ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 7, July 2016

# A Survey study on video forgery detection using scale invariant feature detection Technique and DWT

*Gurjinder Kaur[1], Rishamjot Kaur[2]*

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

*2 Asst.Prof. Department of information technology & Engineering, Baba Farid College of Engineering and Technology, Deon, Bathinda, India*

***ABSTRACT*: In this paper we present the use of digital transmission content like pictures and video has raised, that the incentive to make digital forgeries. Presently, powerful redaction package permits forgers to make perceptually convincing digital forgeries. Consequently, there's a good would like for techniques capable of authenticating digital transmission content. In response to the current, researchers have begun developing digital rhetorical techniques capable of distinguishing digital forgeries. These rhetorical techniques operate by detection imperceptible traces left by redaction operations in digital transmission content. during this we have a tendency to propose many new digital rhetorical techniques to discover proof of redaction in digital transmission content. We use DWT, shift and completely different filters for rhetorical tasks like distinguishing cut-and-paste forgeries from videos frames. in addition, we have a tendency to contemplate the matter of transmission security from the forger's purpose of read. we have a tendency to demonstrate the technique that's accustomed discover the copy paste half from the color image. During this tempered image is their that's accustomed discover the temper image and calculate the frames and their PSNR values.**

**Keywords: Copy –paste , forensics , video, DWT etc.**

## 1.INTRODUCTION

The across the board accessibility of the Internet, combined with the effortlessly accessible video and video catching gadgets, for example, low-value cameras, computerized camcorders and CCTVs have ended up basic part of the general public. Advancements in visual (video) innovations, for example, pressure, transmission, stockpiling, recovery, and video-conferencing have encouraged from multiple points of view to the general public. In the financial learning and experimental advancement, the recordings and recordings accessible at different video sharing and person to person communication sites (like YouTube, Face Book, and so on.) are assuming a huge part. Other than this, different applications such as diversion industry, video reconnaissance, lawful proof, political recordings, video instructional exercises, promotions, and so on imply their exceptional part in today's setting [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 falsifier can deliberately control genuine (real or unique) recordings to make altered or doctored or fake recordings for negligence [1-3]. This thus implies the recordings and recordings that are found in broad communications, for example, TV, mainstream Internet sites, for example, YouTube, might have been altered and the aphorism "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. [04] Hence, however the recordings and recordings from cameras, computerized camcorders and CCTVs can serve as effective "confirmations" in both lawful courts and popular feeling, it is critical to ask whether the recordings and recordings created by these gadgets are really real and has not been messed around with. Simple accessibility of numerous modern video altering apparatuses gives a stage to falsifier to control genuine recordings and make perceptually vague fake recordings. Along these lines, in numerous genuine situations such as court trials, law implementation, criticism, legislative issues, and guard arranging, and so on validness of introduced video should be inspected. Criminological devices and specialists assume a key part to analyze the genuineness of recordings by distinguishing hints of altering. Here, achievement or disappointment of instruments and specialists relies on upon how insightfully altering has been done by the counterfeiter. It is troublesome for legal specialists to recognize messing with recordings if there are no (or little) follows left by counterfeiter while altering. Sadly, because of absence of built up techniques to inspect the realness of recordings, location of messing around with recordings have postured challenges before mainstream researchers, and its earnestness in numerous situations (e.g. recordings as proof amid court trials) looks for quick consideration. This paper takes the survey of different techniques that have been recommended in writing to identify the fabrication or altering in video.


***Figure 1:** Example of original and forged of video [1]*

## 2.TAMPERING OF VIDEO

Video signs are spatial-worldly flags or essentially expressed an arrangement of time differing recordings. The data they pass on is "visual". A monochromatic still video can be numerically spoken to by x (h, v), where x is the force esteem at the even 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 even, v vertical and t transient areas individually. Video altering is generally new territory when contrasted with video doctoring as it is as old as the craft of photography itself where we have various occurrences of genuine instances of fake photos [04]. Altering the advanced video is only adjusting or changing the substance of recordings. This should be possible by different techniques which are exhibited in taking after subsections. While altering a video, target of a counterfeiter is to make an altered or doctored or fake video from genuine or real or unique video.[20] 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 zones where these altered recordings are exhibited as proof to delude the court procedures. Hence, at whatever point recordings are exhibited as proof amid court trials, their credibility are to be analyzed before considering them as confirmation [04].

### 2.1. Treating Attacks in Video

At the point when a malevolent adjustment is performed on a video arrangement, it either assaults on the substance of the video (i.e. visual data exhibited by the casings of the video), or assaults on the transient reliance between the edges. In this way in light of the territorial property of the video successions, we can comprehensively group the video altering assaults into three classes: spatial altering assaults, transient altering assaults and the mix of these two, Spatio-worldly altering assaults [04] [05].

a) Spatial Tempering A falsifier can alter source recordings spatially by controlling pixel bits inside of a video outline or in contiguous video outlines. The operations that should be possible as altering assault in spatial altering are editing and substitution, transforming, content (article) including and uprooting and so forth. These assaults can be productively performed with the assistance of video altering programming, for example, Photoshop.

b) Temporal Tempering This sort of control is done on the succession of casings. Fleeting altering assaults are for the most part influencing the time succession of visual data, caught by video recording gadgets. The regular assaults in worldly altering are edge expansion, outline evacuation and casing reordering or rearranging.

c) Spatio-Temporal Tempering Spatio-fleeting altering assaults are the blend of the both sorts of altering assaults. Outline groupings are changed and in addition visual substance of the edges are altered in the same video. [04][05]

### 2.2. Levels of Tempering Attacks

Also of these sorts of altering assaults, altering should be possible at various levels in video arrangements.

a) Shot Level Tampering At the scene level, a whole scene of a video is controlled like cancellation of a video scene (i.e. scene or shot cut), duplicating of a video scene to somewhere else, and so on. It should be possible utilizing either spatial or fleeting treating[21].

b) Frame Level Tampering In this assault, the control is done on casings of the video. The falsifier might evacuate the casings, include the edges, reshuffle the grouping of edges, and copy the edges from an offered video to adjust the substance of video. This should be possible utilizing transient treating.

c) Block Level Tempering In this kind of assault, the substance of the video casings are dealt with as squares on which the altering assaults are connected. Hinders (a predefined region on the casing of the video) can be trimmed and supplanted, transformed or adjusted in any capacity in square level altering. Spatial altering assaults are regularly performed at piece level.

d) Pixel Level Tempering In pixel level altering, substance of the video edges are changed at pixel level. The video validation framework ought to be sufficiently powerful to separate the typical video handling operation and pixel level altering, since numerous ordinary video preparing operations are performed at pixel level. Spatial altering assaults are normally performed at pixel level. [04][05]

## 3. LITERATURE REVIEW

Several reviews of the literature on video retrieval have been published, from a variety of different viewpoints.

**Tushant A. Kohale[2014]** said that contemplated Digital recordings are the most imperative wellspring of data exchange. The accessibility of capable advanced video handling software's, makes it moderately simple to make computerized falsifications from one or different recordings. In today's reality it is adding so as to anything but difficult to control the video or expelling a few components from the video which bring about a high number of video fabrications. A duplicate move fabrication is made by replicating and gluing content inside of the same video, and possibly post-working it. The identification of duplicate move frauds has ended up a standout amongst the most effectively investigated subjects in visually impaired video legal sciences. The key goals of the proposed methodology is to ponder the impact of various sorts of altering on the computerized

video, recognize video fabrication by duplicate move under numerous sorts of assaults by consolidating piece based and highlight based strategy and precisely finding the copied region[16].

**Salma Amtullah[2014]** conclude that contemplated Tampering in computerized recordings has turned out to be simple because of the accessibility of cutting edge video altering programming's to the clients. Recordings are being altered in an extremely effective way without leaving any visual piece of information. As a result, the substance of advanced recordings can't be underestimated as. There are different sorts of video altering strategies. A standout amongst the most widely recognized altering methods is duplicate move fraud. In duplicate move phony one part of a video is replicated and glued in another part of the same video. In this paper, the aloof video scientific technique is introduced to identify duplicate move fabrication in computerized recordings. The proposed strategy depends on SURF (Speed Up Robust Features) calculation. In this strategy the elements are extricated and their descriptors are acquired by SURF calculation and the Nearest Neighbor methodology is utilized for highlight coordinating to distinguish the duplicate move fabrication in advanced recordings. This recognition technique is observed to be turn and scale invariant and is sufficiently vigorous to commotion, jpeg pressure and obscuring. Numerous duplicate move fabrication is additionally identified by this method[15].

**I. Amerini[2011]** proposed that One of the foremost issues in video crime scene investigation is figuring out whether a specific video is bona fide or not. This can be a significant undertaking when recordings are utilized as fundamental confirmation to impact judgment like, for instance, in a court of law. For the most part, to adjust the video patch to the new setting a geometric change is required. To identify such adjustments, a novel system in light of scale invariant components change (SIFT) is proposed. Such a strategy permits us to both comprehend if a copy–move assault has happened and, moreover, to recoup the geometric change used to perform cloning. Broad exploratory results are displayed to affirm that the strategy can decisively individuate the modified region and, also, to gauge the geometric change parameters with high dependability. The strategy additionally manages numerous cloning.

**P.Kakar[2012]** said that Video manipulation has become commonplace with growing easy access to powerful computing abilities. In this paper, the author propose a novel technique based on transform-invariant features. These are obtained by using the features from the MPEG-7 video signature tools. Results are provided which show the efficacy of this technique in detecting copy-paste forgeries, with translation, scaling, rotation, flipping, lossy compression, noise addition and blurring. We obtain a feature matching accuracy in excess of 90% across post processing operations, and are able to detect the cloned regions with a high true positive rate and lower false positive rate than the state of the art[2].

**S.Bayram[2006]** conclude that A part of the video is duplicated and glued on another part for the most part to hide undesirable bits of the video. Henceforth, the objective in discovery of duplicate move imitations is to recognize video regions that are same or to a great degree comparable. In this paper, the creator audit a few techniques proposed to accomplish this objective. These strategies all in all utilization piece coordinating methodology, which first partition the video into covering squares and concentrate highlights from every square, accepting comparable pieces will yield comparative components. Later, a coordinating step happens where the point is to discover the copied pieces in view of their element vectors. A falsification identification choice is made just if comparative components are recognized inside of the same separation of elements related to associated pieces. The creator inspect a few diverse square based components proposed for this reason in connection to their time intricacy and heartiness to normal preparing scaling up/down, pressure, and rotation[3].

**A.N.Myna[2010]** conclude that after effect of intense video handling devices, advanced video falsifications have as of now turned into a genuine social issue. In this paper he depict a powerful strategy to recognize Copy-Move phony in advanced recordings. Our method works by first applying DWT (Discrete Wavelet Transform) to the information video to yield a diminished dimensional representation. At that point the packed video is isolated into covering squares. These pieces are then sorted and copied squares are recognized utilizing Phase Correlation as closeness model. Because of DWT use, location is initially completed on most minimal level video representation. This methodology radically lessens the time required for the location process and expands exactness of recognition procedure.

**M.C.Stammn [2010]** said that the utilization of advanced recordings has expanded, so has the methods and the motivating force to make computerized video phonies. In like manner, there is an awesome requirement for advanced video scientific methods fit for distinguishing video changes and produced recordings. Various video handling operations, for example, histogram evening out or gamma amendment, are comparable to pixel esteem mappings. In this paper, the creator demonstrate that pixel esteem mappings desert factual follows, which we should allude to as a mapping's characteristic unique mark, in a video's pixel esteem histogram. At that point they propose criminological strategies for distinguishing general structures all inclusive and privately connected differentiation improvement and a technique for recognizing the utilization of histogram leveling via hunting down the recognizing components of every operation's inborn unique mark. Moreover, we propose a technique to distinguish the worldwide expansion of commotion to a formerly JPEG-packed video by watching that the inherent unique mark of a particular mapping will be modified on the off chance that it is connected to a video's pixel values after the expansion of noise[7].

**Dhara Anandpara[2012]** proposed that With appearance of numerous capable altering instruments in the computerized video preparing, video phony is the huge concern today in Digital Forensics Industry. Video falsification can be apply either in single video by adapting some locale of video and sticking it to somewhere else in the same video or in composite video by joining two or more recordings together. The center of my examination work is to build up a criminological framework to recognize both sort of imitation inside of a solitary spot. Numerous Copy-move Forgery Detection (CMFD) calculations have been produced to recognize falsification inside of single video however are not vigorous to geometric change. Twofold JPEG pressure is utilized broadly for restriction of areas for composite recordings fraud, for example, Video Slicing, In-painting and so on. A proposed framework is a combination based framework which will permit to distinguish the video altering utilizing both strategies i.e. CMFD and DJPG. This gives bits of knowledge of utilizing both video location calculations inside of same video and in single system with the goal that discovery is apparent at single spot. A framework will process a probability guide to show the produced region that is collected because of Copy. To lessen computational expense of framework components are extricated from taking the mean estimation of DCT (discrete cosine change) coefficients. The proposed plan is vigorous to duplicate move fabrication, as well as to obscuring or nosing including and with low computational complexities[14].

**Govindraj Chittapur[2014]** proposing legal methods that are fit for recognizing hints of altering in advanced Video without specific equipment. These strategies work under The supposition that video contain actually tampering so as to happen properties which are aggravated, and which can be quantifed, measured, and used to uncover video fakes. In this connection we are proposing systems utilized as a part of duplicate glue and duplicate move interweaved video outlines utilizing factual mean comparision.These procedures give a significant measurable strategies to validating computerized video.[17]

**Mrs. J.D. Gavade [2015]** said that computerized innovation has ended up dominating innovation for making, handling, transmitting and putting away data in different structures, for example, sound, video, content and picture all together we can call it as sight and sound information. With the advancements and improvement in modern video altering innovation and a far reaching utilization of video data and administrations in our general public, it is turning out to be progressively noteworthy to guarantee the dependability of video data. In this manner in reconnaissance, medicinal and different fields, video substance must be secured against endeavor to control them. Such pernicious modifications could influence the choices in light of these recordings. As video altering systems are getting extremely muddled, adjusted recordings are difficult to distinguish. Notwithstanding, when a video is adjusted, some of its fundamental properties get changed. At that point to recognize those progressions which is additionally called as phony recognition, it is expected to utilize complex video handling procedures and calculation. This paper presents survey of the different existing strategies in writing, that are utilized to discover whether the video is genuine one or not.[18]

## 4. PROBLEM FORMULATION

Computerized video crime scene investigation goes for recovering so as to accept the validness of recordings data about their history. Duplicate glue imitation, wherein an area from a video is supplanted with another locale from the same video (with conceivable changes). Since the replicated part originate from the same video, its essential properties, for example, commotion, shading palette and composition, will be perfect with whatever is left of the video and accordingly will be more hard to recognize and distinguish these parts. Advanced video criminology is a fresh out of the plastic new research field which goes for recovering so as to approve the credibility of recordings data about their history. Because of the accessibility of higher arrangement advanced cameras, hello there tech PCs, capable programming and equipment devices in the video altering and controlling field, it get to be feasible for somebody to make, change and adjust the substance of a computerized video and to damage its approval. Fake recordings are commonly used to advance in social Medias and news papers. Numerous cases are noted with respect to the using so as to criticize business and political pioneers fake photographs and recordings. The issue of distinguishing if a video has been manufactured is explored; specifically, consideration has been paid to the case in which a zone of a video is replicated and after that glued onto another zone to make duplication or to cross out something that was ungainly. The photomontage recognition issue, one of the key undertakings is the discovery of video grafting. Video grafting expect cut and glue of video areas from one video onto the another video. The central issues which examine found in the writing can be arranged into the regular, phony discovery, stream mapping, and source distinguishing proof. In this way, the creativity and genuineness of recordings or information much of the time get to be testing issue. Scientists have related the normal issues to the development in PC representation, activity, sight and sound in the relationship of high figuring machines, calculations, builds the many-sided quality of the issue.

## 5. DETECTION OF COPY–MOVE FORGERY

Another basic sort of video falsification is the duplicate move altering. It alludes to the kind of fraud where a part of the casing is replicated and glued into another part, with the reason for including or erasing an item in the video outline. A few strategies are utilized for the location of this fabrication and every one of them rely on upon the presumption that a duplicate move imitation brings noteworthy relationship between's the source outlines and copied ones. A technique that identifies twofold quantization coming about because of twofold MPEG

pressure in computerized video was proposed by Wang et al. [6]. They computed the contrasts between the relating transient and spatial area connection frameworks. As needs be, high relationship empowers the technique to identify profoundly limited altering in districts aslittle as 16X16 pixels with a normal rate of 99.4% with standard deviation.

Table 1: Multi Frequently Happened In Spatio-Temporal Visual Copy–Move On Web Videos. Parameters Are Chosen To Simulate The Real Cases

| | Attacks (Transformations) | Comment & Parameters |
|---|---|---|
| Spatial domain | Gamma | Change gamma factor for each channel |
| | Color | Change the colour of each frame |
| | Gray | Turn the frames into grey |
| | Blur | Blur the frames with Gaussian radius-2 |
| | Contrast | Increase or decrease contrast by 20% |
| | Change of Ratio | Change the ratio from full screen to 4:3 |
| | Noise | Pepper and salt noise |
| | Shift | Horizontal shift the frames by 10% |
| | Flip | Horizontal mirroring of the frames |
| | Scale | Zoom 1.2 or 0.8 with black window |
| | Picture in picture | Place scaled frames into another video |
| | Cam-cording | Angle of the cam changed |
| | Patterns insertion | Insertion of a small logo or subtitles |
| | Letter-box | Black bands on top and bottom |
| | shadow | shadow pixels as background |
| Temporal domain | Frame dropping | Drop frames after re-encoding or add frame |
| | Slow motion | Half the speed |
| | Fast motion | Double speed |
| | Frame rate | 25 to 15 fps |
| | Frame histogram | detection technique |

Other authors developed a method to detect suspicious regions in video recorded from a static scene with the help of noise characteristics of the acquisition device described through a noise level function (NLF) in frame sequence. However, the performance of such a method considerably dips when conventional codec's like MPEG-2 compression is utilized, and this confines the methods practical applicability.

In this regard, copy-move transformations change the visual video appearance of frames in terms of brightness [9]. This work intends to conclude the copy-move attacks. Moreover, copy-move attacks are attributed to video as spatial and temporal copy-move forgery methods. The former is conceptually identical to the one in still image frames and involves the replication of a portion of the frame. On the other hand, the latter involves the replacement of some frames with a copy of prior ones, in order to delete something in the scene of the original video. Partial inter-frame attacks meanwhile, can be described as a portion of a group of frames replaced with the same part from a chosen video frame.

## 6. RESULTS AND DISCUSSION

## 7. CONCLUSION

Among the quickest developing zone of examination in the field of video falsification identification is the passive blind strategies and identification techniques to check the uprightness and genuineness of computerized video arrangement. To this end, current studies devoted to passive blind strategies are not needing earlier learning of the video outlines content or pre-inserted watermarks or mark. In this study, the issue of computerized video controlling discovery is talked about with references to visually impaired strategies for video fabrication identification. Different casings of video fabrication identification strategies are sorted and summed up in this paper and the rendering of some run of the mill video imitation identification calculations techniques are looked at. A portion of the created approaches for the recognition and the determination of video control are fit for restricting altered object areas of casings succession. This current study's discoveries are relied upon to add to techniques and thoughts in the field of advanced video phony detection. At the onset, the downside of existing strategies is identified with issues of mechanization such as human elucidation of poor yields. Another is the change and augmentation to decide the precise area of the video fabrication that includes strategies that embed/evacuate casings and articles to decide the area of inconsistencies .On the other hand, duplicate move fabrication confinement techniques that depend on edges are suitable with edge identification duplication and not the confinement of produced district on the off chance that the video substance is predictable and the former changed locale had lower quality casings than the current outline. In the setting of pixel-based methodologies, the control of location precision sways post processing furthermore, pressure and in this way making the approval of execution measures (i.e. precision, vigor, security) turns into a noteworthy concern attributable to the nonappearance of built up benchmarks what's more, open testing dataset that assesses the genuine exactness of computerized video phony methodologies. Among the critical restriction of video phony discovery techniques is their powerlessness to recognize between noxious control and blameless modifying, similar to red-eye adjustment. Future studies are urged to decide a more powerful factual component that are impervious to a few postprocessing operations.

## 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]. 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.
[9]. 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.
[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. 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.
[12]. T.-T. Ng, S.-F. Chang, and Q. Sun, "Blind detection of photomontage using higher order statistics," in Proc. IEEE Int. Symp. Circuits Systems, Vancouver, BC, Canada, May 2004, vol. 5, pp. V-688–V-691.
[13]. S. Bayram, I.Avcibas, B. Sankur, and N. Memon, "Video manipulation detection," J. Electron. Imag., vol. 15, no. 4, p. 041102, 2006.
[14]. 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.
[15]. Salma Amtullah, Dr. Ajay Koul " Passive Image Forensic Method to detect Copy Move Forgery in Digital Images" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XII (Mar-Apr. 2014), PP 96-104.
[16]. Tushant A. Kohale*, Prof. P. R. Lakhe " Detection of Postoperated Copy Move Image Forgery by Integrating Block Based and Feature Based Method" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014 ISSN: 2277 128X.
[17]. Govindraj Chittapur " DIGITAL DOCTORED VIDEO FORGERY DETECTION TECHNIQUES" International Journal of Advanced Technology & Engineering Research (IJATER) 3rd International e-Conference on Emerging Trends in Technology, ISSN No: 2250-3536 E-ICETT 2014.
[18]. Mrs. J.D. Gavade and Mrs. S.R. Chougule "Review of Techniques of Digital Video Forgery Detection" Advances in Computer Science and Information Technology (ACSIT)Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 3; January-March, 2015 pp. 233-236
[19]. Upadhyay, S. and Singh, S. K., "Video Authentication: Issues and Challenges," *International Journal of Computer Science Issues*, Vol. 9, Issue 1, No. 3, January 2012, pp. 409-418
[20]. Atrey, P. K., Yan, W. Q., Chang, E.C., and Kankanhalli, M. S., "A Hierarchical Signature Scheme for Robust Video Authentication using Secret Sharing," in *Proc. 10th International Multimedia Modeling Conference* (MMM'04), Jan 5-7, 2004, pp. 330-337.
[21]. Malekesmaeili, M., Fatourechi, M., and Ward, R. K., "Video Copy Detection Using Temporally Informative Representative Images," in *Proc. International Conference on Machine Learning and Applications* (ICMLA'09), Dec 13-15, 2009, pp. 69-74.