RESEARCH PAPER | Computer Science | Volume : 3 | Issue : 6 | June 2013 | ISSN - 2249-555X

A New Technique for Video Surveillance

KEYWORDS: Authentication, Fragile watermarking, Digital signature, Intelligent techniques.

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 *Video authentication has gained much attention in recent years. However many existed authentication techniques have their own advantages and obvious drawbacks; we propose a novel authentication technique which uses an intelligent approach for video authentication. Our methodology is a learning based methodology which uses SVM (support vector machine) for learning and classification purpose and a video database as sample data. The proposed algorithm does not require the computation and storage of any digital signature or embedding of any watermark. Therefore it works for raw videos (videos captured in any situation), and useful for real life application of authentication. It covers all kinds of tampering attacks of spatial and temporal tampering. It uses a database of more than 1200 tampered and non-tampered videos and gives excellent results with 93.5% classification accuracy.*

1. INTRODUCTION

Digital video authentication has been a topic of immense interest to researchers in the past few years. Authentication of a digital video refers to the process of determining that the video taken is original and has not been tampered with. In some applications the authenticity of video data is of paramount interest such as in video surveillance, forensic investigations, law enforcement and content ownership [3]. For example, in court of law, it is important to establish the trust- worthiness 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 as-sure 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 [6]. 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 con-tent, 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[2]. 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 [4]. 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 [4]. There-fore 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 in-stance 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 [1]. 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 [3], [1]. And some papers address the classification based on how [5]. A video sequence 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 video sequences. When a malicious alteration is per-formed 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. 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 at-tacks and the combination of these two, spatio-temporal tampering attacks [1]. In [13], authors have presented a wide classification of video tampering attacks including the sub classifications of spatial and temporal tampering.

3. PREVIOUS WORK

In last two decades watermark and digital signature based techniques have been widely used for the pur-

Volume : 3 | Issue : 6 | June 2013 | ISSN - 2249-555X

pose of video authentication. Basically fragile watermarking and digital sig-natures are the two commonly used schemes for video authentication [1]. The authentication data is embedded in to the primary multimedia sources in fragile watermarking schemes. While in digital signature based schemes, the authentication data is stored separately either in user defined field, as like, in header of MPEG sequence or in a separate file. In addition of these two techniques, intelligent techniques have also been introduced for video authentication [3, 14]. Intelligent video authentication techniques are basically learning based techniques which use video databases as sample data for the purpose of learning (training) [3, 14]. Apart from these, digital sig-nature, watermarking and intelligent techniques, some other authentication techniques are also introduced by researchers, which are specifically designed for various cases of malicious attacks. Genuinely video authentication techniques are broadly classified in to four categories: Digital signature based techniques, watermark based techniques, intelligent techniques and other authentication techniques. During the authentication process, 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. Since the digital signature remains unchanged when the pixel values of the frames of the video are changed, they provide better results in the consideration of robustness. In the digital signature based schemes, 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 [15]. Hence the digital signature cannot be forged, and the end user can verify the received video data by examining whether the contents of video data match the information conveyed in the digital signature. In fact, in video authentication, the digital signature can be used to verify the integrity of video data which is endorsed by the signer [15].

The Johns Hopkins University Applied Physics Laboratory (APL) has developed a system for digital video authentication [16]. The video 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 transferred from the camcorder in to the digital video authenticator. This video authentication system splits the video in to individual frames and generates three unique digital signatures 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 completed. The second key is a "public" key which 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 the 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 as tampering in verification process.

In last two decades, a wide variety of watermark based authentication techniques have been presented by various researchers in literature. Based on the application areas, watermarking can be classified in different categories [5].

In addition of 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. In watermark based video authentication techniques, generally, watermarks are embedded in digital videos without changing the meaning of the content of the video data. Further they can be retrieved from the video to verify the integrity of video data. Since the watermarks are embedded in the content of video data, once the data is manipulated, these watermarks will also be altered such that the authentication system can examine them to verify the integrity of video data.

Fabrizio et al. use the video authentication template, which uses bubble random sampling approach for synchronization and content verification in the context of video watermarking [17]. The authentication template is introduced in order to en-sure temporal synchronization and to prevent content tampering in video data [17]. The owners or producers of information resources are being worried of releasing proprietary information to an environment which appears to be lacking in security [18]. On the other hand with the help of powerful video editing tools one can challenge the trustworthiness of digital videos. Chang-yin Liang et al introduced a video authentication system which is robust enough to separate the malicious attacks from natural video processing operations with the cloud watermark [19].

Intelligent video authentication techniques use video databases for learning purpose. The database comprises tampered and non tampered video clips. An intelligent technique for video authentication, proposed by M.Vatsa et al, uses inherent video information for authentication [3], thus making it useful for real world applications.

Apart from digital signature, watermarking and intelligent authentication techniques, some other techniques are proposed by various researchers in the literature for the purpose of authentication of digital videos.

Mohan Kankanhalli et al. proposed a video authentication technique which is based on motion trajectory and cryptographic secret sharing [9]. In this technique, 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 obtained, 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. The authentication technique uses this master key to verify the authenticity of the video. Any modifi-cation in a shot or in the important content of a shot would be reflected as changes in the computed master cap.

3.1 Limitations of existing video authentication techniques

Different challenges are there with the existing video authentication techniques. There is no issue related with the size of authentication code 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, which in turn may give wrong decision. On the other hand fragile watermark based authentication algorithms perform better than algorithms based on conventional cryptography [2]. Fragile and semi fragile watermark based algorithms show good results for detecting and locating any malicious manipulations but often they are too fragile to resist incidental manipulations, and robustness is also challenged in watermark based video authentication systems. Moreover embedding the watermark may change the content of video which is not permissible in court of law [3].

Most of the other video authentication techniques are established for specific tampering attacks. Moreover existing authentication techniques are also affected by compression and scaling operations. On considering all these limitations of existing video authentication techniques, we have proposed an intelligent technique for video authentication which does not require computation and storage of any key or embedding of any secret information in the video data.

Volume : 3 | Issue : 6 | June 2013 | ISSN - 2249-555X

Instead of our algorithm uses a video database of 20 non-tampered originally recorded videos and their more than 1200 tampered copies. The details of video database have been given in experimental results and discussion section.

4. Proposed Methodology

To address these challenges we have proposed an effective video authentication algorithm which computes the inherent local features information from digital video frames statistically and establishes a relationship among the frames. A Support Vector Machine (SVM) [7] based learning algorithm is then used to classify the video as tampered or non -tampered. The algorithm uses inherent video information for authentication, thus making it useful for real world applications.

4.1 Support Vector Machine

A common attacks on a video for tampering are: spatial, temporal and spatio-temporal tampering attacks and further object addition, object removal object modification and frame removal, frame addition and frame shuffling attacks. In our work, for our intelligent video authentication algorithm, we have focused on all the three attacks, spatial, temporal and spatio-temporal attacks. Since we are using SVM based learning and classification technique, it can also differentiate between attack and acceptable operations. Figure, illustrates the concept of the proposed algorithm. The proposed video authentication algorithm computes the correlation information between two video frames. This information is computed locally using corner detection algorithm [20] and then classification is performed using support vector machine [21]. The algorithm is divided into two stages: (1) SVM training (2) tamper detection and classification using SVM.

4.2.1 SVM Training

First step in the proposed algorithm is to train the SVM so that it can classify the tampered and non-tampered video data.

Training is performed using a manually labeled training video database. If the video in the training data is tampered, then it is assigned the label −1 otherwise (if it is not tampered) the label is +1. From the training videos, relative correlation information is extracted. This labeled information is then used as input to the SVM which performs learning and generates a non-linear hyper-plane that can classify the video as tampered and non-tampered. The steps involved in the training algorithm are explained in the Training Algorithm.

Training Algorithm

Input: Labeled training video data.

Output: Trained SVM with a non-linear hyper -plane to classify tampered and non-tampered videos.

Algorithm:

1. Individual frames are obtained from the video data.
2. Corner points are computed from the first and second frame of the video using corner detection algorithm.
3. Let the local correlation between two frames be Li,where i = 1, 2, . . . , m and m is the number of corresponding corner points in the two frames. We define the relative correlation information RC_{jk} between two video frames j and k as,

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

4. Similar to Steps 2-3, relative correlation information is captured for all adjacent Video frames of the video, such as RC_{12} , RC_{23} , and RC_{34} .This relative Correlation information is combined to form a column vector of size (n − 1) × 1, Where n is the number of frames in the video.
5. Steps 1-4 are performed on all the labeled training video data and relative Correlation information RC is computed for each video.
6. Relative correlation information and labels of all the training video data are provided as input to the Support Vector Machine.
7. SVM is trained to classify the tampered and non-tampered data. Output of SVM training is a trained hyperplane with classified tampered and non-Tampered data.

From the training videos, statistical local information (Corner point and Entropy) are extracted. This labeled information is then used as input to the SVM which performs learning and generates a non-linear hyper plane that can classify the video as tampered and non-tampered. All these steps involved in the training of the kernel are explained in the Learning Algorithm.

4.2.2 Tamper detection and classification

We now describe the proposed tamper detection and classification algorithm. Input to the tamper detection algorithm is a video data whose authenticity needs to be established. Similar to the training algorithm, relative correlation information between frames are extracted and the trained SVM is used to classify the video. If the SVM classifies the input video as tampered then the location of tampering is computed. Steps of the tamper detection algorithm are described below.

Training Algorithm

Input: Unlabeled Video data

Output: Classification result as tampered and non-tampered video

Algorithm:

1. Compute the relative correlation information RC for the input video using Steps 1-4 of the training algorithm.
2. Relative correlation information of the input data is projected into the SVM Hyper-plane to classify the video as tampered or non-tampered. If the output of SVM is zero, then the input video is tampered otherwise it is not.
3. If the video is classified as tampered, then we determine the particular frames of the video that have been tampered.
4. Plot the relative correlation information, RC_{jk} of all the adjacent frames of the video, here j = 1, 2, . . . , n − 1 and k = 2, 3, . . . , n.
5. Correlation values showing the maximum deviation in the plot are the values corresponding to the tampered frames.

Fig. 1 shows the video frames from a tampered video that has been subjected to frame addition attack. Similarly Fig.2 shows the video frames of a temporally tampered video that has been subjected to frame removal attack. Here twenty frames are dropped in a video sequence (from frame 21 to frame 40). In fig. 3, a kind of frame alteration attack has been shown in which a small device is removed from the original frame in the tampered frame.

Frame 6 **Added Frame** **Frame 26**

Fig.1 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.

Volume : 3 | Issue : 6 | June 2013 | ISSN - 2249-555X

Frame 19 Frame 20 Frame 41

Fig.2 Example of Frame removal attack. After attack twenty frames, from frame 21 to frame 40 are removed from the video sequences.

Original Frame Tampered Frame

Fig.3. Example of object removal attack. Shows object removal attack with foreground object, where a notebook is removed from the original frame in tampered frame.

6. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed algorithm shows excellent results for temporal tampering attacks. Fig.4 shows the plot of relative correlation information for the 125 probe video frame of the video database in frame additional attack. The plot shows that the relative correlation information of the 5th, 18th, 30th, 42nd 77th and 88th video frames are significantly lower as compared to the relative correlation information of other frames.

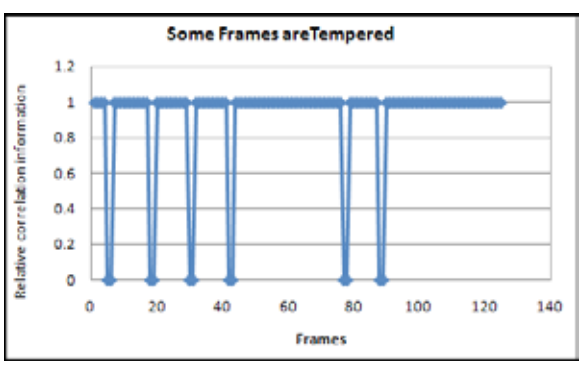

Fig.4 Plot of relative correlation information of a tampered video in which the frames no. 5, 18, 30, 42, 77 and 88 have been tampered subjected to frame additional attack.

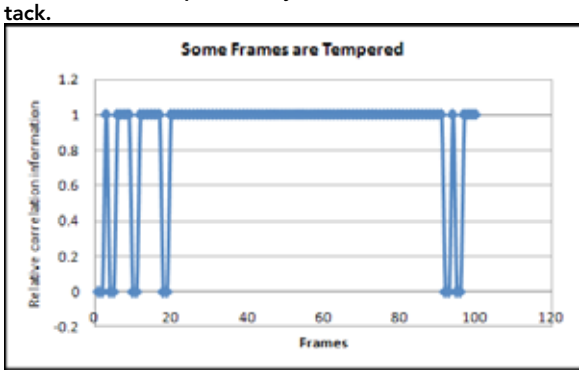

Fig.5. Plot of relative correlation information of a tampered video in which the frames no. 1, 4,10,18,92 and 95 have been tampered subjected to frame removal attack.

For spatial tampering, we have modified the spatial content of the frames of the video with the help of professional software and created the tampered videos for our video database. These tampered videos include almost all kinds of spatial tampering attack. Fig. 6 shows the plot of the relative correlation information as statistical local information for the 66 probe videos of the video database in spatial tampering attack.

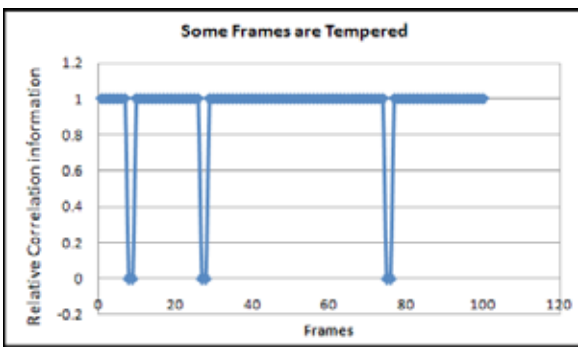

Fig.6. Plot of relative correlation information of a tampered video in which the frames no. 8, 27 and 75 have been tampered subjected to frame spatial tempering attack.

In this figure the relative correlation information of 8th, 27th, and 75th frames are comparatively lower than the relative correlation information of other video frames. Therefore the video frames regarding 8th, 27th, and 75th values in x-axis are declared here as tampered videos.

The validation process of proposed tamper detection algorithm is performed using a video database which contains twenty videos. Experimental protocols for validation process are as follows:

1. We have created a video database of one hundred twenty videos, originally recorded by a DV (DCR-SX65) SONY Handy cam, CCTV camera and a mobile phone camera in various illumination conditions, and camera positions. Some of the videos of the database were taken at close range under controlled lighting conditions in indoor environments and others are taken under natural light (Sunlight) condition in outdoor environments. Some of the videos are recorded at 15 fps (by mobile phone camera) and others are recorded at 23.9 fps. Size of each frame is 352 × 288. These videos are used as the ground truth.
2. For frame alteration (spatial tampering) attacks we used professional software. With the help of this software we altered the contents of the frames of each ground truth video. This alteration is performed in various aspects, such as, object addition and object removal from the frames. 22 copies of each video of the video database are created, subjected to spatial tampering attacks.
3. 15 ground truth videos together with 900 tampered videos are used to train the support vector machine, for frame removal, frame addition and frame alteration attack. This SVM training is performed for all the three kinds of attack, separately with different tampered videos.
4. 10 different non-tampered copies of the remaining 5 ground truth videos are created and these 50 non-tampered videos together with more than 300 tampered videos are used as the probe database to determine the performance of the pro-posed algorithm.

Volume : 3 | Issue : 6 | June 2013 | ISSN - 2249-555X

Table1. Classification Result Of Proposed Video Authentication Algorithm For Tampered And Non-Tempered Videos.

Tempering Attacks	Total Number of Videos	Number of Correctly Classified Video	Classification Accuracy (%)
Non-Tempered	100	100	100
Frame Addition	100	100	100
Frame Removal	100	94	94
Spatial Tempering	100	84	80
Total	400	375	93.5

Thus the overall classification accuracy of the proposed algorithm is 93.5%. These results show the efficacy of our proposed video authentication algorithm for all the three common tampering attacks, namely frame addition, frame removal at-tack and spatial tampering attacks. We also compared the performance of the proposed video authentication algorithm with the motion trajectory based video authentication algorithm [9]. Table 2 depicts a theoretical comparison of both algorithms. Motion trajectory based algorithm [9] is fast and simple but unable to detect some of the tampering attacks (as spatial tampering attacks). On the other hand our proposed algorithm uses an intelligent technique, namely SVM classification which is able to detect both kinds of attack, spatial as well as temporal.

5. 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. Existing video authentication algorithms use watermarking or digital signature based algorithms. Digital signature based algorithm can be deceived, if the digital signature is compromised and watermarking based algorithms are not acceptable in court of law because they have been altered during watermark embedding and extraction. To address these issues we have proposed an efficient video authentication algorithm which can detect multiple video tampering attacks. Our proposed algorithm computes the statistical local information of all of the binary difference frames of the given video and projects them into a nonlinear SVM hyper plane to determine if the video is tampered or not. The algorithm is validated on an extensive video database containing more than 1200 tampered and 20 ground truth videos. The results show that the proposed algorithm yields a classification accuracy of 93.5%. In future we would like to extend the proposed algorithm for rapid camera movement and night vision shot video tampering.

REFERENCE

[1]. 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 | [2]. 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. | [3]. S. Upadhyay, S.K. Singh, M. Vatsa, and R. Singh, "Video authentication using relative correlation information and SVM", In Computational Intelli-gence in Multimedia Processing: Recent Advances (Springer Verlag) Edited by A.E. Hassanien, J. Kacprzyk, and A. Abraham, 2007. | [4]. Law Enforcement/Emergence Services Video Association (LEWA). | [5]. Jana Dittman, Anirban Mukharjee and Martin Steinbach, "Media inde-pendent watermarking classification and the need for combining digital video and audio watermarking for media authentication". International conference on Information Technology: Coding and Computing, 2000. | [6]. 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. | [7]. Vapnik VN (1995). "The Nature of Statistical Learning Theory" Springer Verlag | [8]. Singh R, Vatsa M, Noore A (2006) "Intelligent Biometric infor- mation fusion using support vector Machine". In Soft Computing in Image Processing: Recent Advances, Springer Verlag, 327-350. | [9]. Wei-Qi Yan an Mohan S Kankanhalli, "Motion Trajectory Based Video Authentication" ISCA(3) 2003: 810-813 | [10]. Dajun He, Qibin Sun, Qi Tian, "A semi fragile Object based video authentication system" IEEE ISCAS 2003, Bangkok | [11]. R. Gennaro and P. Rohatgi," How to sign digital Stream", Crypto'97, pp. 180-197, 1997. | [12]. 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. | | [13]. Upadhyay, Saurabh; Singh, Sanjay K;, "Learning based video authen-tication using statistical local information," Image Information Processing (ICIIP), 2011 International Conference on , vol., no., pp.1-6, 3-5 Nov. 2011 doi: 10.1109/ICIIP.2011.6108953. | [14]. 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 IV. | [15]. 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. | [16]. Johns Hopkins APL creates system to detect Digital Video Tampering. http://www.jhu.edu/. | [17]. 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. | [18]. 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. | [19]. 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. | [20]. W. Diffie and M. E. Hellman, New Directions in cryptography, IEEE Trans. on Information Theory, Vol. 22, No. 6, pp.644-654, Nov 1976. | [21]. 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