International Journal of Engineering & Technology, 7 (4.6) (2018) 373-376

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An Overview of Digital Video Tampering Detection Using Passive Methods and D-Hash Algorithm

Anto Crescentia.A[1], Sujatha.G[2]

[1,2]Department of Information Technology([1]M.Tech in Information Security and Cyber Forensics), SRM Institute of Science and Technology, Chennai
**Corresponding author E-mail: antocrescentia3@gmail.com*

Abstract

Video tampering and integrity detection can be defined as methods of alteration of the contents of the video which will enable it to hide objects, an occasion or adjust the importance passed on by the collection of images in the video. Modification of video contents is growing rapidly due to the expansion of the video procurement gadgets and great video altering programming devices. Subsequently verification of video files is transforming into something very vital. Video integrity verification aims to search out the hints of altering and subsequently asses the realness and uprightness of the video. These strategies might be ordered into active and passive techniques. Therefore our area of concern in this paper is to present our views on different passive video tampering detection strategies and integrity check. Passive video tampering identification strategies are grouped into consequent three classifications depending on the type of counterfeiting as: Detection of double or multiple compressed videos, Region altering recognition and Video inter-frame forgery detection. So as to detect the tampering of the video, it is split into frames and hash is generated for a group of frames referred to as Group of Pictures. This hash value is verified by the receiver to detect tampering.

***Keywords**: Video tampering detection, Region altering, Video forensics, anti-forensics, group of pictures*

1. Introduction

Data tampering is that demonstration of intentionally adjusting (wrecking, controlling or altering) information through unapproved channels. These type of data can therefore exists in two states; either in transit (motion) or still (rest). As videos are used as evidences in many judiciary cases it is essential to ensure that there is no alteration of such videos. This is where video tampering detection comes into play. Video altering identification intends to find the hints of changing and in this way assess the realness and integrity of the video file. There are two types of tampering detection methods that can be used, they are passive and active tamper detection methods. Our area of concern is only the passive methods and its techniques. The general classification and each of these methods of passive video tampering identification can further be classified as follows:

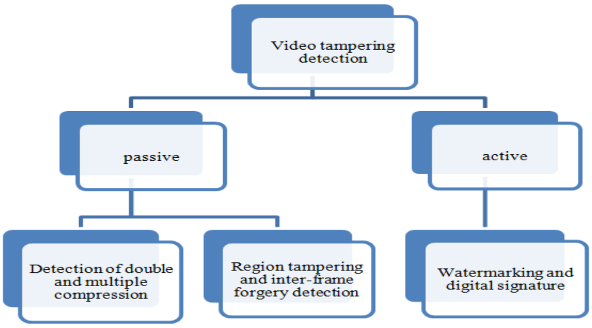
Video tampering detection
passive
active
Detection of double and multiple compression
Region tampering and inter-frame forgery detection
Watermarking and digital signature

Fig.1: Classification of detection methods

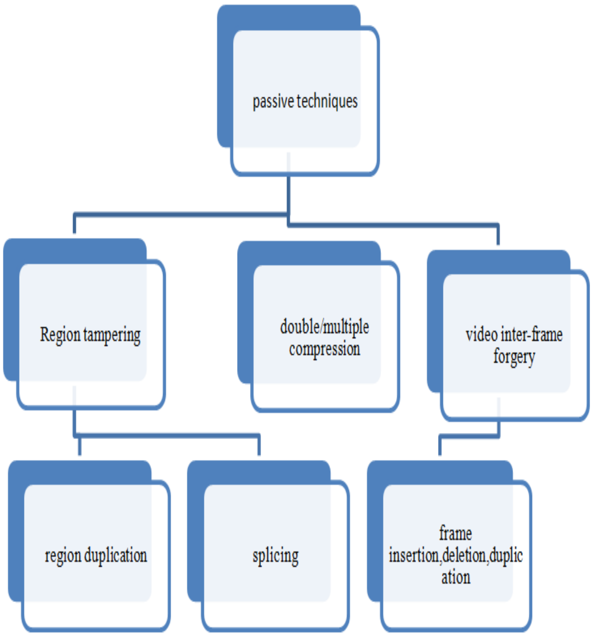
passive techniques
Region tampering
double/multiple compression
video inter-frame forgery
region duplication
splicing
frame insertion,deletion,duplication

Fig.2: Types of passive detection

a) Double or multiple compression detection:

Due to rapid availability of ground-breaking processors and easy to understand programs,the altering of video contents is changing into a frequent occurrence. Besides, after each altering step, any video content is almost perpetually encoded with the end goal to store it utilizing a less amount of memory. Thus, gathering the number of compression steps that are connected to such a multimedia content is a significant piece of information with the end goal to survey its validity.

b) Region tampering detection:

Region tampering detection methods provide data regarding the location of tampering in the spatial as well as temporal domain. This type of tampering can occur either within the same frames or between different frames. This is done by copying a small portion of the frame and pasting at different location within the same frame, or copying explicit regions from a frame and pasting it at another sequence of the identical video. This kind of tampering is detected using the distinction between the frame under examination and non-tampered reference frames.

c) Video inter-frame forgery detection:

Videos regularly offer forensic proof in lawful, medicinal and police examination applications however are more in danger of inter-frame forgeries , that don't appear to be exclusively direct to perform yet are similarly hard to identify also. One will essentially embed or take away a particular frame or set of frames to alter the underlying video content. By and large, adjoining frames in a video with the indistinguishable background have vigorous connection. If the video being tampered, the continuity of the frames correlation is going to be disturbed. So as to perform any form of tampering operation, individual frames are initially extracted and altered with the intention to deceive the user. The recreation of the altered video utilizing the changed frames prompts to perform double compression because of some measure of compression is unavoidable at whatever point a video is saved. The most primitive developments inside the field of video inter-frame forgery detection depended on identification of hints of double compression in video sequences.

Capturing of videos in various devices is very common these days and so is editing of such videos. Thus authentication and integrity validation is very essential in the current scenario and here comes the importance of video forensics. There are various steps used in passive video tampering detection which includes frame separation, hashing of these frames, identifying similar frames and grouping them. This hash generated is used to verify if the video is tampered or not.

2. Problem Statement

Video tampering is a serious issue and it has to be addressed because videos serve as proofs in many cases. Therefore there is a need to provide authentication, check integrity, hence maintaining confidentiality. This paper looks into identifying methods to detect tampering in videos. Strategy that tends to one kind of forgery isn't fit for tending to another sort of forgery, for instance techniques fit for distinguishing frauds based on the motion of the video. To overcome these drawbacks videos are split into frames which are later grouped into blocks called Group of Pictures. It also aims at detecting anti-forensic techniques using hashing techniques.

3. Proposed Methodology

In the proposed architecture the video is taken as input and it is segregated into frames. Hashing algorithm called dhash is used to calculate the hash values of each of these frames. Based on the hamming difference between the adjacent frames they can either be grouped together or not. If the hamming distance is small then they are similar frames and thus grouped together to form a block called the Group of Pictures. The generated hash value is sent along with the video to the receiver. The receiver verifies the integrity of the video by first segregating the frames and then calculating the hash. If the hash values match then there is no tampering

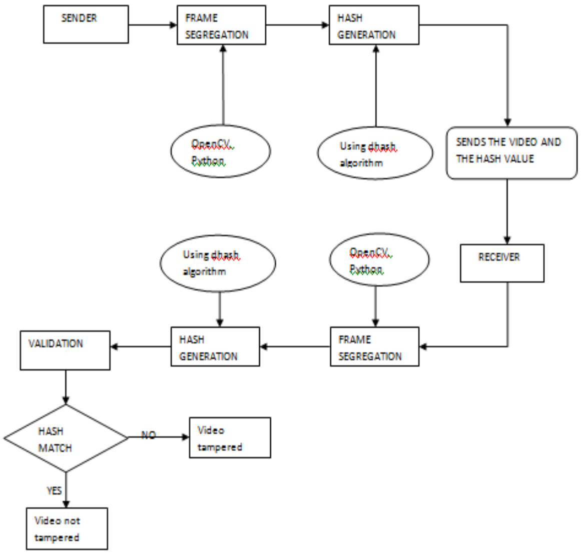

Fig.3: Architecture Diagram

This module deals with disintegration of the video into individual frames. A video is only an accumulation of images which all are shown in a steady progression in order to make the deception of movement exploiting the respectability of vision of human visual framework .In technical terms instead of describing videos as a collection of images we can describe it as collection of frames. A collection of such frames form a block called Group of Pictures (GOP). These GOP have a standard format in the order of I(Intra-coded), B(Bi-directionally predicted) and P(Predicted) frames are with the end goal that the I-frames seems first pursued by B and P frames. Therefore the video has to be segregated as individual frames and this can be done with the help of OpenCV python which takes the video file as input and uses python code to convert it as frames.

a) Hashing of frames:
In order to group the identical frames into a GOP we first have to identify similar frames and to do that we have to find the hash values of each of the frames. There are four steps in image hashing using **dhash algorithm** also known as the difference hashing algorithm. These steps are:

1.Convert to gray scale

2.Resize

3.Compute the difference

4.Build the hash

1. Convert to gray scale:

A color image is made up of combinations of red, green and blue (RGB) pixels which can be thought of as sets of red, green and blue values. By grayscaling the picture we lessen every pixel value to an iridescent intensity value and to convert RGB to gray scale there are various methods they are:

i.The luminescence method: This method finds the mean of the most eminent and least eminent colors which can be given as (maximum(Red, Green, Blue) + minimum(Red, Green, Blue)) / 2.

ii.The mean method: This method simply computes the mean of all the three colours which can be given as (Red + Green + Blue) / 3.

iii.The weighted-average method: This method is similar to the previous one in that it computes the average, but it also estimates a weight for the average. Based on sensitivity green is weighted the most because it is more responsive to the naked eye. This method is also called luminosity method and it's formula is (0.21 Red + 0.72 Green + 0.07 Blue)

2.Resize:

Resizing is nothing but reducing the image to a common standard size that is easy to work with for instance it takes 9x8 pixels, where the width is one pixel more than the height. This helps to erase all the high level frequencies and all the information of the images and this leaves us with 72 as the intensity values, which apparently means that changing the size that is expanding or shrinking an image will not affect it's hash value. This can be done using python or matlab.

3. Compute the difference:

The difference hash algorithm functions by calculating the distinction (i.e., relative angles)between contiguous pixels. On the off chance that we take an input picture with 9 pixels for each line and figure the distinction between contiguous section pixels, we wind up with 8 differences. Eight lines of eight differences (i.e., 8×8) is 64 which will end up being our 64-bit hash.

4. Build the hash:

The last step is to allocate bits and construct the subsequent hash. To achieve this, we utilize a straightforward binary test. For the input picture taken as D and for their resulting set of pixels P we perform the following test as
P[x] > P[x + 1] = 1 else 0.
For this situation, we are trying to find out if the left pixel is more intense than the right pixel. In the event that the left pixel is more intense we set the output value an incentive to one. On the contrary if the left pixel is less intensive than the right pixel we set the output to zero.
b)Comparing the difference of the hashes:
Hamming Distance is used as the criteria to perform the comparison of the hashes. The Hamming distance estimates the total number of bits in two hashes that are different from the other.
It can be summarized that any two hashes having similar hamming distance that is their difference is Zero then it can be inferred that the two hashes are indistinguishable (since there are no varying bits) and apparently the two images are indistinguishable/perceptually comparable too.
In the exact same way we can also infer that hashes with differences greater than 10 bits are in all likelihood different from each other, while Hamming distances somewhere in the range of 1 and 10 are conceivably a variation of an identical picture.

4. Conclusion

A video is tampered by repeating, expelling, embedding and supplanting the
contents inside the frames. There is a developing enthusiasm for recognizing the validity of the videos in a variety of cases. In this paper, we've broke down passive tampering identification ways and conjointly ensured integrity of the video using hashing algorithm. In the current scenario there exists no tools or efficient software for video tampering detection. So as a result of the outcome of our integrity check we can further use it to detect where exactly the video has been tampered and this can be looked into as a fruitful research area

Reference

[1] Piva, "An overview on image forensics," ISRN Signal Processing, vol. 2013

[2] Subramanyam and S. Emmanuel, "Video forgery detection using HOG features and compression properties," in 2012

[3] Ardizzone, E., Mazzola, G., 2015. Image Analysis and Processing | ICIAP 2015: 18th International Conference, Genoa, Italy, September 7-11, 2015, Proceedings, Part II. Springer International Publishing, Cham, Ch. A Tool to Support the Creation of Datasets of Tampered Videos, pp. 665{675.

[4] Bidokhti, A., Ghaemmaghami, S., March 2015. Detection of regional copy/move forgery in MPEG videos using optical ow. In: Articial Intelligence and Signal Processing (AISP), 2015 International Symposium on. pp. 13 17.

[5] Chao, J., Jiang, X., Sun, T., 2013. Digital Forensics and Watermaking: 11th InternationalWorkshop, IWDW2012, Shanghai, China, October 31 { November 3, 2012, Revised Selected Papers. Springer Berlin Heidelberg, Berlin, Heidelberg, Ch. A Novel Video Inter-frame Forgery Model Detection Scheme

[6] Chen, W., Shi, Y. Q., 2009. Digital watermarking. Springer-Verlag, Berlin, Heidelberg, Ch. Detection of Double MPEG Compression Based on First Digit Statistics

[7] Chetty, G., Biswas, M., Singh, R., 2010. Digital video tamper detection based on multimodal fusion of residue features. In: Network and System Security (NSS), 2010 4th International Conference on. IEEE

[8] Cozzolino, D., Poggi, G., Verdoliva, L., Oct 2014. Copy-move forgery detection based on patchmatch. In: 2014 IEEE International Conference on Image Processing (ICIP)

[9] D. Vazquez-Padin, M. Fontani, T. Bianchi, P. Comesana, A. Piva, and M. Barni, "Detection of video double encoding with GOP size estimation," in 2012

[10] Dong, Q., Yang, G., Zhu, N., 2012. A MCEA based passive forensics scheme for detecting frame-based video tampering. Digital Investigation 9

[11] Gironi A, Fontani M, Bianchi T, Piva A, Barni M,"AVideo Forensic Technique for Detecting Frame Deletion and Insertion",In2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2014 May 4.

[12] Hyun DK, Ryu SJ, Lee HY, Lee HK. 2013 Sep; Detection of upscalecrop and partial manipulation in surveillance video based on sensor pattern noise. Sensors. 13(9):12605–31.

[13] Jiang, X., Wang, W., Sun, T., Shi, Y. Q., Wang, S., 2013. Detection of double compression in MPEG-4 videos based on markov statistics. Signal Processing Letters, IEEE 20 (5)

[14] Jin H,"Research of Blind Forensics Algorithm on Digital Image

[15] Tampering",Indonesian Journal of Electrical Engineering and Computer Science,2014 July

[16] Kobayashi M, Okabe T, Sato Y. 2009 Jan Detecting video forgeries based on noise characteristics. Springer Berlin Heidelberg;. p. 306–17.

[17] Lin CS, Tsay JJ. July 2014 A passive approach for effective detection and localization of region-level video forgery with spatiotemporal coherence analysis. Digital Investigation.

[18] Liu H, Li S, Bian S. 2014 May Detecting frame deletion in H 264 video.Springer International Publishing;. p. 262–70.

[19] P. He, X. Jiang, T. Sun, S. Wang, B. Li, Y. Dong, "Frame-wise detection of relocated I-frames in double compressed H.264 videos based on convolutional neural network", J. Vis. Commun. Image Represent., vol. 48, pp. 149-158, Oct. 2017.

[20] Richardson, I. E., 2003. H. 264 and MPEG-4 video compression: video coding for next-generation multimedia. John Wiley & Sons.

[21] S. Chen, S. Tan, B. Li, J. Huang, "Automatic detection of object-based forgery in advanced video", IEEE Trans. Circuits Syst. Video Technol., Nov. 2016

[22] 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, vol. 1

[23] Shanableh T, “Detection of Frame Deletion for Digital Video Forensics”, Digital Investigation2013 Dec 31;10(4):350-60

[24] Su L, Huang T, Yang J. A video forgery detection algorithm based on compressive sensing. Multimedia Tools and Applications. 74(17):6641–56.

[25] W.Wang, H. Farid, "Exposing digital forgeries in video by detecting double quantization", Proc. 11th ACM Workshop Multimedia Secur., pp. 39-48, 2009.

[26] Xu Z, Feng C, Zhang W, Xu Y,“Automatic Location of Frame Deletion Point for Digital Video Forensics”,InProceedings of the 2nd ACM workshop on Information hiding and multimedia security 2014 Jun 11

[27] Y. Su, J. Xu, "Detection of double-compression in MPEG-2 videos" May 2010

[28] Zheng L, Sun T, Shi YQ. Inter-frame video forgery detection based on block-wise brightness variance descriptor. Springer International Publishing; 2014 Oct. p. 18–30.