

Systematic comparison of digital video watermarking aspects with techniques and algorithm designing issue

Anuradha Saini *

Department of Computer Applications

RIMT University Mandi Gobindgarh

Punjab

India

and

Department of Computer Applications

CBSA CGC Landran

Punjab

India

Sushil Bhardwaj [†]

Department of Computer Applications

RIMT University Mandi Gobindgarh

Punjab

India

Rachit Garg

School of Computer Science and Engineering

Lovely Professional University

Punjab

India

Tarandeep Kaur

School of Computer Application

Lovely Professional University

Phagwara

Punjab

India

* E-mail: anuradhasaini1984@gmail.com (Corresponding Author)

[†] E-mail: sushilbhardwaj2010@gmail.com

Abstract

With the coming of innovation, verification and security have turned into the principle perspective during communication over the enormous distance. Unlawful dispersal of digital video is the principal peril to the entertainment world. With the advancement of web access, copied duplicates of digitized video might be essentially scattered to globalized watchers. A few applications of video watermarking in copyright insurance, security, fingerprinting, duplicate control, and comment are tremendously expanding. Consequently, a likely technique for confining such sort of digitalized theft is Digital Video Watermarking. At present, watermarking has arisen as a huge strategy to recognize the legitimacy and validation of the proprietor and to ensure the copyrights. The watermarking approach is used by the analysts to hide the secret data that might be apparent or dark according to the client's need. This paper will outfit the disparate tendencies continued in the space of digital watermarking. Also, a point by point outline of digital video watermarking and writing review is talked about in an even arrangement which can give the bearings to forthcoming scientists to seek after their research in this field.

Subject Classification: 68.

Keywords: Digital video watermarking, LSB, DCT, DWT, DFT, SVD, Characteristics of video watermarking.

I. Introduction

The term computer security, data security and data affirmation are as often as possible utilized reciprocally. In any case, there are some inconspicuous contrasts between them. Data security is a bunch of approaches for dealing with the devices, cycles to shield data and related data frameworks from unapproved access, divulgence, use, obliteration and change. There is a worry about the secrecy, accessibility and respectability. Computer security can zero in on guaranteeing the right activity of the computer situation without worry for the data put away or handled by the computer while data affirmation centers around the purposes behind giving security to the data. It persistently connected with the hierarchical capacity to watch the information from obscure just as to manufacture the information as and when needed by an approved person. The fundamental attributes of standard data security are the accessibility, uprightness, credibility and secrecy. As of now, various methods are utilized to get the data like Cryptography [1], Steganography and Digital Watermarking. Every technique is intended for explicit issue.

With the approach of innovation, the security of the general media information turns out to be dynamically more critical. It is because of digital conduct, that mixed media data can be rehashed, changed, changed over,

and diffused without any problem. The quick information circulation over the framework through pictures, sound, and video become the primary source so as to exchange the information to others in a single tick. It is a direct result of the convenient nature that video and guile are expanding today. Indeed, even the genuine maker of the record may not worry about the information accessible on the web shaped by him/her or the maker cannot be able to get to his information. Accordingly, the current digital watermarking has been created to determine this issue. Watermarking is the methodology of concealing data [2] that is known as watermark, and imprint (mark) into genuine information. In this way, video watermarking implants data in the video for documentation, explanation, and copyright [3]. It is a strategy for inserting stowed away information in mixed media conspire information like sound, printed information for personality, copyright, picture and video.

II. Representation of Digital Video Watermarking

This is a method of embedding data in digital video data or retrieving data from digital video data. Figure 1 shows the digital video watermarking model. This approach is a solution to the property rights problem. However, the growing popularity of video-based applications such as home video recorders and Internet media has increased the need for secure video communications. Image and video watermarking methods are different, and implementing video watermarking causes more problems. For example, video objects are very likely to have similar frames, making the signal extremely vulnerable to video-specific attacks, including all frame-related operations.

Some features of the Digital Video Watermark are described below in Figure 1:

- Copyright protection and broadcast monitoring require real-time operation and minimal complexity.

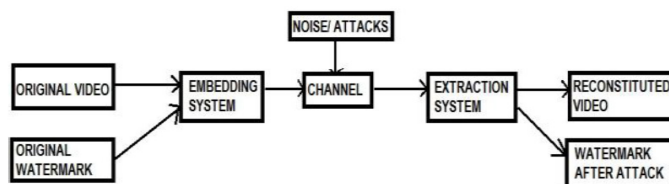


Figure 1
Digital Video Watermarking Model

- High correlation between successive video frames. With an autonomous watermark embedded in each frame, Risk can perform video frame averaging to eliminate important parts of the embedded watermark.
- Video threats such as image averaging, image sharing, statistical research, digital-to-analog conversion, and loss compression, Watermarked video sequences are vulnerable to it [4].

According to different watermark insertion methods, the algorithms for implementing the technique can be divided into three different types i.e. (a) Non-compressed domain video watermarking: These algorithms insert binary text / images into the actual video object;(b)Video Watermarking during compression: In this phase, the watermark is embedded in the object and after implementation both components get the same property [5]. Commonly used standards are MPEG2, MPEG4, and H.26 [6]; (c) Compressed domain video watermarking: This is a special area where you need to embed the content (binary text / image) [7]directly into the data.

Therefore, in relevant and realistic areas, one of the above scheme is used, depending on the requirements and types of watermarks you insert into the host object. Most digital image watermark algorithms have been extended to include video watermarks. Some of the most important points to keep in mind when using such an algorithm are:

- Internally, there is a lot of duplicate data or patterns between the multiple frames of video.
- There is a strong balance between motion and rest areas in the frames of the video objects.
- Strong concerns should be there about real-time and streaming video applications.

III. Domain based Techniques

These watermark schemes are categorized based on various parameters such as domain and document, and can be grouped into a wide range of categories given according to the area of interest i.e. Spatial domain watermarking technology and transform domain watermarking technology which is shown in the Figure 2.

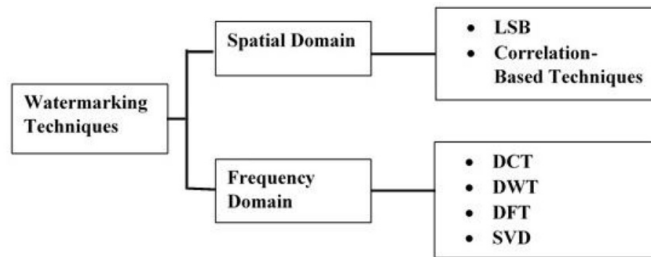


Figure 2
Watermarking Techniques

a) Spatial-domain Watermarks

Spatial domain technology inserts text / images into specific frames of a video object by updating the pixels. They are very simple, convenient to run, and require less computational effort. However, it has not been proven to be reliable or robust and can withstand multiple video-specific attacks.

i. Least significant bit change (LSB)

A direct way to insert a watermark that is inserted in the least significant bit (LSB) of the actual video content. Replacing the LSB is very easy to implement, but at the same time has some limitations. In addition, if an operation is detected, an attacker can easily modify the inserted object.

ii. Correlation method

This method involves the use of the correlation characteristics of noise patterns within the frame of a video object. For example if some noise W is inserted in the image component I as per the equivalence 1 shown here:

$$I_w(a, b) = I(a, b) + k W(a, b)$$

where 'k' is used to represent the constant value which shows the gain, and I_w is the resultant image.

b) Transform Domain Watermarks

Frequency domain technology (domain conversion) changes the coefficients of the modified part of the video according to the insertion scheme, making it difficult to restore the inserted watermark.

i. Discrete Cosine Transform (DCT)

DCT is a method of representing data by summing cosine functions that move at different frequencies [8]. Converts an object from its spatial domain to a translation domain. This technique divides the object into spectral sub-bands. Here, the DCT coefficient is used to calculate the result [9].

ii. Discrete Wavelet Transform (DWT)

In this technique, the video (image) frame is divided into multiple resolution levels. At the first level, it is divided into low to high frequencies [10] consisting of row and column frequencies[13]. This technology is believed to give better and more authentic results when compared to other technologies available. DWT's multi-band decomposition feature makes it possible to produce highly acceptable robustness results for watermarks with excellent visual quality of objects[14].

iii. Discrete Fourier Transform (DFT)

The DFT first checks the brightness of the target frame and then determines the size of the coefficients. The DFT factor is changed and the inverse DFT is applied. This method provides greater robustness when applying basic filtering, sharpening, geometry, and compression attacks compared to other techniques, but it allows you to add an average amount of data to your video content.

iv. Singular Value Decomposition (SVD)

This is a method in which the frequency range is optimally constructed[15][16]. This scheme extracts the frame from the original video and then processes the image in the form of a matrix. This technique is divided into three specific components U, S, and VT. The SVD operation for matrix A (N xN) is defined and shown in following equation.

$$A = USVT$$

where the U and V matrices are singular vectors of diagonally arranged A and S matrix values. It is called the singular value of A.

IV. Critical Aspects

There are various aspects which effects the efficiency of the designed technology but some of the critical aspects are: (a) *Robustness*: which refers

Table 1
Comparison of characteristics on the basis of different techniques

Techniques		Characteristics						
		Robustness	Imperceptibility	Security	Data Payload	Cost	Time	Reliability
	LSB	Less strong in case of geometric attacks	Low	Security depends on key	Very less	Nominal cost	Less time	Reliable (only if more than 1 watermark is embedded)
	Correl. Based	Fragile technique	Low	Less secure method	Less	Nominal cost	Less time	Less reliable
	DFT	Sturdy in case of geometric attacks	High	Highly secure method	Average	Economical cost	High time	Moderate reliable
	DCT	Sturdy against filtering	High	Convenient in case of private watermarking	High	Economical cost	High time	Highly reliable technique
	DWT	Extremely Robust	Very high	Highly secure for private watermarking	High	Highly Expensive	Very high time	Very highly reliable
	SVD	Extremely Robust	Very high	Highly secure method	High	Expensive	High time	Very highly reliable

to the resistance of the watermark to designated class of transformations or modifications or common media operations; (b) *Imperceptibility*: means the invisibility of the embedded watermark in the host signal or final output data. A watermark embedding algorithm is called imperceptible only if the human eye is not able to recognize the difference between the original video or host signal and the watermarked video[7] or watermarked signal; (c) *Security*: It is considered as the difficulty to remove or alter the watermark without damaging the cover image or video or host[17]. The watermarked image or video needs to be completely secure against the attacks or tampering; (d) *Data Payload*: It is the total number of embedded bits (bits of watermark) in the host image or video; (e) *Cost and Time*: It is the monetary amount and time involved in the implementation and in getting efficient system; (f) *Reliability*: It is directly related to the authenticity; In addition, the relationships[18] between the basic characteristics and their comparison by the various watermarking techniques are shown in Table 1.

V. Challenges in designing an algorithm for Video Watermarking

The quick advancement of digital data innovation radically changed the overall population. As of now media items can undoubtedly be made, controlled and put away by digital information proprietor worldwide because of the accessibility of wide range of multimedia instruments. Likewise, blast in the improvement of high web data transmission because of the availability of high speed and bandwidth. Nonetheless, these advantages have brought a significant disturbing issues and number of difficulties that still up in the air recorded beneath.

Video media substance can undoubtedly be modified because of the accessibility of number of video altering instruments like transforming, Photoshop, CorelDraw for adjusting the video information without pointing any apparent clue. In this manner, vulnerability remains present about the respectability and validness of the video. This raises the video verification and respectability insurance issue.

As there is no suitable distinction between the first and copy digital interactive media video object dissimilar to simple information, various amazing protected duplicates can be made by an unapproved client to unlawfully convey or trade through web. Because of this the finance manager from businesses may experiences an enormous efficient loses. This raises the issue of fostering a component for getting and to ensure the copyright of the worry video object.

Video media substance can undoubtedly be modified because of the accessibility of number of video altering instruments like transforming, Photoshop, CorelDraw for adjusting the video information without pointing any apparent clue. In this manner, vulnerability remains to exist about the respectability and validness of the video. This raises the video verification and respectability insurance issue.

The use of fingerprinting is intended to follow the approved customer liable for misguidedly giving the video content to the clients/watchers. Because of a similar issue, a colossal measure of monetary misfortune is looked by the video maker.

Many valuable digital items are dispersed over the TV station. Proprietors of protected recordings need to get their sovereignties each time their property is communicated. A component should be worked to recognize the video thing being communicated.

As earlier examined, digital watermarking is the plausible answer to resolve these issues. Digital video watermarking is as yet a relatively less researched region then, at that point picture watermarking. One of the principle reasons is video having extra high intricacy and separates includes then picture for which amazing, powerful watermarking methods and different arrangements are accessible. Rather than picture watermarking, video watermarking research actually comprise numerous extra issues like changing edge rate, expansion in bit-rate, transient synchronization and edge based assault. The inspiration towards this research is to acquire the inventive answer for securing the copyright issue for video groupings in a vigorous and intangible way. The significant consideration is to have an extraordinary picture addressing copyright data installing in a video material that can later be effectively extricated the valuable data use to guarantee for the copyright of the worry video. Since the video comprising voluminous information therefore the video data should need to compress before storing or move through web to limit the capacity necessities and to help the continuous real time requirements.

Considering this, the outline on video watermarking zeroed in on non-compacted domain as well as executed the video watermarking plans dependent on compressed domain. At last, the significant center is to get the video media material through digital watermarking innovation by examining their applications and necessities as certain difficulties actually required being addressed. The goal is to plan an inventive plan in video watermarking innovation with a subjective investigation of watermarking in uncompressed and compressed domain both.

This paper has begun from the scratch of data security issue and strategies for interactive media objects. Digital watermarking strategy is distinguished as one of the potential answers for getting such items. In continuation with it, the profound investigation of condition of workmanship under uncompressed and compressed domain based digital video watermarking is evaluated and inferred that movement outline based and MPEG-2 based techniques maybe more reasonable for a given application and necessity. By and large, information is created, put away, and scattered carefully. At present, media and magazines have gone through online for furnishing ongoing inclusion of stories with greatest quality sound, fixed pictures, and video series. The advancement in the utilization of publically accessible organizations like; the web has thought about the online accessibility of distributors by giving a quick, and modest approach to communicate its work. The quick development of digital media is limited to news organizations. Henceforth, music can be downloaded and bought through the web, standard photography merchants digitalize and the photos in electric and digital adaptable plans give films dynamic pictures. For the most part, papers and broad communications carefully put away the information and helpless through different modes. First and foremost, digital broad communications might be copied legitimately or illicitly at less expense without information misfortune. In addition, processors license broad communications to be adjusted so it is likely to coordinate pieces of digital signs into their proprietor's work without copyright requirements. The water stamping approach depends on tracking down the ideal bit-example to ensure the implanting system will give superior grade, less information misfortune, secure confirmation, and so forth on the advancement cycle which tracks down the right pieces in the interest of bit limits and wellness, and afterward produce the ideal inserting succession for result.

VI. Conclusion

The general result of this paper will give an enormous understanding and more extensive scope of the area to the scientists seeking after their research work in the said field. The most important challenge of digital video watermarking is to keep up with the quality at the time of recovery of the watermark which should be possible by dealing with different attributes of the watermarked object. The methodologies talked about above will accomplish a high-effectiveness rate and less frame-dropping ratio. The bit choice module of the strategies will give a superior choice of

the pieces to install and make the video watermarking measure safer. It will likewise work for color based watermarking and proposition security and imperceptibility. For the future scientists, the watermarking system would likewise be carried out to test the assorted security assaults like composite attacks, collusion attacks and ambiguity attacks. In addition, there would consistently be some degree to keep up with the balance between the three significant trade-offs i.e., Robustness, Imperceptibility and Capacity.

References

- [1] M. K. Rasheed, A. J. Dawood, "A New Card Authentication Schema Based on Embed Fingerprint in Image Watermarking and Encryption", *Journal of Theoretical and Applied Information Technology*, 97(3), 1018-1029 (15th February, 2019).
- [2] C. S. Hsu, S. F. Tu, "Digital Watermarking Scheme For Copyright Protection And Tampering Detection", *International Journal on Information Technologies & Security*, 11(1), 107-119 (2019).
- [3] G. Döerr and J. L. Dugelay, "A guide tour of video watermarking," *Signal Processing Image Communication*, Vol. 18, No. 4, pp. 263–282 (Apr. 2003).
- [4] Md. Asikuzzaman and Mark R. Pickering, "An Overview of Digital Video Watermarking," *IEEE Transactions On Circuits and Systems For Video Technology*, Volume 28, Issue 9, pp. 2131-2153 (2018).
- [5] Madhuri Rajawat and D. S. Tomar, "A Secure Watermarking and Tampering detection technique on RGB Image using 2 Level DWT," *IEEE Fifth International Conference on Communication Systems and Network Technologies*, pp.638-642 (2015).
- [6] R. Gayathri and Dr. V. Nagarajan, "Secure data hiding using Steganographic technique with Visual Cryptography and Watermarking Scheme," *IEEE ICCSP conference*, pp. 0118-0123 (2015).
- [7] Xiaoyan Yu, Chengyou Wang * and Xiao Zhou, "A Survey on Robust Video Watermarking Algorithms for Copyright Protection", *Appl. Sci.* 2018, 8, 1891; doi:10.3390/app810189, 2018.
- [8] 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).

- [9] Prabhishek Singh, R. S. Chadha "A Survey of Digital Watermarking Techniques, Applications and Attacks" *International Journal of Engineering and Innovative Technology (IJEIT)* (March 2013).
- [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] C. Singh et al., "Performance comparison of Putnam model using new technology trends for software maintenance cost estimation", *JDMSC*, DOI: 10.1080/09720529.2021.2016220
- [12] I Kaur et al., "Artificial Intelligence Techniques for predictive modeling of Vector-Born diseases and its Pathogens", *Archives of Computational Methods in Engineering*, <https://doi.org/10.1007/s11831-022-09724-9>
- [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] Md Shahid and Pradeep Kumar, Digital Video Watermarking: Issues and Challenges, *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* Volume 7, Issue 4, ISSN: 2278 – 1323 (April 2018).
- [15] A. Fita and B. Endebu, "Watermarking Colored Digital Image Using Singular Value Decomposition for Data Protection", *Journal of Mathematical and Statistical Analysis*, 1(2), Researchgate (January 2019).
- [16] Sunesh, Harish Kumar, Watermark Attacks and Applications in Watermarking, National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing (RTMC), Proceedings published in *International Journal of Computer Applications® (IJCA)* (2011).
- [17] Singh AK, Dave M, Mohan A, "Wavelet based Image Watermarking: Futuristic Concepts in Information Security" *ProcNatlAcadSci, India, Sect A* 84(3), pp.345–359 (2014).
- [18] MdShahid and Pradeep Kumar, Digital Video Watermarking: Issues and Challenges, *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* Volume 7, Issue 4, ISSN: 2278 – 1323 (April 2018).