Research Paper

Volume : 2 | Issue : 2 | Feb 2013 • ISSN No 2277 - 8179

Computer Science

KEYWORDS :

A Brief Survey on Video Authentication

Prayag Patel — ME(Dept. of Computer Science & Engg.) S.P.B. Patel College of Engineering, Linch, Mehsana, Gujrat, India.

Saurabh Upadhyay — Department of Computer Science & Engineering, SIT, Gujarat-India.

ABSTRACT

Though the immense development in digital information technology has brought us in the era of powerful information, we are having some severe challenging issues related with information. One of them is the credibility of information. Today, editing or modifying the content of a digital video can be done efficiently and seamlessly. In this paper we present a brief survey on video authentication. We have also discussed the video authentication regarding robustness. Further we have classified the existing video authentication techniques and explained with their short coming. Moreover the difficult scenarios for video authentication have also given by us.

INTRODUCTION

In P2P file sharing systems like Bit Torrent, eMule etc., each user acts as a relay which not only receives the requested contents but also forwards the received portions to other users file sharing systems, various digital formats such as JPEG, BMP,GIF for images and MPEG,H.264/AVC for videos, are available for sharing. On the other hand[1], the un-trusted intermediaries might tamper with the media for a variety of reasons, such as interfering with the distribution of particular files or piggybacking unauthentic content.

The problem become more challenging if some legitimate adjustments, such as cropping and resizing an image are allowed in addition to lossy compression. Here, additional adjustments might not change the meaning of the content, but could be misclassified as tampering [1].

In some applications the authenticity of any given video is of paramount interest such as in video surveillance, forensic investigations, law enforcement and content ownership [29]. For example, in court of law, it is significant to verify the authenticity of any video that is used as evidence. As in another scenario, for example, if a stationary video recorder for surveillance purpose, is positioned on the post of a railway platform to record every activity on that platform along a side, it would be quite simple to remove a certain activity, people or even an event by simply eliminating a handful of frames from these type of videos. On the other hand it would also be feasible to insert, into these videos, certain objects and people, taken from some other cameras and in different time. So video authentication is a process which ascertains that the content in a given video is authentic and exactly same as when captured.

VIDEO TAMPERING

A continuous video sequence V_c (x,y,t) is a scalar real valued function of two spatial dimensions x and y and time t, usually observed in a rectangular spatial window W over some time interval T. If B(x,y,t) is modification vector then the tampered videoM_c (x,y,t) would also be a scalar real valued function of spatial dimensions x and y and time t as follows:

$$M_c(x,y,t)=B(x,y,t)+V_c(x,y,t)$$

When the content of information, being produced by a given video sequence is maliciously altered, then it is called tampering of video data. It can be performed for several purposes, for example to manipulate the integrity of any individual. Since a vast range of sophisticated and low cost video editing tools and software are available in the market that make it easy to manipulate the video content information maliciously, it projects severe challenges to the researchers to be solved.

2.1. Video Tampering Attacks

There are several possible attacks that can be applied on a video to alter the contents of a video data. Formally a panoptic range of authentication techniques have been proposed by the researchers in the literature but most of them have been primarily focused on still images. In various applications, due to immense availability of information in videos, it may be more important if the video authentication system can tell where the modifications happened and how the video is tampered [5]. On considering these where and how, the video tampering attacks can be classified into different categories. A lot of works have been done that concisely address the classification based on where [29], [5]. And some papers address the classification based on how [28]. In general, finding where the video data is modified is more efficient than to find out how the video data is tampered. When a video is being recorded by a video recorder, it captures the scene which is in front of the camera lens, frame by frame, with respect to time. Number of frames being captured by video recorder in a second depends on the hardware specification of the recording device. Thus a video can be viewed as a collection of consecutive frames with temporal dependency, in a three dimensional plane. This is called the regional property of the videos. 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 of the video. Therefore based on the regional property of the videos, the video tampering attacks can be broadly classified into three categories: spatial tampering attacks, temporal tampering attacks and the combination of these two, spatio-temporal tampering attacks [5]. They can be further classified into their subcategories.

2.1.1. Spatial Tampering

In spatial tampering malicious modifications are performed on the contents of the frames (X-Y axis) of videos. The operations that can be performed as tampering attack in spatial tampering are cropping and replacement, morphing, content (object) adding and removing etc [5]. These attacks can be efficiently performed with the help of sophisticated video editing tools and software as Photoshop, etc.

2.1.2. Temporal Tampering

In temporal tampering manipulation is performed on the sequence of the video frames. The focus is on the temporal dependency. Temporal tampering attacks mainly affect the time sequence of visual information, captured by video recording devices. The common attacks in temporal tampering are frame addition, frame removal and frame reordering or frame shuffling.

2.1.3. Spatio-Temporal Tampering

Spatio-temporal tampering attacks are the combination of the spatial and temporal, both kinds of tampering attack. Frame sequences are modified as well as visual contents of the video frames are modified in the same video. The video authentication system should be able to identify both kinds of tampering.

All these tampering attacks are further classified into their subcategories. Spatial tampering can be in effect either at block level or at pixel level. In both the cases the objects of the video

frames are modified. Further the objects of the video frames are classified into two categories: Foreground objects and Background objects. The foreground objects are those which are captured as individual elements, excluding the background, in a frame of the video. And the background object is the background part of the video frame excluding all of the foreground objects. The different pieces of visual information shown in the video frames are modified in spatial tampering attack. Basically the contents of the video frames are treated as objects. Based on these objects and their classification the spatial tampering can be further classified as shown in the following figure.

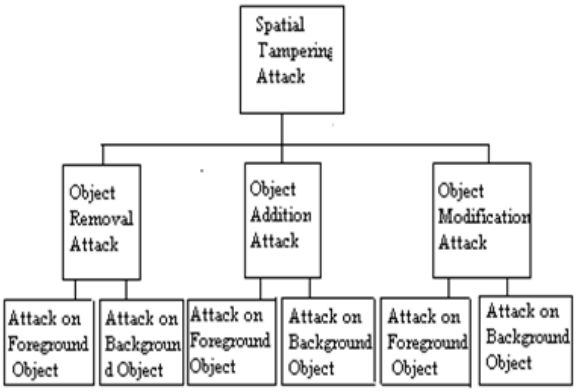


Fig.1. Spatial Tampering Classification

Fig. 1 shows an explicit classification of spatial tampering attacks in reference of objects of the frames.

2.1.1.1. Object Removal Attack

In object removal attack, the objects of the video frames are eliminated. This kind of tampering attack is commonly performed where a particular person wants to hide his/her presence in a certain sequence of video frames. With this kind of tampering attack he /she may disappear in a specific time domain, recorded in the video. This attack can be performed with both kinds of object, foreground objects and background object, as shown in Fig. 2

2.1.1.2. Object Addition Attack

When an object is injected deliberately in a video frame or in a set of video frames then there is a kind of spatial tampering attack: say Object addition attack. In any video, which can be treated as evidence, an additional object can be pasted in a frame or set of frames, with the help of sophisticated video editing software to mislead the investigation agencies as well as court of law. As shown in fig. 3, it can also be performed with both kinds of objects, foreground objects and background objects.

Original Frame Tampered Frame

Fig. 2 (a).

Original Frame Tampered Frame

Fig. 2 (b).

Fig.2. Example of object removal attack. Fig.2 (a) shows object removal attack with foreground object, where a device is removed from the original frame in tampered frame. Whereas Fig.2 (b) shows the object removal attack with background object. Here an object from the background wall is eliminated from the original frame in tampered frame.

2.1.1.3. Object Modification Attack

In Object modification attack, any existing object of the video frame(s) can be altered in such a way that the original identity of that object is lost, and a new object may be in appearance which is totally different from the original object. The object modification attacks can be existed in many prospects in the given video. For instance, the size and shape of the existing object may be changed, the color of the object may be changed or it may be discolored, and with the help of additional effect the nature of the object and it's relation with other objects also may be changed. In fact it is very hard to detect this kind of attack for authentication systems, since these attacks are performed at pixel level. The authentication systems should be robust enough to differentiate this kind of attack with the normal video processing operations. Fig.4 shows a typical example of object modification attack where the face of a person has been changed in such a way that a new person's face is introduced in the altered frame. These attacks can also be performed with both kinds of objects, foreground and background objects.

Besides spatial tampering, temporal tampering attacks have also sub classifications. Temporal tampering attacks can be performed at scene level, shot level and frame level, but the primary focus is on attacking the temporal dependency of the frames of the video.

Original Frame Tampered Frame

Fig.3. (a)

Original Frame Tampered frame

Fig.3. (b)

Fig.3. Example of Object Addition attack. In original frame of Fig.3 (a) one persons is there as major foreground objects, while in tampered frame of Fig.3 (a) an additional person as a foreground object is added. In tampered frame of the Fig.3 (b), not only a foreground object is added but also an additional wall as a background object, in the middle of the frame, is added.

Original Frame Tampered Frame

Volume : 2 | Issue : 2 | Feb 2013 • ISSN No 2277 - 8179

Fig.4. Example of Object modification attack. The face of the person in original frame is modified in tampered frame, in such a way that the new face of the person cannot be identified as the same as in original frame.

We call it 'Third dimensional (dimension with respect to time) attack' on the video sequences. Therefore based on this third dimensional attack we can classify the temporal tampering attacks into following categories.

2.1.2.1. Frame Addition Attack
In frame addition attack, additional frames from another video, which has the same statistical properties, are intentionally inserted at some random locations in a given video. This attack is intended to camouflage the actual content and provide incorrect information [29]. A typical example of the frame addition attack is shown in fig. 5.

2.1.2.2. Frame Removal Attack
In frame removal attack the frames of the given video are intentionally eliminated. In this kind of attack frames or set of frames can be removed from a specific location to a fixed location or can be removed from different locations. It depends upon the intention. Commonly this kind of tampering attack is performed on surveillance video where an intruder wants to remove his/her presence at all. Fig. 6 shows a typical example of frame removal attack

Fig.5 Example of Frame addition attack. In first row the original frame sequence from frame 6 to frame 25 has been shown. After attack, the second row of the frames shows the altered frame sequence in which a new frame is inserted between frame 6 and frame 25. And frame 25 becomes frame 26.

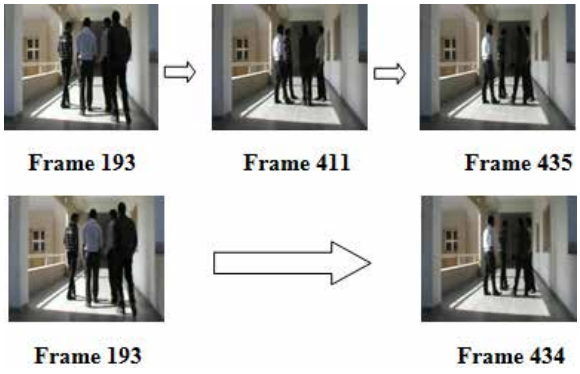
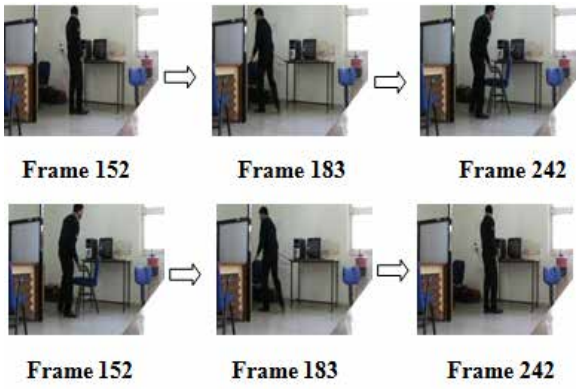


Fig.6 Example of Frame removal attack. The first row of this figure shows the original frame sequence with frame 193, frame 411 and frame 435. In second row of the frame sequence, which shows the tampered frame sequence with frame removal attack, frame 411 is eliminated from the video and hence frame 435 becomes frame 434.

2.1.2.3. Frame Shuffling Attack
In frame shuffling attack, frames of a given video are shuffled or reordered in such a way that the correct frame sequence is intermingled and wrong information is produced by the video as compared to original recorded video. Fig. 7 shows a typical example of frame shuffling attack where two frames are shuffled.



Frame 152 Frame 183 Frame 242 Fig.7. Example of Frame shuffling attack. The first row of this figure shows the original frame sequence with frame 152, frame 183 and frame 242. After the frame shuffling attack, the original frame sequence is tampered as shown in second row of the figure where the positions of frame 152 and frame 242 have been changed.

3. STATE OF THE ART REVIEW
By definition, authenticity means sometimes "as being in accordance with fact, as being true in substance", or "as being what it professes in origin or authorship, as being genuine" [30]. Similarly authentication means to prove that something is "actually coming from the alleged source or origin" [31]. In general, over the last few years Video authentication has received considerable attention by academic world and researchers.

As shown in fig. 8, A typical video authentication system initially starts with the feature extraction. After that, it undergoes the process of specific video authentication algorithm, the authentication data H is generated using the features of the video. This generated data H is encrypted and packaged with the video as a signature or instead it can be embedded into the video content as a watermark. The video integrity is confirmed by computing new authentication data H` for the given video. To check the authenticity of the data, the new authentication data H` is compared with decrypted original authentication data H. If both are matched, the video is treated as authentic else it is constructed to be tampered.

3.1. Classification of Authentication Techniques
The image/video authentication is frequently needed in digital forensic investigations. In digital forensics, the user validates the authentication of an image/video solely by checking the received content [33]-[35].

Watermarking is an another way for insuring the trustworthiness of video information. A semi fragile watermark is embedded in to the video frames. User can assure the authenticity by extracting the watermark from the received content. The system design should ensure that the watermark survives lossy compression but that it breaks as result of malicious manipulations [1].

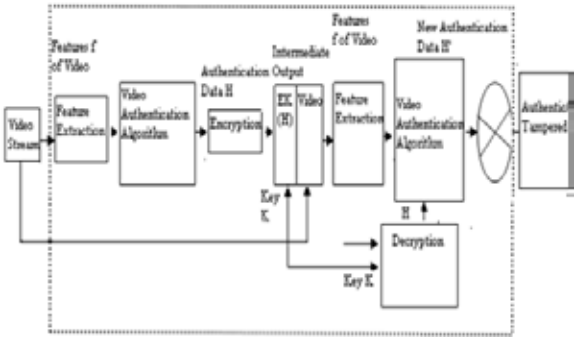


Fig. 8 A Typical Video Authentication System.

Cryptographic hashing might also be use for image authentication. In this technique, the user checks the integrity of received

content using a small amount of data derived from the original content[1].

Many hash base image authentication system achieve robustness against lossy compression by using compression invariant features.

The two fundamental schemes for authentication are fragile watermarking and digital signatures [5]. Moreover the work is done on intelligent techniques for video authentication. Apart from these digital signature, fragile watermarking and intelligent techniques, some other authentication techniques are also introduced by researchers. We are giving here a short classification of video authentication techniques.

3.1.1. Digital Signature Based Authentication

Integrity of multimedia data can be significantly verified by digital signature. Diffie and Hellman were the first,to introduce the authentication of multimedia data in 1976[26]. In the authentication process, digital signatures can be saved in two different ways. Either they can be saved in the header part of the compressed source data, or it can be saved as an independent file. Moreover they can be produced at the time of verification. In the prospective of robustness, its provides enhanced results since the digital signature remains unchanged when the pixel values of the images/videos are changed. The authenticity of the digital signature of the signer to the data depends on the content of data on some secret information which is only known to signer [27].Therefore, the digital signature cannot be copied, and the end user can verify a received multimedia data by investigating whether the contents of data match the information put across in the digital signature. The Johns Hopkins University Applied Physics Laboratory (APL) has developed a system for authentication of digital video [7]. To compute secure computer generated digital signatures for information recorded by a standard digital video camcorder in the authentication system. In the process of recording, compressed digital video is simultaneously written to digital tape in the camcorder and broadcast from the camera into the Digital video authenticator. In this authentication system, video is divided into individual frames and three unique digital signatures are produced per frame-one each for video, audio and (camcorder) control data- at the camcorder frame rate. The process which is used is the key cryptography. In this process two keys were used. The first key is called a "private" key, it is used to generate the signatures and is destroyed when the recording is complete. The second key is a "public" key, which is used for verification. The signatures that are generated make it simple to identify tampering. If a frame, which is added, would not have a signature then it will be detected immediately and if an original frame is tampered, the signature would not match the new data and it will be detected in verification procedure. To generate the digital signature, Ditmann [17] and Queluz [18] used the feature edge /corner of the image. It is stated that this feature is robust against high quality compression and scaling but the difficulty is that the signature generated based on the edge is too long, and the consistency of the edge itself is also a difficulty. The tampered regions were detected by the digital signature and watermarking, but often they are too fragile to resist incidental manipulations. For this type of incidental manipulations structural digital signature [23] can be used for image authentication. This approach makes use of an image's content to construct a structural digital signature (SDS) for image authentication. In this approach [23], many incidental manipulations which can be detected as malicious modifications in other digital signature verifications or fragile watermarking schemes, can be ignored. In the scenario of a station streaming video over network, it is significant for the audiences to have guarantees that the video stream they are watching is indeed from the station. Schemes that are used for this purpose can prevent the malicious parties from injecting commercials or offensive materials into the video streams. Actually this problem has been covered in information security called streaming signing [12] [13], which is an extension from message signing by digital signature schemes. A separate authentication code is written in [3] from the blocks of the video frames. Here the authors Po-Chyi Su et al use the approach of scalar/vector quantization on the reliable features. Once the authentication code is written, it is transmitted along with the video. Thus the authenticity of the given video content can be checked by matching the extracted feature with the transmitted authentication code.

In [1] Authors describe a two state channel that models the target image and then present the image authentication system using distributed source coding.

In their proposed authentication system a pseudorandom projection (based on randomly drawn seedKs) is applied to the original image x and its projection coefficients X, which are quantized to yield Xq. The authentication data are comprised of two parts both derived from Xq. The Slepial-Wolf bit stream S(Xq) is the output of Slepial-Wolf encoder based on LDPC codes [2] and the much smaller digital signature D(Xq,Ks) consist of the seed Ks and a cryptographic hash value of Xq signed with a private key.

The authentication data are generated by a server upon request. Each response uses are different random seedKs. which is provided to the decoder as part of the authentication data.

At the receiving end the user seeks to authenticate the image y with authentication data S(Xq) andD(Xq ,Ks) . It first projection image y to Y in the same way as during authentication data generation using the same random seedKs. A Slepial-Wolf decoder reconstructs Xv' from the Slepial-Wolf bit stream S(Xq) using Y as side information. Finally the image digest of Xq' is computed and compared to the image digest, decrypted from the digital signature D(Xq,Ks) using a public key. If these two image digest do not match, the receiver recognizes that image y is tampered.

Similar to Dittmann's [17] content based digital signature approach for image/ video authentication using edge characteristics, Bhattacharjee and Kutter [25] projected a scheme to generate a digital signature by encrypting the attribute positions in an image. In this approach authentication is accomplished by comparing the positions of the feature point extracted from the targeted image with those decrypted from the previously encrypted digital signature.

3.1.2. Watermarking Based Authentication

Watermarking always remains an important issue for solving authentication problems regarding digital multimedia data, in past few years. A wide range of watermarking techniques have been proposed by various researchers in literature. Based on the application areas, watermarking can be classified in different categories [28]. Beside to ensure the integrity of the digital data and recognizing the malicious manipulations, watermarking can be used for the authentication of the author or producer of the content. Watermarks can be embedded with the multimedia data, without changing the meaning of the content of the data. The advantageous feature with the watermarks is that, they can be embedded without degrading the quality of multimedia data too much. Since the watermarks are embedded in the content of video data, once the data is manipulated, these watermarks will also be modified such that the authentication system can examine them to verify the integrity of data. In [4], authors describe the use of video authentication template, which uses a bubble random sampling approach applied for synchronization and content verification in the context of video watermarking. The authentication template is introduced in order to ensure temporal synchronization and to prevent content tampering in video sequences [4]. Basically in past few years, an increasing use of digital information in our society and availability of very sophisticated and low cost video editing software creates problems associated with copyright protection and authentication. The owners or producers of information resources are being worried of releasing proprietary information to an environment that appears to be lacking in security [9]. On the other hand with the help of powerful video editing software one can challenge the trustworthiness of digital information. In [9], M. P. Queluz presents the generic models with labeling and watermarking approaches for content authentication. In labeling based approach authentication data are written in separate file [9], while in watermarking based approach the authentication information is embedded in the frames. In this labeling-based

authentication system, features C and C` are extracted from the original and modified pictures respectively as according:

$C=f_c(I)$, $C'=f_c(\hat{I})$ In order to assure the authenticity of the label content, it is signed in a trustworthy way, that is, the label is encrypted with a private key(K_{pr}). The label content is produced as:

$L=EKpr\ (C,C_{-I})$

Where C_I is optional information, says Complementary Information, about the frame and its author, assigned by an author society. In the authentication system the corresponding public key Kpu is used to decrypt the label, producing:

$C,C_{-I}=EKpu(L)$

Moreover in [9] M. P. Queluz presents two classical image features for image/video content authentication. The first image feature is concerned with second order image moments. The second feature relies on image edges and it takes the problem of image/video authentication from a semantic view [9]. In image moments feature, for a two dimensional continuous function f(x, y), the moments of order (p+q) is defined as

$$\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} x^p y^q f(x,y)\,dx\ dy$$

For p,q=0,1,2,……..

For a digital image the above equation would be as follows:

$$m_{pq}=\sum_i\sum_j i^p j^q f(i,j)$$

Where f(i,j) represents image color values at pixel site (i, j). Moments are usually normalized dividing it by the image total mass, defined as$\sum_i \sum_j f(i,j)$. Chang-yin Liang, et al [16] proposed a video authentication system which is robust enough to separate the malicious attack from natural video processing operations with the cloud watermark. In the authentication system [16], first of all, the video sequence is split into shots and the feature vectors are extracted from each shot. Then the extracted feature is used to generate watermark cloud drops with a cloud generator [16]. Here, for robustness, content based and semi fragile watermark is used for authentication. In this authentication technique DCT coefficients are evaluated first by partially decoding the given video. After watermarking, the video is encoded again [16]. The extracted watermarks are compared with the features derived from the received video, to check the authenticity of the given video.

3.1.3. Intelligent Authentication Techniques

Intelligent techniques for video authentication use database of videos. The database comprises authentic video clips as well as tampered video clips. As in [29], the authors proposed an intelligent technique for video authentication which uses inherent video information for authentication, thus making it useful for real world applications. The proposed algorithm in [29] is validated using a database of 795 tampered and non tampered videos and the results of algorithm show a classification accuracy of 99.92%. The main advantage of intelligent techniques is that they do not require the computation and storage of secret key or embedding of watermark. The algorithm in [29] computes the local relative correlation information and classifies the video as tampered or non-tampered. Here the algorithm uses Support Vector Machine (SVM) for the classification of the tampered and authentic videos. SVM [10] is a powerful methodology for solving problems in non linear classification, function estimation and density estimation [11]. This algorithm [29] is performed in two stages: (1) SVM training and (2) Tamper detection and classification, usingSVM. In SVM training, the algorithm trains the SVM by using a manually labelled training video database, if the video in the training data is tampered, then it is assigned the label -1 otherwise the label is +1 (for the authentic video). From the training videos, relative correlation information between two adjacent frames of the video is computed, with the help of corner detection algorithm [14]. Then relative correlation information RC is computed for all adjacent frames of the video with the help of

$$RC=\frac{1}{m}\sum_{i=1}^{m} L_i$$

Where Li is local correlation between two frames for i=1,2,... m. and is the number of corresponding corner points in the two frames. The local correlation information RC is computed for each video and the RC with the label information of all the training video data are provided as input to theSVM. With this information of all the video in video database, the SVM [10] is trained to classify the tampered and non tampered video data. Output of SVM training is a trained hyper plane with classified tampered and non tampered video data. In [24], authors integrate the learning based support vector machine classification (for tampered and non tampered video) with singular value decomposition watermarking. This algorithm is independent of the choice of watermark and does not require any key to store. This intelligent authentication technique embeds the inherent video information in frames using SVD watermarking and uses it for classification by projecting them into a non linear SVM hyper plane. This technique can detect multiple tampering attacks.

3.1.4. Other Authentication Techniques

Apart from digital signature, watermarking and intelligent techniques, various other techniques are proposed by researchers for authentication purpose of digital video in the literature. In [19], an authentication scheme for digital video is introduced which is based on motion trajectory and cryptographic secret sharing [19]. In this scheme, the given video is first segmented into shots then all the frames of the video shots are mapped to a trajectory in the feature space by which the key frames of the video shot are computed. 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. Any modification in a shot or in the important content of a shot will be reflected as changes in the computed master key. Here trajectory is constructed, using the histogram energy of the frames of the video shot.

Once the key frames are computed these are utilized to compute the secret frame by extrapolation. Now an interpolating polynomial f(x) is computed by using key frames as follows.

$$\sum_{j=1}^{n+1}\prod_{i=1}^{n+1}\frac{x-x_i}{x_j-x_i}\ I_j$$

This is Lagrange interpolation formulation where the xi position refers to each key frame and Ii is the pixel value of the key frames. By using this equation and extrapolation a frame at x=0 is computed, which is regarded as the secret key. Considering the set of secret keys as another set of shares, the master key frame is computed for that particular video. With this scheme any video can be authenticated by comparing its computed master key with the original master key. This comparison can be performed by using the general cosine correlation measure given by:

$$sim=\frac{I_O\,.\,I_N}{|I_O\,.\,I_N|}$$

Where I_O and I_N are the original master key and the new master key cosidered as vectors. The similarity value would be in the range [0, 1] and if sim = 1, the two master keys would be the same, however if sim = 0, the two master keys would be different. In [20], the key frames are selected by deleting the most predictable frame. In the approach of [21], the key frames are extracted from a video shot based on the nearest feature line. The work in [22] authenticates a video by guaranteeing the edited video to be the subsequence of the original video using a special hash function. The MPEG video standard is one of the most popular video standards in today's digital era. In [15] Weihong Wang and Hany Farid have been worked on MPEG video standard(MPEG-1 and MPEG-2) in this paper they specifically show how a doubly compressed MPEG video sequence

introduces specific static and temporal statistical perturbations whose presence can be used as evidence of tampering. In [6] Hany Farid describes three techniques to expose digital forgeries in which the approach is to first understand how a specific form of tampering disturbs certain statistical properties of an image and then to develop a mathematical algorithm to detect this perturbation. These are Cloning, Lighting and Retouching. In Cloning, a digital image is first partitioned into small blocks of the regions. The blocks are then reordered so that they are placed a distance to each other that is proportional to the differences in their pixel colors [6]. Since it is statistically unlikely to find identical and spatially coherent regions in an image, therefore their presence can be used as evidence of tampering. In lighting approach the direction of an illuminating light source for each object or person in an image is automatically evaluated by some mathematical techniques. The retouching technique exploits the technology by which a digital camera sensor records an image, for detecting a specific form of tampering.

4. DIFFICULT SITUATIONS FOR VIDEO AUTHENTICATION

The surveillance systems has to face the great challenge for the storage and transmission costs of the video clips. So, to reduce the storage and transmission cost only the essential video clips which contain objects of importance are necessary to be sent and stored. Further, in majority of the video surveillance applications, background object changes very slowly in compared to foreground objects. A feasible and efficient solution for this problem is that only the significant objects generally foreground objects are sent out frame by frame in real time while the background object is sent once in a long time period. In such surveillance applications, it is important to provide shield to the authenticity of the video like the authenticity against malicious alterations and the authenticity for the detection of the video source. In surveillance systems which depend on event, the camera will capture the video sequences whenever there is any kind of change in the view of the existed event. If there is uniformity in the scene the camera will not capture the scene. This type of surveillance system is applied in armed forces system for the safety at border. To provide authenticity to the video clips, it is an issue because there is not a proper time gap between the video sequences captured by the surveillance camera. These are the key points which creates considerable challenges to the researchers to solve for authentication.

5. SUMMARY

Video authentication plays a great role in assuring the credibility of video information. However much works has been done in watermarking and digital signature based methodologies, other authentication techniques (including intelligent technique) also produce better results for authentication purpose of video information. The size of authentication code doesn't matter in digital signature based authentication techniques, however, they provide better results regarding robustness, since the digital signature remains unchanged when there is a change in pixel values of the video frames. But if the location where digital signature is stored is compromised then it is easy to deceive the authentication system. On the other hand fragile watermarking based authentication algorithms perform better than algorithm based on conventional cryptography [32]. Fragile and semi fragile algorithm show good results for detecting and locating any malicious manipulations but often they are too fragile to resist incidental manipulations. Moreover embedding the watermark may change the content of video which is not permissible in court of law [29]. In addition of these techniques, intelligent techniques explore the new dimensions in video authentication. However learning based intelligent video authentication algorithm does not require computation and storage of any key or embedding of secret information in the video data, it requires a large database of tampered and non tampered video to let the algorithm learn so that it can classify whether the given video is authentic or not. These techniques are slower than some existing authentication techniques, since they use sufficient large database to learn the algorithm. In other techniques, most of the authentication techniques are established for specific attacks. For example motion trajectory based algorithm only detects the frame addition and deletion attacks (temporal attacks). Moreover compression and scaling operations also affect the performance of existing algorithms.

6. CONCLUSION

Now a days, Video authentication is a very challenging problem and of high importance in several applications such as in forensic inspection of digital video for law enforcement department, video surveyance and presenting video affirmation in court of justice. However with the increase use of powerful video editing tools and technology, there is an extension in the field of video tampering attacks. In upcoming days it is going to be a big nuisance for information security. By analyzing the type of video tampering attacks one can use a variety of video authentication techniques that were presented in this paper. The authentication techniques are definite to the function like surveillance, entertainment industry, medical, copyright, etc. With the advancement of the time, we are getting more concerned towards video applications, in our daily life. There is a great use of video application in our information systems. But with the immense increase of tampering attacks, the information security system has to face several challenges. In future, to classify the acceptable video processing operations from malicious tampering attacks robustness would be one of the key point to get the solution for video authentication techniques. However A perfect video authentication algorithm that identify all kinds of malicious manipulations and that can tolerate all content preserving manipulations is yet to be discovered. We can hope for the better in the future.

Volume : 2 | Issue : 2 | Feb 2013 • ISSN No 2277 - 8179

REFERENCE

[1] Yao-Chung Lin, David Varodayan, and Bernd Girod, Image Authentication Using Distributed Source Coding, IEEE Transaction On Image Processing, Vol. 21, No. 1, January 2012. | [2] A. Liveris, Z. Xiong, and C. Georghiades, "Compression of binary sources with side information at the decoder using LDPC codes," IEEE Commun. Lett., vol. 6, no. 10, pp. 440–442, Oct. 2002. | [3] Po-chyi Su, Chun-chieh Chen and Hong Min Chang, Towards effective content authentication for digital videos by employing feature extraction and quantization. | [4] Fabrizio Guerrini, Reccardo Leonardi and Pierangelo Migliorati A new video authentication template based on bubble random sampling. | [5] Peng Yin, Hong heather Yu, Classification of Video Tampering Methods and Countermeasures using Digital Watermarking Proc. SPIE Vol. 4518, p. 239-246, Multimedia Systems and Applications IV | [6] Hany Farid, Digital doctoring: How to tell the real from fake | [7] Johns Hopkins APL creates system to detect Digital Video Tampering. http://www.jhu.edu/ | [8] Ching-Yung Lin, Shih-Fu Chang, "Issues and Solutions for authenticating MPEG Video" SPIE electronic Imaging 1999. San Jose. | [9] M. P. Queluz Authentication of digital images and video: Generic models and a new contribution. | [10] Vapnik VN (1995) The nature of statistical learning theory. Springer Verlag. | [11] Singh R., Vatsa M., Noore A (2006) Intelligent biometric information fusion using support vector machine. In soft computing in Image processing: Recent advances, Springer Verlag 327-350. | [12] R. Gennaro and P. Rohatgi, How to sign digital stream, Crypto' 97, pp. 180-197, 1997. | [13] J. M. Park, E. K. P. Chong and H. J. Siegel, Efficient multicast packet authentication using signature amortization, IEEE symposium on security and privacy, pp. 227-240, 2002. | [14] Kovesi PD (1999) Image features from phase congruency. Videre: Journal of Computer vision research, MIT Press 1(3). | [15] Weihong Wang, Hany Farid Exposing digital forgeries in video by detecting double MPEG compression. | [16] Chang-yin Liang, Ang Li, Xia-mu Niu Video authentication and tamper detection based on cloud model. | [17] Ditmann, J.; Steinmetz, A; Steinmetz, R., Content based digital signature for motion pictures authentication and content fragile watermarking, Multimedia computing and systems, 1999. IEEE International Conference on, Volume: 2, 1999, Page(s): 209-213 vol. 2. | [18] Queluz, M. P., Toward robust, content based techniques for image authentication, Multimedia signal processing, 1998 IEEE Second workshop on, 1998 page(s): 297-302. | [19] Wei-Qi Yan an Mohan S Kankanhalli, Motion Trajectory Based Video Authentication ISCAS (3) 2003: 810-813 | [20] Latechi L. Wildt D. and Hu J., Extraction of key frames from videos by optimal color composition matching and polygon simplification. Proceedings of MMSP' 2000, Cannes, France, October 2001 | [21] Zhao L., Qi W., Li S., Yang S. and Zhang H., Key frame extraction and shot retrieval using Nearest Feature Line (NFL)., Proceedings of ACM Multimedia 2000. | [22] Quisquater J., Authentication of sequences with the SL2 Hash function application to video sequences, Journal of computer security, 5(3), pp: 213-223, 1997. | [23] Chun-Shien Lu and Hong Yuan Mark Liao, Structural digital signature for image authentication: An Incidental Distortion Resistant Scheme. IEEE Trans. Multimedia, vol. 5, no. 2, pp. 161-173, Jun. 2003. | [24] R. Singh, M. Vatsa, S.K. Singh, and S. Upadhyay, Integrating SVM Classification with SVD Watermarking for Intelligent Video Authentication, In Telecommunication Systems Journal - Special Issue on Computational Intelligence in Multimedia Computing, Springer, 2008. | [25] S. Bhattacharjee and M. Kutter, Compression tolerant image authentication, in IEEE International Conference on Image Processing, 1998, pp. 435-439. | [26] W. Diffie and M. E. Hellman, New Directions in cryptography, IEEE Trans. on Information Theory, Vol. 22, No. 6, pp.644-654, Nov 1976. | [27] P. Wohlmacher, Requirements and Mechanism of IT-Security Including Aspects of Multimedia Security, Multimedia and Security Workshop at ACM Multimedia 98, Bristol, U. K., Sep. 1998. | [28] Jana Dittman, Anirban Mukharjee and Martin Steinbach Media independent watermarking classification and the need for combining digital video and audio watermarking for media authentication. International conference on Information Technology: Coding and Computing, 2000. | [29] S. Upadhyay, S.K. Singh, M. Vatsa, and R. Singh, Video authentication using relative correlation information and SVM, In Computational Intelligence in Multimedia Processing: Recent Advances (Springer Verlag) Edited by A.E. Hassanien, J. Kacprzyk, and A. Abraham, 2007 | [30] The Oxford English Dictionary, 2nd Edition, Oxford University, pp. 795-796, 1989. | [31] The Webster's New 20th Century Dictionary. | [32] Adil Hauzia, Rita Noumeir (2007) Methods for image authentication: a survey. In: Proceedings of the Multimedia Tools Appl (2008) 39:1-46, DOI 10.1007/s11042-007-0154-3 | [33] H. Farid, "Image forgery detection," IEEE Signal Process. Mag., vol.26, no. 2, pp. 16–25, Mar. 2009. | [34] J. Lukas and J. Fridrich, "Estimation of primary quantization matrix in double compressed JPEG images," presented at the Digital Forensic Research Workshop, Cleveland, OH, Aug. 2003. | [35] A. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images," IEEE Trans. Signal Process., vol. 53, no. 10, pp.3948–3959, Oct. 2005. |