International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

A Video Forgery Detection Using Discrete Wavelet Transform and Scale Invarient Feature Transform Techniques

Gurjinder Kaur[1], Rishamjot Kaur[2]

[1]Department of Computer Science & Engineering, Baba Farid College of Engineering and Technology, Deon, Bathinda, India

[2]Assistant Professor, Department of information technology & Engineering, Baba Farid College of Engineering and Technology, Deon, Bathinda, India

Abstract: ***Forensics suggests that the utilization of science and technology within the investigation and institution of facts. Therefore the video or completely different pictures will be transmission to and reconverted into another video by another laptop. Processed crime scene investigation (in some cases referred to as advanced legal science) could be a branch of measurable science as well as the recovery and examination of structure found in processed gadgets. 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. We propose several new digital forensic techniques to detect evidence of editing in digital multimedia content. We use Optical flow, DWT and different filters for forensic tasks such as identifying cut-and-paste forgeries from JPEG compressed videos and SIFT. This SIFT based technique is dependent on feature extraction by using key point detection. This method is mostly used to Detection of malicious manipulation with digital videos (digital forgeries) in case of copy-move attack. The proposed work has been found effective result as comparison to exiting model. In exiting model 98.2143 precision value is calculated while in proposed model we get the value of precision 99.2454.The proposed model get more forgery frame as compared to exiting model. These calculations are not a similar because the previously estimated calculation within the approach that they are connected on the complete frame to concentrate highlights rather than separating the frame into the squares. From the above forgery problem resolving we are using MATLAB toolbox and we are getting the 97% accuracy of the work.***

Keywords: Image, DWT, Forgery, Sift, Optical Flow, MATLAB etc.

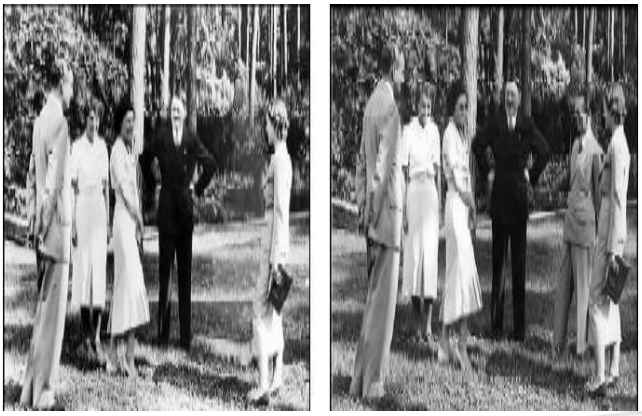
1. Introduction

In today's digital age, our daily life is permeated with digital multimedia content as one of the principal means for communication. As a matter of fact, such information can be created, stored, transmitted and processed in digital format in an extremely easy way, thanks to the wide spread of low-cost cameras and computers and user-friendly editing tools. 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].

2. Tampering of Video

Video signs are spatial-transient signs or basically expressed a grouping of time changing recordings. The data they pass on is "visual". A monochromatic still video can be scientifically spoken to by x (h, v), where x is the power esteem at the flat area h and vertical area v. The monochromatic video sign can be spoken to by x (h, v, t), where x is the power esteem at the h level, v vertical and t transient areas separately. Video altering is generally new region when contrasted with video doctoring as it is as old as the specialty of photography itself where we have various rates of genuine instances of fake photos [04]. Altering the computerized video is only adjusting or changing the substance of recordings. This should be possible by different techniques which are introduced in taking after subsections. While altering a video, goal of a falsifier is to make an altered or doctored or fake video from genuine or real or unique video. These genuine recordings are the hotspot for making altered recordings. The earnestness of video altering relies on upon how and where these altered recordings must be utilized. Court trials are a standout amongst the most generally utilized application territories where these altered recordings are exhibited as proof to delude the court procedures. Subsequently, at whatever point recordings are displayed as proof amid court trials, their genuineness are to be analyzed before considering them as confirmation [04]. While tampering a video, objective of a forger is to create a tampered or doctored or fake video from real or actual or original video. These real videos are the source for creating tampered videos. Tampering can be done either on a single

video (*i.e.* single source) or on multiple videos (*i.e.* many sources) [2] In Figure Joseph Goebbels was erased from the photo which was captured in 1937 during the meet of Hitler and Leni Riefenstahl. First photo is the doctored photo whereas second one is the original photo of that meet [12].



(a) tampered image (b) original image

Figure 1: Example of Copy-Move forgery [12]

Tempering Attacks in Video

a) Spatial Tempering: A forger can tamper source videos spatially by manipulating pixel bits within a video frame or across the video frames (i.e. set of adjacent frames).
b) Temporal Tempering: A forger can tamper source videos by disturbing the frame sequence through frames replacement, frames addition, and by the removal of video frames.
c) Spatio-Temporal Tempering: A forger can tamper videos in combination of both spatial and temporal domain by manipulating pixel bits within a video frame or across the video frames *as* well as disturb the frame sequence[5].

3. 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 1.2. 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]. 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.

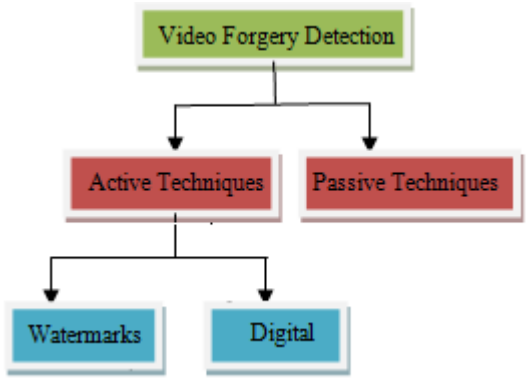


Figure 1.2: Approaches to Video Forgery Detection

4. 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 1.3: Optical flow estimation to obtain motion vectors (left) and pixel velocity magnitudes (right)[17].

5. Introduction to Discrete Wavelet Transforms (DWT)

In wavelet analysis, the Discrete Wavelet Transform (DWT) decomposes a signal into a set of mutually orthogonal wavelet basis functions. These functions differ from sinusoidal basis functions in that they are spatially localized – that is, nonzero over only part of the total signal length. Furthermore, wavelet functions are dilated, translated and scaled versions of a a common function _, known as the mother wavelet [18]. As is the case in Fourier analysis, the DWT is invertible, so that the original signal can be completely recovered from its DWT representation. Discrete Wavelet Transform (DWT) is introduced to overcome the redundancy problem of CWT. The approach is to scale and translate the wavelets in discrete steps as given in equation

$$DWT(\tau_0, s_0) = \frac{1}{\sqrt{s_0^f}} \int_{-\infty}^{\infty} f(t)\, \psi\left(\frac{t - k\tau_0 s_0^f}{s_0^f}\right) dt$$

Where s_0^f is the scaling factor, τ_0 is the translating factor, k and j are just integers. By applying DWT, the Frame is actually decomposed into four sub-bands corresponding to different resolution levels and orientation.

6. 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.[16]

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.

This algorithm is one of the most widely used one for frame feature extraction. SIFT extracts frame features, that are stable over frame translation, rotation and scaling and somewhat invariant to changes in the illumination and camera viewpoint[16].

The SIFT algorithm has four major phases
a) Extrema Detection
b) Keypoint Localization
c) Orientation Assignment
d) Keypoint Descriptor Generation.

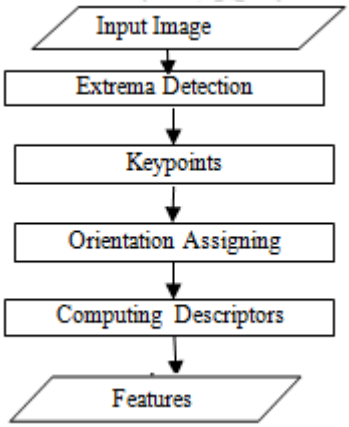


Figure 1.4: Major phases of the SIFT algorithm

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

7. Proposed Work

The major improvement in this work is to detect the forgery part with the help of Key point features and the optical flow algorithm. The optical flow algorithm is the existing algorithm and we have to modify the existing algorithm with the help of DWT and the Sift and Optical flow. 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.

8. Methodology of Work

In methodology section the flowchart of proposed protocol is discussed as in figure 4. It started with the MATLAB toolbox. In which the forgery video is taken as the input video. After that the frame separation is applied to separate the frames of the video. When the frame is separated the optical flow is applied and DWT and Sift is applied to detect the forgery frame.

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 decompose the forgery video frame.
Step 9: Get the forgery video as output.
Step 10 : Get the different parameters.

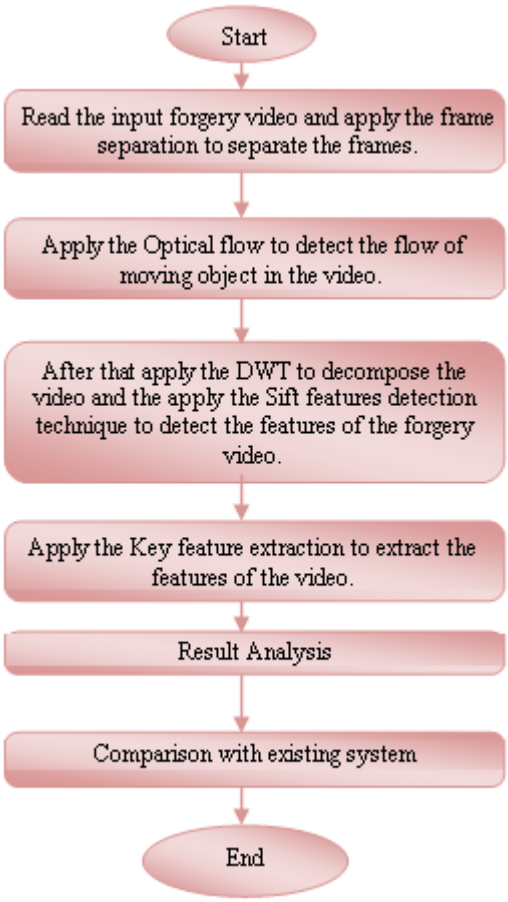


Figure 1.5: Flow chart of work planning

Figure 1.5 represents the flow chart for purposed work that has been done for forgery detection using optical flow, SIFT and DWT. In the forgery detection system first the forgery video is taken as the input video. After that the frame separation is applied to separate the frames of the video. When the frame is separated the optical flow is applied to detect the motion of the input frame of the video. The ROI algorithm is applied to detected the forgery part of the video frame with the help of input video frame. The after that DWT and Sift is applied to detect the forgery frame with compression because some time video is compressed so that the lay man is unable to identify the forgery frame. That is why DWT and Sift is merged and forgery part is detected. After that the Sift feature is used to detect the features of input frame and the forgery frame to identify the forgery part. After that Parameters are calculated

9. Results

We applied our method and the method in [8] to 10 pairs of forged and original videos from REWIND dataset. The result of 07_forged video.avi is showned. After detecting the forgery region parameters are calculated. Each and every window displays the different outputs of the research problems that is defined in the problem formulation. In[8] manually designed an ROI mask for each video sequence but we designed ROi part automatically not manually .The Snap shorts for the result are given below :

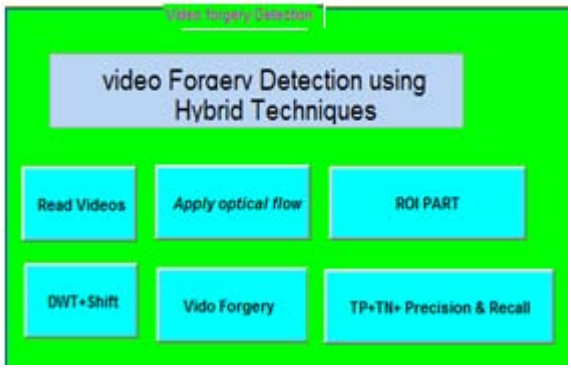


Figure 1.6: Input window of the work

The figure 1.6 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.

Optical flow

The figure 1.7 is the detection of the optical flow on the input forgery frame. when is input frame is processed with the help of frequency and the pixel value. Then the flow of the moving objects the detected. It is processed from the minimum point to the maximum point of the frame.

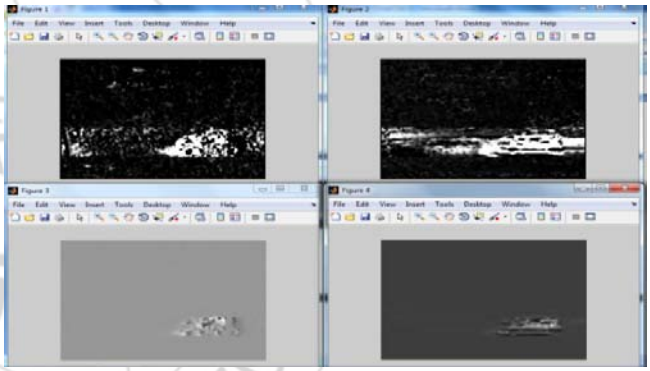


Figure 1.7: Optical flow on the input frame

ROI Mask

In the figure 1.8. The original frame and the forgery frame is processed with ROI algorithm and the forgery part of the video frame is detected.

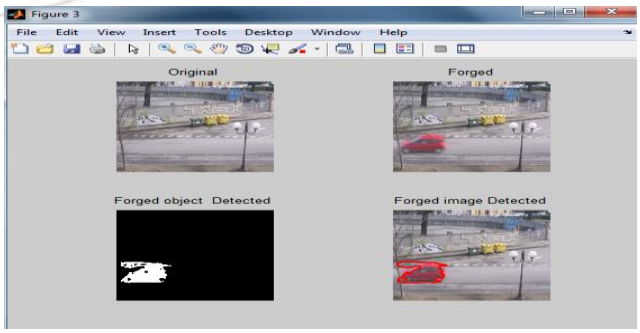


Figure 1.8: ROI mark on the forgery frame

DWT and SIFT Results

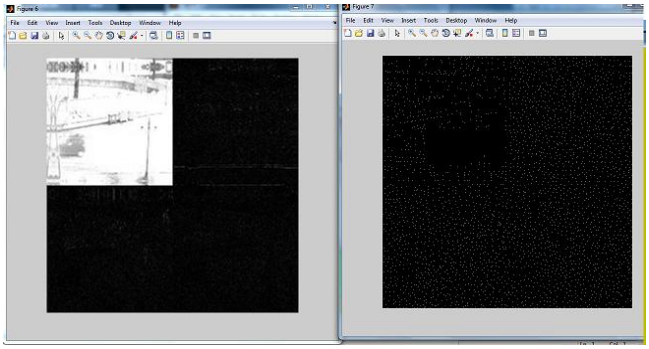


Figure 1.9: Result of dwt and sift

10. Performance Evaluation Parameters

Precision (p): Precision denotes the probability that a detected forgery is truly a forgery. It is denoted by symbol ***p***. It can be calculated as below:

$$p = \frac{TP}{TP+FP}$$

Recall (r): Recall shows the probability that a forged frame is detected. Recall is also known as True Positive Rate. It is denoted by symbol ***r.*** It can be calculated as below:

$$r = \frac{TP}{TP+FN}$$

Where

TP (True Positive): is the number of tampered pixels, which are classified as tampered.

FN (False Negative): is the number of tampered pixels, which are classified as authentic.

TN (True Negative): is the number of authentic pixels, which are classified as authentic

FP (False Positive): is the number of authentic pixels, which are classified as tampered.

Table 1: Comparison table for parameters

S. No	Video name (REWIND Dataset)	Existing Work			Proposed Work		
		Precision	Recall	Accuracy	Precision	Recall	Accuracy
1	Moving car.avi	98.2143	81.1475	95.1608	99.2454	65.1630	97.8587
2	Swimming ducks.avi	97.4153	69.2531	86.3612	98.7184	53.4027	89.5725
3	Cup and elephant.avi	97.3121	51.6820	91.9451	99.1304	46.1734	94.6541
4	Moving ball.avi	96.4537	74.5903	93.1073	97.9489	61.0458	95.5904

Comparison of Proposed Method with Existing Method in [8]

Table 2: comparison table for Proposed and existing work

S. No	Video name (REWIND Dataset)	Total No of Frame	Existing Work[1]			Proposed Work		
			Original Detected	Forged Detected	Percent age	Original Detected	Forged Detected	Percent age
1	Moving car.avi	412	369	43	10%	350	62	15%
2	Swiming ducks.avi	209	160	49	23%	152	57	27%
3	Cup and elephant.avi	261	210	51	19%	196	65	24%
4	Moving ball.avi	329	282	47	14%	270	63	19%

11. 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. In this dissertation, we propose several new digital forensic techniques to detect evidence of editing in digital multimedia content. We use Optical flow, DWT and different filters for forensic tasks such as identifying cut-and-paste forgeries from JPEG compressed videos and SIFT. This SIFT based technique is dependent on feature extraction by using key point detection. This strategy is for the most part used to Location of vindictive control with computerized recordings (advanced frauds) if there should arise an occurrence of duplicate move assault. The proposed work has been discovered viable result as correlation with leaving model. In leaving model 98.2143 exactness quality is figured while in proposed model we get the estimation of precision 99.2454.The proposed model get more phony Frame when contrasted with exiting model.

12. Future Work

In future, some other techniques can be used to detect forgery from videos so as to validate other methodologies with present technique. 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] 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.

[2] P.Kakar and N.Sudha "Exposing Post processed Copy-Paste Forgeries through Transform-Invariant Features", vol. 206, no. 1-3, pp. 178–184, 2011.
[3] S.Bayram,H.T.Sencar and N.Menon"A Survey of Copy-Move Forgery Detection Techniques", submitted to ICASSP 2009, 2009.
[4] 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.
[5] 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.
[6] M.Wu A. Swaminathan and K. J. Ray Liu, "Video tampering identification using blind deconvolution," Proc. IEEE ICIP, 2006.
[7] M.C.Stamnn,"Forensics Detection of Video Manipulation Using Statistical Intrinsic Fingerprints", IEEE Transactions on information Forensics And Security , vol. 5 No 3, 2010.
[8] Amir Bidokhti , Shahrokh Ghaemmaghami , " Detection of Regional Copy/Move Forgery in MPEG Videos using Optical Flow" AISP 2015 IEEE
[9] M. Chen, J. Fridrich, M. Goljan, and J. Luká˘s, "Determining video origin and integrity using sensor noise," IEEE Trans. Inf. Forensics Security, vol. 3, no. 1, pp. 74–90, Mar. 2008.
[10] T.-T. Ng, S.-F. Chang, J. Hsu, L. Xie, and M. P. Tsui, "Physics-motivated features for distinguishing photographic videos and computer graphics," in Proc. ACM Multimdedia, Singapore, 2005, pp. 239–248.
[11] 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.
[12] 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.
[13] T.-T. Ng, S.-F. Chang, and Q. Sun, "Blind detection of photomontage using higher order statistics," in Proc. IEEE Int. Symp. Circuits, May 2004, vol. 5, pp. V-688–V-691.
[14] S. Bayram, I.Avcibas, B. Sankur, and N. Memon, "Video manipulation detection," J. Electron. Imag., vol. 15, no. 4, p. 041102, 2006.
[15] 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)
[16] D. G. Lowe, "Distinctive Image Features from Scale-Invariant Keypoints," Interna-tional Journal of Computer Vision, vol. 60, no. 2, pp. 91–110, Nov. 2004.
[17] Zhang, J., Su, Y., and Zhang, M., "Exposing Digital Video Forgery by Ghost Shadow Artifact," in *Proc. MiFor'09,* October 23, 2009, pp. 49-53.
[18] A. Graps, "An Introduction to Wavelets," IEEE Computational Sciences and Engineering, vol. 2, no.2, pp 50-61, 1995.
[19] Weihong Wang, Hany Farid, "Exposing Digital Forgeries in Video by Detecting Double MPEG Compression" MM&Sec'06, September 26–27, 2006, Geneva, Switzerland.
[20] Weihong Wang, Hany Farid, "Exposing Digital Forgeries in Video by Detecting Double Quantization" MM&Sec'09, September 7–8, 2009, Princeton NJ, USA.
[21] Yongjian Hu1,2, Yufei Wang2, Bei-bei Liu2, "An Improved Fingerprinting Algorithmfor Detection of Video Frame Duplication Forgery" International Journal of Digital Crime and Forensics 2011.
[22] Yuxing Wu, Xinghao Jiang, Tanfeng Sun and Wan Wang, "Exposing video inter frame forgery based on velocity field consistency." 2013 IEEE International Conference on Acoustic, Speech and Signal Processing (ICASSP) pp. 393-397.