International Journal of Computing and Network Technology
ISSN (2210-1519)
Int. J. Com. Net. Tech. 6, No. 2 (May-2018)

http://dx-doi.org/10.12785/ijcnt/060202

Lightweight Digital Watermarking Method for Videos Forgeries Detection

Tawfiq Barhoom[1] & Mohammed Arabid[2]

[1,2]*Faculty of Information Technology Islamic University, Gaza, Palestine*

Received: 5 Jan. 2018, Revised: 8 March 2018, Accepted: 21 March. 2018, Published: (1 May 2018)

Abstract: With the advancement of the digital video and digital image editing tools, this increases the difficulty for humans to identify visually the authentic video from the forged copy. This needs a powerful method that investigates various video from tempering attempts. There are several previous types of research, which propose methods for video forgery detection. These works suffer from consuming the memory and much-comparing power. The consequence is increasing the execution time. This research proposes a lightweight method; this means reduce memory usage and execution time for detecting forgery in video streams. The method based on using mathematical schema structure to explore various forgeries type on streaming videos. Experiments have been conducted on a dataset of 27 videos covering different cases using local IP camera, cases like using compression algorithms and some tempering effects. The result indicated that the system achieved high relevant measures with 97% accuracy on detecting duplication on a case of lossless compression and 95% on the other compression algorithms; on the other hand, on detecting cloning forgeries our system achieved a highly relevant measure with 86% on a case of lossless compression.

Keywords: Digital Tampering, Digital Forensics, Video Forgery, Streaming attacks, Digital Watermarking, Streaming Security.

1. INTRODUCTION

Forgery is the process of making, adapting or imitating objects. Forgeries are not new to mankind but are a very old problem. In the past, it was limited to art and literature but did not affect the general public. Nowadays, due to the advancement of digital video processing software and editing tools, a video can be easily manipulated and modified[1], This is mainly due to the availability of low-cost hardware and photo editing software which makes it easy to manipulate and alter digital videos without leaving any obvious trace. Therefore there is a rapid increase in digitally manipulated forgeries in mainstream media and on the Internet [2], in addition, The task of validating a given multimedia content has become harder task because of the huge amount of possible alterations operated on it.

In general, the video is a series of images, the forgery can take place on the image level, and Digital image forgery detection techniques are classified into active and passive approaches. In the active approach, the digital image requires pre-processing of an image such as watermark embedding or signature generation, which limits their application in practice, Active techniques such as digital watermarking [3, 4] and digital signature [5, 6], the passive techniques do not need any digital signature to be generated or to embed any watermark [7, 8].

In this research we proposed a new method; this method is designed to be integrated in surveillance cameras system, in order to detect the duplication in live video and offline video stream by using a random watermark (pixel), in specific slice of the images, so we can compare these slice of image series not all of the image to ensure that there are no forged regions in the specific area with an efficient and effective way. The aim of our method is to Protect Private and Sensitive Areas that have important streaming content; these areas should have quality security cameras software to detect image series forgery on the live videos, on an effective and fast way to prevent crime by identifying potential criminal activity and help responsible to respond more quickly to incidents.

Based on our knowledge, this is the first work to explore forgeries like duplication and cloning in video streams and define the places in the given video that have forgery, that means it takes care about demonstrating the integrity of the given video not only demonstrating the authenticity of video stream like the previous research, Current research in forgery detection is mainly limited to

E-mail: tbarhoom@iugaza.edu.ps, arabidmohamed@gmail.com

image tampering detection technique (not video), it can be some sort of cryptographic to produce mathematical scheme for demonstrating the authenticity and integrity of concerned video.

As far as we aware of, this is the first effort that aims to offer detector forgeries system on video streaming, the proposed system is expected to act as a new version of SVR system that can explore different forgeries type on video.

2. RELATED WORKS

Many types of research have been presented to the passive technique they used optical flow and Hog algorithm that already used to detect moving objects to measure the difference luminance between original and forged image, and show that they have perfect accuracy on detecting temporal and spatial forgeries. Moreover, they proposed techniques that need much resources and execution time to be configured, not like our proposed lightweight method that can detect spaitio-tempering forgery on time of capturing video by injecting forged video streams or captured watermarked videos with perfect accuracy and less detecting runtime.

Mathews et al. [9] They proposed a method based on spatial correlation calculation, This method based on discontinuity in the optical flow variation sequence that can be used for detecting forgeries in videos. The limitation of this technique is that it is only effective when the second compression quality is higher than the first compression quality. And computational cost of the algorithm is the drawback.

Wan Wang et al. [10] They calculate the optical flow variation sequence and adopt anomaly detection schema to locate discontinuity points to explore the different type of forgeries. On the other hand they used a small forgery dataset two original videos with 3000 frames, also the optical flow estimation method need some improvement on case the forgery less correlated to normal changes in original videos moreover the frames after forgery were re-encoded with the same coding standard (MPEG-2).

Randeep Kaur et al. [11] they detect the editing digital multimedia content by using some technique like optical flow to detect the flow of the moving objects and the forgery object, to verify the video they used Invariant Feature Transforms (SIFT); It displays the number of key points extracted from input image, to detect the matches' key points consequently the forged part on the image. The major improvement in this work is to detect the forgery part with the help of Key point features and the optical flow algorithm.

Subramanyam et al. [12] They proposed algorithm, for copy-paste forgery detection is based on Histogram of Oriented Gradients (HOG) feature matching and video compression properties . The benefit of using HOG features is that they are robust against various signal processing manipulations, the parameter cell size of the Hog feature generation is set adaptively to reduce the false positive rate and increase the detection accuracy for spatial forgery detection. The frames with high correlation for duplicated regions compared to authentic regions are selected for detection purpose.

3. STREAMING SYSTEM DETECTION

On the first step Watermark embedding algorithm has been applied to the compressed frames captured by the camera, to provide identity to the continues captured frame. after passing these frames into the motion detection algorithm, excel file has been generated to save the position and the value of each watermark embedded in the captured frame to be used in detecting forgeries of the recorded video file.

The proposed digital watermarking method includes three stages: stage one as embedding algorithm as shown on "Fig. 1", second stage as tempering stage, different types of forgeries have been carried out on the videos that captured from stage one, and the third stage detecting algorithm as shown on "Fig. 2".

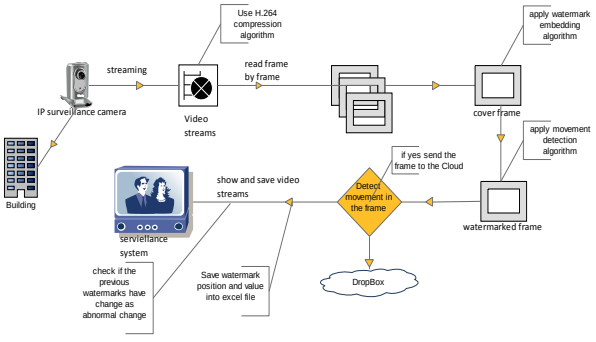

Figure 1. Proposed Streaming System Detection

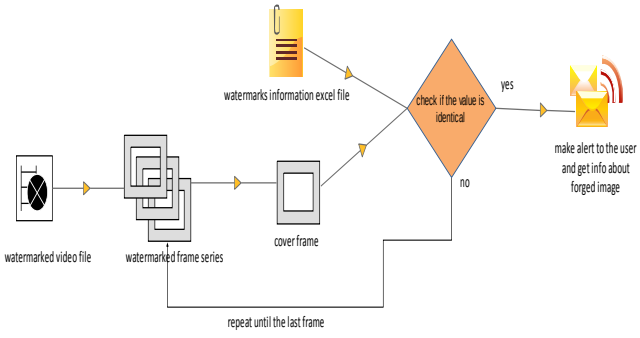

Figure 2. Watermark detection algorithm

A. *Embedding algorithm*

On embedding algorithm the image passes through different steps, in the first step while the streaming capture is open, a loop is used to read frame by frame to insert the watermarks. In the second step, a number of hidden pixels or watermarks are inserted into each frame that reads from the streaming loop, a mathematical equation has been used to assign these pixels to generate the embedded frame. This stage also considers as encryption stage since a predefined watermarks values (public key) inserted into the concerned video. On the end of this stage, values about the original video have been saved as (private key) different to the embedded values to be used later on detection stage.

B. *Distortion/ Tempering Stage:*

There are too many free video editing programs available on the market like (Avidemux 2.7, Movavi Video Editor 14, VideoPad Video Editor, HitFilm express 2017). In our proposal, VideoPad tool has been used in this stage to apply the two types of forgeries temporal cloning duplication forgeries on the produced videos.

On this stage, MOV, AVI, MP4, Lossless compression format have been applied to the origin video that affected by two forged portion of 5440 frames, that means, each forged version have 10880 forged frames.

C. *Detection/ Retrieval Stage:*

Streaming detection system trait temporal cloning duplication forgeries that applied on the previous stage, by checking if there are some regions in the video series have watermarks value different to the saved value and change as abnormal change, depending on the number of different watermarks that change as abnormal change detector streaming system will identify the forged stream.

4. PERFORMANCE EVALUATION AND ASSESSMENT

To evaluate the performance of streaming detection system, experiments have been conducted to detect video forgeries, in the video streaming that captured from IP surveillance camera.

The dataset is a set of three videos recorded using streaming detection system; captured on different places, size, and different forgery places, to measure the accuracy, and to determine the suitable resources needed to run our system.

The following figure fig. 3 shows a frame before and after making temporal forgeries.

Figure 3. Image before and after temporal forgeries

The proposed streaming system detection can detect and find if there is any change occurred on the videos, moreover, define the start and end of the forged part on the concerned videos by comparing the video with the original values of watermarks that spread on the video file.

That means when we applied any format like MP4, AVI and MOV to the origin videos except lossless compression algorithms, consequently, the values of watermarks will be changed from the beginning of the video to the end. Detector streaming system will detect the difference and inform that there are changes occurred to the original video, and define if the video has forgeries like duplication and cloning not only compression changes, moreover, define type and place of forgery on the concerned forged video.

Streaming system detection developed based on the information that there are abnormal changes when affected by Spatio-Temporal Tempering (Frame sequences are altered as well as visual contents of the frames are modified in the same video.) [13, 14], fig. 4 and fig. 5 illustrate the difference between original captured video and the same lossless forged video.

By this analysis main objective of this research has been achieved by determining if there were forgeries carried out, in addition, to determine the place and types of forgeries in the given video.

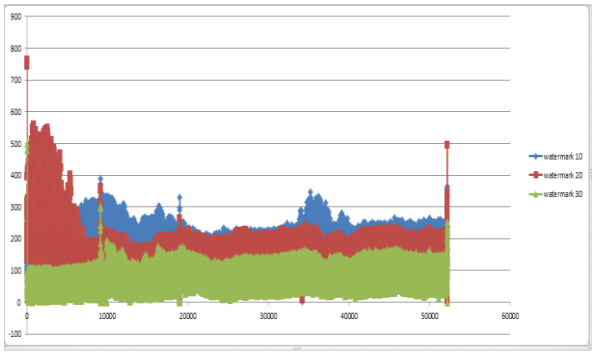

Figure 4. Watermarks 10, 20, 30 for original video.

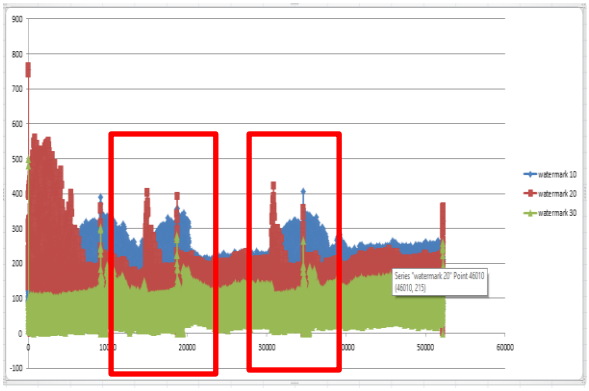

Figure 5. Watermarks 10, 20, 30 for Forged Lossless

The following table tab. 1 depicts the accuracy of one experiment that established on our research using Equ. 1

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Equation 1. Calculate the accuracy of the streaming detection system

TP column show number of frame that consider as not forged and on fact not forged, TN column show number of frames that consider forged and on fact forged, FP column show number of frames that consider forged and on fact not forged, FN column show frame number that consider not forged but on fact forged frames.

TABLE I. DEPICTS VARIOUS VERSIONS OF FORGED VIDEOS THAT HAVE FORGERY EFFECTS AND IT ACCURACY.

Video format	TP	TN	FP	FN	Accuracy
MP4	38726	10011	2334	880	0.938
AVI original	38824	10313	2297	517	0.944
MOV	38776	10318	2297	560	0.945
Lossless	41062	9463	14	1412	0.972

Tab. 1 illustrates in details the result values of using detector streaming system to detect effects forgery. As shown in the table, the accuracy of the detector system is approximately 94% for the different versions and for lossless 97% of accuracy is achieved.

5. CONCLUSION

In this work, we have developed a detector streaming system to make streaming and detecting forgery at the same time, the system can detect some effects that carried out like, if the original video compressed by any of compression methods, make duplication that means when replacing portion of the origin video by another portion from the same video that has a same duration like the replaced portion. Another effect that can be detected by our detector streaming is cloning effect, that means clone yourself on the same video, in other words, make two or more copies of yourself in the concerned video.

Our work proposes a simple encryption-decryption algorithm that can be used on the live streaming or on a recorded video; it is spatially designed to the sensitive videos, accessing the data stream and investigate the original video data, to explore any change on the original video.

REFERENCES

1. Redi, J.A., W. Taktak, and J.-L. Dugelay, Digital image forensics: a booklet for beginners. Multimedia Tools and Applications, 2011. 51(1): p. 133-162.
2. Wang, J., et al., Fast and robust forensics for image region-duplication forgery. Acta Automatica Sinica, 2009. 35(12): p. 1488-1495.
3. Shih, F.Y., Multimedia Security: Watermarking, Steganography, and Forensics. 2017: CRC Press.
4. Khan, A., et al., Intelligent reversible watermarking and authentication: Hiding depth map information for 3D cameras. Information Sciences, 2012. 216: p. 155-175.
5. Tzeng, C.-H. and W.-H. Tsai. A new technique for authentication of image/video for multimedia applications. in Proceedings of the 2001 workshop on Multimedia and security: new challenges. 2001. ACM.
6. Lu, C.-S. and H.-Y. Liao, Structural digital signature for image authentication: an incidental distortion resistant scheme. IEEE transactions on multimedia, 2003. 5(2): p. 161-173.
7. Qazi, T., et al., Survey on blind image forgery detection. IET Image Processing, 2013. 7(7): p. 660-670.
8. Asghar, K., Z. Habib, and M. Hussain, Copy-move and splicing image forgery detection and localization techniques: a review. Australian Journal of Forensic Sciences, 2017. 49(3): p. 281-307.
9. Mathews, M.R. and S. Sreedharan, Detection and Localization of Video Copy-Move Forgery in Temporal and Spatial Domain. 1 June 2015 Volume-5 Issue-1
10. Wang, W., et al. Identifying video forgery process using optical flow. in International Workshop on Digital Watermarking. 2013. Springer.
11. Randeep Kaur, E.J.K., Video Forgery detection using Hybrid techniques. International Journal of Advanced Research in Computer and Communication Engineering December 2016 5(12).
12. Subramanyam, A. and S. Emmanuel. Video forgery detection using HOG features and compression properties. in Multimedia Signal Processing (MMSP), 2012 IEEE 14th International Workshop on. 2012. IEEE.
13. Yin, P. and H.H. Yu. Classification of video tampering methods and countermeasures using digital watermarking. in Multimedia Systems and Applications IV. 2001. International Society for Optics and Photonics.
14. Upadhyay, S. and S.K. Singh, Video authentication: Issues and challenges. International Journal of Computer Science, 2012. 9(2012).

Tawfiq S. Barhoom, Associated Prof. of Computer Science, Computer Science Department, Faculty of IT, Islamic University-Gaza, he got B.Sc. Computer Science from Omdurman Ahlia UniversitySudan,(1991-1995) and Master degree, and he has – M.Sc. Computer science, Department of computer science and engineering from Shang hai Jiao Tong University (SJTU)– ShangHai – China, (1996- 1999) and his has – PhD in Applied computer Technologies, Department of computer science and engineering from ShangHai Jiao(2004).

Mohammed K.S. Arabid, Senior web developer, Information Technology Department, Ministry of Foreign Affairs, he got B.Sc. Computer science from Tunis Al Manar Univirsity (2009), and he has M.Sc. Information Technology from Islamic univesity of Gaza (2018).