Digital Video Watermarking: Issues and Challenges

Md Shahid and Pradeep Kumar

Abstract: A pilfered duplicate of a digital video would be easily disseminated to the global audience because of the rapid high-speed internet. Due to impeccably replicable nature of digital video, numerous unlawful duplicates of the original video can be made. A video can undergo several intentional attacks like frame dropping, averaging, cropping and median filtering and unintentional attacks like the addition of noise and compression which can compromise copyright information, thereby denying the authentication. Hence techniques are needed to secure copyrights of the proprietor and counteract illegal copying. One of the techniques is Video Watermarking strategy for concealing some sort of information into digital video sequences that are orders of successive still frames. In this paper, we study properties of video watermarking, the arrangement of computerized video watermarking systems, watermark attacks, its applications, issues and challenges for video watermarking. At last, we propose some future research directions.

***Index Terms*—** Watermarking techniques, Attacks, LSB, DWT, DCT, DFT, FFT, SVD.

I. INTRODUCTION

A large amount of digital multimedia data is available today, which can be perfectly copied and rapidly disseminated at large scale. This consequently has raised concerns from the content owners, when they realized that traditional protection mechanisms, such as encryption, were no longer sufficient. Sooner or later, digital content has got to be decrypted and to be presented to users. At this very moment, the protection offered by encryption no longer exists. As a result, digital watermarking has been studied as a complementary technology. After Image watermarking scientist invented video watermarking [1, 2]. Watermarking is a process of embedding copyright information into the cover-data, also called host- data in order to protect the intellectual right and the originality of cover data. The host-data can be text, audio, video, etc. It is just an extension of the watermarking concept [3]. With the same and optimized length of the video, video watermarking allows embedding more data without degrading
the quality of the host-video much. A digital video is made of a sequence of still images/frames. Video watermarking hides the data-information about the authenticity or integrity of host- video in the frames of host-video. One can either select some frames of the host video or all to embed a watermark into video. This process of embedding watermark into video is called video watermarking [1]. Both of the data hiding techniques- Steganography as well as watermarking use similar techniques to hide information into host-data. And

both of them are used to hide information but their goals are different. In Digital Watermarking the content owner is concerned about the quality of host-data as well as integrity of watermark. In Steganography, the sender and the recipient of the data are more concerned about integrity of hidden information only, which is encoded in host-data and it is hidden only unlike watermark which can even be visible to the public.

2. General Properties of Video Watermarking

Some of the general properties of video watermarking are given below, which play a very significant role in video watermarking:

2.1 Imperceptibility:

The watermark should be imperceptible in such a way that third person should not be able to find out whether a video is watermarked or not [4].

2.2 Robustness:

Whenever a video is shared there are some distortions. The watermark should be robust against malicious attacks in such a way that even if the cover video changes, copyright data, which is embedded into cover video, should not get affected [5, 6].

2.3 Time complexity and Computational cost:

Cost of embedding a watermark into host- data and to extract the embedded watermark from the cover data should be less [4].

2.4 Capacity and Payload:

The amount of data to be embedded in cover data or host data is called capacity. Payload is the number of watermark bits in the cover data. Number of watermark bits in the host-data varies from one application to other [5, 7].

2.5 Security:

The watermark and original data should not be accessible to the unauthorized user. Watermark and original data should not be affected by any form of attacks [4, 5].

3. CLASSIFICATION OF VIDEO WATERMARKING TECHNIQUE

In the Fig 2, classification of video watermarking is shown which has been done depending upon perception and domain.

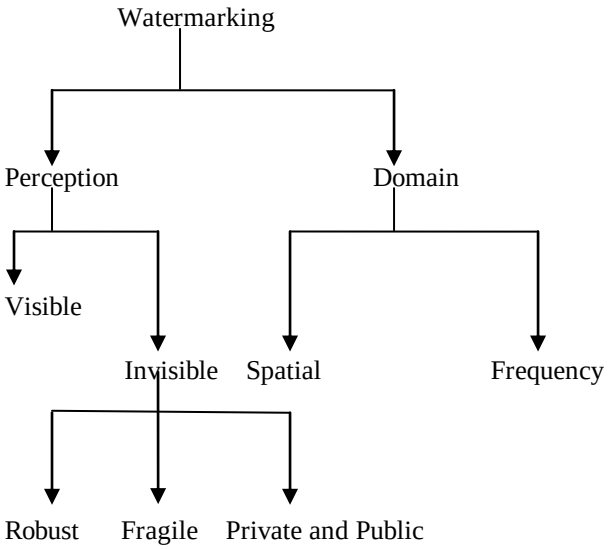

Fig 2: Classification of Video Watermarking Techniques.

3.1 Spatial Domain Method (SDM):

In the spatial domain method, a watermark is embedded by modifying the pixel value; which is made of digital information of the host video [4, 9]. This method is faster as compared to Frequency domain in simplicity and less computational complexity [5]. This method is less robust to geometric attacks and less resistant to noise, compression and low pass filtering [6].

3.1.1 Least Significant Bit (LSB):

It is simplest watermarking technique; the watermark is directly embedded by changing some of the lower-oder bits of each pixel. The amount of watermark data in LSB technique is very less and restricted [7]. The least significant bit (LSB) technique is used for simple operation to embed information in a cover image or frame. The LSB technique is that inside of a cover, image pixels are changed by bits of secret message.

3.1.2 Correlation -Based Technique:

It is one of the spatial domain techniques of watermarking, in this approach of digital watermarking; the watermark is embedded by incorporating pseudorandom noise pattern to luminance value of video pixels. The pseudorandom noise (MN) pattern i.e. A(y, z) is added to host- image B(y, z) the outcome is watermarked image BA(y, z). Here (y, z) represent position of watermark. $BA(y, z) = B(y, z) + k^* A(y, z)$. k is the gain factor. [6].

3.2 Frequency Domain Method (FDM):

In the frequency domain method, the watermark is embedded into host-data after converting digital information into frequency using transformation tools [4]. This method of watermarking is more robust, efficient and secure as compared to spatial domain [6].

3.2.1 Discrete Fourier Transform (DFT):

In this approach, a watermark is embedded only in the first frame of a group of pictures. The full DFT technique is applied to identify frame to be watermarked and magnitude of the coefficient is calculated [6].

3.3.1 Singular Value Decomposition (SVD):

It is used to get diagonalized matrices. In this technique, singular value of original image is used to embed the watermark. The length and coefficient of watermark effect watermarking technique [6]. SVD is one of the mathematical tools to analyze matrices. A square matrices A of M x N size is decomposed into three matrices X,Y,Z such that A=XYZT. Where, ZT transpose of Z, X, Y are orthogonal matrix and z is square diagonal [12].

3.3.2 Discrete Cosine Transform (DCT):

This works as a tool to convert spatial domain into frequency domain. In DCT, data is represented in terms of frequency [7].
Embedding of watermark is performed in first k highest magnitude of DCT coefficient of image/frame. The result obtained after applying DCT coefficient will be an image of sum of varying magnitude and frequency. Horizontal frequencies vary from left to right and vertical frequencies top to bottom. Watermark in mid band gives better robustness to attacks and imperceptibility [4, 6].

3.3.3 Discrete Wavelet Transform (DWT):

This technique is based on wavelets concept with varying frequency with respect to duration. Multi-resolution decomposition of images and frames is possible in DWT. The wavelet is divided into 4 sub bands LL, LH, HL, and HH. The first letter in sub band refers to frequency applied for rows and second letter refers to filter applied to columns [13].

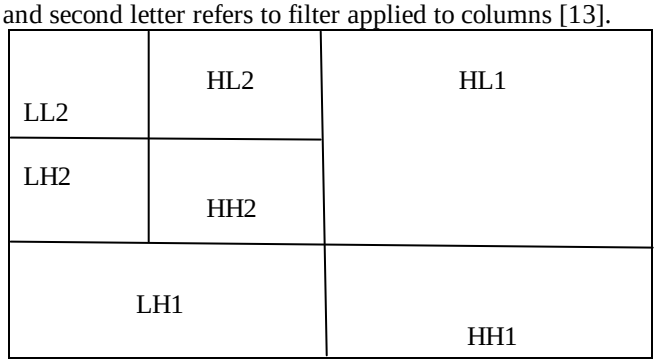

Fig 3: 2-levels DWT Scheme

We present in a tabular form a comparative analysis of different standard watermarking techniques in terms of their features. Following are the expressions used in the table :

RO: Robustness, IM: Imperceptibility

SE: Security

PL: payload , CC: Computational Cost

TC: Time Complexity, RE: Reliability.

Features	LSB	DFT	DCT	DWT	SVD
RO	Less robust against geometric distortion	High robust against geometric distortion	High robust against filter	High robust against geometric distortion	High robust against geometric distortion
IM	Less compared to others.	High	High	Better watermark length and visual quality	Better length of co-efficient effect visual quality
SE	Less secure, usually depends on choice key	Highly secure	Better, semi private watermarking	Better, semi private watermarking	High private watermarking
P	Less, limited data can be added	Average	High	High	High
CC	Less	Reliable cost	Reliable cost	Very high	High
TC	Less	High	High	Very high	high
RE	Better for multiple watermark	High	high	Very high	Very high

4. VIDEO WATERMARKING APPLICATIONS

Following are the some applications of digital video watermarking:

- Source Tracking
- Video Authentication
- Copy-right protection
- Broadcast Monitoring of Video Sequences

5. WATERMARK ATTACKS

The existing class of attacks contains many attacks: e.g. simple attacks, geometric attacks, cryptographic attacks, protocol attacks, etc. Here, we describe some of these attacks types.

5.1 Active attacks:

Attackers can manipulate data and make it undetectable. But in the active attack of digital watermarking, the attacker tries deliberately to eliminate the watermark or simply make it undetectable. This type of attack is grave for many applications where the purpose of the watermark is of no use when it can't be detected.

5.2 Passive attacks:

In passive attacks, attacker does not try to remove the watermark but simply attempts to determine if a given mark is present or not. Protection against these kind of attacks is of the utmost importance in covert communications where the simple knowledge of the presence of watermark is often more than one wants to grant.

5.3 Geometric attacks:

These kinds of attacks just distort the watermark detector synchronization with the embedded data; it means these attacks do not remove the embedded watermark itself. [8, 21, 18].

5.4 Collusion attacks:

In these kinds of attacks, the attacker tries to remove the watermark as for the active attacks but the method is quite different. In order to eliminate the watermark, the attacker uses many copies of the same data, containing each different watermark, each signed with a key to construct a new copy without any watermark. These kinds of attacks are not so easy.

5.5 Forgery attacks:

In these kinds of attacks, the hacker's goal is to embed a new watermark rather than removing one. By doing so, it allows one to modify the protected data and then, re-implants a new

given key to replace the destructed one, thus making the corrupted image seems legit.

5.6 Simple Attacks:

In these kinds of attacks, the attacker attempts to impair the embedded watermark by manipulating the watermark and host data without any attempt to identify and isolate the embedded watermark.

6. RELATED WORK

Sanjai Kumar and Ambar Dutta reviewed in the paper, performance analysis of spatial domain digital watermarking techniques. where they implemented two spatial domain algorithms for digital watermarking and compared them with respect to different performance metrics in the presence and absence of different types of noise. From the experimental results they found that the algorithm using the concept of maximum entropy block in the cover image (Algorithm – 2) performed better as compared to Algorithm – 1. It was also found from the results that Algorithm – 1 is more robust with respect to Gaussian noise compared to Algorithm – 2. Both the algorithms are robust with respect to salt-and-pepper noise [20].

Namita Tiwari and Sharmila reviewed a paper , Digital Watermarking Applications, Parameter Measures and techniques[24]. They found that for security purpose transformation techniques are more suitable and Spatial domain techniques are easy to implement.

Revathi.B, Vijaya Geetha.R, Vengadapathiraj.M, Maheswaran.U and Karunakaran proposed a paper , digital video watermar king algorithm for content validation using singular value decomposition [25]. They found that the contrast in Table 1 method is good when associated to the existing watermarks. As an anticipated work, can go for inlaying diverse watermarks on the different frames of the content.

Naved Alam proposed a scheme in the paper, A Robust Video Watermarking Technique using DWT, DCT, and FFT[26]. It shows from the results that watermarked video sequences are very much susceptible to pirate attacks.

Chitrasen and Tanuja Kashyap proposed a technique in the paper [27], Robust Video Watermarking using Discrete Cosine Transform and Third level Discrete Wavelet Transform. They found that When the embedding strength is stronger, the robustness is greater but visual experience is worse. From the result, it shows that the proposed algorithm has a strong ability to resist different watermark attacks.

M. Sundararajan and G.Yamuna proposed a technique in the paper[28], dwt based scheme for video watermarking, from the results, it shows that the proposed scheme is efficient by means of imperceptibility and robustness.

Paramjit Kaur and Dr. Vijay Laxmi proposed a scheme in the paper[29], An Upgraded Approach for Robust Video Watermarking Technique Using Stephens Algorithm. From the results, it shows that embedded video is excellent with high PSNR, better efficiency and has very low visual artifacts.

Bhargavi Latha S, Venkata Reddy Dasari and Damodaram Avula proposed a scheme in the paper [30], Robust Video Watermarking Using Secret Sharing, SVD, DWT and Chaotic Firefly Algorithm. From the experimental results, it's found that the proposed technique of video watermarking is better in terms of performance when compared with state of art methods.

R.Lancini, F.Mapelli and S.Tubaro proposed a video watermarking technique in the paper [32], a robust video watermarking technique in the spatial domain. From the results, it shows that the proposed technique allows us to hide invisible data in a retrievable way.

Amir Houmansadr and Shahrokh Ghaemmaghami proposed a video watermarking technique in the paper[33], A Novel Video Watermarking Method Using Visual Cryptography. Frpm the reults, it shows that method hasa high resilience against geometric distortions and other non-hostile video processing schemes.

Chien-Chuan Ko and Bo-Zhi Yang proposed a technique of video watermaking in the paper[34],An Integrated Technique for Video Watermarking. From the results, it shows that this method can resist attacks such as JPEG compression, sharpening, median filter, blur, drop noise, brightness adjustment,cropping, Gaussian noise, and MPEG compression etc.

7. ISSUES AND CHALLENGES FOR VIDEO WATERMARKING

From the study of digital watermarking techniques, we have found that when a watermarked video is shared there is always a chance of being attacked. Therefore, during the design of a watermark algorithm, these are following some issues which need to be addressed properly:

- Capacity and Payload
- Robustness
- Transparency
- Security

8. CONCLUSION

This paper is an attempt to review digital video watermarking techniques, their properties, their applications, attacks and classifications. Reviewed literature showed that there are many types of digital video

watermarking techniques that play crucial role in data protection in any form like images, audios, text and/or videos. Researchers used different types of equations in their literature to hide the information in the cover video, which is sequence of still frames. To further improve the video watermarking techniques and make the system more robust and secure from various attacks integration of various video watermarking techniques are required.

References:

[1] Yafeng Zhou and Wing W.Y. Ng Conference paper on influence between digital watermarking and steganography | IEEE, ISSN: 2158-5709, 16 December 2013.
[2] 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.
[3] 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
[4] Prabhishek Singh, R S Chadha "A Survey of Digital Watermarking Techniques, Applications and Attacks" International Journal of Engineering and Innovative Technology (IJEIT), March 2013.
[5] Sourav Bhattacharya, T. Chattopadhyay, Arpan Pal, ―A Survey onDifferent Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC‖, IEEE 2006
[6] 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
[7] Dr.V.Seenivasagam, S. Subbulakshmi, S. Radhamani,―A survey on video watermarking and its applications‖ International journal of advanced research in computer science and software engineering, vol 4,issue 3, march 2014
[8] 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.
[9]Mustafa Osman Ali and Rameshwar Rao, "Digital Image Watermarking Basics, and Hardware Implementation", International Journal of Modeling and Optimization, Vol. 2, No. 1, February 2012.
[10] Gui Feng, Kai Huang "H.264 Video Standard Based Zero Watermarking Technology", project supported by the Natural Science Foundation of Fujian Province of China.
[11] Mrs. Anita Jadhav, Mrs. Megha Kolhekar, "Digital Watermarking in Video for Copy Right Protection",International Conference on Electronic Systems,Signal Processing and Computing Technologies,2014.
[12] Y.J.Song, T.N.Tan "Comparison of Four Different Digital Watermarking Techniques", Proceedings of
ICSP2000.
[13] Hitesh Panchal,Kunal Acharya, Pradip Panchal,Naimish Thakar "Digital Watermarking on Extracted Key Frames from Uncompressed Color Video using 4- Level DWT" , 3rd International Conference on Computer Engineering and Technology,2010.
[14] Swati Patel ,Anilkumar Katharotiya, Mahesh Goyani-A survey on digital video watermarking‖ Int. J.Comp. Tech. Appl., Vol 2 (6), 3015-3018
[15] T. L. Gilbert, Formulation, Foundations and Applications of the PhenomenologicalTheory Ferromagnetism, Ph.D. dissertation, Illinois Inst.Tech., Chicago, IL, 1956, unpublished.
[16] Mahima Jacob, Saurabh Mitra,‖ Video Watermarking Techniques‖, IJRTE, Vol 4, Pp 1- 4,2015
[17] Lalit Kumar Saini, Vishal Shrivastava,‖ A Survey of Digital Watermarking Techniques and itsApplications‖, IJCST, Vol 2, Pp 70-73,2014
[18 Rakesh Ahuja, S. S. Bedi,‖ All Aspects of Digital Video Watermarking Under an Umbrella‖, Ijigsp, Vol 12, Pp 54-73, 2015
[19] Amit Kumar Singh, Nomit Sharma, Mayank Dev and Ananad Mohan| An International Conference Paper, A novel technique for digital image watermarking in spatial domain, IEEE, 2012.
[20] Sanjai Kumar and Ambar Dutta| An International Conference paper, Performance analysis of spatial domain digital watermarking techniques, ISBN: 978-1-5090-2552-7,IEEE, 2016.
[21] Xing Chang, Weilin Wang, Jianyu Zhao, Li Zhang,"A Survey of Digital Video Watermarking",2011 Seventh International Conference on Natural Computation,61-65.
[22] 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.
[23] Dolly Shukhla and Manish Sharma - Robust Scene-Based Digital Video Watermarking Scheme Using Level-3 DWT: Approach, Evaluation, and Experimentation | Spinger , January 2018, Volume 61, Issue 1, pp 1–12.
[24] Namita Tiwari and Sharmila - Digital Watermarking Applications, Parameter Measures and Techniques, IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.3,March 2017.
[25]Revathi.B, Vijaya Geetha.R, Vengadapathiraj.M, Maheswaran.U and Karunakaran- digital video watermar king algorithm for content validation using singular value decomposition, International Journal of Science, Engineering and Technology Research (IJSETR)Volume 5, Issue 4, April 2016.
[26]Naved Alam - A Robust Video Watermarking Technique using DWT, DCT, and FFT, Volume 6, Issue 6,June2016,International Journal of Advanced Research in Computer Science and Software Engineering.
[27] Chitrasen and Tanuja Kashyap - Robust Video Watermarking using Discrete Cosine Transform and Third level Discrete Wavelet Transform, Journal of Engineering Research and Application Vol. 7, Issue 10, (Part -1) October 2017, pp.87-92.
[28] M. Sundararajan and G.Yamuna- dwt based scheme for video watermarking, IEEE, International conference on Communication and Signal Processing, April 3-5, 2013, India.
[29] Paramjit Kaur and Dr. Vijay Laxmi - An Upgraded Approach for Robust Video Watermarking Technique Using Stephens Algorithm, IJCSMC, Vol. 3, Issue. 11, November 2014, pg.612–622
[30] Bhargavi Latha S, Venkata Reddy Dasari and Damodaram Avula - Robust Video Watermarking Using Secret Sharing, SVD, DWT and Chaotic Firefly Algorithm, nternational Journal of Intelligent Engineering and Systems, Vol.11, No.1, 2018
[31] 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
[32] R.Lancini, F.Mapelli and S.Tubaro- A robust video watermarking technique in the spatial domain, IEEE, International Symposium on VIPromCom Video/Image Processing and Multimedia Communications 16-19 June 2002.
[33] Amir Houmansadr and Shahrokh Ghaemmaghami- A Novel Video Watermarking Method Using Visual Cryptography, IEEE, International Conference on Engineering of Intelligent Systems
22-23 April 2006.
[34] Chien-Chuan Ko and Bo-Zhi Yang -An Integrated Technique for Video Watermarking., 6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2007) 11-13 July 2007

Authors

Md. Shahid received his Diploma Engineering in Computer and B.E computer Engineering degree from Jamia Millia Islamia University, New Delhi. He is pursuing M.Tech from Maulana Azad National Urdu University , Gachibowli, Hyderabad, India. His main research area is Digital Image Processing(DIP).

Dr Pradeep Kumar is an Associate Professor in the Department of Computer Science & Information technology at Maulana Azad National Urdu University, Hyderabad (Telangana State). He received his Master's degree in Computer Technology and Applications from Delhi Technological University, formerly Delhi College of Engineering, Delhi University. He completed his Ph.D. from the University School of Information & Communication Technology (USICT), Guru Gobind Singh Indraprastha University (GGSIPU), Delhi. His research interests include software reliability engineering, models for software metrics, machine learning, neural network modeling and soft computing. He has more than 25 publications in journals of international repute including national journals, conferences and proceedings of the international conferences. He is a Member of Association for Computing Machines (ACM) India.