IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

Video Forgery detection using Hybrid techniques

Randeep Kaur[1], Er. Jasdeep Kaur[2]

CSE Department, GZS PTU Campus, Bathinda[1, 2]

Abstract: Digital video forensics aims at validating the authenticity of videos by recovering information about their history. In a copy-paste forgery, a region from a video is replaced with another region from the same video. 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. In this paper DWT is used to compress the frame 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 frame and the forgery frame.

Keywords: Frame, Video, forgery, DWT and SIFT 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 Figure 1.1. Active video

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

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.

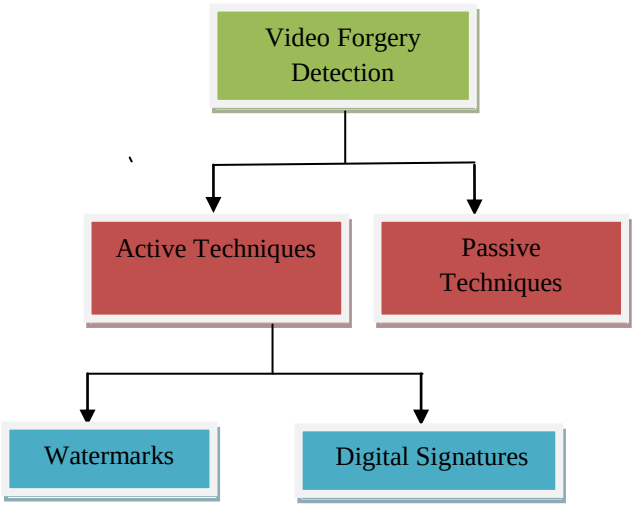

Figure 1.Approaches to Video Forgery Detection [2]

III. INTRODUCTION TO SCALE INVARIANT FEATURES TRANSFOR (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 key points 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 key points 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 hashtable implementation of the generalized Hough transform. Each cluster of 3 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].

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

V. PROBLEM FORMULATION

Digital video forensics aims at validating the authenticity of videos by recovering information about their history. 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. Due to the availability of higher solution digital cameras, hi-tech personal computers, powerful software and hardware tools in the video editing and manipulating field, it become possible for someone to create, alter and modify the contents of a digital video and to violate its validation. Fake videos are many times used to publicize in social Medias and news papers. Many cases are noted in regard to the defaming business as well as political leaders by using fake photos and videos. The problem of detecting if a video has been forged is investigated; in particular, attention has been paid to the case in which an area of an video is copied and then pasted onto another zone to create duplication or to cancel something that was awkward.

The photomontage detection problem, one of the fundamental tasks is the detection of video splicing. Video splicing assumes cut and paste of video regions from one video onto another video. 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. This thesis discusses the copy paste forgery detection in videos using Statistical fingerprints.

VI. 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.

VII. METHODOLOGY OF WORK

In methodology section the flowchart of proposed protocolis discussed as in figure 1.

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.

VIII. 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 reduce the replication and noise.
Step6: Apply optical flow to detect the forgery frame.
Step7: Apply ROI mask to detect the forgery frame.
Step8: Apply DWT to compress the forgery video frame.
Step 9: Apply shift to matching the feature points in forgery frames.
Step 10: Get the forgery video as output.
Step 11: Get the different parameters.

IX. RESULTS AND DISCUSSION

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 2. Input window of the work

The figure 2: 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.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

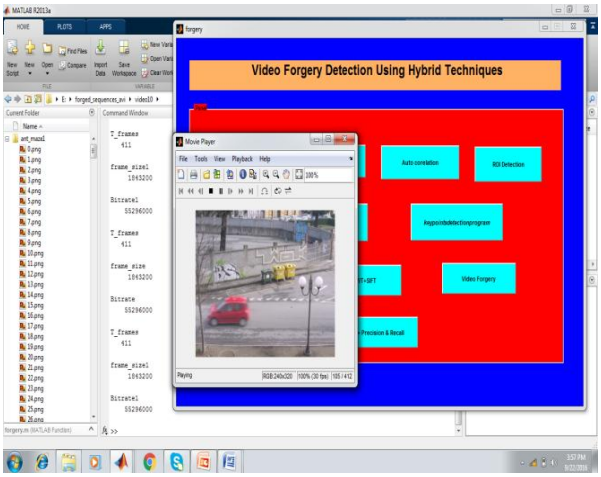

Figure 3: Read the input video

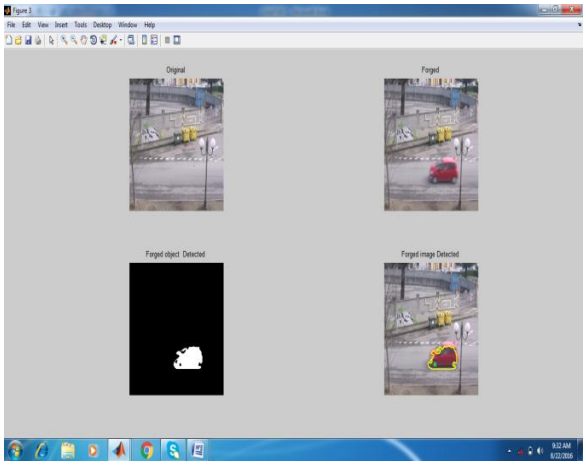

Figure 5: ROI mark on the forgery frame

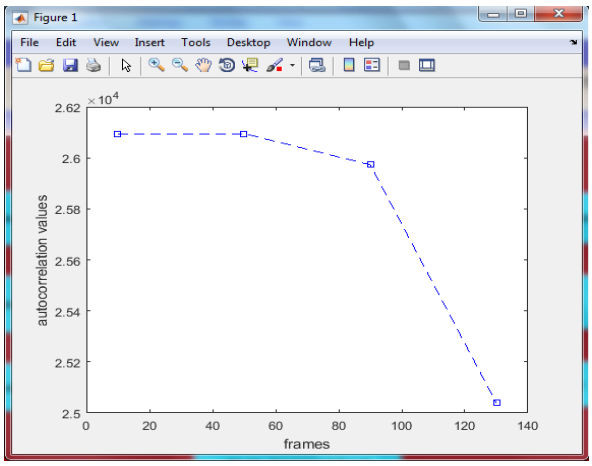

Figure 4: Auto Correlation Graph

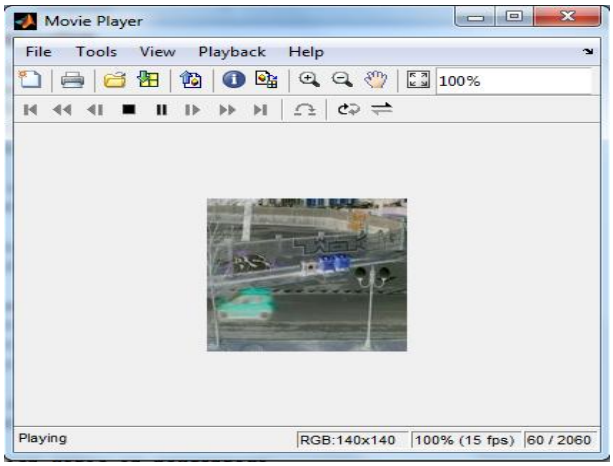

Figure 6: Detection of forgery in video

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
380.png	1455	380.png	1455
410.png	1572	410.png	1572

Table .2 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
5	06_Original.avi	261	250	11	200	61
6	01_Original.avi	209	200	09	180	29

DOI 10.17148/IJARCCE.2016.51221

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

Table 3 Parameter Table

S. No	Video Name (Rewind Dataset)	Old			New		
		Precision	Recall	PSNR	Precision	Recall	PSNR
1.	07_forged.avi	0.40	1.00	34.0	0.50	1.00	50.1
2	09_forged.avi.	0.35	1.00	34.1	0.48	1.00	55.4
3	06_forged.avi	0.25	1.00	36.2	0.40	1.00	48.25
4	01_forged.avi	0.41	1.00	35.2	0.44	1.00	41.58
5	02_forged.avi	0.35	1.00	37.0	0.58	1.00	50.1
6	03_forged.avi	0.31	1.00	34.0	0.61	1.00	49.25
7	04_forged.avi	0.46	1.00	33.8	0.59	1.00	48.95
8	05_forged.avi	0.41	1.00	37.9	0.48	1.00	53.55
9	08_forged.avi	0.32	1.00	35.4	0.49	1.00	55.12
10	10_forged.avi	0.39	1.00	37.0	0.55	1.00	54.01

X. CONCLUSION

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.The Digital videos are usually compressed with MPEG-x or H-26x coding standard. The tampering has to be accomplished in uncompressed domain in order to perform the operations such as frame deletion, frame insertion and many more. Considering facts that include size and format, tempered video has to be encoded. Thus, the occurrence of double compression may expose digital forgery. 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 this dissertation, we propose several new digital forensic techniques to detect evidence of editing in digital multimedia content. In this work I have used the optical flow to detect the video forgery with the Region of interest algorithm. We use DWT method for dimensionality reduction of video frames. For the verification and authenticity the SIFT is used to detect the key feature points on the video and some important features of the videos. In this work precision, recall and PSNR is calculated. The value of precision is 61%, and PSNR is 56% in our algorithm.

XI. 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 can be applied like DCT, correlation and filters.

It can also extended on the real time crime department videos. So that the criminal will be easily identified. It can also extended with the help of Other techniques so that the better results may be produced.

REFERENCES

[1]. A merini, I., Barni, M., Caldelli, R., and Costanzo, "Counter-forensics of SIFT-based copy-move detection by means of key point classification", EURASIP Journal on Image and Video Processing, volume -18, page no-101-105, 2013.
[2]. A.C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling", IEEE Transactions on Signal Processing, volume- 53, page no. 758–767, 2005.
[3]. Chen, L., Lu, W., and Ni, J, "An Image Region Description Method Based on Step Sector Statistics and its Application in Image Copy-Rotate/Flip-Move Forgery Detection", International Journal of Digital Crime and Forensics (IJDCF) , volume -4, page no. 49-62,2013.
[4]. Chen, L., Lu, W., Ni, J., Sun, W., and Huang, J. (2013). "Region duplication detection based on Harris corner points and step sector statistics", Journal of Visual Communication and Image Representation, Volume-24, page no. 244-254, 2013
[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), Volume-31, 2012
[6]. Liu, G., Wang, J., Lian, S., & Wang, Z, " A passive image authentication scheme for detecting region duplication forgery with rotation", Journal of Network and Computer Applications, Volume-34, page no.1557-1565, 2011.
[7]. Liu, M.-H., & Xu, W.-H, " Detection of copy-move forgery image based on fractal and statistics", Journal of Computer Applications, Volume-8, 2011.
[8]. M. Chen, J. Fridrich, M. Goljan, and J. Luká˘s, "Determining image origin and integrity using sensor noise", IEEE Trans. Inf. Forensics Security, Volume-3, page no. 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, Volume-43, page no. 1–10, 2005.
[10]. M. K. Johnson and H. Farid, "Exposing digital forgeries in complex lighting environments", IEEE Trans. Inf. Forensics Security, Volume-2, page no.450–461, Sep. 2007.
[11]. M.C. Stamnn, "Forensics Detection of Image Manipulation Using Statistical Intrinsic Fingerprints", IEEE Transactions on information Forensics And Security, Volume-5, 2010.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

[12]. M.K. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting", Proc. ACM Multimedia and Security Workshop, New York, page no. 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, "Bibliography on blind methods for identifying image forgery", Signal Processing Image Communication, Volume-25, page no.389-399, 2010.
[15]. Math, S., & Tripathi, R, "Digital Forgeries: Problems and Challenges", International Journal of Computer Application, Volume-5, 2010.
[16]. Muhammad, G., Hussain, M., Khawaji, K., and Bebis,G, "Blind copy move image forgery detection using dyadic undedicated wavelet transform" Paper presented at the Digital Signal Processing (DSP),2011.
[17]. P.Kakar and N.Sudha "Exposing Post processed Copy-Paste Forgeries through Transform-Invariant Features", Volume-206, page no. 178–184, 2011.
[18]. Pan, X. Z., and Wang, H. M, "The Detection Method of Image Regional Forgery Based DWT and 2DIMPCA", Advanced Materials Research, Volume-532, page no.692-696, 2012.
[19]. Piva, A, "An Overview on Image Forensics", ISRN Signal Processing, 2013.
[20]. Pujari, V. S. and Sohani, M., "A Comparative Analysis on Copy Move Forgery Detection in Spatial Domain Method Using Lexicographic and Non Lexicographic techniques" IJECCE, Volume-3, page no. 136-139, 2012.
[21]. Pujari, V. S., & Sohani, M, "A Comparative AnalysisOn Copy Move Forgery Detection Using Frequency Domain Techniques", International Journal of Global Technology Initiatives, Volume-1, page no.104-111, 2012.
[22]. S. Bayram, I.Avcibas, B. Sankur, and N. Memon, "Image manipulation detection", J. Electron. Imag., Volume- 15, page no. 041-102, 2006.
[23]. S.Bayram, H.T.Sencar and N. Menon, "A Survey of Copy-Move Forgery Detection Techniques", submitted to ICASSP, 2009.