Digital Video Tampering Detection Techniques

C

Ramesh ChandPandey
Department of Computer Engineering, Indian Institute of Technology (BHU), India

Sanjay Kumar Singh
Department of Computer Engineering, Indian Institute of Technology (BHU), India

K.K. Shukla
Department of Computer Engineering, Indian Institute of Technology (BHU), India

INTRODUCTION

We can define video many ways, Time varying image is known as video or Changing of Image in temporal domain is known as video or Transformation of 4 D(X,Y,Z,T) physical object in 3 D(X,Y,T) is known as video.(T-temporal domain, (X,Y,Z)- Spatial Domain). An image is defined by spatial coordinates(X,Y)and its intensity function F(X,Y). When (X,Y) and intensity value is discrete at every point in image plain then we call image digital image(Gonzalez & Woods,2002). Due to high availability of low cost s/w editing tools, it is very easy to tamper the digital video. Some modification in video does not lead to malicious tampering in video for example modification in video to increase quality of video. Illegal, improper and malicious intension for modifying video to conceal some important information, event or object is known as video tampering. According to video we can divide video tampering detection techniques in two categories: first one is active video tampering detection techniques and second one is passive video tampering detection techniques. In active video tampering detection techniques we use the concept of digital Signature and digital watermark or combination of both. But in passive video tampering detection techniques we do not have any information regarding digital signature and digital watermark. If we have no information of camera from which video was taken then we call it blind video. The techniques used to detect tampering in blind and passive video is known as blind and passive video tampering detection techniques. Video tampering and tampering detection both are tough in comparison to image tampering and tampering detection. People follow the concept seeing is believing but video tampering has disproven this concept. Video tampering detection is necessary because people are using video tampering to defame popular person, concealing important information and presenting it as proof in the court to get judgment in his favors. If we have active video then it is easy to detect tampering by using digital signature and digital watermark, but if we have no information about source camera and video does not contain digital signature or digital watermark then it is very challenging to detect video tampering. Generally Internet streaming video does not contain information regarding source camera, digital signature and digital watermark. Blind and passive video tampering detection is new era for researcher and research work in this area is going on. In video mainly three types tampering arise first one is spatial tampering second one is temporal tampering and last is spatial-temporal tampering. In spatial tampering we generally focus on intra frame but in temporal and spatiotemporal we focus on interframe. In passive video spatial tampering detection techniques can be roughly categorized into five category 1) Pixel Based 2) Format based3) H/W or Camera based 4) Physics based 5) Geometric based H.Farid(2009).In pixel based tampering detection we mainly focus on intra frame and spatial coordinate of intra frame. The various video tampering approach in this category is Copy Move, Splicing, and Resampling. Format based technique include Double MPEG compression, MPEG Blocking etc. H/W or Camera based tampering detection use Sensor Noise, Color filter array, Camera response function, Chromatic aberration, White balancing and

DOI: 10.4018/978-1-4666-5888-2.ch125

gamma correction features of Camera used in shooting video. In physics based video tampering detection we mainly focus on light direction and light environment for video tampering detection. In geometric based tampering detection we mainly focus on principal point and Metric measurement. If we want to detect temporal tampering in passive video then we can use the concept of motion compensated edge artefacts (MCEA) for I, P and B frames in video.

BACKGROUND

Video tampering is new in comparison to image tampering.Active and passive image tampering detection play important role to detect tampering in active and passive video. As we have discussed previously that moving images/frames with time axis is video. So if we want to detect video tampering in passive video or blind passive video then we can take help of passive and blind image tampering detection techniques. Generally MPEG video contain three types frame I) I frame II) P frame III) B frame. I frame is known as Intra frame and have least compression and high quality; P frame is known as predictive frame and have higher compression ratio and less quality in comparison to I frame; B frame is known as bidirectional frame and have highest compression ratio and least quality. I frame of any video is approximately equal to JPEG image. Generally if we want to detect tampering in video we extract frame from video and try to find some clue from that frames.So we can say, indirectly we are utilizing passive image tampering detection techniques in passive video tampering detection techniques. Copy move and splicing is a main images/frames tampering method. In copy move image/frame tampering some part of image/frame is cloned or copy paste by same image/frame. A lot of copy move detection techniques have been proposed to detect copy move tampering. First solution to this problem is proposed by (Fridrich, Soukal, & Lukas, 2003) an exhaustive search is performed by comparing the image/frame to every cyclic-shifted versions of itself, which requires (M*N) 2 steps for an image/frame sized M by N. They also proposed to use the autocorrelation properties of the image/frame to detect the duplicated regions. Another approach to detect copy-move forgeries is the block-matching method, which divides the image into overlapping blocks. This approach attempts to detect connected image blocks which were duplicated. (Popesc & Farid, 2004) proposed PCA (principal component analysis), which work well with additive Gaussian noise and JPEG compression. In the same manner (Li. Guohui, Wu.Qiong, Tu & Sun, 2007) retrieve features by applying SVD to low frequency wavelet bands. Next challenge for copy move tampering detection is to find out duplicated block in minimum time complexity. Lexico graphical sorting was answer of this problem which sort similar feature vector in minimum time. However, the computation complexity of the block-matching method could be quite high, and larger resolution makes the problem more crucial. (Wang & Farid, 2007) proposed new computational technique to detect duplication in forge video. Region duplication in frames was detected by matching phase correlation among frames blocks.(Zhang, Feng, & Su, 2008) implement region duplicacy concept in static image by introducing wavelet decomposition. (Amerini, Ballan, Caldelli, Del Bimbo, & Serra, 2011) proposed A SIFT based forensic method for copy move attack detection and information recovery. In this article SIFT based approach not only detect copy move tampering but also recover information regarding geometric transformation which was used in copy move tampering.(Xu, Liu, & Dai, 2012) proposed new idea for fast detection of copy move forgery on the basis of phase correlation. (Amerini, Barni, Caldelli, & Costanzo, 2013) proposed Counter forensic of SIFT based copy-move detection by means of key point classification. In this article authors have discussed the counter approach adopted by user when attacker attack on SIFT features which is used in copy-move tampering detection.

Further, in splicing image/frame tampering we create single image/frame with the help of two frame/image. Several methods have been proposed to detect splicing attack in image/frame. (Shi, Chen, & Chen, 2007)proposed a blind splicing detection approach based on a natural image model.The natural image model consists of statistical features including moments of characteristic functions of wavelet sub-bands and Markov transition probabilities of deference 2-D arrays. This method has higher accuracy in comparison method proposed by (Ng, Chang, & Sun, 2004). (Mahdian & Saic, 2009) proposed blind image forgery detection method using noise inconsistencies. This proposed method capable of dividing an investigated