Detection of Video and Multimedia Copy-Move Forgery using Optical Algorithm and GLSM Clustering

Seemanthini.K, Manjunath S S, Raghuram A S, Sneha N P

***Abstract:** Digital Videos and multimedia copy-move forgery detection is a trending topic in multimedia forensics. Protecting videos and other digital media from tampering has become a cause of concern. Video copy-move forgery has increasingly become a type of cybercrime that is employed to using videos for various malicious purposes such as providing fake evidences in court rooms, spreading fake rumors, using it to defame a person. A lot of approaches have been proposed for detecting the traces left by any forgery caused due to the copy-move operation. In this paper, we conduct a survey on these existing approaches which are applied for the detection of copy –move videos and also for the identification forgery in the images. In some of the existing methods, the problem of copy-move video forgery has been addressed using different techniques. Techniques such as noise residue, motion and brightness gradients, optical flow techniques solve only part of the whole problem. This survey analyses the current solutions and what they offer to address this problem.*

***Keywords:** Noise residue , Copy-move forgery, optical flow, copy- move forgery, Motion brightness*

I. INTRODUCTION

The Rapidly growing different kinds of techniques and software used in digital images, videos and forgery like Light works, Adobe Premiere pro have led to the rise in multimedia forgeries without leaving any significant traces. These, malicious tampers might lead to various different judicial and societal issues. For example, manipulated images or videos has been used in courts as fake evidences, also to provide the public with fake news and mislead them. The present techniques available are not robust and efficient enough to address these forgeries. Meanwhile, now it has become impossible to detect any multimedia forgery by human intuition. Usually, the digital forensic techniques can be broadly classified by making use of two different techniques: active and passive forgery detection. A couple of common active forgery detection approaches include the watermarking [2] and digital signatures [3], [4]. However, these two techniques make use of still images, need special hardware for implementation. The passive or blind forgery detection methodologies explore the intrinsic features in the media left due to the use of devices which are used for acquisition or manipulation techniques, without making use of some sort of signals that are pre-embedded. It has become a promising tool used in digital visual media however still in a new field that is emerging and in the development stage. The passive forensic approaches are implementable only for the detection of digital images and not for videos.

Video forgery and other multimedia forgery techniques has influenced the swift rise in a broad spectrum of achievable changes which is in employment, namely frame erasure, frame inclusion and compressing of videos. Copy-move forgery is also a part of these alterations that is becoming common these days. It is relatively simple in its operation, but to recognize copy move forgery since they moved objects and frames belong to the same video. Different kinds of methodologies have been implemented and deployed to recognize any kind of frame copy-move forgeries, it is classified as image characteristic based and video characteristic based. The algorithms that are a part of digital image characteristic based identify and then splinter image characteristic of each frame to identify correlation including gray values, texture, noise and different modes of color. In the second type, the rest of algorithms investigate various distinctive characteristics in videos that encompass of movement characteristics, compressed videos and the coding characteristics.(including dimension, bitrates, frame grouping) to analyse and identify the special effects that might be produced when one tries to make use of the copy-move operation on video frames. In spite of the various different forgery recognition solutions provided for copy move forgery has been projected, existing approaches are incapable to deal with the subsequent issues:

Large estimation density: Image pixel based or the direct correlation based methodologies usually face the burden of high computation which effects its performance. It is relatively tedious to analyse a collection of different frames present in a video consisting of large volumes of data, moderately bigger than digital silent images.

Revised Manuscript Received on December 12, 2019.
***** Correspondence Author

Prof. Seemanthini.K, Asst.Professor, Dept.of ISE,Dayananda Sagar Academy of Technology And Management, Bangalore,

Dr.Manjunath S S, HOD, Dept.of CSE, ATME College of Enginering, Mysore

Raghuram A S, Asst.Professor, Dept.of CSE, ATME College of Enginering, Mysore Sneha N P4

Asst.Professor, Dept.of CSE, ATME College of Enginering, Mysore
seemanthini_k@dsatm.edu.in[1], manjunathdsatm@gmail.com[2] , rbraghuram958@gmail.com[3],sneha.np23@gmail.com[4]

-unbalanced detection presentation: The approaches that are based on picture features, that include texture, different modes of colours, noise and pixel gray values, can be attacked regularly or via post-preprocessing of videos including additional noise and secondary compression. Some of the methodologies that have been introduced and are existing, reckon the robustness of the detection algorithm, and usually assign fixed sensitive parameters for detection.

- Lack of applicability: Few implementations impose restriction to the video that is to be detected in terms of the format of the video record, the dimension of tampered images , tampering approaches used in unsmooth manipulation and in stationary camera reduces the business application of the algorithms in video forensics. These issues suggest that a real-time frame copy move forgery detection approach is in far above the ground , provided it must fulfill three uncomplicated necessities: such as negligible estimation complexity, greatest accurateness along with high-quality stoutness and well-built applicability.

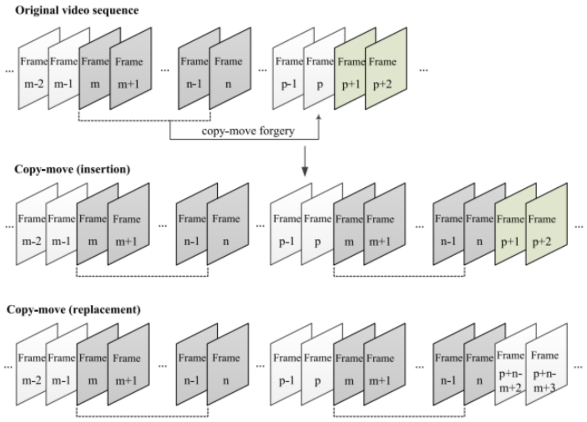


Figure 1:Illustration of copy-move forgery detection

II. IMAGE PROCESSING

Image processing requires adoption of digital image processing algorithms that are deployed to process an image into the satisfactory format. It is a subclass or a fraction of digital signal processing that has a numerous advantages pros above analog image processing. It provides a superior group of algorithms to be implemented to the input data and can be used to overcome problems such as distortion in the signals and the noise in the images. Given that the input images can be represented as two dimensional or as multidimensional images.

III. VIDEO PROCESSING

Video processing is used to improve the quality of the images captured. Video processing applications include astronomy, medicine, image compression, sports, rehabilitation, motion pictures, surveillance, production industries, robot control, TV productions, biometrics, photo editing, and so on.

IV. LITERATURE SURVEY

Liu, Yuqing et al.[1] conclude, using this paper that many former detection algorithms have been unable to address video forgery with a satisfactory trade-off between detection speed and accuracy. In this method. A Coarse detection scheme is used to identify the points that are abnormal. After that each and every digital video frame is transformed from three dimensional RGB color to two dimensional reverse chromaticity that is in incorporation with the Zernike moment correlation. These recognized points are extracted precisely from the unusual points by making use of a Tamura coarse feature analysis to conduct the process of fine detection. Coarse detection is quite efficient in terms of the detection speed and also provides a relatively small omission ratio. The paper that has been presented, consists of the authors making use of a passive-blind approach for the purpose of inter-frame forgery detection that comprises of inserting frames, deleting frames, replacing frames and copy–move operation applied on frames. The detection methodology extracts the juggle points based on ZOCM and Tamura coarseness feature by using the coarse-to-fine models.

Chih-Chung Hsu et al [2] conclude, a new methodology that precisely locates the forged regions in digital videos by making use of correlation values of noise residue is successful in detection. Here, video forgery is detected by the authors method which makes use of a number of block-level correlation values of noise residual and are obtained as a feature for classification. A two-phase approach is employed to assess the parameters of the model. Subsequently, a Bayesian classifier is applied to detect the optimal threshold value based on the parameters that were estimated. A couple video imprinting schemes are made use of in order to simulate the couple of unique kinds of forgery methods so as to evaluate the performance. The Simulation results depict that the approach being used provides good accuracy. However, this model does not address the issues of forgery in still images and other forms of multimedia.

Kingra Staffy.et al[3] conclude that the model that has been proposed can identify any kind of frame based forgery in the videos of the format of MPEG-2 and H.264 encoded videos. First, the algorithm performs objective analysis of prediction residual and then optical flow gradients are analysed to further find any kind of tampering that is done. The algorithm that the author has provided in this paper also has the potential of identifying the precise location of forgery. After testing the algorithm in different types of forensic environments and parameters the results indicate an accuracy of the range of 80% and 83% for detection and tamper locating, irrespective of the size of the frames. However, the use of a fine detection process will improve the accuracy.

Devanshi Chauhan.et al[4] conclude, the detection of forgery in a still image can be carried out using the techniques of Image splicing and Image retouching. BFSN Clustering, Hierarchical clustering and key point methods such as Euclidean distance and its results are studied and analysed under the copy move forgery. However, the model suggested in this paper cannot be applied to video and for other forms of multimedia.

Chun-Shien Lu et al[5] conclude that the approach of making use of a digital signature scheme that uses the contents of an image to build a digital signature known as structural digital signature (SDS) for image authentication is efficient for the purpose of forgery and tampering detection.

The experimental tests conducted for analyzing the efficiency of the algorithm that the algorithm proposed is absolutely effective for image authentication.

Lucas et al[6] concluded, that for the computation of optical flow there are smoothing effects that can be analysed in local and global methods that are diffrential. As a prototype of methods that were local the authors made use of the least-square fit. For the global method the Horn and Schunck approach was used. A basic confidence measure is proposed as a part of the algorithm to sparsify the flow fields of energy that are dense on the basis of global methods like the most possible reliable local estimated that is to be found. There can then be comparisons drawn between the quality of local and global methods. Experimental results have indicated that the proposed algorithms will give excellent results over a wide set of densities.

Horn Brian et al. [7] concluded that in any mage the optical flow is a representation of velocities of the objects and the patterns of brightness in an image. It can also be said to be the relative movement of an entity in an image and the viewer of the image. The unsmooth continuity in the optical flow map can help in segmenting the images.

This algorithm is developed in order to calculate the optical flow from a series of images. The basis of the development of this algorithm is that the velocity of flow in an image has two elements and the equation of image brightness gives only one constraint. Then, the flow smoothness is used as the second constraint. The authors then developed an iterative approach to solve the equation that was obtained. It included cases of lapcian and cases where it became infinite at singular points. This can be used in image forgery detection.

Bruce D et al. [8] proposed, that Image registration can be used for forgery detection.Image registration is used to identify a number of distict features or in the computer vido applications like motion analysis, stereo vision and pattern recognition.This image registration methodology consists of the extraction of the spatial intensity gradient of the images to find the good match by making use of the kind of newton-paphson iteration. This approach is quicker as it tests for a small set of potential matches between an image than the existing system.

Feng et al[9] concluded, that one can make use of the statistical characteristics of DF itself in order to avoid the dependency of detection on the side effect of the deletion of frame and the precise location of DF can be obtained. The similarity in spikes with respect to the mean of the motion for the RI, DP and residual statistic. Hence, the interference RI is needed to be removed.

Subsequently, the authors classify between DP and RU by evaluating the fluctuation strength of motion residual of an individual frame in which DPs have spikes that are manifested and RIs are inserted into adjacent frames. But the process mentioned above is relatively unstable and relay's on a video frame's content. The authors propose the use of an incremented feature adaptive threshold detection approach for the detection of the precise location of DPs which is automated in a forged video.

Zhao et at.[10] proposed a forgery detection methodology that is passive and robust for copy-move forgery that operates without the presence of digital watermarks or information on the signatures. If we consider the copy-move forgery it is likely that there exists a pair of regions that have been tampered in the process of forgery, that acts as the basis for all of the passive approaches of forgery recognition. An image that has not been tampered with is usually smooth in terms of the velocities of the objects present across the frame and no presence of the two forged regions is identified. Therefore, the objective of passive based approaches . Due to the difference in the size and also the shape of the copied regions it is not feasible to detect the tampered regions by comparing each pixel. The more feasible option available is to break down the entire image into permanent dimension of overlap blocks and then determine the forged pair. The important step is the extraction of few apt and unique characteristics from all the blocks that are obtained in order to implement efficient detection of the tampered parts of a video clip. Hence, the use of a good characteristic can represent the entire division of the frame and also is robust with respect to post-processing operation, this also results in the devised algorithm to have low computational complexity.

A.V. Subramanyam et al.[11] concluded that, it is effective to use the histogram of gradient features and the properties of video compression for the purpose of video forgery detection. The false positive rate is decremented by the assignment of HOG feature generation in terms of parameter cell size which also increments the accuracy of detecting any kind of forgery. In this video tampering detection method the frames with large value of replicated correlation regions are compared to authentic regions that are chosen for the purpose of forgery detection. Experimental test depict that the approach that is proposed provides precise accuracy for the detection of forgery when various approaches are applied like video solidity, scaling and denoising for spatial tampering detection whereas compression and filtering process for temporal tampering and forgery detection.

Abbasi Aghamaleki et al.[12] proposed, developed an method for the detection of forgery of a video in the format of MPEGx that is passive in its approach. Here, the author proposes a new algorithm for inter-frame tampering and localization in MPEGx coded videos. The basis of the algorithm that is proposed are the traces of quantization error in residual errors of P-MB in P frames. The domain that is temporal is used for the identification of the traces of forgery. Hence, the use of a particular algorithm enhances the quantization traces in the domain that is used by exploring the quantization-error-rich area in the frames of the video.

The proposed algorithm is capable of detecting forgery and localization of the insertion of a frame or deletion of a frame and double compression with various GOP structures and different lengths.

Kobayashi et al.[13] concluded, The main feature used is using noise characteristics to find the absence of consistency in frames of a video. The authors implement the method that is proposed to videos that are suspected to be tampered via various means of tampering. The authors demonstrate the use of this method to find any region that is suspected to tampering by the superimposition of a region from another video from another video by verifying the variations in the characteristics of noise from one region to another. Contrary to few of the other digital video forgery detection methods, the method that has been used by the authors is relatively robust to the mixing of noise into the data that is used as the input as the authors actually make use of the noise characteristics itself. In this study, we notice that the authors devise a technique for detection of forgeries in a stationary video clip based on inconsistencies in NLFs. After finding, the characteristic of noise present in each pixel, the author estimates the probability of the video from each pixel. The method that is proposed is used to accurately evaluate NLFs and also the posterior of tampering when a couple NLFs are separated. In spite of unfavourable conditions, the method which is proposed is able to detect few suspected pixels in the region of forgery, that is helpful to find regions in the data that acts as the input which may be tampered.

Wu et al.[14] concluded, that the algorithm proposed on basis of the consistency of velocity field is efficient. It detects forgery of video that is done on the inter-fames of a video clip (i.e., consecutive deletion of frame and consecutive duplication of a frame in a video). The generalized extreme student zed deviate (ESD) experiment is used to find the forgery types and identify the location of position of manipulations in forged videos. Test results depict the effectiveness of their algorithm. However, it lacks efficiency in other forms of multimedia.

Tanfeng Sun et al.[15] concluded, that an incremented and slightly improved model for the purpose of video tampering identification that is based on MPEG double compression in effective. Double compression imports some disturbance into the coefficients of Discrete Cosine Transform (DCT) , that is actually not allowed in the parametric logarithmic law for first digit distribution of quantized Alternating Current (AC) coefficients. A 12-D characteristic has a possibility to be obtained from all the group of pictures (GOP) also a framework of machine learning is used for enhancement of the accuracy of detection. Subsequently, a approach that uses another machine learning framework as its architecture is used. Support Vector Machine (SVM) is used to evaluate the natural bit rate scale in a video that is compressed doubly.

Experimental results show high accuracy and effectiveness.

V.METHODOLOGY

The block diagram of the proposed methodology is given below:

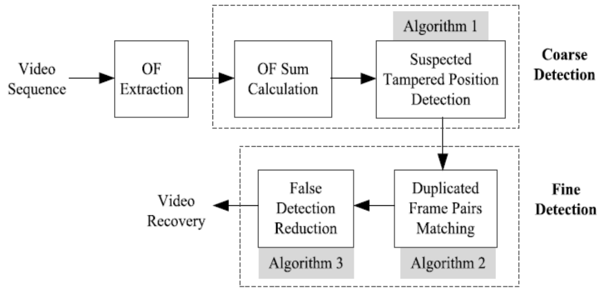


Figure 2: System Architecture

The methodology of the proposed model is defined as a conceptual model that defines the structure, behavior and the views of the system. The architectural behavior explains the structure and the behavior of the system.There have been efforts to formalize languages to describe system architecture, collectively these are called architecture description languages (ADLs). A Machine Learning Algorithm named Logistic Regression is used to train the system and create a model from the available data set.The data set consists 2 types of videos- Forged and non-Forged(original). Initially, these videos are converted into a number of frames which they represent. These frames are then converted into greyscale and the optical flow map is generated for the given video.

From this optical flow map, the features like motion are extracted. The optical sum consistency is tested to determine the suspected tampered points. After that the GLCM and validation check algorithms are applied to further reduce any kind of tampering go undetected. The system then returns if the video is forged or not forged.

The first phase of the project involves converting videos into frames that represent a still image. Then the RGB image/frame is converted into a Grayscale image, here we use the image block processing concept followed by coarse-to-fine detection.

1. Coarse Detection

In the second module of the project, the Optical flow algortihms is used to find the sum of consistency and detect any suspected tampered points in the frame sequence.

2. Fine Detection

In the next phase of the project, the GLCM algorithm is applied to detect any duplication in frames (i.e., adding or removal of any object) followed by frame detection and frame validation algorithms to further detect any tampering and recover the original frame/image.

The proposed system first train a machine learning model to preprocess the dataset of videos.

The proposed model is developed for four modules.

1. Data collection and training
2. Applying Optical Algorithm to determine consistency and feature extraction
3. Applying GLCM and clustering the features
4. Predicting if the video is forged or not

Data collection and training: The first module deals with the code(algorithm) to import the video and process it (into grayscale) for which a learning model is used. The Logistic regression is used to create the model for training the data sets. The data sets are collected from Surrey University Library for Forensic Analysis (SULFA) and then trained.

Applying Optical Algorithm to determine consistency and feature extraction: After conversion into grayscale we apply the optical flow algorithm to determine the consistency in the frames. Also the image block processing concept is used for breaking the frame in a smaller size for edge detection.

Applying GLCM and clustering the features: The third module consists GLCM algorithm to do the texture analysis and determining any tampering in the video frame.The K-nearest neighbour algorithm is used for classification and clustering of video frames that are similar.

Predicting if the video is forged or not: The fourth module uses deep learning algorithms like SVM, Naïve bayes are used for prediction of whether a video is forged or non-forged.

VI. RESULT

OF is the distribution of apparent movement velocities of brightness patterns in videos, which can give important information about the image spatial arrangement and change rate of objects.

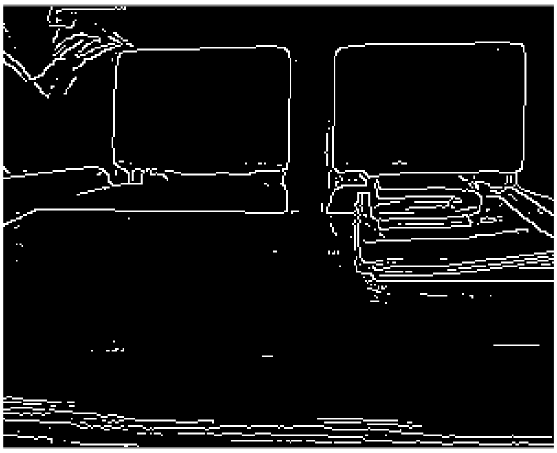
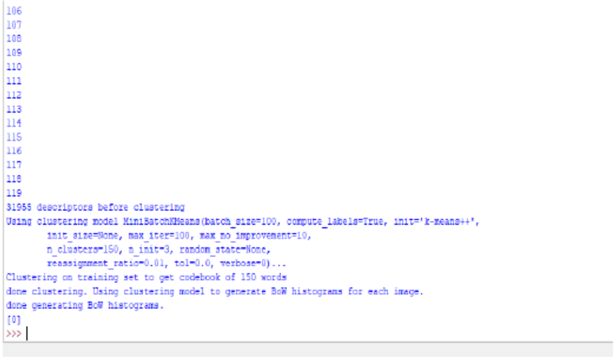


Figure 3:Generation of OF map for a video

Conducting a series of experiments to evaluate the performance of the proposed detection scheme in this section. The experimental data and evaluation standards are introduced first.

Then the involved parameters are determined with a subset of tampered video sequences. Finally, we present the experimental results and comparison analysis with four existing classical algorithms in terms of detection accuracy, robustness, efficiency, and applicability.



```
106
107
108
109
110
111
112
113
114
115
116
117
118
119
31955 descriptors before clustering
Using clustering model MiniBatchKMeans(batch_size=100, compute_labels=True, init='k-means++',
        init_size=None, max_iter=100, max_no_improvement=10,
        n_clusters=150, n_init=3, random_state=None,
        reassignment_ratio=0.01, tol=0.0, verbose=0)...
Clustering on training set to get codebook of 150 words
done clustering. Using clustering model to generate BoW histograms for each image.
done generating BoW histograms.
[0]
>>> |
```

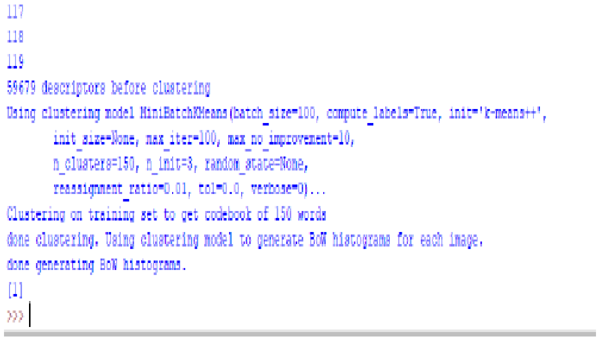
Figure 4: Showing a result that video is not forged

Processing a video is nothing but converting a video into number of frames, as shown in the above result first the video is converted into 119 numbers of frames then its tested with series of machine learning algorithms those accuracy is also calculated and if video is forged then the output is 1 otherwise 0

When a video is forged the optical flow map is generated and the system returns 1 as shown in the figure below.

Processing a video is nothing but converting a video into number of frames, as shown in the above result first the video is converted into 119 numbers of frames then its tested with series of machine learning algorithms those accuracy is also calculated and if video is forged then the output is 1 otherwise 0

When a video is forged the optical flow map is generated and the system returns 1 as shown in the figure below.



```
117
118
119
59679 descriptors before clustering
Using clustering model MiniBatchKMeans(batch_size=100, compute_labels=True, init='k-means++',
        init_size=None, max_iter=100, max_no_improvement=10,
        n_clusters=150, n_init=3, random_state=None,
        reassignment_ratio=0.01, tol=0.0, verbose=0)...
Clustering on training set to get codebook of 150 words
done clustering. Using clustering model to generate BoW histograms for each image.
done generating BoW histograms.
[1]
>>> |
```

Figure 5: When a video is forged

VII. CONCLUSION

An ideal copy-move forgery detection algorithm should be able to strike a balance between the efficiency, robustness and applicability under different degrees of forgery. In the survey, we assessed the strategies various forgery detection techniques. The proposed system deals with detection of Video forgery detection. This method ensures that any kind of fake or tampered video is detected quickly and identified as a forged video. In previously proposed techniques like using noise correlation, brightness gradients and watermarking the algorithms only solved part of the problems with respect to video forgery.

Hence, the proposed system

uses Deep learning algorithms to strike an effective balance between efficiency, robustness and applicability.

The current algorithm is applicable to only videos. In the future this can be extended to images, audio clips etc.

VIII. REFERENCES

1. Liu, Yuqing & Huang, Tianqiang. (2015). Exposing video inter-frame forgery by Zernike opponent chromaticity moments and coarseness analysis.
2. Hsu, Chih-Chung & Hung, Tzu-Yi & Lin, Chia-Wen & Hsu, Chiou-Ting. (2008). Video forgery detection using correlation of noise residue. MMSP. 170-174. 10.1109/MMSP.2008.4665069.
3. Kingra, Staffy & Aggarwal, Naveen & Singh, Raahat. (2017). Inter-frame forgery detection in H.264 videos using motion and brightness gradients.
4. Survey on keypoint based copy-move forgery detection methods on image.(2014) Devanshi Chauhan, Dipali Kasat, Sanjeev Jain, Vilas Thakare
5. Chun-Shien Lu and H. -. M. Liao, "Structural digital signature for image authentication: an incidental distortion resistant scheme,"in *IEEE Transactions on Multimedia*.
6. Lucas/ Kanade Meets Horn/Schunch: Combining Local and global optic Flow Methods(2004).
7. Determining optical flow Berthold kp, Horn Brian, G Schuck
8. Lucas, Bruce D. and Takeo Kanade. “An Iterative Image Registration Technique with an Application to Stereo Vision.” *IJCAI*.
9. Feng, Chunhui & Xu, Zhengquan & Zhang, Wenting & Yanyan, xu. (2014). Automatic location of frame deletion point for digital video forensics. 10.1145/2600918.2600923.
10. Zhao, Jie & Guo, Jichang. (2013) Passive forensics for copy move image forgery .
11. Subramanyam, A.V. & Emmanuele Using HOG feature compression property IEEE(2012).
12. Abbasi Aghamaleki, Javad & Behrad, Alireza. (2016). Inter-frame video forgery detection and localization using intrinsic effects of double compression on quantization errors of video coding. Signal Processing: Image Communication. 47. 10.1016/j.image.2016.07.001.
13. Michihiro Kobayashi & Okabe, Takahiro & Sato, Yoichi. (2011). Detecting Forgery From Static-Scene Video Based on Inconsistency in Noise Level Functions. Information Forensics and Security, IEEE Transactions on. 5. 883 - 892. 10.1109/TIFS.2010.2074194.
14. Wu, Yuxing & Jiang, Xinghao & Sun, Tanfeng & Wang, Wan. (2014). Exposing video inter-frame forgery based on velocity field consistency. ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings. 2674-2678. 10.1109/ICASSP.2014.6854085.
15. Tanfeng Sun & Wang, Wan & Jiang, Xinghao. (2012). Exposing video forgeries by detecting MPEG double compression. Acoustics, Speech, and Signal Processing, 1988. ICASSP-88., 1988 International Conference on 1389-1392. 10.1109/ICASSP.2012.6288150.

AUTHOR PROFILE

Seemanthini.K received the B.E. degree in Computer Science & Engineering from People’s Education Society College of Engineering, Mandya. and the M.Tech degree in Computer Science & Engineering from R.V.College of Engineering, Bangalore. She is currently pursuing research in Computer Vision and Pattern recognition under VTU, Belgaum. Her current research interests are anomaly event detection, Group Event detection and Action Recognition.

Manjunath S.S has received B.E degree in 2000 from Mysore University, Mysore and M.Tech degree in 2005 from VTU University, Belgaum, Karnataka, India. He completed Ph.D in Computer Science from University of Mysore, India. Currently he is working as a HOD & Professor at ATME.His experience in teaching started from the year 2000. His areas of interests include microarray image processing, medical image segmentation and clustering algorithms.