# Video Anti Forensic - A Review

Monika Ramesh Chourasiya
*Computer Science and Engineering*
*G.H. Raisoni College of Engineering and Management*
*Amravati,Maharashtra,India*
*e-mail:monika.rs.chourasiya@gmail.com*

*Asst. Prof. Avinash P.Wadhe*
*Computer Science and Engineering*
*G.H. Raisoni College of Engineering and Management*
*Amravati,Maharashtra,India*
*e-mail: aviwadhe@gmail.com*

***Abstract-*** In the recent years the availability of the digital multimedia devices (such as cameras, mobile-phones, digital recorders, etc.) has increased rapidly. Digital photos have been widely used as historical records and as evidences of real happenings in applications from journalist reporting, police investigation, law enforcement, insurance, medical and dental examination, military, and museum to consumer photography. Forensic investigation endeavors to use science to uncover the transferred evidence and discern its meaning. The examination requires that the evidence be reliable and accurate to ensure a correct outcome. However, criminals may use anti-forensic methods to work against the process or interfere with the evidence itself. In this paper different techniques of anti-forensic are explained. Each of these proposed techniques accounts for distinct actions that compromise the availability or usefulness of evidence to the forensic process.

***Keywords:*** *Digital Forensics, Anti Forensics, Categories of Video Anti Forensics.*

*****

## I. INTRODUCTION

Digital cameras are widely used today all over the world. Several factors, such as the integration of digital video cameras into cell phones and laptops, as well as the increasing affordability of high quality digital video cameras, have caused digital video content to become pervasive throughout society[8].Digital video is commonly used by news organizations for reporting purposes, as well as evidence of specific events by law enforcement, legal institutions, and governmental organizations.

As multimedia is the new era of the current generation. Multimedia belongs to digital images, video, audios, documents and etc. most of the things came in digital form as it's easily accessible. Digital multimedia forensics involves the study and development of techniques to determine the authenticity,

processing history, and origin of digital multimedia content without relying on any information aside from the digital content itself. The broad availability of tools for the acquisition and processing of multimedia signals has recently led to the concern that images and videos cannot be considered a trustworthy evidence, since they can be altered rather easily. Sometimes the all information is protected and authenticated and sometimes they are not. When the things were not authenticated there raise a term for tampering. Reliance on digital video for applications in which its authenticity is critical is complicated by the fact that digital video can easily be manipulated using editing software. . To cope with these issues, signal processing experts have been investigating effective video forensic strategies aimed at reconstructing the processing history of the video data under investigation and validating their origins. To prevent digital forgers from gaining an upper hand, the digital forensics community must develop and study anti-forensic operations.

However, as digital editing is developing rapidly, verifying the authenticity and integrity of digital videos is facing challenges in digital forensics. Forensic analysts must now face the problem of anti-forensic techniques, which consist in modifying the forging process in order to make the unauthorized alterations transparent to forgery detection algorithms. Though many existing forensic techniques are capable of detecting a variety of standard image manipulations, they do not account for the possibility that -forensic operations may be designed and used to hide image manipulation fingerprints. To protect against this scenario, it is crucial for researchers to develop and study anti-forensic operations so that vulnerabilities in existing forensic techniques may be known. An intelligent forger can design anti-forensic anti operations to hide editing fingerprints and fool forensic techniques. Anti-forensic techniques are actions which goal is to prevent proper forensic investigation process or make it much harder. These actions are aimed at reducing quantity and quality of digital evidence. Anti-forensics aims to make investigations on digital media more difficult and therefore, more expensive. In this paper different anti forensic techniques are explained along with their prevention measures.

## II. LITERATURE SURVEY

Sowmya K.N , H.R. Chennamma[1]proposed that digital video forensics is still in its infant stage .Due to tampering reliability of the digital video is under threat.

A set of anti forensic techniques has been proposed to erase or falsify a video's compression. Proposed techniques derive new methods which can hide the frame deletion fingerprints and can

make frame deletion undetectable. As digital editing operation techniques leaves behind fingerprints anti forensics operations may also leaves behind their own fingerprints.

Shweta P. Kachhawal,Prof. Avinash P. Wadhe[2] described a technique for detecting double quantization in digital video that results from double MPEG compression or from combining two videos of different qualities.

Jingxian Liu, XianguiKang[9] proposed that to detect the use of frame deletion anti forensics technique a countering anti forensics method has been proposed. After a countering anti forensics method has been proposed an improved anti forensics technique is designed to fool the frame deletion technique. Thus, the experimental results shows that the proposed countering anti forensic method which improves the anti forensics techniques and can make the frame successfully undetectable and can effectively detect the use of anti forensics techniques.

Harshal S. Bhagwat, Prof. Avinash P. Wadhe[3], This paper describe and taken a critical review on the reliability of various forensic techniques that are very useful for investigator i.e outcomes of a image forensic analysis that means evidence may serve as probative facts in court.

## III. ANTI FORENSICS

Digital videos have found great use in journalism; criminal investigation and surveillance. Many video forensic techniques have been proposed to verify the authenticity of digital videos as the digital videos can be easily altered but several anti-forensic techniques are developed to make the manipulations undetectable. To increase the authenticity of the videos several techniques have been developed such as video frame deletion which increases the prediction errors to make the forgery of frame deletion undetectable.

Anti-forensics is defined as methods used to prevent (or act against) the application of science to those criminal and civil laws that are enforced by police agencies in a criminal justice system. Anti-forensics makes investigations on digital media. The study of anti-forensic operations may also lead to the development of techniques capable of detecting when an anti-forensic operation has been used. Anti forensic is capable of fooling forensic techniques. Anti-forensic operations designed to hide fingerprints of image manipulation may be applied to an image. It lead to the identification of fingerprints left by anti-forensic operations and the development of techniques capable of detecting when an anti-forensic operation has been used to hide evidence forgery. As anti forensics developers continue to produce tools, however, it becomes incumbent upon academia and industry to coordinate and fund anti-Anti forensics research and development.

Anti-forensics tools and methods will continue to provide difficulties and challenges to the digital investigation and e-discovery communities .It is important to note that while many of the anti forensics methods might make information derived from an investigation useless as evidence in court, they may not diminish the intelligence value of the information; reasonable doubt in the mind of a jury does not translate into non-actionable information for an intelligence gatherer.

## IV. TECHNIQUES OF VIDEO ANTI FORENSICS

Just as there are varying definitions of anti-forensics, several groupings of anti-forensic methods have been proposed. Anti-forensic techniques are developed to make the manipulations undetectable. Several anti-forensic techniques are designed to mislead forensic analysis by concealing or removing fingerprints left by tampering operations. Frame deletion may be performed by a video forger who wishes to remove certain portions of a video sequence .In the same way; a forger may wish to falsify an event by inserting a sequence of new frames into a video segment. Various new techniques have been proposed such as new video frame deletion or addition forensic and anti-forensic techniques along with a new framework for evaluating the interplay between a forger and forensic investigator.

### *A. Frame Deletion Fingerprints:-*

Frame deletion fingerprints starts with the video compression. Due to the uncompressed digital video files size, virtually all digital video undergoes compression during the process of storage or transmission. All the frames are not predicted in order to prevent the propagation of channel and decoding errors. The video sequence is segmented into sets of frames known as ‘groups of pictures’ (GOPs**).** These frame types are known as: intra-frames (I-frames), predicted-frames (P-frames), and bidirectional-frames (B –frames)[4].According to the manner in which they are predicted and compressed, within each GOP, frames are assigned one of three types. Each GOP begins with an I-frame. The remainder of each GOP consists of P-frames and B-frames .P-frame motion estimation is performed by first segmenting the frame into 16 × 16 pixel macro blocks in MPEG-1 and 2.The sequence of I-, P-, and B-frames always occurs in the same pattern in MPEG-1, MPEG-2, and similar codecs, i.e the structure of each GOP is fixed. The GOP structures are allowed to be adjusted depending on the amount of motion in the scene in the newer video compression standards such as MPEG-4 and H.264. The simple example of this is, rapidly changing scenes can be encoded using shorter GOPs because the accuracy of motion compensation greatly decreases as new objects enter each frame.

### B. *Detection of Frame Deletion or Addition*

In many cases, frames are added or deleted from the digital video sequence. For doing this the forger must decompress the video before frames are added or deleted, and then recompress the video after it has been altered. Each GOP in the recompressed video will contain frames that belonged to different GOPs during the initial compression, when frames are deleted from or added to a digital video[7]. When a P-frame is predicted from an anchor frame that initially belonged to a different GOP, an increase in the total prediction error is observed [7]. This effect can be seen in Fig.51, which shows an example of frame deletion for a video compressed using a fixed GOP sequence.

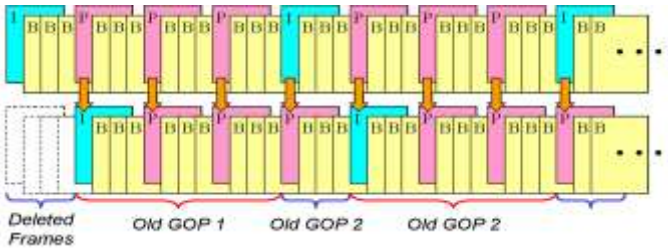


**Fig. 5.1** Illustration of the effects of frame deletion on a video frame sequence. The original video sequence is shown along the top of this figure and the altered video sequence is shown along the bottom. Each GOP in the altered video contains frames from two different GOPs in the unaltered video sequence.[4]

As it requires human inspection of the P frame prediction error sequence or it's DF, there are certain several shortcomings while this frame addition or deletion detection technique takes place., It can only be used on videos that are compressed by a codec with a fixed GOP pattern, because this detector relies on identifying periodic increases within the P-frame prediction error sequence. If their implementations adaptively change the GOP length so it cannot be used on videos compressed using more recently developed encoders such as MPEG-4 or H.264[4].This is because the increase in the P-frame prediction error will not occur periodically unless a fixed GOP pattern is used.

### C. *Temporal Fingerprint Model:-*

A model of the effect of frame deletion or addition followed by recompression on a video's P-frame prediction error sequence has been proposed, in order to design an automatic frame deletion or addition detection technique as well as an anti-forensic method to remove frame addition and deletion fingerprints. Let the P-frame prediction error sequence of an unaltered video that has been compressed oncee1(n) and the prediction error sequence of that same video after nD frames have been deleted followed by recompression is denoted by e2(n). The relationship between the altered and unaltered videos' P-frame prediction error sequences using the equation,

$$e2(n) = e1(n - nD)(1 + s(n)). \quad (5.2)$$

In this equation, the signal s (n) denotes the temporal fingerprint caused by frame deletion [5].Based on whether the video codec used to perform compression employed a fixed length GOP or an adaptively changing one there are two different models of the temporal fingerprint.

#### 1. *Model for Fixed Length GOPs:-*

During the initial compression relative to the locations of the GOPs used during recompression, frame deletion causes a constant shift in the position of each GOP which gives rise to the temporal fingerprint's periodicity. As a result, each new GOP will contain frames from exactly two GOPs present during the initial application of compression in a repetitive fashion.

#### 2. *Model for Variable Length GOPs:-*

Based on the amount of motion in a scene newer video compression standards such as MPEG-4 or H.264 allow the GOP length to vary. When frames are deleted from a video then recompressed using one of these codecs, GOPs in the recompressed video will be comprised of frames belonging to multiple different GOPs used during the first compression, but this will not occur in a repeating pattern, Some new GOPs may contain frames from more than two GOPs used during the original compression, while others will contain frames from only one. Nonetheless, frame deletion will alter the GOP which each frame belongs to, but in a random fashion rather than a fixed one. As a result, spikes in the P-frame prediction error sequence occur in a random fashion[5].

### D. *Frame Deletion Anti-Forensics*

Frame deletion fingerprints are deleted from the videos P-Frame prediction error sequence, when a sequence of frame from a digital video is deleted undetectably. Frame deletion fingerprints are not present in the P-Frame prediction error sequence stored in video. This is done by modifying the process of motion estimation. The procedure is as follows:-

At the first P-Frame error sequence which is free from frame deletion fingerprint is constructed. The motion vectors of some macro blocks are selectively set to zero. The prediction error associated with these macro blocks is recalculated in order to match the P-Frame prediction with the target error. The total prediction errors for some frames are increased by choosing motions vectors that yield poor predicted frames. The set of

motion vectors that maximizes the prediction error associated with each macro block are searched if the target prediction error of a particular P-Frame is greater than the error incurred during setting the entire frames motion vector to zero.

### *E. Detecting The Use Of Frame Deletion Anti-Forensics:-*

Anti-Forensics operations may leave behind new fingerprints of their own. This can be proved for the case of the deletion and addition anti-forensics. For removing the frame deletion fingerprints from the P-Frame prediction sequence of a video, in order to increase the prediction error that video motion vector must be altered. The true motion present in the video does not change despite if this. Therefore, there is a discrepancy between many of the motion vectors stored in an anti-forensically modified video and the true motion of that video scene. This is done only for the altered video. In order to minimize each frame's prediction error, normal video encoder will attempt to estimate scene motion as accurately as possible in the case of an unaltered video.

These discrepancies between a video's stored motion vectors and the actual motion of the scene are fingerprints left by frame deletion anti-forensics .For detection of the use of frame deletion anti forensics, there is a comparison between the compressed video's P-frame motion vectors to an estimate of the true motion present in the video scene.

### *F. Detecting Frame Deletion:-*

There are two automatic frame deletion or addition detection techniques used to address the weakness in Wang and Farid detection technique. The two techniques exploits the periodic nature of frame deletion fingerprints for fixed GOP length encodes while the another one is suitable for use on videos compressed using variable GOP lengths.

The detector can assume the knowledge of the fingerprint's period, because the number of P frames in one GOP can be determined from the encoded video. The phase is unknown to the detector since it depends on information like the number of frames deleted and the point in the video sequence at which frame deletion occurs, that is hidden from forensics investigator. Therefore, fingerprint detection is well suited for the frequency domain, where the presence of periodic signal can be readily determined without requiring information about its phase.

### *V. Remedial Actions Against Anti forensics Frame Deletion Detection:-*

In order to create data suitable a set of 36 standard video test sequences in the QCIF format (i.e. a frame size of 176 × 144 pixels) are compiled. Initially, a database of forged videos is created to test the forensics effectiveness of our proposed frame deletion detection. To do this, from the beginning of each unaltered video sequence 3, 6 and 9 frames are deleted. After the deletion of these frames they are compressed using a fixed length GOP and then recompressed each video. This corresponded to removing ¼, ½ and ¾ of a GOP respectively. For testing against the frame addition, 6 frames are added to the beginning of each unaltered video sequence compressed with a fixed length GOP then recompressed these videos. Additionally, 6 frames are deleted from the videos compressed using random varying GOP lengths. To determine whether the frame deletion or addition had occurred in each video, proposed technique is used in conjunction with a series of different decision thresholds.

## *V. Conclusion*

Thus, this paper gives the different anti forensics techniques which makes manipulations undetectable. Frame deletion fingerprints starts with the video compression. The GOP structures are allowed to be adjusted depending on the amount of motion in the scene in the newer video compression standards such as MPEG-4 and H.264. In detection of frame deletion and addition technique, forger must decompress the video before frames are added or deleted, and then recompress the video after it has been altered. Another anti forensic technique is the temporal fingerprint model in which there are two models i.e Model for Fixed Length GOPs and Model for Variable Length GOPs. Frame Deletion Anti-Forensics is the technique where frame deletion fingerprints are deleted from the videos P-Frame prediction error sequence, when a sequence of frame from a digital video is deleted undetectably. Detecting the use of frame deletion anti- forensics the another anti forensic technique. Anti-Forensics operations may leave behind new fingerprints of their own. This can be proved for the case of the deletion and addition anti-forensics. For removing the frame deletion fingerprints from the P-Frame prediction sequence of a video, in order to increase the prediction error that video motion vector must be altered. Action to prevent anti forensic technique is also discussed for the frame deletion detection. Thus, different anti forensic techniques are explained in this paper along with their prevention measures.

## *References*

[1] Sowmya K.N, H.R. Chennamma, "A Survey on Video Forgery Detection" International Journal of Computer Engineering and Applications, Volume IX, Issue II, February www.ijcea.com ISSN 2321-3469, 2015

[2] Shweta P. Kachhawal,Prof. Avinash P. Wadhe, "Study Of Different Video Forensics Techniques" IEEE Sponsored International Conference On Empowering Emerging Trends In Computer, Information Technology & Bioinformatics International Journal of Computer, Information Technology &

Bioinformatics (IJCITB) ISSN: 2278-7593, Volume-2, Issue-2, 2014.

[3] Harshal S. Bhagwat, Prof. Avinash P. Wadhe, "Review On Techniques Of Digital Image Forensics" IEEE Sponsored International Conference On Empowering Emerging Trends In Computer, Information Technology & Bioinformatics International Journal of Computer, Information Technology & Bioinformatics (IJCITB) ISSN: 2278-7593, Volume-2, Issue-2, 2014.

[4] Matthew C. Stamm , "Digital multimedia forensics and anti forensics'',2012

[5] Matthew C. Stamm, W. Sabrina Lin, K. J. Ray Liu, "Temporal Forensics and Anti-Forensics for Motion Compensated Video", Ieee Transactions On Information Forensics And Security, Vol. 7, No. 4, August 2012

[6] Simone Milani, Marco Fontani, Paolo Bestagini, Mauro Barni, Alessandro Piva, Marco Tagliasacchi and Stefano Tubaro, "An overview on video forensics", APSIPA Transactions on Signal and Information Processing , Volume 1 , August 2012

[7] W. Wang and H. Farid, "Exposing digital forgeries in video by detecting double MPEG compression", In Proc. ACM Multimedia and Security Workshop, pages 37–47, Geneva, Switzerland, 2006.

[8] Matthew C. Stamm and K. J. Ray Liu, "Anti-Forensics For Frame Deletion/Addition In Mpeg Video", Dept. of Electrical and Computer Engineering, University of Maryland, College Park.

[9] Jingxian Liu, Xiangui Kang**,** "Anti-Forensics of Video Frame Deletion"**,** Science and Technology, Sun Yat-Sen University, Guang-zhou 510006.

*Author's Profile*

Miss. Monika R. Chourasiya has completed her B.E from SGBAU Amravati University and she is presently pursuing her Master of Engineering (CSE) from G.H. Raisoni College of Engineering and Management, Amravati SGBAU. Her research interest is Digital Forensics.

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.