IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-5, May 2018 E-ISSN: 2347-2693

B-Frames: Efficiency Analysis for Digital Video Tampering Detection in Videos with Variable GOP Structure

V.Joshi[1*], S. Jain[2], C. Bansal[3]

[1*]SOCA, ITM University, Gwalior, India
[2] SOCA, ITM University, Gwalior, India
[3] MCA, BVICAM, GGSIPU, New Delhi, India

Corresponding Author: vaishali.joshi22@gmail.com, Tel.: +91-99681-19223

Available online at: www.ijcseonline.org

Accepted: 23/May/2018, Published: 31/May/2018

***Abstract*—** Digital video tampering is an act of malicious modification of video content. This could be done to hide or cover an object or to alter the meaning conveyed by the digital video. The research performed is summarized in this paper by analyzing various inter frame forgery detection approaches for digital video, proposed so far, highlighting the strengths and weaknesses of each approach discussed. All approaches proposed so far are making use of P-frames for forgery detection. Comparison of P-frames and B-frames has been performed in terms of complexity and accuracy of algorithms developed using each of them. All the way through the research performed, authors tried to access the worth of B-frames in digital video forgery detection.

***Keywords*—** Video Forgery Detection, Group of Pictures (GOP), B-frames, Video tampering, Intra Frame, Predicted Frame, Bi-directional frames, High efficiency video coding

I. INTRODUCTION

A moving picture formed by rapidly displaying a group of pictures (GOP) is called a **digital video**. These pictures are called **frames**. Figure 1 shows the video sequence.

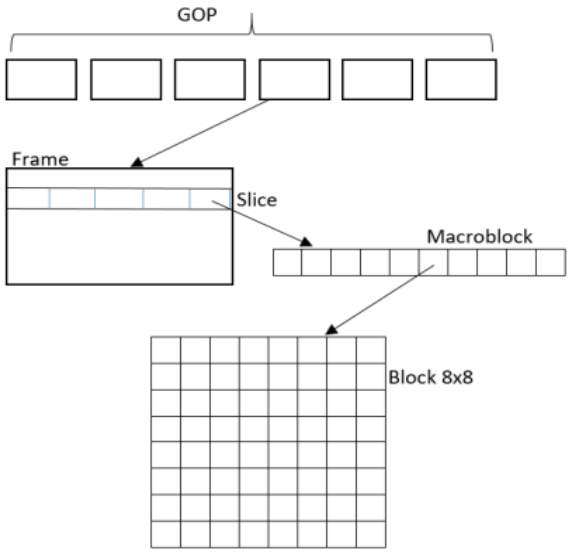

Figure 1. Video Sequence

Array of pixels (8x8) is known as a block. Frames are segmented into array of blocks known as macro-blocks. Slice is a string of arbitrary length consisting of consecutive macro-blocks [1].

In order to store or transfer the videos over a network in decreased file size, various video compression techniques are available to reduce and remove redundant video data.

Various video compression standards are Motion JPEG, MPEG-4, H.245 and H.256 etc. The latest and most efficient encoding standard is H.265 (HEVC).

The encoding and decoding standard for a particular video should be same, and this pair of algorithms working together is called video codec (encoder/decoder) [2].

To achieve compression video frames can be divided into 3 categories:

- I-frame: This is Intra frame. It can be thought of as a JPEG image. These frames are independent and coded by themselves.
- P-frame: This is predicted frame. Encoding/decoding a P-frame requires information from previously encoded/decoded I or P frame.
- B-frame: This is Bi-directionally predicted frame. Encoding/decoding of a B-frame requires information from surrounding (previous and next) I or P frames.

Intra frame is also called key frame as it independently carries all the processing information. P-frames and B-frames are

© 2018, IJCSE All Rights Reserved

called Inter frames (I-frames) because they have data dependency on other type of frames. Inter frames help to achieve video compression because they only store the information which is different from the information stored in the frames on which they depend. This save data and thus inter frames use comparatively lesser space than intra frames.

Illegal or improper alteration of the contents of video is known as video tampering. There is an escalation in the ease with which videos can be tampered with the help of easily available software. Hence, to maintain the integrity of the video, forgery detection has become imperative. Video forgeries are broadly categorized as intra-frame forgeries and inter-frame forgeries.

A. Intra-frame Forgeries

The video sources can be spatially attacked by altering the pixels within the individual video frames. This sort of forgery is called intra-frame forgery or spatial tampering. Figure 2 displays three kinds of spatial tampering-

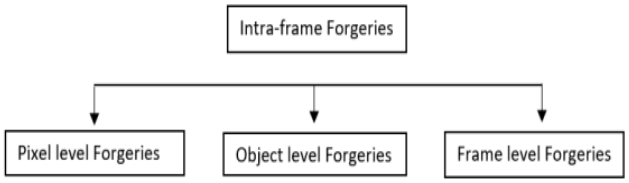

Figure 2. Types of Intra-Frame Forgeries

1. *Pixel-level Forgeries*- In pixel level forgeries, the video content is tampered at pixel level. This can be done by cloning/copy move, re-sampling or splicing individual pixels.
   - In *cloning*, any portion of the video frame can be copy moved within the same frame. This tampering is easy to detect because it leads to change in the original pixel alignment.
   - *Re-sampling* is transforming a genuine frame, or a part therein, by applying some geometrical transformations like scaling, rotation, skewing etc. [3] The features of the image are changed without making apparent changes in its content [4].
   - *Splicing* is copy-pasting. Content from other frames/images is copy pasted onto the target frame to violate its credibility.
2. *Object-level Forgeries*-Fabricating the video frame by attacking its objects is called object-level forgeries. Both foreground and background objects can be ambushed by adding, removing or modifying them [5].
3. *Frame-level Forgeries*- When tampering is up scaled to cover the entire frame, frame-level forgery is implied. This can be done by replacing, cropping, morphing or modifying the entire frame.

B. Inter-frame Forgeries

In inter-frame forgeries, the sequence of frames is the target of malicious tampering. This type of forgery is also called temporal forgery.

Usual temporal attacks involve addition, removal, reordering or averaging of the frame as shown in figure 3 [5].

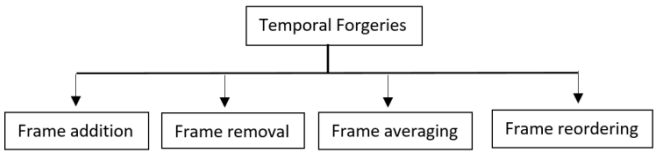

Figure 3. Types of Temporal Forgeries

1. *Frame addition*-Video frames having same statistical attributescan be inserted into the target video frame sequence to tamper the original video content [5].
2. *Frame removal*- When intentions go awry, particular video frames can also be dropped / removed from the original video frame sequence. The purpose of this attack is to hide information.
3. *Frame averaging*- A target frame can be replaced by a frame created by taking the average of the target frame and its nearest neighboring frames. This is called frame averaging [6].
4. *Frame reordering*- The frames can also be shuffled in the video sequence to display incorrect sequence of events with respect to time.

Over the years, plentiful of video tampering detection algorithms have been proposed [7].To the best of author's knowledge, almost all of these algorithms take into account I-frames and P-frames. B-frames happen to be disregarded from the forgery detection algorithms, especially from inter-frame forgery detection techniques. To give insight into the basic fundamentals, section 2 talks about the elementary approaches to video forgery detection. In section 3, we look forward to the problem definition to clearly state the aim of this research. Subsequent sections talk about the features of B-frames, the existing scenario of the digital video forgery detection techniques and the proposed scenario for the same. The last section concludes the research along with future enhancements in the field of video forgery detection using B-frames.

The research paper is organized as follows: Section I contains the Introduction of the study about type of possible video forgeries. Section II explains techniques of video forgery detection. Section III contains problem definition which tells the notion of writing this research paper. Author is trying to access the use of B-frames in detecting digital video tampering efficiently as they are used in efficient video coding. Section IV contains all the relevant work done so far

© 2018, IJCSE All Rights Reserved

in the area of digital video tampering detection in last 10 years. The study is summarized in the form of Table No. 1. Section V contains methodology and proposed algorithm. It contains pseudo code and flow chart of proposed algorithm. Author concluded the study in Section with limitations and future extension of the study.

II. TECHNIQUES OF VIDEO FORGERY DETECTION

There are two elementary approaches to digital video tampering detection- active and passive [8].

2.1 Active techniques for video forgery detection

When some secondary data like digital signatures or digital watermark is embedded into the images, so that this prior information becomes the crucial factor for forgery detection, then these types of techniques are called active approaches to video forgery detection [9]. Not all devices are specially equipped with this technology of embedding digital watermark or digital signatures at the time of image capturing, therefore active techniques are not main stream now. Another modus operandi for embedding information is while further processing the image. However, this may lead to demeaning of the video image quality. The integrity detection of these watermarks or signatures helps to detect forgery in the frames.

However, the active approach cannot refrain the person responsible for embedding encryption from tampering the video. Due to these disadvantages of active forgery detection approaches, passive approach came into account.

2.2 Passive techniques for video forgery detection

Passive approach determines the credibility of the video without relying on the pre ingrained information like digital signatures, watermark etc. Video tampering results in the distortion of the mathematical and statistical properties of the original video. This distortion (digital footprints) is exploited to detect forgery by passive methods. Passive approach is also called blind video forgery detection. There are numerous algorithms proposed for passive video forgery detection [7], [8].

Blind passive tampering detection techniques can be predominantly classified into following two types [9]:

1. Visual methods- They are contingent on optical clues like irregularities in images, light distortion on an object within a frame etc.

2. Statistical methods- These methods scrutinize the pixel values of the frames. They are mathematical and calculation based. Special hardware and software may also be required. Statistical methods are more robust as compared to visual methods.

Some key aspects in passive video forgery detection techniques include source device identification from which the video is captured, tampering detection by recording forgery evidences and detection of computer generated frames created by exploiting advance hardware and software tools.

III. PROBLEM DEFINITION

With numerous software at hand, carrying out inter frame forgeries is plain sailing. However, detection of these forgeries is equally strenuous. Forgery detection becomes even more difficult when adaptable GOP structure comes into consideration, like in H.264/AVC codec. To the best of author's knowledge, most of the blind passive forgery detection techniques in case of adaptable GOP structure work on I-frames and P-frames. This research tries to analyze the efficiency of B-frames for this type of video tampering detection. The research further tries to explore the possible reasons for paying no heed to B-frames in tampering detection algorithms till date.

IV. RELATED WORK

Till date, numerous algorithms have been proposed to detect video forgeries of different kinds. Reference number [8], [7] and [14] presents the latest wide-ranging and thorough inspection of the published research works in the domain of passive video forgery detection techniques. After analyzing the well-presented summary of all the techniques, Table No. 1 lists down some of the techniques of particular interest of this paper.

The techniques listed employ P-frames to detect forgeries of different kinds. The contribution of P-frames over shadows the significance of B-frames. Following are some of the algorithms which work on P-frames

Frame deletion detection approach based on motion and brightness attribute. Reference [12] introduced detection of frame deletion and its localization using Motion Compensated Edge Artifacts (MCEA).MCEA calculation is independent of the original video content. A drop in the temporal correlations between the adjoining video frames is a result of successive frames deletion in the video sequence. This temporal correlation was found to be closely related to the MCEA energy. MCEA energy values were used to determine an impact factor which indicated the target GOP subjected to tampering. The detection accuracy was claimed to be directly proportional to the number of frames deleted. This approach was applicable on a fixed GOP video structure but ceased to perform when the number of deleted frame were a multiple of the GOP length.

Reference [13] proposed a more refined approach to reference [12].The MCEA difference between adjoining P-frames is used to analyze the spikes (if any) in the Fourier transform domain which indicated inter-frame forgery. The localization of the tampering is not a part of this algorithm. Just like [12] this algorithm also worked on fixed GOP structure and failed if the number of frames deleted was a multiple of the GOP. Moreover this approach was incapable to detect forgery inH.264/AVC codec due to its advanced features. However

© 2018, IJCSE All Rights Reserved

this approach did not consider the effect of B-frames on the MCEA calculation of P-frames.

Sequence of Average Residual of P-frames (SARP) based technique to detect frame deletion. The difference in the predicted P-frame and the original P-frame constitutes the P-frame residual. Tampered video differ from the original video in terms of time and frequency domain attributes. To detect frame deletion forgery in H.264 codec, Sequence of Average Residual of P-frames (SARP) was deployed in time as well as frequency domain. Analysis of the SARP periodicity in the time domain indicated frame deletion. In frequency domain, spikes are witnessed at particular positions in the Discrete Time Fourier Transform (DTFT) spectrum as a result of these periodicities. These positions in DTFT spectrum help to localize the deleted frames in the given sequence. This technique achieved better detection results with an accuracy of 92%. However, this technique assumed fixed GOP structure for testing and is less flexible due to its implementation on only certain type of videos.

In addition to SARP, authors analyzed the magnitude of P-frame prediction error. As an improvement of the technique mentioned above, the magnitudes of the prediction error of P-frame was also examined to detect frame deletion and frame insertion type tampering. An anti-forensic method was inspected by which tampering footprints can be concealed by explicitly raising the prediction error of the P-frame of the forged video. Subsequently, a counter anti-forensic technique was proposed in which comparison between the actual prediction error and the prediction error of the forged video was studied. This approach was operative wholly in the frequency domain. Tampering localization was not achieved but this technique worked independent of the video encoding algorithm used to compress the video in initial stages. This algorithm worked on the P-frames' prediction errors but no similar approach was proposed for the B-frames.

Time and spatial domain analysis of quantization effects based inter-frame forgery detection. Reference [16] proposes an algorithm to detect and identify inter-frame forgery. This research encompassed three modules which were- detection of double compression in video, malignant inter-frame forgery detection and decision fusion.

Primarily, double compression detection involved analysis of the spatial domain by exploiting the characteristics inferred from the most significant digit distribution of Discrete Cosine Transform (DCT) coefficients in I-frames. Further an SVM classifier was utilized to discern double compression. This method had an accuracy of 87.1%. However, double compression does not inevitably entail malignant forgery. Consequently, time domain analysis of MARE (Mean Absolute of Residual Error) of P-frames was utilized to detect inter-frame forgery. This constituted the second module of this research where malicious frame insertion or frame deletion forgeries were detected by analyzing the difference between the kind of peaks in the MARE sequences of forged and original video. Time domain analysis had an advantage of tampering localization over frequency domain analysis. 83.39% accuracy was achieved by this frame-deletion detection technique.

Further the tertiary module categorized the input videos into three kinds- SCV (Single Compressed Videos), DCV (Double Compressed Videos) without malignant forgery and DCVs with malignant forgery. This module worked on the results of the prior two modules of detecting double compression and detecting inter-frame forgery.

As per [14], the accuracy of double compression detection was inversely proportional to the quantization scale of the primary compression. In addition to this, with the increase in the ratio of the first and second scales of quantization, a decrease in the reliability on this frame deletion detection technique was seen. Moreover, this research was limited to a fixed GOP structure of the test videos and only deletion of an entire GOP could be detected by the proposed method.

DCT (Discrete Cosine Transform) coefficient analysis, a video once tampered can be re-compressed by the forger. The forged video is re-compressed because without it the video inter-frames would visually appear "blockier" due to the de-synchronization of the GOP caused by the re-shuffling of frames between adjoining GOPs (due to frame insertion or frame deletion) [19]. This double compression of a video can be an indication of possible tampering, although it doesn't always necessarily imply malicious forgery. Discrete Cosine Transform (DCT) is the essence of JPEG compression. Images are compressed into 8x8 blocks of pixels called data unit. These data unit values are converted into sum of cosine function by DCT. DCT segregates a picture into parts which differ in importance due to their image quality. Inter-frame forgery disturbs the distribution of the DCT coefficients and leads to visible periodic artifacts in the histograms of frames which are double quantized. Reference [7] and [14] summarized various DCT based proposed algorithms where double compression was detected by studying the periodic pattern in the DCT coefficient histogram of I-frames and the error of motion histogram of P-frames. This approach took advantage of the fact that video frames within the same GOP have higher correlation because a P-frame uses the I-frame of its GOP as reference frame directly or indirectly. Frame insertion or deletion within a GOP leads to increase in the motion error estimation of P-frames due to shift in the GOP, leading to periodic peaks in the histogram. This method worked efficiently even if number of frames inserted or deleted was a multiple of 3. However, constraining to a fixed GOP structure, this method failed if the number of frames inserted/deleted were multiples of the GOP length.

© 2018, IJCSE All Rights Reserved

Exposure of chain of video re-compression by generating a residual series formed on the sequence of prediction error of P-frames. Reference [17] focuses on frame deletion tampering followed by a heterogeneous chain of recompression using a different GOP. This research focused on detecting forged videos, finding original GOP size and estimating the number of deleted frames. This research came up with an approach which analyzed the implicit periodic fingerprints in the prediction error sequence of P-frame. To detect recompression, residual sequence was produced which was based on the prediction error sequence of P-frame. The residual sequence underwent periodicity analysis to detect recompression. When recompression with a different GOP size takes place, some I-frames may become P-frames in the new sequence. However their anchor frame would no longer be in the same GOP sequence, resulting in higher periodic errors in these P-frames as compared to other P-frames. These spikes in the prediction error sequence indicate forgery. This research was highly accurate for H.264 codec and worked for all types of encoders. Since B-frames uses two reference frames (forward and backward), therefore, this research did not consider B-frames for simplicity. However, the efficiency of B-frames in this research was not discussed.

Using VPF (Variation of Prediction Footprint) based GOP size estimation. To detect double compression and estimate the original GOP size used in the first compression, an approach utilizing Variation of Predictive Footprint (VPF) was proposed. This technique was based on variable GOP structure and provided a high detection accuracy of 94% in case of H.264 encoded videos. If an originally compressed video was re-compressed (post tampering) with a different GOP size, and an I-frame is re-encoded as a P-frame, an aberrant drop in the number of S-macroblocks occur but the number of I-macroblocks increase. This footprint was used to detect double compression. Inter-frame forgery can be detected by analyzing the non-periodic peaks in the VPF caused by the tampering. This technique took into account only I-frames and P-frames and exploited the drift in the count of I-MBs and S-MBs in the P-frames which were I-frames before re-compression. This technique failed to work when the initial frames of the video were deleted. However, this disadvantage was successfully dealt by the authors of research reference [20], but the frames into consideration remained I-frames and P-frames.

To the best of author's knowledge, no inter-frame passive video forgery detection technique has been proposed which works on the B-frames. This research further tries to analyze the grounds of this isolation.

Table 1. Summary of passive video forgery detection techniques working on P-frames

Reference no.	Technique	Type of Forgeries detected	Author's remark
[12] and [13]	Motion-compensated edge artifacts (MCEA) based forgery detection technique.	Inter-frame forgery detection technique to detect frame deletion.	• This method is efficient in predicting the original GOP structure of the digital video. • It works for fixed GOP structures. • This algorithm fails when the number of frames deleted are a multiple of the GOP length. • It exploited the difference in MCEA between adjacent P-frames, without taking into account B-frames.
[14] and [15]	Sequence of Average Residual of P-frames (SARP) based technique.	Detection of frame deletion in H.264 encoded videos.	• It specifies the position of deleted frame in the frame sequence. • A fixed GOP structure is assumed. • Similar algorithm not devised for B-frames.
[14]	In addition to SARP, magnitude of P-frame prediction error is also analyzed.	Detects both frame insertion and deletion.	• Localization of tampering is not achieved. • Magnitude of B-frame prediction error not taken into account.
[16]	Time and spatial domain analysis of quantization effects. Performs time-domain analysis of MARE (Mean Absolute of Residual Errors) of P-frames.	Inter-frame forgery detection and double compression detection.	• Fixed GOP structure has been assumed. • Residual errors can be generated from the bi-directional motion compensated temporal prediction.
[7]	DCT(Discrete Cosine Transform) coefficient analysis	Double compression detection method.	• Works for fixed GOP structure. • Performance fails if the number of deleted frames is a multiple of the length of the GOP.

© 2018, IJCSE All Rights Reserved

			• Motion error of P-frames is taken into account but not of B-frames.
[17]	Exposure of chain of video re-compression by generating a residual series formed on the sequence of prediction error of P-frames.	Detects video re-compression using a different GOP. It also estimates the original GOP structure and the frames deleted to forge the video.	• B-frames are not considered in this work to minimize complexity.
[18] and [20]	Using VPF (Variation of Prediction Footprint) based GOP size estimation.	Detects double compression in video frames.	• Depends on the re-encoding of I-frames as P-frames and the count of specific macro-blocks in them. • B-frame influence is averted.

V. METHODOLOGY

B-frames are bi-directionally predictive frames. It uses both backward and forward frames to make its predictions.

Some properties of B-frames are [10]-

1. B-frames are encoded and decoded from the previous and next I-frame or P-frame. The predictions obtained from the previously encoded/decoded reference frames are averaged to create a B-frame.
2. B-frames are of lesser size than P-frames and I-frames. They help to achieve maximum proportion of data compression and thus increase the coding efficiency by a considerable amount. Compression ratio of B-frames in MPEG-x videos is 50:1 as compared to I-frame and P-frames which is 7:1 and 20:1 respectively. However the time and effort to encode/decode a B-frame is higher than the other two frames.
3. The decoder buffer memory required for B-frame is more than that of I-frame or P-frame. This is because two frames (previous and next) are compared and hence should be stored to reconstruct the B-frame.
4. An inter-frame can be decoded only when the frames from which it is predicted have already been decoded. Therefore B-frames require the reordering of the coding order because the reference frame (I or P) positioned next to the B-frame being predicted is coded first.
5. If prediction type is considered on the macro-block basis within an individual frame, then a B-frame can be composed of all 3 types of MBs i.e. intra MB, predicted MB and bi-predicted MB.
6. The latest codec systems like H.264 allow more than two reference frames to be used to predict a B-frame [10]. It also supports having random order of display relationship with respect to the frame(s) used for its prediction.
7. More are the B-frames, greater is the coding efficiency but lesser is the robustness.
8. To avoid growing of propagation error, in general, B-frames are not used as reference frames for predicting other frames. Though, in future B-frames may be used as reference in newer encoding methods like AVC. .This property prevents them from having an impact on any other frame. Therefore, their encoding quality can be further dropped without affecting other frames in the sequence. This is advantageous because in an error prone environment, it prevents the propagation of errors further in the frame sequence.
9. B-frame is incapable to support random access. This lack of flexibility in access is one of the major disadvantages of these frames.
10. The number of B-frames and their order in the GOP can vary according to the application. The demand of higher compression leads to the increase in the number of B-frames. However, the correlation of B-frame with its referenced frame is indirectly proportional to the number of B-frames in the sequence.
11. Another disadvantage of B-frames is that they cause a lot of frames delay both at the encoding and decoding end. At the encoding end it has to wait for the future I or P frame to encode the required B-frame. On the decoder's side it has to hold already decoded I or P frames to decode the prior B-frames dependent on them [11].

Pseudo code for proposed algorithm:

- Input the video.
- Decode video frames.
- Extract features of each decoded B-frames like temporal distances between previous and next I-frames and current B-frame and previous I-frame.
- Find block artefacts based on macro block selected for coding the video.
- Calculate variation of prediction footprints by finding distance between two B-frames.
- Apply transformation.
- Check for presence of spikes?
    a. If spikes are absent, the video is Authentic video
    b. Else the video id tampered

© 2018, IJCSE All Rights Reserved

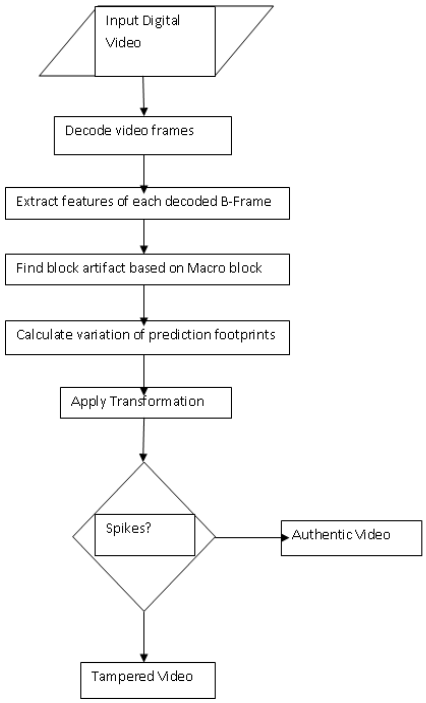

Figure 4. Flow-Chart of Proposed Algorithm

VI. CONCLUSION AND FUTURE SCOPE

Community from varied set of fields such as judicial forensic experts, multimedia security experts etc. are still demanding for improved techniques to deal with the challenges of video tampering. The conclusion may be drawn based on the research performed is that the proposed algorithm for making use of B-frames in digital video tampering detection is as follows: B-frames can enhance the accuracy of tampering detection just like it increases the compression ratio while capturing or editing video contents. It may increase the localization accuracy of tampered region in doctored digital video. The proposed algorithm may be expensive in terms of space complexity. But as hardware support is not a setback these days, it will not weigh down the performance of proposed algorithm.

The research can be implemented in the future using MATLAB / Java to devise an efficient algorithm to detect inter-frame passive video tampering using B-frames that conform to the advantages of the proposed ideas discussed earlier. In MATLAB, with the help of Computer Vision System Tool-Box, feature detection, extraction and implementation of algorithm can be performed.

REFERENCES

[1]. B.G. Haskell and A. Puri: MPEG Video Compression Basics, Chapter 2. In:L. Chiariglione (ed.), The MPEG Representation of Digital Media, DOI 10.1007/978-1-4419-6184-6_2, © Springer Science+Business Media, LLC 2012.

[2]. I. Amerini, R. Becarelli, R. Caldelli, and M. Casini. A feature-based forensic procedure for splicing forgeries. Mathematical problems in Engineering, 2015

[3]. W. Wong and H. Farid "Exposing Digital Forgeries in video by detecting double quantization" Proceeding of MM& SEC 2009, ACM 978-1-59593-857-2/07/0009

[4]. Salam A.Thajeel and Ghazali Bin Sulong:State of the art of copy-move forgery detection techniques: a review. In: IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 6, No 2, November 2013.

[5]. Sowmya K.N., H.R. Chennamma: A survey on video forgery detection. In: International Journal of Computer Engineering and Applications, Volume IX, Issue II, February 2015.

[6]. C. Cruz-Ramos, R. Reyes-Reyes, M. Nakano-Miyatake, H. Perez-Meana: A Blind Video Watermarking Scheme Robust to Frame Attacks Combined with MPEG2 Compression. In: Journal of Applied Research and Technology, Vol. 8, No. 3, December 2010.

[7]. Staffy Kingra, Naveen Aggarwal and Raahat Devender Singh: Video Inter-frame Forgery Detection: A Survey. In: Indian Journal of Scienceand Technology, Vol 9(44), DOI: 10.17485/ijst/2016/v9i44/105142, November 2016.

[8]. Ainuddin Wahid Abdul Wahab, Mustapha Aminu Bagiwa, Mohd Yamani Idna Idris, Suleman Khan and Zaidi Razak: Passive Video Forgery Detection Techniques: A Survey. In: 2014 International Conference on Information Assurance and Security (IAS).

[9]. Tanzeela Qazi, Khizar Hayat, Samee U. Khan, Sajjad A. Madani, Imran A. Khan,Joanna Kołodziej, Hongxiang Li, Weiyao Lin, Kin Choong Yow and Cheng-Zhong Xu: Survey on blind image forgery detection. In: in IET Image Processing, Accepted on 19th February 2013 doi:10.1049/iet-ipr.2012.0388.

[10]. D. Labartino, T.Bianchi, A. De Rosa, M. Fontani, D. V´azquez-Pad,A. Piva, M. Barni, "Localization of Forgeries in MPEG-2 Videothrough GOP Size and DQ Analysis" MMSP'13, Sept. 30 - Oct. 2, 2013, Pula (Sardinia), Italy.

[11]. Umesh Kumar Singh, Chanchala Joshi, Suyash Kumar Singh, "*Zero day Attacks Defense Technique for Protecting System against Unknown Vulnerabilities*", International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.1, pp.13-18, 2017Su, Y., Zhang, J., Liu, J.: Exposing digital video forgery by detecting motion-compensated edge artifact. In: Proceedings of International Conference on Computational Intelligence and Software Engineering, Wuhan, China. Vol. 1, no. 4, pp. 11–13 (2009).

[12]. Qiong Dong, Gaobo Yang, Ningbo Zhu: A MCEA based passive forensics scheme for detecting frame-based video tampering. In: Digital Investigation, November 2012, DOI:0.1016/j.diin.2012.07.002

[13]. Raahat Devender Singh and Naveen Aggarwal: Video content authentication techniques: a comprehensive survey. In: 19 January 2017 © Springer-Verlag Berlin Heidelberg 2017.

[14]. Huang, Xinyi, and Jianying Zhou, eds. *Information Security Practice and Experience: 10th International Conference, ISPEC 2014, Fuzhou, China, May 5-8, 2014, Proceedings*. Vol. 8434. Springer, 2014.

[15]. Javad Abbasi Aghamaleki& Alireza Behrad: Malicious inter-frame video tampering detection in MPEG videos using time and spatial

© 2018, IJCSE All Rights Reserved

domain analysis of quantization effects. In: Springer Science+Business Media New York 2016, Accepted: 23 September 2016.

[16]. Jingxian Liu and Xiangui Kang: Exposing Heterogeneous Chain of Video Recompression. In: Guangdong Key Lab of Information Security, School of Data and Computer Science, Sun Yat-Sen University, Guangzhou 510006, China.

[17]. Vázquez-Padín, D., Fontani, M., Bianchi, T., Comesana, P., Piva, A. Barni, M.: Detection of video double encoding with GOP size estimation. In: Proceedings on IEEE International Workshop on Information Forensics and Security, Tenerife, Spain, 151 (2012)

[18]. Hee-Meng, Ho: 'Digital Video Forensics: Detecting MPEG-2 Video Tampering through Motion Errors'. In: MSc. Information Security 2011/12, Royal Holloway University of London.

[19]. A. Gironi, M. Fontani, T. Bianchi, A. Piva, M. Barni (2014). A video forensic technique for detecting frame deletion and insertion. In: 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Firenze, May 2014. pp. 6226-6230.

[20]. Xin-Wei Yao, Yue-Feng Cen, Wan-Liang Wang, Xiao-Min Yao, Shuang-Hua Yang and Tie-Qiang Pan: IPB-frame Adaptive Mapping Mechanism for Video Transmission over IEEE 802.11e WLAN. In: ACM SIGCOMM Computer Communication Review, Volume 44, Number 2, April 2014.

[21]. Jianmei Yang & Tianqiang Huang & Lichao Su: Using similarity analysis to detect frame duplication forgery in videos.In: Published online-20 November 2014, Springer Science+Business Media New York 2014.

[22]. A.V. Subramanyam and Sabu Emmanuel: Pixel Estimation Based Video Forgery Detection. In:Acoustics, Speech and Signal Processing, 1988. ICASSP-88., 1988InternationalConference on October 2013.

[23]. Lichao Su & Tianqiang Huang & Jianmei Yang: Avideo forgery detection algorithm based on compressive sensing. In: Springer Science+Business Media New York 2014, 2 March 2014.

[24]. Jianmei Yang & Tianqiang Huang & Lichao Su: Using similarity analysis to detect frame duplication forgery in videos. In: Springer Science+Business Media New York 2014, Published online: 20 November 2014.

[25]. Liyang Yu·Qi Han·Xiamu Niu: Feature point-based copy-move forgery detection: covering the non-textured areas. In: Published online: 4 December 2014 at Springer Science+Business Media New York 2014.

[26]. Mohammad Jafari, Neda Abdollahi, Ali Amiri, Mahmood Fathy, "*Generalization of Determinant Kernels for Non-Square Matrix and its Application in Video Retrieval*", International Journal of Scientific Research in Computer Science and Engineering, Vol.3, Issue.4, pp.1-6, 2015

[27]. Ashish Kumar Kushwaha and Avinash Wadhe: Design and Implementation of Forensic Framework for Video Forensics. In: International Journal of Current Engineering and Technology, Accepted 02 April 2015, Available online 07 April 2015, Vol.5, No.2 (April 2015).

[28]. D. V´azquez-Pad´ın, M. Fontani, T. Bianchi, P. Comesa˜na, A. Piva, M. Barni: Detection of video double encoding with GOP size estimation. In: WIFS'2012, December, 2-5, 2012, Tenerife, Spain. 978-14244-9080-6/10/$26.00 copyrights-2012 IEEE.

[29]. Markus Flierland Bernd Girod: Generalized B Pictures and the Draft H.264/AVC Video Compression Standard. In: IEEE Transactions on circuits and systems for video technology.

[30]. Bruno Zatt, Marcelo Porto, Jacob Scharcanski, Sergio Bampi: GOP structure adaptive to the video content for efficient H.264/AVC encoding. In Proceedings of ICIP International Conference on Image Processing, September2010.

[31]. Nikhilkumar P. Joglekar1, Dr. P.N. Chatur: A Compressive Survey on Active and Passive Methods for Image Forgery Detection. In: International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 4 Issue 1 January 2015, Page No. 10187-10190.

[32]. Harmanpreet Kaur and Manpreet Kaur: Inter frame Video Duplication Forgery Detection: A Review. In: International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 4 Issue 8 Aug 2015, Page No. 13806-13809.

[33]. Aldrina Christian, Ravi Sheth: Digital Video Forgery Detection and Authentication Technique - A Review. In: 2016 IJSRST | Volume 2 | Issue 6 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X.

Authors Profile

Mrs. Vaishali Joshi pursed Bachelor of Science (Mathematics Honors) from Barkatullah University, Bhopal in 1999 and Master of Computer Applications (MCA) from Rajiv Gandhi Prodyogiki Vishwavidyalaya (RGPV), The state Technical University of Madhya Pradesh, Bhopal in 2002. She is currently pursuing Ph.D. from ITM University Gwalior and currently working as Assistant Professor in Department of Computational Applications, in Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi since 2013. She is a life member of IETE & Computer Society of India (CSI) since 2013. Se has published many research papers in reputed international Conferences and Journals.

Dr. Sanjay Jain has more than 15 years of experience in industry and academia. He has done his PhD in Computer Science and Engineering from Rajiv Gandhi Prodyogiki Vishwavidyalaya (RGPV), The state Technical University of Madhya Pradesh, Bhopal. He is currently working as Associate Professor in School of Computer Applications (SOCA), ITM University, Gwalior, Madhya Pradesh. He also holds the post of Dean Student Welfare in the University. He is a member of IETE & Life member of Computer Society of India. Dr. Jain has also been resource person in many Faculty Development Programs conducted country wide. He has chaired session in prestigious international conference INDIACom-2015. He has published many research papers and case studies in national and international journals.

Ms.Chahat Bansal has done her graduation from Delhi University in science in 2015. She is persuing Master in Computer Applications from Guru Gobind Singh Indraprastha University, New Delhi. She always been a meritorios student and participated in many research activities during her studies. She has qualified National Eligibility Test (NET) for Junior Research Fellowship in December 2017.

© 2018, IJCSE All Rights Reserved