International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Design and Implementation of Forensic Framework for Video Forensics

Ashish Kumar Kushwaha† and Avinash P. Wadhe‡

†Department of Computer Science & Engineering, SGBAU, India
‡Department of PG Studies (Computer Science & Engineering), SGBAU, India

Accepted 02 April 2015, Available online 07 April 2015, **Vol.5, No.2 (April 2015)**

Abstract

With rapidly growing technology, Video became most important weapon in the fight to against people who break the law by capturing them red handed. Evidence captured on video is considered to be more reliable, more accurate and more convincing than eyewitness testimony alone. But due to growth in multimedia editing software Digital Photographs and videos can be no longer considered proof of evidence. Evidence can be easily tempered using software. So we propose a new forensic framework, ***Forensic framework for Video Forgeries*** *capable of video Steganalysis and detection of tampering in digital video without any specialized hardware. Framework can be used for the forensic of videos using enhanced forensic techniques and also used to detect any hidden data in the video. The objective of the framework is to provide the easy and handy Video Forensic Framework to forensic community for validation of evidence before presenting it to court for law enforcement.*

Keywords: *Video Forensics, Video Steganalysis, Forensics Framework.*

1. Introduction

Due to availability of low-cost digital and sophisticated video cameras and the availability of video sharing websites such as YouTube, digital videos become most important part in Day to day life. Since videos can be easily manipulated using Available tools, their authenticity cannot be taken for granted. Tampering a digital video not an easy task, it is challenging and time consuming task as compare to still image, but video editing software can be a easy way to manipulate video. Of course not every video forgery is equally consequential; the tampering with footage of a popstar may matter less than the alteration of footage of a crime in progress. But the alterability of video undermines our common sense assumptions about its accuracy and reliability as a representation of reality. As digital video editing techniques become more and more sophisticated, it is ever more necessary to develop tools for detecting video forgery.

1.1 Video Forgeries

The movie industry is probably the strongest driving force for improvement of video manipulation technology. With the video editing technology currently available, professionals can easily remove an object from a video sequence, insert an object from a different video source, or even insert an object created by computer graphics software. Certainly, advanced video manipulation technology greatly enriches our visual experience. However, as these techniques become increasingly available to the general public, malicious tampering. Although tampering with video is relatively hard, in recent years we have begun to encounter video forgeries. Growth in video tampering is creating a huge impact on our society. Although currently only a few digital video forgeries have been exposed, such instances are eroding the public trust in video. Therefore, it is urgent for the scientic community to come up with methods for authenticating video recordings.

1.2 Watermarking

One solution to video authentication is digital watermarking. There are several types of watermark. Among them, fragile and semi-fragile watermarks can be used to authenticate videos. Fragile watermarking works by inserting imperceptible information that will be altered if there is any attempt to modify the video. Later, the embedded information can be extracted to verify the authenticity of the video. The semi-fragile watermark works in a similar fashion. The difference is that it is less sensitive to classical user modifications such as compression. The assumption is that these modifications do not affect integrity of the video. The

*Corresponding **author Ashish Kumar Kushwaha** is a PG Student and **Avinash P. Wadhe** is working as Assistant Professor

major drawback of the watermarking approach is that a watermark must be inserted at precisely the time of recording.

1.3 Forensic framework for Video Forgeries

Forensic framework is designed in to detect digital forgeries without help of watermarking (Digital authentication), the fundamental assumption behind our techniques is that tampering with a digital video may disturb certain underlying properties of the video and these perturbations can be modelled and estimated in order to detect tampering. we can divide framework in 3 module

- Video Analysis
- Video Forensics
- Video Steganalysis.

Video Analysis

In this module we are propose techniques for enchaining video analysis. In this module we propose new advance approaches like

Video Stabilization:

Removes shaky motion from the video sequence to produce stabilized videos. This is used to focus the target in the video easy without any disturbance. This is a important video enhancement technique for video Analysis

Video Display with Live Histogram

This technique displays the live histogram of video sequence. A **histogram** is a visual way to display frequency data using bars. A feature of histograms is that they show the frequency of continuous data. Histogram block computes the frequency distribution of the elements in each frame by sorting the elements into a specified number of discrete bins.

Scene Change Detection: This technique detect the major change in video sequence with any frame is added or deleted from the video, and then this technique will identify it.

Face Detection: This technique automatically detect the face of the suspect in the video sequence and mark face by square box. Face detection and tracking are important in many applications including activity recognition, automotive safety, and surveillance.

Video Forensic

De-interlaced. Sometimes, interlaced videos are de-interlaced to minimize combing artifacts. The de-interlacing procedure introduces correlations among the pixels within a frame and between frames. Tampering, however, is likely to destroy these correlations

Frame Duplication Detection Techniques for detecting image duplication have previously been proposed. These techniques, however, are computationally too inefficient to be applicable to a video sequence of even modest length. Therefore, we propose new method for detecting video duplications.

Double MPEG: When an MPEG video is modified, and re-saved in MPEG format, it is subject to double compression. In this process, two types of artifacts – spatial and/or temporal will likely be introduced into the resulting video. These artifacts can be quantified and used as evidence of tampering.

Re-projection A simple and popular way to create a bootleg video is to simply record a movie from the theatre screen. Such a re-projected video usually introduces distortion into the intrinsic camera parameters; the distortion to camera skew in particular is evidence of tampering.

Frame Forensic Technique is used to perform various forensic techniques on selected frame of video.

Video Steganalysis

Steganalysis is the study of detecting messages hidden using steganography, this is analogous to cryptanalysis applied to cryptography. In video Steganalysis, for determination video is stegged (Contain hidden data) or not there are several step are as follows

In first step, Raw video is converted into a MPEG Format, (Video should not be re-compressed for better result)

After that in next step of steganalysis extracts the data from stegged fiel and create the feature for statistical classifier.

This ensemble classifier then classify whether frames a stegged in video sequence, if most of frames are stegged then entire video is said to stegged

Video steganalysis there are 3 steps

- Feature Sets Description
- Frame Classification
- Video Classification

Each technique focuses on one specific form of tampering and cannot be applied singlehandedly to detect all video forgeries. Using these modules in combination, provide promising beginning to detecting forgery in digital videos without watermarks.

2. Literature Survey

Bestagini *et al.* proposed that Video codec identification is an important task while proving the

authenticity of video content. Video sequences are usually available in compressed format since the very acquisition. Therefore, being able to detect the adopted coding architecture reveals information about both the possible presence of alterations, and video origin. The author presents two detectors that permit to identify the adopted coding architecture for a given video sequence. The first detector extend the robustness of the idempotent detector permitting an effective detection. The second detector extends the possibilities of the idempotent detector by permitting the identification of coding schemes that are not known by the analyst. Michael Tok, Marko Esche *et al.* explains the parametric merge candidate for high efficiency video coding. He present a novel Merge candidate for improving already existing vector prediction techniques based on higher order motion. Simone Milani, Marco Fontani *et al.* proposed an overview paper on different video forensics techniques. In this paper he explains that, it is possible to divide video forensic techniques into three macro-areas concerning the acquisition, the compression, and the editing of the video signals. Ghulam Qadir *et al.* explained SULFA (Surrey University Library for Forensic Analysis) for the bench-marking of video forensic techniques. This new video library has been designed and built for the purpose of video forensics specifically related to camera identification and integrity verification.

Weihong Wang, Hany Farid gave a method detecting re-projected video for finding tampering in digital video. He explains projection of video from planer and non planer surface. Some authors proposed their work for detecting double quantization for detecting digital forgery. Some proposed duplication technique is described. The authors explains two ways of duplication i.e. frame and region duplication. And some proposed their work for techniques for detecting double MPEG compression in digital video. In digital video, the static and temporal parameters are used to detect tampering.

For video steganalysis, an early but comprehensive treatment is from Budhi. This work looked at detecting data embedded using additive white Gaussian noise in the spatial domain. By using data from surrounding frames, which they call *collusion*, an estimation of the current frame is achieved. Several different collusion approaches are tried, including simple linear averaging, weighted averaging and block based reconstruction of reference frames. Block based reconstruction searches for similar blocks in nearby frames and copies them into a new reference frame. The difference of this reference frame and the original is then used to estimate the embedded data. Their features use statistics such as kurtosis, entropy, and 25^{th} percentile over this estimation. They mention that their technique can apply to the DCT domain and test it using two different methods of embedding, though without considering the encoding process (for example, P/B frames).

A performance enhancement is proposed by Jainsky in *MoViSteg* which also uses motion estimation to reconstruct a frame. They employ an asymptotic relative efficiency based detector, which is efficient for large samples and weak signals. The detector uses an adaptive threshold that is based on statistics from sample frames in the video. While they do not give overall accuracy, they report at 60% true positive to 10% false positive rate at 75 dB Peak Signal-to-Noise-Ratio (PSNR). Most recently B. and F. Liu use collusion with a window of frames limited by a predetermined correlation threshold. They use a simple linear collusion that averages the surrounding frames. While they obtain good results (from 88–100% at 40% embedding, depending on the embedding scheme), the watermarking techniques they test against make very distinctive changes in the DCT values used. Two of them increase the range of values, which will show up in the global histogram. Another simply removes several DCT values in select blocks, which would cause noise in the dual histogram.

3. Description of the Proposed Work

The video stabilization technique is used works without any previous knowledge it automatically detect the background plane in the video sequence and uses its observed distortion to correct for camera motion. The algorithm used for stabilization is divided into two steps

1. Determine the affine image transformation between all neighbouring frames of video using estimate Geometric Transformation function. This function is applied to point correspondence between two frames.
2. Wrap the video frames to achieve a stabilized video

For this we will used the Computer vision System toolbox.

The scene change detection technique is divided into two parts

1. For making the algorithm sensitive to small changes, algorithm finds the edges from the two consecutive video frames.
2. From identified edges, the section of one video frame is compared with another using the Block Processing Block. If the number of different sections exceeds a specified threshold, the example determines that the scene has changed

The face detection process start with detection of object in our case we are detecting face(we can also configure the technique to detect other object like nose eyes etc).The face detection is done using the vision.CascadeObjectDetector in matlab. The cascade object detector uses the Viola-Jones detection algorithm and a trained classification model for detection.

The Frame duplication detection start with calculation of histogram value of first frame in video

sequence, then correlation coefficient is calculate between the calculated histogram value and histogram value of all other remaining frame in the video sequence, this process done for all the frame in the video sequence. After this we compare correlation coefficient this threshold value if this value is greater than threshold this frame is considered to be duplicate.

De-interlacing Interlace videos is a combination of the top and bottom fields in of video sequence. The de-Interlacing of such video is done using line repetition, linear interpolation, or vertical temporal median filtering.

In forensic framework for Video Forgeries have proposed an anti-forensic operation capable of removing the temporal fingerprint that arises in MPEG video sequences when frames are added or deleted followed by recompression. We have identified properties of the temporal fingerprint and used these to model the effect of frame deletion or addition on the P-frame prediction error sequence. Our proposed anti-forensic technique operates by selectively increasing the prediction error in certain P-frames of the video so that the P-frame prediction error sequence approximates a target prediction error sequence obtained using our model. The prediction error in each P-frame is increased by setting the motion vectors of certain macroblocks within that frame to zero, then recalculating the prediction error for the frame. Experimental results demonstrate that our proposed anti-forensic technique is capable of removing the temporal fingerprint from MPEG videos that have undergone frame deletion or addition.

Conclusion

In the Field of video forensic, there is very little works is done till date therefore Video forensic is hot research topic nowadays. Although there are many tool are available for video forensic for video tampering detection but most of them have very few and basic functionality and none of them are able to perform steganalysis operation on video. So propose Video Forensic Frame work will be a better forensic framework for Forensic community with enhances techniques for Video Forensic. This framework will be able to detect any tempering in video including detection of hidden data in video sequence. Video Forensic framework will also provide a better presentation of evidence for law enforcement. Video Forensic framework will be most reliable and handy framework for video forensic.

References

P. Bestagini, S. Milani, M. Tagliasacchi, S. Tubaro (2013), Video Codec Identification Extending The Idempotency Property in ISBN: 978-82-93269-13 University of Paris

Michael Tok, Marko Esche, Alexander Glantz, Andreas Krutz, and Thomas Sikora (2013), A Parametric Merge Candidate for High Efficiency Video Coding in 2013 Data Compression Conference.

Simone Milani, Marco Fontani, Paolo Bestagini, Mauro Barni, Alessandro Piva, Marco Tagliasacchi and Stefano Tubaro (2012). An overview on video forensics. APSIPA Transactions on Signal and Information Processing,1, e2 doi:10.1017/ ATSIP.2012

Ghulam Qadir, Syamsul Yahaya, Anthony TS Ho (2011), Surrey University Library for Forensic Analysis (SULFA) of Video Content

Weihong Wang, Hany Farid Detecting Re-Projected Video

Weihong Wang, Hany Farid (2009) Exposing Digital Forgeries in Video by Detecting Double Quantization, MM&Sec'09, September 7–8, 2009, Princeton NJ, USA. Copyright 2009 ACM 978-1-59593-857-2/07/00

Weihong Wang, Hany Farid (September 20–21, 2007) Exposing Digital Forgeries in Video by Detecting Duplication in ACM MM&Sec'07, , Dallas, Texas, USA

Weihong Wang, Hany Farid (2006), Exposing Digital Forgeries in Video by Detecting Double MPEG Compression in ACM MM&Sec'06, September 26–27, Geneva, Switzerland.

U. Budhia and D. Kundur (2004), Digital video steganalysis exploiting collusion sensitivity, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense III, vol. 5403, pp. 210—-221

J. S. Jainsky, D. Kundur, and D. R. Halverson (2007), Towards digital video steganalysis using asymptotic memoryless detection, Proceedings of the 9th workshop on Multimedia & security - MM&Sec '07, p. 161.

B. Liu, F. Liu, and P. Wang (2008), Inter-frame Correlation Based Compressed Video Steganalysis, 2008 Congress on Image and Signal Processing, pp. 42– 4

P. Bestagini, M. Fontani, S. Milani, M. Barni (2012), An Overview on Video Forensics 20th European Signal Processing Conference (EUSIPCO 2012)

Weihong Wang (June, 2009), Digital Video Forensics

Kevin Bryan (2013) , Video Steganalysis for Digital Forensics Investigation Open Access Dissertations. Paper 48.

Matthew C. Stamm and K. J. Ray Liu , Anti-Forensics For Frame Deletion/Addition In Mpeg Video

M. C. Stamm, S. K. Tjoa, W. S. Lin, and K. J. R. Liu (Mar. 2010), Anti-forensics of JPEG compression, in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process., pp. 1694 – 1697.

Prof. Avinash P. Wadhe: Received the B.E from SGBAU Amravati University and M-Tech (CSE) From G.H Raisoni College of Engineering, Nagpur (an Autonomous Institute). He is currently an Assistant Professor with the G.H Raisoni College of Engineering and Management, Amravati SGBAU Amravati University. His research interest include Digital Forensics, Network Security, Data mining and Cloud Computing .He has contributed to more than 20 research paper. He had awarded with young investigator award in international conference.

Ashish Kumar Kushwaha: Received the B.E from RTMNU Nagpur University and pursuing ME (CSE) From G.H Raisoni College of Engineering and Management, Amravati. His research interest include Digital Forensics, Neural network, Data mining and Cloud Computing.