www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 5 May 2017, Page No. 21328-21332
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i5.23

Digital Video Watermarking Techniques: A Review

Arti Bhardwaj[1,2], Ajay Khuteta[2,2]
[1]Poornima College of Engineering, Jaipur, Rajasthan
[2] Senior Professor Department of Computer Science and Engineering, Poornima College of Engineering, Jaipur, Rajasthan
[1]artibhardwaj011@gmail.com
[2]khutetaajay@poornima.org

Abstract – Now a days internet becomes the most popular for exchange data & information over worldwide. These data & information are available on the internet in the form of digital media. In the era of internet authentication, protection and illegitimate redistribution of digital multimedia has become an essential issue. Digital Watermarking can be used to secure these illegal redistribution and reallocation. Digital Watermarking was invented against illegal work, owners' authentication and security. Digital Video Watermarking is method to hiding some kind of data like audio, image, text into digital video sequences which is nothing but orders of successive still images. In this paper, we discuss about digital video watermarking techniques, robustness and also present the application where the uses of watermarking techniques and for better performance of video watermarking. We survey on properties of video watermarking, classification of video marking techniques, application and watermark attacks.

Index Terms— **Attacks, Content protection, Digital properties, DWT, DCT, DFT, FFT, SVD, Security, Watermarking techniques.**

I. INTRODUCTION

Security is a prime concern in this digital world. Thousands of bits are being transmitted from one place to another through internet. The only concern for the sender is that the data is being transmitted reliably and securely. Data should be decrypted only by the authorized person. Various ways were invented for transmission of data.

Steganography and watermarking are two techniques which data transmit data by hiding it in any other digital media. Steganography technique follow the hidden technique where text hide in image and text. When comes to hiding images it is referred to as watermarking. Watermarking of digital data shadows the steganography and it is hide the digital data behind other data. In source image and hidden image both has the highest preference.

In watermarking techniques, image and data can be hide in other type of image data, video data & audio data,. It is more secure as now the data is encrypted more precisely in image form. The watermarks divide into two parts visible and invisible. Image can be hide in image, video, audio and text in image watermarking. After Image watermarking scientist invented video watermarking.[1,2] .

In data security field, video watermarking is a main feature. Video watermarking allows to embed more data with the same and optimized length of video also it maintains the quality of the video up to a great extent and hence enhances the data limit for embedding data.

Video Watermarking concept generate from image watermarking concept where the illegal distribution and copyright identification is appended on the source image for the reason of safety and security of image . A video is a group of number of digital images or we can say sequence of still images, so video watermarking hide the data in the frames of video. From these Frames of video select any frame and then embed the data in this select frame, this is called video watermarking.[1]

II. General Properties of Video Watermarking

Here are some general properties which are play very important role in video watermarking process, given below.

2.1 Imperceptibility:

The embedded watermark data should not modify, effect or loss the superiority of original data. If a human cannot find out the difference between the watermarked data and original data, this is called imperceptible watermark.

2.2 Robustness:

When a video is shared usually there will be some noise and unwanted data. The watermark should be robust against all cleared and mischievous attack. Even when data of the video changes copy right data should not get change .

2.3 Unambiguous:

The extracted watermark should be individually identifying the original owner of the video.

2.4 Reliability:

A watermark has a high reliability, if the degradation of watermark data causes is very difficult to identify for the viewer.

2.5 Capacity and Payload:

Capacity is particular embed data to be embedded in cover work. The total number of watermark bits in host (source) data is called payload. The payload can varies from one application to other.

2.6 Interoperability:

Watermark process system should be interoperable, which is used to perform the compressed and decompressed operations.

2.7 CBR (Constant Bit Rate):
In bit stream domain, watermark bits should not increase the Bit rate.

2.9 Blind detection scheme:
for matching images of video frames of original data in video sequence. We need huge amount of data for matching these images in detection scheme. But we need original data which is use in non-blind detection scheme. in blind detection scheme we don't need original data and it is beneficial for video watermarking.

2.8 Random detection:
Detection of digital watermark data can be done in the video at any point, in the video watermarking[2].

2.10 Security:
The Watermark data and original data should be accessible only by the authorized user. The hackers and unknown user cannot attacks and must be unable to extract the watermark data and the original data. The watermark data and original data should not effect and change by any attacks.

2.11 Computational Cost and Time Complexity:
The cost to embed watermark into host data and to extract watermark should be consistent. It is important to select a suitable complexity watermarking algorithm to avoid high complexity problems like more software and hardware resources. Less Time taken by watermarking algorithm can increase the efficiency .**[R2,R3]**

III. Classification of Video Watermarking Technique

Video watermarking techniques can be classified which are depending upon perception and insertion domain as shown in Fig 2 [3][8].

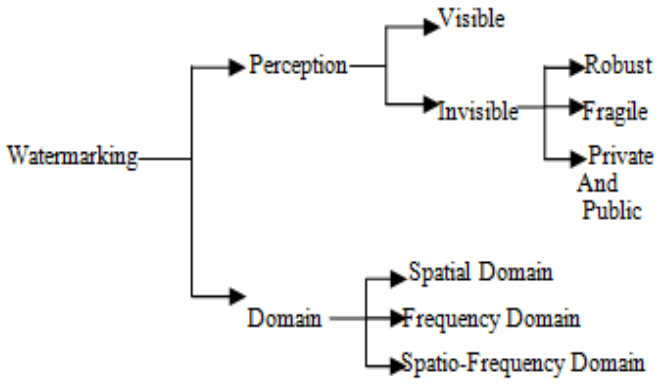

Fig 2: Classification of Video Watermarking Techniques

3.1 Spatial Domain Method (SDM):
The spatial domain method, embed the watermark by changing the pixel values of the host video in frames. Spatial domain method is closer related to Frequency domain with simplicity and less computational complexity. The process is less robust to geometric distortion and less resistant to noise, low pass filtering and comparison[9.11].

3.1.1 Least Significant Bit (LSB):
Watermark is embedded by modifying lower order bit of each pixel, it is simplest watermarking technique. The payload of LSB technique is very less and restricted.

3.1.2 Correlation -Based Technique:
It is a straight forward watermark methodology to embed watermark by adding pseudorandom noise pattern to luminance value of video pixel. The pseudorandom noise (MN) pattern i.e. P(x, y) is added to cover image Q(x, y) the outcome is watermarked image QP(x, y).Here (x, y) represent position of watermark. QP(x, y) = Q(x, y) + k* P(x, y). where k is gain factor. The spatial method can provide better robustness and average payload if image is decomposed into blocks and multiple watermarks is embedded in blocks by optimal watermarking technique.

3.2 Frequency Domain Method (FDM):
The watermark is embedded in frequency domain as an alternative of spatial domain. Watermark is spread out to entire image so it is more robust, secure & efficient rather than spatial domain .

3.2.1 Discrete Fourier Transform (DFT):
In this approach, watermark is embedded only in first frame of group of pictures in videos. The full DFT technique is applied to detect frame to be watermarked and magnitude of coefficient is calculated. DFT method is robust in contradiction of linear/nonlinear filtering, refining and fight back geometric transformation like scaling spin and cropping[9,10].

3.3 Spatio-Frequency Domain Method (SFD):
The watermark is embedded by changing coefficient of applied frame of video transform.

.

3.3.1 Singular Value Decomposition (SVD):
SVD is a numerical watermarking technique which is used to get diagonal zed matrices from given matrix. In video watermark the length and coefficient of watermark can effect video watermarking technique. SVD is mathematical tool to evaluate matrices. Like A is a square matrices, size of matrix A is M x N which is decomposed into three matrices X,Y,Z so that $A=XYZ_T$. Z_T transpose of Z, X, Y are orthogonal matrix and z is square diagonal .

3.3.2 Discrete courier Transform (DCT):
It is a spread spectrum communication method in this the data is signified in terms of frequency. Embedding of watermark is done in first k highest magnitude of DCT coefficient of image data. The result found after applying DCT coefficient will be image of sum of varying magnitude and frequency. A horizontal frequency varies from left to right and a vertical frequency varies from top to bottom. Watermark in mid band gives enhanced robust and imperceptibility[15] .

3.3.3 Discrete Wavelet Transform(DWT):
In Watermarking, Discrete Wavelet Transform depend on wavelet. These frequency of wavelet varying with respect to time. Multi-resolution decomposition of image and frames of given video is possible in DWT. The wavelet is divided into four sub bands which are LL, LH, HL, HH. The first letter in sub band denotes to frequency applied for rows and second letter denotes to filter applied to columns. Watermarking in each band provide some essential advantage, watermarking in LL provide resistance against compression, watermarking in LH, HL and HH robustness against noise and filters.

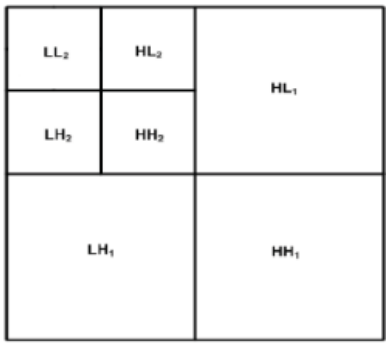

Fig 3: 2-levels DWT Scheme

Here in this table the comparative analysis of different standard watermarking techniques with respect to some significant features and types of video watermarking technique The expressions used in the table are as follows: R: Robustness, IP: Imperceptibility, S: Security, P: payload, C: Computational Cost, T: Time Complexity, RE: Reliability.[3,4]

Features	LSB	DFT	DCT	DWT	SVD
R	Less robust against geometric distortion	High robust against geometric distortion	High robust against filters	High robust against geometric distortion	High robust against geometric distortion
IP	Less compared to DFT,DCT, DWT,SVD	High	High	Better, Watermark length and key effect visual quality	Better, length of co-efficient effect visual quality
S	Less secure, usually depend on choice of key	High secure	Better, semi-private waterm arking	Better, semi-Private watermarki ng	High, Private watermar king
P	Less, limited data can be added	average	High	High	High
C	Less	Reliable cost	Reliabl e cost	Very High	High
T	Less	High	High	Very High	High
RE	Better, for multiple watermarki ng	High	High	Very High	Very High

IV. Video Watermarking Applications

There are some applications of digital video watermarking over world-wide are shown below:

4.1 Fingerprinting :

There are two type of application in video streaming where one is pay-per-view and second is Video-on-demand . In these application fingerprints policy is used in digital watermarking. by fingerprinting any person's information which is in video or image data than can find easily that person over internet if he/she breaking the rule. [6,7].

4.2 Source tracking:

Not the same recipients catch in a different way watermarked content.

4.3 Video authentication:

In Authentication, we save the signature watermark into the header folder, but the header field still be disposed to tempering. So we can easily directly embed these type of authentication information data directly as a watermark.

4.4 Content protection or Copyright protection:

Content protection or Copyright protection is important application in digital watermarking or video watermarking. To find copyright owner in video watermarking for copyright protection over world-wide network.

4.4Broadcast monitoring of video sequences:

Broadcast related to television and over television there are many type of videos, images and product broadcast. In watermarking, system put watermark on each and every video and product for this type broadcast monitoring aver channel[4,6,7].

V. Watermark Attacks

Watermark attacks are given below

5.1 Active attacks:

Hackers can hack data and make it as undetectable. but in active attack in watermarking hackers remove watermark and make it unrecognizable. This type of attack is serious for many applications as well as copy control, owner identification, fingerprinting, and proof of ownership, in which the purpose of the mark is beaten when it cannot be detected. However, it is not a thoughtful problem for authentication or covert communication.

5.2 Passive attacks:

In this attack hackers do not want to remove the present watermark in image and video. Hackers find the watermark is present or not i.e. is trying to identify a secret communication.

5.3 Geometric attacks:

Geometric attacks do not eliminate the embedded watermark itself, but it misrepresents the watermark detector synchronization with the embedded information [12,13,18].

VI. Related Work

Mehdi Fallahpour, Shervin Shirmohammadi, Mehdi Semsarzadeh, and Jiying Zhao proposed approach in paper,"Tampering Detection in Compressed Digital Video Using Watermarking", [1] that is based on the semi-fragile video watermarking technique to detect the tampering in compressed videos. The fragile watermarking method cannot differentiate the tampering from common video processing operation such as compression, sharpening, brightness increasing. To distinguish the tampering from common video processing applications semi-fragile video watermarking scheme is designed. The watermark is generated by the macroblock's and frame's indices, and watermark is embedded in highest zero quantized DCT level within each block. They have implemented and evaluated the method using the H.264/AVC codec also in order to increase the security of system algorithm also takes advantage of content-based cryptography. The method stated in this paper is used to detect

the tampering in videos in spatial and temporal domain. The method is designed in such a way that it is easy to configure the system to adjust transparency, capacity, and robustness according to specific application in hand. This method leads to smaller video distortion i.e. degradation of PSNR is 0.88dB and decrease in structural similarity index by 0.0099 with 0.05% bit rate increase.

Bhaskaran et al. proposed approach in patent , " Fragile Watermark for Detecting Tampering in images",[2] that is related to the fragile watermarks for tamper detection in images. The watermarking scheme for images which includes techniques for insertion and extraction of fragile watermark in DCT domain and to determine whether the image so watermarked has been tampered with or not. In watermark insertion process the bits of the digital signature of the hash function of image are embedded into the frequency coefficients of the image.

The tamper detection is done by extracting the watermark which is embedded during watermark insertion process from the image, hash value computed as in insertion process and verified by using public key whether the extracted watermark is valid signature of the hash value.

H.-Y. Huang, C.-H. Yang, and W.-H. Hsu, proposed approach in paper, "A video watermarking technique based on pseudo-3-D DCT and quantization index modulation," [3] that is an effective watermarking scheme using pseudo-3-D DCT and quantization index modulation (QIM). The watermark insertion process is done by adjusting the correlation between the selected blocks in uncompressed domain. The watermark is extracted by blind process. The embedding factor is calculated by using the pseudo 3-D DCT. With the help of QIM the watermark is embedded into compressed domain into the quantization regions of successive frames and secrete embedding key is generated which is further useful in extraction of the watermark. The proposed method have good transparency and robustness also the method survive against filtering, luminance change, compression and noise attacks but the proposed method is not robust against geometric transformation such as rotation, scaling, and cropping.

De Oliveira, P. R. , Andreia Fondazzi Martimiano, L. ; Delisandra Feltrim, V. ,Brasilino Marcal Zanoni, G., proposed approach in paper " Energy Consumption Analysis of the Cryptographic Key Generation Process of RSA and ECC Algorithms in Embedded Systems", states the characteristic of safety related authentication, the author in this paper presents the energy consumption analysis between the key generators for the RSA and ECC algorithms. To improve the security of communication cryptographic keys can be used between entities that are communicating for authentication process. To check the correlation between energy consumption and runtime test is conducted. They have implemented algorithm in C language and the executions were carried out in the Beagle Board platform. The ECC algorithm presented has a lower energy consumption than the RSA algorithm.

Maneli Noorkami, and Russell M. Mersereau, proposed approach in paper "Digital Video Watermarking in P-Frames With Controlled Video Bit-Rate Increase." [5] states a common approach for embedding the watermark in I-frames. They have shown that the video bit rate increase can be held to reasonable value by limiting the watermark to nonzero-quantized ac residuals in P-frames. Since the nonzero-quantized ac residuals in P-frames correspond to non-flat areas that are in motion, temporal and texture masking are exploited at the same time. They proposed watermark embedding in nonzero quantized ac residuals with spatial masking capacity in I-frames. Since locations of nonzero-quantized ac residuals is lost after decoding.

Jordi Serra-Ruiz and David Megias, proposed approach in paper " DWT and TSVQ-based semi-fragile watermarking scheme for tampering detection in remote sensing images," [6] presents the semi-fragile image watermarking scheme used in remote sensing images. The signature of hyper spectral or multispectral image is used to embed the watermark in suggested scheme. The scheme suggested in this paper detects a forgery of the watermarked image, e.g. a tampered region. The original image which is to be watermarked is segmented in 3-D blocks and, for each block, DWT and a tree structured vector quantizer is built. By using iterative algorithm these trees manipulated the selected condition gets satisfied by resulting image. The tampering attacks can be avoided by partially modifying each tree according to secret key. The internal structure of the tree is determined by using this secret key. The trees are built using only the LL sub-band of the DWT to make watermarked image robust against near lossless compression. The results show that the method is robust against JPEG2000 compression and works correctly with remote sensing images also detects copy and replace attacks within same image segments.

J. Zhang, A. T. S. Ho, G. Qiu, and P. Marziliano, proposed approach in paper, " Robust video watermarking of H.264/AVC," [7] that is based on a framework for detecting tampered information in digital videos. Using the proposed technique it is possible to detect several types of tampering with a pixel granularity. The framework uses a combination of temporal and spatial watermarks that do not decrease the perceived quality of the host videos. We use a modified version of Quantization Index Modulation (QIM) algorithm to store the watermarks. Since QIM is a fragile watermarking scheme, it is possible to detect local, global, and temporal tampers and also estimate the attack type. The framework is fast, robust, and accurate.

Y. Wang and A. Pearmain, proposed approach in paper, " Blind MPEG-2 video watermarking in DCT domain robust against scaling," [8] that is blind watermarking technique which does not need original information in watermark detection process, as explained in are more desirable in watermark extraction. The DCT domain blind MPEG-2 watermarking technique is presented, which is generally robust against geometric transformation such as arbitrary ratio scaling. The turbo codes are used for error correction. The method is used for block-DCT-based video compression techniques. Simplicity and blindness are the main advantage of proposed scheme.

VII. CONCLUSION

Conclusion of this review is that there are many type of watermark techniques which are helpful to protect the data in the form of image, audio, text and video .so we can use these techniques of watermark in video where video is combination of sequence of frames. And we can create some different type of equation to hide data or image data in frames of video.

REFERENCES

[1] Jashandeep Kaur Kang, Rakesh Kumar, Kamaljeet Kainth, " *Review paper on video watermarking*" International journal of advanced research in computer science and software engineering, vol.6, issue 6, june 2016.

[2] Ankitha.A.Nayak et al. Int. Journal of Engineering Research and Applications .ISSN : 2248-9622, Vol. 4, Issue 12(Part 6), December 2014, pp.39-44

[3] Swati Patel ,Anilkumar Katharotiya, Mahesh Goyani, " A survey on digital video watermarking" Int. J. Comp. Tech. Appl., Vol 2 (6), 3015-3018 .

[4] T. L. Gilbert, *Formulation, Foundations and Applications of the Phenomenological Theory of Ferromagnetism*, Ph.D. dissertation, Illinois Inst. Tech., Chicago, IL, 1956, unpublished.

[5] Dr.V.Seenivasagam, S. Subbulakshmi, S. Radhamani, "A survey on video watermarkingand its applications" International journal of advanced research in computer science and software engineering, vol 4, issue 3, march 2014

[6] Mahima Jacob, Saurabh Mitra," Video Watermarking Techniques", IJRTE, Vol 4, Pp 1-4,2015

[7] Lalit Kumar Saini, Vishal Shrivastava," A Survey of Digital Watermarking Techniques and its Applications", IJCST, Vol 2, Pp 70-73,2014

[8] Rakesh Ahuja, S. S. Bedi," All Aspects of Digital Video Watermarking Under an Umbrella", Ijigsp, Vol 12, Pp 54-73, 2015

[9] Miss. Shital Divekar, Prof. Nitin Dawande, Prof. Suresh Rode, "Review on video watermarking techniques" International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 5, May 2016

[10] Sourav Bhattacharya, T. Chattopadhyay, Arpan Pal, "A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC", IEEE 2006

[11] Gopika V Mane, G. G. Chiddarwar, "Review Paper on Video Watermarking Techniques", *International Journal of Scientific and Research Publications*, Volume 3, Issue 4, April 2013 1 ISSN 2250-3153

[12] Wiem Trabelsi, Mohamed Heny Selmi, "Multi-signature robust video watermarking" *1st International Conference on Advanced Technologies for Signal and Image Processing* , Sousse, Tunisia, March 2014.

[13] Xing Chang, Weilin Wang, Jianyu Zhao, Li Zhang,"A Survey of Digital Video Watermarking",2011 Seventh International Conference on Natural Computation,61-65.

[14] Peter Meerwald, Andreas Uhl, "Blind motion-compensated video watermarking", In Proceedings of the 2008 IEEE Conference on Multimedia and Expo, ICME '08, pp. 357-360, Hannover, Germany, June 23 - 26, 2010.

[15] Maneli Noorkami, Russell M. Mersereau, Fellow, IEEE"Digital Video watermarking in P-Frames With Controlled Video Bit-Rate Increase, " IEEE Transactions on Information Forensic and Security, Vol. 3, No. 3, 2008.

[16] Liang Huang, "Research on the MPEG-2 Video Watermarking Scheme Based on Spread Spectrum Technology," iccet, vol. 2, pp.408-411, 2009 International Conference on Computer Engineering and Technology, 2009.

[17] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," IEEET on Multi., vol. 4, no. 1, pp. 121-128, March 2002.

[18] Mehdi Fallahpour, Shervin Shirmohammadi, Mehdi Semsarzadeh, and Jiying Zhao, "Tampering Detection in Compressed Digital Video Using Watermarking," IEEE Transactions on Insrumentation and Measurement, vol. 63, no. 5, May 2014.

[19] Bhaskaran et al.," Fragile Watermark for Detecting Tampering in images", U. S. Patent Number 6064764, may 16,2000.

[20] H.-Y. Huang, C.-H. Yang, and W.-H. Hsu, "A video watermarking technique based on pseudo-3-D DCT and quantization index modulation," IEEE Trans Inf. Forensics Security, vol. 5, no. 4, pp. 625–637, Dec. 2010.

[21] De Oliveira, P. R. ,Andreia Fondazzi Martimiano, L. ; Delisandra Feltrim, V. ; Brasilino Marcal Zanoni, G.," Energy Consumption Analysis of the Cryptographic Key Generation Process of RSA and ECC Algorithms in Embedded Systems", Latin America Transactions, IEEE (Revista IEEE America Latina) Volume:12 , Issue: 6 , Pages: 1141-1148, sept 2014. .

[22] Jordi Serra-Ruiz and David Megias, "DWT and TSVQ-based semi-fragile watermarking scheme for tampering detection in remote sensing images," 2010 Fourth Pacific-Rim Symposium on Image and Video Technology.

[23] J. Zhang, A. T. S. Ho, G. Qiu, and P. Marziliano, "Roubust video watermarking of H.264/AVC," IEEE Trans. Circuits Syst., vol. 54, no. 2, pp. 205–209, Feb. 2007.

[24] Y. Wang and A. Pearmain," Blind MPEG-2 video watermarking in DCT domainrobust against scaling," IEE Proc.-Vis. Image Signal Process., Vol. 153, No. 5, October 2006.