



Copyright Protection and Content Integrity for Digital Video Based on The Watermarking Techniques

Alaa Maher Mahmood *, Majid Jabbar Jawad and Mohammed Abdullah Naser

Department of Computer Science, College of Science for Women, University of Babylon,
Babylon, Iraq

alaam147@gmail.com, wsci.majid.jabbar@uobabylon.edu.iq, and
wsci.mohammed.abud@uobabylon.edu.iq

ABSTRACT: Nowadays the digital video is doing important duties in our life. The digital video can be used in several applications, such as in the civil and military application. In addition, digital video can be sent and received by using the modern communication (especially the Internet). Due to availability of the digital video through the unsecure communication channel (Internet) and availability of the modern applications, anyone can exploit this situation by editing or observation the digital video easily. Therefore, the owners of the digital videos don't trust the communication channel later. This case will affect the applications that depend on the digital video. The digital watermarking technique is one of several techniques by which we can overcome the above challenges. This study proposed a survey on video authentication and copyright protection based on the digital watermarking technique. Some information is presented, such as the requirements of digital video watermarking technique, some video authentication and copyright watermarking technique, possible attacks on video

watermarking. In addition, future, challenges in field of video authentication copyright protection based on the watermarking technique.

Keywords: Watermarking, Video Copyright Protection, Video Integrity, Video Authentication.

1. Introduction

Digital Video is a series of digital photos that are quickly viewed with a digital audio, it is a representation of the motion of visual images in a way that the digital data are encoded [12]. Transmitting the video through the internet might be unsecure, so that anyone can deal with the video (watch or manipulate it by some video editing tools). The video can be tampered by any person who is professionally done video editing. Video tampering where an attacker can intentionally (or un-intentionally) modify the original video to create tampered video, this would restrict the applications that depend on the video. There is a need for a reliable or true video in the court which means law enforcement, defense planning, defamation, politics etc., the video is checked by experts using tools to detect tampering to decide whether the video is tampered or not, but the attacker is cleverly tampering the video so that this attack is not discovered by tamper detection tools, Because of the few ways in which video or video integrity is examined, video-based applications will face many challenges in the security field. There is a way to protect the video from tamper and fraud using digital watermarking. Digital watermarking is a way through which to hide a watermark (text, image, audio, video) in a message (text, image, audio, video) in order to maintain the integrity of the message and its continuation [15].

The rest of the paper is organized as follows. In section 2, the benefits of digital video are presented. The reason of applying watermarking on digital video is presented in section 3. Requirements of digital watermarking techniques is listed in

the section 4. Applications of digital watermarking is listed in section 5. The possible attacks on the digital video watermarking is illustrated in the section 6. Types of Digital Video Watermarking Techniques is illustrated in section 7. Literature survey on schemes that proposed for digital video watermarking in section 8. In addition, conclusions and suggested for future works is listed in the section 9.

2. Benefits of Digital Video:

There are several benefits of digital video. The important benefits can be listed as follows [12]:

1. Digital video is useful in many areas such as the in the educational and medical fields.
2. At the present time the increased development in the technologies of the video (transmitting the video, video conferencing, video compression) have helped in many situations.
3. Digital video has become shared on the social media (Facebook, YouTube, WhatsApp etc.), it facilitates the communication, now people can call each other by video calls.
4. There are additional uses of the video in, video tutorial, advertisement, legal evidence etc.

3. Why Digital Video Watermarking?

The authenticity of video data is the essential importance in some applications, such as video surveillance, criminal investigation, content ownership, and law enforcement, for example, if the video is used as evidence in the court of justice it must be checked for accuracy, means whether it is reliable or not. another example, suppose a fixed video recorder for surveillance purposes is placed on the rail platform pole to scan each activity on this platform along the side. The attacker can be easily manipulating the video using some video editing tools. he can delete an

important people, events, scenes, or a set of frames. he can also insert in the video objects, events or people that are not related to the video in any way for criminal issues. such as [14]:

1. A video clip can be manipulated in an intelligent way to destroy the reputation of an individual.
2. Some crimes could not be definitively proven in court. Because of that malefactors get free from their penalty.
3. sometimes it is not easy to verify that the video which is used as evidence in the court is the same as the original that is filmed from the camera in the case of surveillance systems.
4. Another case we cannot assure that the video being played in TV is from a dependable news channel.

In such cases, forgery is not permitted. Therefore, there is a need for video authentication and copyright protection techniques. So, video authentication Is a process used to check the reliability of digital video. In other words, the video authentication system maintains the integrity of the digital video and confirm that the video used is not tampering [13]. While copyright protection is a method used to include a watermark in the video to maintain its ownership [16].

4. Requirements of Perfect Digital Video Watermarking Schemes

There are several requirements for a perfect watermarking technique. Depends on the application that it is used for. But there should be a balance between these requirements because there is a relation between them whereby increasing in one might leads to decreasing of the other. In copyright protection application it concerns on robustness among the requirements, while in authentication application it focus on the location of the tampered area and if the tamper is intentional or unintentional [6].

These requirements are:

1. **Robustness:** is the degree of resistance of the watermark for any attack. The degree of robustness depends on the application used. For copyright protection application, it requires high robustness against any kind of attacks. While for authentication application, it does not need a high level of robustness [18].
2. **Statistically undetectable:** For applications that require a watermark to be hidden, this process must be completed accurately so that the watermark cannot be perceived visually or in statistical methods. The watermark should not affect the visual appearance of the video in order to not reduce the commercial importance of the video [19].
3. **Fidelity:** One of the main requirements of watermarking is the Fidelity. A perfect watermarking technique should have a high fidelity. Disturbance done by embedding the watermark must not overtake a certain level that the viewer can make sense of [19].
4. **Speed:** Is less concerned of the watermarking requirements because of the evolution in the physical components and computational techniques [19].
5. **Capacity:** is the number of bits of the watermark allowed to be included in the video. And Because of the large size of the video, the capacity is also not the main concerns. The size of watermark depends on the application that specifies the watermark data type and embedding strategy [19].
6. **Use of the Key:** Improving security by using a secret key involves encryption techniques that promote the robustness of the watermark algorithm [19].
7. **Low Error Probability:** this condition is required in the detection step. A perfect watermark system should accurately detect the watermark with the least probability of detection failure [19].
8. **Security:** only the authorized user can access to the watermark.

9. Unambiguity: for copyright application the watermark should carry clear information about the possessor of the video.
10. Real-time Detector Complexity: there are applications that requires a real time execution for example, on demand video. So that the algorithm of the detection and extraction should have low complexity so it can demand in an appropriate time [19].

5. Applications of Digital Watermarking

There are many interesting applications that use the watermark for many purposes [20]:

1. Owner Identification: the watermark displays the content ownership.
2. Copy Protection: The watermark is used to avoid some people that are creating unlawful copies of the multimedia.
3. Content Authentication: Here the watermark is used to verify whether the content is integrated or not. In other words, whether the content was attacked or not, and determine the location of the attack.
4. Fingerprinting: The watermark is used here to trace the authorized users who infringe the privacy of the license and distribute illegally the copyrighted content. There for, the information about the customer should be contained in the content, such as the customer ID number.
5. Broadcast Monitoring: the watermark is used for advertising and entertainment industries to control content.
6. Medical Applications :Here the watermark is used to authenticate the medical contents in order not to mix the data of two patients because this may lead to a disaster.
7. Data Hiding (Covert Communications): Hidden data transfer is one of the oldest applications of a watermark. It hides the secret message into a cover message to prevent unauthorized person of manipulating it.

8. Forensic Tracking: It determines the origin of the content, especially the illegal content.
9. Remote Triggering: Identifies content and then the action is automatically done while distribution.

5. Possible Attacks on Digital Video Watermarking

In general, attacks are classified into two categories:

1. Active Attacks: In this type of attack the attacker discovers the watermark and manipulates it so that it will not be recognized afterwards. This is a major concern in the protection of copyright, copy control, fingerprints and others [20]. There are many examples of this type, including those who try to delete the watermark or replace it with another or manipulation so that it is difficult to distinguish, some of the active attacks are listed below:
 - a. Removal attack: In this type of attacks the attacker tries to delete the watermark from the watermarked media. Such attacks avail from the fact that the watermark is usually an added noise signal exist in the host signal [16].
 - b. Collusion attack: In collusive attacks, the goal of the attacker is to remove the watermark. The attacker tries to reach several copies of the same data and attack them, compare the watermarks of each one, and then create a new copy does not contain a watermark. This type of attack is a problem in the applications of fingerprinting. But this attack is not widely deployed because the attacker may not be able to access many versions of the same data [20].
 - c. Interference attack: There are some optimization operations on the digital media may cause a noise. For example, filters, Lossy compression, and enhancement processes [16].

d. Geometric attack: An example of this type of attack is all the modifications that occur on the geometry of a digital medium such as flipping, rotation, cropping, etc. [16].

e. Security Attack: here the attacker tries to know the watermarking algorithm in order to modify the watermark and make it invalid. The algorithm of the watermark is considered secure if the embedded watermark cannot be found, manipulated, or falsified [16].

f. Forgery attacks: In this type of attack the attacker tries to embed a new watermark instead of removing the original one in order to manipulate the message as he desired, this is the main problem in data authentication [20].

2. Passive attacks: the attacker is not intended to remove or manipulate the watermark but he is trying to determine if a watermark is existing or not. This is one of the covert communications considerations [20].

6. Types of Digital Video Watermarking Techniques.

Digital Watermarking techniques are classified based on several perspectives [15]:

1. Based on Human Perception [15]:

There are two types of watermark from the human point of view:

a. Visible watermarking: the information of the watermark is visible. this information is mostly a logo or text, that defines the owner of the media.

b. Invisible watermarking. The watermark is hidden in the media to make it invisible for the attacker in order to protect the content. It is used in authentication and copyright processes.

2. Based on the domain of embedding:

All watermarking techniques are working within two domains [21]:

a. Spatial Domain:

These techniques embed the watermark directly on the data without converting it into another domain. It is easy to apply, and faster than the transfer domain techniques. Some of the spatial domain techniques are:

1. Least significant bit modification (LSB): It is the simplest technique to insert a watermark in the least significant bits of some randomly selected pixels of the cover frame of the video. The main advantage of this method is its ease of implementation on images. This method does not affect the quality of the image when we include the watermark into the image the quality will not be decomposed. It provides high cognitive transparency. The main disadvantage of LSB is that the watermark is fragile against any signal processing attacks.
2. Additive Watermarking: In this technique a watermark is included in a spatial domain by adding a pattern of random noise to the intensity of the frame pixels. The noise signal is integers such as (-1, 0, 1) but sometimes it is a floating number. To make sure that the watermark can be found, the noise is generated by a key, so that the correlation between different numbers of different keys will be very low.
3. Spread-spectrum Modulation (SSM) Based Technique: This technique hides the watermark by combining (in a linear way) the cover frame with a small random noise signal that is modulated by the hidden watermark.

b. Transformed domain

These techniques are used more widely compared to the spatial domain techniques. Here the watermark is not hidden directly in the cover, but it is initially converted into coefficients and concealed in it. Some of these techniques are listed below:

1. Discrete Cosine Transform (DCT): It represents data in the frequency domain instead of the color domain. The advantage of this method is that the watermark has more transparency compared to spatial domain techniques. DCT

technique is more robust compared to spatial domain techniques. It is robust against image processing operations like enhancement filters, quantization, brightness and contrast adjustment, etc. but, it is not easy to execute and it takes a lot of computational operations. And it is fragile against geometrical attacks like rotation, scaling, etc. DCT watermarking technique can be classified into Global DCT watermarking and Block based DCT watermarking.

2. Discrete Wavelet Transform (DWT): This technique is built on the basis of small wavelets with a short period and uneven frequency. It Splits the image into four transactions (LL, LH, HL, HH). where the highest frequency is in the section LL and lowest frequency is HH. This technique is modern and it is used in many applications including compression, watermarking and digital image processing.

3. Discrete Fourier transform (DFT): This technique has a function that convert the values of the data from the continuous domain into frequency components. It has durability against geometric attacks such as rotation, resizing, cropping, translation etc.

3. Based on the level of information required to detect the embedded data:

This category is classified into three types [21]:

a. Blind Watermarks: These methods do not need the original cover to detect the hidden watermark.

b. Semi-Blind Watermarks: These methods need special information from the original cover to discover the hidden watermark contained in the watermarked signal.

Non-Blind Watermarks: These methods need the original cover to detect the hidden watermark in the watermarked signal. They are more robust to any attack on the signal compared to blind methods.

4. Based on application:

This classification related to the types of the robustness, which can be classified as follows [11]:

- a. Fragile Watermarks: here the watermark is weak for any attack (intentional or unintentional) and it can be easily destroyed.
- b. Semi-Fragile Watermarks: These watermarks are fragile against intentional attacks and robust against unintentional attacks. It is used to verify the integrity of the content.
- c. Robust Watermarks:

These watermarks cannot be easily broken. The watermark must remain permanently intact so that removing or destroying the strong watermark will result in destroying the quality of the content. This method can be used to for copyright protection of the content.

7. Literature Survey

There are many proposals on several watermark technologies that are used for copyright protection and content authentication.

1. Shih- Wei Sun and Pao-Chi Chang [1] have presented a temporal synchronization scheme for watermarking the video by Comparing the profile statistics. The profile statistics, contain several parameters represented by several characteristics such as position mean and variance in x- and y- directions, of a frame in a video sequence. The sender can easily calculate it and send it to the receiver as a side information. The receiver can detect the temporal attacks such as dropping, transposition, and insertion by doing a comparison between the received side information and the characteristic parameters that are calculated from the received video. The experimental results have displayed that the accuracy of re-synchronizing the attacked video back to

the original one is from 72.41 % to 98.15 % for various video sequences based on single frame matching.

2. Gwenaëlle Doërr and Jean-Luc Dugelay [2] have proposed a blind frame-by-frame embedding scheme. They used two very common video watermarking systems. both watermark modulation and embedding strength modulation will be used to design alternative embedding schemes which showed an excellent action against intra-video collusion attacks. This type of attack aims to remove the implicit watermark. And because the used method is frame-by-frame, the attacker can access to each frame and modify it.
3. Aldrina Christian and Ravi Sheth [3] proposed a method that use encryption, decoding, and DCT watermarking technique. At first, they converted video into frames. Encrypted the watermark and embedding it into the video. At the embedding step there were a frame extraction, encrypt the watermark, and apply DCT technique.
4. Jing Zhang, etl. In [4] have proposed a robust video watermarking method of the video coding principle H.264/AVC. They used 2-D 8-bit watermarks like those used as Brands or logos can be used as non-changeable watermarks to protect the copyright. A gray scale watermark style is changed at first to be suitable for the computational constraints of H.264 / AVC, Then, included in the compressed range of the video data. Using the suggested method, it can obtain a high robustness and good quality for the visual look without increasing total bit-rate. Experimental results showed that the algorithm is robust against transcoding process and the Signal processing attacks that are common such as bit-rate reduction, Gaussian Filtration and enhancement of the brightness.
5. Young-Yoon Lee, etl. [5] have proposed two algorithms. In the first one the feature of a frame is its presence, we propose two temporal feature modulation algorithms that extract a feature from each video frame and modulate the

features for a series of frames to embed a watermark codeword. In the first algorithm, the existence of a frame is used as the frame feature, and a watermark codeword is embedded into the original video by skipping selected frames. In the second algorithm, the centers of gravity of blocks in a frame are used as the frame feature. By modifying the centers of gravity, we embed 1-bit information into the frame. Simulation results demonstrate that the proposed algorithms are robust against compression and temporal attacks.

6. Siyue Chen and Henry Leung [6] have proposed a chaotic semi-fragile method for content authentication. The Information about the time for video frames is modified to chaotic system parameters. The output of the system (a noise-like signal) is considered the watermark and embedded in the discrete cosine transform domain using block-based DCT technique. The Included information is reformulated by the maximum likelihood estimator. Transitory tampering can be found by the difference between extracted information and noticed time information. The variation of the extracted watermark from the original one allows us to determine the place of spatial manipulation. It appears that the proposed scheme could meet the requirements for authenticating the digital video of surveillance system.
7. Chen Ling and Wenjun Zhang in [7] have presented a semi-fragile watermarking technique for video authentication process. It is established by a hybrid feature. This feature consisted of a threshold of gray level and relative total variation edge feature. From the sender end the watermark is encoded and included in the main diameter of the 8×8 DCT coefficients. At the receiver end, if the arrived video was tampered in a particular part this method could locate the tampering area. The experimental results showed that this proposed technique could recognize the intentional attacks from the unintentional attacks and it was robust against H.264 compression and could detect malicious attacks.

The results also showed that this method has a higher retrieval and accuracy than current methods.

8. T.Srinivasa Rao, Dr.Rajasekhar R Kurra [9] have presented In this proposed work, a developed SVD conversion algorithm is used for including and extracting the watermark. The experimental results showed that the proposed watermark process is safer than the current SVD method.

9. Chhaya S. Gosavi and Suresh N. Mali [10] have proposed a secure and reliable video watermarking method to detect Hacking in camcorder using the Discrete Cosine Transform (DCT) technique and Schur Decomposition. The watermark is secured by scrambling. The scrambling is done by using Arnold transformation and then splitting it into subparts. the scrambled watermark parts are included into audio sequence and frames of the video by applying a robust DCT technique and Schur decomposition. The selection of the frames is random there for the security here was improved. Experimental results showed that the method is robust to various attacks and had a high secure. Table 1 illustrates more details on all the works being reviewed.

Table (1), The related works with some details

No.	Authors	Application	Attacks performed	Video Watermarkig Domain
1	Shih- Wei Sun and Pao-Chi Chang	Security of video	transposition, dropping, and insertion.	Spatial Domain
2	Gwena`el Do`err and Jean-Luc Dugelay Senior	Security of video	collusion attacks	Spatial Domain
3	Aldrina Christian and Ravi Sheth	Authentication	adding frame, dropping frame, replacing frame	Frequency domain: DCT

4	Jing Zhang, etl.	Copyright protection	bit-rate reduction, Gaussian filtering and contrast enhancement	Frequency domain: DCT
5	Young-Yoon Lee, etl.	Fingerprinting	compression and temporal attacks.	Spatial Domain
6	Siyue Chen and Henry Leung	Authentication	JPEG compression, median filtering and contrast enhancement	Frequency domain: DCT
7	Chen Ling and Wenjun Zhang	Authentication	H.264 lossy compression, noise and Gaussian filtering	Frequency domain: DCT
8	Srinivasa Rao, Dr.Rajasekhar R Kurra	Authentication	frame dropping, averaging and lossy compression.	Frequency domain
9	Chhaya S. Gosavi and Suresh N. Mali	Copyright protection	signal processing, video processing attacks and camcorder attack	Frequency domain: DCT

8. Conclusions and Suggestions for Future Works

This study proposed a survey on video authentication and copyright protection based on the digital watermarking technique. After surveying the proposed schemes related to the above studying some recommendations can be listed as follows:

- a) It is good idea to apply the suggested schemes (previously) related to applying digital watermarking technique for copyright protection of digital image or image authentication on video copyright or video authentication.
- b) Approximately, the number of suggested schemes that related to applying watermarking techniques for video authentication application is less than other applications. So, in future, it is good idea to focus on the video authentication.

REFERENCES

1. Sun, Shih-Wei, and Pao-Chi Chang. "Video watermarking synchronization based on profile statistics." *Security Technology*, 2003. Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on. IEEE, 2003.
2. Doërr, Gwenaëll, and J-L. Dugelay. "Security pitfalls of frame-by- frame approaches to video watermarking." *IEEE Transactions on Signal Processing* 52.10 (2004): 2955-2964.
3. Christian, Aldrina, and Ravi Sheth. "Secured Digital Video Authentication System." (2017).
4. Zhang, Jing, et al. "Robust video watermarking of H. 264/AVC." *IEEE Transactions on Circuits and Systems II: Express Briefs* 54.2 (2007): 205-209.
5. Lee, Young-Yoon, et al. "Temporal feature modulation for video watermarking." *IEEE Transactions on Circuits and Systems for Video Technology* 19.4 (2009): 603-608.
6. Lee, Young-Yoon, et al. "Temporal feature modulation for video watermarking." *IEEE Transactions on Circuits and Systems for Video Technology* 19.4 (2009): 603-608.
7. Ling, Chen, and Wenjun Zhang. "Semi-fragile Watermarking for Video Content Authentication Based on Hybrid Feature." *電腦學刊* 25.2 (2014): 48-57.
8. L.Shafnam, Selvi, L.Shammi, "Privacy-Preserving Confidential Auditing For Data Storage Security Using Cloud Computing", *International Journal Of Innovations In Scientific And Engineering Research (Ijiser)*, Vol 1 Issue 3 Mar 2014, Pp.202-207.
9. Rao, T. Srinivasa, and Rajasekhar R. Kurra. "A Smart Intelligent Way of Video Authentication Using Classification and Decomposition of Watermarking Methods." *arXiv preprint arXiv:1404.7237* (2014).
10. Gosavi, Chhaya S., and Suresh N. Mali. "Secure, Robust Video Watermarking to Prevent Camcorder Piracy." *Indian Journal of Science and Technology* 10.18 (2017).
11. Papinwar, Sonal R. "Forgery Detection in Video Using Watermarking: A Review."
12. Christian, Aldrina, and Ravi Sheth. "Digital Video Forgery Detection and Authentication Technique-A Review." *International Journal of Scientific Research in Science and Technology (IJSRST)* 2.6 (2016): 138-143.
13. Parmar, Zarna, and Saurabh Upadhyay. "A review on video/image authentication and temper detection techniques." *International Journal of Computer Applications* 63.10 (2013).
14. Upadhyay, Saurabh, and Sanjay Kumar Singh. "Video authentication-an overview." *International Journal of Computer Science and Engineering Survey* 2.4 (2011): 75..

15. Mahajan, Dipali Latesh, and Suvarna Amit Gogate. "Overview of Digital Watermarking and its Techniques." *KHOJ: Journal of Indian Management Research and Practices* (2016): 197-204.
16. Elango, S., Dr G. Thirugnanam, and R. Shankari. "A Survey of Digital Video Watermarking Techniques for Copyright Protection and Authentication." *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering* 4.4 (2015).
17. Rey, Christian, and Jean-Luc Dugelay. "A survey of watermarking algorithms for image authentication." *EURASIP Journal on applied signal processing* 2002.1 (2002): 613-621.
18. Hsu, Chiou-Ting, and Ja-Ling Wu. "DCT-based watermarking for video." *IEEE Transactions on Consumer Electronics* 44.1 (1998): 206-216.
19. Shojanazeri, Hamid, Wan Azizun Wan Adnan, and Sharifah Mumtadzah Syed Ahmad. "Video watermarking techniques for copyright protection and content authentication." *International Journal of Computer Information Systems and Industrial Management Applications* 5.1 (2013): 652-660.
20. Kaur, Ramanjeet, Arwinder Kaur, and Shalini Singh. "A Survey and Comparative Analysis on Video Watermarking." (2016).
21. Rashid, Aaqib. "Digital Watermarking Applications and Techniques: A Brief Review." *International Journal of Computer Applications Technology and Research* 5.3 (2016): 147-150.

