IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 9, Issue 6, Dec - Jan 2022
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

A Guide tour on security techniques for multimedia data

Dr.S.Ponni alias sathya[1] , Dr.S.Ramakrishnan[2] , Dr.S.Nithya[3]

[1]Assistant Professor(SS), IT department, Dr.Mahalingam college of Engineering and Technology, Pollachi.

[2]Professor, IT department, Dr.Mahalingamcollege of Engineering and Technology, Pollachi.

[3]Assistant Professor(SS), IT department, Dr.Mahalingam college of Engineering and Technology, Pollachi.

Abstract

The multimedia is a mixture of various forms of data like test, images, graphics and video. In the current scenario, the usage of multimedia data by society has increased. The content transferred between the sender and receiver, has all the possibility to be accessed by the unauthorized party and also the original content is subjected to various attacks such as digital signal processing attacks, image processing attacks, video processing attacks, false positive attacks and geometric attacks. To provide the security to the content, avoid the illegal communication and resolve the ownership problem, the watermarking based technique is adapted. This paper exposes the overview about watermarking technique, reveals various researches in recent past for multimedia data and discusses the applications of watermarking.

Keywords: Multimedia, Video watermarking, Data security, Copy right

1. Introduction:

In worldwide, the transfer of digital product through the network has become high. The customer wants to easily buy their digital product through the internet in the digital market. But the authentication was not ensured during the transaction. For the purpose of certifying the transaction process and providing the legal ownership rights to the authorized party, the concept of watermarking has been applied to the multimedia data. The digital watermarking is used to interface the gap between distribution of digital data and copyright. In the source data, digital watermarks are commonly inserted as a plain text or a transformed signal using an embedding algorithm with secret key and a noise pattern. The effective watermarking technique should maintain the balance among the robustness, imperceptibility and security.

2. Watermarking Framework

The watermark is a secret data which may be a text, image or audio signal, embedded into the source data by adapting the suitable algorithm. The source data may be text, image, audio or video. The effectiveness of the algorithm is based on the secret key and working methodology. The robustness of the algorithm depends on the appropriate technique adapted for embedding the watermark within the source data. The secret key plays a vital role in the watermark embedding and extraction process. In embedding phase the secret data is inserted into the source data, which can be detected in the extraction phase from the watermarked data with the help of secret key. The embedding and extraction process are shown in Fig.1 and Fig.2 respectively.

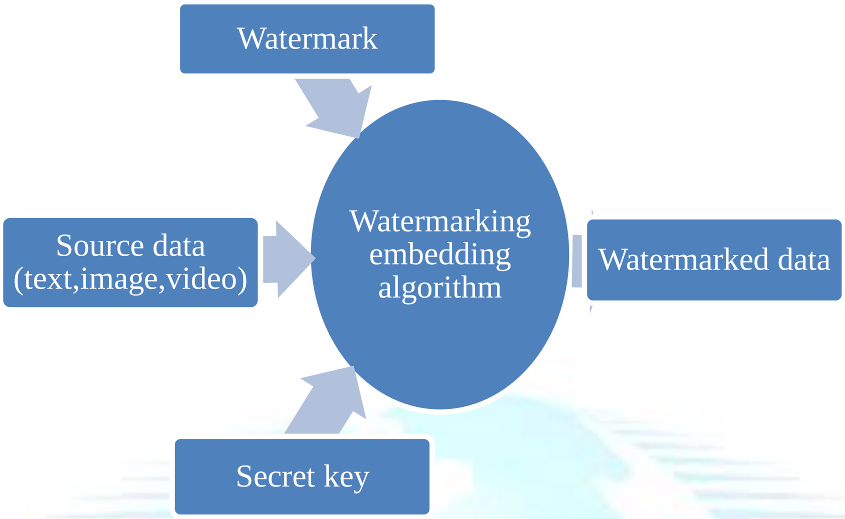
Watermark
Source data (text,image,video)
Watermarking embedding algorithm
Watermarked data
Secret key

Figure 1 .Flow of Watermark Embedding

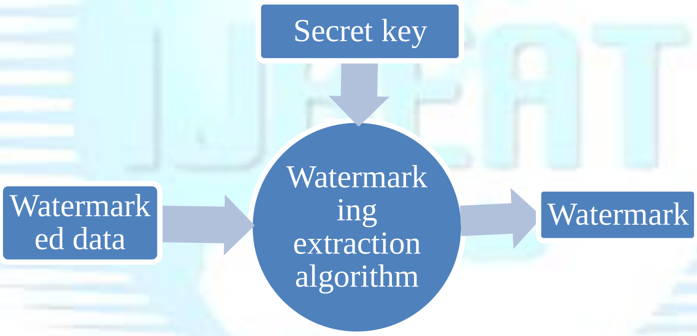

Figure 2 .Flow of Watermark Extraction

2.1 Classifications in watermarking

The watermarking system is primarily categorized into four types based on the document used, perception, application and domain. Digital watermarking is applicable to various types of documents such as text, audio, image and video. Based on the perception, it can be classified into visible and invisible watermarks. In general, invisible watermarks are mostly used. Based on the application it may be a source or destination.

According to the working domain, video watermarking techniques are classified in to spatial domain, frequency domain, hybrid and compressed domain. Lastly, extraction methods can be categorized as private, semi-private and public watermarking, according to the necessity of the original media.

The effective video watermarking remains a challenging problem since the original video contains large volume of redundant data, on the other hand keeping more robustness for protecting ownership rights is tough. According to the robustness the watermarking method can be classified into robust, semi-fragile and fragile. Different levels of robustness will be chosen for different applications according to the requirement. Applications for copyright protection would require using a robust watermark. The classification of watermarking is shown in Fig.3.

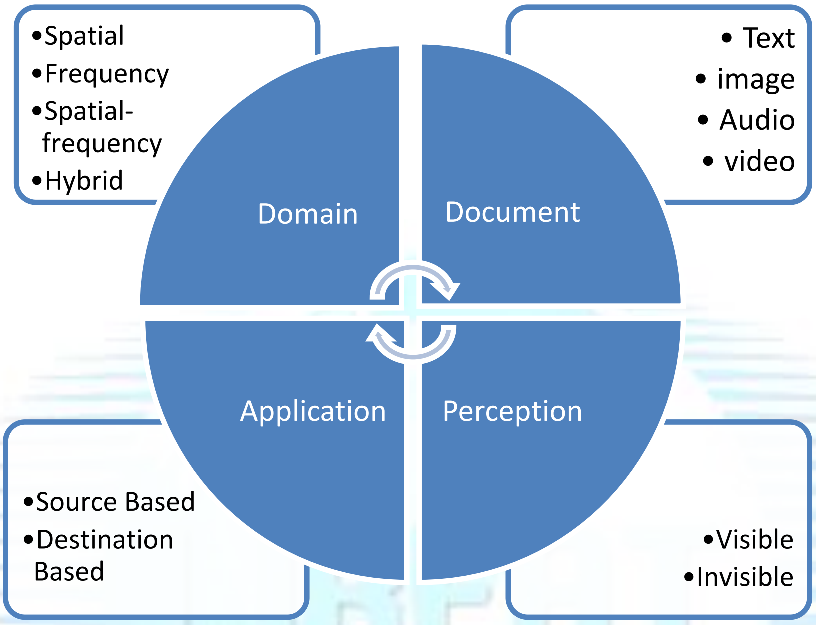

Figure 3. Classifications in watermarking

Apparently any image watermarking technique can be extended to watermark videos, but in reality video watermarking techniques need to meet other challenges than that in image watermarking schemes such as large volume of redundancy exists among the frames and imbalance between the motionless and motion frames, real-time requirements in the video broadcasting etc. Watermarked video sequences are very much susceptible to pirate attacks such as frame averaging, frame swapping, statistical analysis, digital-analog conversion and lossy compressions.

3. Video watermarking

Video watermarking is the process of authenticating the video by applying various watermarking technique. Generally the binary image or audio signal is embedded as a watermark. The video may be a compressed or uncompressed video. Many watermarking algorithm developed for images are extended to videos but due to the following reasons they are not properly working for videos.

i) Between the frames there is a huge amount of redundant data.

ii) The video contains both motion and motionless frames.

iii) Not suitable for real time or streaming video applications.

The following terminologies are important for the design of Video Watermarking systems. Which are represented in the Table 1.

Table 1.Various terminologies used in video watermarking

Terminology	**Definitions**
Digital video	Group of frames
Robustness	To resist the modification or removal of watermark from the source
Imperceptibility	Changes according to the Human visual system
Non detectable	The inserted watermark should be non-detectable.
Data Pay load	Amount of data to be hide with in the video
Complexity	It depends on the watermarking embedding and extraction algorithm.
Security	Provides the authorized access to the watermarked data

In order to identify the watermark, there are two different techniques available, which are

- Blind watermarking:
  The watermark can be detected without the support of source data.
- Non-blind watermarking:
  The watermark can be detected with the help of source document.

Various researchers have developed variety of algorithm for securing the video from unauthorized access. Each algorithm has its merits and demerits with respect to the robustness and imperceptibility of the watermark and the methodology resist for various kinds of attacks such as signal processing attacks, image processing attacks, geometric attacks, false positive attack and video processing attack .These methodologies are discussed as follows.

Majid Masoumi et al [3] proposed wavelet based a video copyright protection. In this methodology the color video is taken for processing, 3D wavelet transform was applied into the motion frames and then the coefficients of middle and high frequency subbands are selected for watermark embedding. The spread spectrum technique was applied for the purpose of selecting the wavelet coefficients for watermark embedding. The pseudo random numbers were used for selecting the location to insert the watermark. This methodology was robust against the various image and video processing attacks such as filtering, addition of noise, lossy compression and frame oriented attacks. This methodology was blind hence it was used for public watermarking system.

RangdingWang et al [4] proposed video authentication system for H.264 and AVC videos. This methodology serves the solution for content based copyright protection and video authentication. The authentication code was generated based on the consistent features extracted from the frame block of the video. This code can be used to detect the malicious attacks occurred during the processing. Authentication code was embedded into the diagonally presented DCT coefficients using modulation concept. The watermark was the frame index of the video frame. The tampering can be noticed by mismatch between the observed and extracted value of frame index. This method was robust against the common signal processing attacks.

Po-Chyi Su et al [5] proposed a watermarking technique for authenticating the content of H.264/AVC. The serial number of the video segments is selected as watermark, which were embedded into the indices of the non-zero quantization coefficients of the individual frames. This methodology addresses the issue of synchronized watermark detection by adapting the frequently changed frames for computing the distortion; hence it supports to find the sequence of the embedded watermark. This watermarking scheme can protect the watermark from transcoding process and also produce good imperceptibility to the watermark and video.

He Yingliang et al [6] proposed a watermarking algorithm for Video-on Demand service of the compressed video. The spreading of CDMA approaches was applied for modulating the copyright and user information which are selected as a watermark data; it was embedded into the luminance component of the video frame. The watermark embedding area was the, orderly first non-zero coefficients of the 4*4 block in the I-frame. The error compensation technique was applied for reducing the distortion transpired in the quantization process. The XOR based rule was employed in the watermark embedding because the number of non-zero coefficients is comparatively lesser, after the quantization. This methodology was used to protect copyright and also tracking the piracy.

Osama S. Faragallah [7] prosed, watermarking technique for protecting video using DWT and SVD. The DWT was applied into video frames to decompose the frame up to 2 levels. The HH, LH and HL bands were selected for watermark embedding. The DWT and SVD were used to obtain the features based on frequency localization of transform and capture the geometric information of frames. In this technique error correction code was applied and the watermark data was embedded with temporal and spatial redundancy. The aim of this methodology was to increase the robustness against the bit oriented attacks, desynchronization attacks, image oriented attacks and video processing attacks.

Majid Masoumi et al [8] proposed a data hiding technique based on spatial and temporal characteristics for ownership verification of video data. This methodology was framed for avoiding the malicious replication and dissemination of digital content. This technique was outlined with code division multiple access technique and discrete wavelet transform. By using the CDMA with pseudo random numbers the binary watermark was disseminated into the HH, LH and HL subbands. The R component of the video was only taken for watermarking. This method was useful for public oriented applications hence it was blind. This method was highly resistant against the various frame based attacks such as frame transposing, dropping, averaging and image processing attacks such as addition of noise, resizing, filtering and lossy compression. This method was assessed by various video quality metrics namely PSNR, MSE and SSIM.

Marwen hasnaoui et al [9] proposed a video watermarking technique based on quantization index modulation technique. This method was used to minimize the error probability with respect to the addition of white and Gaussian noise. The data payload was also considered. In this methodology, the experiment was conducted for one hour of video data.
Xiyao Liu et al [10] proposed a zero watermarking scheme for protecting 3D videos. In this methodology the master share generated from the temporally informative representative images identified from the video frames. Then the ownership shares are generated based on the copyright information about the user and master share. Those shares are formulated based on the Visual Secret Sharing scheme, which stores the copyright information about the users. The advantage of this methodology was to protect from distortion and exhibits robustness against the video processing attacks. This algorithm was not resilient against the geometrical attacks such as rotation and cropping.

Chun-Shien Lu et al [11] proposed a frame dependent watermarking technique for VLC domain. This methodology addresses the various issues such as real time detection, bit-rate control and resistance against various attacks. The watermark embedding was based on the variable length code word. The transparent watermark was embedded into the appropriate position. This algorithm withstand the attacks like copy detection, collusion and watermark estimation attacks.

Yuan-GenWang et al [12] proposed, watermarking technique for audio video coding standard. In this methodology, the watermark was embedded by two ways. In first way it was embedded into the luminance component of the video. The embedding location was selected based on the particle swarm optimization technique (PSO) hence it was resistant against the signal processing attacks. In second way, the watermark was embedded into the chrominance component based on the just noticeable distortion. The watermark was successfully detected by entropy coding technique.

Ta Minh Thanha et al [13] proposed, frame patch matching based watermarking technique for video. The KAZE feature matching algorithm was employed for matching the features of frame patch with the all the frames in the video. This matching was performed for selecting the watermark embedding and extraction region. The watermark was embedded into the DCT based randomly selected blocks in the matched region. In extraction stage, the watermark was extracted from the distorted video based on the feature points and RST (rotation, scaling, and translation) parameters. This methodology was robust against the temporal attacks, video processing attacks and geometric attacks. This algorithm was mainly focused to avoid the illegal distribution of video data.

Rupachandra Singh et al [14] proposed, visual cryptography with scene change detection based video watermarking technique for providing the security to the copy right. The DWT was applied into the source video. The dissimilar parts of single watermark was embedded into the different scenes based on the owner share, it was devised based on the frame mean of available frames in a scene and the binary watermark. Then the identification share was modeled based on the frame mean of the attacked video. This algorithm was robust against various attacks such as impulse noise, Gaussian noise injection, cropping, compression, filtering, blurring, gamma correction and frame based attacks.

Roopalakshmi et al [15] proposed a technique for video copy detection based on PCA and audio fingerprint. This methodology was designed for content based copy detection. The audio feature with principal component analysis was used. In this algorithm, the feature vectors are calculated in multiple stages, initially MFCC with spectral descriptors was applied to detect the audio features. In the next stage these features are processed by principal component analysis for obtaining compact feature. The selected fingerprint was matched by using weighted Euclidean distance. The experiment was tested for TRECVID-2007 dataset. The indexing method was used to accurately detect the existing copy. This algorithm was resistant against the video transformation and editing attack.

YanLiu et al [16] proposed a watermarking technique based on radon transform with one dimensional discrete Fourier transform. The highest temporal frequency based frames were taken for watermark embedding. The watermark was the fence shaped pattern. The radon transform was applied into the selected frames in the video, and then the pattern was embedded into the selected frames. This algorithm was robust against the geometric attacks such as translation, aspect-ratio changes, rotation and video processing attacks such as frame swapping, frame dropping, addition of noise, filtering, histogram equalization and lighting change. This methodology improved the fidelity of the watermarked video.

Hefei Ling et al [17] proposed a watermarking technique for video based on the affine invariant features. This technique was appropriate for DCT based compressed video. In this methodology, Harris affine detector was used to obtain the invariant feature points. The decoding process was accomplished by making transformation between block DCT and sub-block DCT. This algorithm was robust against the geometric distortions such as scaling, rotation, aspect ratio changes, cropping, signal processing attacks, frame conversion, video format conversion and frame dropping.

Nilkanta Sahu et al [18] proposed, watermarking technique for video based on Scale invariant feature transform. The video scene was identified based on side plane. In this algorithm, the embedding location was identified and the SIFT features were generated based on the changed intensity value from the side plane of the source video. These features were used as watermark. This algorithm was robust against the attacks such as temporal scaling and frame dropping.

Amlan Karmakar et al [19] proposed a video watermarking scheme for blind video using Discrete cosine transform. In this method watermark was embedded in the middle position of the luminance component of video. The square block from the luminance channel was chosen for embedding. This embedding block was varied for consecutive frames. The Zernike moments of the selected square blocks were computed for extraction of the watermark. The random number generator was used for embedding and extraction process. This method was resistant for various attacks such as rotation, collusion and video processing attacks.

Agilandeeswari et al [20] proposed a watermarking technique for video based on fuzzy inference system with neural network. This methodology mainly concentrates about the payload, robustness and imperceptibility. The Bi-directional Associative Memory was used as a neural network for making the weighted matrix, which was embedded into the entire frames available in the video. The DWT was applied into the host video and the embedding process was performed in the middle level frequency band of the all (Y,Cb,Cr) components with different threshold. Fuzzy inference system was used for generating the different threshold values based on the attributes of luminance, edge values of the frames and texture. This algorithm outperforms in terms of imperceptibility and robustness for various attacks.

Tanima Dutta et al [21] proposed a compressed domain based watermarking technique to avoid the copyright for HEVC video standard. The invisible watermark was embedded into the predicted intra block with size (4*4) of the encoded video .The embedding region was selected by random key generator. The embedding algoritm was designed in align with the strength of the compressed domain and features of the HEVC video. This methodology was used to reduce both the growth of video bit rate and the degradation of the visual quality of the video. This algorithm withstands different kinds of attacks such as compression, addition of noise and filtering and also maintained the robustness and quality with acceptable level. This approach was applicable to public applications because it was blind.

Pejman Rasti et al [22] proposed a watermarking technique for color video based on entropy analysis and QR decomposition. In this algorithm, the motionless frames of the each channel in the video were separated by block based approach. The embedding region was selected based on the entropy analysis; the entropy of the individual block was compared with the average entropy of the available blocks. The lower entropy block was selected for watermark embedding. At the end the moving frames were combined with the watermarked frame to produce the watermarked video. This method was highly resistant against the signal processing attacks.

Yanjiao Shi et al [23] proposed an authentication technique for video based on moving object. In this method dual watermarking was performed. Initially each moving object of the relevant frame was embedded with the relevant frame index for the purpose of reducing the temporal attacks. Subsequently, the second watermark was found by combining the content of the moving object with the authentication code which was embedded into the frame. In the reverse process the watermark was extracted by synthesized frame method. This methodology was resistant for spatial and temporal based attacks.

Ponni et al [24] proposed a watermarking technique for video based on the Fibonacci and DWT with SVD. In this methodology the Fibonacci sequence was used for making the key frame selection table. The LH sub-band was selected for watermark embedding. The Fibonacci-Lucas transform was applied to scramble the watermark image. In the embedding phase, the singular value of the scrambled watermark block was added to the singular value of the key frame with suitable scaling factor. This methodology was robust against the various attacks such as image processing, video processing.

There are number of other multimedia security algorithms proposed by various researchers, some of the cited algorithms are listed in the Table 2.

Table 2. Various Multimedia Security Techniques

S.No	***Algorithm name***	***Author details***	***Year of publication***
1.	Content adaptive watermarking	Yu-Tzu Lin et al.	2008
2.	HDWT-based watermarking technique	Ester Yen et al.	2008
3.	Buffer sharing based Video watermarking technique	Ju Wang et al.	2009
4.	2D-scan-based wavelet watermarking technique	Sourour et al.	2009
5.	Hardware assisted watermarking technique	Elias et al.	2009
6.	Dual watermarking algorithm for AVS video	Yuan-GenWang et al.	2009
7.	Fragile watermarking approach for satellite video	Chuen-Ching Wang et al.	2010
8.	Visual cues and MPEG-7 descriptors based technique	Onur Kuçuktunç, M et al.	2010
9.	Particle swarm optimization based dither modulation scheme	C.H. Wua et al.	2011
10.	Neural Watermarking Approach	Jose Aguilar et al.	2011
11.	Longest common substring technique for watermark detection	Taha M. Mohamed et al.	2011
12.	MCEA based passive forensics scheme	Qiong Dong et al.	2012
13.	Dual watermarking algorithm for Video-on-Demand service	He Yingliang et al.	2012
14.	SURF based hashing algorithm	Gaobo Yang et al.	2012
15.	Reliable information embedding algorithm	Qing Chen et al.	2012
16.	Histogram Modification based Watermarking technique.	M.Cedillo-Hernandez et al.	2013
17.	Visual cryptography based Video watermarking technique.	Th. Rupachandra et al.	2013

18.	Dual tree complex wavelet transform based watermarking technique.	Gaurav Bhatnagar et al.	2013
19.	segment matching for detecting temporal-based video copies	Chih-Yi Chiu n et al.	2013
20.	spatio temporal video pattern based technique	Liujuan Cao et al.	2013
21.	spatio-temporal HVS and DCT based algorithm	Antonio Cedillo et al.	2014
22.	DWT-SVD based Video Watermarking	Divjot Kaur Thind et al.	2015
23.	Colour Based Video Copy Detection technique	Renu Mary Thomas et al.	2015
24.	Digital video tampering detection	K. Sitara et al.	2016
25.	Real-time spatial scalable video coding based watermarking scheme	Adamu Muhammad Buhari et al.	2016
26.	video encryption based chaos system	Wassim Hamidouche et al.,	2017
27.	Tunable data hiding in partially encrypted H.264/AVC videos	Dawen Xu et al.	2017
28.	Multiplicative video watermarking technique	Faride Madine et al.	2018
29.	Fingerprinting based multimedia content broadcasting system	Minoru Kuribayashi et al.	2018
30.	Fibonacci based video watermarking in DWT–SVD domain	Ponni Alias Sathya, S. et al.	2018
31.	YCbCr Color Space based watermarking	Tan. Y et al.	2019
32.	HEVC Integrity Verification Scheme	Osama s. Faragallah et al.	2020
33.	Resolving ownership rights of video data	Ponni alias sathya et al.	2021
34.	Bit stream domain based video watermarking	Jing Sun et al.	2021

3.1 Applications of Video Watermarking

Video watermarking is applied in to various fields for securing their data. The various applications are as follows,

- Broad cast monitoring
- Error recovery
- Proof of ownership
- Steganography
- Cryptography
- Authentication
- Fingerprinting
- Copy right control
- Data compression

- Video tagging

4. Conclusion

This paper focuses the overview of watermarking system and discussed the literature survey of video watermarking techniques. From the survey, the following weakness are inferred

- The existing watermarking algorithm does not maintain the trade-off between robustness, imperceptibility.
- The watermark is not robust to attacks which are specifically targeted to videos, such as frame dropping, averaging and statistical analysis.
- The bit rate of the watermark is low. Some algorithms embed only one bit information as the watermark.
- Existing techniques are not considering the audio channel in video.
- None of the existing watermarking schemes resists to all the attacks such as signal processing attacks, image processing attacks, geometric attacks, video processing attacks and false positive attacks.

References

1. *Asikuzzaman, M. and Pickering, M.R., 2017. An overview of digital video watermarking. IEEE Transactions on Circuits and Systems for Video Technology.*
2. *Chang, X., Wang, W., Zhao, J. and Zhang, L., 2011, July. A survey of digital video watermarking. In Natural Computation (ICNC), 2011 Seventh International Conference on (Vol. 1, pp. 61-65). IEEE.*
3. *Masoumi, M. and Amiri, S., 2013. A blind scene-based watermarking for video copyright protection. AEU-International Journal of Electronics and Communications, 67(6), pp.528-535.*
4. *Masoumi, M., Rezaei, M. and Hamza, A.B., 2015. A blind spatio-temporal data hiding for video ownership verification in frequency domain. AEU-International Journal of Electronics and Communications, 69(12), pp.1868-1879.*
5. *Xu, D., Wang, R. and Wang, J., 2011. A novel watermarking scheme for H. 264/AVC video authentication. Signal Processing: Image Communication, 26(6), pp.267-279.*
6. *Su, P.C., Wu, C.S., Chen, F., Wu, C.Y. and Wu, Y.C., 2011. A practical design of digital video watermarking in H. 264/AVC for content authentication. Signal Processing: Image Communication, 26(8-9), pp.413-426.*
7. *He, Y., Yang, G. and Zhu, N., 2012. A real-time dual watermarking algorithm of H. 264/AVC video stream for Video-on-Demand service. AEU-International Journal of Electronics and Communications, 66(4), pp.305-312.*
8. *Faragallah, O.S., 2013. Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain. AEU-International Journal of Electronics and Communications, 67(3), pp.189-196.*
9. *Hasnaoui, M. and Mitrea, M., 2014. Multi-symbol QIM video watermarking. Signal Processing: Image Communication, 29(1), pp.107-127.*
10. *Liu, X., Zhao, R., Li, F., Liao, S., Ding, Y. and Zou, B., 2017. Novel robust zero-watermarking scheme for digital rights management of 3D videos. Signal Processing: Image Communication, 54, pp.140-151.*
11. *Lu, C.S., Chen, J.R. and Fan, K.C., 2005. Real-time frame-dependent video watermarking in VLC domain. Signal Processing: Image Communication, 20(7), pp.624-642.*
12. *Wang, Y.G., Lu, Z.M., Fan, L. and Zheng, Y., 2009. Robust dual watermarking algorithm for AVS video. Signal Processing: Image Communication, 24(4), pp.333-344.*
13. *Thanh, T.M., Hiep, P.T., Tam, T.M. and Tanaka, K., 2014. Robust semi-blind video watermarking based on frame-patch matching. AEU-International Journal of Electronics and Communications, 68(10), pp.1007-1015.*
14. *Singh, T.R., Singh, K.M. and Roy, S., 2013. Video watermarking scheme based on visual cryptography and scene change detection. AEU-International Journal of Electronics and Communications, 67(8), pp.645-651.*
15. *Roopalakshmi, R. and Reddy, G.R.M., 2011. A novel approach to video copy detection using audio fingerprints and PCA. Procedia Computer Science, 5, pp.149-156.*
16. *Liu, Y. and Zhao, J., 2010. A new video watermarking algorithm based on 1D DFT and Radon transform. Signal Processing, 90(2), pp.626-639.*

17. *Ling, H., Wang, L., Zou, F., Lu, Z. and Li, P., 2011. Robust video watermarking based on affine invariant regions in the compressed domain. Signal Processing, 91(8), pp.1863-1875.*
18. *Sahu, N. and Sur, A., 2017. SIFT based video watermarking resistant to temporal scaling. Journal of Visual Communication and Image Representation, 45, pp.77-86.*
19. *Karmakar, A., Phadikar, A., Phadikar, B.S. and Maity, G.K., 2016. A blind video watermarking scheme resistant to rotation and collusion attacks. Journal of king saud university-computer and information sciences, 28(2), pp.199-210.*
20. *Loganathan, A. and Kaliyaperumal, G., 2016. An adaptive HVS based video watermarking scheme for multiple watermarks using BAM neural networks and fuzzy inference system. Expert Systems with Applications, 63, pp.412-434.*
21. *Dutta, T. and Gupta, H.P., 2016. A robust watermarking framework for High Efficiency Video Coding (HEVC)–Encoded video with blind extraction process. Journal of Visual Communication and Image Representation, 38, pp.29-44.*
22. *Rasti, P., Samiei, S., Agoyi, M., Escalera, S. and Anbarjafari, G., 2016. Robust non-blind color video watermarking using QR decomposition and entropy analysis. Journal of Visual Communication and Image Representation, 38, pp.838-847.*
23. *Ponni alias Sathya S., Ramakrishnan S., 19 January 2018, 'Fibonacci Based Key Frame Selection and Scrambling for Video Watermarking in DWT-SVD Domain', Springer - Wireless Personal Communications, (https://doi.org/10.1007/s11277-018-5252-1), Print ISSN 0929-6212, Vol. 102,No. 2, pp.2011-2031.*
24. *Shi Y, Qi M, Yi Y, Zhang M, Kong J. Object based dual watermarking for video authentication. Optik-International Journal for Light and Electron Optics. 2013 Oct 1;124(19):3827-34.*
25. *S Ponni alias sathya et al 2021 J. Phys.: Conf. Ser. 1767 012053*
26. *J. Sun, X. Jiang, J. Liu, F. Zhang and C. Li, "An anti-recompression video watermarking algorithm in bitstream domain," in Tsinghua Science and Technology, vol. 26, no. 2, pp. 154-162, April 2021, doi: 10.26599/TST.2019.9010050.*