to the bound together areas to ask the recognized falsification districts The planned forgery detection algorithmic rule achieves far better detection results even below numerous difficult conditions the sooner strategies all told aspects. We have analyzed the results obtained by the each SIFT and SURF and it is well-tried that the planned technique SURF is giving more satisfactory results by both subjective and objective analysis.

Keywords—*copy-move; forgery detection; adaptive over-segmentation; feature point matching; neighboring blocks; super pixels; feature points*

1. Introduction

The digital image process is that the distinguished analysis domain within the twenty first century wherever its presence is clearly ascertained in numerous fields. The digital image process could be a vital constituent of the spectrum and therefore the security field stay collectively of the key analysis areas on that heap of analysis has to be done to secure the privacy and therefore the counseling with larger strength. The forgery has become the key involved space within the twenty first and plenty of analysis is disbursed within the literature however still achieving the required results remained as unsolved issue. The digital pictures area unit thought-about because the primary supply of the medium used for too meet the terribly purpose which incorporates the information transmission, the information compression, the information activity and therefore the numerous alternative applicable analysis areas. The forgery of the pictures has reach to the new level to cause serious problems within the twenty first century and it creates true wherever the distinction between solid the cast the solid and non-forged documents identification become the largest disadvantage, that is self-addressed in economical method victimization the projected work.

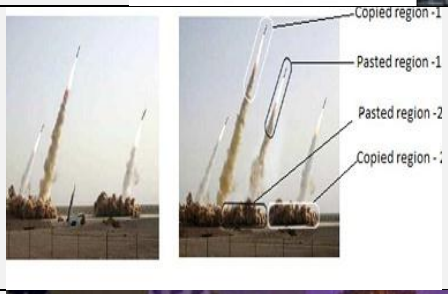
Image forgery performance is simple today. Virtual photograph is copy-flow forgery, in the course of which we've were given to copy the real place and paste it to a exclusive part of regular photograph. In literature we have a tendency to saw that such a lot of forgery detection techniques area unit developed to copy–move

forgery detection which input picture is segmental into overlapped rectangular blocks to hunt down tampered regions with the help of wonderful cost redesign (DCT) constant.Luo et al. for block feature we have a tendency to used RGB color elements in addition as direction data during this technique. Li et al during this to urge image feature we have a tendency to used 2 ways specifically distinct ripple remodel (DWT) and Singular worth Decomposition(SVD). Mahdian and Saic during this paper for feature extraction twenty four blur-invariant moments area unit thought-about. Bayram et al. to urge the feature, remodel technique used is Fourier-Mellin remodel (FMT). Wang et al. to urge the Block options, issues of mean intensity with totally different radii area unit thought-about. Ryu et al. to urge block options there's thought of Zernike moments. RavoSolorio and Nandi to urge block options there's thought of data Entropy. I. Amerini, L. Ballan to urge block options there's thought of Scale Invariant Feature remodel (SIFT). There are unit 2 existing ways for forgery detection, one is block primarily based that work on input image to divide it into 2 regions as regular region overlapping region so it matches with the image pixels to urge solid regions or their remodel is taken for process. Another is vital purpose primarily based forgery detection during which there's duplicate region detection.

2. Types of Digital Image Forgery

Imitation pictures became widespread in society nowadays. Therefore, the meddling pictures area device product common in scandal, techniques. One will notice sturdy sound stable pictures wont to sensationalize news, unfold political info and rumors, introduce mental emotional internal. Since the credibleness ofphotos suffers, it is essential to plot techniques a good way to verify their genuineness and trustiness of pix.The frauds region unit grouped into five noteworthy classifications: picture modifying, Image intersection, Copy-Move (cloning), Morphing, and Enhanced. the essential kind is picture modifying, wherever the methodology is utilized for improves a photo or diminishes bound component of a photo and upgrades the picture quality for catching the peruser's consideration. Among this strategy, the talented picture editors alter the foundation, fill some captivating hues, and work with tint immersion for conditioning and leveling. The second kind is image junction wherever the various parts from multiple pictures area unit pose in an exceedingly single image to convey an inspiration. Copy-move imitations zone unit some of the time identified by discovering coordinating districts inside the picture, however late examination has adopted an extra element based strategy, focusing on coordinating choices (as in protest recognition)instead of squares, if you want to permit for numerous picture adjustments that is probably wont to deliver greater persuading fabrications. The forward sort is Morphing and amid this sort the picture and video will be uncovered into particular impact were the one protest on picture is progressed toward becoming to an alternate question inside the elective picture. The transforming is utilized to exchange the single picture from someone else picture by exploitation consistent progress between 2 pictures.

Table 1: Types of Digital Image Forgery

Types	Detail	Appearance
Imageretouching,	An example of forgery where the original image and a forged image shows the difference [19].	
ImageSplicing,	In these images some parts of image copy from base image like shark. The base image (helicopter rescue) first turns over horizontally and the shark image is pasted to make new forged image. The forged image is not splicing with the original helicopter rescue image [20].	
CopyMove(cloning),	The images shows the copy-move attack and in left side image three rockets and in The forged image contains four rockets [21].	
Morphing,	The left and right images are original the middle image is -morphing image [19].	
Enhanced	The authentic picture is upper right aspect and after that more advantageous photo with shade trade, after perform blur on heritage, finally original image (decrease proper)Current.	

3. Literature Survey

A. Detecting Duplicated Image

A technique that works by 1st applying principal element analysis to little mounted - size image blocks to yield a reduced dimension illustration was planned by Alin C Popescu et al. (2004). Whereas performing arts the on top of technique we are able to realize some duplicate pictures (noises). Then the duplicate regions are detected by lexicographically (the follow of aggregation dictionaries).Sorting the whole image blocks. This can be terribly wonderful and actual appropriate technique to yield a reduced dimension illustration. It's sensitive to jpeg lossy compression and additionally it's additive to noise.

B. Fast Copy-Move Forgery Detection

A methodology to discover copy- move forgery by dividing the image into overlapping blocks of equal size, extracting feature for every block and representing it as a vector and writing all the extracted feature vectors victimization the lowest kind, was planned by Hwei-jen sculpture et.al (2009). Base kind dramatically reduces the time quality and in addition the adopted decisions enhance the power of resisting of varied attacks like JPEG compression and person noise. each potency and high detection rates unit of measurement incontestable.

C. Robust Copy-move Forgery

Sevinc Bayram et al.(2009) projected to use Fourier- Mellin remodel (FMT) choices that unit of measurement invariant to scaling and translation. A replacement detection theme that makes use of investigation bloom filters is to boot introduced by them. It detects copy move forgery very accurately albeit the forged image is turned, scaled or very compressed. This detection theme improves the efficiency. But the strength of the maneuver is reduced.

D. Detection Digital Images Using SURF

B.L.Shivakumar et al. (2011)proposed a technique to discover duplication areas. As a result of one in all of the not unusual photograph forgery techniques is reproduction flow forgery (CMF).Identification of the CMF will be detected by the duplication regions exploitation sped up strong options (SURF) keypoints. This SURF extracts the block options (BF) during a reliable method. Keypoints are extracted from pictures. The duplication region is detected with totally different sizes. The result shows that CMF with minimum false match for pictures with high resolution. a couple of little derived regions weren't with success detected.

E. A Sift-Based Forensic Method

Irene Amerini et al. (2011) proposed a method to support image forgery detection based on SIFT algorithm. Thus, the algorithm is

used to detect the regions which are duplicated and determine the geometric transformation applied to perform such tampering. But, the main drawbacks of this technique, it is unable to detect the image with uniform texture and salient keypoints.

F. Exposing Transform-Invariant Features

Pravin Kakar et al. (2012) have planned a way supported transforming-invariant alternatives. These got y utilizing the options from MPEG-7 photograph signature gadgets.This method completed realistic results, accuracy and very low false positives. Thus, these alternatives square measure invariant to not unusual picture process operations.

4. Proposed Forgergy Detection Method

The forgery detection has been gaining the eye from the years because of its sheer significance within the actual time scenario examine for the effective detection of the picture forgery and itsframework is carried out as follows and its illustration is described in the Fig.1.

- In this process the key method within the projected study,that is administrated by victimization the accommodative over-segmentation methodology and therefore the segmental blocks are known as image blocks (IB).
- The irregular block segmentation is followed by the dimensions Invariant Feature rework (SIFT) technique, wherever it's applied to the every segmental block to.
- The suspected forgery regions indication is that the another vital side of the planned study, that is obtained by playacting the matching between theblock options with each other and therefore the matched feature points are termed because the labelled Feature Points (LFP) that is more used as reference for forgery region detection. Eventually, we generally tend to endorse the Forgery vicinity Extraction manner to sight the forgery area from the host photograph regular with the extracted LFP.

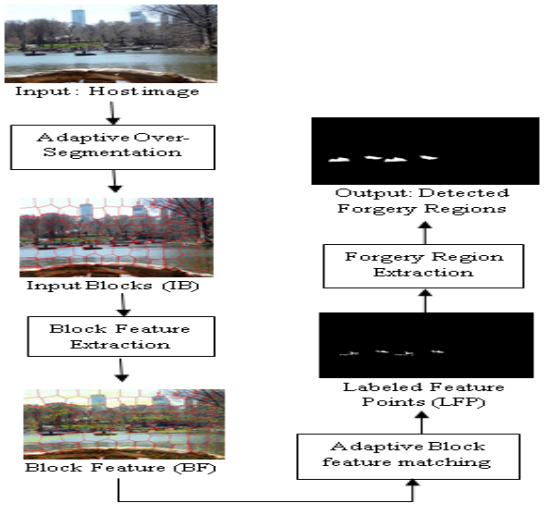


Fig. 1: The proposed copy-move forgery detection scheme framework

A. Versatile Over Division Calculation

The adaptive Over-Segmentation rule, that is analogous to once the dimensions of the host pictures will increase.To handle these issues, we have a tendency to projected. the non-covering division will diminish the system costs contrasted and the covering blocking; in addition, much of the time, the unpredictable and significant districts will speak to the imitation locale higher than the normal pieces. However, the initial size of the super pixels in SLIC is troublesome to make your mind up.In sensible utilizations of duplicate move phony recognition, the host pictures and furthermore the duplicate move districts zone unit very surprising of different sizes and have diverse substance, and in our imitation identification method, entirely unexpected totally extraordinary introductory sizes of the super pixels will turn out various falsification location comes about.

We have performed an oversized range of experiments to hunt the connection between the statistical distribution of the host pictures and also the initial size of the superpixels to get smart forgery detection results. we have a tendency to performed a four-level DWT, exploitation the 'Haar' wave, on the host image; then, the low-frequency energy ELF and high-frequency energy extremely high frequency is calculated exploitation (1) and (2), severally.

With the low-frequency energy ELF and high-frequency energy extremely high frequency, we Will calculate the proportion of the low-frequency distribution overseas terrorist institution exploitation (3), in line with that the preliminary size S of the superpixels is printed as in (4)

$$E_{LF} = \sum |CA_4| \quad (1)$$

$$E_{HF} = \sum_i \left(\sum |CD_i| + \sum |CH_i| + \sum |CV_i| \right), i = 1,2,\dots,4 \quad (2)$$

$$P_{LF} = \frac{E_{LF}}{E_{LF} + E_{HF}} . 100\% \quad (3)$$

$$S = \begin{cases} \sqrt{0.02 \times M \times N} P_{LF} > 50\% \\ \sqrt{0.01 \times M \times N} P_{LF} \leq 50\% \end{cases} \quad (4)$$

$M \times N$ represents the dimensions of the host image; and P LF approach represent the percent of the low-frequency distribution

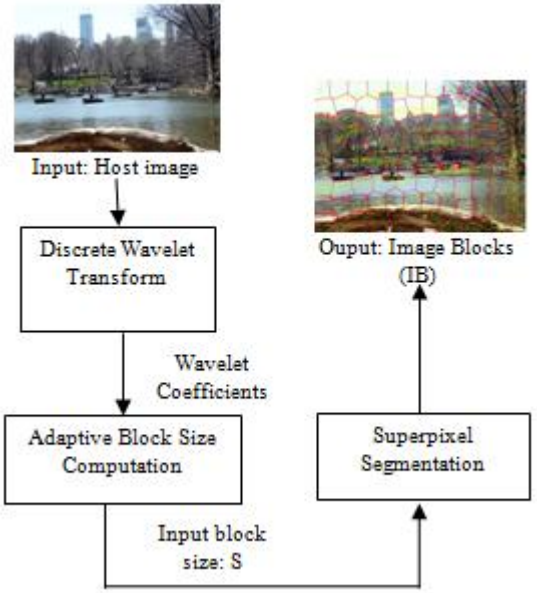


Fig. 2: The adaptive over-segmentation flowchart

B. Block Feature Extraction Algorithm

After the host image is metameric into image blocks, block options square measure extracted from the picture blocks (IB). The usual block-primarily based forgery detection strategies extracted options of a comparable length due to the fact the block options or directly used the pixels of the photo block because the block alternatives. However, those alternatives replicate within the important the content of the photo blocks, going out the scenario facts. Also, these options don't seem to be immune to varied image transformations. Therefore, during this project, the feature point's square measure extracted from each photo block as block alternatives and consequently the feature points need to be sturdy to numerous distortions, like photograph scaling, rotation, and JPEG compression. The characteristic motive extraction techniques, SIFT and SURF are huge used.The characteristic point's generated victimization those techniques rectangular degree robust in opposition to commonplace photo manner operations like rotation, scale, blurring,and compression.

Experiments have shown that the results obtained victimization SIFT square measure additional constant and have higher performance compared to different feature extraction strategies. Hence, during this project SIFT is employed for feature purpose extraction. Therefore, each block characteristic incorporates irregular block vicinity records and consequently the extracted SIFT characteristic points.Initial sizes in keeping with the given host photos, with which every photo may be decided to be the correct block preliminary dimension to boom the forgery detection outcome.

C. Block Feature Matching Algorithm

In a large portion of the triumphant piece based absolutely ways, the square coordinating methodology yields a selected block strive as long as there are unit several opportunity As quickly as the move vector surpasses a client specific edge, the coordinated obstructs that contributed thereto specific move vector locale unit known as regions which may additionally are derived and affected. In our system, as a result of the block feature consists of a collection of characteristic points, we have a tendency to planan awesome technique to locate the matched blocks.

D. Forgery Region Extraction Algorithm

As soon as the tagged function facets (LFP) square measure extracted, there's a wish to find the forgery areas conjointly. On the grounds the degree completely the places of the forgery regions. Forgeryvicinity Extraction algorithmic software is hired to find out the cast regions diverse as it should be. To get the suspected regions (SR), a method by using the usage of substitution the LFP with the tiny first-rate pixels is projected. This also can be accomplished via segmenting the host image all proper as tiny super pixels. The local color picks of the first-rate-pixels that rectangular degree acquaintances ofthe presumed districts (SR) are estimated to support the precision and bear in mind about expenses.

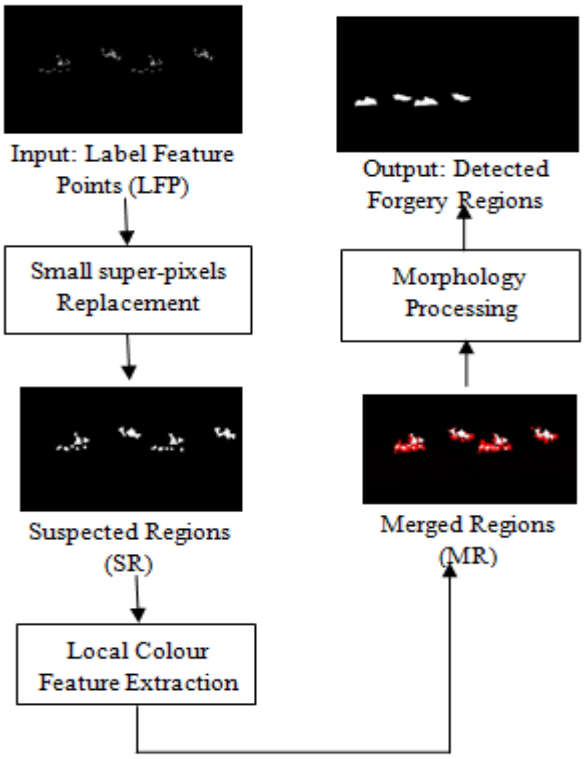


Fig. 3: Flow diagram of the Forgery Region Extraction algorithmic rule

Algorithm: Forgery Region Extraction

STEP-1: Load the Labeled Feature Points (LFP), apply the SLIC set of rules with the initial size S to the host photograph to section it into small superpixels as function blocks, and update each labeled feature factor with its corresponding feature block, accordingly generating the Suspected Regions (SR).

STEP-2: Measure the nearby color characteristic of the superpixels neighbor to the SR, referred to as neighbor blocks; when their colour function is much like that of the suspected

regions, we merge the neighbor blocks into the corresponding SR, therefore growing the merged regions (MR).
STEP-3: Apply the morphological near operation into MR to finally generate the detected forgery areas.

5. Results and Discussion

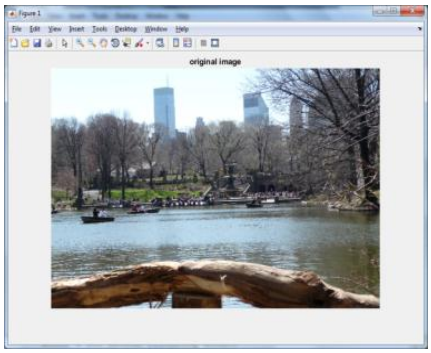


Fig. 4.1: Original Image

Original image is nothing but is used before tampering an image. Duplicate move fabrication is one of the altering techniques used to control advanced pictures.

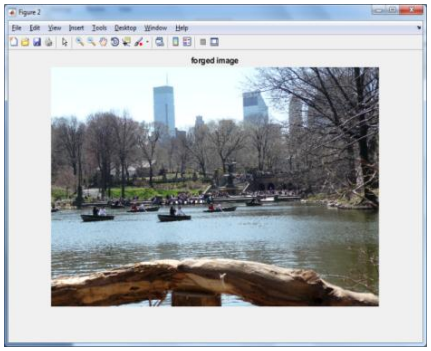


Fig. 4. 2: Forged Image

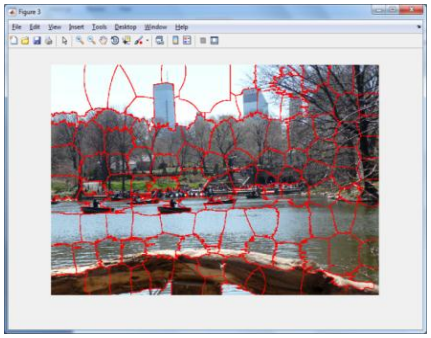


Fig. 4.3: Adaptive Over Segmentation

Adaptive over segmentation is by and large used for the conversion of photograph into sub-blocks

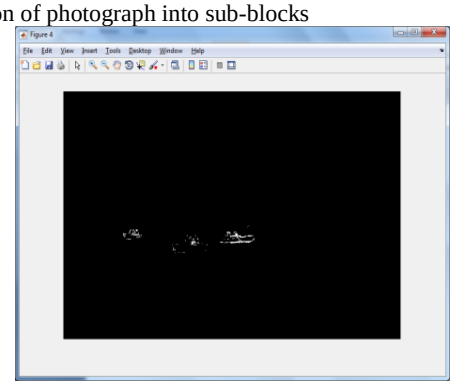


Fig. 4.4: Label Feature Points

Label key points are nothing but suspected region from an image which may not be the original content of an image.

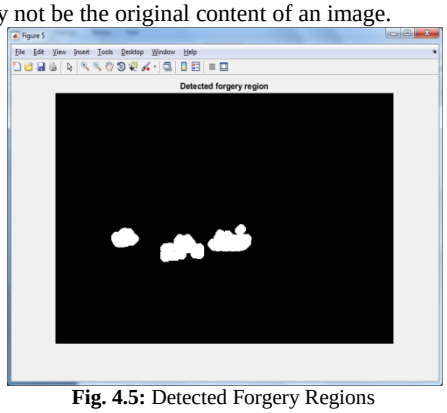


Fig. 4.5: Detected Forgery Regions

Detected forgery region of an image is output of forgery region extraction algorithm.

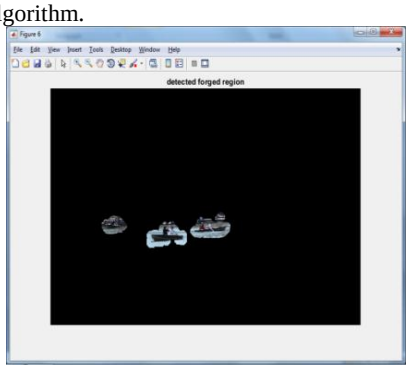


Fig. 4.6: Final Detected Forged Region

Finally detected region is shown in color image, to know better extracted part from original image.

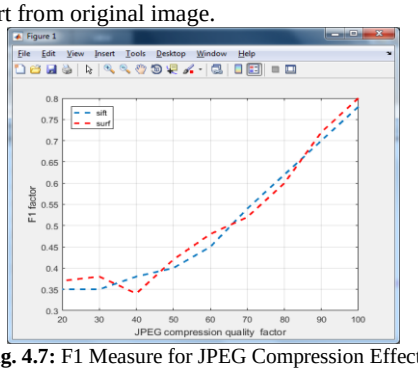


Fig. 4.7: F1 Measure for JPEG Compression Effect

The JPEG compressed pics are the forgery pics. The compression can be with a high-quality factor varying from 100 to 20, in steps of -10. So here we've to check the full of 48×9=432 photos.

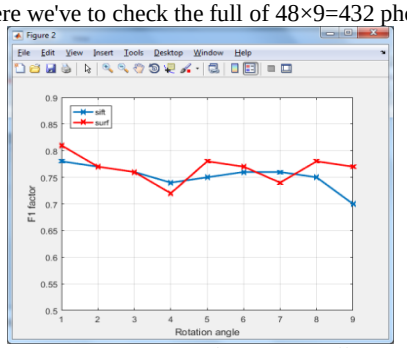


Fig. 4.8: F1 Measure for Rotation Effect

The regions which are copied are rotated via the turned around attitude various from 2º to 10º, in steps of 2º,and the rotation angles are about 20º, 60º and 180º as nicely. So here we've got to check the full of 48×8=384 photos.

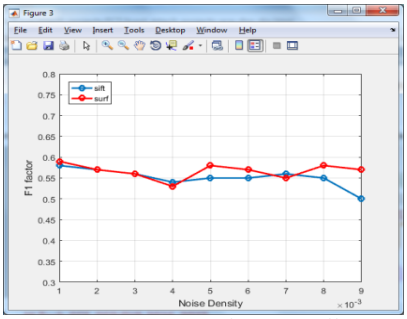


Fig. 4.9: F1 Measure for Noise Effect

Noise effect is checked here.Total 48 forged host images are present in the dataset.

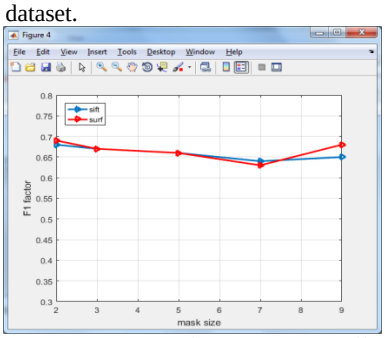


Fig. 4.10: F1 Measure for Median Filter Effect

F1 measure is calculated by applying median filter for input image and checked robustness of system.

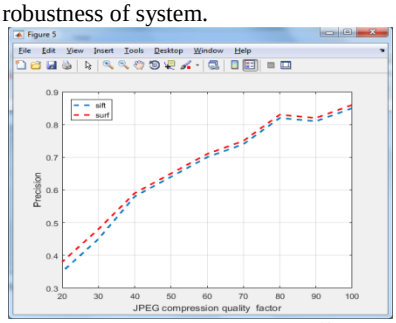


Fig. 4.11: JPEG Compression Effect

The JPEG compressed images are the forgery photographs. The compression can be with a excellent issue varying from 100 to twenty,in steps of -10. So here we've got to check the overall of 48×9=432 photos

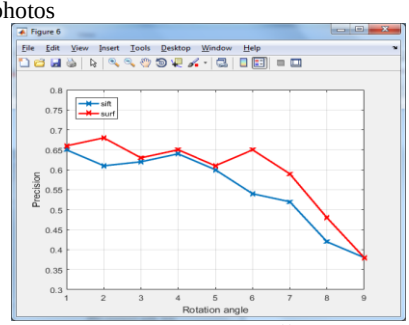


Fig. 4.12: Rotation effect

The JPEG compressed photos are the forgery images. The compression can be with a satisfactory component various from one hundred to 20, in steps of -10. So here we have to test the entire of 48×9=432 pics

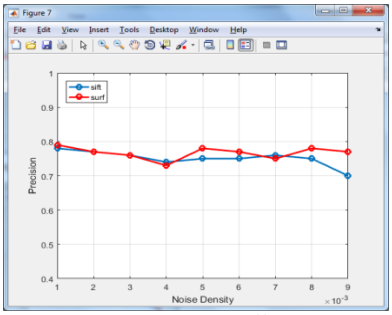


Fig. 4.13: Noise effect

Noise effect is checked here.Total 48 forged host images are present in the dataset. These images are scaled down from 90% to 10% in steps of 20%. So here we have to test the total of 48×5=240 images.

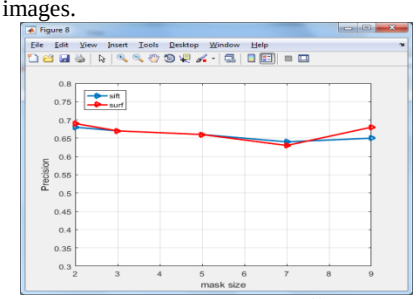


Fig. 4.14: Median Filter Effect

F1 measure is calculated by applying median filter for input image and checked robustness of system. By this implementation we can say that by SURF we can get robust system.

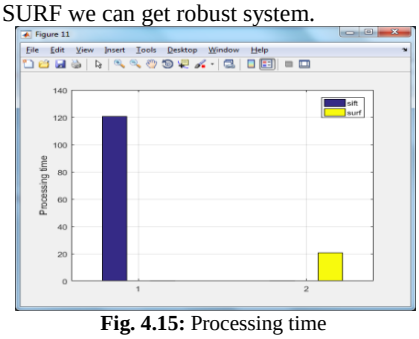


Fig. 4.15: Processing time

We checked here processing time required to execute both by SIFT and SURF. Time required to execute the implementation by SURF is very less.

6. Conclusion

This paper is given all the image fabrication ideas and numerous ways to differentiate forgery space from a picture. Rangeof ways and their impediments are talked concerning very well during this paper. Copy Move impersonation space in leading edge footage is additional inevitable issue within the interior of the past a handful of decades. Varied ways are projected to handle this issue. This paper provides transient investigation to differentiate copy move extortion recognizable technique. This in like manner covers limitations of varied frameworks used for standoff technique to acknowledge copy move manufacture. The shut work could also be extended by proposing a very distinctive methodology could also be overcome.So, there would like a very distinctive calculation which can conquer the restrictions and provides extra precise outcomes by subjective and objective examination.

References

[1] Yang and C.-L. Huang, "Copymove Forgery Detection in Digital Image," Advances in Multimedia Information Processing-PCM 2009, Ed: Springer, Pp. 816-825, 2009.

[2] Mahdian And S. Saic, "Blind Methods For Detecting Image Fakery," IEEE Aerospace And Electronic Systems Magazine, Vol. 25, Pp. 18-24, 2010.
[3] Shivakumar and L. D. S. Santhosh Baboo, "Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods," Global Journal of Computer Science And Technology, Vol. 10, 2010.
[4] K. N. Qureshi and A. H. Abdullah, "A Survey on Intelligent Transportation Systems," Middle East Journal of Scientific Research, Vol. 15, 2013.
[5] W. Lu, W. Sun, J.-W. Huang, And H.-T. Lu, "Digital Image Forensics Using Statistical Features and Neural Network Classifier," In Machine Learning and Cybernetics, 2008 International Conference on, Pp. 2831-2834, 2008.
[6] S. Bayram, B. Sankur, N. Memon, and İ. Avcibaş, "Image Manipulation Detection," Journal of Electronic Imaging, Vol. 15, pp. 041102-041102-17, 2006.
[7] Popescu and H. Farid, "Exposing Digital Forgeries By Detecting Traces of Resampling," Signal Processing, IEEE Transactions On, Vol. 53, pp. 758-767, 2005.
[8] E. Dirik, S. Bayram, H. T. Sencar, and N. Memon, "New Features To Identify Computer Generated Images," In Image Processing, 2007. ICIP 2007. IEEE International Conference On, pp. Iv-433-Iv-436, 2007.
[9] M. Kharrazi, H. T. Sencar, and N. Memon, "Blind Source Camera Identification," In Image Processing, 2004. ICIP'04. 2004 International Conference On, pp. 709-712, 2004.
[10] M.-J. Tsai and G.-H. Wu, "Using Image Features To Identify Camera Sources," In Acoustics, Speech And Signal Processing, 2006. ICASSP 2006 Proceedings. 2006 IEEE International Conference On, 2006.
[11] M.-J. Tsai and C.-S. Wang, "Adaptive Feature Selection for Digital Camera Source Identification," In Circuits and Systems, 2008. Iscas 2008. IEEE International Symposium On, pp. 412-415, 2008.
[12] Y. Sutcu, S. Bayram, H. T. Sencar, and N. Memon, "Improvements on Sensor Noise Based Source Camera Identification," In Multimedia And Expo, 2007 IEEE International Conference On, pp. 24-27, 2007.
[13] R. Bausvs and A. Kriukovas, "Digital Signature Approach for Image Authentication," Electronics & Electrical Engineering, 2008.
[14] T. Chen, J. Wang, and Y. Zhou, "Combined Digital Signature and Digital Watermark Scheme for Image Authentication," In Info-Tech and Info-Net, 2001. Proceedings. ICII 2001-Beijing. 2001 International Conferences On, pp. 78-82, 2001.
[15] X. Zhou, X. Duan, and D. Wang, "A Semifragile Watermark Scheme for Image Authentication," In Multimedia Modelling Conference, 2004. Proceedings. 10th International, pp. 374-377, 2004.
[16] M. Sridevi, C. Mala, and S. Sanyam, "Comparative Study of Image Forgery and Copy-Move Techniques," In Advances In Computer Science, Engineering & Applications, Ed: Springer, Pp. 715-723, 2012.
[17] S. Rawat and B. Raman, "A Chaotic System Based Fragile Watermarking Scheme for Image Tamper Detection," AEU-International Journal of Electronics and Communications, Vol. 65, pp. 840-847, 2011.
[18] M. Kirchner and R. Bohme, "Hiding Traces of Resampling in Digital Images," Information Forensics And Security, IEEE Transactions on, Vol. 3, pp. 582-592, 2008.
[19] H. Shah, P. Shinde, and J. Kukreja, "Retouching Detection And Steganalysis," IJEIR, Vol. 2, pp. 487- 490, 2013.
[20] R. Granty, T. Aditya, and S. Madhu, "Survey on Passive Methods of Image Tampering Detection," In Communication And Computational Intelligence (INCOCCI), 2010 International Conference On, pp. 431-436, 2010.
[21] M. Sridevi, C. Mala, and S. Sandeep, "Copy–Move Image Forgery Detection in a Parallel Environment," 2012.
[22] W. Luo, J. Huang, and G. Qiu, "Robust Detection of Region-Duplication Forgery in Digital Image," In Pattern Recognition, 2006. ICPR 2006. 18th International Conference On, pp. 746-749, 2006.
[23] J. Wang, G. Liu, H. Li, Y. Dai, and Z. Wang, "Detection of Image Region Duplication Forgery Using Model With Circle Block," In Multimedia Information Networking and Security, 2009. Mines'09. International Conference on Mines, pp. 25-29, 2009.
[24] N. D. Wandji, S. Xingming, and M. F. Kue, "Detection of Copy-Move Forgery in Digital Images Based On DCT," International Journal of Computer Science Issues (IJCSI), Vol. 10, 2013.
[25] S. Bayram, H. T. Sencar, and N. Memon, "An Efficient and Robust Method for Detecting Copy-Move Forgery," In Acoustics, Speech And Signal Processing, 2009. ICASSP 2009. IEEE International Conference, pp. 1053-1056, 2009.