DIGITAL VIDEO INPAINTING DETECTION USING CORRELATION OF HESSIAN MATRIX

Mustapha Aminu Bagiwa[1], Ainuddin Wahid Abdul Wahab[2], Mohd Yamani IdnaIdris[3], Suleman Khan[4]

[1, 2, 3, 4] Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, 50603, Kuala Lumpur, Malaysia

[1]Department of Mathematics, Faculty of Science
Ahmadu Bello University, Zaria
Nigeria
Email: mstphaminu@siswa.um.edu.my[1], ainuddin@um.edu.my[2], yamani@um.edu.my[3], suleman@siswa.um.edu.my[4]

ABSTRACT

The use of digital video during forensic investigation helps in providing evidence related to crime scene. However, due to freely available user friendly video editing tools, the forgery of acquired digital videos that are used as evidence in a law suit is now simpler and faster. As a result, it has become easier for manipulators to alter the contents of digital evidence. For instance, inpainting technique is used to remove an object from a video without leaving any artefact of illegal tampering. Therefore, this paper presents a technique for detecting and locating inpainting forgery in a video sequence with static camera motion. Our technique exploits statistical correlation of Hessian matrix (SCHM) to detect and locate tampered regions within a video sequence. The results of our experiments prove that the technique effectively detect and locate areas which are tampered using both texture and structure based inpainting with an average precision rate of 99.79% and an average false positive rate of 0.29%.

Keywords: Digital Video, Video Forensic, Video Forgery, Video Inpainting, Hessian Matrix

1.0 INTRODUCTION

The advancement in digital technology coupled with the influx of user friendly multimedia acquisition devices has made the use of media applications such as digital videos very common in our daily lives[1][2].However, due to the nature and usage of these media applications, it has become hard to find tampering artefact with naked eyes in a video created by a forgery process[3][4]. Such forgery processes have raised the question of integrity and validity of digital videos, especially when presented as admissible legal evidence in a court of law. In order to validate the integrity and authenticity of digital videos, video forensic related approaches were developed. Video forensic has recently witnessed a great deal of concern in the research community because of its extensive applications in different areas ranging from digital media corporations, scientific research, publications, journalism, criminal investigations, and security surveillance systems that require the authentication and verification of a digital video as discussed in[5].The advancement in digital video technology has facilitated the way videos are manipulated using less expensive and affordable softwares such as Premiere[1] and Vegas[2] without leaving a visual trace[6][7]. Illegal manipulation of digital video is extremely difficult and sometimes impossible to detect using visual examination.

There are numerous illegal manipulation attacks to be performed on a digital video. These manipulation attacks include copy move attacks [8], duplication attacks [9], object removal or insertion [10] using inpainting, and chroma key technique respectively.

Inpainting manipulation is a technique used to illegally remove or restore an object from a video by taking the advantage of the temporal and spatial information arising from neighbouring scenes within the video.

Common forensic approaches for detecting video inpainting involve the use of either active or passive approaches as discussed in[11]. Active approaches are based on watermark and digital signatures [12][13]. Passive or blind approaches are based on the analysis of extracted internal features of a video called artefacts or fingerprints as discussed in [2][14][15]. The artefacts are created or introduced during a video processing task and are useful for forgery detection[16]. An example of such artefacts includes chromatic aberration from

[1]http://www.adobe.com/products/premiere-elements.html
[2]http://www.sonycreativesoftware.com/vegaspro.html

camcorder lens [17][18][19], dust on lenses[20], noise from sensors[21], and hardware imperfections; which may involve faults or defects[22]. Therefore, this research has been motivated by the rate at which digital videos are been forged without leaving a visual clue of illegal tampering.

This paper addresses forgery detection that is done using both texture and structure inpainting in a digital video. We suggest the use of Statistical Correlation of Hessian Matrix (SCHM) property of a video for inpainting forgery detection in a digital video.

Moreover, the paper is divided into 8 sections. Section 2 explained the introduction to inpainting forgery; Section 3 discusses related work on video inpainting detection techniques. Section 4 discusses our proposed detection technique based on SCHM. Section 5 highlights the experimental results of the technique and Section 6 provides a comparison of our proposed technique with other techniques selected from the literature. Section 7 provides a discussion while summary and conclusions are mentioned in Section 8.

2.0 VIDEO INPAINTING

Generally, inpainting is a restoration mechanism that involves the gradual filling of an area in a digital image or video by its neighbouring pixel information [23]. The use of inpainting technique started with digital images, but has gradually extended to digital videos. Initially, inpainting technique was used to remove portions that are damaged in an old image using its neighbour pixel information. A user chooses an object that is to be removed and the inpainting algorithm automatically completes the damaged portion with the information from neighbouring pixels. Schemes for digital inpainting are categorized into two types such as structure and texture inpainting [24].

Structure based inpainting fills in the video frame damaged region with information extracted from a structured region similar to copy paste technique while in texture inpainting; the damaged region is filled using the neighbourhood pixel information from the video frame.

Moreover, inpainting have a number of applications ranging from restoration to compression of digital images and videos. However, digital video manipulators exploit inpainting technique to create a forged video by removing objects from it and filling the empty area with matching background content from the same video. Shown in Fig.1 is an example of video inpainting forgery in which a walking man is been removed in a video frame in Fig.1(a) and the region completed with textures that are sampled from another part of the frame in Fig.1(b)[25].

a. Original frame b. Inpainted frame

Fig. 1 Example of digital inpainting

3.0 RELATED WORK

There are ongoing researches on video inpainting forgery detection. The approaches that are used in video inpainting detection are divided into active and passive techniques as shown in Fig. 2.

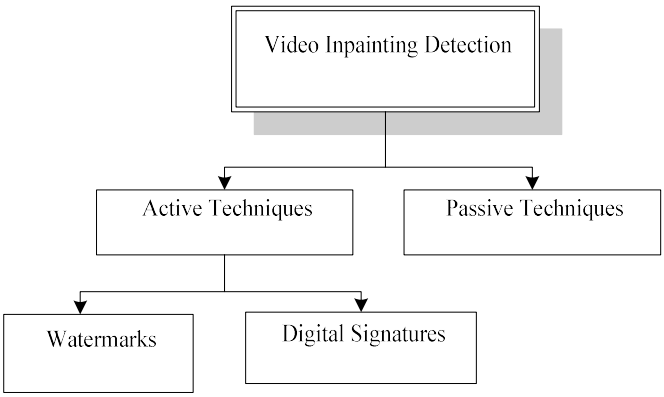

Fig.2 Video inpainting detection approaches

Active detection techniques rely on the use of watermark and digital signatures. However, the problem with active techniques is the insertion of digital watermark into the video which requires the use of some trusted devices. This problem makes active techniques unsuitable for tampering detection. Passive techniques on the other hand focus on the extraction of salient features called artefacts from a video. These artefacts are similar to the traces of evidence that are found at a physical crime scene during investigation. Once the traces are identified, techniques can be developed to extract and analyze them for anomalies that will signify illegal alteration. This is why passive technique is useful for detecting illegal tampering and has been of keen interest in the forensic community nowadays. Passive techniques are based on a hypothesis that excellent tampering will elude human visual detection. However, the statistical or mathematical characteristics of the video may be altered in the process. The difference between active and passive technique in video forensic in terms of the approach used for each technique, target, application requirements, and objective are highlighted in Table 1.

Table 1 Active versus passive technique

Video Forensic Techniques	Approach Used	Target	Application Requirement	Strength
Active techniques	Watermark and Digital Signatures	Authentication	Robustness and sensitivity	Integrity verification
Passive techniques	Mathematical features analysis	Tampering detection	Robustness, sensitivity and good precision rate	Illegal tampering detection and integrity verification

Variety of passive techniques for video forensic analysis are an extension of image forensic analysis for tampering detection [26]. Moreover, most passive techniques are based on the video characteristics and tampering artefacts. An example of such characteristics and artefacts includes noise residue characteristics [27], readout noise characteristics [28], sensor pattern noise, variation in noise level functions [29], ghost shadow artefacts [30], and lightening and compression artefacts [31].

A technique was proposed to detect illegal video manipulation using readout noise feature in [28]. Dual forgery schemes were addressed with this technique. The first forgery scheme addressed is frame insertion within a sequence of video frames; the detection of such forgery was achieved by making a comparison of each frame readout noise with the mean readout noise from the entire video. The second forgery scheme addressed involves region tampering or inpainting within a frame. This kind of forgery is identified using the statistical comparison of the readout noise across a frame region and the mean readout noise of the entire video frames. Their paper is only theoretical with little experimental details. However, it is still considered as the pioneer work in video inpainting forgery detection.

Another video inpainting forgery detection technique with a more experimental backing that uses the mathematical analysis of discrete cosine transform (DCT) coefficient was proposed in [32].This method

comprises of a three stage process involving DCT block formation, quantization, and entropy coding. The method has an inpaint forgery detection rate of 88%. However, this method suffers lower quantization when dealing with high compression quality videos.

Furthermore, a forgery detection technique involving tampered region from an inpainting operation in a video using statistical noise residue correlation(SCNR) was proposed in [27]. The detection technique relies on a fact that tampering affects the SCNR within frame regions in a video thereby producing a mark difference between the tampered and non-tampered areas. The technique uses a wavelet de-noising filter to extract the noise residue from a video[33]. A blocking partition of size $\boldsymbol{N} \times \boldsymbol{N}$ is done on individual frame. The mathematical correlation across neighboured partitions are analysed for inpainting forgery detection. The result of the method has witnessed a good detection rate only for good quality videos. The authors define good quality videos as videos having 30 frames per second(fps) and a frame resolution of (720×480) with a 8.5 Mbps bit rate. Experimental results of the technique show that the use of noise statistics is a dependable mechanism for good quality digital videos with an average detection precision rate of 98.22% whereas, delicate when dealing with compressed videos. Moreover, obtaining the noise residue from a video during forensic analysis is difficult and takes a reasonable time to achieve. Though, their finding reveals that the quality of a video affects the inpainting forgery identification precision. It also highlighted the need for better and faster features since noise feature extraction takes time to achieve.

Photo shot noise feature was proposed in order to address the noise feature extraction and video quality issue in [27] as discussed in [34][35]. Implemented for different purpose, the photo shot noise feature was used to detect tampered regions in a video from an inpainting operation in [36]. Regions in a video forged by another video that originated from another camera from an inpainting operation will show inconsistencies with other sections of the video that are not forged. However, the technique only focuses on static video scenes. Inpainting forgery operation associated with a moving object at that time remains an open problem.

The use of Ghost Shadow Artefacts(GSA) was proposed in order to detect video inpainting forgery associated with moving objects in[30]. GSA are unnatural flicker like structures that are observed in a video resulting from the discontinuity across an inpainted region [37]. The authors create a panoramic image called mosaic by combining multiple frames together. Mathematical morphological operations and accumulative differencing were used to obtain the moving foreground track. Inconsistency between mosaic foreground and that of the foreground track indicates forgery. However, the technique is more reliable to videos having undergone MPEG compression and recompression.

In order to address the problem of uncompressed videos, a technique used to detect inpainting video forgery using zero connectivity feature and fuzzy[38] membership function was proposed in[39]. A video is segmented into multiple independent frames. A zero connectivity label is then applied on blocks to get a matching degree for all blocks in forged areas. A construction of an ascending semi – trapezoid membership function is performed for the computation of fuzzy membership function. Finally, tampered regions are determined using a cut set method. Experimental results of the technique record a 95% detection rate. The limitation of this work is its applicability to only uncompressed videos.

A technique involving compressed and uncompressed video used for detecting object removal from inpainting that use artefacts from blocked motion estimation analysis was proposed in [40]. The technique extracts motion features across adjacent frames. Motion vector magnitude is used as the determinant between tampered and non-tampered portions of the video. Experiments have shown that the technique is efficient in detecting inpainting forgery in a video that is recorded with a moving background. However, sophisticated inpainting that involves complex interpolation algorithms such as spline interpolation remains a challenge to this technique. This challenge arises because of the discrepancies in motion vector estimation.

The challenge of motion vector estimation from the technique in [40] was addressed by introducing the concept of practical quantization estimation theory in [41]. A pixel from a particular frame is estimated across a collection of pixels that are derived from other frames in a Group of Picture(GOP). The error existing from the exact and estimated value is compared against a pre-defined threshold for the identification of double compression frames and frames from a GOP. Experiments have shown the method is successful and used to detect inpainting forgery of interlaced, progressive, or lower bit rate frames in a GOP. However, frames and small region tamper localization pose a challenge to this method.

Inpainting forgery detection and localization approach by statistically analysing artefacts from a temporal spatial domain of a 3D video was proposed in [42]. Experiments have shown the technique has reasonable copy paste inpainting detection accuracy for good quality videos.

An improvement on the work of [42] was presented in [43] by automatically locating the exact region of tampering in a 3D video. The technique detects and locate tampered region in a video from inpainting using spatio-temporal slicing and coherence analysis (STCA). The abnormality in the spatio-temporal coherence between tampered regions within video sequence is used as an evidence for tampered region identification. However, the technique has a high computational complexity.

In this paper, we exploit the statistical correlation existing between the Hessian Matrix properties from a video sequence to detect inpainting forgery. This work provides a solution for the need and use of better and faster features for digital video inpainting forgery identification.

4.0 PROPOSED DETECTION TECHNIQUE

This section provides the discussion of our proposed technique for structure and texture based inpainting forgery detection. Our technique is aimed at detecting regions in a video that are tampered using structure and texture based inpainting. A stepwise detection chart of our proposed technique including pre-processing, hessian correlation of spatially indexed blocks and forged region identification is shown in Fig. 3 below.

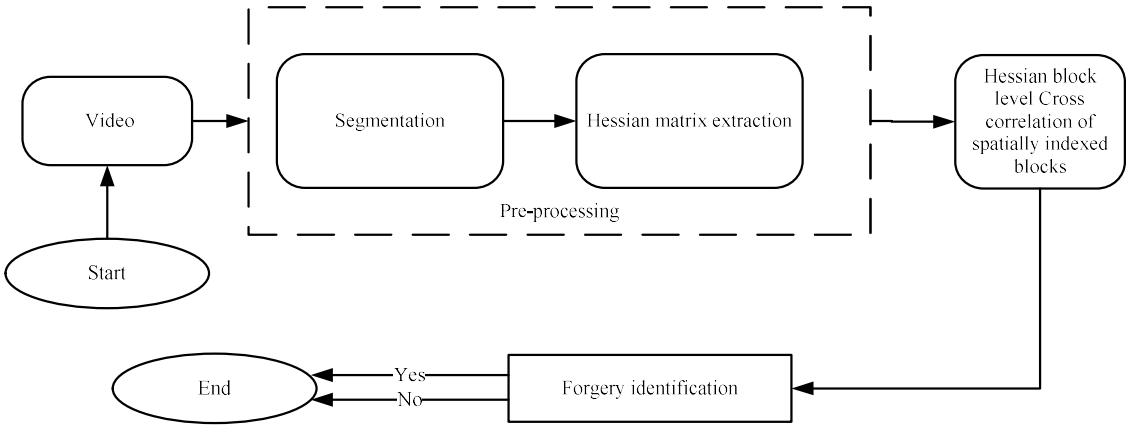

Fig.3 Block diagram of proposed approach

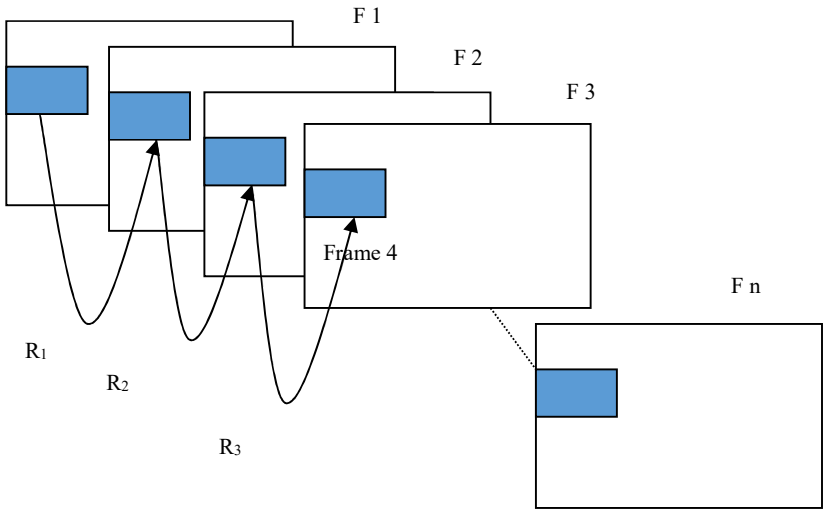

Fig.4 Correlation computation of Hessian matrix

A video to be analyzed for inpainting forgery detection is first divided into multiple independent frames. A frame is a digital still image that is extracted from a digital video. An example is shown in Fig. 4 in which F1 represent frame 1, F2 represent frame 2, F3 represent frame 3 and Fn represent frame n where n is the last frame of the video. Each frame is further divided into blocks of $\boldsymbol{N} \times \boldsymbol{N}$ partitions shown as shaded sections of Fig. 4, where the value of $\boldsymbol{N}$ is 16. We choose a small value of $\boldsymbol{N}$ in order to obtain a reduced dimension representation that will allow the identification of the variation of hessian correlation values from the video.

The next step is the pre-processing step in which an automatic segmentation is performed on each frame of the video using a mathematical morphological operation segmentation technique. The Hessian Matrix corresponding to each frame block is then computed in order to obtain the corresponding eigenvalues and eigenvectors. The correlation $\boldsymbol{R}$ of the Hessian Matrix blocks is computed as shown in Fig. 4.

Finally, tampered regions are located by the analysis of block level Hessian Matrix correlations. This is achieved using an Otsu threshold mechanism in order to obtain a better classification. A pseudo code description of the algorithmic steps is shown in algorithm 1 below.

Algorithm 1: Pseudo code description of algorithm

Algorithm

Input
A video sequence with frames
Output
Inpainted video frame blocks

1. Read video
2. Partition the video sequence into frames $f_1, f_2, f_3 \ldots \ldots \ldots f_n$
3. Next_Frame = 1
4. Number_Of_Frames← n
5. while (Next_Frame< = Number_Of_Frames)
6. {
7. *Divide the segmented frames into $\boldsymbol{N} \times \boldsymbol{N}$ block sizes*
8. *Perform semi-automatic segmentation on each frame*
9. *Generate the Hessian Matrix for each $\boldsymbol{N} \times \boldsymbol{N}$frame block*
10. *Perform block level correlation computation $\boldsymbol{R}$between neighboured $\boldsymbol{N} \times \boldsymbol{N}$blocks*
11. *If ($\boldsymbol{R}$> a predefined threshold){*
12. *block is tampered*
13. *Else*
14. *block not tampered*
15. *}*
16. *Next_Frame= Next_Frame+ 1*
17. }
18. End While
19. End

4.1 Segmentation

In order to provide image frames that will represent meaningful and convenient information for ease of analysis, we perform a semi-automatic segmentation onto the entire video frames. This allows us to locate original objects in each frame and its corresponding boundaries such as line and curves. In the experiment, sefexa[3]semi-automatic image segmentation tool was used to obtain the segmentation model across the entire video frame as shown in Fig. 5a and 5b.

[3]http://www.fexovi.com/sefexa.html

Original frame 1 Inpainted frame 1 Segmented frame 1

(a)

Original frame 2 Inpainted frame 2 Segmented frame 2

(b)

Fig.5 Segmentation of video frames

4.2 Hessian Matrix Generation

For a given sequence of frames belonging to a video, the Hessian Matrix is derived from the frame 2nd order partial derivative [44]. Given a video sequence represented as a continuous function $v(f_1, f_2, \dots, f_n)$ where v is a video having multiple frame sequences. The Hessian Matrix represented by H_m of the video v is given by equation 1.

$$H_m = \begin{bmatrix} \frac{\partial^2 v}{\partial f_1^2} & \frac{\partial^2 v}{\partial f_1 \partial f_2} \dots \dots & \frac{\partial^2 v}{\partial f_1 \partial f_n} \\ \frac{\partial^2 v}{\partial f_1 \partial f_2} & \frac{\partial^2 v}{\partial f_2^2} \dots \dots & \frac{\partial^2 v}{\partial f_2 \partial f_n} \\ \frac{\partial^2 v}{\partial f_1 \partial f_1} & \frac{\partial^2 v}{\partial f_n \partial f_2} \dots \dots & \frac{\partial^2 v}{\partial f_n^2} \end{bmatrix} \quad (1)$$

The partial derivatives are obtained by calculating the difference in intensity between neighbourhoods of the pixels in the segmented frames by applying equation 1. The difference in the intensity between pixels in the same neighbourhood is calculated by scanning each frame in the video in a single pass keeping a running count of the number of pixels at each intensity value which in turn can be used to construct a visual histogram of the intensity differences between neighboured pixels.

Light intensity affects the scene radiance of a video, thereby creating variations in the pixel intensity levels across certain pixel regions within a video frame. This variation is a good clue for tamper detection. Thus, a Hessian Matrix provides a description of a 2nd order intensity variations surrounding a chosen pixel region[45]. Once the Hessian Matrix is obtained, the eigenvalues and eigenvectors can be easily obtained to extract the orthonormal coordinates aligning the second order structure of each frame [46].The extracted Hessian Matrix $H(i,j)$ from the video frame is used in our technique to identify tampered regions. The general advantage of using the Hessian Matrix property is mainly because of its reliability in identifying characteristic interest points for image analysis.

In addition, the rationale behind the use of Hessian Matrix in this paper is its uniqueness in establishing a better and faster mechanism for which key points in a video frame can be calculated across pixel blocks. This allows the ease for the identification of intensity gradient changes across frame pixel blocks with less computation burden thereby simplifying the detection technique.

4.3 Correlation of Hessian Determination

Let $H(i,j)$denotes the generated Hessian Matrix at pixel values from the 2nd order intensity variations surrounding a chosen pixel block of size $\boldsymbol{N \times N}$. We modelled the correlation existing between $\boldsymbol{N \times N}$ neighboured frame blocks as represented in Fig. 4 by equation 2.

$$R = \frac{\Sigma_{i=1}^{n}\Sigma_{j=1}^{n}\left(H_{i,j}^{t}-\bar{H}\right)\left(H_{i,j}^{t-1}-\bar{H}\right)}{\sqrt{\Sigma_{i=1}^{n}\Sigma_{j=1}^{n}\left(H_{i,j}^{t}-\bar{H}\right)^{2}\left(H_{i,j}^{t}-\bar{H}\right)^{2}}} \qquad (2)$$

Where t represents the t^{th}frame and $\overline{H}$ is the average of the Hessian Matrix for all frames t_i where i takes a value from 1, 2, 3,……, n and n representing the last frame in the video. The statistical correlation of the Hessian Matrix in a forged region is usually changed in terms of increment or decrement depending on the kind of forgery done. Fig. 6 and Fig.7 are histograms of correlation for two aligned frames for structure and texture video inpainting forgery respectively at an Otsu threshold of 0.9956. The curves represent the non-tampered hessian blocks and regions that are tampered.

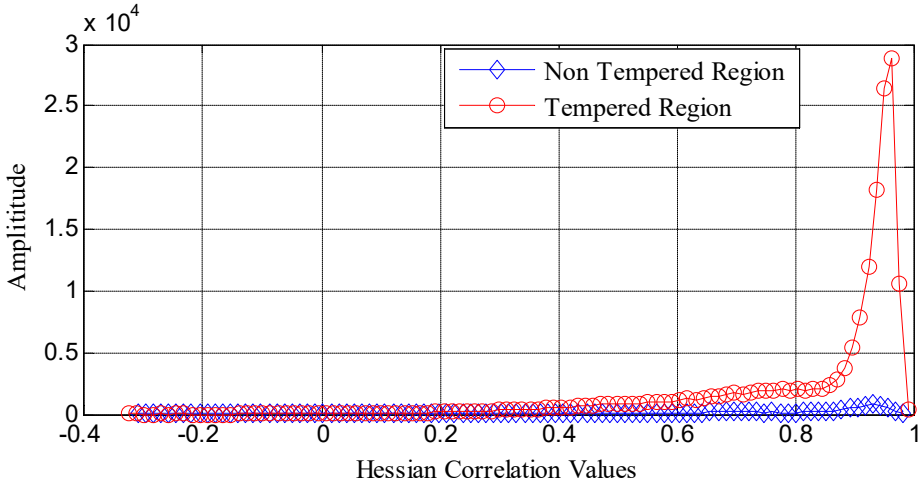

Fig.6 Hessian values correlation between two neighbouring video frame for structure based inpainting

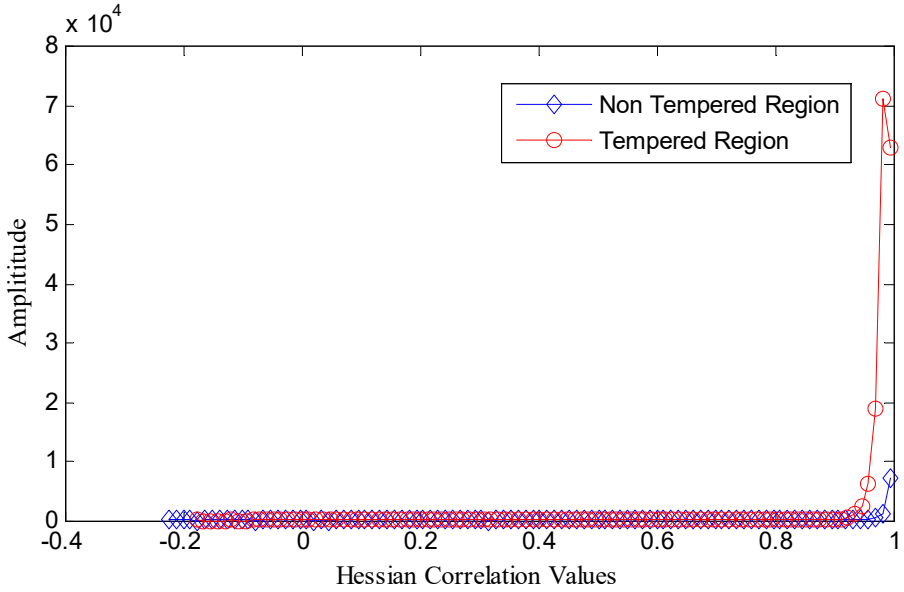

Fig. 7 Hessian values correlation between two neighbouring video frame for texture based inpainting

As shown in Fig.6 above, correlations of the two slopes are noticeably different. The graph shows a considerably high variation in amplitude of the correlation of hessian values from 0.6 to 1 between the two slopes while an almost equal correlation values can be observed from -0.2 to 0.6. The high variation in the correlation between the spatially indexed block is caused as a result of big object tampering in some regions of the video frame where the object has been removed. The same can be observed in the hessian correlation values in Fig. 7 between the ranges of 0.9 to 1.
In order to further test the robustness of our proposed technique, we conducted similar experiments on tampered videos involving small object removal as shown in Fig. 8 in which a small bird is removed from a video.

Fig.8 Sample frames for small region inpaint

The histograms of hessian correlation for the small inpaint region forgery detection from Fig. 8 are shown in Fig. 9 and Fig. 10 for structure and texture video inpainting at an Otsu threshold of 0.9956.

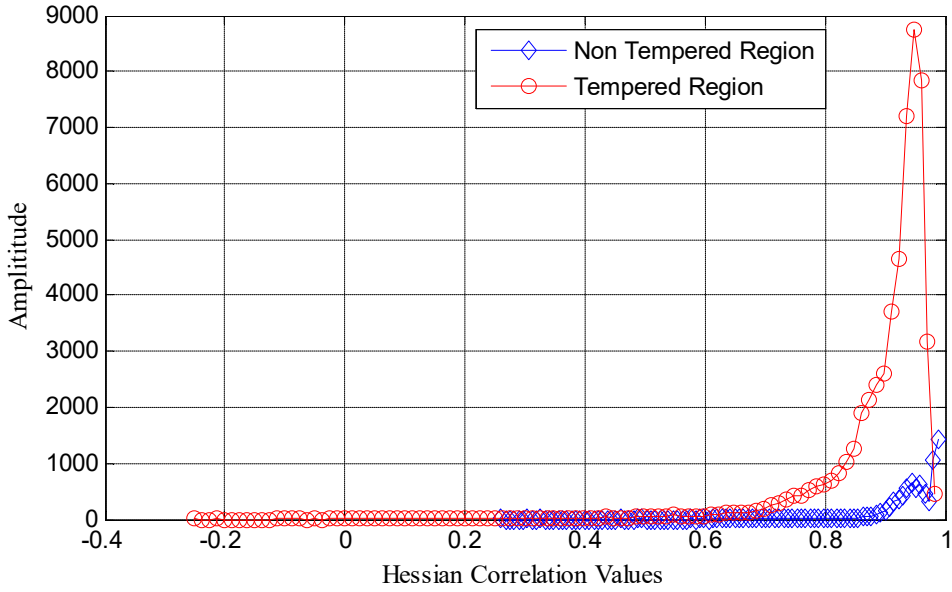

Fig.9 Hessian values correlation between two neighbouring video frame for small object structure based inpainting

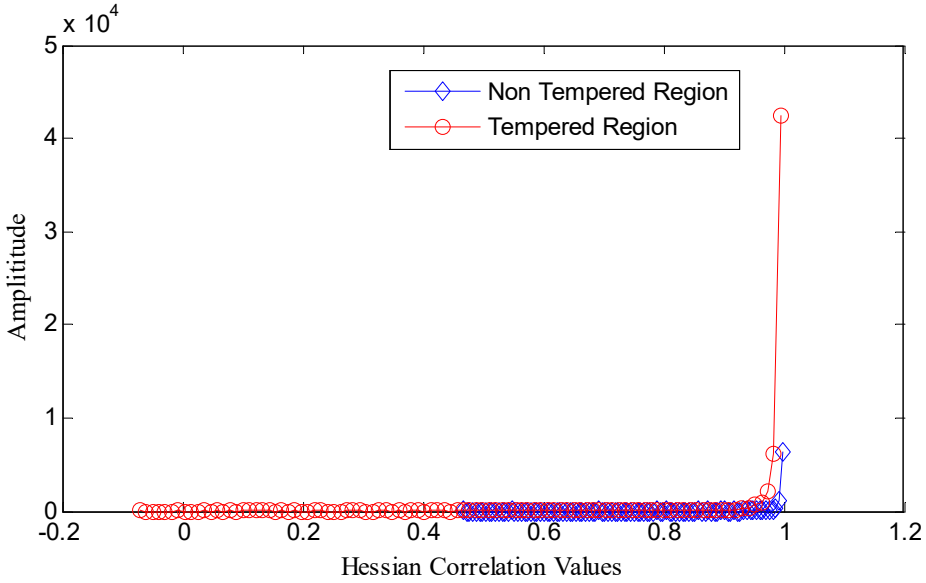

Fig.10 Hessian values correlation between two neighbouring video frame for small object texture based inpainting

The difference of hessian correlation of the affected region shows high variations interms of amplitude for structure based inpainting while a low amplitude variation is observed for texture based inpainting. This proves that the size of the object that is removed from a video has no significant impact on the overall proposed detection technique. However, the variation of correlation in terms of amplitude might differ depending on the inpainting mechanism used.

5.0 EXPERIMENTAL RESULTS

In our experiment, we made use of twenty test video sequences having a still background that are obtained from [25] and [27]. The summary of the test videos with respect to the number of frames for independent video, frame size, total objects within the video, and objects been removed are shown in Table 2.

Table 2 Summary of test videos

Test Video	No of Frames	Frame Size	No. of objects	Removed Objects
Video Sequence 1	330	320 × 240	6	1
Video Sequence 2	190	720 × 480	1	1
Video Sequence 3	200	720 × 480	1	1
Video Sequence 4	162	320 × 240	1	1
Video Sequence 5	200	480 × 720	5	1
Video Sequence 6	200	240 × 320	3	1
Video Sequence 7	200	240 × 320	8	1
Video Sequence 8	200	240 × 320	25	1
Video Sequence 9	340	240 × 320	2	1
Video Sequence 10	528	240 × 320	5	1
Video Sequence 11	200	240 × 320	1	1
Video Sequence 12	200	240 × 320	1	1
Video Sequence 13	200	240 × 320	1	1
Video Sequence 14	512	240 × 320	4	1
Video Sequence 15	320	240 × 320	1	1

Video Sequence 16	180	240 × 320	6	1
Video Sequence 17	120	240 × 320	3	1
Video Sequence 18	120	240 × 320	1	1
Video Sequence 19	200	240 × 320	1	1
Video Sequence 20	200	240 × 320	2	1

The proposed detection technique is evaluated based on two performance metrics rates. The metrics are precision and false positive rates. The results are summarised in Table 3 with a high precision rate and low false positive rates.

Table 3. Performance evaluation of the proposed technique

Video	Precision (%)	False Positive (%)
Video Sequence 1	99.54	0.78
Video Sequence 2	99.86	0.07
Video Sequence 3	99.97	0.02
Video Sequence 4	95.98	0.11
Video Sequence 5	99.56	0.04
Video Sequence 6	73.95	0.50
Video Sequence 7	98.20	0.13
Video Sequence 8	96.38	0.97
Video Sequence 9	98.58	1.78
Video Sequence 10	95.76	0.01
Video Sequence 11	98.63	0.03
Video Sequence 12	99.46	0.14
Video Sequence 13	95.32	0.43
Video Sequence 14	97.86	0.13
Video Sequence 15	99.12	0.02
Video Sequence 16	98.49	0.15
Video Sequence 17	99.03	0.01
Video Sequence 18	98.35	0.03
Video Sequence 19	93.47	0.03
Video Sequence 20	99.20	0.23

Furthermore, Fig.11 is a sample of non-tampered video frames with the corresponding inpainted ones and detection result using our proposed technique for three selected test video sequences from the data set used. The blue squares in the detection column of Fig. 11 indicate pixel regions where an object has been removed.

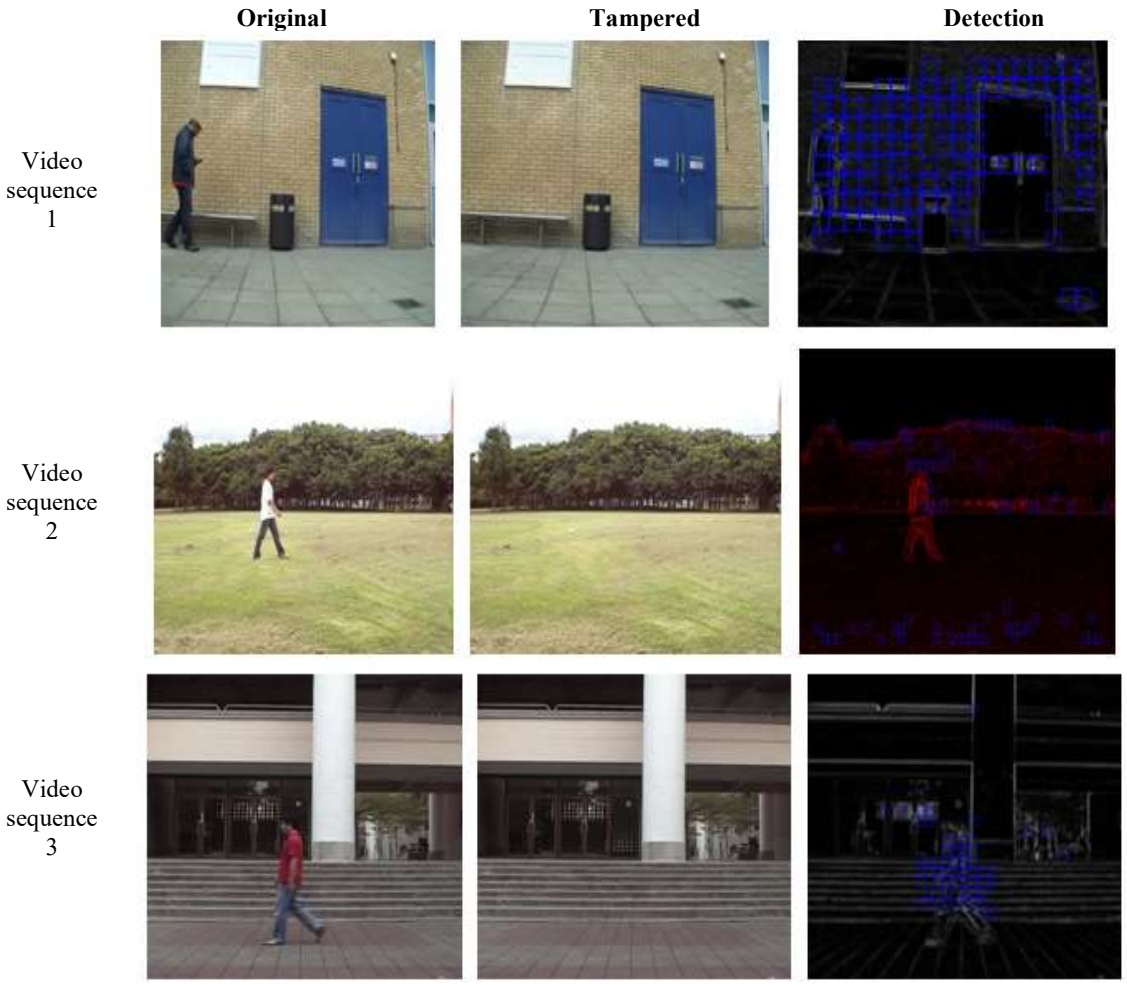

Fig.11Non-tampered frame, Tampered frame from inpainting and Detection results

6.0 COMPARISON WITH OTHER DETECTION TECHNIQUES

The performance of the proposed technique is compared with techniques proposed in [27], [30] and [43]. These selected techniques are considered because of their popularity and average performance rate of 96.61, 93.40 and 97.52 respectively for video inpainting forgery detection over the years. The performance of our technique is measured based on three metrics involving precision rate, false positive rates, and execution time. The mathematical equations for the precision rate and false positive rates are given in equation 3 and 4.

$$Precision = \frac{Number\ of\ correct\ detection}{Numbe\ \ of\ correct\ detection + Number\ of\ incorrect\ detection} \quad (3)$$

$$Recall = \frac{Number\ of\ incorrect\ detection}{Number\ of\ incorrect\ detection + Number\ of\ miss\ detection} \quad (4)$$

All three techniques were evaluated on a benchmark dataset designed by [25] and [27] for video inpainting forgery detection. Table 4 shows the comparison result of the precision and false positive rates for the different selected detection techniques.

Table 4 Comparison between SCHM, SCNR, STCA and GSA

Reference	Detection Approach	Average Precision Rate (%)	False Positive rate (%)
Hsu et. al (2008) [27]	SCNR	96.61	1.18
Zhang et. al (2009) [30]	GSA	93.4	6.60
Lin et. al (2014) [43]	STCA	97.52	3.22
Proposed	SCHM	99.79	0.29

The SCHM shows a higher percentage precision compared to the SCNR, GSA and STCA. Similarly, the comparative result of false positive rate among the four techniques proves that our technique based on SCHM records a low false positive rate compared to SCNR, GSA and STCA techniques.

Moreover, the average execution time compared to the techniques proposed in [27][30][43] is summarized in Table 5 for twenty test video sequences. The experiments were run using Matlab on an Intel Celeron computer having a 1.83 GHz processor speed, 64 bit operating system, and 4GB RAM. The comparative execution time shows that our proposed technique (i.e., SCHM) has the shortest execution time. This is because of the relative speed of hessian matrix generation from a video and the limited number of processing steps proposed in our technique making it both efficient and simpler. However, we believe technique based on SCNR shows a relatively longer execution time than the proposed technique based on SCHM because of the reasonable time spent for noise residue extraction in SCNR, the technique based on GSA also shows a longer execution time than the proposed technique based on SCHM because of its complex processing stages involved in the extraction of ghost shadow artefacts from a video. The technique based on STCA also shows a longer execution time than the proposed technique based on SCHM because of its complex computational burden for spatio-temporal analysis.

Table 5: Execution time for different detection approaches

	Execution Time(seconds)			
Video Sequences	**SCNR[27]**	**GSA[30]**	**STCA[43]**	**SCHM**
1	794.00	712.34	612.34	683.20
2	1417.92	1335.54	1432.65	1329.64
3	2228.54	1329.64	1276.78	1165.98
4	201.56	175.66	177.48	141.09
5	428.97	711.02	596.71	537.39
6	537.39	813.76	463.39	337.12
7	244.21	534.54	346.87	237.29
8	240.08	320.34	474.13	239.62
9	223.91	354.37	387.65	250.20
10	1562.44	1894.76	2341.91	1436.10
11	302.34	436.65	513.59	232.14
12	298.32	341.21	259.13	239.54
13	267.66	336.88	265.15	239.63
14	1578.21	1753.90	1965.57	1265.32
15	934.23	974.86	1007.27	832.15
16	289.38	369.34	349.32	226.34
17	204.22	385.23	338.54	198.67
18	286.29	303.41	297.85	187.43
19	316.71	493.43	457.4	234.67
20	269.58	324.75	397.19	254.43
Average	**631.298**	**695.0815**	**698.046**	**513.3975**

7.0 DISCUSSION

In this paper, a SCHM technique is proposed for the detection of structure and texture video inpainting forgery. We choose Hessian Matrix features from a video because of its reliability in identifying characteristic interest points for video frame analysis. We tested the SCHM technique using two different dataset from [25] and [27]. These dataset are chosen because of their wide usage for video forgery analysis. We evaluate the performance of SCHM using precision rate, which in this case is the true positive rate, false positive rate, and execution time.

The precision or true positive is when an inpainted region is correctly identified as inpainted, false positive is when an inpainted region is wrongly identified as not inpainted.

To determine the performance of our technique, we perform different experiment using different video sequences. The results of the experiment prove that the proposed SCHM technique has a good precision rate with an average of 99.79% and a low false positive detection rate with an average of 0.29%. The precision rate improvement is because of the ability of our Hessian features to capture the local structure of the pixel information in a given region regardless of size and intensity values. Furthermore, the proposed SCHM has also shown a faster execution time as compared to other techniques as shown in Table 5.

Finally, the results obtained from the experiments conducted have shown that the proposed SCHM detection technique can effectively be used for both structure and texture video inpainting forgery identification.

8.0 CONCLUSION AND FUTURE DIRECTIONS

This paper presented a technique for detecting video inpainting forgery involving structure and texture inpainting using statistical correlation of Hessian Matrix. Our experiments have shown that the use of hessian feature has significantly improved video inpainting forgery detection precision by approximately 3% compared to SCNR, 6% compared to GSA and 2% compared to STCA. A reduction in the number of false positive detection rate is also recorded as compared to SCNR, GSA and STCA. Based on the results obtained in this paper, we believe that the use of Hessian correlation is a useful technique in detecting inpainting forgery in a video.

However, combining Hessian properties with other video features such as sensor pattern noise, photo shot noise, and quantization noise may enhance the reliability and accuracy of the forgery detection scheme. The combination of Hessian Matrix and quantization noise features can be studied as a future research. Thus, the proposed technique can be further exploited to detect other kind of forgery, such as frame duplication and video looping. Furthermore, the use of semi-automatic segmentation in our work may just be a first step for a good pre-processing mechanism. Future work also includes the use of automatic segmentation methods for pre-processing. This way, it will be possible to further reduce the execution time of the proposed technique.

ACKNOWLEDGEMENT

This work is partially funded by the Ministry of Education, Malaysia under the University of Malaya High Impact Research Grant UM.C/625/1/HIR/MoE/FCSIT/17 and the Tertiary Education Trust Fund (TETFund), Ahmadu Bello University, Zaria Nigeria.

REFERENCES

[1] V.A. Chandrasetty and S.M Aziz. "Resource efficient LDPC decoders for multimedia communication" VLSI journal, 48: p. 213-220, 2015.

[2] A. Feizollah, N. B. Anuar, R. Salleh, F.Amalina, R. U. R. Ma'arof, and S.Shamshirband "A study of machine learning classifiers for anomaly-based mobile botnet detection". Malaysian Journal of Computer Science, 26(4), 2014.

[3] A. ElGamal, N. Mosa, and W. ElSaid. "A Fragile Video Watermarking Algorithm for Content Authentication based on Block Mean and Modulation Factor" Restoration, 20(21): p. 22, 2013.

[4] R.W. Taylor, E.J. Fritsch, and J. Liederbach. "Digital crime and digital terrorism". Prentice Hall Press 2014.

[5] A. Rocha,W. Scheirer, T. Boult and S. Goldenstein."Vision of the unseen: Current trends and challenges in digital image and video forensics". ACM Computing Surveys (CSUR) 43(4): p. 26, 2011.

[6] A. W. A. Wahab, M. A. Bagiwa, M. Y. I. Idris, Khan, S., Razak, Z, and Ariffin, M. R. K.. "Passive video forgery detection techniques: A survey". In IEEE International conference of Information Assurance and Security (IAS). pp. 29-34, 2014.

[7] W. H. Chuang, H. Su, and M. Wu. "Exploring compression effects for improved source camera identification using strongly compressed video". 18th IEEE International Conference on Image Processing (ICIP). 2011.

[8] S.Bayram, H. T.Sencar and N. Memon. "A survey of copy-move forgery detection techniques". IEEE Western New York Image Processing Workshop pp. 538-542, 2008.

[9] G. Liu, J. Wang, S. Lian and Z Wang. "A passive image authentication scheme for detecting region-duplication forgery with rotation". Journal of Network and Computer Applications, 34(5), 1557-1565, 2011.

[10] C. Guillemot and O. Le Meur. "Image inpainting: Overview and recent advances". Signal Processing Magazine, IEEE, 31(1), 127-144 2014.

[11] L. Su, T. Huang, and J. Yang. "A video forgery detection algorithm based on compressive sensing". Multimedia Tools and Applications, p. 1-16, 2014

[12] Y. Li, H. Guo, and S. Wang "A multiple-bits watermark for relational data". Journal of Database Management (JDM), 19(3): p. 1-21, 2008.

[13] Y. AL-Nabhani, H. A. Jalab, A. Wahid and R. Md Noor. "Robust Watermarking Algorithm for Digital Images Using Discrete Wavelet and Probabilistic Neural Network". Journal of King Saud University Computer and Information Sciences (JKSUCIS), 2015

[14] F. Di Martino and S. Sessa. "Fragile watermarking tamper detection with images compressed by fuzzy transform". Journal of Information Sciences, 195: p. 62-90, 2012.

[15] A. Ismail, M. Y. I. Idris, N. M. Noor, Z. Razak, and Z Yusoff. "MFCC-VQ Approach ForQalqalahTajweed Rule Checking". Malaysian Journal of Computer Science, 27(4), 2014.

[16] Q. Li, N. Memon, and H.T. Sencar. "Security issues in watermarking applications-A deeper look". 4th ACM international workshop on Contents protection and security. ACM, 2006.

[17] H. Farid. "Image forgery detection". Signal Processing Magazine IEEE, 26(2): p. 16-25, 2009.

[18] B. Mahdian and S. Saic. "A bibliography on blind methods for identifying image forgery". Signal Processing: Image Communication, 25(6): p. 389-399, 2010.

[19] S. Milani, M. Fontani, P. Bestagini, M. Barni, A. Piva, M. Tagliasacchi and S Tubaro"An overview on video forensics". APSIPA Transactions on Signal and Information Processing, 1: p. e2, 2012.

[20] A. E. Dirik, H. T. Sencar and N. Memon. "Digital single lens reflex camera identification from traces of sensor dust". Information Forensics and Security, IEEE Transactions on, 3(3), 539-552 (2008).

[21] C. T. Li. "Source camera identification using enhanced sensor pattern noise". Information Forensics and Security, IEEE Transactions on, 5(2), 280-287 2010.

[22] D. A. Forsyth and J. Ponce. "Computer vision: a modern approach". Prentice Hall Professional Technical Reference, 2002.

[23] M. Mansourvar, S. Shamshirband, R.G. Raj, R. Gunalan and I. Mazinani. An Automated System for Skeletal Maturity Assessment by Extreme Learning Machines. PLoS ONE 10(9): e0138493. doi: 10.1371/journal.pone.0138493 (2015).

[24] M. Bertalmio, L. Vese,, G. Sapiro, and S. Osher. "Simultaneous structure and texture image inpainting". IEEE Transactions onImage Processing 12(8), 882-889, 2003.

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

[26] A. C. Popescu and H. Farid. "Exposing digital forgeries in color filter array interpolated images". IEEE Transactions on Signal Processing.53 (10): p. 3948-3959, 2005.

[27] C. Hsu, T. Hung, C. Lin and C. Hsu."Video forgery detection using correlation of noise residue". IEEE 10th Workshop on Multimedia Signal Processing, 2008.

[28] A. H. De, H. Chadha, and S. Gupta. "Detection of forgery in digital video". The 10th World Multi Conference on Systemics Cybernetics and Informatics, 2006.

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

[30] J. Zhang, Y. Su, and M. Zhang. "Exposing digital video forgery by ghost shadow artifact". Proceedings of the First ACM workshop on Multimedia in forensics. ACM, 2009.

[31] S. Ye, Q. Sun, and E. C. Chang. "Detecting digital image forgeries by measuring inconsistencies of blocking artifact". IEEE International Conference on Multimedia and Expo, 2007

[32] J. He, Z. Lin, L. Wang, and X. Tang "Detecting doctored JPEG images via DCT coefficient analysis". Computer Vision–ECCV Springer. p. 423-435, 2006.

[33] K. M. Mihcak, I. Kozintsev, K. Ramchandran and P. Moulin."Low-complexity image denoising based on statistical modelling of wavelet coefficients". Signal Processing Letters, IEEE, 6(12): p. 300-303,1999.

[34] J. Lukas, J. Fridrich, and M. Goljan."Digital camera identification from sensor pattern noise". IEEE Transactions on Information Forensics and Security 1(2): p. 205-214, 2006.

[35] J. Lukáš, J. Fridrich, and M. Goljan. "Detecting digital image forgeries using sensor pattern noise". International Society for Optics and Photonics 2006.

[36] M. Chen, J.Fridrich, M. Goljan and J.Lukas."Determining image origin and integrity using sensor noise"., IEEE Transactions on Information Forensics and Security3(1): p. 74-90, 2008.

[37] R, M. Kirberger "Imaging artifacts in diagnostic ultrasound—a review". Veterinary Radiology & Ultrasound 36(4): p. 297-306, 1995.

[38] A. Feizollah, N. B. Anuar, R. Salleh, and A. W. A. Wahab. "A review on feature selection in mobile malware detection". Digital Investigation, 13, 22-37, 2015

[39] S. Das, G. D. Shreyas, and L.D. Devan. "Blind Detection Method for Video Inpainting Forgery". 2012.

[40] L. Li, X. Wang, W. Zhang, G. Yang and G. Hu. "Detecting removed object from video with stationary background". Digital Forensics and Watermarking Springer. p. 242-252, 2013.

[41] A. Subramanyamand S. Emmanuel. "Pixel estimation based video forgery detection". IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2013.

[42] C. S. Lin and J. J. Tsay. "Passive approach for video forgery detection and localization". The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013).The Society of Digital Information and Wireless Communication, 2013.

[43] C. S. Lin and J. J. Tsay. "A passive approach for effective detection and localization of region-level video forgery with spatio-temporal coherence analysis". Digital Investigation. 11(2): p. 120-140, 2014.

[44] T. Lindeberg. "Scale-space: A framework for handling image structures at multiple scales". CERN EUROPEAN ORGANIZATION FOR NUCLEAR RESEARCH-REPORTS-CERNp. 27-38, 1996.

[45] Y. Sato, S. Nakajima, H. Atsumi, T. Koller, G. Gerig, S. Yoshida and R. Kikinis"3D multi-scale line filter for segmentation and visualization of curvilinear structures in medical images" .CVRMed-MRCAS'97Springer, 1997.

[46] A. F. Frangi, W. J. Niessen, K. L. Vincken and M. A. Viergever."Multiscale vessel enhancement filtering". Medical Image Computing and Computer-Assisted Intervention MICCAI'98. Springer. p.130-137, 1998.