TAF
Journal of Advances in Technology and Engineering Research
JATER
2019, **5**(5): 199-206

PRIMARY RESEARCH

Video forgery detection based-on passive (blind) approach

Noraida Haji Ali [1], Fadilah Harun [2*]

[1, 2] Faculty of Ocean Engineering Technology and Informatics, Universiti Malaysia Terengganu, Terengganu, Malaysia

Keywords

Authentication video
Passive techniques
Video forgery detection
counterfeiting

Received: 7 May 2019
Accepted: 9 July 2019
Published: 31 October 2019

Abstract

Current communication technology can ease sharing multimedia data such as images, text, graphics, audio, and videos online or offline. A multimedia editing tool can be downloaded freely and used efficiently to be editing the content of video clips. To solve integrity and originality, video clips are very challenging and require some complex methods. How to ensure that the content or the structure of the video provided or downloaded from the internet is original and just as recorded? Video forgery is a technique to generate fake videos with malicious intent by inserting, deleting, duplication their contents. Therefore, the video's originality can be questioned and need to be verified. Video forgery detection is intended to determine the originality of video content, whether the video has undergone any unethical change. The video forgery detection technique has two approaches, active and passive. This study focuses on the detection of tampering video using a passive approach because it is not dependent on pre-embedded information to determine the originality of the video. The passive approach will be extracting this feature from the video and analyzing them for different forgery detection. A passive approach is better than the active one as it relies on fake video available and features and its properties without needing the original video. The research focus was to apply a passive approach to develop a new model for video forgery detection. This model will be used to build a powerful tool for detecting video authenticity. Therefore, it can help certain parties, especially those involved in legal activities.

I. INTRODUCTION

With the speedy development of multimedia and communication technology, it can facilitate content sharing such as text, pictures, and videos online or offline without unlimited access. Multimedia editing tools can be freely downloaded and can edit the content of video with good or bad intentions. Automatically when the changes made, the video content and its structure will be altered. To ensure the quality and originality of the video clips is preserved, it requires different methods to claim that the video is authentic and the same as recorded. In general, video forgery attacks are to tamper the authenticity of video data and its content for malicious attention. Nowadays, the originality of the video plays an essential role in a few fields like, in forensic and police investigations, court cases and ownership of patents. Video authentication is a process which verifies that the information and structure in a video clip is original and exactly same as when recorded [1, 2].

The video definition can be considered a moving image sequence called frames. The basic video architecture is a hierarchy structure. The hierarchy structure formed by video, scenes, shots and frames [3, 4, 5, 6]. Figure 1 shows the video data model based-on segmentation has a hierarchy structure. Normally the structure of video has a few parts; there are scene, shot, and frame. Scene has one or more shots, and frame is one of the many still images which compose the complete moving picture [7, 8].

[*] Corresponding author: Fadilah Harun
[†] email: elaharun@yahoo.com

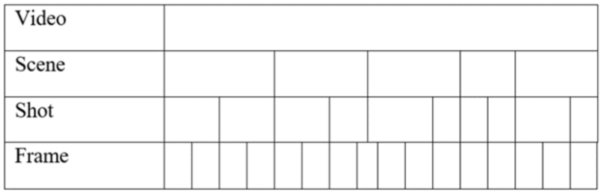


Fig. 1. Video basic structure

Now many digital media websites are available such as YouTube, Vimeo, Dailymotion and so on. The content of the video can be tampered for bad intentions by using video editing tools or software, such as Paint, Adobe Premiere, Adobe Photoshop and more. Forgeries can be committed by tampering different domains associated with the video sequence. There are two types of video forgeries:

- Inter-frame forgeries–These forgeries involved the frames in the video. Usually, its involved frame removal or insertions.
- Intra-frame forgeries-in this forgery it modifies the actual content, usually in this forgery involved copy-paste forgeries and upscale crop.

An important study was done a decade ago in the field of forgery detection. Figure 2 shows a number of publications that related to video authentication research. The research focus involved with four types of video forgery detection techniques (copy-move, image splicing, resampling, retouching) within the past two decades, during the year 2000-2010, grouped from Science Direct. Some observations can be highlighted from this finding are:

i) Increased research in video authentication.
ii) Most research focuses on copy-move detection.
iii) Detection of others type forgery also gives a new impact in a decade ago compared to the first decade.

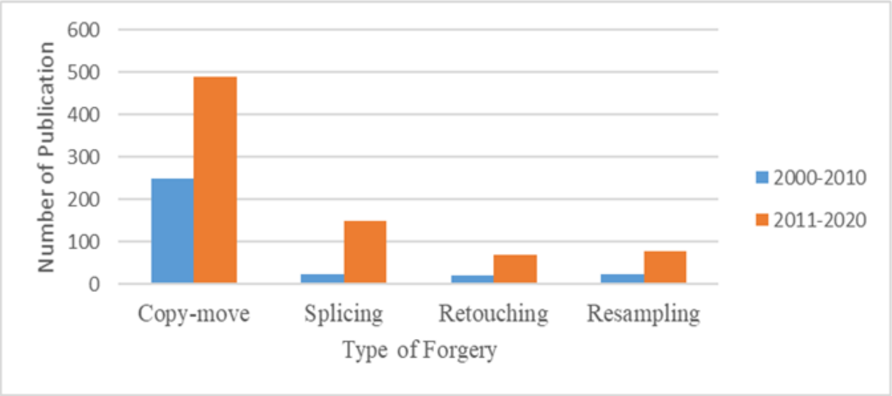


Fig. 2. Publications on video authentication

Video forgery detection techniques can be categorized into two categories; active (non-blind) and passive (blind) [3]. Active forgery detection techniques must have some information about the image which may have been inserted during recording or later stages.

A passive forgery can be categorized as dependent and independent tampering. In a dependent forgery, whether alterations can be done in the same image as copying and pasting (cloning) some areas in images or more than one image can be combined (image splicing) to get the composite to convince. On the other hand, free counterfeiting is forgery, where some of the same image properties are manipulated. Examples of independent forgery include resampling, retouching, image rotation, scaling, resizing, increased noise, fuzzy, image compression, etc. There is no knowledge involved in the image of making passive forgery more practical in real life.

II. RESEARCH BACKGROUND

A few of research about video data have been done by several researchers. One of the previous researches done by [9] stated that:

- There are still lacking on security issues of the video content.
- A free image editing software can download, and it gives changes to alter the contents and structure (by inserting, deleting and rotation) of video easily.

Based on previous research [10] it cannot determine either the video is an original structure or not without comparing it with the original one. The prototype was developed to ex-

ISSN: 2414-4592
DOI: 10.20474/jater-5.5.2

tract the structure contained in a video that was input by the user. The user must input two videos, original and edited video into the prototype to determine the authentication of video structure. Its limitation when we had only one video, and it cannot compare either is original or not. Usually, the user is difficult to understand and define the basic structure of the content appearing in a video. There are many various methods that can be used to determine the video authenticity as it is widely used in fields such as police and forensic investigations, customs cases, or as evidence in court. Mostly using watermarking and digital signature methods, but it cannot be used if no pre-process insertion is done [11]. In this study is to aim to solves video forgery based-on the passive approach. Among the media data types that have been mentioned, video is the most challenging compares to others and have a lot of problems because it has a massive number of frames and images to treat [3]. This task quite challenging because of the structure of the clip video contains images sequence. Besides that, each video has its own rules and formats. A video is an alteration with the lousy intention to ruin its authentication by secretly inserting, deleting or shuffling its information [11]. Effects of the modifications made depending on the situation and where it is used. Such in the political world, the alterations maybe can be affected by their carrier where it used to defame a personality to win a vote. The video integrity and originality that been displayed cannot be accepted readily as proof.

In this study, will propose the approach that can detect malicious attacks and locate the attacks occur, and it easy to retrieve the content of video data with the use of a passive approach. The outlook from this study hopes it can produce a new model for video authentication detection based-on a passive approach. This model will be used to develop a prototype for video forgery detection. There are various techniques used to determine the authenticity of a video, but only with the use of a passive approach can detect the authenticity of the video without reference techniques [12].

III. VIDEO FORGERY

Video forgery detection consists of two approaches, as shown in Figure 3.

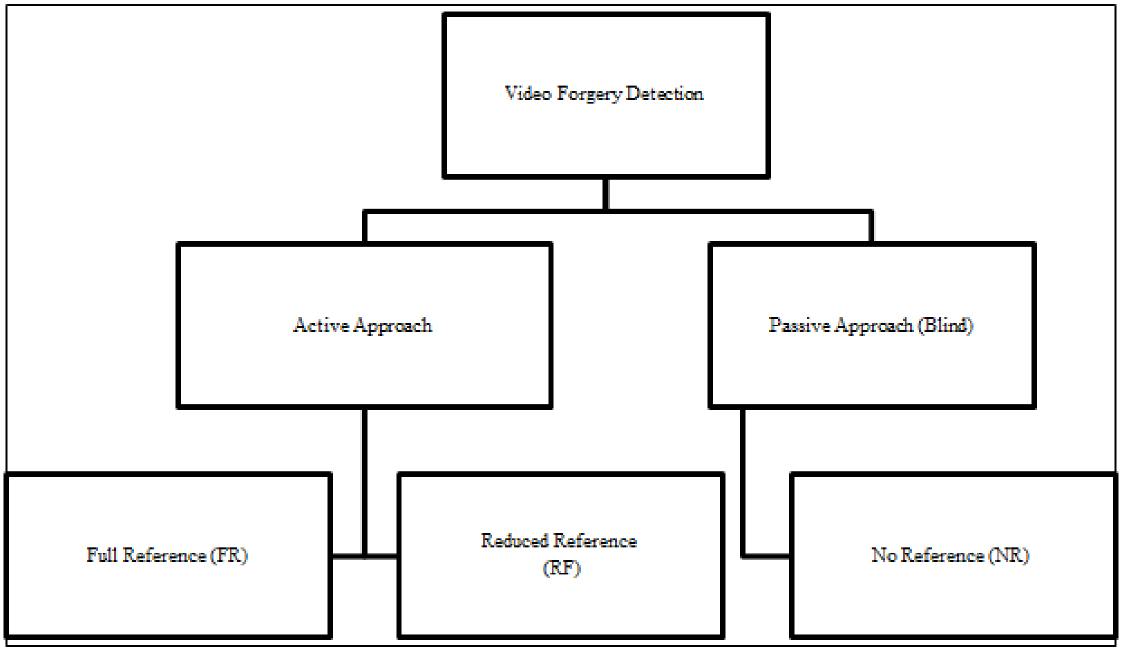


Fig. 3. Video forgery approach

In an active approach, it's focused on unseen data, and it requires pre-processed information like digital watermark, digital fingerprints or digital signature. If the video is had an alteration, then it can be detected through watermarking or signature to the identification of the tampering results. The active approach cannot be successes if pre-embedding process not be inserted (watermark or signature not found) in the video. Video quality assessment for active approach can be divided into two parts, full and reduced reference. In comprehensive reference, the forged can be detected based on the original video as a reference. However, are some cases, the active approach used digital watermark or signature to identify the tampering occurs in the video, also known as a Reduced Reference. Reduced reference only works with partial available (pre-embedding process) from the original video.

ISSN: 2414-4592
DOI: 10.20474/jater-5.5.2

Passive approach no depending on pre-embedding information that video contains naturally occurring properties or inherent fingerprint, which is unique due to different video imaging devices and its characteristics. This approach functionally without involvement any specialized hardware and information on video content. It assumes that the video has some features that are consistent in the original video; which is will be changed if any alteration happens. These features will be extracted and analyze it's different for video forgery detection purposes.

IV. VIDEO FORGERY DETECTION BASED ON PASSIVE APPROACH

With the constraint of active techniques, more current research focuses on passive or blind video forgery detection. Passive approach to video forgery detection techniques are methods for determining the originality of video without comparing or depending on the source [13]. Passive approach functions with the necessary process that video contains inherent properties which are unique based on video imaging devices and its features. If the video is not being altered then the basic of statistical correlation features still the same compared with the source similar scheme and characteristics.

In a passive approach, it's stated that the pattern of the original video is identifiable based on two different issues, that is video recording devices (source of the video) and video processing inside them (malicious alteration). The original patterns would be modifying after tampering. Figure 4 shows the basic process of video forgery detection based on passive approach [14].

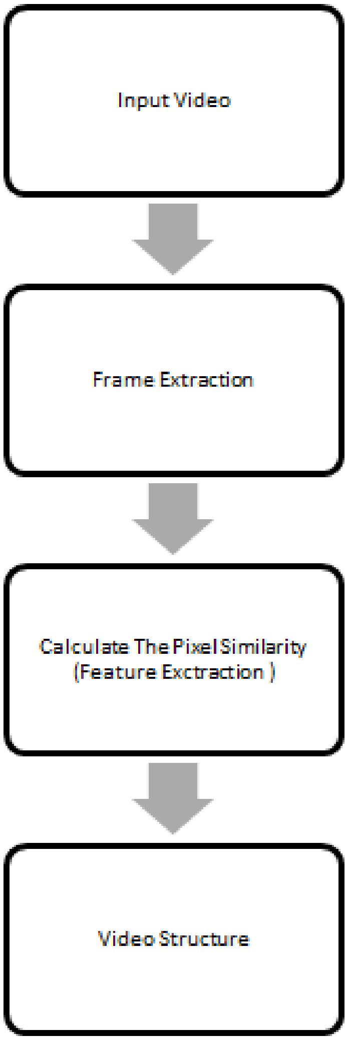


Fig. 4. Video forgery detection based on passive approach

ISSN: 2414-4592
DOI: 10.20474/jater-5.5.2

A digital video comes from different source and the issues a concern is about source identification. However, different video source has different features and characteristics as well as have different pattern of video images. In basic video forgery detection model, the features and the pattern from original video (video source) are extracted using knowledge of video original model. Then, all the same patterns and the features are measured to determine the originality of the video based on the video source. In Figure 5 shows the basic of video extraction process using shot boundary detection.

First, video features were extract and it acquire the patterns of video original or altered mainly using knowledge of video handling model or sometimes its combine with the statistical features.

Then, distance between features and patterns will be comparing to decide either the input video is altered or not. By using passive approach, it can determine the originality of video based on the patterns of the digital images themselves. Feature extraction in passive approach is an important process to determine the authentication of video.

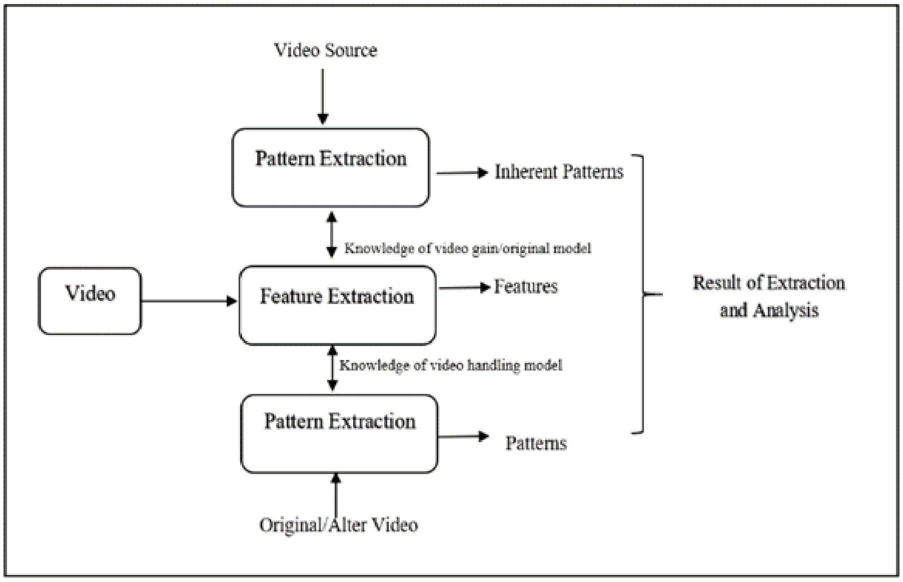


Fig. 5. Video extraction process using shot boundary detection

V. VIDEO EXTRACTING

One of the most used methods of video tampering is deleted, replace or adding objects from video through overlapping frames. This process is done using video processing software. An example of these tampering operations shown in Figure 6 and Figure 7.

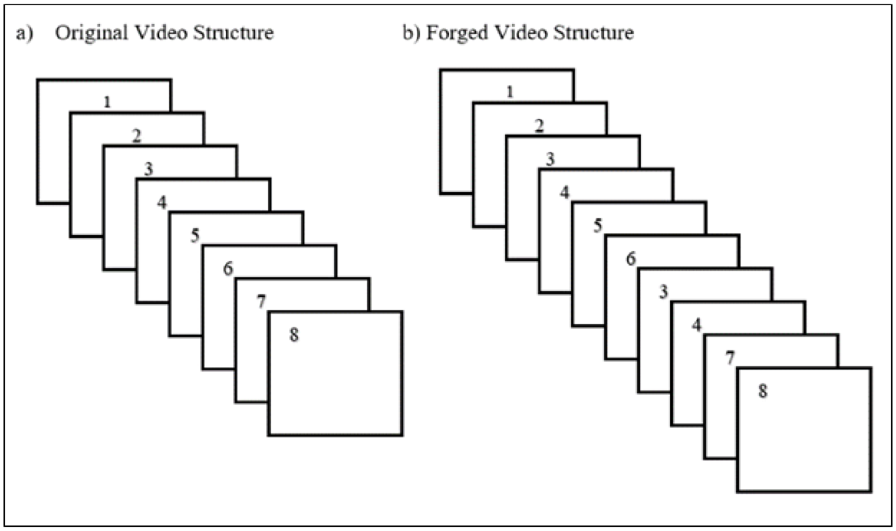


Fig. 6. The structure of frame addition in the video

ISSN: 2414-4592
DOI: 10.20474/jater-5.5.2

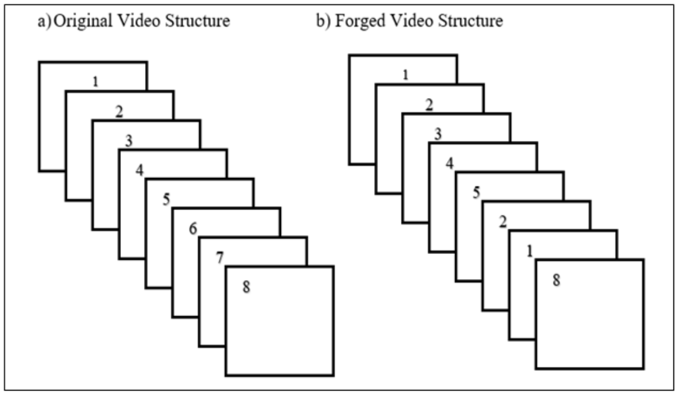
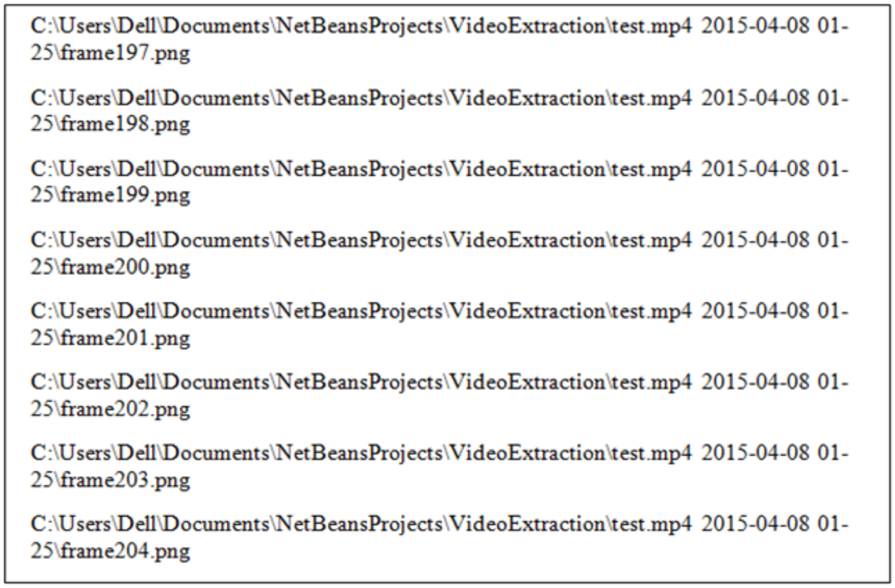


Fig. 7. The structure of frame replacement in video

Because of the high similarity between the original sequence and the copy sequence, similarity analysis is a practical method for detecting this forgery issues. However, most previous algorithms could not achieve good accuracy and efficiency. To solve this regarding issues, this study proposes an algorithm for extracting video structure to detect frame or image alterations based on similarity analysis using a blind approach. By seeking those video sequences with high similarities, the algorithm will be determining whether the video has been tampered or not, as well as can quickly locate the source sequences and their redundancy. The algorithm proposed in this study is to improve the detection of tampering attacks by using shot boundary detection and passive approach.

The use of shot boundary detection is to extract the video into the hierarchy structure (scene, shot and keyframe) and can quickly determine the relationship between its level components [15]. A shot boundary detection can be identified when the feature contrast gives accurate changes more significant than the threshold [16]. With the used of shot boundary detection hope it can detect the alterations made of a video and locate the tamper occurs so it can be more easily to retrieve the video content.

The extraction process involves three processes that are, comparison between the frames available in the video clips to get the full list of a possible number of shots. Later, the equation process for each shot is possible to find the percentage difference in determining each scene. The percentage differences are set to establish each main framework that exists in a video clip. The first step, the video will be read as the input for this process. Through the processing of frames, all frames in the video will be read sequentially. Each existing sequence of frames will be changed into the block (shot). Figure 8 shows a video clip that is already input, and frame processing is done to determine the number of available shots.

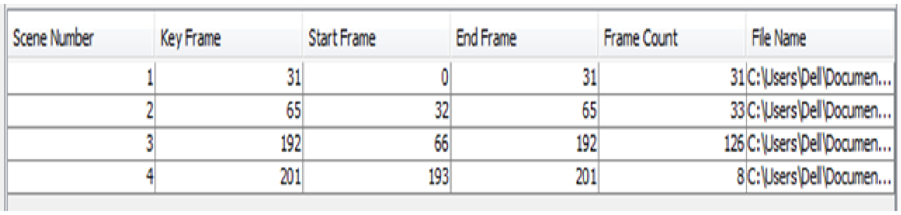


```
C:\Users\Dell\Documents\NetBeansProjects\VideoExtraction\test.mp4 2015-04-08 01-
25\frame197.png

C:\Users\Dell\Documents\NetBeansProjects\VideoExtraction\test.mp4 2015-04-08 01-
25\frame198.png

C:\Users\Dell\Documents\NetBeansProjects\VideoExtraction\test.mp4 2015-04-08 01-
25\frame199.png

C:\Users\Dell\Documents\NetBeansProjects\VideoExtraction\test.mp4 2015-04-08 01-
25\frame200.png

C:\Users\Dell\Documents\NetBeansProjects\VideoExtraction\test.mp4 2015-04-08 01-
25\frame201.png

C:\Users\Dell\Documents\NetBeansProjects\VideoExtraction\test.mp4 2015-04-08 01-
25\frame202.png

C:\Users\Dell\Documents\NetBeansProjects\VideoExtraction\test.mp4 2015-04-08 01-
25\frame203.png

C:\Users\Dell\Documents\NetBeansProjects\VideoExtraction\test.mp4 2015-04-08 01-
25\frame204.png
```

Fig. 8. The frame extraction process

ISSN: 2414-4592
DOI: 10.20474/jater-5.5.2

The extraction process is a process between the two consecutive frame blocks is done through a percentage gap set of frames to determine each scene that exists. Then the percentage of each frame is set by the differences available on the pixel of each extracted image. Subsequently, the video structure extraction resulted in a full list of the number of scenes, shot and key frames. Figure 9 shows an example of the result for the extraction process. It's proved that in the video there is a relationship between scene, shot and keyframes. Relations composition explains the function inherent in the structure of the video. Relationships can determine belonging of each scene, shot and keyframes. Based on the structure of the video are commonly used, it cannot describe the structure more clearly.



Scene Number	Key Frame	Start Frame	End Frame	Frame Count	File Name
1	31	0	31	31	C:\Users\Dell\Documen...
2	65	32	65	33	C:\Users\Dell\Documen...
3	192	66	192	126	C:\Users\Dell\Documen...
4	201	193	201	8	C:\Users\Dell\Documen...

Fig. 9. Result of the extraction process

VI. CONCLUSION

Multimedia data types are divided into several types, among them, text, pictures, audio and video. But video is one of the most common problems compared to other types, and video authentication is one of the current issues nowadays. Video authentication detection is a widespread issue, and it's not an easy task to handle the originality of video sequences when it not depends based on the original video. One of the ideal solutions to deal with this issue is used passive approach in video authentication detection techniques. In video forgery detection aims to find the proof of tampering by evaluating the originality of video evidence and its divide into an approach, active and passive. The passive approach can give a better result compare to the active approach because it depends on basic information (pattern) without need extra information and hardware requirements. The used of passive approach will give exact and accurate findings with structured video. This research aims to solved video authentication issues with the used of shot boundary detection and passive approach. It will be used to develop a prototype to solves the problems in video and detect the tampering locations.

REFERENCES

[1] S. Upadhyay and S. K. Singh, ``Video authentication: Issues and challenges,'' *International Journal of Computer Science Issues*, vol. 9, no. 1, pp. 409-418, 2012.

[2] R. Sawant and M. Sabnis, ``A review of video forgery and its detection,'' *Journal of Computer Engineering*, vol. 20, no. 2, pp. 1-4, 2018. doi: https://doi.org/10.9790/0661-2002030104.

[3] R. Suryanita, H. Maizir, and H. Jingga, ``Prediction of structural response based on ground acceleration using artificial neural networks,'' *International Journal of Technology and Engineering Studies*, vol. 3, no. 2, pp. 74-83, 2017. doi: https://doi.org/10.20469/ijtes.3.40005-2

[4] X. Zhu, X. Wu, J. Fan, A. K. Elmagarmid, and W. G. Aref, ``Exploring video content structure for hierarchical summarization,'' *Multimedia Systems*, vol. 10, no. 2, pp. 98-115, 2004. doi: https://doi.org/10.1007/s00530-004-0142-7

[5] F. C. Jian, L. Hui, and W. J. Tao, ``Video hierarchical structure mining,'' in *International Conference Proceedings of Communications, Circuits and Systems*, California, CA, 2006.

[6] L. S. Affendey, A. Mamat, H. Ibrahim, and F. Ahmad, ``Video data modelling to support hybrid query,'' *International Journal of Computer Science and Network Security*, vol. 7, no. 9, pp. 53-59, 2007.

[7] O. A. Osahenvemwen and O. F. Odiase, ``Effective management of handover process in mobile communication network,'' *Journal of Advances in Technology and Engineering Studies*, vol. 2, no. 6, pp. 176-182, 2016. doi: https://doi.org/10.20474/jater-2.6.1

[8] T. Catarci, M. Donderler, E. Saykol, O. Ulusoy, and U. Gudukbay, ``Bilvideo: A video database management system,'' *IEEE MultiMedia*, vol. 10, no. 1, pp. 66-70, 2003. doi: https://doi.org/10.1109/MMUL.2003.1167924.

[9] M. P. Queluz, ``Authentication of digital images and video: Generic models and a new contribution,'' *Signal Processing: Image Communication*, vol. 16, no. 5, pp. 461-475, 2001. doi: https://doi.org/10.1016/S0923-5965(00)00010-2

[10] N. H. Ali, F. Harun, and N. M. M. Nor, ``Video structure retrieval using video extraction analyzer,'' *International Journal of Research in Engineering & Advanced Technology*, vol. 3, no. 5, pp. 45-70, 2015.

[11] A. W. A. Wahab, M. A. Bagiwa, M. Y. I. Idris, S. Khan, Z. Razak, and M. R. K. Ariffin, ``Passive video forgery detection techniques: A survey,'' in *10th International Conference on Information Assurance and Security,* New York, NY, 2014.

[12] J. S. Boreczky and L. A. Rowe, ``Comparison of video shot boundary detection techniques,'' *Journal of Electronic Imaging*, vol. 5, no. 2, pp. 122-129, 1996. doi: https://doi.org/10.1117/12.238675

[13] Q. Dong, G. Yang, and N. Zhu, ``A mcea based passive forensics scheme for detecting frame-based video tampering,'' *Digital Investigation*, vol. 9, no. 2, pp. 151-159, 2012. doi: https://doi.org/10.1016/j.diin.2012.07.002

[14] W. Luo, Z. Qu, F. Pan, and J. Huang, ``A survey of passive technology for digital image forensics,'' *Frontiers of Computer Science in China*, vol. 1, no. 2, pp. 166-179, 2007.

[15] M. P. S. Sowjanya and R. Mishra, ``Video shot boundary detection,'' *International Journal of Electronics, Communication & Instrumentation Engineering Research and Development*, vol. 1, no. 2, pp. 23-56, 2012.

[16] M. S. P. Waghmare and A. Bhide, ``Shot boundary detection using histogram differences,'' *International Journal of Advanced Research in Electronics and Communication Engineering*, vol. 3, pp. 1460-1464, 2014.