Journal of Theoretical and Applied Information Technology
20th April 2015. Vol.74 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DETECTION OF VIDEO FORGERY: A REVIEW OF LITERATURE

Omar Ismael Al-Sanjary[1], GhazaliSulong[2],
[1], [2]MaGIC-X (Media and Games Innovation Centre of Excellent), Faculty of Computing, UniversitiTeknologi Malaysia, Skudai, 81310, Johor Bahru, Malaysia.

E-mail: [1]omis_mit2020@yahoo.com, [2]ghazali@utmspace.edu.my

ABSTRACT

In the current times the level of video forgery has increased on the internet with the increase in the role of malware that has made it possible for any user to upload, download and share objects online including audio, images, and video. Specifically, Video Editor and Adobe Photoshop are some of the multimedia software and tools that are used to edit or tamper medial files. Added to this, manipulation of video sequence in a way that objects within the frame are inserted or deleted are among the common malicious video forgery operations. In the present study, literature concerning video forgery is reviewed primarily those that use several video forgery detection in the form of passive blind method on three types of forgery namely cloning forgery, source cameral identification and splice forgery. The present study employed a video authentication method that detects and determines both region duplication and frame duplication in terms of video forgery, and locates factors that impact video forgery. In the present study, video processing into sub-blocks and the moments geometric features for every macro-block were extracted. This led to the enhanced accuracy of detection. Moreover, the optimum sorting algorithm led to minimized computational time taking account number of blocks and features numbers into consideration.

Keywords: *Video Forgery Detection, Group Of Pictures (GOP), Copy–Move Forgery Detection*

1. INTRODUCTION

The existence of digital video and digital image editing tools has made it challenging to accurately authenticate multimedia content. The current manipulation technique and the dynamic multimedia technology evolution made it possible even for a novice to easily delete an object from a video sequence, or add an object from another video source, or insert an object developed by graphics software designer. It has become complicated to comprehend and differentiate an authentic video from a tampered one. This is due to the several forgery methods that the public can avail with, which as a result, recordings of video processing have become a great challenge [1, 2]. In recent years, blind digital video forgery detection has been employed to determine the authenticity of digital video forms a topic that has been of significance among researchers.

Video forgery primarily falls into two methods based on their approaches; active approaches and passive-blind approaches. The first approach (active approach [3-6]) is primarily focused on the invisible data and requires pre-embedding of information like watermark, fingerprint into images or digital signatures, and to identify them through integrity detection of the pre-embedded information. On the other hand, the latter approach is more appropriate for some occasions like video, photo image or audio [7].

Specifically, passive approaches can be divided into three general types [8, 9] namely splicing, source identification and copy-move forgery. Such approaches are used for the detection of digital video and double compression video tampering like MPEG or H.246. This is clear from the several works dedicated to digital video tampering detection [10-15]. These methods are effective in the detection of traditional forgery operations and it is often beneficial to determine the digital video authenticity with the help of video object detection, video double compression, video frame of region duplication, frame-based tampering and image double JPEG compression.

Journal of Theoretical and Applied Information Technology
20th April 2015. Vol.74 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A duplicate sequence of video frames to hide or mimic a specific event is depicted in Figure 1. For instance, if a person is video recorded via a camera, the portion of the video depicting the human body can be erased by copying and moving a sub-sequence frame to cover the removal. It is challenging to detect this type of video forgery if the copy-move procedure is carefully and actually carried out. Consequently, this is where the importance of video forgery lies [16, 17].

Figure 1: *Example of original and forged of video [17]*

In the present study, the performances of some typical video forgery algorithms are compared and an overview of passive digital video authentication method is demonstrated. Added to this, the existing blind forgery detection methods are reviewed. Specifically, this study concentrates on the categorization of different research methods to detect and localize traces of changed regions on passive-blind methods in video sequences. Some of the algorithms are presented in the results and discussion section and it is evident that no distinction exists between malicious manipulating and innocent retouching, like red-eye correction or artistic changes. Towards the end, the study is concluded and the author offers future directions of study to determine new research problems in the field of video forgery detection.

The remaining parts of the paper are organized in the following manner; Section 2 explains the video forgery doctoring detection tools and section 3 provides the study framework. This is followed by section 4 that demonstrates tampering of video content in passive methods and section 5 that provides a review of related work in literature. Section 6 contains an overview of video compression and the final section provides discussion and conclusion.

2. TOOLS FOR VIDEO FORGERY DOCTORING DETECTION

Although video appears to be more complicated when it comes to image development, temper forged video has become easier now than before, owing to the availability of video editing tools. Meanwhile, videos are extensively utilized as surveillance video and are deemed to be a significant evidence of effectiveness as opposed to a single photo. There are various methods of tampering in a video forgery; among them being inserting or eliminating frames, changing frame sets, introducing, duplicating or deleting objects form the video sequence scenes. Both video forgery and video forensic methods may be classified as spatial-frame (attack/analysis is carried out frame-wise, while taking a frame at a time into consideration) or temporal frame (where the connections between adjacent frames are focused on). Passive method techniques can be categorized into three namely image splicing, source identification and copy/move forgery. In literature many studies have been dedicated to video forgery detection [18 - 22]:

2.1 Source Identification

According to [23, 24], source camera identification is a crucial issue that focuses on many issues that are linked to source class, like model, brand, sensor type. The authentication of source refers to a process that examines whether or not something stems from the claimed source (The Webster's New 20th Century Dictionary).

According to Kang et al. [25], a source camera identification method can delete the interference and bring about the correlation to Circular Correlation Norm (CCN) value and further make use of the CNN as the test statistic that decreases the false positive rate to half of the statistic peak of correlation energy (PCE). In case of an image with Frame Dimension 512X512 pixels at zero false positives (FP), the true positive rate (TPR) of accuracy is said to be 99.9%.

Additionally, the source camera identification and manipulation detection was introduced by Redi [26]. In the first category, authentication hinges on detecting camera fingerprints (the traces left by the image frame acquisition phases and the storage phases). The methods use the camera fingerprint to determine various models of cameras or the different exemplars of the same camera model.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

But according to [27-29], source identification is still ineffective when utilized between 9-15 cameras and in mobile camera model. The results may be negatively impacted by the increasing camera identification. It was noted that source identification methods hinges on the robust statistics features of source camera identification hardware such as Ns and CCD sensor features that are more dependable than camera software parts (CFA interpolation algorithms). Furthermore, in [27] it was found that quantifying double compression artifacts assist in the difficulty in localization of the forgery when the image is analyzed or compressed via low quality factor in majority of methods. On the other hand, in [28, 29] camera sensor noise was utilized to relate a distinct method-identification camera with a video and to determine tampering of video regions through passive methods.

2.2 Splicing

According [30] image frame splicing is used on the original image frame with additional images to produce a manipulated copy [31, 32]. This method works when some object of other images is added to the original frame for the purpose of hiding or modifying the image frame content. Moreover, splicing forgery is a common type of image tampering that copies and pastes from another image frame – it works on an image effectively more than on a video.

The normality of the color edge or otherwise provides significant evidence of frame manipulation [33, 35]. In case of region-based methods splicing detection, consistency is confirmed on the obstetric model of the frame and estimated when investigating the source image.

Similarly, [31] brought forward a digital image splicing detection method through the exploitation of specular highlights in the eyes. A statistical image model for splicing detection was proposed by Farid [34], a version of which is the blind image forgery detection method that extracts features of classification via the Hilbert-Huang transform (HHT) and statistical model that hinges on the moments of characteristic functions. This involves the application of wavelets transform to differentiate the spliced region detection [53]. Their findings showed that the method is able to detect high accuracy of passive splicing localization detection.

2.3 Detection Of Copy–Move Forgery

Another common type of video forgery is the copy-move tampering. It refers to the type of forgery where a part of the frame is copied and pasted into another part, with the purpose of adding or deleting an object in the video frame. Several methods are used for the detection of this forgery and all of them depend on the assumption that a copy-move forgery brings significant correlation between the source frames and duplicated ones. A method that detects double quantization resulting from double MPEG compression in digital video was proposed by Wang et al. [36]. They calculated the differences between the corresponding temporal and spatial domain correlation matrices. Accordingly, high correlation enables the method to detect highly localized tampering in regions as small as 16X16 pixels with an average 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 [37].

	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 [38] developed a method to detect suspicious regions in video recorded from a static

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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 [39]. 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.

3. FRAMEWORK OVERVIEW IN VIDEO FORGERY DETECTION

Studies [40-47] were dedicated to digital image forensics but only a few have touched upon digital video forgery detections. One of the most popular tampering artifacts in video forgery is copy-move forgery. In this domain, it is challenging to detect regions or frames as the forged location may differ with regards to size and rate of compression. Video forgery detection methods are primarily utilized to determine the spatial domain and temporal domain of copy-move tampering.

In Figure 2, the general detection method consisting of extract frames from the source video, feature extraction, overlapping block matching, and forgery decision are presented. This method enables the application of many extraction techniques like the DCT, DWT, PCA, among others and allows the application of various matching methods [44] like K-SVD tree and radix sort.

In editing a video sequence, the processing methods consists of three steps; first, the input sequence of frames are decoded; second, the actual frames sequence is edited and; third, the edited video is re-encoded (possibly with a distinct codec or different coding parameters).

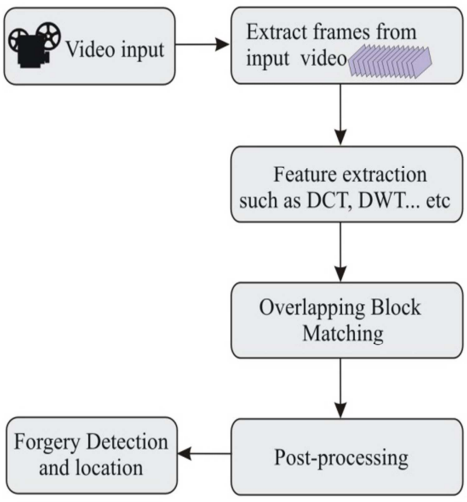

Figure 2: Shows The General Forgery Detection

In other studies such as [40], Xiaoling brought forward a method that authenticates and detects tampered algorithm combined with semi-fragile watermark embedded into DCT coefficient with the help of Compressing Sensing Theory. He utilized MPEG-2 compression video as the research object, where content authentication of inner I-frames and tamper detection of P-frame can be carried out. The result showed that the algorithm Semi-fragile Watermarking algorithm obtained top effectiveness when it comes to ability and accuracy.

In a related study Wang et al. [41] developed a method involving the use of the temporal and spatial correlation to determine frames duplication but the location of frame duplication is inaccurate in case of small forged regions. Similarly, [42] created a method according to two types of attacks; 1) spatial (pixel) copy-move attack detected via Histogram of Oriented Gradients (HOG), 2) temporal copy-move attack detected via exploitation of MPEG0-2 GOP structure.

Also, Wang & Farid [43] proposed a video tampering detection method through the detection of duplicate frames. In such a method, a doubly compressed MPEG video frames sequence provides specific static and temporal statistical disarrangement whose existence can be used like an originally encoded MPEG compression method where frames are edited and re-saved as a doubly compressed MPEG video.

Meanwhile, [44] used the multimedia software tools to delete some moving frames objects in a

Journal of Theoretical and Applied Information Technology
20th April 2015. Vol.74 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

video sequence and referred to it as one of the common methods of video forgery of frames. The differences of features between a video of frames were obtained with the help of Compressed Sensing, K-SVD (k-Singular Value Decomposition) and random projection was utilized to relay the features into the lower-dimensional subspace that is clustered by k-means. The detection results are eventually combined for each frame.

Hsu et al. [45] brought forward video splicing method and demonstrated a technical method to detect forged frame regions in a video with the help of correlation of noise residue. The method primarily hinges on the notion that the tampered frames transform the correlation of noise residue on each frame and differentiates them from the non-tampered parts. The results of the experiments reveal that the noise correlation is fairly dependable feature in case of fine-quality video although it is vulnerable to noise quantization. Added to this, the noise residue extraction is a complex process [45] – spatial (intra-frame) forgery and temporal (inter-frame) forgery. In the former, the tamper-free form, the same videos are utilized for clipping, and the inter-frame frames from the video are utilized for tampering.

In a related study [47], a method according to the Tamura texture features and algorithm was proposed with the help of the vector matrix of the video through video frame extraction. The method calculates the differences between the Tamura texture feature vector and the adjacent vector matrix. In case the differences are lower than the threshold, their distance is contrasted for the serial number with the threshold and the pairs of the serial numbers bigger than the distance threshold is recorded to locate the copy-move sequences.

In another related study, Davarzani et al. [48] proposed an efficient technique to detect copy-move forgery with the help of Multire solution Local Binary Patterns (MLBP). The method is effective to be applied to distortions and highlighting variance of region duplicated even following rotation, scaling, JPEG compression, blurring and noise adding. The image is pictured into blocks, with every block extracted with the help of LBP and RANSAC algorithm.

4. TAMPERING OF VIDEO CONTENT IN PASSIVE APPROACHES

Video tampering involves compression trough the removal of the temporal frames, the temporal redundancy and spatial redundancy. In spatial and temporal domain, forgery detection involves manipulation involving three types of video tampering; [49]; 1) spatial domain referred to as spatial tampering, 2) temporal domain referred to as temporal tampering and 3) a combination between the two – spatio-temporal domain referred to as spatio-temporal tampering as presented in Figure 3.

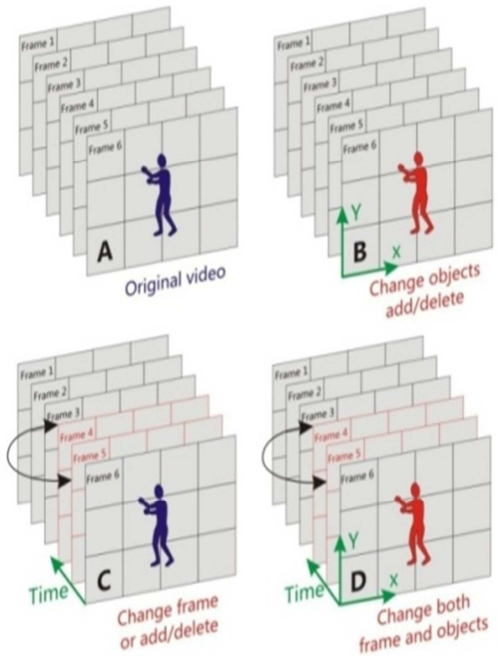

Figure: 3: An Example Of (A) Original Video (B) Spatially Tampered Video (C) Temporally Tampered Video And (D) Spatio-Temporal Tampered Video.

Furthermore, Figure 4 presents studies [13, 15, 56-59] dedicated to digital video tampering detection published between the years 2005 and 2013 in Science Direct, IEEE, and conferences and journals.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

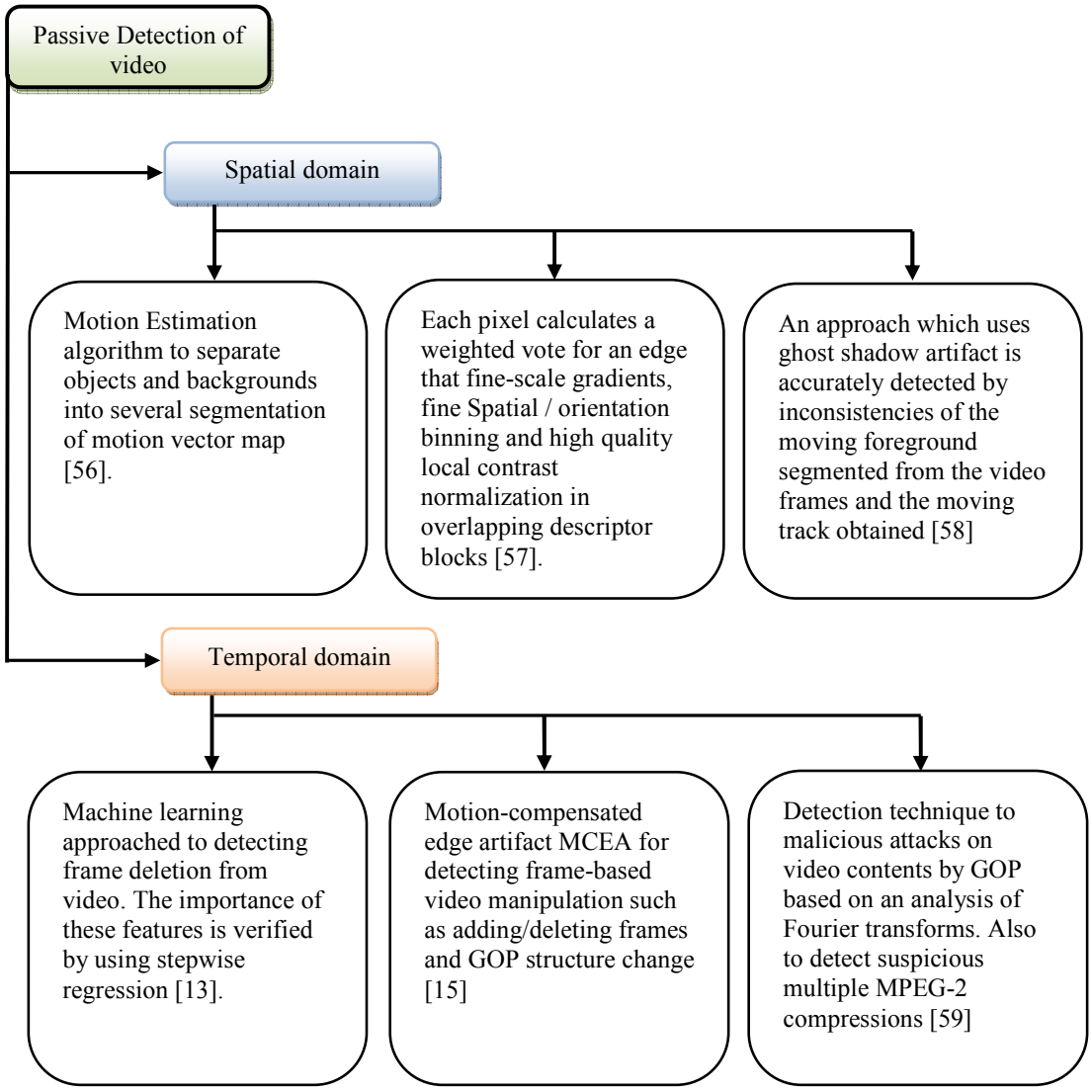

Figure: 4: This Shows The Number Of Papers Related To Digital Video Passive Approaches

4.1 Tampering In Spatial Domain

Owing to spatial nearby pixel, the video data is related with blocks where a motion vector is identified for blocks of 8X8 that are utilized for a luminance sample. Each pixel's value is quantized through a specific finite precision. The Discrete Cosine Transform (DCD) coding methods are used in MPEG algorithms and motion vectors are evident for every 16-col by 16-line frame region (macro-blocks). In this regard, spatial domains can be known be known between a manipulated video's two duplicated frames [49].

To detect forgery copying or moving in the spatial domain, a video frame is tampered with by cutting, copying, pasting, and moving – such processes can also be employed on still images. The forged regions are basically post-processes and could maintain their true values. The suitable choice would be macro-blocks structure as it can impost threshold on the matching or the extraction of considerable frames (RFs) from the comparison area. In this regard, the frame overlapping blocks in a block matching strategy region is an appropriate

Journal of Theoretical and Applied Information Technology
20th April 2015. Vol.74 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

method for features extraction based upon which blocks are compared to identify their similarities.

Every individual pixel comprise of three components namely the ***luminance component (Y)*** and two ***chrominance components (Cb and Cr)*** as presented in Figure 5 that represents slice and macro-blocks structure.

.

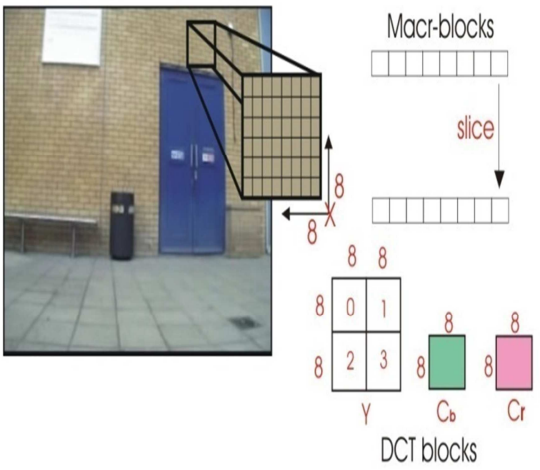

Figure: 5: *shows Slice and macro-blocks Structure*

4.2 Tampering In Temporal Domains

In the temporal field [50, 51] the video frames are tampered with via deletion, insertion and average of frame. In this regard, video temporal tampering can be carried out in three levels, frame level, scene/shot level and video level. In the first level, tampering entails the insertion or removal of frames that lead to tampered videos with minimized or maximized frame count. Such frames may be intermediate video frames that or frames collection spread into double scenes. Temporal domain which is in close proximity in video frames often has a significant level of similarity.

An example of frame is depicted in figure 6 – one that entails the removal of a frame at the level. Added to this, removing may be at the scene level where the entire scene is deleted by frame deletion. Scene level deletion is often known as shot cut or scene cut. In contrast to frame drop. Frame count remains the same while video frames are swapped to develop a tampered video from actual video source [52].

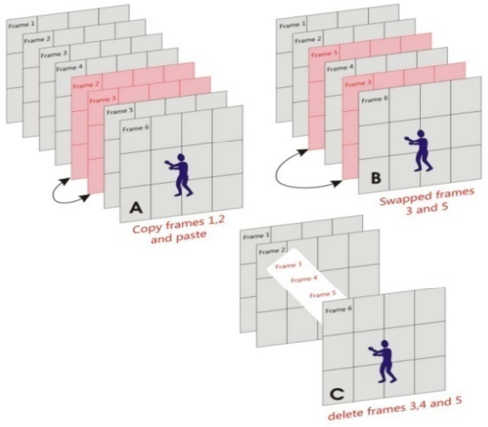

Figure: 6: *An example of (A) Frame Drop, (B) Frame Swapping, and (C) Frame Copying where source is the video sequence presented.*

Moreover, at the frame level, such swapped frames can be of video frames comprising of one or two scenes where there is a change of entire scene (i.e. the entire scene frames are swapped with other scene frames. An example of frame tampering through frame swapping is presented in Figure 5B. In this case, frame count is increased is a source video is manipulated via video frames copying and pasting to another location in the source video [53, 54]. The copied frames may be the intermediate frames taken from a video scene or at the scene level. A whole scene can be copied and pasted following another scene. Copying can also be done at the video level where the entire frames of a video sequence are copied and pasted into another such that a source video copy is developed.

In the context of copy-move tampering, the number of frames of source videos is shifted to another location. On the other hand, in frame averaging, an average frame is inserted between two scan lines sets in a video frame [52, 55]. Also, in substitution of frames, a video frame by another frame of the source video is carried out in what is referred to as a 'a foreign frame'.

5. RELATED WORK

To the best of the researcher's knowledge, passive approaches are the most important methods in the detection of digital video forgery [60-69]. Table 2 displays the summarized video forgery detection methods, under the headings of classifier, frame dimension with data set, and prior work, and remake of the evaluation performance.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: Shows Summarizes Of Video Forgery Detection; Method And Classifier Extracted Features With Dataset By Previous Work

Auther's	Methods	Classifier	Dataset & Frame Dimension	Accuracy	Remake the Performance evaluation
Richao, C., et al. [60], (2014)	Statistical feature extraction, camera identification, A new concept of (AWOB), & Wavelet transform.	SVM	20 videos: 320 x 240	95%	This method is efficient to detect motion object from static background subtraction technique, & then the object boundary is located
Wang, Q., et al. [61], (2014)	Correlation coefficients gray, Normalization & Quantization & distinguishing features	SVM	5 videos: 256×256	98.79%	The method involves small dataset & is not efficient in classifying frame insertion & frame deletion forgery.
Su, L., [62], (2014)	Compressive sensing (k-SVD), linear transformation such as Wavelet Transform (WT) & Fourier Transform (FT)	K-Means clustering	20 videos: 640×480	89.6%	This work's ambiguity needs more details on methods, & video contain complex motions to detect the moving foreground removed from static background
Jaiswal, S., [63], (2013)	PES feature extraction: Transformations like DCT, DFT, DWT	SVM	20 videos: 176x144	N/A	This method is efficient & suitable for removing /inserting frames, double MPEG decompression
Bestagini, P., et al. [64], (2013)	The algorithm detects the attack by analyzing the footprint left in the residual. Two features are computed between adjacent frames, & provedto be robust to mild compression.	Two-class classifier	20 videos: 320×240.	87%	The important phases of the proposed methods are feature extraction, reduction of dimensionality when there is a projectile with 3D correlation between detection of image & video -based attack
Vázquez-Padın, D., et al. [65], (2012)	New forensic footprint based on the variation of the macro-block prediction types (VPF) in the P-frames &, also estimate the size of a GOP	One-class classifier	14 videos: 352×288	94%	The method is not efficient due to using more than one for compressed video such as MPEG-2, MPEG-4, & H.264, & compression is one limitation which decreases performance.
Chen, R., et al. [66], (2012)	Object detection produce significant coefficients by using two methods NSCT & Gradient for RGB channels in AWOB	SVM	9 videos: 320×240.	95%	This method is efficient to detect motion object produced by deleting, moving objects in video
Chetty, G., et al. [67], (2010)	Extraction of intra-frame & inter-frame pixel sub-block noise residue features between three different types of correlation	Three-class classifier	Internet streamed movies= N/A	92%	The method is needed more results and also achieved very accurate results of segmentation which effectively extract video tamper detection
Zhang, J., et al. [58], (2009)	Based on a ghost shadow artifact which is usually appeared when moving object is removed by video inpainting. & a given pixel of the accumulative frame gives the number of times, the gray level at that position is different from the corresponding pixel value in the reference frame.	N/A	3 videos: 720×480	N/A	This method didn't mention for accuracy & classifier also needs a complex & an efficient algorithm for detecting ghost shadow & used very small data set to compare with others researching
Su, Y., et al. [68], (2009)	Based on motion compensated edge artifact is proposed frame-deletion	One-class classifier	5 videos	N/A	The method is weak & proposed algorithm has shown a reliable performance against different artifacts such as pixel blocks in a frame
Wang, W., [69], (2007)	Correlation coefficient in duplicate frames, & Fourier transform in removing people or objects from a video	One-class classifier	2 videos: 480×720	84.2%	The method is useful for automatic image frame to detect frame & region duplication

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The detection of blurring can be manipulated via the statistical characteristics of object-based forgery operations. In relation to this, Richao et al. [60] conducted an analysis of the concept of AWOB using statistical features as wavelet coefficients and the moment features that details the average gradient of every color channel were taken to include in the SVM. According to the experimental findings, the accuracy of detection is around 95% and the data set consisted of 20 videos from SULFA.

Moreover, Wang et al. [61] brought forward a method on the basis of the assumption that the correlation coefficients of gray values lying between the sequences of video following normalization and quantization to determine inter-frame forgeries involving small data set (five videos). The accuracy was found to be 98.79%.

Similarly, Su [62] proposed a method that detected tampering on the basis of compressive sensing with the help of feature clustering of the differences between frames obtained via K-SVD. The results showed an accuracy of 89.6%. Also, in [63] the method analyses impacts the attacks in temporal domain through machine learning methods.

Meanwhile, Bestagini et al. [64] conducted analysis of the footprints in terms of video sequence through a detection algorithm that enables a forensic analyst to determine video forgeries and localize them in the domain of spatio-temporal They tested the analysis on 120 actual frame sequences with the resolution of 320X240 pixels comprising 20 videos. The results showed an analysis accuracy of 87%.

Moreover, Vazquez-Padin et al. [65] brought forward a technique that estimates the GOP size with a video sequence based on the assumption that VPF becomes evident in P-frames that are intra-coded in the first double encoding. The experiment involved 14 video sequences allowing an accuracy of 95%. In relation to this, [66] provided a description of a method that determines video object contour on the basis of non-sub sampled contourlet transform and gradient information that employed feature vector combined with SVM. Their dataset comprised 9 videos with the frame 320X240 and the accuracy was found to be 95%. However, this method is not very effective in detecting forgery areas in static scene videos. As a result, it is not appropriate for the detection of suspicious level areas in videos taken by a moving camera.

In relation to the above studies, Chetty et al. [67] suggested a method of video tampering detection based on transformation of feature from several intra-frame and inter-frame pixel sub-blocks in video sequences and their multi-modal combination. The emulated copy-move tamper scene revealed that the quantization residue features performance for the entire experiments is similar to noise residue features. But the method is frame-level forgery focuses and thus it did not locate the issue of region-level tampering and localization.

Furthermore, [68] brought forward a new approach to detect motion-compensated edge artifact to determine the changes of correlation among adjacent frames. Also, [69] proposed duplicate frames or frame parts to delete people or objects from the video-call in painting. Their method only worked in frame manipulation detection and not in localization of tampered object regions.

6. VIDEO COMPRESSION

Different video standards are used for compressing digital videos [72][73] and these include H.261, H.263, MPEG-1, MPEG-2, MPEG-4) as well as various bit rates upon which different applications are operated. There is an increasing requirement for video tans coding [45, 70]. Figure 7 displays three frame types for an MPEG encoded video sequence, the first being the source intra (I frame) that is independently coded on all frames and affords the leas compression level. The second is the predictive coded frame (P frame) that is coded on the basis of prior coded frame. P-frames can take significant compression compared to I-frames but it forsakes quality [1] that may comprise of intra-coded macro-blocks and lastly, bi-directionally predictive (B frame) that is coded on the basis of prior and future coded frames, with each providing different compression levels. Hence, the video sequence is initially divided into a group of pictures referred to as GOP [2, 65].

The MPEG compression algorithms [71] is attributed to its basis, which comprises of two kinds of methods – motion compensation and motion vector, where the former decreases the temporal redundancy and the latter transforms the domain (DCT) [72] according to compression to minimize the spatial redundancy. Moreover, motion-

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

compensated methods are employed with causal (pure predictive coding) as well as non-causal predictors (inter-polative coding). The prediction error in the form of the remaining signal is compressing with the help of spatial redundancy reduction (DCT). The motion related information is according to 8X8 macro-blocks and relayed along with the spatial information [73]. The spatial and temporal redundancy reductions are required for high compression of MPEG compression algorithms owing to the continuous frames which are quite similar to each other. In other words, if the first frame is encoded where ever region is relayed to the second frame, the latter can be predicted.

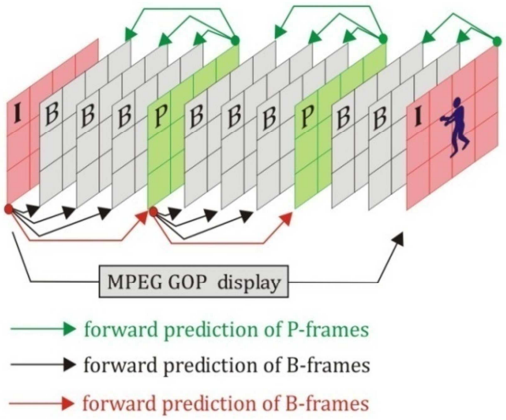

Figure: 7: Arrows Show Prediction Dependencies Between Frames

In a related study, Wang et al. [69] examined forgery in the aspect of error introduced when motion between frames is approximated in the MPEG video compression. According to them, the motion error turns are valuable as between each MPEG file frame, a predictable kind of motion error is detected. On the other hand, if the frames are removed, the error is noticeably changed. The combined outcome of error detection and the JPEG compression test is invaluable for detecting forgery when a handful of frames are removed (Wang & Farid.

7. DISCUSSION AND CONCLUSION

Among the fastest growing area of research in the field of video forgery detection is the passive-blind methods and detection methods to verify the integrity and authenticity of digital video sequence. To this end, current studies dedicated to passive-blind methods are not in need of prior knowledge of the video frames content or pre-embedded watermarks or signature. In this study, the issue of digital video manipulating detection is discussed with references to blind methods of video forgery detection. Various frames of video forgery detection methods are categorized and generalized in this paper and the rendering of some typical video forgery detection algorithms methods are compared. Some of the developed approaches for the detection and the determination of video manipulation are capable of localizing tampered object locations of frames sequence. This study's findings are expected to contribute to methods and ideas in the field of digital video forgery detection.

At the onset, the drawback of existing methods is related to issues of automation like human interpretation of poor outputs. Another is the modification and extension to determine the accurate location of the video forgery that involves methods that insert/remove frames and objects to determine the region of inconsistencies.

Accordingly, the first step identifies that the camera source identification is still confined to 9 to 15 cameras and in mobile camera identification and as such, the result can be negatively affected by the increasing number of cameras. It is not applicable for the detection of suspicious level regions in videos taken by a moving camera. Moreover, the camera source identification methods is noted to be dependent on intrinsic camera hardware features like lens and CCD sensor characteristics that generate valid outcomes compared to those based on the software parts of the camera (e.g. CFA interpolation algorithms). Further, the video double compression artifacts add difficulty to localization of the forgery especially when the video being analyzed is compressed by a low quality factor in most methods..

Second, the image-splicing forgery detection in its accurateness is depleted after processing operations, which could lead to edge blurring, loss of compression and added noise although confined to the detection methods that can be expanded to image and audio. Comprehending the perception of visual semantics is significant in the identification of the extent of forgery. Lastly, copy-move forgery detection are computationally expensive and they bring about high false positives, and use high correlation between original and forged parts of the video frames in order to detect and determine copy-paste forgery. However, high correlation between frames is commonplace in natural videos, and the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

method is not appropriate if copied regions are obtained from other views.

On the other hand, copy-move forgery localization methods that are based on frames are appropriate with frame detection duplication and not the localization of forged region in case the video content is consistent and the prior modified region had lower quality frames than the current frame. In the context of pixel-based approaches, the manipulation of detection accuracy impacts post-processing and compression and thus making the validation of performance measures (i.e. accuracy, robustness, security) becomes a major concern owing to the absence of established benchmarks and public testing dataset that evaluates the actual accuracy of digital video forgery approaches. Among the significant limitation of video forgery detection methods is their inability to distinguish between malicious manipulation and innocent retouching, like red-eye correction. Future studies are encouraged to determine a more robust statistical feature that are resistant to several post-processing operations.

REFERENCES

[1] Wang, W. (2009). Digital video forensics (Doctoral dissertation, Dartmouth College Hanover, New Hampshire).

[2] Sun, T., Wang, W., & Jiang, X. (2012, March). Exposing video forgeries by detecting MPEG double compression. In *Acoustics, Speech and Signal Processing (ICASSP), 2012 IEEE International Conference on (pp. 1389-1392). IEEE.*

[3] Suhail, M. A., & Obaidat, M. S. (2003). Digital watermarking-based DCT and JPEG model. *Instrumentation and Measurement, IEEE Transactions on, 52(5),* 1640-1647.

[4] Di Martino, F., & Sessa, S. (2012). Fragile watermarking tamper detection with images compressed by fuzzy transform. Information Sciences, 195, 62-90.

[5] Chen, H., Chen, Z., Zeng, X., Fan, W., & Xiong, Z. (2008, December). A novel reversible semi-fragile watermarking algorithm of MPEG-4 video for content authentication. In Intelligent *Information Technology Application, 2008. IITA'08. Second International Symposium on* (Vol. 3, pp. 37-41). IEEE.

[6] Ram, S., Bischof, H., & Birchbauer, J. (2009). Active fingerprint ridge orientation models. In *Advances in Biometrics* (pp. 534-543). Springer Berlin Heidelberg.

[7] Peng, F., Nie, Y. Y., & Long, M. (2011). A complete passive blind image copy-move forensics scheme based on compound statistics features. *Forensic science international*, 212(1), e21-e25.

[8] Shivakumar, B. L., & Santhosh Baboo, L. D. S. (2010). Detecting copy-move forgery in digital images: a survey and analysis of current methods. *Global Journal of Computer Science and Technology*, 10(7)..

[9] R. Esmaeilani, "Source Identification Of Captured Video Using Photo Response Non-Uniformity Noise Pattern And Svm Classifiers," 2014.

[10] Lin, C. S., & Tsay, J. J. (2014). A passive approach for effective detection and localization of region-level video forgery with spatio-temporal coherence analysis. *Digital Investigation.*

[11] Davarzani, R., Yaghmaie, K., Mozaffari, S., & Tapak, M. (2013). Copy-move forgery detection using multiresolution local binary patterns. *Forensic science international*, 231(1), 61-72.

[12] Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Del Tongo, L., & Serra, G. (2013). Copy-move forgery detection and localization by means of robust clustering with J-Linkage. *Signal Processing: Image Communication,* 28(6), 659-669.

[13] Shanableh, T. (2013). Detection of frame deletion for digital video forensics. *Digital Investigation,* 10(4), 350-360.

[14] Sheng, YL.,& Tian, Q H. (2013). Video Copy-Move Forgery Detection and Localization Based on Tamura Texture Features. In *International Congress on Image and Signal Processing (CISP 2013)* (pp. 864-868).

[15] Dong, Q., Yang, G., & Zhu, N. (2012). A MCEA based passive forensics scheme for detecting frame-based video tampering. *Digital Investigation*, 9(2), 151-159.

[16] Lin, G. S., & Chang, J. F. (2012). Detection of frame duplication forgery in videos based on spatial and temporal analysis. *International Journal of Pattern Recognition and Artificial Intelligence,* 26(07).

[17] Qadir, G., Yahaya, S., & Ho, A. T. (2012). Surrey university library for forensic analysis (SULFA) of video content.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[18] Di Martino, F., & Sessa, S. (2012). Fragile watermarking tamper detection with images compressed by fuzzy transform. *Information Sciences,* 195, 62-90.

[19] Di Martino, F., &Sessa, S. (2012). Fragile watermarking tamper detection with images compressed by fuzzy transform. *Information Sciences,* 195, 62-90.

[20] Lin, C. S., &Tsay, J. J. (2014). A passive approach for effective detection and localization of region-level video forgery with spatio-temporal coherence analysis. *Digital Investigation.*

[21] Shivakumar, B. L., & Santhosh Baboo, L. D. S. (2010). Detecting copy-move forgery in digital images: a survey and analysis of current methods. *Global Journal of Computer Science and Technology*, 10(7).

[22] Shaid, S. Z. M. (2009). *Estimating optimal block size of copy-move attack detection on highly textured image* (Doctoral dissertation, Thesis Submitted to the University of Technology, Malaysia, 2009. Available at http://www. csc. fsksm. utm. my/syed/images/files/publications/thesis/estimating_ optimal_block_size_for_copy-move_attack_detection_on_highly_textured_image. pdf)..

[23] Kot, A. C., & Cao, H. (2013). Image and Video Source Class Identification. In *Digital Image Forensics* (pp. 157-178). Springer New York.

[24] Popescu, A. C., &Farid, H. (2005). Exposing digital forgeries in color filter array interpolated images. *Signal Processing, IEEE Transactions on,* 53(10), 3948-3959.

[25] Kang, X., Li, Y., Qu, Z., & Huang, J. (2012). Enhancing source camera identification performance with a camera reference phase sensor pattern noise. *Information Forensics and Security, IEEE Transactions on*, 7(2), 393-402.

[26] Redi, J. A., Taktak, W., &Dugelay, J. L. (2011). Digital image forensics: a booklet for beginners. Multimedia Tools and Applications, 51(1), 133-162.

[27] Birajdar, G. K., &Mankar, V. H. (2013). Digital image forgery detection using passive techniques: A survey. *Digital Investigation,* 10(3), 226-245.

[28] Chen, M., Fridrich, J., Goljan, M., & Lukáš, J. (2007). Source digital camcorder identification using sensor photo response non-uniformity. In *Electronic Imaging* 2007 (pp. 65051G-65051G). International Society for Optics and Photonics.

[29] Kurosawa, K., Kuroki, K., & Saitoh, N. (1999). CCD fingerprint method-identification of a video camera from videotaped images. In *Image Processing,* 1999. ICIP 99. Proceedings. 1999 International Conference on (Vol. 3, pp. 537-540). IEEE.

[30] Thajeel, S. A., &Sulong, G. B. (2013). State of the art of copy-move forgery detection techniques: a review. *International Journal of Computer Science Issues (IJCSI),* 10(6).

[31] Chen, L., Lu, W., Ni, J., Sun, W., & Huang, J. (2013). Region duplication detection based on Harris corner points and step sector statistics. *Journal of Visual Communication and Image Representation,* 24(3), 244-254.

[32] Liu, M. H., & Xu, W. H. (2011). Detection of copy-move forgery image based on fractal and statistics. Jisuanji Yingyong/ *Journal of Computer Applications*, 31(8), 2236-2239.

[33] Johnson, M. K., & Farid, H. (2007). Exposing digital forgeries through specular highlights on the eye. In *Information Hiding* (pp. 311-325). Springer Berlin Heidelberg.

[34] Farid, H. (2003). A picture tells a thousand lies. New Scientist, (2411), 38-41.

[35] Li, X., Jing, T., & Li, X. (2010, December). Image splicing detection based on moment features and Hilbert-Huang transform. In *Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on* (pp. 1127-1130). IEEE.

[36] Wang, W., & Farid, H. (2009, September). Exposing digital forgeries in video by detecting double quantization. In *Proceedings of the 11th ACM workshop on Multimedia and security* (pp. 39-48). ACM.

[37] Wu, X., Li, J., Zhang, Y., & Tang, S. (2008). Spatio-temporal visual consistency for video copy detection.

[38] Kobayashi, M., Okabe, T., & Sato, Y. (2010). Detecting forgery from static-scene video based on inconsistency in noise level functions. *Information Forensics and Security, IEEE Transactions on*, 5(4), 883-892.

[39] Kim, C., & Vasudev, B. (2005). Spatiotemporal sequence matching for efficient video copy detection. Circuits and Systems for Video Technology, *IEEE Transactions on*, 15(1), 127-132.

[40] Xiaoling, C., & Huimin, Z. (2012). A Novel Video Tamper Detection Algorithm Based on

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Semi-fragile Watermarking. In *Advances in Information Technology and Industry Applications* (pp. 489-497). Springer Berlin Heidelberg.

[41] Wang, W., & Farid, H. (2007, September). Exposing digital forgeries in video by detecting duplication. In *Proceedings of the 9th workshop on Multimedia & security* (pp. 35-42). ACM.

[42] Subramanyam, A. V., & Emmanuel, S. (2012, September). Video forgery detection using HOG features and compression properties. In *Multimedia Signal Processing (MMSP), 2012 IEEE 14th International Workshop on* (pp. 89-94). IEEE.

[43] Wang, W., & Farid, H. (2006, September). Exposing digital forgeries in video by detecting double MPEG compression. In *Proceedings of the 8th workshop on Multimedia and security* (pp. 37-47). ACM.

[44] Su, L., Huang, T., & Yang, J. (2014). A video forgery detection algorithm based on compressive sensing. *Multimedia Tools and Applications*, 1-16.

[45] Hsu, C. C., Hung, T. Y., Lin, C. W., & Hsu, C. T. (2008, October). Video forgery detection using correlation of noise residue. In *Multimedia Signal Processing, 2008 IEEE 10th Workshop on* (pp. 170-174). IEEE.

[46] Kancherla, K., &Mukkamala, S. (2012). Novel blind video forgery detection using markov models on motion residue. In *Intelligent Information and Database Systems* (pp. 308-315). Springer Berlin Heidelberg.

[47] Sheng, YL., & Tian, Q H. (2013). Video Copy-Move Forgery Detection and Localization Based on Tamura Texture Features. In *International Congress on Image and Signal Processing (CISP 2013)* (pp. 864-868).

[48] Davarzani, R., Yaghmaie, K., Mozaffari, S., &Tapak, M. (2013). Copy-move forgery detection using multire solution local binary patterns. *Forensic science international*, *231*(1), 61-72.

[49] Sheng, YL.,& Tian, Q H. (2013). Video Copy-Move Forgery Detection and Localization Based on Tamura Texture Features. In *International Congress on Image and Signal Processing (CISP 2013)* (pp. 864-868).

[50] Upadhyay, S., & Singh, S. K. (2011, November). Learning based video authentication using statistical local information. *In Image Information Processing (ICIIP), 2011 International Conference on* (pp. 1-6). IEEE.

[51] Yu, J., &Srinath, M. D. (2001). An efficient method for scene cut detection.Pattern Recognition Letters, 22(13), 1379-1391.

[52] Thakur, M. K. (2013). Tampered videos: detection and quality assessment.

[53] Kobayashi, M., Okabe, T., & Sato, Y. (2009). Detecting video forgeries based on noise characteristics. In Advances in *Image and Video Technology* (pp. 306-317). Springer Berlin Heidelberg.

[54] Atrey, P. K., Yan, W. Q., &Kankanhalli, M. S. (2007). A scalable signature scheme for video authentication. Multimedia Tools and Applications, 34(1), 107-135.

[55] Wolf, S., & Pinson, M. (2009, January). A no reference (nr) and reduced reference (rr) metric for detecting dropped video frames. *In Fourth International Workshop on Video Processing and Quality Metrics for Consumer Electronics, VPQM.*

[56] Shih, T. K., Tang, N. C., & Hwang, J. N. (2007, July). Ghost shadow removal in multi-layered video inpaintinga. In *Multimedia and Expo, 2007 IEEE International Conference on* (pp. 1471-1474). IEEE.

[57] Dalal, N., &Triggs, B. (2005, June). Histograms of oriented gradients for human detection. In *Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on* (Vol. 1, pp. 886-893). IEEE.

[58] Zhang, J., Su, Y., & Zhang, M. (2009, October). Exposing digital video forgery by ghost shadow artifact. In *Proceedings of the First ACM workshop on Multimedia in forensics* (pp. 49-54). ACM.

[59] Qin, Y. L., Sun, G. L., Wang, S. Z., & ZHANG, X. P. (2010). Blind Detection of Video Sequence Montage Based on GOP *Abnormality. Act Electronica Sinica*, 38 (7), 1597-1602.

[60] Richao, C., Gaobo, Y., & Ningbo, Z. (2014). Detection of object-based manipulation by the statistical features of object contour. *Forensic Science International*.

[61] Wang, Q., Li, Z., Zhang, Z., & Ma, Q. (2014). Video Inter-Frame Forgery Identification Based on Consistency of Correlation Coefficients of Gray Values. *Journal of Computer and Communications*, *2*(04), 51.

[62] SU, L., HUANG T. & YANG J. (2014). A video forgery detection algorithm based on

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

compressive sensing.*Multimedia Tools and Applications, 1-16.*

[63] Jaiswal, S., &Dhavale, S. (2013). Video Forensics in Temporal Domain using Machine Learning Techniques. *International Journal of Computer Network & Information Security*, *5*(9).

[64] Bestagini, P., Milani, S., Tagliasacchi, M., &Tubaro, S. (2013). Local tampering detection in video sequences. In *Multimedia Signal Processing (MMSP), 2013 IEEE 15th International Workshop on* (pp. 488-493). IEEE.

[65] Vázquez-Padın, D., Fontani, M., Bianchi, T., Comesana, P., Piva, A., &Barni, M. (2012). Detection of video double encoding with GOP size estimation. In*IEEE Int. Workshop on Information Forensics and Security (WIFS)*.

[66] Chen, R., Dong, Q., Ren, H., & Fu, J. (2012). Video Forgery Detection Based on Non-Subsampled Contourlet Transform and Gradient Information. *Information Technology Journal*, *11*(10).

[67] Chetty, G., Biswas, M., & Singh, R. (2010). Digital video tamper detection based on multimodal fusion of residue features. In *Network and System Security (NSS), 2010 4th International Conference on* (pp. 606-613). IEEE.

[68] Su, Y., Zhang, J., & Liu, J. (2009, December). Exposing digital video forgery by detecting motion-compensated edge artifact. In *Computational Intelligence and Software Engineering, 2009. CiSE 2009. International Conference on* (pp. 1-4). IEEE.

[69] Wang, W., &Farid, H. (2007, September). Exposing digital forgeries in video by detecting duplication. In *Proceedings of the 9th workshop on Multimedia & security* (pp. 35-42). ACM.

[70] Xin, J., Lin, C. W., & Sun, M. T. (2005). Digital video transcoding. Proceedings of the IEEE, 93(1), 84-97.

[71] Le Gall, D. (1991). MPEG: A video compression standard for multimedia applications. *Communications of the ACM,* 34(4), 46-58.

[72] Fridrich, A. J., Soukal, B. D., &Lukáš, A. J. (2003). Detection of copy-move forgery *in digital images. In in Proceedings of Digital Forensic Research Workshop*

[73] Richardson, I. E. (2004). H. 264 and MPEG-4 video compression: video coding for next-generation multimedia. John Wiley & Sons.