Video Authentication- An Overview

Saurabh Upadhyay[*], Sanjay Kumar Singh[†]

*Associate Professor, SIT, Gujarat
s4upadhyay@gmail.com
[†]Associate Professor, IT BHU, Varanasi
[†]sks.cse@itbhu.ac.in

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 broadly classified into four categories: digital signature based techniques, watermark based techniques, intelligent techniques and other techniques. Furthermore we give the shortcomings of different categories of video authentication techniques in brief.

KEYWORDS

Video authentication, Fragile watermarking, Digital signature, Intelligent techniques, Tampering attacks

1. INTRODUCTION

Information has always had a great role in our society, in history, as well as today. Its control has always been very significant for the individuals, organizations and for countries too. It can express from a very tiny moment of our life to the history of the universe. In contrast to early days of human society, today we can transmit the information thousands of kilometers within a couple of seconds. This makes a great impact on the development of our society.

Though this immense development in information technology has brought us in the new era of powerful information, but it has also posed some severe challenges related with the information. One of them is credibility of the information.

In today's digital era, communication and compression techniques facilitate sharing of multimedia data such as image and video [33]. However multimedia editing tools can be used to efficiently and seamlessly alter the content of digital data, thus compromising the credibility of information. The increasing sophistication of computing devices and its equipments have made digital manipulation of video sequences very easy to perform. Ensuring the trustworthiness and integrity of a digital video has become considerably challenging. This is because of one of the significant properties of digital data, i.e., a copy of digital multimedia data behaves the same as the original one.

1.1. Why the video authentication is needed?

In some applications the authenticity of video data is of paramount interest such as in video surveillance, forensic investigations, law enforcement and content ownership [33]. For example, in court of law, it is important to establish the trustworthiness of any video that is used as evidence. As in another scenario, for example, suppose a stationary video recorder for surveillance purpose, is positioned on the pillar of a railway platform to survey every activity on that platform along a side. It would be fairly simple to remove a certain activity, people or even an event by simply removing a handful of frames from this type of video sequences. On the other hand it would also be feasible to insert, into this video, certain objects and people, taken from different cameras and in different time. A video clip can be doctored in a specific way to defame an individual. On the other hand criminals get free from being punished because the video (used as evidence), showing their crime cannot be proved conclusively in the court of law. In the case of surveillance systems, it is difficult to assure that the digital video produced as evidence, is the same as it was actually shot by camera. In another scenario, a news maker cannot prove that the video played by a news channel is trustworthy; while a video viewer who receives the video through a communication channel cannot ensure that video being viewed is really the one that was transmitted [53]. These are the instances where modifications cannot be tolerated. Therefore there is a compelling need for video authentication.

So video authentication is a process which ascertains that the content in a given video is authentic and exactly same as when captured. For verifying the originality of received video content, and to detect malicious tampering and preventing various types of forgeries, performed on video data, video authentication techniques are used.

These techniques also detect the types and locations of malicious tampering. In fact a wide range of powerful digital video processing tools are available in the market that allow extensive access, manipulations and reuse of visual materials[32]. Since different video recording devices and close circuit television camera system become more convenient and affordable option in the private and public sectors, there is a corresponding increase in the frequency in which they are encountered in criminal investigations [34]. The video evidences have significant role in criminal investigations due to their ability to obtain detailed information from their own. And they have tremendous potential to assist in investigations [34]. Therefore it would be necessary to take utmost care to make sure that the given video evidence, presented in the court, is authentic.

2. VIDEO TAMPERING

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 done for several purposes, for instance to manipulate the integrity of an individual. Since a wide range of sophisticated and low cost video editing software are available in the market that makes it easy to manipulate the video content information maliciously, it projects serious challenges to researchers to be solved.

2.1. Video Tampering Attacks

There are several possible attacks that can be applied to alter the contents of a video data. Formally a wide range of authentication techniques have been proposed in the literature but most of them have been primarily focused on still images.

However the basic task of video authentication system is to prove whether the given video is tampered or not. But in several applications, due to large availability of information in video

sequences, it may be more significant if the authentication system can tell where the modifications happened (It indicates the locality property of authentication) and how the video is tampered [5]. On considering these where and how, the video tampering attacks can have different classifications. A lot of works have been done that briefly address the classification based on where [33], [5]. And some papers address the classification based on how [36]. In general, finding where the multimedia data is altered is more efficient than to find out how the multimedia data is tampered.

When a video is being recorded by a video recording device, 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 recording device in a second depends on the hardware specification of the device. Thus a video sequence can be viewed as a collection of consecutive frames with temporal dependency, in a three dimensional plane, as shown in Figure1.

Figure1.

This is called the regional property of the video sequences. When a malicious alteration is performed on a video sequence, 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. A continuous video sequence 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 is modification vector then the tampered video would also be a scalar real valued function of spatial dimensions x and y and time t as follows:

Therefore based on the regional property of the video sequences, we can broadly classify the video tampering attacks into three categories: spatial tampering attacks, temporal tampering attacks and the combination of these two, spatio-temporal tampering attacks [5].

3. AUTHENTICATION TECHNIQUES

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]. Another definition of authentication is to prove that something is "actually coming from the alleged source or origin" [31].

A video authentication system ensures the integrity of digital video and verifies that whether the given video has been tampered or not. But in most of the cases, especially in the court of law, it may be more beneficial if the authentication system can tell where the tampering happens and how the video is tampered.

A typical video authentication system is shown in figure 2. For a given video, authentication process starts with feature extraction. After that, with a specific video authentication algorithm, the authentication data H is generated using the feature f of the video. This authentication data H is encrypted and packaged with the video as a signature or alternatively it can be embedded into the video content as a watermark. The video integrity is verified by computing new authentication data H` for the given video. 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 considered as tampered video. An ideal video authentication system, to be effective, must support the properties such as sensitivity to malicious alteration, localization and self recovery of altered regions, robustness to normal video processing operations, tolerance against some loss of information, compactness of authentication data, sensitivity against false intimation and computational feasibility. In fact in addition to having robustness against benign operations, an ideal video authentication system must make a given video resistant against all possible attacks and must verify whether a given video is tampered or not. Benign operations are those video processing operations that do not modify its content semantically such as geometric transformations, image enhancements and compression. Once the verification is done for the given video, it would be useful to find where and how the tampering has been done.

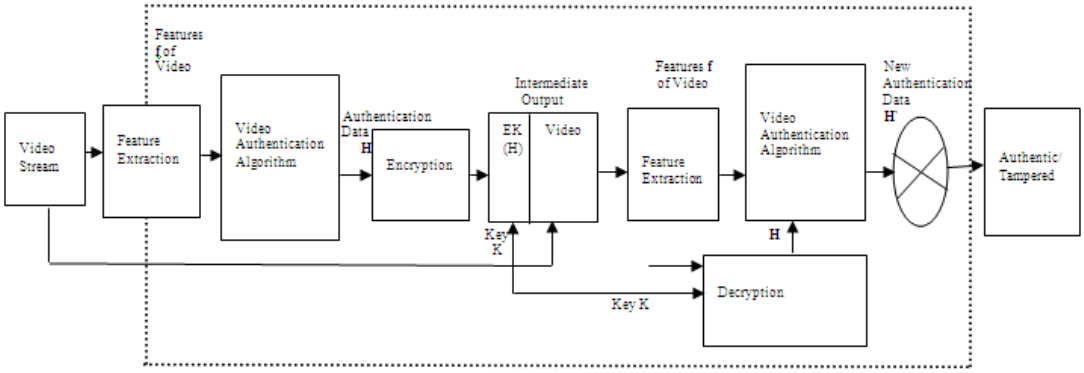

Figure2. A Typical Video Authentication System

However, based on the objectives of authentication, an authentication system can be categorized as complete verification system and content verification system. Techniques that are proposed

for complete verification consider that the multimedia data, which is to be authenticated, have to be exactly the same as the original one. Content verification is a characteristic of multimedia data authentication.

3.1. Classification of Authentication Techniques

In past few years, watermarking and digital signatures have been widely used for the purpose of video authentication. Different techniques have their own advantages and shortcomings. In fact fragile watermarking and digital signatures are the two commonly used schemes for authentication.

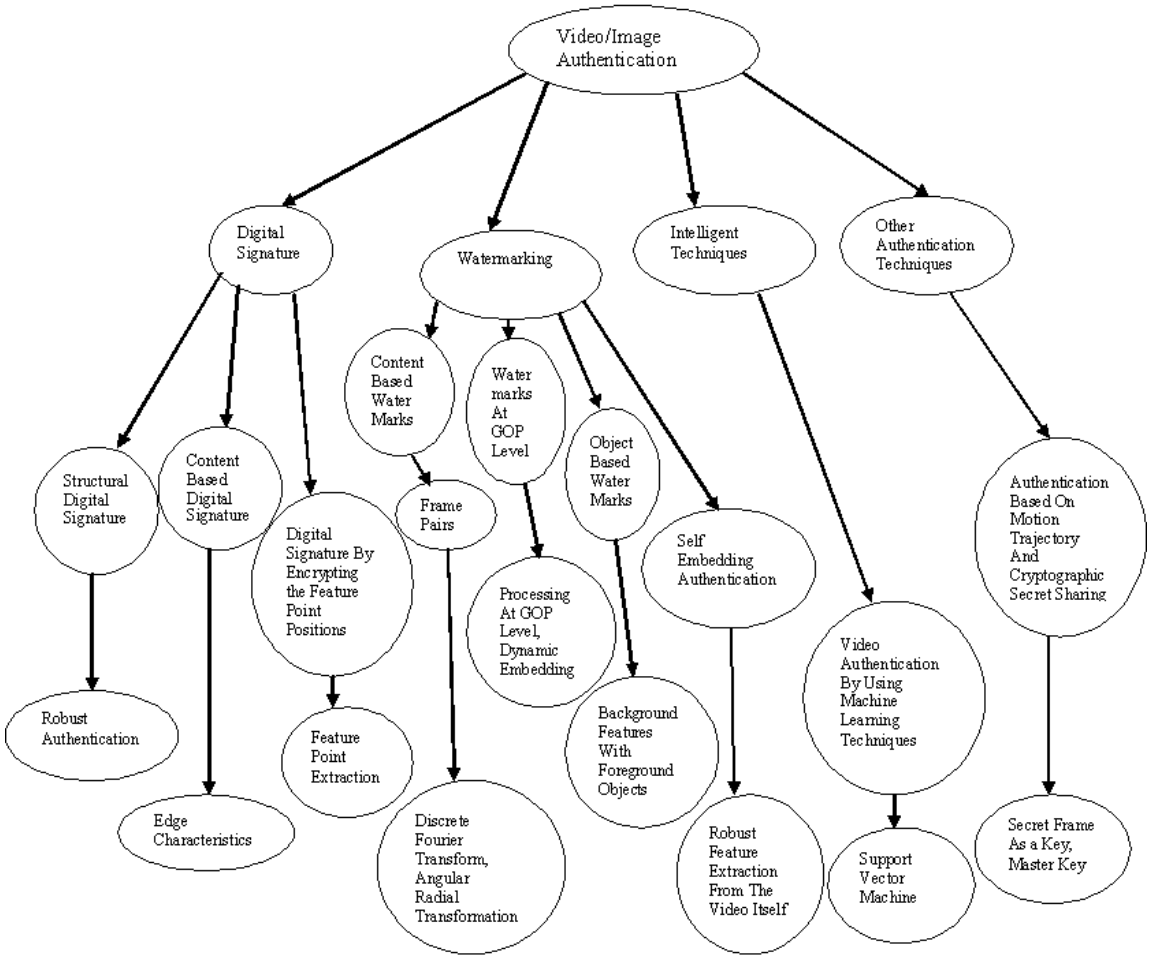

Figure3. Tree Structure of Authentication Techniques

Fragile watermarking embeds the authentication data into the primary multimedia sources, while digital signature stores the authentication data separately, either in user defined field, as like, in the header of MPEG sequence, or in a separate file [5]. Moreover there also have been works on intelligent techniques for video authentication [33, 45]. Intelligent authentication techniques use learning based techniques for authentication purpose. Apart from these digital signature, fragile watermarking and intelligent techniques, some other authentication techniques are also

introduced by researchers, which are specifically designed for various cases of malicious attacks. Basically video authentication techniques are broadly classified into four categories: Digital signature based techniques, watermark based techniques, intelligent techniques, and other authentication techniques. Figure.3. represents a tree structure of authentication techniques which have been commonly proposed for the purpose of video/image authentication.

3.1.1. Digital Signature

Integrity of multimedia data can be greatly verified by digital signature. For the authentication of multimedia data, it was first introduced by Diffie and Hellman in 1976[26]. For the purpose of authentication, digital signatures can be saved in two different ways. Either they can be saved in the header of the compressed source data, or it can be saved as an independent file. Further they can be produced for verification. In the prospective of robustness, since the digital signature remains unchanged when the pixel values of the images/videos are changed, they provide better results. In the digital signature authentication, 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]. Hence, the digital signature cannot be forged, and the end user can verify a received multimedia data by examining whether the contents of data match the information conveyed in the digital signature. In fact digital signature can be used to verify the integrity of multimedia data which is endorsed by the signer.

In [8], two types of robust digital signatures are used for video authentication in different kinds of situations. The first type of authentication signature is used in situation where the GOP (Group of Pictures) structure of the video is not modified, after transcoding or editing processes. The situation, where the GOP structure is modified and only the pixel values of picture are preserved, a second type of digital signature is used.

In another work, video authentication is done by generating digital signatures for image blocks and using them as watermarks [3]. In this approach localization packet, watermark insertion is done via LSB modification of pixel values. As compared to [2] where video tampering is identified through an analysis of watermark sequencing, here (explicit) block ID's are used for this purpose.

The Johns Hopkins University Applied Physics Laboratory (APL) has developed a system for authentication of digital video [7]. The authentication system computes secure computer generated digital signatures for information recorded by a standard digital video camcorder. While 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 separated into individual frames and three unique digital signatures are generated per frame-one each for video, audio and (camcorder) control data- at the camcorder frame rate.

Here the key cryptography is used. One key, called a "private" key is used to generate the signatures and is destroyed when the recording is complete. The second a "public" key is used for verification. The signatures that are generated make it easy to recognize tampering. If a frame has been added it would not have a signature and will be instantly detected and if an original frame is tampered the signature would not match the new data and it will be detected in verification process.

In digital signature based video authentication schemes, different features are used for different applications. Ditmann [17] and Queluz [18] used the edge /corner of the image as the feature to generate the digital signature. They claimed this feature is robust against high quality

compression and scaling but the problem is that the signature generated based on the edge is too long, and the consistency of the edge itself is also a problem. Formally digital signature based authentication techniques are able to detect regions that have been tampered, 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. The characteristic of the SDS is that it can tolerate content preserving modifications while detecting content changing modifications. 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 which are able to both protect the integrity of the message and prevent the signer's repudiation.

In another technique, a separate authentication code is written in [43] from the blocks of the video frames. Here the authors Po-Chyi Su, Chun Chieh Chen and Hong Min Chang 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. The authentication code chosen by authors is sensitive to malicious modifications of video data. The proposed work also considers two classical false detection tests. These are false alarms and misses. In the situation of former false detection test, the authentication scheme wrongly signals a happening of tampering while the normal video processing operations are there. In the later situation, false detections are related to misses of detection after an actual tampering on video content has been performed. This work is resilient to lossy compression procedures, while the tampered regions on the video frames can be located if malicious attacks were applied [43]

Navjit Saikia and Prabin K. Bora present a scheme for video authentication in [44] that generates the message authentication code (MAC) for a group of frames (GOF) using coefficients from the last but one high pass band at full level of temporal wavelet decomposition. This digital signature based scheme uses temporal wavelet transform for the generation of message authentication code. After the extraction of GOFs from the video, these GOFs are recursively decomposed into high pass band up to a certain level using temporal wavelet transform [46]. At this level the high pass band consists of two frames. In the signature generation process, these frames are divided into some blocks of fixed sizes. These blocks are randomly mapped on to a set of groups, using a mapping key in such a way that each group contains equal number of blocks. With the transform coefficients and these groups of blocks, a set of linear combination values is evaluated for each frame in the high pass band. And with these sets of linear combination values, message authentication code (MAC) is obtained for the GOF. In the signature verification process, the distances d ($MAC_{i,1}$, $MAC`_{i,1}$) and d($MAC_{i,2}$, $MAC`_{I,2}$) are calculated where d is any distance measure and { $MAC_{i,1}$, $MAC_{i,2}$ } is the MAC of i^{th} GOF of the original video and {$MAC`_{i,1}$, $MAC`_{i,2}$} is the MAC of corresponding GOF calculated at receiver site. Here the GOF of the video would be authentic if these two distances are below some predefined threshold values, otherwise tampered. When all GOFs in it are found authentic then the given video is declared as authentic video. This authentication scheme would be

advantageous for spatio-temporal manipulations, since it is effective for spatial tampering as well as for temporal tampering.

Similar to Dittmann's [17] content based digital signature approach for image/ video authentication using edge characteristics, Bhattacharjee and Kutter [25] proposed a scheme to generate a digital signature by encrypting the feature points 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

Watermarking always remains a significant issue for solving authentication problems regarding digital multimedia data, in past few years. A wide variety of watermark based authentication techniques have been proposed by various researchers in literature. However watermarking techniques can be used for authenticating various multimedia data, but most of the work has been done for image and video authentication. Based on the application areas, watermarking can be classified in different categories [36]. Besides ensuring 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 [39], 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 [39].

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 have created problems associated with copyright protection and authentication. One of the main advantage of digital world is that here perfect copying is performed easily. That causes severe security related issues. The owners or producers of information resources are being worried of releasing proprietary information to an environment that appears to be lacking in security [40]. On the other hand with the help of powerful video editing software one can challenge the trustworthiness of digital information. In [40], M. P. Queluz presents the generic models with labeling and watermarking approaches for content authentication, in which existing techniques for content authentication are described and compared. In labeling based approach authentication data are written in separate file [40], 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, say *Complementary Information*, about the frame and its author, assigned by an author society. Besides image-dependent features, the label can also convey this information. In the authentication system the corresponding public key Kpu is used to decrypt the label, producing:

$$C, C_I = EKpu(L)$$

Moreover in [40] M. P. Queluz presents two classical image features for image/video content authentication. The first image feature is concerned with second order image moments. It has a less computational requirement with small memory which makes it more advantageous computational feature. The second feature relies on image edges and it takes the problem of image/video authentication from a semantic, higher level point of view [40]. In image moments feature, for a two dimensional continuous function *f(x, y)*, the moments of order (p+q) is defined as

$$m_{pq} = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} x^p \, y^q \, f(x,y) \, dx \; dy \qquad \text{For p, q=0, 1, 2, ……}$$

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 $\sum_i \sum_j f(i,j)$. He also presents a brief comparison of labeling approach with watermarking for tamper detection, which is independent of applications where they can specifically be implemented. The video authentication techniques using the watermarking approach have wide dimension in the literature. For the authentication of H.264 compressed video stream, which provides high compression efficiency and compression quality, Tsong-Yi Chen et al [15], proposed a system in watermark authentication code is used at Block Sub-band Index and Coefficient Modulation to embed in the quantized AC coefficient of I frame. For verifying the integrity of live H.264 encoded video bit stream, Razib Iqbal et al [55] proposed an authentication scheme which utilizes MPEG-21 gBSD for hard authentication in the compressed domain. The scheme uses content based authentication data which is derived from a hash value and embeds a fragile watermark [55].

For the robust digital video authentication, Aaron T. Sharp et al proposed [56] an authentication scheme which watermarks motion vectors in the video stream. The proposed method is not computationally complex, produces almost no visual distortion, and can be accomplished in real time [56]. Some of the authentication techniques implement watermarks that are invisible and robust, but they do not take the advantage of video specific properties [57, 58]. These systems often perform some sort of manipulation on a single frame and are generally computationally intensive [57, 58].

In [41], Chang-yin Liang, Ang Li and Xia-mu Nin proposed a video authentication system which is robust enough to separate the malicious attack from natural video processing operations with the cloud watermark. The authentication system in [41] first of all splits the video sequence into shots and extracts the feature vector from each shot. Then the extracted feature is used to generate watermark cloud drops with a cloud generator [41]. Here, for robustness, a con tent based and semi fragile watermark is used for authentication. In this authentication technique DCT coefficients are evaluated firstly by partially decoding the given video. After watermarking the video is encoded again [41].

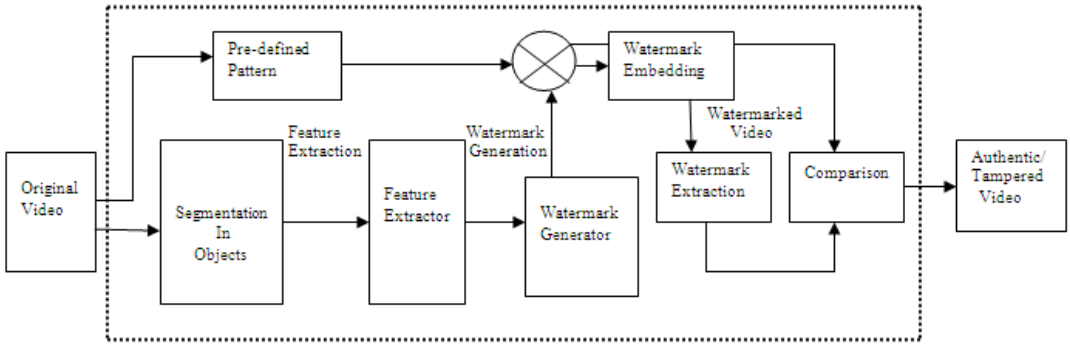

Figure4. A Watermarking Based Authentication System

Invariable features of the video are selected for content based watermarking. The watermarks are then embedded back into DCT coefficients of the video. The extracted watermarks are compared with the features derived from the received video, to check the authenticity of the given video.

Figure 4 shows a video authentication system that uses watermark to verify the integrity of the video. In this system, the given video is first segmented into objects. According to spatial content of the video, feature extractor extracts the feature of the video.

After feature extraction, watermark generator generates the watermark according to features and embeds the watermark into video. At the receiving site, video encoder extracts the watermark from the video. If this watermark matches the original watermark, the given video is claimed as authentic. However attacks on watermarks may not necessarily remove the watermark [28], but can disable its readability. Image/video processing operations and transforms are commonly employed to create and apply watermarks on the multimedia data. These techniques can also be used to disable or overwrite watermarks. Multiple watermarks can be placed in an image and one cannot determine which one is valid [29].

In [2], the proposed algorithm explains the frame-pair concept where one video frame would watermark another frame downstream based on a specific sequencing and a key. Basically in this approach three points are there: First the watermark is derived from the video itself, therefore cannot be pirated. Second if video frames are taken out, it is possible to identify their locations by simply monitoring the breaks in authentication key sequence. And third, video frames that are removed could actually be recovered because frame pairs contain copies of other frames disguised as watermarks. In this approach unless both frames are removed, frame restoration is possible. Watermarking can also be used for the authentication of compressed video [4]. Here the watermarking of compressed video [4] is done by identifying label carrying VLCs in MPEG-2 bit stream. In this approach every bit in the watermark payload is compared with the LSB of the current label carrying VLC. If they are the same, the VLC remains unchanged, if they are not, the LSB is replaced by the watermark bit. The embedded watermark may be used for the authentication of video and protection against tampering.

For the authentication of MPEG video, authentication data can be embedded at the group of pictures (GOP) level [5]. Since it is almost infeasible to embed information in all pictures of a

video clip or embed all the information for each picture in a video clip, Dynamic Embedding for each picture in a digital video can be adopted [5]. In this approach current GOP's authentication data (bits) are embedded into next GOP. Basically this approach has three advantageous features. First, by making each watermarked GOP dependent upon other GOP, the problem of watermark counterfeiting becomes computationally impossible and thus reduces the chances of success for the attackers. Second, for MPEG video, if watermark is added in I picture in a GOP, it results in drift errors for the following P or B pictures in the same GOP. If the video quality requirement is in demand, the drift errors should be corrected, the correction could cause the changes of the authentication bits and thus need to re-add the watermark in I picture. This will cause dead loop. Therefore it would be advantageous to embed the authentication data at the GOP level. Third, this operation is causal and saves much memory to store a GOP's data.

For the investigation of the authenticity of uncompressed video signal, the quality of digitization process is considered significantly [6]. The way the A/D conversion is done is important for the result. For this purpose the histogram of gray values can be checked. Previously Lin et al [8] and Peng et al [9] have worked on compressed domain schemes that are robust against transcoding and editing operations. For computing the signature Lin [8] used the difference in DCT coefficients of frame pairs. Since the value of DCT coefficients can be modified keeping their relationship preserved, it is vulnerable to counterfeiting attacks. Peng [9] used DC-DCT coefficients as features to build watermark.

An object based watermarking scheme for video authentication is proposed by Dajun et al [11]. They use background features to embed the watermark into foreground objects to establish a relation between background and the foreground of a video. Here the raw video is segmented into foreground objects and background video, the watermark is generated by using the features extracted from both the foreground and background. The watermark is then embedded into foreground objects, so that a secure link between foreground objects and the back ground is created. At the receiving end integrity between the foreground objects and the background can be verified by comparing two sets of codes: one is the watermark extracted from the objects and the other is regenerated from both the received object and the background. If these two sets of codes are the same, then the video is claimed as authentic.

A more robust authentication scheme for scalable video streaming by employing Error Correction Coding (ECC) in different ways [14] has also been produced. This scheme achieves an end - to-end authentication independent of specific streaming infrastructure. Actually this scheme is an extension from [16] where a semi fragile authentication framework, for images in terms of ECC and public key infrastructure, is used.

In another work, a semi fragile object based authentication solution is produced for MPEG 4 video [42]. To protect the integrity of the video objects /sequences, a content based watermark is embedded into each frame in the Discrete Fourier Transform domain before the MPEG 4 encoding. A set of angular radial transformation (ART) coefficients are selected as the robust features of the video objects. Error Correction Coding (ECC) is used for watermark generation and embedding. The main difference between the frame based video application and the object based video application lies in the utilization of the shape information.

In a self embedding authentication system [24], a robust and important feature of the video is extracted and embedded in to the video at the sending site; the detector retrieves this original feature from the watermark and compares it with the feature extracted from the received video to determine the authenticity of the video. If the difference exceeds a threshold, the received video

will be claimed as un-authentic video. Chen et al [54], proposed a watermarking scheme for video authentication specially targeted at surveillance applications.

3.1.3. Intelligent Techniques

Intelligent techniques for video authentication use database of video sequences. The database comprises authentic video clips as well as tampered video clips. As in [33], 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 [33] 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 [33] computes the local relative correlation information and classifies the video as tampered or non-tampered. Performance of this algorithm is not affected by acceptable video processing operations such as compression and scaling. Here the algorithm uses Support Vector Machine (SVM) for the classification of the tampered and authentic videos. SVM [47] is a powerful methodology for solving problems in non linear classification, function estimation and density estimation [48]. In fact SVM is a non linear classifier that performs classification tasks by constructing hyper planes in a multi dimensional space and separates the data points in different classes. This algorithm [33] is performed in two stages: (1) SVM training and (2) Tamper detection and classification, using SVM. In SVM training, the algorithm trains the SVM by using a manually labeled 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 [49]. 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 m 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 the SVM. With this information of all the video in video database the SVM [47] 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 [45], 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 there 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 firstly 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. For a particular video shot, in figure 5, vertical axis indicates the histogram energy of each frame of the shot and the horizontal axis marks the frame number in the shot. A polyline belonging to the video shot is drawn which is a motion trajectory. This figure also shows the process of key frames extraction from the video shot.

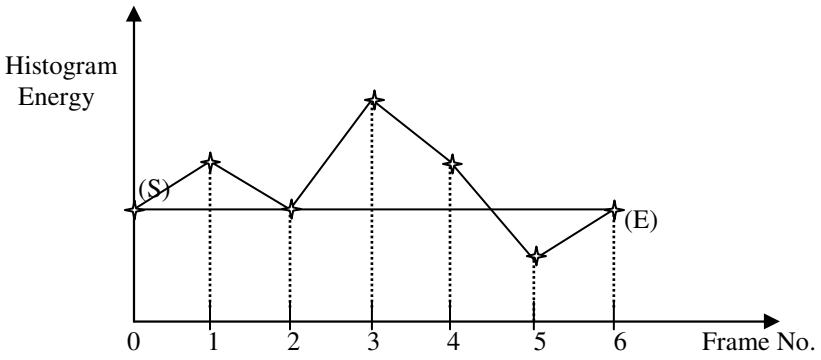

Figure5. Frames with their histogram energy for a video shot.

The starting frame S and the last frame E of the trajectory are connected to each other. Then a distance d between each frame point and this line is computed by using:

$$d = \frac{|Ax+By+C|}{\sqrt{A^2+B^2}}$$

Where d is the distance from a point (x, y) to the straight line $Ax + By + C = 0$.

After that the point at the maximum distance from the line is chosen and the corresponding frame is declared as one of the key frames in this shot. Once the key frames are computed these are utilized to compute the secret frame by extrapolation as shown in Figure 6. Here the x coordinate indicates the locations of the key frames for the purpose of computing the polynomial for secret sharing and the y coordinate indicates the value of the pixels of each frame [19]. Now an interpolating polynomial $f(x)$ is computed by using key frames as follows.

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

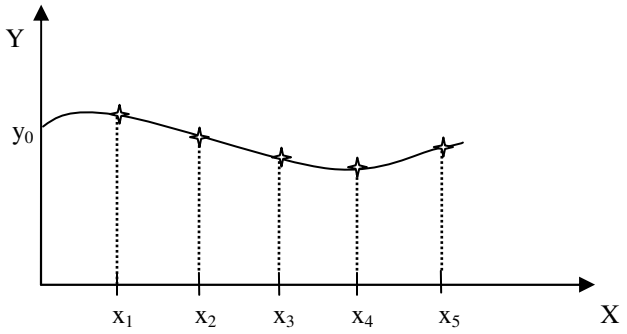

Figure6. Secret Frame Extrapolation.

This is Lagrange interpolation formulation where the x_i position refers to each key frame and I_i 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:

$$sim = \frac{I_O \cdot I_N}{|I_O \cdot I_N|}$$

Where I_O and I_N are the original master key and the new master key considered 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. Here the authors also claim that if the similarity value is high then the video has undergone benign transformations. But if the similarity value is low, then the video must have undergone some significant tampering. In [20], the key frames are selected by deleting the most predictable frame. In the approach of reference [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 [37] Weihong Wang and Hany Farid have 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 a MPEG video sequence, there are three types of frames: *I*-frame, *P*-frame and *B*-frame. Each with different level of compression occurs in a periodic sequence in the MPEG video. Amidst all the frames *I*-frames are the highest quality frames of the video sequence, which are usually encoded by standard JPEG compression scheme. In the *I*-frame, compression is achieved at spatial level by reducing spatial redundancies within a single frame [37]. Temporal redundancies are concerned with *P*-frames arcos the frames of video sequence. For achieving double MPEG compression, *I*-frames of the MPEG video sequence are compressed twice. For this purpose when the frames are double quantized with different step size, there is a significant difference in their histogram. When the step size decreases in image quantization, some bins in the histogram are empty while in greater step size some bins of the histogram contain more samples than their neighboring bins [37]. In both cases of double quantization, periodicity of the artifacts is introduced in to histograms. This artifact would be used as evidence of double compression and hence tampering. In temporal analysis, addition or deletion of frames from a video sequence and re-encoding the resulting sequence, results in a large motion error between consecutive *P*-frames of the video, since they originated from different GOPs. Moreover this increased motion error would be

periodic, occurring throughout each of the group of pictures following the frame deletion or addition. Periodic spikes in the motion error indicate tampering [37].

In [38] 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 with a distance to each other that is proportional to the differences in their pixel colors [38]. 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.

A robust video authentication system should tolerate the incidental distortion, which may be introduced by normal video processing such as compression, resolution conversion and geometric transformation, while being capable of detecting the intentional distortion, which may be introduced by malicious attack. There has also been some work for scene change detection of video sequences in the literature.

4. CHALLENGING SCENARIOS FOR VIDEO AUTHENTICATION

In some of the surveillance systems storage and transmission costs are the important issues. In order to reduce the storage and transmission cost only those video clips containing objects of interest are required to be sent and stored. Moreover in most of the surveillance applications, background object changes very slowly in comparison to foreground objects. A possible efficient solution in these scenarios is that only the objects of interest (mostly foreground objects) are sent out frame by frame in real time while the background object is sent once in a long time interval. In such surveillance applications, it becomes very important to protect the authenticity of the video: the authenticity against malicious alterations and the authenticity for the identity of the transmission source (i.e. identify the video source). In event based surveillance systems, the video sequences are captured when there is any kind of change in the scene (existence of an event) which would be captured by the camera. If there is uniformity in the scene in such a way that there is not any change in the scene then the surveillance camera does not capture any video sequence. This kind of surveillance system is used in military system for border security purpose. Authenticity for this kind of video sequences is a challenging issue because there is no proper time sequence in video sequences which are captured by surveillance camera.

S. N.	Video Authentication Techniques	References	Work
1.	Digital Signature	8	Two digital signatures for different conditions of manipulations
		3	Digital signatures are generated for image blocks and used as watermark.
		7	An authentication system, which computes secure computer generated digital signatures for information recorded by a standard digital video camcorder.
		17, 18	Digital signature generated by feature(edge/corner) extraction
		23	Structural digital signature for robust authentication
		25	Digital signature by encrypting the feature points positions in an image.
		12,13	Protection of the integrity of the message and prevent the signer's repudiation.
		43	Authentication Technique with the approach of scalar/vector quantization on the reliable features, also considers two classical false detection tests for robustness. These are false alarms and misses.
		44	This digital signature based scheme uses temporal wavelet transform for the generation of message authentication code.
2.	Watermarking	2	Frame-pair concept where one video frame would watermark another frame downstream based on a specific sequencing and a key.
		4	The watermarking of compressed video is done by identifying label carrying VLCs in MPEG-2 bit stream.
		5	Watermark embedded at the group of pictures (GOP) level.
		9	DC-DCT Coefficients are used as features to build watermarks.
		11	Background features are used to embed the watermark into foreground objects to establish a relation between background and the foreground of a video
		39	Introducing video authentication template, which uses a bubble random sampling approach applied for synchronization and content verification in the context of video watermarking
		40	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.
		41	Splits the video sequence into shots and extracts the feature vector from each shot. Then the extracted feature is used to generate watermark cloud drops
		14	Robust authentication scheme for scalable video by employing Error Correction Coding (ECC) in different ways
3.	Intelligent Authentication Techniques	33	Algorithm uses Support Vector Machine (SVM) for the classification of the tampered and authentic videos
		81	Integration of the learning based support vector machine classification (for tampered and non tampered video) with singular value decomposition watermarking.
3.	Other Authentication Techniques	38	Three techniques to expose digital forgeries.
		19	Video authentication based on motion trajectory and cryptographic secret sharing
		21	For the authentication, the key frames are extracted from a video Shot based on the nearest feature line.

In another scenario where a surveillance camera is recording the postmortem activity of a human body in postmortem house, any kind of disturbance in recording (due to electricity problem or some other hardware problem) would be resulted in frame dropping. This would be a severe issue since some important activities may have happened during frame dropping and these activities may have been missed to be recorded by surveillance camera. Authentication of this kind of video sequence is also a very challenging task because we are not in the condition of detecting all the positions where and how many frames have been dropped. These all are the different scenarios which pose considerable challenges for the authentication purpose.

5. SUMMARY

Figure 3 presents a tree structure of the authentication techniques that can be used for video authentication. The four children node of the root node covers almost all the methodologies that can be used for video authentication purpose. The leaf nodes of the tree structure show the key points of their grandparent node methodologies. This tree structure shows how all the methodologies use different approaches for video authentication. Table1 depicts a succinct view of classification of all the work that has been done for video authentication. All the works are classified into methodologies used for authentication purpose. All described methods can detect malicious manipulations. Moreover, most of them are robust against content preserving manipulations. According to this summary table most of the algorithms are quite similar in performance. However most of the work has been done in watermarking and digital signature methodologies, other techniques (including intelligent technique) also produce better results for authentication purpose. There is no issue related with the size of authentication code in digital signature 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 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 [33].

In addition of these techniques, intelligent techniques explore the new dimensions in video authentication. However learning based intelligent authentication algorithm does not require computation and storage of any key or embedding of secret information in the video data, it requires a large enough database of tampered and non tampered video to learn the algorithm 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

Video authentication is a very challenging problem and of high importance in several applications such as in forensic investigations of digital video for law enforcement agencies, video surveillance and presenting video evidence in court of law. However with growing development in video editing tools and wide availability of these powerful editing software, video tampering attacks explores new dimensions in various fields. It becomes difficult to deal with the authenticity of raw video sequences. If we are having only a raw captured video without any watermark or any kind of digital signature, then it is difficult to authenticate that video with the help of watermark based or digital signature based authentication techniques. In this situation we cannot compute and match any pre embedded watermark or pre generated digital signature. Therefore watermark and digital signature based techniques are helpless in this situation.

Intelligent authentication techniques can perform better, however, in this scenario. With the help of intelligent authentication techniques we can establish a frame by frame relation (by using any statistical feature of the frame such as edges or corner points in the frame) for a particular video and learn whether the processed video is tampered or authentic. Following this procedure with a vast sample data (a vast database of tampered and non tampered video sequences) and using a non linear classifier such as SVM, we can establish a kernel in a hyper dimensional plane that can classify whether the given video is authentic or not. Intelligent techniques perform better in the case of authenticating a raw compressed video, since these techniques do not need any computation or storage of key. Major drawback with the intelligent techniques is that, for even a single kind of attack, they need a sufficient large amount of databases of tampered and authentic video sequences to learn. That makes these techniques a little bit slower in comparison to other techniques.

In section 4 we have introduced new challenging scenarios where the conventional authentication techniques might not perform well. For these kinds of challenging situations specific and efficient authentication algorithm must be developed. However specifically designed algorithm cannot be generalized for all kinds of tampering attacks. In future it is going to be a big menace for information security. By analyzing the various video authentication techniques that were presented in this paper we can say that the authentication techniques are specific to the applications (surveillance, entertainment industry, medical, copyright...). In most of the applications robustness is more significant i.e., there is a need to tolerate some content preserving manipulations such as compression, filtering and geometrical transformations against malicious manipulations. A perfect video authentication algorithm that detects all kinds of malicious manipulations and that can tolerate all content preserving manipulations is yet to be discovered. We can hope for better in the future.

REFERENCES

[1]. B.G Mobasseri, M.S.Sieffert, R.A.Simard, Content Authentication and tamper detection in digital video, Proc. IEEE International conference on Image Processing, Vancouver, September 10-13, 2000.

[2]. B.G.Mobasseri, A.E.Evans, Content dependent video authentication by self water marking in color space, Proc. Security and watermarking of multimedia contents III, vol. 4314 pp.35-46, January 21-26, 2001.

[3]. M.V. Celik et al, Video authentication with self recovery, Proc. Security and watermarking of multimedia contents IV vol. 4314, pp. 531-541, January 21-24, 2002.

[4]. Daniel Cross, B.G. Mobasseri, Water marking for self authentication of compressed video, Proc. IEEE International Conference on Image Processing, Rochester, NY, September 22-25, 2002

[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]. Zeno j. Geradts, Jurrien Bijhold, Forensic Video investigation with real time digitized uncompressed video image sequences p. 154-164, Investigation and Forensic Science Technologies

[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]. Peng, Heather, A semi fragile water marking system for MPEG video authentication, ICASSP 2002, Orlando.

[10]. Pradeep K. Atrey, Wei-Qi Yan, Ee-Chien Chang, Mohan S. Kankanhalli, A hierarchical signature scheme for robust video authentication using secret sharing.

[11]. Dajun He, Oibin Sun, Oi Tian, A semi fragile object based video authentication system IEEE ISCAS 2003, Bangkok.

[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]. Qibin Sun, Dajun He, Zhishon Zhang and Qi Tian, A secure and robust approach to scalable video authentication ICME2003.

[15]. Tsong-Yi Chen, Thou-Ho Chen, Yin-Ting Lin, Yin-Chan Chang, Da-Jinn Wang, H.264 Video authentication based on semi fragile watermarking, DOI 10.1109/IIH-MSP, 2008 IEEE.

[16]. Qibin Sun, Shih-Fu Chang and K. Mean, A new semi fragile image authentication framework combining ECC and PKI infrastructure, ISCAS 2002, Phoenix, May 2002.

[17]. Titman, 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]. Queue, 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]. Martinian, E.; Wornell, G. W.; and Chen, B., Authentication with Distortion Criteria, Submitted to IEEE Trans. Information Theory.

[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]. Neil F. Johnson, An Introduction to watermark Recovery from Images, Center for Secure Information System, George Mason University, Fair Fax, VA 220304444

[29]. S. Craver, N. Memon, B. Yeo and N. M. Yeung, Resolving Rightful Ownerships with Invisible watermarking Techniques: Limitations, Attacks and Implications, IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, pp. 573-586(1998).

[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]. 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

[34]. Law Enforcement/Emergence Services Video Association (LEWA)

[35]. Pramateftakis, A., Oelbaum, T., Diepold, K. (2004).Authentication of MPEG-4-based surveillance video. Proceedings of IEEE International conference on Image Processing, 1, 33-37.

[36]. 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.

[37]. Weihong Wang , Hany Farid, Exposing digital forgeries in video by detecting duplication, Proceedings of the 9th workshop on Multimedia & security, September 20-21, 2007, Dallas, Texas, USA

[38]. Hany Farid, Digital doctoring: How to tell the real from fake, Significance, 3(4): 162-166, 2006

[39]. Fabrizio Guerrini, Reccardo Leonardi and Pierangelo Migliorati A new video authentication template based on bubble random sampling, Proc. of the European Signal Processing Conference 2004

[40]. M.P. Queluz, Authentication of Digital Images and Video: Generic Models and a New Contribution, Signal Processing: Image Communication, Vol.16, pp. 461-475, January 2001.

[41]. Chang-yin Liang, Ang Li, Xia-mu Niu Video authentication and tamper detection based on cloud model, Proceedings of the Third International Conference on International Information Hiding and Multimedia Signal Processing (IIH-MSP 2007), p.225-228, November 26-28, 2007.

[42]. Dajun He, Qibin Sun, and Qi Tian: A semi-fragile object based video authentication system. ISCAS (3) 2003: 814-817.

[43]. Po-chyi Su, Chun-chieh Chen and Hong Min Chang, Towards effective content authentication for digital videos by employing feature extraction and quantization, IEEE Transactions on Circuits and Systems for Video Technology Volume 19 , Issue 5 (May 2009), p: 668-677, 2009.

[44]. Navajit Saikia, Prabin K. Bora, Video Authentication Using Temporal Wavelet Transform, adcom, pp.648-653, 15th International Conference on Advanced Computing and Communications (ADCOM 2007), 2007.

[45]. 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 .

[46]. C. I. Podil chuk, N. S. Jayant, and N. Farrardin, Three dimensional sub band coding of video IEEE Trans. Image processing vol. 4 no. 2, 1995, pp.125-139

[47]. Vapnik VN (1995) The nature of statistical learning theory. Springer Verlag.

[48]. 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
.

[49]. Kovesi PD (1999) Image features from phase congruency. Videre: Journal of Computer vision research, MIT Press 1(3).

[50]. Kundur, D., Implications for high capacity data hiding in the presence of lossy compression, Information Technology: Coding and Computing, 2000, Proceedings. International Conference on, 27-29 March 2000, Page(s): 16 -21

[51]. Watson, A.B., Visually optimal DCT quantization matrices for individual images, Data Compression Conference, 1993. DCC '93, 30 March-2 April 1993, Page(s): 178 -187.

[52]. Bloom I., Cox I. and Kalker T. Copy Protection for DVD Video. Proceedings of lEEE, July, 1999, 87, 7

[53]. P.K. Atrey, W. Yan, and M.S. Kankanhalli, A scalable signature scheme for video authentication, presented at Multimedia Tools Appl., 2007, pp.107-135.

[54]. S. Chen and H. Leung, Chaotic watermarking for video authentication in surveillance applications, *IEEE Trans. Circuits Systems Video Technology,* vol. 18, no. 5, pp. 704-709, May 2008 .

[55]. Razib Iqbal, Shervin Shirmohammadi and Jiying Zhao, Compressed Domain Authentication of Live Video, IEEE International Conference on Signal processing and communications (ICSPC 2007) 24-27 November 2007, Dubai, United Arab Emirates.

[56]. Aaron T. Sharp, James Devaney, Austin E. Steiner, Dongming Peng, Digital Video Authentication with motion vector watermarking, 978-1-4244-7907-8/10, 2010 IEEE.

[57]. Bandyopadhyay, P.; Das, S.; Paul, S.; Chaudhuri, A.; Banerjee, M., A Dynamic Watermarking Scheme for Color Image Authentication, Advances in Recent Technologies in Communication and Computing, 2009. ARTCom '09. International Conference on, pp.314-318, 27-28 Oct. 2009.

[58]. Das, S.; Bandyopadhyay, P.; Paul, S.; Ray, A.S.; Banerjee, M.; "A New Introduction towards Invisible Image Watermarking on Color Image," Advance Computing Conference, 2009. IACC 2009.
IEEE International, pp.1224-1229, 6-7 March 2009

Short Biography

Saurabh Upadhyay received the B. Tech. degree in computer science and engineering in 2001 and is currently working toward the Ph.D. degree in computer science at U.P. Technical University, India. He is an Associate Professor in the Department of Computer Science and Engineering, Saffrony Institute of Technology Gujarat, India. He is actively involved in the development of a robust video authentication system which can identify tampering to determine the authenticity of the video. His current areas of interest include pattern recognition, video and image processing, watermarking, and artificial intelligence

Sanjay K. Singh received the Ph.D. degree in computer science from U.P. Technical University, India. From 1997–2007, he was faculty member at Purvanchal University, India. Currently he is a Reader in Department of Computer Science and Engineering at Institute of Technology, BHU, India. He is a certified Novel Engineer and Novel administrator. His research has been funded by UGC and AICTE. He has over 30 publications in refereed journals, book chapters, and conferences. His research interests include computational intelligence, biometrics, video authentication and machine learning. Dr. Singh is a member of IET.