A Review on Video/Image Authentication and Temper Detection Techniques

Zarna Parmar
Dept. of computer science and Engg.
S.P.B. Patel College of Engineering,
Gujarat, India.

Saurabh Upadhyay
Associate prof., Dept. of CSE.
S.P.B. Patel College of Engineering,
Gujarat, India.

ABSTRACT

With the innovations and development in sophisticated video editing technology and a wide spread of video information and services in our society, it is becoming increasingly significant to assure the trustworthiness of video information. Therefore in surveillance, medical and various other fields, video contents must be protected against attempt to manipulate them. Such malicious alterations could affect the decisions based on these videos. A lot of techniques are proposed by various researchers in the literature that assure the authenticity of video information in their own way. In this paper we present a brief survey on video authentication techniques with their classification. These authentication techniques are generally classified into following categories: digital signature based techniques, watermark based techniques, and other authentication techniques.

General Terms

Image Processing, Authentication

Keywords

Video Authentication, Video Tempering, Authentication Techniques

1. INTRODUCTION

At the present time reputation of multimedia demands the systems which are efficient and intelligent in order to deal with the large number of multimedia information. Authentication means act of verifying the truth of an entity**.** This may involve confirming the distinctiveness of an artifact, or ensuring that an artifact is original. Multimedia editing software allows manipulating the content of digital information. It is indispensable to substantiate the truthfulness of video recordings used as evidence in sensible proceedings. Researches in video authentication are in its early stage, therefore much of the research work remains open [2]. It is hard to assert the best video authentication techniques yet. In several applications the legitimacy of video data is of foremost importance such as in video examination, forensic investigations, law enforcement and content ownership [1]. Any video applications may have at least three parties: The producer who generates the video. The receiver receives the video from producer via third party. Here the third party could be either a storage contrivance (such as CD/DVD) or a busy and receiver can also be a third party if, it forwards the video to any other party. The attacker targets this third party category for altering the video content [1].

1.1. Need for the video authentication

Visual data can be altered using sophisticated processing tools without leaving any visible hint of the alteration. So doubt would always exist that it had been deliberately tampered with to incriminate or exonerate the suspect. The video data can be created artificially by computerized techniques such as morphing. Therefore the true source of the data must be shown to use them as legal manifest.

It is hard to ensure that the digital video produced as manifest, is the same as it was actually recorded. For affirming the originality of video content, to detect malicious tampering and preventing various types of forgeries performed on video data, video authentication techniques are used [2].

These methods are also useful in video identification. Video identification refers to a process that recognizes the existence of a particular video clip in large amount of multimedia data. For example, in an advertisement supervising scenario where a commercial company or an individual can automatically identify in real time whether a TV channel is playing their video advertisement for the specified time. A TV channel may cut few frames to earn more time and the money**.**

2. TAMPERING OF THE VIDEO CONTENT

When the content of information, being produced by a given video sequence, is maliciously altered, then it is called tampering. It can be done for several purposes, for instance, to manipulate the integrity of an individual, to offend an individual, or to hide the content of information provided in the video [2].In short, it is easy to alter the content of information maliciously, that leads to serious issues for the researchers to be solved.

2.1. Video tampering attacks and detection

Alteration in a video can be done by camera tampering or by scene changing. In [3], Some examples are presented regarding a camera tampering, i.e. a person holding some object in front of the camera so that it could interrupt a recording scene, spray painting on the camera lens, or tilt the camera so that it focus in a different direction. In order to be detected, such an event must be sustained for several seconds. Camera tampering detection algorithms ought to be sensitive to any significant camera motion. The number of false detection events should be minimized. In [3], a paper presents a novel technique for camera tampering detection**.** This method identifies camera tampering by detecting large differences between older frames of video and more recent frames [3]. Moreover, the effects of adjusting the internal parameters of the algorithm are examined. The performance of this method is shown to be extremely favorable in real-world settings [3]. On the other hand, tampering can be done on the content of the prerecorded video by the software programs easily available in market. Shot/scene changes are often modeled as rapid or transient transitions, and thus image

features can be compared by looking only at consecutive frames of video [3]. When a malicious modification is performed on a video, it either attacks on the contents of the video (i.e. visual information presented by the frames of the video), or attacks on the temporal dependency between the frames [2]. The techniques are used to verify that video is either authentic or tampered. For example, digital signatures, data embedding and watermarking techniques. Other authentication techniques have also been developed by researchers that are specifically designed for various cases of malicious attacks. In [13], authors have presented a technique to indentify the tampering in the image using blind deconvolution. Considering the direct output image captured by the camera as authentic, and introduced an algorithms to detect further malicious processing was applied to image.

3. AUTHENTICATION TECHNIQUES

In [2], authors have represented that, video authentication techniques are classified in four categories: Watermark based techniques, Digital Signature based techniques, and other authentication techniques. Among these techniques, digital signature and fragile watermarking techniques are commonly used for video authentication.

3.1. Digital signature

The digital signature method introduced by Diffie and Hellman in 1976. The digital signature shall depend on the content and some secret information which is only known to the signer [5]. Therefore, it cannot be forged, and the appraiser can verify whether the content of video information matches the information contained in the digital signature. In other words, we can trust the signer as well as his/her digital signature to verify the data integrity [5]. In signature based techniques, the sender first extracts the key features from the original copy of image/video and then features are encrypted using a private key, resulting in signature [8]. The receiver can use the sender's public key to decrypt the signature in order to authenticate the received image. The signature is usually stored somewhere other than in the media itself [8]. The digital signature is stored individually in user defined field, like, in header of MPEG sequence or in a separate file [1]. Because multimedia data are stored in specific file format, the digital signature can be considered as being "embedded" in the data [5]. Digital signature methods have taken few research directions – message authentication code (MAC, AMAC, and AIMAC), visual hash, robust hash and digital signature itself [4]. These techniques pursue a common technique for authentication: feature extraction and subsequent use of the features for later authentication [4]. A technique for image authentication is proposed by [4] in a semi fragile way to detect the tampered pixels of an image. Chih-Hsuan Tzeng and Wen-Hsiang Tsai [6], has presented a new authentication scheme based on the use of a new type of digital signature, which works for color as well as geometric visual appearance, and prevents explosion of the signature size in the mean time [6]. They proposed technique composed of two processes, signature generation and signature authentication using authentication and then tamper localization.

3.1.1 Signature generation

In digital signature generation process, edge detection algorithm was applied to detect and classify each non-overlapping block *bk* with same size m×m in two types, smooth block and edge block [6]. This size is set as standard unit to detect tampering.

The standard deviation of pixel value was used in a smooth block as a feature. The feature was then encoded with a digital signature. A precedent bit with value "0" was set to indicate the existence of a smooth block. Edge blocks contain more details and have larger color variances than smooth blocks; it is neither efficient nor sufficient to represent edge blocks using only color information [6].

3.1.2 Authentication Process

The features of the image/video are compared with the features recorded in corresponding digital signature. This will show whether the particular image/video is tampered [6]. The process decrypts the digital signature by using the decryption key Kd. Assume, block classification is performed on the block B of a frame, and the result B' was derived. This result might not be the same as the block type B [6]. The verification process was performed on four combinations of these two types of block. 1. B and B' are new blocks. 2. B and B' are edge blocks. 3. B is a smooth block and B' is an edge block and 4. B is an edge block and B' is a smooth block. The proposed method by authors in [6] is simple and computationally efficient. Because the proposed authentication technique is digital signature-based, it inherits the merits of using the digital signature such as asymmetric authentication which is more flexible than the existing schemes that require the original embedding key for authentication[6]. There are mainly two means of authentication exist for digital multimedia content. One is soft authentication technique which allows alteration of digital data as long as it does not put down perceptual quality [9]. The other is a hard authentication technique which does not allow any alteration to the video bit stream. This technique can be considered as a form of lossless authentication [9]. Digital signatures are one way of achieving hard (lossless) authentication. Ramaswamy and K.R. Rao in [9], proposes a hard video authentication and sender verification scheme for video sequences compressed using H.264/AVC Main Profile by using digital signatures and cryptographic hash. Many other techniques are proposed which uses digital signature based techniques. In [14] authors have described a content based video/image authentication technique. The signature is generated by first extracting the features from image/video and then encrypting these features. In the authentication process, decryption of the signature takes place and feature code is decrypted. The resulting data will show whether the content of the video/image is tampered. In [10], authors have presented brief review about various kinds of digital signature based authentication techniques for secure video. The hash function combined with multi-signature to authenticate reports or interviews. In contrast to this scheme, the SHA algorithm was applied for hashing function and digital signature. A brief review of robust digital signature, feature based digital signature and hierarchical digital signature also presented in the paper.

3.2. Watermarking

In watermarking schemes, authentication data is embedded with multimedia data**.** Different watermarking schemes are proposed to prevent illegal copying and malicious alteration. The watermarking techniques work on either compressed or uncompressed information [7]. Various types of watermarking schemes have been proposed for different applications. For copyright-related applications, the embedded watermark is required to be protected from different types of malicious and non-malicious operation to some degree. The authors in [7] presented that the altered content of information is still valuable in terms of business significance or adequate in terms of perceptual quality. Hence, generally these techniques are robust for copyright-related applications. The watermarking techniques can be employed in spatial or frequency domain using various transforms like Fourier, DCT, DWT, and Fractal etc [7].

3.2.1. Watermarking technique for spatial domain

The watermarking technique is implemented using these steps.

1. Convert Video Color Space

2. Motion Estimation

3. Block Selection Criteria

4. Watermark Generation

5. Watermark Embedding

6. Watermark Extraction

7. Quality Measurements

The authors in [7] have implemented the steps that are used to embed the watermark with the input video.

1. Extract loaded color video into frames.
2. Apply block matching motion estimation techniques on the subsequent frames.
3. Select only those frames that have sufficient number of motion blocks which is compatible with the watermark size.
4. From the selected frames use a given threshold to select the best blocks during the matching process.
5. Perform the wavelet transformation on the selected best blocks.
6. Embed a random Gaussian distribution as a proposed watermark into the selected blocks (Apply only to the HL and LH wavelet bands).
7. Extract the embedded watermark.
8. Apply some attacks on the watermarked frames in the video.
9. Evaluate the conducted results using PSNR for embedding and similarity for extracting process before and after attacks.

3.2.2. *Watermarking technique for Frequency domain*

The video watermarking scheme in frequency domain follows the same steps used for the spatial domain [7], but the watermark is embedded and extracted to/from the wavelet blocks (HL and LH) bands. The HL and LH bands are embedded with watermark because of two reasons:

1. LL band consists of a large amount of energy in the signal. So, if there is an abrupt motion in the video frames, the inserted at watermark cannot be robustly extracted when it is threatened by attacks [7].
2. HH band consists only of some details information and it is very fragile to embed watermark in it [7].

A recoverable image authentication algorithm based on digital watermarking is proposed in [8]. In this method, the image was first fragmented into separate, equal size and was examined to acquire two set of information**:** one for tamper detection and other for image recovery [8]. For tamper detection, the relations between image blocks were established in order to discourage an adversary's attempt to alter the image [8]. In addition, the designed authentication system was tactless to the regular image processing operations. Moreover, in order to attain the improved recovery result, an image block with more complex contents (referred to as an edge block) was further divided into sub-blocks [8].

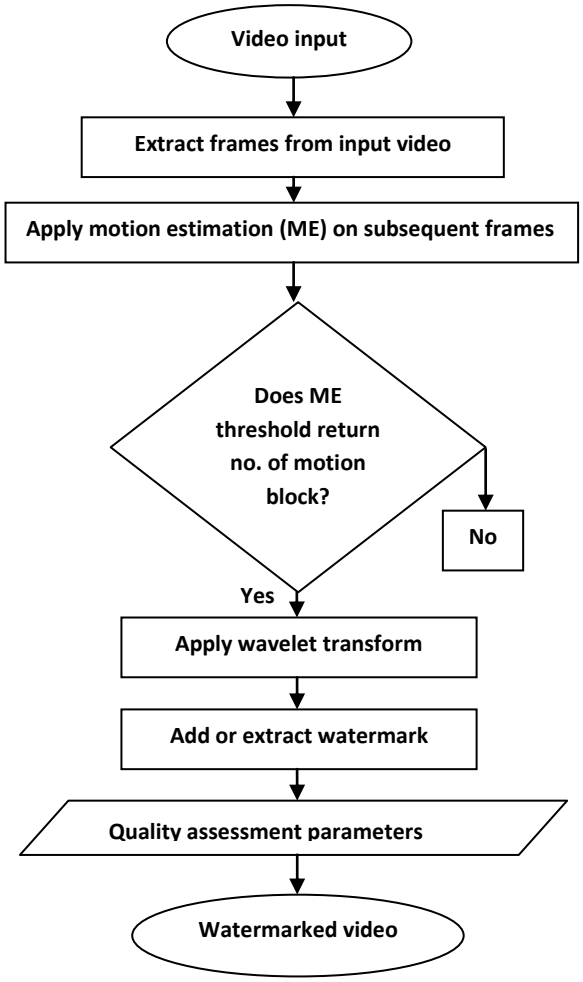

Fig 1: Diagram for watermarking a video

3.3. Other video authentication techniques

Generally an authentication is required for digital communication**.** Researchers have done experiments for protection of digital information by different procedures [10]. Apart from Digital Signature and Watermark based techniques, other intelligent techniques for video authentication are also proposed. Some techniques for video authentication are discussed here, that does not rely on digital signature or watermark techniques.

Two techniques have been presented by Weihong Wang and Hany Farid in [11], which can detect duplicated frames in video. The two approaches were used by the authors to examine the methods, one is frame duplication and other is region duplication. In the frame duplication method, the basic approach used is, first partitioning a full length video sequence in to short overlapping sub-sequences [11]. These compact sub-sequences are extracted and compared throughout entire video. A video sequence, f(x, y, t), $t \in [0, L-1]$, of length L, it would be computationally intractable to search for duplication by comparing all possible sub-sequences of arbitrary length and positions in time [11]. As the measure of similarity, the correlation coefficient is used**.** A temporal co-relation matrix is then generated, which embodies the correlation between all the pairs of frames in a sub-sequence. The correlation coefficient between pairs of these matrices is then computed [11]. If a computation two sub-sequences with a correlation results above a specified threshold (close to 1) is considered as duplicated frame. Another approach used in [11], is region duplication. In a

video sequence, some part of several consecutive frames can be duplicated, so a different method is used to detect the duplicated region. First, scene recorded by the stationary camera and then, recorded by the moving camera. Tampering of the video is very efficiently detected in above method.
A forger will always try to leave no hint that could be able to detect video or image has been tampered, for that they try to match the tampered region with the original one. Generally, it is necessary to replace, resize, stretch or rotate a portion image [12]. However, this seems to be imperceptible to detect these kinds of changes in the image but it introduces a correlation into the image. In [12], Alin C. Popescu and Hany Farid have described a technique is able to automatically detect such correlations in any portion of image. In [2], brief overview of an authentication technique for digital video is described which is based on motion trajectory and cryptographic secret sharing [2]. In the proposed method, the video sequence is firstly segmented into number of sub-sequences then each frame of the video sequence is mapped to a trajectory in the feature space by which the key frames of the video shot are computed [12]. Once the key frames are evaluated, a secret frame is computed from the key frames information of the video shot. These secret frames are used to construct a hierarchical structure and after that final master key is obtained. This master key is used to identify the authenticity of the video.

4. CONCLUSION

To recapitulate, paper represents different authentication techniques offered by the researchers, which are mainly classified into digital signature based, watermarking based and other authentication techniques. It is essential that the information represented is immune to the different kind of manipulations to some extent. Much of the future work can be done to develop efficient and robust techniques. Moreover, these techniques are not only limited to video data but also can be applied on images.

5. REFERENCES

[1] Saurabh Upadhyay, Sanjay Kumar Singh, Video Authentication: Issues and Challenges, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3, January 2012.

[2] Saurabh Upadhyay, Sanjay Kumar Singh-"Video Authentication- An Overview", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011.

[3] Ribnick, S. Atev, O. Masoud, R. Voyles and N. Papanikolopoulos, "Real-Time Detection of Camera Tampering", Proc. IEEE Int'l Conf. Advanced Video and Signal based Surveillance (AVSS 2006), pp. 10−10, Nov. 2006.

[4] R.Bausys and A.Kriukovas, "Digital Signature Approach for Image Authentication", Electronics and Electrical engineering, Vilnius Gediminas Technical University, Lithuania, ISSN 1392-1215.2, No.6(86), 2008.

[5] Ching-Yung Lin, "Watermarking and Digital Signature Techniques for Multimedia Authentication and Copyright Protection," Ph.D. Thesis, Columbia University, Dec. 2000.

[6] Chih-Hsuan Tzeng, Wen-Hsiang Tsai, "A new technique for authentication of image/video for multimedia applications". MM&Sec 2001: 23-26

[7] Jamal HUSSEIN1 and Aree MOHAMMED2, "Robust Video Watermarking using Multi-Band Wavelet Transform", IJCSI International Journal of Computer cience Issues, Vol. 6, No. 1, 2009.

[8] Yuan-Liang Tang and Chih-Jung Hung, "Recoverable Authentication of Wavelet-Transformed Images," ICGST International Journal on Graphics, Vision and Image Processing, Vol. SI1, pp. 61-66, 2005.

[9] Nandakishore Ramaswamy, K. R. Rao, "Video authentication for H.264/AVC using digital signature standard and secure hash algorithm", NOSSDAV 2006, 21.

[10] R N Mandavgane and N.G.Bawane. "Digital Signature Schemes for Secure Video.", IJCA Proceedings on National Conference on Innovative Paradigms in Engineering and Technology, (NCIPET 2012) ncipet (4):1-4, March 2012.

[11] Weihong Wang, Hany Farid, "Exposing digital forgeries in video by detecting duplication", MM&Sec 2007: 35-42.

[12] Alin C. Popescu, Hany Farid, "Exposing digital forgeries by detecting traces of resampling", IEEE Transactions on Signal Processing, 53(2-2): 758-767 (2005).

[13] Ashwin Swaminathan, Min Wu, K. J. Ray Liu, " Image Tampering Identification using Blind Deconvolution", ICIP 2006: 2309-2312.

[14] Ching-Yung Lin and Shih-Fu Chang, "Generating Robust Digital Signature for Image/Video Authentication," Multimedia and Security Workshop at ACM Multimedia, Bristol, UK, Sept. 1998.