WATERMARKING FOR VIDEO AUTHENTICATION

[1]Pathak Utsav A
Department of Electronics and Communication
Sarvajanik College of Engineering and Technology
Surat, India
Email:[1]utsavpathak.3787@gmail.com

***Abstract*— In law examples like surveillance and forensics video is presented as proof. Because of that it is extreme importance to establish the validity and dependability of the video data. Since the H.264 / AVC-based video products are becoming increasingly popular, are issues of copyright protection and authentication that are appropriate for this very important standard. Here in this dissertation different techniques for video authentication are studied. Here different types of spatial and temporal tampering attacks are considered for video and to check authenticity of video intelligent technique like SVM based machine learning is used to identify temporal attacks like frame adding, frame removing etc. For authentication different parameters are studied for video like PSNR, NC, BER.**

Keywords—watermarking, authentication, embedding, extracting, DWT, DCT, DFT, H.264/AVC, SVM, SVD

I. INTRODUCTION

Today in multimedia creation and delivery from authoring content provider to the receivers everything seems to be digital. The benefits of digital processing and distribution, example transmission without noise, software in place of hardware processing and superior re-configurability of systems, are well recognized and obvious. But distribution of digital media is main disadvantage. For example, in terms of media generators and content providers, the opportunity of infinite replication of computerized data without loss of loyalty is not desirable for the reason that it tends to substantial economic losses. Digital copy or copy protection, since access to plain text versions of protected data must be a minimum estimate of the receiver, which then produce and distribute illegal copies are issued, it may be of limited value. In actuality tries of preventing copy are always get bypass.

Another method of protecting intellectual property rights (IPR) is the embedding of digital watermarks in the multimedia data. The watermark is a computerized code unsolvable, robust, and imperceptibly implanted in the host information and for the most part contains data about the starting point, status and target of the information. Although unutilized specifically for copy safety, it can help identify the starting place and ending point of multimedia information and as a "last line of defense", allow proper proceedings in case of doubt of copyright violation.

Although copyright protection is the mainly popular application of watermarking techniques, there are other, plus data validation means fragile watermarks that impaired or damaged by manipulations implanted transfer of worth added services in the multimedia data, and embedded data identification for purposes other than protection of copyright, some example tracking and monitoring of data. An illustration of a data monitoring system is the automatic registration and monitoring of radio broadcasting, to automatically pay the royalties the IPR owner of the broadcast data.

The progress of watermarking methods has some of the design compromises. Watermark should be robust. It is compared with standard data manoeuvring, including digital-to-analog conversion and digital format conversion. Security is a particular concern, and watermark should withstand attack attempts by competent persons. On the second note watermark should not be perceptible and as many information as it can. Generally watermark embedding and recovery should have little complication, since for a variety of applications, a synchronized watermark is popular.

A. *Requirement of Digital Watermarking*

1) A watermark will transmit to great extent information possible, which means that the watermark data should have high data rate.
2) A watermark should be generally kept undisclosed and accessible only by sanctioned person. This necessity is known as watermark security and it is typically achieved by using cryptographic keys.
3) Including all signal processing that can happen and how unauthorized person try to change a watermark is in the host data is stayed with it. This scheme is known to watermark robustness. It is an important prerequisite for protection of data or access control applications, but also applications for which the watermarks are not essential to cryptographically sure, for illustration, applications where watermark transmit the information to the public less important.
4) A watermark should however as non-removable, are imperceptible.

This fundamental set of needs may be supplemented with extra needs depending on media in which watermark is to be embedded and the application.

1) Watermark recovery may or may not get approved to employ unwatermarked original host data.
2) Based on purpose watermark embedding like video fingerprinting may require concurrent example. Embedding in real may need compressed domain embedding techniques for complication reasons.
3) Depending on use watermark is needed to be capable to transmit random information. While in different applications just some predefined watermarks must be installed and for disentangling it might be adequate to verify vicinity of one of the predefined watermarks.

According to [6] some of these desires and the consequential design issues will be painted in greater detail.

1) Watermark Security and Keys: If the security, that is, confidentiality of the embedded information is essential, for embedding and extraction one or more than one secure keys are used. For example, in lots of systems, pseudo-random signals are embedded as a watermark. In this situation, the description and the seeds of the pseudo-random number generator are used as keys. Here two security levels are used. Users which are not authorized can't decode embedded watermark in the first stage, but can know whether it have watermark. Now in second level users which are not authorized can't sense that data have watermark or not however the embedded data can't be read without secret key. Here systems embed two watermarks one with public key and other with secret key. On the other hand, a scheme was introduced that use combined public key with a private key, and embeds it instead of multiple watermarks. There are some issues such as generation of secret key, distribution and management needs to consider as well as other aspects of system integration.

2) Robustness: When making any watermarking algorithm robustness is the main issue because robustness introduced again by standard data processing and data attacks distortion is an important prerequisite. Standard Data Processing includes all data manipulation and modifications that the data could in the normal distribution chain to undergo, such as data processing, printing, enlargement and format conversion. "Attack" is the data manipulation with the purpose of affecting, disrupting or removing the embedded watermark. Although it is possible to design robust watermark method, it should be noted that a watermark is only robust, as long as it is private, the as long as they will not be of anyone reading device.

3) Imperceptibility: Perceptual clearness in important requirement of watermarking. The embedding procedure must not launch artifacts in host data which are noticeable by viewer. On the other part, it is important that watermark amplitude is as high as promising for good robustness. Thus, there is always trade-off between imperceptibility and robustness in construction of watermarking method. Normally, watermark should be embedded just below some threshold so that no one can notice its presence. However, for genuine image, video and audio signals it is hard to find such threshold value.

4) Watermark Recovery With or Without the Original Data: In watermark recovery if the original unwatermarked data is available then recovery generally becomes more robust. Also easy use of new data set in recovery process the finding of distortion that alter geometry of the data. For example, if watermarked image has been rotated by an assailant this thing will help. However in some application such as data monitoring and data tracking right to use to the unique data is impossible in every cases. In video watermarking because of the large volume of data it is not practically good to use the original data even though it is available.

However for watermark extraction we can make techniques which do not require the original data. Some kind of modulations is performed in most watermarking techniques in which the distorted novel data set is considered. If we know this distortion or in recovery process if it can be modelled, clearly planned techniques permit its control without facts of the original. In fact, in most current methods there is no need of the original data for recovery.

B. *Basic principle of watermarking*

The basic idea of watermarking is to embed a watermark signal into the host data that is to be watermarked such that the watermark signal is unremarkable and secure in the mixture of signal but later on it can partly or fully be recovered from the signal mixture if the proper cryptographically secure key for recovery is used.

Watermark embedding process is shown below in Fig.1

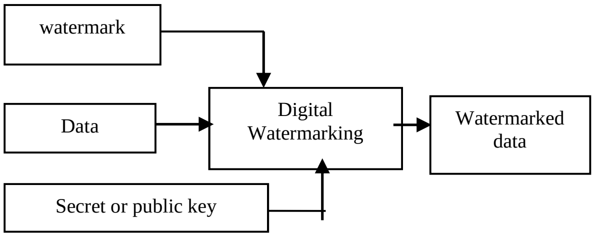
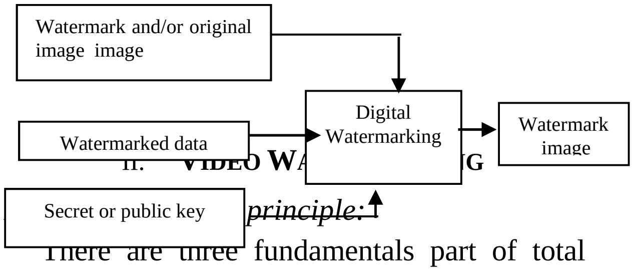


Figure 1 watermark embedding process[6]

Figure 2 watermark extraction process[6]



II. VIDEO WA[illegible]G

[illegible] principle:

There are three fundamentals part of total digital watermarking system [4]: generation of watermark, embedding of watermark and extraction/detection of watermark. In Figure 3 Block diagram for embedding and extraction of watermark is shown:

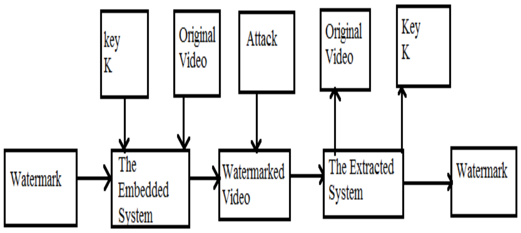


Figure 3 principle of video watermarking [4]

B. *Video watermarking Characteristics*

Video watermarking not only contain the features of image watermarking but also posses its own features [4].

- **High real-time.** Video that is three dimensional has more quantity of data than the image. So there is large computation quality and it requires large time for embedding/extracting. Using video compression standard such as VLC code word, motion vector coding are efficient algorithm for the procession of embedding.
- **Random detection.** This means that we can detect the watermark in video in any position not the place according to the video playback.
- **The combination of video codec standard.** In storage or transmission video is in compressed formats, so without specific video codec standard research of information hiding technology can't do anything. Video information hiding technology can accomplish the real time requirement combining with encoding and decoding standard.
- **Enhanced robustness.** This means that the scheme of video watermarking must guarantee that it can oppose almost all kind of attacks or processing.
- **Blind detection scheme.** If the detection scheme is Non-blind that it will require the original data in extraction. But it is not very convenient to use the original data which is so large. While detection scheme of Blind type does not require any original data in extraction.

C. *Video watermarking model*

There are three types of solution for video watermarking algorithm based on the strategy of embedding [4]:

1) The uncompressed video i.e. original video
2) video codec
3) The compressed video.

The type of the solution is shown in the figure 4.

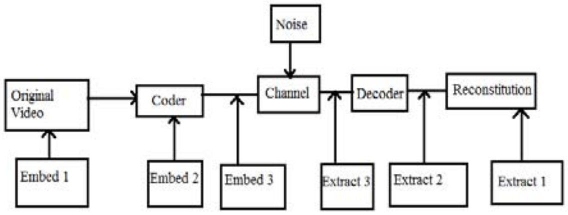


Figure 4 video watermarking model [4]

The uncompressed video[4]: In this type of video watermarking embedding of watermark is done directly into the original video sequence and then the encoding of watermark containing video is done. Here the advantage of watermarking technology of still image and combination with the structural characteristics of video frames makes the solution of video watermarking. The benefit of this watermarking algorithm is it is comparatively mature. We can apply methods like spread spectrum, the human vision model, image adaptive watermarking irreversible, synchronous detection mechanism to this video watermarking system. But the demerit of solution is video bit rate will be increased and it will effect video rate of constancy; and watermark may get lost after the compression and encoding of the video data. If the video is in compressed form than first we have to decode it and then after embedding watermark re-encoding of video has to be done. But with this process complexity will get increase and the quality of video will get decreased.

Solution based on video codec[4]: In encoder embedding and detection module for watermarking are introduced. There are video compression standards like ISO / IEC of MPEG-1, MPEG-2, MPEG-4 and ITU-T of H. 261, H. 263, etc in today’s life. Block based transform coding and motion compensation prediction coding are the fundamental idea. Here the embedding is done in encoding phase of video. Characteristics of encoded data and principle of video data compression like transformation to the spatial redundancy, quantization and entropy coding, the motion compensation, motion estimation, etc are used here. The real time processing of watermark embedding and extracting is simple to achieve. The relative simple process of watermark embedding in the transform domain coefficient does not increase the bit rate of video; also we can make watermarking algorithm for multiple attacks, because embedding of watermark is done in transform domain and it is combined with the encoding process. GOP error accumulation is occurred because we need to modify the encoder and decoder and also the video codec in unable to perform common embedding and detection of watermark.

The compressed domain video[4]: In this solution watermark is embedded straight into the compressed encoded bit stream of video. Here there is no requirement of decoding and re-encoding of video which is the advantages of this solution and because of that it will not degrade the video quality and there is low computation complexity. Here disadvantage is the bit-rate of compressed video constrain the size of watermark to be embedded. Error in video decoder will limit the strength of the watermark and the coding standard and the video compression algorithm will constrain the strategy of embedding. The computational complexity is low and rate of watermark embedded is high. But the capability to deal with channel interference is poor which is the disadvantage; by adding random bits in the VLC code using same algorithm can destroy the watermark; extraction of watermark will also get effected of traditional filtering, re-sampling and time-domain scaling processing.

D. *Algorithm of video watermarking*

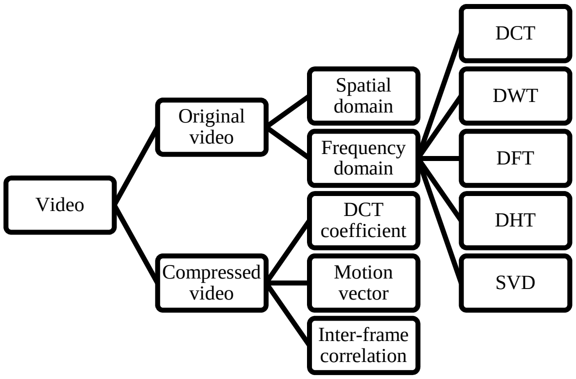


Figure 5 video watermarking algorithms [4]

Other than all this technique one technique is intelligent technique which is machine learning based technique in which the different classifiers (like SVM, NN etc.) are used to train the network first and after the network is trained it will provide whether the video is tampered or not. This technique is more suitable for temporal tampering like frame removal, frame dropping and frame shifting which is discussed in section III.

III. Video Tampering Attacks

To change the content of video data there are several attacks are performed. Video data is the collection of consecutive frames with temporal or time dependency which is viewed in a three dimensional plane. This is known as the regional property of the video sequences. If malicious changes on video sequence is applied it can either attacks on the content of data like frames of video presenting visual information, or executed attacks on the temporal or time dependency within the frames. Therefore video tampering attacks are classified in three types based on the regional property of the video sequences: attacks of spatial tampering, attacks of temporal tampering and the combination of these two, attacks of spatio-temporal tampering

A. *Attacks of Spatial Tampering*[5]

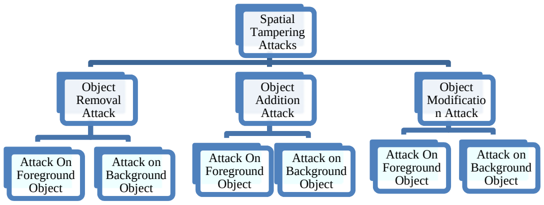

Spatial Tampering Attacks
Object Removal Attack
Object Addition Attack
Object Modification Attack
Attack On Foreground Object
Attack on Background Object
Attack On Foreground Object
Attack on Background Object
Attack On Foreground Object
Attack on Background Object

Figure 6 different spatial tampering attacks [5]

B. *Object removal attack*

In this type of attack in [5], the objects of the frames are removed from the frame by some technique. This type of attack is often carried out where a specific person wants hide his/her presence in particular sequence of frames. This attack can be carried out with two types of objects, object in the foreground and object in background.

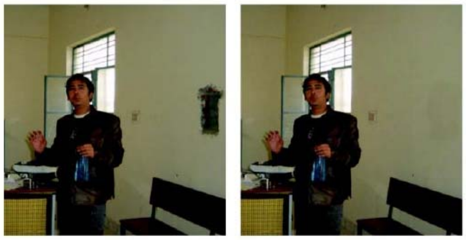


Figure 7 object removal attack [5]

C. *Object addition attack*

In this type attack in [5], an object is added in a frame or in a series of frames, than this kind of manipulation is known as content or object addition attack. It can also be carried with both kinds of objects, objects in foreground and objects in background.

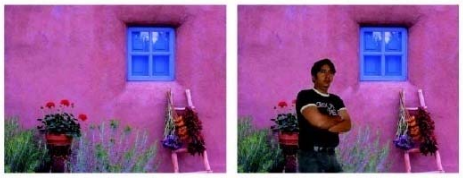


Figure 8 object addition attack [5]

D. *Object modification attack*

In this type of attack in [5], an existing object of the frame(s) modified in such a way that the existing identity of that object are lost, and a new appearance of object is obtained that is totally changed from the original object. Like example, the size and shape of the existing object to be changed, which may be to alter or discolour the color of object, and using additional effect of the nature of the subject and its relation with other object also be changed.

E. *Temporal tampering*

In this type the manipulation with the sequence of frame is performed. The concentration is on the time dependency. Temporal manipulation attacks are mainly based the temporal sequence of visual information captured from video recording device. Frame addition, frame removal and frame shuffling or rearranging are the common attacks in this type of tampering.

F. *Frame addition attack*

In this type of attack as shown in figure 9 another frame is added in between the original video frames at some random position.

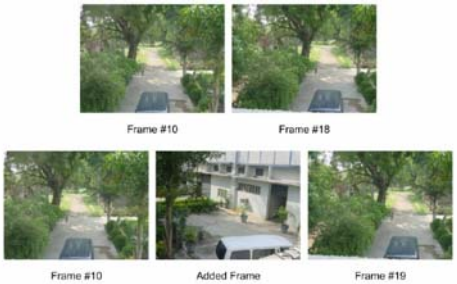


Figure 9 frame addition attack [5]

G. *Frame removal attack*

In this type of attack as shown in figure 10 frames from the video sequence are removed intentionally from particular place to the fixed place or can be removed from various locations. Often this type of manipulation attack on video surveillance in which an attacker wants to remove his/her presence at all.

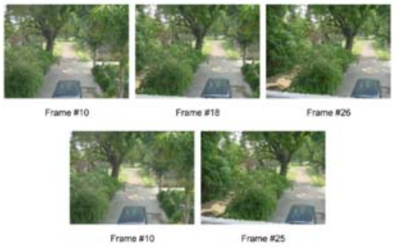


Figure 10 frame removal attack [5]

H. *Frame shuffling attack*

In this type of attack as shown in figure 13 position of frames are changed from its original place in a way that correct frame are mixed with this and compared to original video it will produce false information.

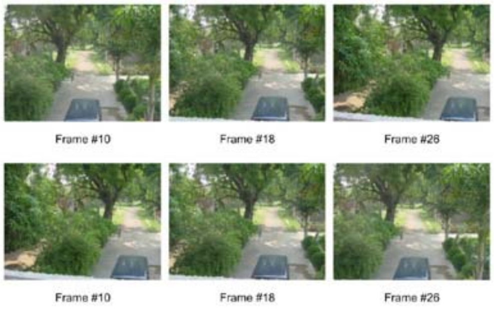


Figure 11 frame shuffling attack [5]

IV. Result and Analysis

A. *Result for DWT and SVD based watermarking technique*

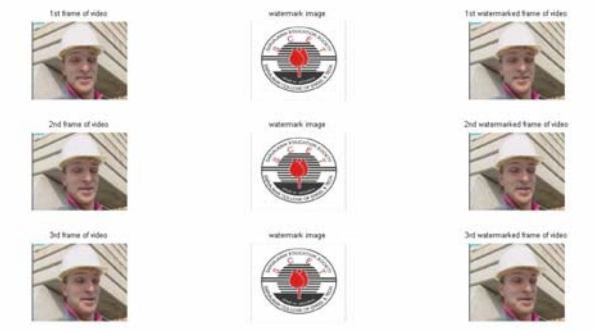


Figure 12 plot of original frame, watermark image and watermarked frame for foremen video sequences

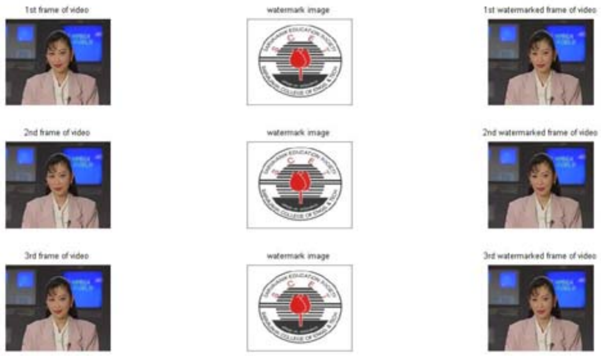


Figure 13 plot of original frame, watermark image and watermarked frame for akiyo video sequences

Table 1effect of alpha on PSNR

Frame	PSNR for alpha=0.01	PSNR for alpha =0.2	PSNR for alpha=0.5
1	64.6296	38.0136	30.7344
2	64.7064	38.0172	30.7360
3	64.8109	38.0131	30.7375
4	64.7181	38.0200	30.7381
5	64.6689	38.0115	30.7445
6	64.6031	38.0222	30.7419
7	64.5421	38.0178	30.7445
8	64.5408	38.0196	30.7475
9	64.6031	38.0277	30.7451
10	64.5433	38.0108	30.7292
11	64.5421	38.0081	30.7321
12	64.6082	38.0128	30.7306
13	64.6812	38.0034	30.7309
14	64.6299	38.0083	30.7453
15	64.5603	38.0183	30.7450
16	64.5184	38.0088	30.7334

17	64.7123	38.0013	30.7218
18	64.6838	38.0113	30.7252
19	64.6484	38.0001	30.7292
20	64.8175	38.0019	30.7320
21	64.7751	38.0088	30.7240
22	64.8806	38.0085	30.7183
23	64.7646	38.0064	30.7181
24	64.6792	38.0110	30.7344
25	64.7285	38.0060	30.7178
26	64.9755	37.9960	30.7372
27	64.8462	37.9988	30.7346
28	64.8556	37.9914	30.7200
29	64.8449	38.0037	30.7366
30	64.8887	38.0015	30.7341

Table 2different value of PSNR

Frame	Foremen sequence	Akiyo sequence	Coastguard sequences	Mobile sequences
1	64.6296	64.3329	65.3159	65.7317
2	64.7064	64.4098	65.5910	65.2913
3	64.8109	64.3353	65.3889	65.4455
4	64.7181	64.2950	65.6423	66.4177
5	64.6689	64.3329	65.3144	66.1273
6	64.6031	64.3712	65.6568	66.2293
7	64.5421	64.4098	65.4617	66.2256
8	64.5408	64.3353	65.1568	66.1165
9	64.6031	64.3712	65.6487	65.8891
10	64.5433	64.4098	65.3039	65.1424
11	64.5421	64.5704	65.3204	65.3783
12	64.6082	64.4512	65.5028	65.7847
13	64.6812	64.3929	65.3323	66.1237
14	64.6299	64.3544	65.4347	66.2999
15	64.5603	64.2785	65.5696	66.3717
16	64.5184	64.2038	65.2876	66.3300
17	64.7123	64.2410	65.3904	66.8335
18	64.6838	64.1282	65.2876	66.0241
19	64.6484	64.3305	65.3836	66.3717
20	64.8175	64.3258	65.3458	66.3946
21	64.7751	64.4390	65.3700	66.2109
22	64.8806	64.3210	65.1017	66.4447
23	64.7646	64.4366	65.2891	66.1165
24	64.6792	64.5104	65.0165	66.0276
25	64.7285	64.4317	65.1066	66.0523
26	64.9755	64.4317	65.1230	66.1889
27	64.8462	64.5054	65.1632	65.6892
28	64.8556	64.6363	65.0953	66.1345
29	64.8449	64.5154	65.2250	66.4875
30	64.8887	64.6083	65.2506	66.4797

B. *Result of extraction for DWT-SVD based technique*

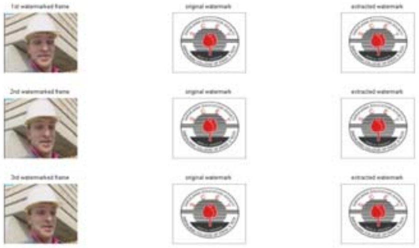


Figure 14 Plot of watermarked frame, original watermark and extracted watermark

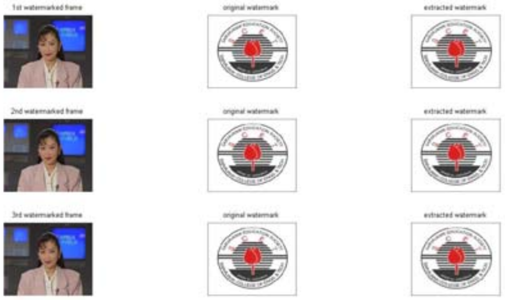


Figure 15 Plot of watermarked frame, original watermark and extracted watermark

C. *Results for embedding algorithm for SVD based blind watermarking*

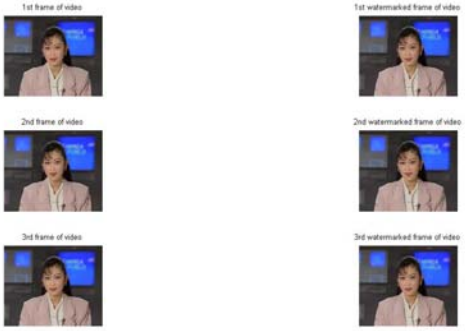

1st frame of video
1st watermarked frame of video
2nd frame of video
2nd watermarked frame of video
3rd frame of video
3rd watermarked frame of video

Figure 16 Plot of watermarked frame, original watermark and extracted watermark for akiyo video sequence

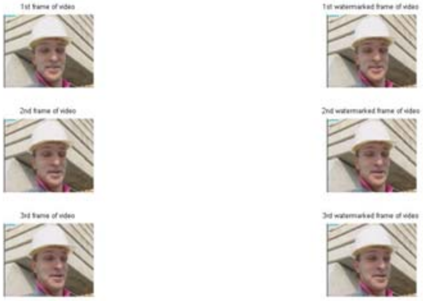

1st frame of video
1st watermarked frame of video
2nd frame of video
2nd watermarked frame of video
3rd frame of video
3rd watermarked frame of video

Figure 17 Plot of watermarked frame, original watermark and extracted watermark for foremen video sequence

Table 3 effect of alpha on PSNR

Frame	Akiyo	Coastguard	Foremen	Mobile	Stefan
	video sequence	video sequence	video sequence	video sequence	video sequence
1	34.9909	40.0441	46.0997	41.5930	48.3405
2	34.9654	39.7700	44.8927	41.0430	47.5796
3	34.9720	39.4477	43.6452	41.0286	46.7698
4	34.9997	39.0292	43.1152	40.7109	46.1011
5	35.0428	39.0046	42.5823	40.3819	45.1913
6	35.1261	39.1059	41.4183	40.1005	44.9520
7	35.1136	39.1436	39.9214	39.4494	47.0060
8	35.0739	38.8404	38.8685	39.0021	49.0354
9	35.0045	38.6690	38.5416	38.5619	48.3838
10	34.9673	38.4641	38.7939	38.1057	49.3549
11	34.9773	38.2944	38.9434	37.5686	50.7529
12	34.9108	38.2595	38.8975	37.0766	50.6056
13	34.8743	38.2148	39.7543	36.3896	49.3658
14	34.8567	38.2764	41.8741	36.1033	47.1649
15	34.8898	38.2906	45.2542	35.8666	46.4206
16	34.9145	38.3787	49.9624	35.7272	45.7651
17	34.8838	38.6268	46.1365	35.7811	47.8917
18	34.8545	39.1234	43.4867	35.8834	46.8934
19	34.8298	39.8234	42.9556	35.6988	46.3849
20	34.8014	40.6285	43.7165	35.7100	44.8815
21	34.7913	41.2848	43.8526	36.0210	43.7876
22	34.7510	41.6579	43.5334	36.3706	43.8136
23	34.7518	41.9771	43.0033	36.7656	43.0265
24	34.7397	42.2592	43.2658	36.8671	43.9926
25	34.7384	42.9248	43.8237	36.8690	44.2327

26	34.7557	43.2294	44.5120	36.8515	43.6151
27	34.8524	43.6386	45.3358	36.8628	43.8070
28	34.9141	43.7868	46.2837	36.8000	44.0003
29	34.8710	43.7379	47.0449	36.8367	43.7540
30	34.8285	43.7033	47.4946	36.8432	43.3340

V. Conclusion

By doing this dissertation, for video authentication different methods have been studied. For video two types of attacks are possible one spatial tampering attack and the other one temporal tampering attack

For spatial tampering attacks different techniques has been studied and for implementation purpose two techniques SVD based blind video watermarking and DWT-SVD based watermarking algorithm has been employed. Both techniques have their merits and demerits. Former one is blind technique in which original watermark is not required to extract the watermark while latter is non-blind technique in which original watermark is required during the extraction. While value of PSNR is good in DWT-SVD based technique.

For temporal tampering attacks SVM based machine learning technique is studied. This technique is best suited for this type of attacks and gives good results with good accuracy.

References

[1] Dawen Xu, Rangding Wang, Jicheng Wang, “A novel watermarking scheme for H.264/AVC video authentication ”, Signal Processing: Image Communication(Elsevier) 26 (2011)267–279

[2] Osama S. Faragallah, “Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain”, Int. J. Electron. Commun. (Elsevier) 67 (2013) 189–196

[3] Po-Chyi Su, Chin-Song Wu, Ing-Fan Chen, Ching-Yu Wu, Ying-Chang Wu, “A practical design of digital video watermarking in H.264/AVC for content authentication ”, Signal Processing: Image Communication(Elsevier) 26 (2011)413–426

[4] Xing Chang, Weilin Wang, Jianyu Zhao, Li Zhang, “A Survey of Digital Video Watermarking”, Seventh International Conference on Natural Computation 2011 IEEE

[5] Richa Singh, Mayank Vatsa, Sanjay K. Singh, Saurabh Upadhyay, “Integrating SVM classification with SVD watermarking for intelligent video authentication”, Telecommun Syst(Springer) (2009) 40: 5–15

[6] Hartung, F.; Kutter, M., "Multimedia watermarking techniques," Proceedings of the IEEE , vol.87, no.7, pp.1079-1107, Jul 1999

[7] Wenhai Kong; Bian Yang; Di Wu; Xiamu Niu, "SVD Based Blind Video Watermarking Algorithm," *Innovative Computing, Information and Control, 2006. ICICIC '06. First International Conference on* , vol.1, no., pp.265,268, Aug. 30 2006-Sept. 1 2006

[8] Upadhyay, S.; Singh, S.K., "Learning based video authentication using statistical local information," *Image Information Processing (ICIIP), 2011 International Conference on* , vol., no., pp.1,6, 3-5 Nov. 2011

[9] Mohd Shahidan Abdullah, Azizah Abd Manaf, “An Overview of Video watermarking Techniques”, Postgraduate Annual Research Seminar 2007

[10] Ankita Hood, N.J Janwe, “A Review on Video Watermarking and Its Robust Techniques”, International Journal of Engineering Research & Technology (IJERT), vol.2 Issue 1, January-2013

[11] Potdar, V.M.; Song Han; Chang, E., "A survey of digital image watermarking techniques," *Industrial Informatics, 2005. INDIN '05. 2005 3rd IEEE International Conference on* , vol., no., pp.709,716, 10-12 Aug. 2005

[12] Bhattacharya, S.; Chattopadhyay, T.; Pal, A., "A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC," *Consumer Electronics,*

2006. ISCE '06. 2006 IEEE Tenth International Symposium on , vol., no., pp.1,6

[13] Rashel Sarkar, Smitha Ravi, “A Survey of Digital VideoWatermarking”, the international journal of computer science & application, vol.1, no.2, April-2012

[14] Hamid shojanazeri, Wan Azizum Wan Adnan, Sharifah Mumtadzah Syed Ahmad, “Video Watermarking Techniques for Copyright protection and Content Authentication”, International Journal of Computer Information Systems and Industrial Management Applications, volume 5(2013), pp.652-660

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