Digital Signature Schemes for Secure Video

R. N. Mandavgane
Nagpur University
B.D. College of engineering
Sevagram, Wardha

N.G.Bawane.
Nagpur University
Principal, S.B.Jain institute Technology,
Management and Research, Nagpur

ABSTRACT

Wireless multimedia delivery is becoming increasingly important in today's networks. Due to the explosive growth of the Internet and increasing demand for multimedia information on the web, streaming video over wireless networks has received tremendous attention from academia and industry. Data origin and data integrity authentication are very important factors in video security. Extensive research has been conducted in this area with different techniques. In this paper, digital signature techniques are reviewed for authenticating video.

General Terms

Video security.

Keywords

Digital signature, authentication, video.

1. INTRODUCTION

The communication field is changing rapidly from wired to wireless communication, analog to digital communication, AM to FM and so on. Simultaneously in digital data, malicious tampering of data is also a very much essential problem to deal with. Naturally an authentication of data is required for digital communication. Many Researchers have done an experiment for security in digital data by different techniques. While for data authentication many practical solutions exist, authentication for streaming media is challenging because the media delivery is often over an unreliable channel where packet loss may occur. Also video may be tampered in between. Hence security in video streaming is very important issue. One of the techniques is digital signature technique. One category of authenticating video is by digital signature approach. The digital signature approach is based on the idea of extracting invariant features from video data and encoding them to form digital signatures. To certify a received video, two feature sets are compared. The two sets are one being extracted from the received video and the other from the digital signature. Signature should protect the message conveyed by the content of image/video and not the particular representation of that content [10]. So even if images/videos are modified by processing, that does not affect the content of the image. Signatures can be used to verify the authentication of such image/video.

Different techniques were proposed by different researchers for digital signatures. These are loosely fall into two groups [9] where highly compressed image/video serves as digital signature or content based signature which consists of feature of image/video. Feature vector of an image is that which adequately describes the content of an image. Paper [10] specifies several different such as edge information, DCT co-efficient and color or intensity histograms. Authenticity using intensity histogram [10], Using DCT co-efficient [11], edge based digital signature [4], color and geometric visual feature [5] are observed.

The paper is organized in the following way. In section 2 digital signatures is explained briefly. In section 3 different techniques are studied. In section 4 observations about the different schemes are discussed. Paper is concluded in section 5.

2. DIGITAL SIGNATURE

Loosely speaking, a digital signature scheme offers a cryptographic analogue of handwritten signatures. A digital signature scheme is typically used by a signer .The signer begins by running some key-generation algorithm to produce a pair of keys (pk; sk), where pk will be called the signer's public key and sk is the signers private key. The signer then publicizes its public key. Once a signer has established a public key pk as discussed above, digital signature schemes allow the signer to "certify" (or "sign") a message in such a way that any other party who knows pk can verify that the message originated from the signer and has not been modified in any way.

A typical video authentication system from [7] is shown in fig 1a. In the authentication process, for a given video, The authentication schemes processes the features extracted from the video and outputs the authentication data which is using the encryption key to from the signature. The video integrity is verified by computing the new authentication data using the same authentication algorithm and features. The new authentication data is compared with the original authentication data as shown in fig 1b.I If both match, video is treated as authentic otherwise it is considered as tampered.

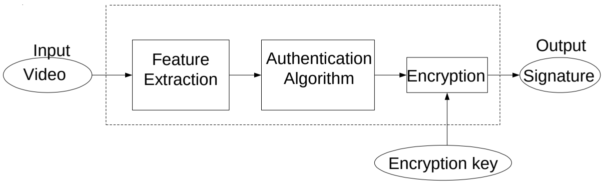

Fig 1a: Authentication process

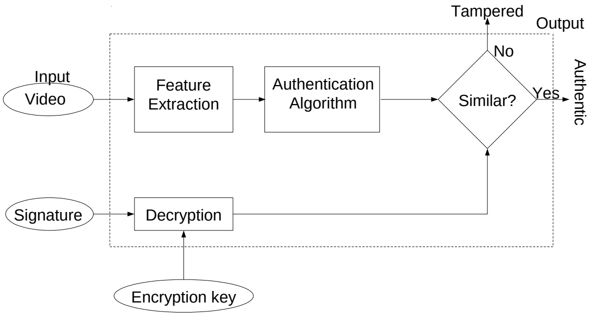

Fig 1b:Verifcation process

3. DIGITAL SIGNATURE SCHEMES

Different schemes were observed for authenticating video. These are multi signature based, robust digital signatures, feature based digital signature and hierarchical digital signature schemes.

3.1 Multi signature

In [1] ,the concatenation property of Tillich –Zemor one way hash function is combined with a Gulliou-Quisquater multi signature scheme in a journalism context for the authentication of sequences. The Aim is to authenticate reports or interviews. In [2], an efficient system guaranteeing to detect whether the images of an original video sequence have been modified between the original recording and the moment of viewing was presented. In this scheme instead of Tillich –Zemo hash function, the SHA algorithm was used along with the Gulliou-Quisquater protocol for hashing function and the signature scheme.

3.2 Robust digital signature

In reference [3] authors suggested two robust digital signature methods as shown below in fig 2 and fig 3. In[11] same concept was explained.

The first method assumes a picture P includes $P_{blockdata}$ and p_{others} .$P_{blockdata}$ includes codes of DCT coefficients, used to generate feature codes. P_{others} include all other codes in P of which hash values is obtained. Then a combination of the feature codes and hash values of each picture are hashed to get digital signature. In second type of digital signature generation, if DCT coefficients may change the only consistence property is the pixel values of pictures were considered. The digital signature was generated picture by picture considering the pixel values.

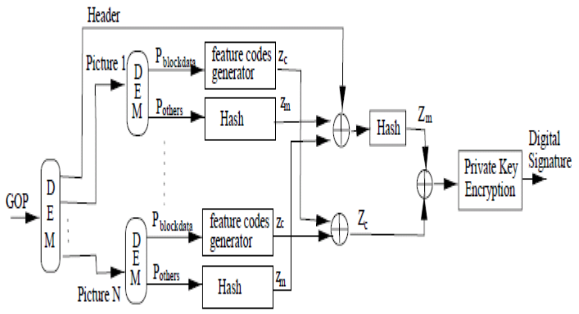

Fig 2: Robust digital signature 2.

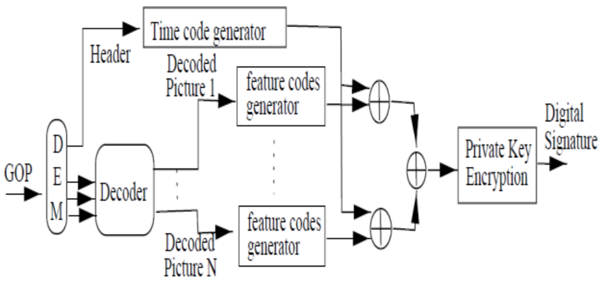

Fig 3: Robust digital signature 3.

3.3 Feature Based digital signature

Different feature extraction methods are found in the literature as below.

3.3.1 Intensity histogram based digital signature

In [10], intensity histogram was used for finding the digital signature. Here the images were divided into blocks and intensity histogram was computed separately for each block. By keeping the variable size blocks fine details of the images can be protected.

3.3.2 Edge based digital signature

In edge based digital signature generation [4], the following method is adopted.

1. The edge detection of the image or video frame is done. The result of this is that a new image is consisting of grey and black values for the edges and white for the background is created. This is called edge characteristics. This characteristic was generated by Canny edge detector algorithm [12].
2. Then it is transformed into a binary edge pattern.
3. Then a VLC (variable length code) for data reduction is obtained.
4. Finally a signature is obtained using a private key.

For a video with two many frames a method has to be applied for all the frames and hence it becomes complicated for verification. Image and video data are composed of both color and geometric information and this particular aspect is ignored in this method.

3.3.3 Color and geometric features based digital signature.

Another authentication scheme was proposed by chih-husan Tzeng and Wen Hsiang Tsai in [5] which exploits both color and geometric visual features and also made an attempt to reduce the signature size. The method for digital signature generation is as follows.

1 A significant edge detection method was applied to an input image/video. The significant edge detection classifies each non overlapping block into two types, smooth blocks and edge blocks. If there is at least one connected component with size larger than 4 in the corresponding binary image, then block is classified as edge block or else it was called as smooth block.

2 Smooth blocks were represented by their mean values. For edge block representation binary edge patterns are used as features. Use of binary edge pattern also prevents the size of the digital signature from explosion.

3 At least the digital signature was constructed by cascading all the encoded features extracted from the blocks followed by an encryption key for security purposes which further encrypts the cascaded bit stream.

3.4 Hierarchical digital signature

The next scheme was proposed in [6] is based on motion trajectory and image sharing. The step for signature generation is as follows. It is shown in fig 4.

1 Video was segmented into shots.
2 Motion trajectories were established for every shot.
3 The Key frames are identified in each shot.
4 Compute the secret frame of all shots using key frames.
5 Compute the master key from all the secret frames.

The next work in fig 5 was found in [7] and [8] as hierarchical structure. The method used in [6] is based on the motion trajectory and image sharing whereas in this case differential energy computation is used for the key frame identification. The steps for the signature generation are below.

1 Here input video was segmented into video shots.

2 Then for each video shot a key frame was obtained by differential energy computation.
3 A secret frame at the key frame level was computed based on the private key i.e. the key at the key frame level.
4 Using the key frames and secret frames at the video shot level another secret frames were computed based on private key at the shot level.
5 Finally the master key from all secret frames based on a private key at video level was computed.

4. OBSERVATIONS

It is observed that the schemes in [1] & [2] for authentication protect every single bit of the video content and do not allow any form of manipulation but in several situations compressed videos need to be further processed to accommodate various application requirements. These schemes also do not take into account the problem of the sound.

In [10], it is found that the scheme was based on the use of the histograms of image blocks and the generated digital signature requires a large amount of space for storage. In [3], Difference in DCT coefficients are used for computing digital signatures But this is vulnerable since the value of DCT coefficients can be modified keeping their relationship preserved. In [4], use of video compression might result in the distorted edge in the reconstructed image. Therefore some extracted edge features might be slightly moved or shifted. Hence the correctness of authentication is somewhat affected.

In [5], edge detection method was used which is also a vulnerable to content modification because if a smart attacker modifies the content keeping the edges presented the authentication will failed.

In [6], motion trajectory based selection of key frames was proposed where as in [7] and [8] key frames are selected by using differential energy computation.

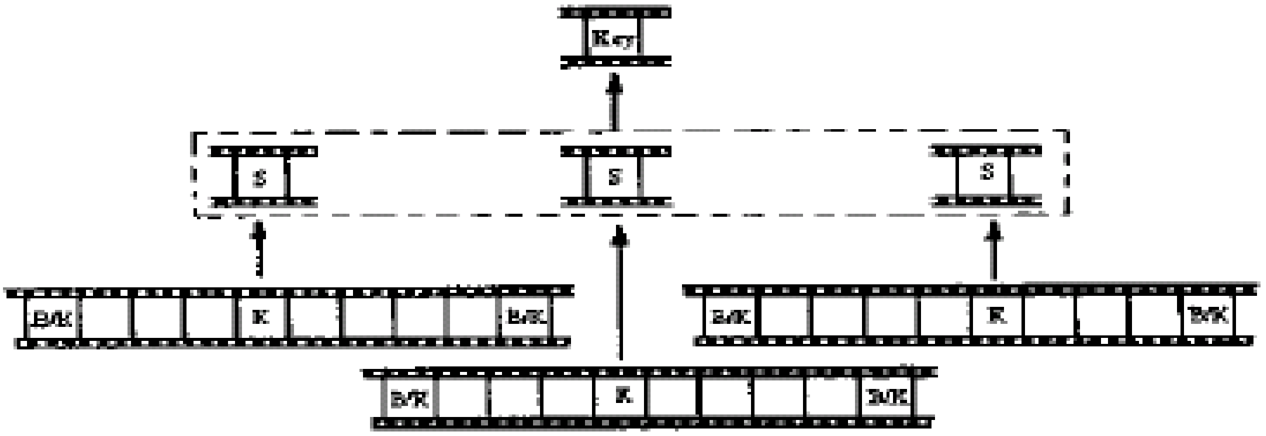

Fig 4: Motion trajectory and image sharing.

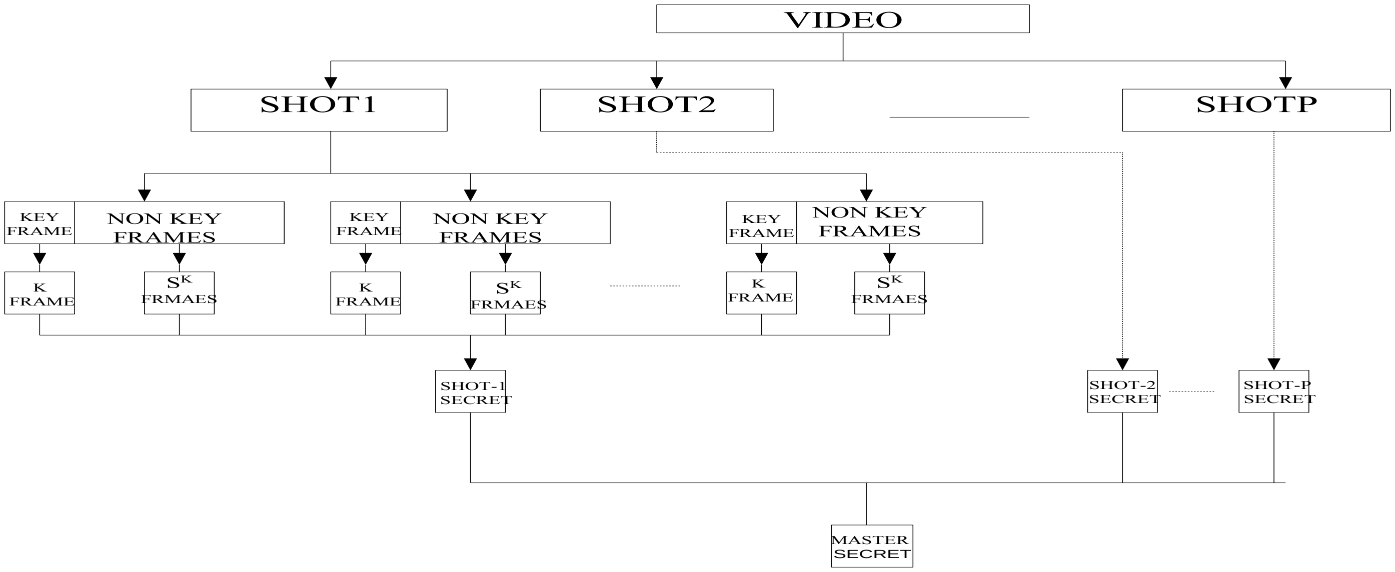

Fig 5: Hierarchical structure.

5. CONCLUSION AND SCOPE

To recapitulate, different authentication method has been reviewed. From The above discussion, it was seen that digital signature was applied to the content description thereby authenticating the content of the image. In modern coding standards scalability is a new important trend in video coding standards. Digital signature schemes for authentication do not address scalability. Hence there is a need to optimize these techniques.

Further work on this authentication includes the study of remaining different techniques such as watermarking, cryptographic techniques as Hash chaining and Merkle Hash trees. Finally the complete scalability structure of these dimensional scalable streams will be considered for authentication.

6. REFERENCES

[1]Jean Jacques Quisquater, Marc Joye, "Authentication of Sequences with the SL_2 Hash Function: Application to Video sequences", Published in Journal of Computer Security , pp 213-223, !997.

[2] J.J Quisquater, B. Marq, M. Joye and A. Bernard, " Practical Solution to Authentication of Images With A secure Camera", Published in I.K.Sethi and R.C. Jain, Eds., Storage and retrieval for Image and video Databases V, Vol. 3022 of Proc.SPIE pp. 290-197, SPIE, 1997.

[3]Ching-yung lin andshia-fu chang, "Issues and Solutions for Authenticating MPEG Video", IEEE International conference on Acoustics, Speech and Signal processing, vol. 3657 pp 54-65, April1999.

[4]Jana Dittmann, Arnd Steinmetz, Ralf Steinmetz, " Content based digital Signature for Motion picture Authentication and Content Fragile Watermarking" In IEEE international conference on multimedia computing and systems, vol. 2, pp 209-213, 1999

[5] Chih Husan Tzeng and Wen Hsiang Tsai, "A New Technique for Authentication of Image/Video for Multimedia Applications", In Multimedia and security workshop at ACM multimedia, Ottawa ,Canada, pp 23-26, 2001

[6]Wei Qi Yan and Mohan Kankanhalli, "Motion Trajectory Based Video Authentication", IEEE ISCAS, Bangkok, vol. 3, pp 810-813, 2003

[7]Pradeep K. Atrey , Wei Qi Yan and Mohan S. Kankanhalli , "A scalable signature scheme for video authentication," Multimedia Tools Appl.,vol 34, pp 107-135, July 2007.

[8]Pradeep K. Atrey , Wei Qi Yan and Mohan S. Kankanhalli , " A Hierarchical Signature Scheme for Robust Video Authentication using secret sharing", In International Multimedia Modeling conference, Brisbane ,Australia, pp 330-337. 2004

[9]Ee-Chien Chang, Mohan S. Kankanhalli, Xin Guan, Zhiyong huang, yinghui Wu, " Robust Image Authentication using Content Based compression", In Multimedia Systems,Springer-Verlog 2003

[10]Marc Schneider and Shih-Fu-Chang, "A Robust Content based Digital Signature for Image Authentication", IEEE Internatinal conference on Image Processing, Lausanne, Switzerland, pp. 227-230, 1996.

[11]Ching-Yung Lin And Shih-Fu Chang, "Generating Robust Digital Signature for Image/Video Authentication", In Multimedia and Security Workshop at ACM Multimedia 98, Bristol U.K. September 1998.

[12]J. F. Canny, "A Computational approach to edge detection" IEEE Trans. On Pattern analysis and machine intelligence. Vol. PAMI-8, Nov. 1986.