iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 4 **Issue:** IX **Month of publication:** September 2016

**DOI:**

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

# Video Forgery Detection Using DWT, Optical Flow and SIFT Methods

Manpreet Kaur[1], Er. Mandeep Kaur[2]
[1]*M. Tech Scholar,* [2]*Assistant Professor*
*Guru Kashi University, Talwandi Sabo Guru Kashi University, Talwandi Sabo*

***Abstract:*** ***Digital video offer many attributes for tamper detection algorithms to take advantage of, specifically the color and brightness of individual pixels as well as the resolution and format. These properties provide scope for the analysis and comparison between the fundamentals of digital forgeries in an effort to develop a better algorithm for detecting tampering in a video. Copy-paste forgery, wherein a region from a video is replaced with another region from the same video (with possible transformations). Because the copied part come from the same video, its important properties, such as noise, color palette and texture, will be compatible with the rest of the video and thus will be more difficult to distinguish and detect these parts. Digital video forensics is a brand new research field which aims at validating the authenticity of videos by recovering information about their history. . Researchers have related the natural issues to the advance in computer graphics, animation, multimedia in the association of high computing machines, algorithms, increases the complexity of the issue. This thesis discusses the copy paste forgery detection in videos using Statistical fingerprints. In this work DWT is used to compress the images and optical flow is used to detect the flow of the moving objects and the forgery object. But the sift technique is used to detect the key features of the original image and the forgery image. The existing algorithm is compared with the new algorithm with precision, recall and total original frame and the detected forgery frame in the input video. In this work 98% accuracy is detected.***
***Keywords: DWT, SIFT, Optical Flow etc.***

## I. INTRODUCTION

The broad accessibility of the Internet combined with the effortlessly accessible video and video catching gadgets, for example, low-value cameras, advanced camcorders and

CCTVs have ended up essential part of the general public. Advancements in visual (video) innovations, for example, pressure, transmission, stockpiling, recovery, and video-conferencing have caused from various perspectives to the general public.

In the financial learning and exploratory advancement, the recordings and recordings accessible at different video sharing and long range interpersonal communication sites (like YouTube, Face Book, and so forth.) are assuming a critical part. Other than this, different applications like amusement industry, video observation, lawful confirmation, political recordings, video instructional exercises, commercials, and so on mean their uncommon part in today's connection [1].

Aside from numerous great things, there are some darker sides of visual (video) data, for example, abuse or the wrong projection of data through recordings. One of them is video altering, where a counterfeiter can deliberately control genuine (real or unique) recordings to make altered or doctored or fake recordings for negligence [3]. This thusly implies the recordings and recordings that are found in broad communications, for example, TV, well known Internet sites, for example, YouTube, might have been altered and the maxim "a photo talks a thousand words" while as yet remaining constant – might now have a covered up and subverted meaning, i.e., their realness can no more dependably be underestimated. [2] Hence, however the recordings and recordings from cameras, advanced camcorders and CCTVs can serve as intense "confirmations" in both legitimate courts and general conclusion, it is critical to ask whether the recordings and recordings created by these gadgets are genuinely bona fide and has not been messed with. Simple accessibility of numerous complex video altering devices gives a stage to falsifier to control genuine recordings and make perceptually vague fake recordings.

Consequently, in numerous genuine situations such as court trials, law requirement, criticism, legislative issues, and barrier arranging, and so forth validness of introduced video should be inspected. Legal devices and specialists assume a key part to analyze the legitimacy of recordings by identifying hints of altering. Here, achievement or disappointment of apparatuses and specialists relies on upon how shrewdly altering has been done by the falsifier. It is troublesome for criminological specialists to distinguish messing with recordings if there are no (or little) follows left by counterfeiter while altering. Lamentably, because of absence of built up techniques to inspect the validness of recordings, identification of messing around with recordings have postured challenges before mainstream researchers, and its reality in numerous situations (e.g. recordings as confirmation amid court trials) looks for

quick consideration.[3]

## II. VIDEO FORGERY DETECTION

Digital video offer many attributes for tamper detection algorithms to take advantage of, specifically the color and brightness of individual pixels as well as the resolution and format. These properties provide scope for the analysis and comparison between the fundamentals of digital forgeries in an effort to develop a better algorithm for detecting tampering in a video. Two types of video forensics schemes are widely used for video forgery detection: Active schemes and Passive schemes. In the active schemes, a watermark is used to detect tampering. However, this scheme needs a facility to embed the watermark [3]. On contrary, the Passive schemes extract some intrinsic characteristics of video to detect the tampered regions.

Video forgery detection seeks to find evidence of tempering by evaluating the authenticity of digital video evidence. Approach to video forgery detection in the literature can be categorized into active detection and passive detection as seen in Fig 1.1 [5]. Active video forgery detection is mainly based on watermark and digital signature. This has seen active research in the world of digital community for years and has recorded a significant progress [8]. Active detection depends on watermark or digital signature which can be found only in a few cameras such as Epson Photo PC 700/750Z, 800/800Z, 3000Z and Kodak DC290. Most other cameras lack this technology, making active technique extremely hard to use. Passive video forgery detection aims at extracting internal features of a video for the purpose of detecting forgery. This is because excellent tempering will elude human perception whereas statistical or mathematical characteristics of the video have been altered.

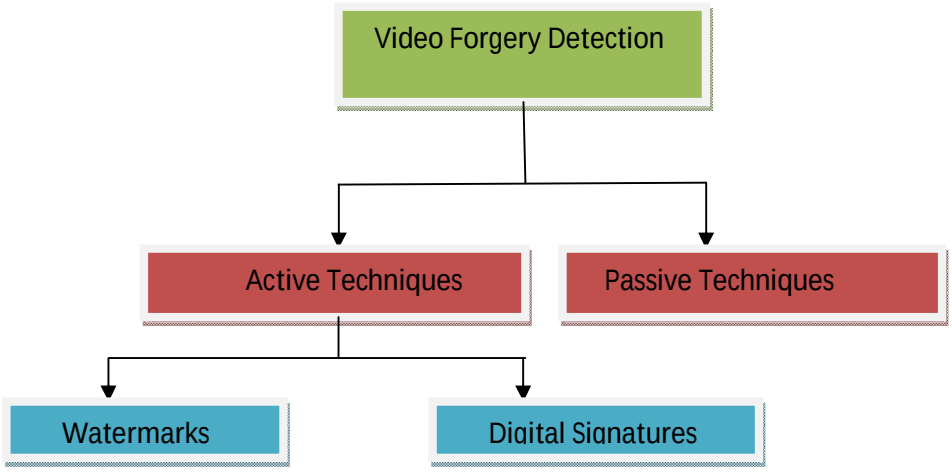



Figure 1 : Approaches to Video Forgery Detection[2]

## III. INTRODUCTION TO SCALE INVARIANT FEATURES TRANSFORM (SIFT)

Scale-invariant feature transform (or SIFT) is an algorithm in computer vision to detect and describe local features in images. The algorithm was published by David Lowe in 1999.[1]

For any object in an image, interesting points on the object can be extracted to provide a "feature description" of the object. This description, extracted from a training image, can then be used to identify the object when attempting to locate the object in a test image containing many other objects. To perform reliable recognition, it is important that the features extracted from the training image be detectable even under changes in image scale, noise and illumination. Such points usually lie on high-contrast regions of the image, such as object edges.

Another important characteristic of these features is that the relative positions between them in the original scene shouldn't change from one image to another. For example, if only the four corners of a door were used as features, they would work regardless of the door's position; but if points in the frame were also used, the recognition would fail if the door is opened or closed. Similarly, features located in articulated or flexible objects would typically not work if any change in their internal geometry happens between two images in the set being processed. However, in practice SIFT detects and uses a much larger number of features from the images, which reduces the contribution of the errors caused by these local variations in the average error of all feature matching errors.

SIFT [2]can robustly identify objects even among clutter and under partial occlusion, because the SIFT feature descriptor is invariant to uniform scaling, orientation, and partially invariant to affine distortion and illumination changes.[1]This section summarizes

Lowe's object recognition method and mentions a few competing techniques available for object recognition under clutter and partial occlusion.

SIFT keypoints of objects are first extracted from a set of reference images[1] and stored in a database. An object is recognized in a new image by individually comparing each feature from the new image to this database and finding candidate matching features based on Euclidean distance of their feature vectors. From the full set of matches, subsets of keypoints that agree on the object and its location, scale, and orientation in the new image are identified to filter out good matches. The determination of consistent clusters is performed rapidly by using an efficient hash table implementation of the generalized Hough transform. Each cluster of 3 or more features that agree on an object and its pose is then subject to further detailed model verification and subsequently outliers are discarded. Finally the probability that a particular set of features indicates the presence of an object is computed, given the accuracy of fit and number of probable false matches. Object matches that pass all these tests can be identified as correct with high confidence.[3]

## IV. OPTICAL FLOW

Optical flow or optic flow is the pattern of apparent motion of objects, surfaces, and edges in a visual scene caused by the relative motion between an observer (an eye or a camera) and the scene. The concept of optical flow was introduced by the American psychologist James J. Gibson in the 1940s to describe the visual stimulus provided to animals moving through the world.[3] Gibson stressed the importance of optic flow for affordance perception, the ability to discern possibilities for action within the environment. Followers of Gibson and his ecological approach to psychology have further demonstrated the role of the optical flow stimulus for the perception of movement by the observer in the world; perception of the shape, distance and movement of objects in the world; and the control of locomotion.[4] The term optical flow is also used by roboticists, encompassing related techniques from image processing and control of navigation including motion detection, object segmentation, time-to-contact information, focus of expansion calculations, luminance, motion compensated encoding, and stereo disparity measurement.[5][6].

## V. OPTICAL FLOW FOR MOTION ESTIMATION IN VIDEO

Optical flow is the distribution of the apparent velocities of objects in an image. By estimating optical flow between video frames, you can measure the velocities of objects in the video. In general, moving objects that are closer to the camera will display more apparent motion than distant objects that are moving at the same speed.

Optical flow estimation is used in computer vision to characterize and quantify the motion of objects in a video stream, often for motion-based object detection and tracking systems.

Figure 2: Optical flow estimation to obtain motion vectors (left) and pixel velocity magnitudes (right).

Algorithm

Step 1: Read the color forgery video from dataset .Step 2: Apply the frame separation to separate the frames with the help of :

```
nFrames = videoObj.NumberOfFrames;
vidHeight = videoObj.Height;
vidWidth = videoObj.Width;
T_frames=nFrames-1;
```

Step 3: Write the number of frames into original folder.

Step 4 :Apply fspecial filter to remove the Gaussian noise .

Step 5: Apply imfilter to reduced the replication and noise.

Step6: Apply optical flow to detect the forgery frame.

Step7: Apply shift to matching the feature points in forgery frames.

Step 8: Apply DWT to Compress the forgery video frame.
Step 9: Get the forgery video as output.
Step 10 : Get the different parameters.
The different windows are detected with different results. Each and every window displays the different outputs of the research problems that is defined in the problem formulation. The Snap shorts for the result are given below :

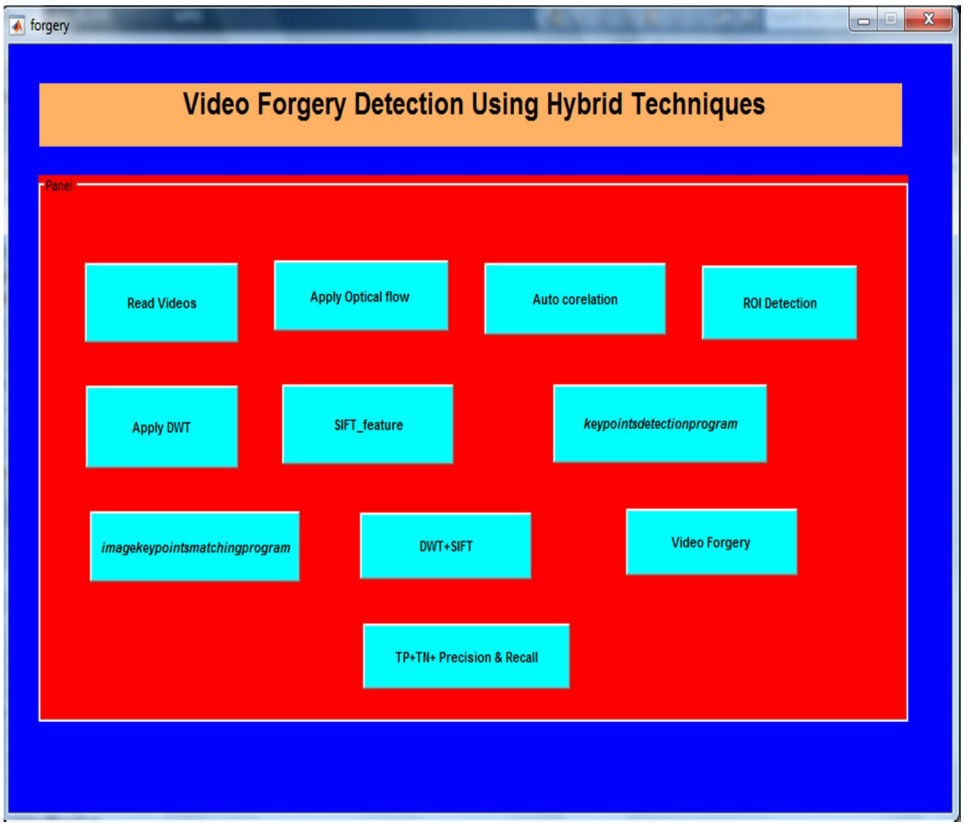



Figure 3: Input window of the work

The figure 5.1 is the input GUI windows that have many buttons and each button perform the different operations. In this window the video is processed or read operation is applied.
ROI Mask

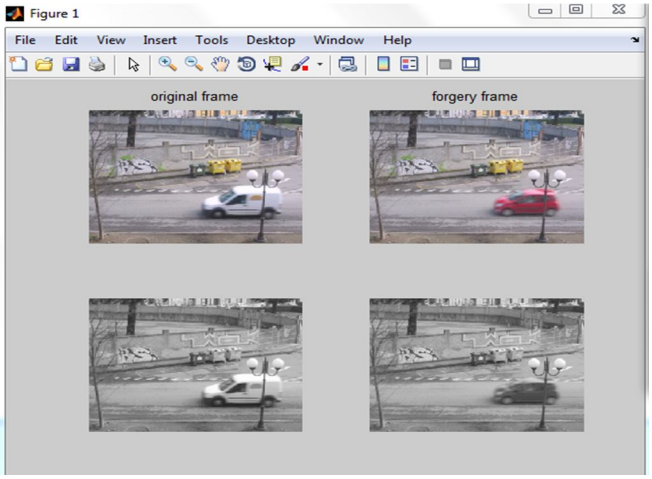



Figure 4. ROI mark on the forgery frame (a)

Volume 4 Issue IX, September 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

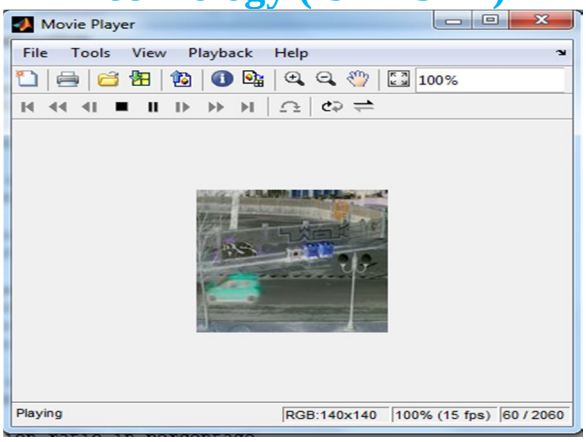


Figure 5. Forgery output video

Table 1: Key Feature Extraction

| Name of forgery Image | Forgery key points extracted | Name of Original Image | Original key points extracted |
|---|---|---|---|
| **109.png** | 1485 | 109.png | 1556 |
| **106.png** | 1410 | 106.png | 1580 |
| **107.png** | 1480 | 107.png | 1515 |
| **108.png** | 1460 | 108.png | 1546 |

Comparison Table of Old and new work

| S.No | Video name (REWIND Dataset) | Total No of Frames | New original detected | New forgery detected | Old Original detected[1] | Old Forgery detected[1] |
|---|---|---|---|---|---|---|
| **1.** | 07_forged.avi | 412 | 150 | 262 | 190 | 222 |
| **2** | 09_forged.avi. | 292 | 120 | 172 | 150 | 142 |
| **3** | 06_forged.avi | 261 | 126 | 135 | 130 | 131 |
| **4** | 01__forged.avi | 209 | 81 | 128 | 100 | 109 |

## VI. CONCLUSION

Digital video forensics aims at validating the authenticity of videos by recovering information about their history. Copy-paste forgery, wherein a region from an video is replaced with another region from the same video (with possible transformations). Because the copied part come from the same video, its important properties, such as noise, color palette and texture, will be compatible with the rest of the video and thus will be more difficult to distinguish and detect these parts. Digital video forensics is a brand new research field which aims at validating the authenticity of videos by recovering information about their history. The fundamental problems which research found in the literature can be categorized into the natural, forgery detection, flow mapping, and source identification. Therefore, the originality and authenticity of videos or data in many cases become challenging problem. Researchers have related the natural issues to the advance in computer graphics, animation, multimedia in the association of high computing machines, algorithms, increases the complexity of the issue.In response to this, researchers have begun developing digital forensic techniques capable of identifying digital forgeries. These forensic techniques operate by detecting imperceptible traces left by editing operations in digital multimedia content. In this dissertation, we propose several new digital forensic techniques to detect evidence of editing in digital multimedia content. We use DWT and different filters for forensic tasks such as identifying cut-and-paste forgeries from JPEG compressed videos. Additionally, we consider the problem of multimedia security from the forger's point of view.

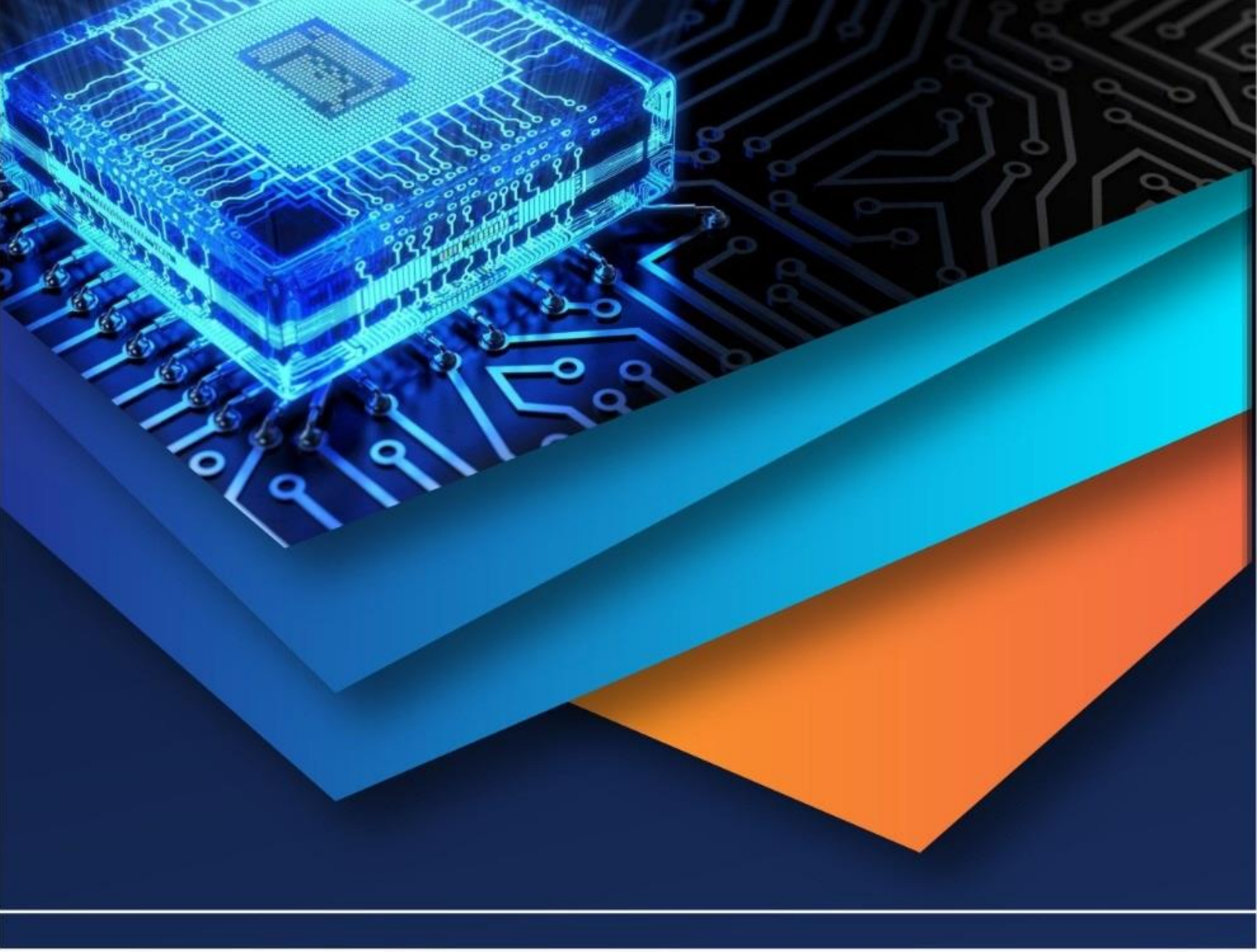
## VII. FUTURE WORK

In the future we can use real time videos to detect the copy and paste part with the help of frames and masking. To detect these different techniques applied that is DCT, correlation and filters.

## REFERENCES

[1] A merini, I., Barni, M., Caldelli, R., & Costanzo, A.(2013). Counter-forensics of SIFT-based copy-movedetection by means of keypoint classification. EURASIPJournal on Image and Video Processing, 2013(1), 18.
[2] A.C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," IEEE Transactions on Signal Processing, vol. 53(2), pp. 758–767, 2005.
[3] Chen, L., Lu, W., & Ni, J. (2012). An Image RegionDescription Method Based on Step Sector Statistics and itsApplication in Image Copy-Rotate/Flip-Move ForgeryDetection. International Journal of Digital Crime andForensics (IJDCF), 4(1), 49-62.
[4] Chen, L., Lu, W., Ni, J., Sun, W., & Huang, J. (2013).Region duplication detection based on Harris corner pointsand step sector statistics. Journal of Visual Communicationand Image Representation, 24(3), 244-254.
[5] Dhara Anandpara" A Joint Forensic System to Detect Image Forgery using Copy Move Forgery Detection and Double JPEG Compression Approaches" International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.
[6] Liu, G., Wang, J., Lian, S., & Wang, Z. (2011). Apassive image authentication scheme for detecting regionduplicationforgery with rotation. Journal of Network andComputer Applications, 34(5), 1557-1565.
[7] Liu, M.-H., & Xu, W.-H. (2011). Detection of copy-moveforgery image based on fractal and statistics. Journal ofComputer Applications, 8, 061.
[8] M. Chen, J. Fridrich, M. Goljan, and J. Luká˘s, "Determining image origin and integrity using sensor noise," IEEE Trans. Inf. Forensics Security, vol. 3, no. 1, pp. 74–90, Mar. 2008.
[9] M. K. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," in Proc. ACM Multimedia and Security Workshop, New York, NY, 2005, pp. 1–10.
[10] M. K. Johnson and H. Farid, "Exposing digital forgeries in complexlighting environments," IEEE Trans. Inf. Forensics Security, vol. 2, no.3, pp. 450–461, Sep. 2007.
[11] M.C.Stamnn,"Forensics Detection of Image Manipulation Using Statistical Intrinsic Fingerprints", IEEE Transactions on information Forensics And Security , vol. 5 No 3, 2010.
[12] M.K. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," Proc. ACM Multimedia and Security Workshop, New York, pp. 1–9, 2005.
[13] M.Wu A. Swaminathan and K. J. Ray Liu, "Image tampering identification using blind deconvolution," Proc. IEEE ICIP, 2006.
[14] Mahdian, B., & Saic, S. (2010). Bibliography onblind methods for identifying image forgery. SignalProcessing: Image Communication, 25(6), 389-399.
[15] Math, S., & Tripathi, R. (2010). Digital Forgeries: Problems and Challenges. International Journal of ComputerApplications, 5(12).
[16] Muhammad, G., Hussain, M., Khawaji, K., & Bebis,G. (2011a). Blind copy move image forgery detection usingdyadic undecimated wavelet transform. Paper presented atthe Digital Signal Processing (DSP.
[17] P.Kakar and N.Sudha "Exposing Post processed Copy-Paste Forgeries through Transform-Invariant Features", vol. 206, no. 1-3, pp. 178–184, 2011.
[18] Pan, X. Z., & Wang, H. M. (2012). The Detection Method of Image Regional Forgery Based DWT and 2DIMPCA.Advanced Materials Research, 532, 692-696
[19] Piva, A. (2013). An Overview on Image Forensics.ISRN Signal Processing, 2013.
[20] Pujari, V. S., & Sohani, M. (2012a). A Comparative Analysison Copy Move Forgery Detection in Spatial Domain MethodUsing Lexicographic and Non Lexicographic techniques.IJECCE, 3(1), 136-139.
[21] Pujari, V. S., & Sohani, M. (2012b). A Comparative AnalysisOn Copy Move Forgery Detection Using Frequency DomainTechniques. International Journal of Global TechnologyInitiatives, 1(1), E104-E111.
[22] S. Bayram, I.Avcibas, B. Sankur, and N. Memon, "Image manipulation detection," J. Electron. Imag., vol. 15, no. 4, p. 041102, 2006.

[23] S.Bayram,H.T.Sencar and N.Menon"A Survey of Copy-Move Forgery Detection Techniques", submitted to ICASSP 2009, 2009.
[24] S.Khan and A.Kulkarni ,"Reduced Time Complexity for Detection of Copy-Move Forgery Using Discrete Wavelet Transform" International Journal of Computer Applications (0975 – 8887) Volume 6– No.7, September 2010.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY