International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.6, pp : 816-817 1 June 2014

Detecting Duplication and Double MPEG Compression-A Survey

Gayatri Dakhode
M.tech CS Engineering
Astral Institute of Technology and Research, Indore
Email- gayatrida11@gmail.com

Abstract: With the advent of high quality digital video cameras and low cost video editing software, it is becoming easier to tamper with digital video. A common form of manipulation is copy move forgery in video and double MPEG compression of video. This paper performs an review on the detecting copy move forgery and double MPEG compression in video.

Keywords- Digital Tampering, Digital Forensics, copy move forgery, Double MPEG, Digital video

1. Introduction

Nowadays authenticating a given digital video content has become more difficult because of the possible diverse origins and the potential alterations that could have been operated on it. This is due to the availability of inexpensive, easily operable multimedia devices and with high quality data processing tools, algorithms, has made the video processing accessible to a wide range of users. When the digital content is used to support legal evidences its important details could be maliciously hidden or erased or duplicated from the recorded scene, and the true original source can be concealed. The detection of copyright infringements and validation of legal property of multimedia data may be difficult; this fact can be exploited to pretend on its original characteristics i.e. low quality contents re-encoded at high quality [ii, iii]. A common and easy manipulation is to remove people or objects from a video sequence or simply remove undesired event from a video. When done carefully, this digital tampering is very difficult to detect. Such a copy move forgery done in images also and the methods for detecting image duplication have been proposed in [x, xi].

This paper give a survey on the efficient techniques for detecting duplication i.e. copy move forgery in the digital video. The digital watermarks and signatures offer a solution to authentication. This paper gives information about methods for detecting traces of tampering in digital video that do not rely on digital watermarks or signatures. This work follows similar approaches to detecting traces of tampering in digital images (e.g. [iv, v, vi, vii, viii, ix, xi]). Also this paper gives information about a doubly compressed MPEG video sequence which introduces static and temporal statistical perturbations and these perturbations can be used as evidence of tampering.

2. Related Work

So many methods are available till today for detecting tampering in digital video. Few related work is studied here:

Wang and Farid [xii] targets copy move detection directly in video. This method uses a kind of divide and conquers approach: the whole video is split in subparts, and different kinds of correlation coefficients are computed in order to highlight similarities between different parts of sequence. There is only one work authored by Wang and Farid that targets on the copy move forgery in digital video [i].

Wang and H. Farid [iii] proposed how a doubly compressed MPEG video sequence introduces specific static and temporal statistical perturbations and these perturbations presence can be used as evidence of tampering .Such type of a video emerge when, an originally encoded MPEG video is edited and resaved as a MPEG video.

W. Wang and Farid [xiii] proposed a one of the best technique for detecting double quantization in digital video that results from double MPEG compression, it shows how the double quantization introduces statistical artifacts that are easily not visible to the user, can be used to detect tampering.

3. Methodology

3.1 Detecting Duplication in video:

Frame Duplication:

Consider a video where three frames are duplicated to remove the object. This type of manipulation is very easy to perform due to video editing software’s and can be difficult to detect visually particularly in a video taken from stationary surveillance camera. Given a video sequence of length L, it would be computationally intractable to search for duplication by comparing all possible subsequences of arbitrary length and positions in time. The computationally efficient algorithm for detecting duplicated video frames that is robust to compression artifacts is proposed in [xii].

Basic approach is to partition full length video sequence into short overlapping subsequences. An efficient to compute representation that embodies both the temporal and spatial correlations in each subsequence is then extracted and compared throughout the entire video sequences. Similarity in the temporal and spatial correlations is then used as evidence of duplication [xii].

Region Duplication:

The frame duplication method shows how to detect duplicated frames in a video sequence. In some cases the part of several frames are duplicated. This form of duplication will not be detected using frame duplication method. So this form of tampering can be detected using this method. Consider that, a subset of pixels of unknown location are duplicated and placed in another frame at a different spatial location, the shift between the given pair of frames is estimated using phase correlation technique which is briefly described in [xii].

3.2Double MPEG Compression:

Fig (1) illustrates methodology proposed by Wang and Farid [iii]. In following fig (1), the first row is an original MPEG encoded sequence. The subsequent rows show the effect of deleting the three frames in the shaded region of first row. Shown in the second row are the reordered frames, and in the third i.e. last row, the re-encoded frames. The I-frame earlier to the deletion is subjected to double compression. Some of the frames following the deletion move from one GOP sequence to another GOP. This double MPEG compression gives rise to specific static and temporal statistical patterns that may be used as evidence of tampering of forged digital video.

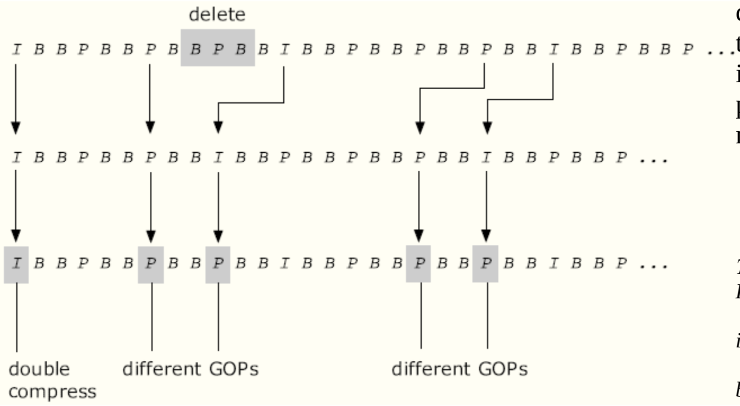
delete
I B B P B B P B B P B B I B B P B B P B B P B B I B B P B B P ...
I B B P B B P B B I B B P B B P B B P B B I B B P B B P ...
I B B P B B P B B P B B I B B P B B P B B P B B I B B P ...
double compress
different GOPs
different GOPs

Fig (1): MPEG sequence of short 31 frames [iii]

Static:
When I-frame goes to the deletion gives its identity and will be re-encoded using JPEG compression, it achieves compression by quantizing the DCT coefficients. When an I-frame is compressed twice, with different bit rates, the DCT coefficients are subject to two levels of quantization. This double compression leaves behind a specific statistical signature in the distribution of DCT coefficients [ix, iii].

Temporal:
The first frame of each group of picture (GOP) is an I-frame. This I frame is only statically compressed, effectively corrects for motion estimation errors that accumulate throughout each GOP. With respect to the initial I-frame, each P frame is either directly or indirectly encoded

As an example, consider the effect of deleting the first six frames of following sequence:

I B B P B B P B B P B B I B B P B B P B B P

After the deletion of first six frames leaves as,

P B B P B B I B B P B B P B B P

After re-encoding, becomes,

I B B P B B P B B P B B I B B P

In the first Group of Picture of this sequence, the I-frame and first P-frame are from the first Group of Picture of the original sequence. The second and third P frames in the re-encoded sequence, are the I frame and first P frame from the second GOP of the original sequence. When this new sequence is re-encoded, expect a larger motion error between the first and second P frames, since they are originated from different GOPs. Moreover, this increased motion error will be periodic, occurring throughout each of GOPs following the frame deletion. This change in motion error is due to the, all of the P frames within a single GOP are correlated to the initial I frame. The temporal perturbation is used as evidence of tampering [iii].

4. Conclusion

There are different techniques to detect the copy move forgery and double MPEG compression in video. These two techniques are used in conjunction in video forensic to make harder to doctor digital video. This paper does an extensive survey on the technique to detect duplication and double MPEG compression in video. There is a great challenge for this work to perform the performance survey of using these techniques in conjunction to make increasingly harder to doctor digital video.

References

i. *P. Bestagini, M. Fontani, S. Milani, A. Piva, M. Tagliasacchi, S. Tubaro, " An Overview On Video Forensics," in 20th European Signal Processing Conference, Romania, August 2012*

ii. *Weihong Wang and Hany Farid, " Detecting re-projected video," in information hiding ,2008*

iii. *Weihong Wang and Hany Farid, "Exposing digital forgeries in video by detecting double MPEG compression," in MM&Sec,2006*

iv. *J. Lukas, J. Fridrich, and M. Goljan, "Detecting digital image forgeries using sensor pattern noise," in Proceedings of the SPIE, volume 6072, 2006.*

v. *M. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," In ACM Multimedia and Security Workshop, New York, 2005.*

A. *Popescu and H. Farid, "Exposing digital forgeries by detecting traces of re-sampling ," IEEE Transactions on Signal Processing 53(2):758-767,2005.*

vi. *Popescu and H. Farid , "Exposing digital forgeries in color filter array interpolated images," IEEE Transactions on Signal Processing, 53(10):3948-3959,2005.*

vii. *T. Ng and S. F. Change, "A model for image splicing," In IEEE International Conference on Image Processing, Singapore, October 2004.*

A. *Popescu and H. Farid, "Statistical tools for digital forensics ," in 6th International Workshop on Information Hiding, Toronto, Canada,2004.*

viii. *Popescu and H. Farid , " Exposing digital forgeries by detecting duplicated image regions." Technical Report TR2004-515, Department of Computer Science, Dartmouth College, 2004.*

ix. *J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy move forgery in digital images," In Proceedings of Digital Forensic Research Workshop, August 2003.*

x. *Weihong Wang and H. Farid, "Exposing digital forgeries in video by detecting duplication," in MM&Sec, 2007.*

xi. W. Wang, H. Farid, "Exposing digital forgeries in video by detecting double quantization," MM&Sec , 2009.