applied sciences

MDPI

Review

A Survey on Robust Video Watermarking Algorithms for Copyright Protection

Xiaoyan Yu, Chengyou Wang * and Xiao Zhou

School of Mechanical, Electrical and Information Engineering, Shandong University, Weihai 264209, China; xyy@mail.sdu.edu.cn (X.Y.); zhouxiao@sdu.edu.cn (X.Z.)

* Correspondence: wangchengyou@sdu.edu.cn; Tel.: +86-631-568-8338

Received: 16 September 2018; Accepted: 4 October 2018; Published: 11 October 2018

Abstract: With the development and popularization of the Internet and the rise of various live broadcast platforms, digital videos have penetrated into all aspects of people's life. At the same time, all kinds of pirated videos are also flooding the Internet, which seriously infringe the rights and interests of video copyright owners and hinder the healthy development of the video industry. Therefore, robust video watermarking algorithms for copyright protection have emerged as these times require. In this paper, we review robust video watermarking algorithms for copyright protection based on original videos and compressed videos. Basic models and properties of video watermarking algorithms are described, and the evaluation indexes corresponding to each property are also introduced. To help researchers understand various existing robust watermarking algorithms quickly, some basic information and the quantitative estimation of several performances are analyzed and compared. Finally, we discuss the challenges in the research of robust video watermarking algorithms, and give possible development directions for the future.

Keywords: video watermarking; copyright protection; robustness; performance comparison; evaluation indexes; overview

1. Introduction

The digitization of multimedia information, along with the development of computer technology and networks, has brought great convenience to the generation, storage, and dissemination of digital products, such as images, audios, and videos. Especially, network bandwidth and computer storage capacity have been greatly improved under the influence of Moore's law [1]. Meanwhile, with the widespread popularity of the Internet, the exchange of multimedia information has penetrated into every corner of social life. In recent years, webcast and video-on-demand (VOD) services have begun to rise and spread rapidly around the world, and the developments of the film and TV show industries are booming. As a result, the number and duration of online videos are increasing explosively, and the content is all-encompassing. Through the Internet, people can copy, process, and transmit videos of interest at will, which brings great convenience to people. However, it is followed by illegal acts such as piracy, infringement, and stealing, which not only damage the intellectual property rights of digital works' owners, but also affect the market order of electronic publications. Additionally, pirated works may pose a great threat to the safety of users because they are of poor quality and may carry and spread computer viruses. The issue of piracy infringement is undoubtedly a huge obstacle to the healthy development of the video industry. Therefore, copyright protection for digital video is extremely urgent [2].

The conventional copyright protection technology is cryptography [3], which guarantees the security of digital products through a secret key. Whether the important information is processed by a symmetric key system or a public key system with higher security, the obtained data are all garbled, so in the transmission process, attackers can only see these garbled codes and cannot decipher the confidential information, thus they cannot pirate. However, if the code transmitted between the two sides of the communication always seems to be meaningless, it may easily attract the attention and interest of attackers and then become the target. Once the cipher text is cracked, the encrypted data will become easily available. In addition, the copyright owner cannot monitor the files decrypted by legal users. As a result, the protection of encrypted data becomes ineffective and intellectual property rights cannot be traced and confirmed. Under this background, information hiding technology [4] with camouflage characteristics has emerged as these times require.

Information hiding technology hides important information in another open digital product, and then confidential information is transmitted by delivering the open carrier, which is an effective method to realize the secure transmission of confidential information in the network [5,6]. Information hiding technology mainly includes steganography [7], digital watermark [8], and covert communication [9], and its main branches are shown in Figure 1.

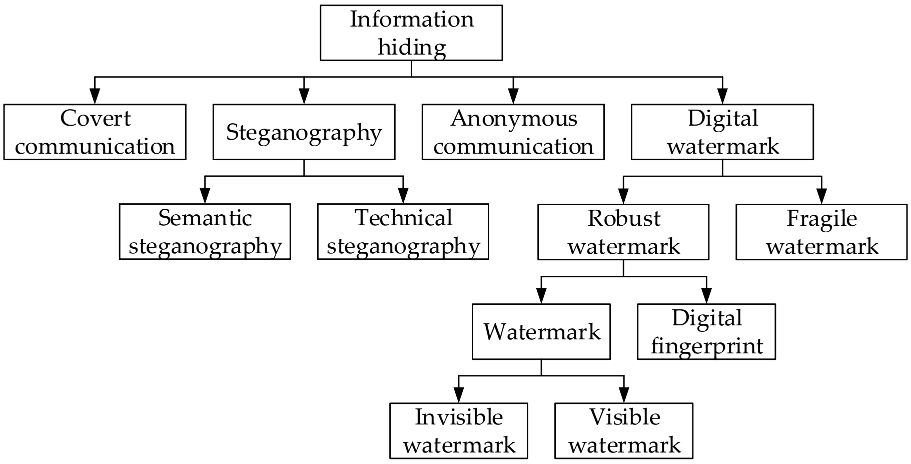

Figure 1. Main branches of information hiding.

Among these technologies, digital watermark, an important branch of information hiding, can truly solve the problem of copyright protection for digital products. It embeds invisible signs into digital products such as copyright information or authentication information. In this way, unauthorized users cannot detect the hidden information, and copyright protection can be achieved. When pirated products appear, product owners can extract hidden information to prove the copyright ownership and trace the acts of infringement. Besides, they can also provide legal evidence for charging illegal infringement. The original purpose of digital watermarking technology is to protect copyright. With the development of the technology, its application scope has become more and more extensive, including copyright protection, copy control, fingerprint identification, content authentication, broadcast monitoring, video tracking, and so on [10]. Meanwhile, its application objects have also been gradually extended from the early still digital images to other fields, such as videos, audios, and documents. With the increasing demand of digital video applications in people's daily life, videos gradually occupy an important position in multimedia digital works. At the same time, video content has gradually become the mainstream of information displayed on the Internet, so the copyright protection of video products has become more and more important. Consequently, video watermarking technology has become a research hotspot [11]. The application of video watermark in copyright protection is shown in Figure 2.

According to the characteristics of watermarks, they can be divided into three categories: robust watermark, fragile watermark, and semi-fragile watermark [12]. The robust watermark can resist various attacks, so it is often used for copyright protection. The fragile watermark is very sensitive to tampering attacks. Any attacks, including common signal processing attacks, may destroy the watermark information. As a result, it is mainly used for content authentication and tampering detection. The semi-fragile watermark combines the advantages of the robust watermark and fragile watermark. It can distinguish the common signal processing operations from malicious attacks. In this paper, we will focus on robust video watermarking algorithms for copyright protection.

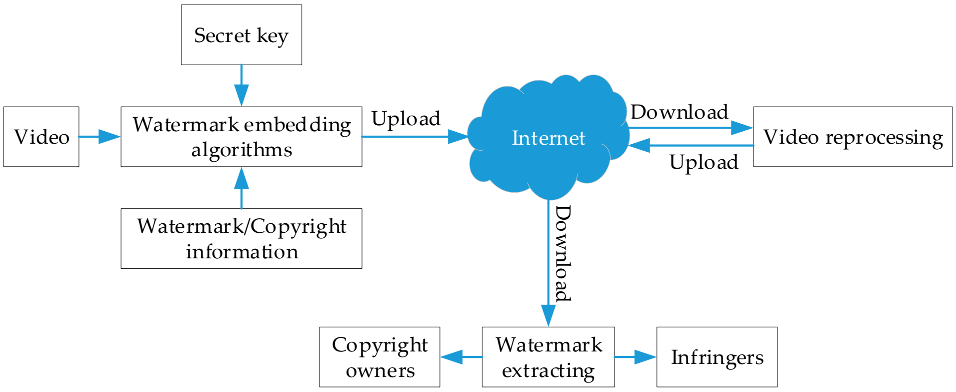

Figure 2. The application of video watermark in copyright protection.

The rest of this paper is organized as follows. Section 2 expounds the basic models of robust video watermarking algorithms, which include the watermark generation, watermark embedding, and watermark extraction. Properties of video watermarking algorithms are described in Section 3, and evaluation indexes of every property are also introduced. The literature study on robust watermarking algorithms based on original videos is presented in Section 4. Section 5 overviews robust watermarking algorithms based on compressed videos. Conclusions and possible further development directions are given finally in Section 6.

2. Basic Models of Video Watermarking

The robust video watermark is an important branch of digital video watermarks, which uses the temporal redundancy and spatial redundancy of video content to embed watermark information to achieve video copyright protection. General robust video watermarking algorithms include three components: watermark generation, watermark embedding, and watermark extraction or detection. According to the application of watermark technology, the emphasis of the algorithm in these three parts will also change accordingly. A framework of a general robust video watermarking algorithm is shown in Figure 3.

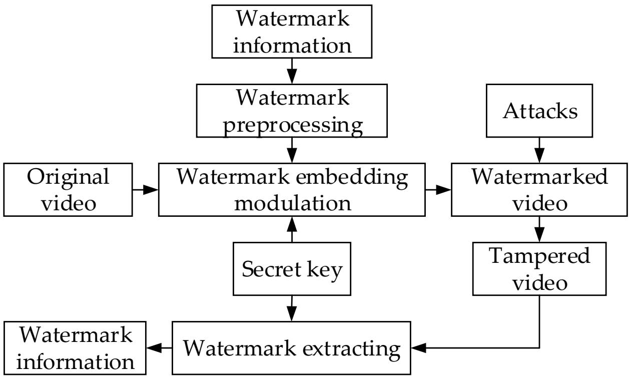

Figure 3. A framework of a general robust video watermarking algorithm.

2.1. Watermark Generation

Watermark generation is a crucial step in robust video watermarking algorithms. Watermark generation, which is also called watermark preprocessing, randomly scrambles watermark information to enhance the security of the watermarking algorithm. The general model of watermark generation is shown in Figure 4.

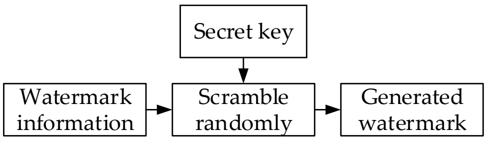

Figure 4. The general model of watermark generation.

Now, several main encryption algorithms used in watermark preprocessing stage will be introduced.

2.1.1. Arnold Transform

Arnold transform [13], also called cat map, can be seen as a combination process of stretching, compressing, folding, and splicing. Through this process, watermark information can be scrambled, which makes the original meaningful watermark become meaningless. Arnold transform has periodicity, that is, if it is continuously carried out on the image, finally the original image can be obtained. The period of transform is related to the size of the image. For watermark images with size of $N \times N$, the definition of Arnold transform can be expressed as:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mathrm{mod}(N), \tag{1}$$

where $[x\, y]^{\mathrm{T}}$ represents the pixel coordinate in original image; $[x'\, y']^{\mathrm{T}}$ denotes the transformed pixel coordinate; and a, b, and N are all positive integers. In general, the period P of transform is related to the size of N: P increases with the increase of N. This transform not only is a reversible transform, but also has good effectiveness and is easy to implement. However, its recovery time is long.

2.1.2. Magic Square Transform

Magic square transform [14] uses the defined magic square matrix to block the watermark image, and determines the size of blocks according to the image complexity. Magic square matrix is an n-order matrix with natural numbers $1, 2, \cdots, n$ as elements, which can be shown as:

$$\boldsymbol{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}. \tag{2}$$

If the elements in $\boldsymbol{A}$ meet:

$$\sum_{i=1}^{n} a_{i,j} = \sum_{j=1}^{n} a_{i,j} = \sum_{i=1}^{n} a_{ii} = \sum_{j=1}^{n} a_{jj} = \frac{n(n^2+1)}{2}, \tag{3}$$

then the matrix $\boldsymbol{A}$ is called the standard magic square matrix. This transform also has periodicity. For an image with the size of $N \times N$, the transform period is N^2. This transform is fast, safe, and robust, but the scrambling effect is poor, and the computational complexity is high.

2.1.3. Logistic Chaotic Map

Chaos refers to the seemingly random irregular movement occurring in a deterministic system. For a system, it is described by deterministic theory while its behavior is uncertain, unrepeatable, and unpredictable, which is the chaotic phenomenon. In chaotic systems, chaotic sequences can be reconstructed accurately using initial values. The ergodic statistical characteristic of Logistic chaotic sequences [15] is similar to zero-mean white noise, which has good randomness, correlation, and complexity. It is impossible to correctly predict chaotic sequences for a long time. Logistic chaotic sequence can be defined as:

$$x_{k+1} = \mu x_k(1 - x_k), \tag{4}$$

where $0 \leq \mu \leq 4$ is the branch parameter. In practical applications μ is limited to [3.57, 4]. This algorithm has better confidentiality than other general algorithms, and it has high fidelity, good security, sufficient bandwidth, and strong real-time feature. However, it also has shortcomings of high computational complexity and low operation efficiency.

In addition, there are other schemes to encrypt watermark information, such as pseudorandom number generator, encoding, spread spectrum technology, and so on. Through encryption, the difficulty of deciphering can be further enhanced, and the security of watermark can be improved.

2.2. Watermark Embedding

Watermark embedding is the process which embeds binary strings representing author's information or copyright information into the original video through a specific embedding algorithm. The embedding algorithm must take the balance between invisibility and robustness of the watermark into account. The model of embedding process is shown in Figure 5.

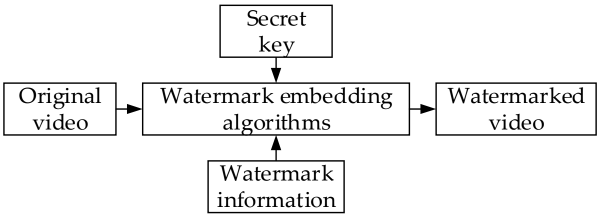

Figure 5. The model of embedding process.

According to the different embedding positions of watermarks, video watermarking algorithms can be divided into three types: original video-based watermarking algorithm, video watermarking algorithm in encoding process, and video watermarking algorithm after compression. Video watermarking algorithms obtained by these three embedding methods have their own advantages and disadvantages.

2.2.1. Original Video-Based Watermarking Algorithms

For an original video-based watermarking algorithm, the original host video is treated as an aggregate of a series of still images that are temporally continuous. Watermark information is embedded into the original video, and then the watermarked video is recompressed [16]. The advantages of these kinds of algorithms include (i) that the implementation of the algorithm is relatively simple, and many watermarking schemes applied to still images are also suitable for the algorithm and (ii) the algorithm does not rely on specific video compression standards and has strong universality. Its disadvantages include (i) watermark extraction requires complete decoding, which leads to high complexity; (ii) watermark information can be easily removed by a compression standard with a high compression ratio; and (iii) the compressed host video needs to be decoded first, and then encoded after watermark embedding.

2.2.2. Video Watermarking Algorithms in Encoding Process

The video watermarking algorithm in encoding process usually realizes watermark embedding by modifying several redundant spaces of video in the process of compression coding, such as quantized discrete cosine transform (DCT) coefficients, prediction modes, motion vectors, etc. The advantages of this type of algorithms include (i) embedding watermark into quantized coefficients is simple and effective, and has little influence on the code rate of video streams and (ii) it can be directly combined with corresponding video coding standards and, through the modification of the encoder, the watermark can be embedded and extracted in real time. Its disadvantages include (i) the embedding capacity of the watermark is affected by video coding parameters and (ii) it needs to modify the encoder and decoder, which limits the introduction of some watermarking algorithms to a certain extent.

2.2.3. Video Watermarking Algorithms after Compression

The video watermarking algorithm after compression searches for redundant space in the compressed bit stream and embeds watermark information into it. The advantages of this type of algorithms include (i) the algorithm is independent of the corresponding codec and has high efficiency and (ii) the computational redundancy is small and the fidelity is high. Its disadvantages include (i) the redundant space available for watermark embedding is very small, which leads to limited capacity; and (ii) the robustness of the algorithm is poor.

To sum up, each algorithm has its own advantages and disadvantages. In practical application, different watermark types are selected according to different occasions and different requirements.

2.3. Watermark Extraction

Watermark extraction is the inverse process of watermark embedding. The position of watermark embedding is determined first, and then the watermark is extracted from the video data combining the secret key with the watermark extraction algorithm. Finally, the extracted watermark is decoded to obtain the original watermark information. The basic model of watermark extraction is shown in Figure 6.

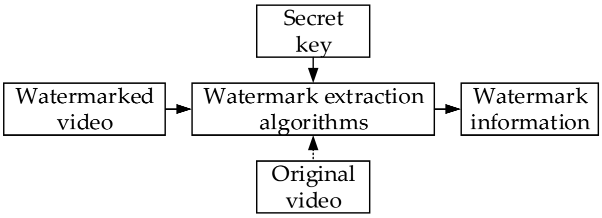

Figure 6. The basic model of watermark extraction.

The watermark detection process is used to detect whether there is watermark information in video data, which is a probability judgment process based on statistical principles. According to whether the original video is needed to participate during the process of watermark extraction, the watermark algorithms can be divided into two categories: blind detection algorithms and non-blind detection algorithms [17]. Blind detection algorithms that do not require original videos are generally used.

3. Properties of Video Watermarking

A video is composed of a series of temporally continuous images, but it is not just a simple combination of images, because adjacent frames not only have high correlation but also have a large amount of spatial and temporal redundancy. Therefore, video watermarking algorithms not only have some characteristics of image watermarking algorithms, such as imperceptibility, robustness, watermark capacity, and security, but also have their own unique characteristics, such as random detection, real-time processing, code rate constancy, and combination with video coding standards [18]. In different applications, watermarking algorithms need to meet different requirements. For general robust video watermarking algorithms, performance is usually evaluated by analyzing their imperceptibility, robustness, watermark capacity, and real-time processing. In addition, for watermarking algorithms in compressed domain, bit increase rate (BIR) may be measured as one of the performance metrics. Next, these properties and their evaluation indexes will be introduced.

3.1. Imperceptibility

Imperceptibility, also called invisibility, requires that the watermark information embedded in the video cannot be perceived by the human eye. In other words, the embedding of watermark information cannot significantly affect the visual quality of the video. Although many watermarking algorithms are visible now, their application is limited to specific occasions. Invisible watermarking algorithms occupy the mainstream position. How to find embedding positions in the video, which can not only minimize the influence on the visual quality, but also have strong robustness, is one of the key contents in the research of robust video watermarking algorithms.

Mean peak signal-to-noise ratio (MPSNR) and mean structural similarity index (MSSIM) [19] are commonly used to quantitatively evaluate the imperceptibility of video watermarking algorithms. If the number of watermarked frames is K and the size of video frames is $M \times N$, the definition of MPSNR I_{MPSNR} is given as:

$$I_{\text{MPSNR}} = \frac{1}{K}\sum_{k=1}^{K} PSNR_k, \tag{5}$$

$$\text{PSNR}_k = 10\log_{10}\frac{255^2}{\text{MSE}_k}(\text{dB}), \tag{6}$$

$$\text{MSE}_k = \frac{1}{M \times N}\sum_{m=1}^{M}\sum_{n=1}^{N}[f_k(m,n) - f_{kw}(m,n)]^2, \tag{7}$$

where f_k is the k-th original video frame; f_{kw} is the k-th watermarked frame; and MSE is the mean square error between f_k and f_{kw}.

Sometimes, MPSNR cannot be well associated with subjective evaluation results, so MSSIM is introduced to evaluate video quality. The definition of MSSIM I_{MSSIM} is shown as:

$$I_{\text{MSSIM}} = \frac{1}{K}\sum_{k=1}^{K} SSIM(f_k, f_{kw}), \tag{8}$$

$$\text{SSIM}(f_k, f_{kw}) = \frac{(2\mu_{f_k}\mu_{f_{kw}} + C_1)(2\sigma_{f_k f_{kw}} + C_2)}{(\mu_{f_k}^2 + \mu_{f_{kw}}^2 + C_1)(\sigma_{f_k}^2 + \sigma_{f_{kw}}^2 + C_2)}, \tag{9}$$

where μ_{f_k} and $\mu_{f_{kw}}$ represent the mean values of the original frame and the watermarked frame, respectively; σ_{f_k} and $\sigma_{f_{kw}}$ are the variances of the original frame and the watermarked frame, respectively; $\sigma_{f_k f_{kw}}$ denotes the covariance of the original frame and the watermarked frame; and C_1 and C_2 are two constants to maintain stability.

3.2. Robustness

Robustness means that the watermark information can still be extracted completely or recognized correctly from the video which is subject to various normal image processing operations or malicious tampering attacks. As long as the video does not lose its use value after being attacked, the embedded watermark information cannot be destroyed. Similarly, if the embedded watermark information is destroyed, the video quality should be reduced to lose its use value.

Robustness-related attacks that video watermarking algorithms should be able to resist include three types: normal image processing attacks, geometric attacks, and temporal synchronization attacks. Several typical attacks corresponding to these three types of attacks are listed in Table 1. To evaluate the performance of various algorithms in Sections 4 and 5 conveniently, the corresponding abbreviations of various attacks are also listed.

Table 1. Several typical attacks and their corresponding abbreviations.

Signal Processing Operations	Geometric Attacks	Temporal Synchronization
Gaussian filter (GF), Median filter (MF)	Scaling (Scl)	Frame dropping (FD)
Average filter (AF), Wiener filter (WF)	Cropping (Crp)	Frame swapping (FS)
Circular filter (CF), High-pass filter (HPF)	Rotation (Rtt)	Frame insertion (FI)
Gaussian noise (GN), Impulsive noise (IN)		Frame averaging (FA)
Salt & pepper noise (SPN), Speckle noise (SN)		Frame cropping (FC)
JPEG, MPEG-2, MPEG-4, H.264, H.265		
Gamma correction (GC), Sharpening (Shp)		
Histogram equalization (HE), Blurring (Blu)		
Luminance modification (LM), Recompression (Rec)		
Contrast enhancement (CE), Transcoding (Trs)		

In general, normalized correlation (NC) and bit error rate (BER) are used to quantify the robustness of watermarking algorithms. NC is used to estimate the similarity between the extracted watermark and the original one [20]. For watermark images with size of $M \times N$, the definition of NC I_{NC} can be expressed as:

$$I_{\text{NC}} = \frac{\sum\limits_{i=1}^{M}\sum\limits_{j=1}^{N} W(i,j) \times W'(i,j)}{\sum\limits_{i=1}^{M}\sum\limits_{j=1}^{N} W(i,j)^2}, \tag{10}$$

where $W(i,j)$ and $W'(i,j)$ denote the pixel values at coordinates (i,j) in original watermark and extracted watermark, respectively. The value range of NC is [0, 1]. The higher the value of NC, the stronger the anti-attack ability of watermarking algorithm.

BER is used to estimate the error rate between the extracted watermark and the original watermark [21]. The definition of BER I_{BER} is shown as:

$$I_{\text{BER}} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|W(i,j) - W'(i,j)\right| \times 100\%, \tag{11}$$

where $W(i,j)$ and $W'(i,j)$ denote the pixel points at coordinates (i,j) in original watermark and extracted watermark, respectively. The smaller the BER, the better the robustness.

3.3. Watermark Capacity, BIR, and Real-Time Performance

Watermark capacity refers to the number of watermark bits embedded in unit time or a single video. The watermark capacity, imperceptibility, and robustness are mutually restricted [22], and their relationship is shown in Figure 7.

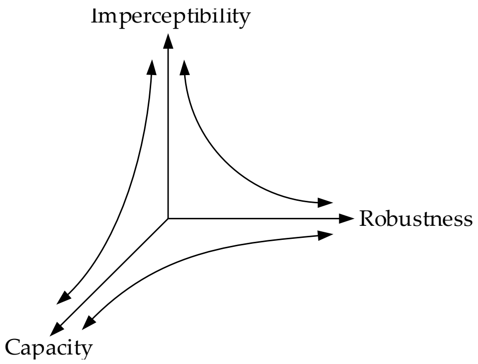

Figure 7. Relationship among watermark capacity, imperceptibility, and robustness.

For a specific watermarking algorithm, if it needs good imperceptibility in practical applications, it is necessary to avoid too much modification to the original video. As a result, the watermark capacity will be reduced. Meanwhile, too little modification will also lead to a decrease in the robustness of the algorithm. If the algorithm needs to have good robustness in practical applications, it will definitely need to make more modifications to the video, which will increase the watermark capacity and reduce the imperceptibility of the watermark. Theoretically speaking, it is impossible to design a watermarking algorithm that can achieve the three optimally at the same time. It is necessary to realize a compromise among the three according to the actual situation. When designing robust video watermarking algorithms, the robustness is improved as much as possible on the premise that watermark capacity and imperceptibility can meet certain conditions. Watermark capacity is usually quantified by the number of watermark bits embedded in the video.

BIR is used to measure the increase of the video bit rate, which is often measured in watermarking algorithms based on compressed videos.

Real-time performance refers to the low complexity of watermark embedding and extracting, which is usually evaluated by the length of time. Only when the watermarking algorithm meets the real-time requirement, can the smoothness of video data stream be ensured. The better the real-time performance of the watermarking algorithm is, the wider its application scope will be.

4. Robust Watermarking Algorithms Based on Original Videos

The watermark algorithms based on original videos take uncompressed video sequences as objects to process. The watermark information is embedded into the original video, and then the video frames containing the watermark are compressed and encoded. According to whether watermarking algorithms are combined with image transformation, they can be further divided into two types: robust video watermarking algorithms in spatial domain and robust video watermarking algorithms in transform domain.

4.1. Video Watermarking in Spatial Domain

Video watermarking algorithms in spatial domain usually embed the watermark directly into the luminance or chrominance components of the original video, which often have two prominent characteristics: low complexity and high payload. The main spatial domain methods include least significant bit (LSB) modification [23], spread spectrum modulation [24], and so on. Among them, the LSB method is the most classical embedding method, which embeds the watermark into the LSB of the component. H. Kaur and E. V. Kaur [25] proposed an invisible video watermarking algorithm using an optimized LSB technique. A pseudorandom number generator and secret key are used to improve the secure of the algorithm. Although LSB substitution is an extremely simple technique, its robustness is very poor. To improve the robustness, Bayoudh et al. [26] proposed a multi-sprites dynamic video watermarking algorithm based on speed-up robust features (SURF), which can effectively resist collusion and transcoding attacks. The watermark information is embedded into three YUV color space components by modifying the middle significant bit (MIDSB) and LSB, which can provide high level of robustness and invisibility.

Watermarking algorithms based on the spread spectrum are also effective spatial domain algorithms. The original video frames are scanned according to orders to obtain a one-dimensional signal, and the watermark information is modulated into pseudorandom sequences by spread spectrum technology and embedded in the video signal [27]. In a previous paper [28], the watermark was expanded to the same size as the video frame, and then embedded frame by frame. Since the same watermarks in different frames amplify each other during the averaging process, the proposed scheme can resist frame averaging attacks. To improve the robustness to different attacks, Preda and Vizireanu [29] introduced cyclic error correction codes to resist bit errors of watermark. Spread spectrum is adopted to spread the power spectrum of the watermark. Spatial redundancy is used to embed the spread watermark in luminance pixels and temporal redundancy is used to embed the same watermark in each frame of each group.

There are also many other robust video watermarking algorithms in spatial domain. For example, Venugopala et al. [30] decomposed the grayscale watermark image into eight bit-plane images and embedded them into different scenes of original video. Some pixel values of Y component in video frames are selected and grouped, and the watermark is embedded by adjusting the relative relationships of pixel values in every group. Bahrami and Tab [31] proposed a semi-blind video watermarking algorithm based on SURF and block classification. The best frames of each shot and the best regions or blocks of best frames, which are robust to resist multiple attacks, can be selected using shot segmentation and attack tests. The block classification technique based on canny edge detection is adopted to divide selected robust blocks into two kinds: edge blocks and flat blocks. Then, the owner's share information can be obtained by combining the classification results and watermark information. To resist scalable recompression and transcoding attacks, a robust video watermarking algorithm based on a spatial uniform mapping model was proposed by Li et al. [32]. Frames before scene change are selected for embedding using histogram difference method, which can resist the aimless frame dropping attack. The binary image with fixed size is processed by Arnold transform, and then uniformly embedded into the blue component of selected frames through a spatial random mapping algorithm.

Watermarking algorithms in spatial domain are widely used in the early stage due to its low complexity. However, with the development of video coding technology, its robustness is poor and thus its application scope is limited. The summary comparison of several watermarking algorithms in spatial domain is shown in Table 2.

Table 2. Summary comparison of several watermarking algorithms in spatial domain.

Ref.	Type	Watermark Preprocessing	Embedding Position
[26]	Blind	Encoding	MIDSB of Y component; LSB of U and V components
[28]	Blind	Pseudonoise sequence	Each frame
[29]	Blind	Pseudorandom noise generator	Luminance component of each frame
[30]	Blind	-	Luminance component of each frame
[31]	Semi-blind	-	Blocks with robustness to most attacks
[32]	Blind	Arnold transform	Frames selected by scene change

4.2. *Video Watermarking in Transform Domain*

Video watermarking algorithms in transform domain transform video frames into the frequency domain first, and then modify the coefficients in the frequency domain to achieve the purpose of watermark embedding. After embedding, the video is converted back to the spatial domain from the frequency domain to obtain the watermarked video. Common frequency domain transforms include DCT, discrete wavelet transform (DWT), singular value decomposition (SVD), etc. In addition, many watermarking algorithms in transform domain combine two or more transforms together to improve the performance using the advantages of different transforms.

4.2.1. DCT-Based Watermarking Algorithms

Due to the energy compaction characteristic of DCT, the energy of video frames after DCT transform is mainly concentrated in DC coefficients and low-frequency sub-band [33]. Compared with the high-frequency sub-band, the human eye perception and robustness are better in the low-frequency sub-band. Therefore, the selection of watermark embedding positions should consider the compromise between invisibility and robustness. Liu et al. [34] proposed a robust video watermarking algorithm in DCT domain based on high-frequency coefficients correlation algorithm. To prevent high-definition (HD) videos from unauthorized copying, Cheng et al. [35] proposed a recoverable video watermarking algorithm in DCT domain based on code division multiple access (CDMA) modulation. Nguyen and

Duan [36] embedded eight bit-plane images decomposed from a grayscale watermark image into DCT coefficients with robustness, which were selected in the video luminance component using an even-odd quantization algorithm. In a previous paper [37], selected regions, based on the properties of the human visual system (HVS), were converted to the YUV space, and then the Y component was processed to extract Krawtchouk moments using optimal orders which can maximize the quality of the reconstruction. The DCT scheme is implemented to the obtained Krawtchouk moments to achieve the embedding process combining the secret key. Thanh et al. [38] adopted the KAZE feature to achieve the synchronization between the watermark embedding and extracting regions in the video watermarking algorithm. The KAZE feature points are extracted from a video frame, and matched with those of frame-patch to detect the embedding and extracting regions in all frames. The watermark is inserted into randomly generated blocks in matched regions in DCT domain.

What is more, the quantization index modulation (QIM) [39] scheme is adopted in many DCT-based watermarking algorithms [40–43]. In another past paper [40], to reduce computation time, a pseudo-3D DCT transform by two times of DCT transform was introduced. By adjusting the correlation between DCT coefficients of selected blocks, the watermark is embedded into continuous video frames converted into pseudo codes before compression combining the QIM scheme. While embedding the watermark, some information is recorded as a secret key to strengthen the security of the algorithm. Huang et al. [41] combined QIM with pseudo-3D DCT and proposed a blind video watermarking algorithm. Pseudo-3D DCT is used to obtain the embedding factor and useful messages. The watermark is embedded into the luminance component of each I frame in original video based on the correlation between DCT coefficients. The use of QIM makes it easy to derive the embedding position of the watermark. However, this algorithm cannot resist geometric attacks, like scaling. Combining the spatial and temporal dimensions of video sequences, Campisi and Neri [42] proposed a watermark embedding technique based on QIM and rational dither modulation (RDM). The video is divided into spatial and temporal dimensions, and projected into the 3D DCT domain. Then, a set of transform coefficients are selected according to the rules for watermark embedding. Cedillo-Hernandez et al. [43] applied a spatiotemporal saliency-modulated just noticeable distortion (JND) profile to a video watermarking algorithm, which adopted the JND method to control the watermark strength and make the distortion of the video under the sensitivity threshold. The algorithm combines the saliency-modulated JND profile and QIM model to achieve embedding of watermark. In addition, it takes full advantage of the spatiotemporal characteristics of video sequence to minimize its perceptual redundancies and reduce the computational complexity.

Compared with watermarking algorithms in spatial domain, DCT-based watermarking algorithms are more robust. However, for strong geometric attacks, the robustness of the DCT-based watermarking algorithm is poor. The summary comparison of several watermarking algorithms in DCT domain is shown in Table 3.

Table 3. Summary comparison of several watermarking algorithms in DCT domain.

Ref.	Type	Watermark Preprocessing	Embedding Position
[34]	Blind	Arnold transform	High-frequency coefficients of R, G, and B components
[35]	Blind	CDMA	DCT coefficients of Y component
[36]	Blind	-	Robust DCT coefficients selected in Y component
[37]	Non-blind	-	Selected coefficients in KDCT matrix of Y component
[38]	Semi-blind	Arnold transform	Low-frequency DCT coefficients of Y component
[40]	Blind	Permuted processing	AC values of selected DCT blocks in Y component
[41]	Blind	Pseudorandom generator	Y component of each I frame
[43]	Blind	-	AC coefficients of each 2D DCT block in Y component

4.2.2. DWT-Based Watermarking Algorithms

Due to the excellent spatial localization, frequency spread, and multiresolution characteristics of the methods in the wavelet domain, many algorithms based on DWT are gaining popularity. Abdulfetah et al. [44] proposed an adaptive video watermarking algorithm based on visual models.

To obtain JND masking, the visual model is designed by analyzing luminance masking, texture masking, and entropy masking. On the basis of the JND threshold, the scrambled watermark is embedded in mid-frequency coefficients. El'Arbi et al. [45] embedded different parts of the watermark into several shots of a video sequence. On the basis of the motion activity analysis, region complexity and motion information are combined to separate different regions of the original video into perceptually distinct categories. The embedding positions of the watermark are adjusted adaptively based on HVS. In another previous paper [46], shot detection was adopted to obtain key frames and moving frames from the video, and watermark bits were embedded into two high-frequency coefficients of the first-level DWT randomly. Based on matching at least two feature points generated by scale invariant feature transform (SIFT) in the original video frame and the frame containing watermarks, the frame that is subject to rotation attacks can be recovered. On the basis of integer wavelet and SIFT, Gao et al. [47] proposed a video dual watermarking algorithm to resist geometric attacks. The integer wavelet transform is adopted to divide the video frame into a low-frequency sub-band and a medium–high frequency sub-band. For coefficients in the medium–high frequency sub-band, various motion characteristics are calculated using the block matching algorithm, and then the threshold of human visual masking based on the video frame can be obtained. As a result, the watermark is inserted into the medium–high frequency sub-band adaptively. For coefficients in the low-frequency sub-band, due to the stability of the coefficient histogram to geometric attacks, the watermark is embedded into the neighboring bins. In a past paper [48], to achieve a compromise between the invisibility of the watermark and adaptability to attacks, the watermark was embedded into the second level of the medium–high frequency wavelet coefficients using the secret key and quantization method. In addition, the use of error correction codes and the scheme that embeds the same watermark in different frames redundantly play a great role in improving the performance of the algorithm. On the basis of [48], Preda and Vizireanu [49] proposed a robust watermarking algorithm based on quantization and spread spectrum technology. An optimal quantization model based on the characteristics of HVS is introduced to quantize wavelet coefficients selected from different sub-bands, and then the watermark embedding process can be achieved. To prevent the collusion attack, Gupta et al. [50] adopted DWT to resize frames into 512 × 512 based on security model, and the maximum mean values of LL and HL bands were used to select watermark positions. In addition, the group search optimization (GSO) algorithm is applied to optimize the selected positions. In another past paper [51], scene change analysis was applied to detect the motion part of color video, and then 3D DWT was performed over these frames to obtain wavelet coefficients. By using a spread spectrum technique, the watermark is embedded into selected 3D coefficients of HL, LH, and HH sub-bands. The experimental results show that the algorithm has good transparency and robustness. Bhardwaj et al. [52] proposed a robust video watermarking algorithm using significant frame selection (SFS) based on lifting wavelet transform (LWT) coefficient difference. Significant frames are selected according to the mathematical relationship among the number of original video frames, the size of coefficient blocks, and the embedding capacity. Using LWT, the luminance component Y of the selected frame is decomposed into three levels, and the LH_3 sub-band coefficients are obtained for watermark embedding.

Although DWT-based watermarking algorithms can be better when combined with HVS, its robustness to translation attack and scaling attack is weak. The summary comparison of several watermarking algorithms in DWT domain is shown in Table 4.

Table 4. Summary comparison of several watermarking algorithms in DWT domain.

Ref.	Type	Watermark Preprocessing	Embedding Position
[44]	Blind	Arnold transform	Middle-frequency DWT coefficients of Y component
[45]	Blind	Pseudorandom generator	Middle-frequency DWT coefficients of Y component
[46]	Blind	Arnold transform	High-frequency DWT coefficients of Y component
[47]	Non-blind	Chaotic encryption	Selected blocks of Y component based on human visual masking threshold
[48]	Blind	Spread-spectrum technique	LH_2, HL_2, and HH_2 sub-bands of Y component
[49]	Blind	Pseudorandom generator	LH_2, HL_2, and HH_2 sub-bands of Y component
[50]	Blind	Resize	LL and HL sub-bands
[51]	Blind	Spread-spectrum technique	3D coefficients of HL, LH, and HH sub-bands
[52]	Blind	Random shuffling	LH_3 sub-band of luminance component

4.2.3. SVD-Based Watermarking Algorithms

SVD is a special matrix transformation, which can transform a matrix to two orthogonal matrices and one diagonal matrix with singular values. From the perspective of image processing, the singular value of images has good stability, and it embodies the intrinsic characteristics of images rather than the visual characteristics. These characteristics of SVD make it widely used in the field of robust video watermarking, and the watermark information is often embedded in the singular values matrix to get good imperceptibility [53]. Usually, it is adopted together with DWT in robust video watermarking [54–60]. In a past paper [54], a fast gradient magnitude similarity deviation (GMSD) algorithm was used to detect the shot boundaries of the video sequence, and then representative key-frames can be extracted. After the watermark information is encrypted by a new chaotic encryption, DWT and SVD are combined to embed the watermark information into extracted key-frames. Adul and Mwangi [55] also proposed a blind video watermarking algorithm based on a hybrid SVD/DWT technique. DWT is applied to the G components of selected frames, and then the obtained diagonal detail coefficients are implemented with SVD to embed watermark information into singular values matrices. To obtain high robustness with low payload, four kinds of embedding methods were proposed and compared in another past paper [56]. The fourth method, which combines the scene change detection and the spread spectrum approach, inserts only single watermark in the whole video, achieving the lowest payload but strong robustness. Sathya and Ramakrishnan [57] extracted key frames by scene change detection based on histogram difference method combining with the Fibonacci sequence. Before embedding, the watermark is scrambled by Fibonacci–Lucas transform to improve the security of the algorithm. The encrypted watermark is divided into blocks and embedded into the selected key frames based on the DWT and SVD. Agilandeeswari and Ganesan [58] decomposed the color watermark image into 24-bit planes and scrambled them by Arnold transform before embedding. Contourlet transform (CT) is used to capture smooth contours in video frames selected by scene change detection, and DWT is used to obtain better multiresolution sub-bands. Then, SVD is implemented to select DWT sub-bands to embed the watermark. In a past paper [59], the selection of key frames was realized by chaotic map. DWT is performed on selected video frames, and SVD is performed on the transformed frames and watermark image, respectively. The two obtained singular value matrices are added to complete the watermark embedding. The algorithm proposed by Shanmugam and Chokkalingam [60] takes all video frames as processing objects. DWT is adopted to luminance components of video frames, and 2-level DWT is implemented to the LH sub-bands. SVD is performed on the obtained HL_2 sub-bands using its high stability, and then watermark embedding can be realized.

Hybrid DWT-SVD algorithms can not only have higher relevancy to human perception, but also reduce the dimension of data, which means that they can combine the advantages of DWT and SVD. However, using SVD of watermark image in embedding phase will lead to false positive detection problems [61]. The summary comparison of several SVD-based watermarking algorithms is shown in Table 5.

Table 5. Summary comparison of several SVD-based watermarking algorithms.

Ref.	Type	Watermark Preprocessing	Embedding Position
[54]	Blind	Chaotic encryption	Singular value matrix of LL_1 sub-bands in Y component
[55]	Blind	Pseudorandom generator	Singular value matrix of diagonal detail coefficients of G component
[56]	Non-blind	SVD	Singular value matrix of LL_2 sub-bands in Y component
[57]	Blind	Fibonacci–Lucas transform	Singular value matrix of LH sub-bands of R component
[58]	Non-blind	Arnold transform	Singular value matrix of 2-level DWT LH and HL sub-bands in Y component
[59]	Blind	Chaotic map	Singular value matrix of LL sub-bands in Y component
[60]	Blind	2-level DWT	Singular value matrix of HL_2 sub-bands of LH sub-bands in Y component

4.2.4. Hybrid Transform-Based Watermarking Algorithms

To combine the advantages of different transformation methods to better improve the performance, many watermarking algorithms in the hybrid domain have emerged [62–66]. In a previous paper [62], scene identification and scene summarization were adopted to generate the video summary, and then the summary was used to detect the first type of feature regions by using the crowdsourcing technique. The second type of feature regions are detected by using the moving objects and the mosaic frame generated from the original video. After these two types of feature regions are merged, the final mosaic is generated, and the watermark is embedded into it by DCT, DWT, and SVD methods. To resist frame blending and projection attacks, Gaj et al. [63] combined DCT and 3D-DWT together to embed the watermark. Depending on the energy compression property of DCT and the multiresolution property of DWT, some hybrid DWT/DCT-based video watermarking algorithms have been proposed [64,65]. In another past paper [66], a zero-video watermark algorithm based on 2D-DWT and pseudo-3D DCT was proposed. The introduction of the log-polar transform improves the robustness to rotation operations. The watermark is encoded into a code division multiple access watermark through spread spectrum technology and then SVD is combined to embed the watermark. The summary comparison of several watermarking algorithms in hybrid domain is shown in Table 6.

Table 6. Summary comparison of several watermarking algorithms in hybrid domain.

Ref.	Type	Watermark Preprocessing	Embedding Position
[62]	Blind	Scrambling	Feature regions obtained by crowdsourcing and moving objects
[63]	Blind	-	Low-frequency DCT coefficients of regions around SIFT points in LLL sub-bands
[64]	Blind	Arnold transform	Middle-frequency components
[65]	Blind	Index mapping table	Three selected DCT coefficients of LL_2 sub-bands in suitable channel
[66]	Blind	Spread spectrum and Logistic map	Feature values generated by dual transform and log-polar in luminance component

In addition, to help readers know the performance of original video-based algorithms involved in the paper quickly, Table 7 gives the quantitative comparison of invisibility and robustness of several typical algorithms in spatial, DCT, and DWT domains, and Table 8 gives the quantitative comparison of invisibility and robustness of several typical algorithms in hybrid domain.

In Tables 7 and 8, the numbers in "( )" indicate the parameters of attacks and "-" shows that the attack is not mentioned in the reference. The reason may be that the algorithm cannot resist the attack, or the authors have not considered it. In addition, the full names of several typical attacks corresponding to the abbreviations mentioned in Tables 7 and 8 are given in Table 1.

Table 7. Quantitative comparison of invisibility and robustness of several typical algorithms in spatial, DCT, and DWT domains.

	Ref.		[26]		[29]	[38]	[41]	[43]	[45]	[46]		[48]	[52]	
	PSNR (dB)		[58, 73]		[33, 44]	36.85	[31, 69]	[44, 56]	56.18	≥38		[45, 49]	41.50	
	SSIM		-		-	≥0.93	-	[0.97, 1]	-	[0.99, 1]		-	-	
	Robustness		NC	BER	BER	NC	NC	BER	NC	NC	BER	BER	NC	BER
ATTACKS	MF (3 × 3)		-		≤0.007	-	0.993	-	-	-	-	0.149	0.990	0.005
	GN	(0.004)	0.259	0.440	(0.0005)	-	0.997	0.050	-	(0.05)		(0.005)	(0.01)	
		(0.006)	-		0.000			0.090	-	0.985	0.015	0.001	0.841	0.080
	SPN (0.0005)		1.000	0.000	0.000	-	0.993	-	-	-	-	0.000	(0.01) 0.937	0.032
	JPEG (Q = 80)		-		≤0.447	-	-	-	-	0.713	0.287	0.020	0.999	0.000
	MPEG-2	(4 Mbps)	-		≤0.406	-	1.000	0.008	0.940	-	-	0.074	-	0.065
		(2 Mbps)			≤0.476	-	1.000	0.009		-	-	0.252	-	0.201
	MPEG-4	(2 Mbps)	0.921	0.027	-	1.000	-	0.008	0.790	-	-	-	-	-
		(1 Mbps)	0.921	0.027		1.000		0.009						
	Scl	(1.2)	1.000	0.000	-	1.000	-	0.064	0.673	-	-	-	(0.5)	
		(0.8)	0.868	0.046		1.000		0.023					0.979	0.012
	Crp	(40%)	0.495	0.129	-	-	-	-	0.660	0.718	0.282	-	(25%)	
		(20%)	1.000	0.000		-				0.863	0.136		0.926	0.043
	FD (10%)		Robust		-	0.677	-	-	Robust	0.996	0.004	0.015	0.894	0.051
	FA (10%)		-		≤0.006	1.000	-	-	Robust	0.996	0.004	0.013	-	-
	Other attacks the algorithm can resist		PN, IN, AF, GF, HPF, Trs, Rtt, H.264, and FS		Blu	GF, Rtt, FI, FS, and Blu	WF, LM, and H.264	IN, Trs, and H.264	CE, LM, and Rtt	IN, Blu, Shp, GC, Rtt, FS, and FC		Blu and LM	SN, GF, AF, HE, Shp, LM, GC, and H.264	

Table 8. Quantitative comparison of invisibility and robustness of several typical algorithms in hybrid domain.

	Ref.		[54]		[57]		[58]		[63]	[64]	[66]	
	PSNR (dB)		[44, 50]		[41, 53]		[55, 68]		[32, 46]	48.726	-	
	SSIM		-		-		≥0.700		≥0.976	-	-	
	Robustness		NC	BER	NC	BER	NC	BER	NC	NC	NC	BER
ATTACKS	MF (3 × 3)		1.000	0.000	0.963	-	0.883	0.048	0.784	0.994	0.998	0.003
	GN (0.01)		1.000	0.000	0.970	0.127	0.954	0.022	-	0.985	0.982	0.025
	SPN	(0.01)	1.000	0.000	0.970	0.269	-	-	0.864	(0.05)	0.999	0.002
		(0.02)	-	-			0.988	0.035	0.788	0.995	0.994	0.009
	FA		0.990	0.013	0.950	0.300	-			0.921	0.976	0.034
	FD		-		0.983	0.163	0.985	0.019	-	0.933	0.985	0.020
	FS		-		0.990	0.120	0.941	0.036	-	0.936	0.980	0.027
	Other attacks the algorithm can resist		CF, Blu, Shp, HE, Crp, Scl, and H.264		Blu and LM		Rtt and CE		GF, CE, LM, Scl, and H.265	Shp, HE, and GC	GF, NF, Crp, and Rtt	

5. Robust Watermarking Algorithms Based on Compressed Videos

In the Internet the amount of video data is huge, so it is usually stored and transmitted in compressed form. The conventional watermarking algorithm, based on original video, needs to decode the video completely in order to embed and detect the watermark, which is not suitable for compressed videos. With the successive promulgation of international video coding standards, some video watermarking algorithms based on compressed domain have emerged as the times require. They embed watermark information into compressed videos, so watermark embedding processes must be combined with corresponding video coding standards. In this section, we will focus on introducing robust video watermarking algorithms based on three coding standards, which include moving picture experts group (MPEG) [67], H.264/advanced video coding (H.264/AVC) [68], and H.265/high efficiency video coding (H.265/HEVC) [69].

5.1. MPEG-Based Watermarking Algorithms

MPEG is an expert group established jointly by the international organization for standardization (ISO) and the international electrotechnical commission (IEC) in 1988 to develop standards for the encoding, decoding, and synchronization of television image data and audio data. The standards developed by this expert group are called MPEG series standards, and different versions of the standards show different uses and visual quality, which have played a revolutionary role in promoting the development of multimedia communication. Next, MPEG-2 and MPEG-4 standards will be introduced, and several video watermarking algorithms based on them will be summarized.

MPEG-2 is a lossy compression standard for video and audio organized and formulated by MPEG in 1994. It is a compression scheme for standard digital television and high-definition TV under various applications, and its coding rate ranges from 3 Mbit/s to 100 Mbit/s [70]. To reduce the computational complexity, many video watermarking algorithms in the compressed domain only need partial decoding in watermark embedding process [71–73]. To resist scaling attacks, Wang and Pearmain [71] proposed a MPEG-2 video watermarking algorithm based on shadow-frame generation in the compressed domain combined with DCT transform. In the watermark embedding phase, only partial decoding of MPEG-2 video and conversion between full DCT and block DCT are needed, and in the watermark extraction process, through the use of turbo codes, the BER can be reduced. On the basis of the in-depth analysis of video encoding formats under MPEG-2 standard, Li et al. [72] proposed a video watermarking algorithm based on DC coefficients. This algorithm also does not need to decode all the video data, and it does inverse DCT after the inverse quantization process. The watermark information is embedded into the last DC coefficient of the last macroblock of each slice in luminance component, which can solve the blocking artifacts. In a past paper [73], the watermark image was decomposed into eight binary images, and every image was embedded into different scenes of the video sequence. A suitable set of DCT coefficients partially decoded from compressed videos is found by combining with a visual mask based on local image features. The watermark is embedded by modifying these selected DCT coefficients, which can improve the image fidelity. In another past paper [74], a watermark system was designed from the architecture level combining with data compression, which has configurable spatial and frequency domain embedding and very large scale integrated circuit (VLSI) architecture. In yet another past paper [75], a new video watermarking method, based on empirical principal component analysis (PCA) decoding, was proposed. The intensity of embedding factors is determined according to the energy of high-frequency sub-bands and visual saliency. Decoding is performed through the comparison among elements of first principal component generated by empirical PCA, and the watermark is embedded in LL sub-bands adaptively.

MPEG-4 is a multimedia communication standard with a wide range of data rates established by MPEG in 1998. Its code rate covers a range of 5 kbit/s to 5 Mbit/s, and its aim is to support a variety of multimedia applications. Barni et al. [76] embedded the watermark into video objects by applying some predefined relationships between pairs of quantized DCT coefficients, which were in luminance blocks of pseudo-randomly selected macroblocks (MBs). Watermarks are equally embedded in intra and inter MBs, and the masking method is also used to limit the visual artifacts in watermarked video object planes (VOPs). Bian and Zhu [77] proposed a watermarking algorithm based on MPEG-4 fine granularity scalability (FGS) video codec, which embedded watermarks during the encoding process. The algorithm can eliminate the error propagation caused by watermark in normal video and use error propagation caused by watermark adjustment to protect video content. In a past paper [78], the embedding strength of the watermark was adjusted according to local image characteristics, and then the spatial spread spectrum watermark was directly embedded into the MPEG-4 bit stream by modifying DCT coefficients. In another past paper [79], the scene change detection was adopted to select key frames in the compressed domain, and local areas of these key frames were selected based on the extraction of feature points. On the basis of the Watson's perceptual model, the watermark embedding process is achieved adaptively. Gujjunoori and Amberker [80] proposed two watermark embedding schemes: Human visual system for achieving high visual quality (HVSVIS) and human visual system for achieving better embedding capacity (HVSCAP). The HVSVIS method embeds watermark information in middle-frequency DCT coefficients realizing high visual quality, and the HVSCAP method achieves higher embedding capacity by maintaining better visual quality. The summary comparison of several watermarking algorithms based on MPEG is shown in Table 9.

Table 9. Summary comparison of several watermarking algorithms based on MPEG.

Ref.	Type	Standard	Embedding Position
[71]	Blind	MPEG-2	AC coefficients of luminance component of shadow frames
[72]	Blind	MPEG-2	Last DC coefficient of the last macroblock of each slice in Y component
[73]	Blind	MPEG-2	DCT coefficients of luminance blocks decomposed from bit streams
[74]	Blind	MPEG-2	Spatial or frequency domain of Y-component
[75]	Blind	MPEG-2	LL sub-bands of I frames
[76]	Blind	MPEG-4	Luminance blocks of selected MBs
[78]	Blind	MPEG-4	DCT coefficients of luminance blocks of VOPs
[79]	Blind	MPEG-4	Local areas of I frames based on the extraction of feature points
[80]	Blind	MPEG-4	Middle-frequency DCT coefficients of Y-component of I frames

5.2. H.264-Based Watermarking Algorithms

H.264, which is also the 10th part of MPEG-4, is a highly compressed digital video codec standard proposed by the joint video team (JVT) composed of the international telecommunication union-telecommunication (ITU-T), video coding expert group (VCEG), and ISO/IEC & MPEG. It has a higher data compression ratio and higher video picture quality [81]. Compared to the MPEG standard, H.264 adopts some different technologies, like prediction technology, so many conventional video watermarking algorithms are no longer applicable. Most robust video watermarking algorithms based on H.264/AVC choose to embed watermarks into DCT coefficients [82–86]. For the VOD service, He et al. [82] proposed a real-time double watermarking algorithm. Through an effective error compensation mechanism and XOR mapping rules, copyright information and user information are embedded into I frame and P frame, respectively, as two watermarks. According to the characteristics of HVS, Zhang et al. [83] proposed a more accurate JND model to determine the watermark embedding strength by taking luminance masking, contrast masking, and spatial frequency sensitivity function all into account, and introduced it into video watermarking algorithm by the analysis of the energy distribution drift error. Buhari et al. [84] proposed a watermarking algorithm for spatial scalable video coding based on HVS, which embedded watermark information into high texture blocks of video streams. Gaj et al. [85] expanded the existing motion coherence region detection algorithm in the compression domain to detect moving objects in video shots, and embedded watermark information into them to resist geometric attacks. To achieve higher video visual quality and slight bit rate increase, Fallahpour et al. [86] embedded watermark information in the last nonzero level of quantized DCT (QDCT) blocks. In a past paper [87], the I_4 × 4 type of macroblocks (MBs) based on energy content were used to selectively distribute watermark rows to greatly improve the robustness against the video transcoding attack. Based on the newly proposed bit stream syntax elements in H.264 standard, Li et al. [88] embedded a watermark into the index of the reference frame during video encoding. A block modification technique based on optimization model is proposed, which can control robustness and video bit rate by manipulating two parameters. The summary comparison of several watermarking algorithms based on H.264 is shown in Table 10.

Table 10. Summary comparison of several H.264-based watermarking algorithms.

Ref.	Type	Watermark Preprocessing	Embedding Position
[82]	Blind	CDMA technique	Low-frequency DCT coefficients of Y component of I frames
[83]	Blind	Spread spectrum	Medium–high frequency DCT coefficients of I frames
[84]	Non-blind	Pseudorandom sequence	Highest energy coefficient in 4 × 4 luma intra-predicted blocks
[85]	Non-blind	DCT	DCT coefficients of motion coherent blocks in all frames
[86]	Blind	Encryption operation	High-frequency DCT coefficients of all frames
[87]	Blind	Random sequence	I_4 × 4 type of MBs of I frames
[88]	Blind	Pseudorandom sequence	Index of the reference frame

5.3. H.265-Based Watermarking Algorithms

H.265, also called HEVC, was officially approved by ITU-T and ISO/IEC in 2013. It is the successor of H.264/AVC, and has better compression performance. It can transmit higher quality network video with limited bandwidth, and only needs half of the original bandwidth to play a video with same quality [89]. With the development and wide application of HEVC, video watermarking algorithms based on HEVC have become a hot research topic. Gaj et al. [90] used the motion information of the inter prediction frame adjacent to I frame to obtain the motion characteristics of I frame. The watermark is embedded by modifying the number of nonzero transform coefficients (NNZ) difference of 4 × 4 luma blocks in consecutive intra prediction frames. Due to watermark embedding, drift error will occur. To eliminate the drift error, many related algorithms have been proposed one after another [91–96]. On the basis of a past paper [90], Gaj et al. [91] analyzed the intra prediction process of HEVC standard, and embedded the watermark into pixels that were not involved in the prediction process. In this way, the drift error caused by watermark embedding can be resisted. In another past paper [92], to avoid intra frame drift errors, the direction conditions of intra prediction were given first, and the information was embedded into multi-coefficients in luminance components of 4 × 4 DCT blocks of selected frames which can satisfy the condition. Based [92], Liu et al. gave three conditions of intra prediction direction and multi-coefficients in [93], and the message was embedded into multi-coefficients in luminance components of 4 × 4 discrete sine transform (DST) blocks of selected frames satisfying the specific condition. Cai et al. [94] selected 4 × 4 texture blocks in luma prediction unit (PU) for embedding based on the HVS. The watermark is adaptively embedded into quantized DST (QDST) coefficients in 4 × 4 luma PU using the sum invariability method. Chang et al. [95] proposed a first data hiding algorithm for HEVC intra-coded frames based on DCT/DST. The characteristics of block DCT and DST coefficients are explored to determine the positions of transform coefficients that can be perturbed and will not propagate errors to adjacent blocks. Elrowayati et al. [96] proposed a robust HEVC watermarking algorithm based on repetition-BCH syndrome code technology, which can not only resist distortion drift but also preserve the extracted watermark with good quality. The watermark is encoded by repetition-BCH code first, and then embedded into the quantized DCT/DST residual coefficients of transform units (TU) within the different size of TUs of I frames. After studying the spatiotemporal characteristics of the HEVC encoded video, Dutta and Gupta [97] embedded the watermark invisibly into low-frequency nonzero quantized AC coefficients in 4 × 4 blocks of I frames, which can minimize the synchronization error. In addition, a framework composed of public key and private key is presented to enhance the security. To obtain better perceptual quality, they embedded the watermark into P frames invisibly [98]. Based on the analysis of spatiotemporal characteristics of compressed video, suitable blocks for embedding can be located, which can further minimize the quality degradation and improve the robustness. Long et al. [99] proposed a separable reversible data hiding and encryption algorithm based on HEVC video. The signs and phases of the motion vector difference and the signs of residual coefficients are encrypted by the key generated by Rivest Cipher 4 (RC4), and the hiding key is used to embed the data into the nonzero AC residual coefficients. In a past paper [100], a HEVC-based watermarking algorithm with high payload was proposed, and the watermark was embedded into quantized transform coefficients (QTCs) during the encoding phase. Based on all phase biorthogonal transform (APBT) and SVD, Wang et al. [101] proposed a video watermarking algorithm against HEVC recompression. In the watermark preprocessing process, the watermark is compressed by APBT, which increases the embedding capacity by more than three times. Aiming at the HEVC coding process, Yang and Li [102] proposed an efficient information hiding algorithm based on motion vector space coding. The mapping relationship between the motion vector set and points in the motion vector space is defined first, and the secret information is embedded into the motion vectors of the smallest PUs in coding tree unit (CTU). Shanableh [103] proposed a new information embedding scheme based on modifying split decisions of HEVC video. At the encoding phase, the mapping relationship between split decisions of the coding unit (CU) and its characteristic variables is calculated to generate model weights that can be used to predict the split decisions, and then the message is embedded according to the prediction and real split decisions of each CU. The summary comparison of several watermarking algorithms based on H.265 is shown in Table 11.

Table 11. Summary comparison of several H.265-based watermarking algorithms.

Ref.	Type	Watermark Preprocessing	Embedding Position
[90]	Blind	-	NNZ difference of 4 × 4 luma TBs of intra-predicted frames
[91]	Blind	Pseudorandom sequence	4 × 4 luma TBs with high NNZ values in homogeneous regions of I frames
[92]	Blind	Encoding	Multi-coefficients of the 4 × 4 luminance DCT blocks of selected frames
[93]	Blind	Encoding	Multi-coefficients of the 4 × 4 luma DST blocks of selected frames
[94]	Blind	-	QDST coefficients in 4 × 4 luminance PU of I frames
[95]	Blind	-	QDCT and QDST coefficients of intra prediction residuals
[96]	Blind	BCH code	Residual QDCT or QDST coefficients within the different size of TUs of I frames
[97]	Blind	-	Low-frequency nonzero quantized AC coefficients in 4 × 4 blocks of I frames
[98]	Blind	-	Low-frequency nonzero quantized AC coefficients in 4 × 4 blocks of P frames
[99]	Blind	Exclusive OR operation	Nonzero AC residual coefficients
[100]	Blind	-	LSBs of selected nonzero of QTCs of I frames
[101]	Blind	Arnold transform and APBT	Nonzero coefficient blocks in luminance components with the size of 4 × 4, 8 × 8, and 16 × 16 of I frames
[102]	Blind	Binarization	Motion vectors of the smallest PUs in CTU

In addition, to help readers know the performance of compressed video-based algorithms involved in the paper quickly, Table 12 gives the quantitative comparison of invisibility, capacity, BIR, and robustness of several typical algorithms in compressed domain. In Table 12, the numbers in "( )" indicate the parameters of attacks and "-" shows that the attack is not mentioned in the reference. The reason may be that the algorithm cannot resist the attack, or the authors have not considered it. The full names of several typical attacks corresponding to the abbreviations mentioned in Table 12 are given in Table 1.

Table 12. Quantitative comparison of invisibility, capacity, BIR, and robustness of several typical algorithms in compressed domain.

Ref.			[75]	[83]	[85]	[88]	[91]	[97]	[98]
PSNR (dB)			50.89	36.33	[25, 44]	[32, 42]	[32, 50]	[30, 35]	[40, 44]
Capacity (bit)			2080	1317	-	1680	100 bits/I frame	-	-
BIR (%)			-	≤1.26	≤2.90	≤6.48	≤2.08	≤0.27	≤0.14
Standard			MPEG-2	MPEG-4	H.264	H.264	H.265	H.265	H.265
Robustness			BER	BER	NC	BER	NC	BER	BER
ATTACKS	GF (5 × 5)		-	0.008	0.603	0.070	0.848	0.157	-
	GN (0.001)		≤0.197	(0.005) 0.038	-	0.060	0.763	0.017	0.131
	SPN	(0.01) (0.02)	-	0.038 -	0.61 0.49	-	0.877 0.774	(0.001) 0.015	(0.001) 0.106
	Rec		-	0.006	-	0.044	0.812	0.074	0.070
	Other attacks the algorithm can resist		MF, FS, FA, FI, MPEG-2, and H.264	-	MF, Rtt, and Scl	LM, Blu, Shp, and H.264	Scl, CE, FA, FD, and H.264	AF, H.264, and H.265	AF, H.264, and H.265

At present, the research on watermarking algorithms based on original videos is relatively mature, and the research focus is on the video watermarking algorithm based on HEVC coding standard. In summary, the research status of robust video watermarking algorithms for copyright protection is shown in Figure 8.

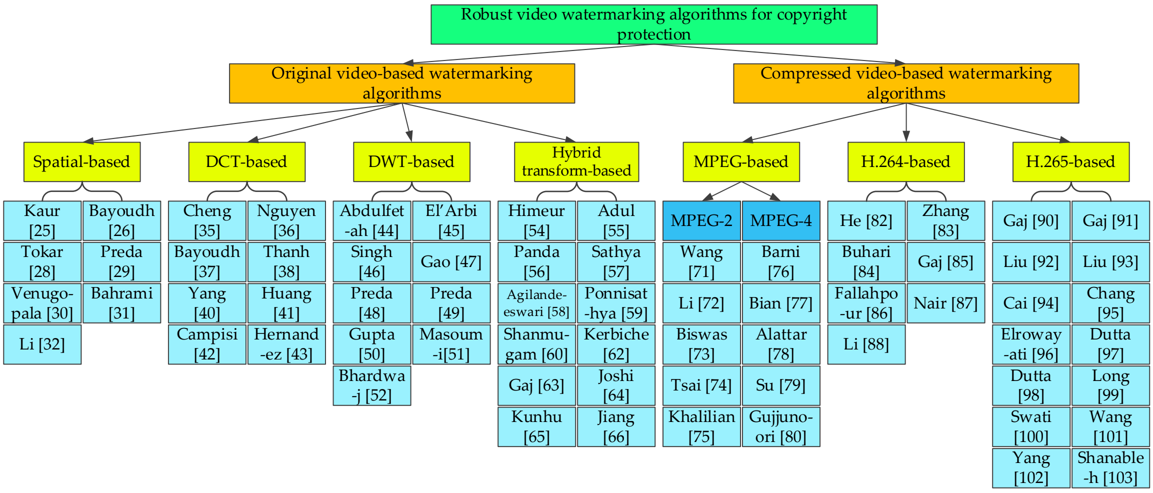

Figure 8. The research status of robust video watermarking algorithms for copyright protection.

6. Conclusions and Outlook

6.1. Conclusions

In recent years, many review papers on video watermarking have been published. Some provide overviews of video watermarking algorithms for specific applications or video watermarking algorithms in specific domains [104,105]. The workload of these papers is less than that of our paper. Others are reviews of various types of video watermarking algorithms for different applications, like the study of Asikuzzaman and Pickering [106]. Additionally, many image watermarking algorithms and 3D video watermarking algorithms have also been reviewed previously [106]. There are few targeted review papers that focus solely on robust video watermarking algorithms for copyright protection in recent years, so we wrote this paper. The basic models and properties of video watermarking algorithms are introduced first, and the evaluation indexes corresponding to each property are described. Robust video watermarking algorithms for copyright protection are summarized and divided into two categories: original video-based watermarking algorithms and compressed video-based watermarking algorithms. Original video-based watermarking algorithms are subdivided into watermarking algorithms in the spatial domain and transform domain; and compressed video-based watermarking algorithms are subdivided into watermarking algorithms based on MPEG-2, MPEG-4, H.264, and H.265. The basic information and quantitative estimation results of the performance of some typical algorithms are analyzed and compared. Through Tables 2–12, researchers can easily understand and grasp the embedding methods and performance of these typical algorithms involved in the paper so as to carry out more in-depth research and innovation.

6.2. Challenges and Outlook

Although many robust video watermarking algorithms have been proposed, the research on robust video watermarking algorithms still faces many challenges, which include the tradeoff between watermark capacity, invisibility, and robustness; combining with video coding standards; random detection, that is, the watermark can be detected in a small segment of video sequences at any position in the video; how to reduce the computational complexity; high real-time performance to ensure the smoothness of the video data stream, etc. Therefore, how to balance the relationship between invisibility and robustness while improving the watermark capacity and security is still the ongoing focus of researchers. Due to the high complexity of HEVC, the number of researches on the video watermarking algorithm based on HEVC is relatively low at present. Future watermarking algorithms in the compressed domain will realize watermark embedding based on in-depth analysis of the characteristics of the HEVC encoding process. Various fast algorithms and parallel algorithms will be developed and introduced into the video watermarking algorithms to shorten the operation time and meet real-time requirements. In addition, artificial intelligence schemes, like neural networks, may be introduced into video watermarking algorithms to select blocks that are more suitable for watermark embedding. What is more, H.266, also known as versatile video coding (VVC), has started the standardization process officially on 10 April 2018, and is expected to achieve formulation and publication of the standard by 2020. With the promulgation of H.266/VVC standard, robust video watermarking algorithms based on H.266 will also become the focus of researchers.

Author Contributions: X.Y. and C.W. reviewed robust video watermarking algorithms in recent years; X.Y. and X.Z. classified the involved algorithms and analyzed the data; X.Y. and C.W. drafted the manuscript; X.Y. and X.Z. revised the manuscript.

Funding: This work was funded by the National Natural Science Foundation of China (No. 61702303) and the Shandong Provincial Natural Science Foundation, China (No. ZR2017MF020).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Eldering, C.A.; Sylla, M.L.; Eisenach, J.A. Is there a Moore's law for bandwidth? *IEEE Commun. Mag.* **1999**, *37*, 117–121. [CrossRef]
2. Wolfgang, R.B.; Podilchuk, C.I.; Delp, E.J. Perceptual watermarks for digital images and video. *Proc. IEEE* **1999**, *87*, 1108–1126. [CrossRef]
3. Lempel, A. Cryptology in transition. *Comput. Surv.* **1979**, *11*, 285–303. [CrossRef]
4. Jung, K.H. A survey of reversible data hiding methods in dual images. *IETE Tech. Rev.* **2016**, *33*, 441–452. [CrossRef]
5. Carpentieri, B.; Castiglione, A.; De Santis, A.; Palmieri, F.; Pizzolante, R. One-pass lossless data hiding and compression of remote sensing data. *Future Gener. Comput. Syst.* **2019**, *90*, 222–239. [CrossRef]
6. Parah, S.A.; Sheikh, J.A.; Akhoon, J.A.; Loan, N.A.; Bhat, G.M. Information hiding in edges: A high capacity information hiding technique using hybrid edge detection. *Multimedia Tools Appl.* **2018**, *77*, 185–207. [CrossRef]
7. Atawneh, S.; Almomani, A.; Sumari, P. Steganography in digital images: Common approaches and tools. *IETE Tech. Rev.* **2013**, *30*, 344–358. [CrossRef]

8. Van Schyndel, R.G.; Tirkel, A.Z.; Osborne, C.F. A digital watermark. In Proceedings of the 1st IEEE International Conference on Image Processing, Austin, TX, USA, 13–16 November 1994.
9. Zhang, H.X.; Zhang, Z.Y.; Qiu, P.L. A novel algorithm of covert communication. *Acta Electron. Sin.* **2003**, *31*, 514–517.
10. Doërr, G.; Dugelay, J.L. A guide tour of video watermarking. *Signal Process. Image Commun.* **2003**, *18*, 263–282. [CrossRef]
11. Lu, C.S.; Liao, H.Y.M. Multipurpose watermarking for image authentication and protection. *IEEE Trans. Image Process.* **2001**, *10*, 1579–1592. [PubMed]
12. Verma, V.S.; Jha, R.K. An overview of robust digital image watermarking. *IETE Tech. Rev.* **2015**, *32*, 479–496. [CrossRef]
13. Devi, B.P.; Singh, K.M.; Roy, S. New copyright protection scheme for digital images based on visual cryptography. *IETE J. Res.* **2017**, *63*, 870–880. [CrossRef]
14. Channapragada, R.S.R.; Prasad, M.V.N.K. Digital watermarking based on magic square and Ridgelet transform techniques. *Adv. Intell. Syst. Comput.* **2014**, *243*, 143–161.
15. Liu, R. An improved Logistic chaotic map and self-adaptive model for image encryption. *J. Comput. Methods Sci. Eng.* **2016**, *16*, 287–301. [CrossRef]
16. Biswas, S.N.; Nahar, S.; Das, S.R.; Petriu, E.M.; Assaf, M.H.; Groza, V. MPEG-2 digital video watermarking technique. In Proceedings of the International Instrumentation and Measurement Technology Conference, Graz, Austria, 13–16 May 2012.
17. Wang, C.Y.; Zhang, Y.P.; Zhou, X. Review on digital image watermarking based on singular value decomposition. *J. Inf. Process. Syst.* **2017**, *13*, 1585–1601.
18. Zheng, X.S.; Zhao, Y.L.; Li, N. Classification model and enhancement of robustness in video digital watermark. In Proceedings of the Chinese Control and Decision Conference, Yantai, China, 2–4 July 2008.
19. Li, Z.H.; Zhang, Z.Z.; Guo, S.; Wang, J.W. Video inter-frame forgery identification based on the consistency of quotient of MSSIM. *Secur. Commun. Netw.* **2016**, *9*, 4548–4556. [CrossRef]
20. Wang, C.Y.; Zhang, Y.P.; Zhou, X. Robust image watermarking algorithm based on ASIFT against geometric attacks. *Appl. Sci.* **2018**, *8*, 410. [CrossRef]
21. Hu, H.T.; Hsu, L.Y. Exploring DWT-SVD-DCT feature parameters for robust multiple watermarking against JPEG and JPEG2000 compression. *Comput. Electr. Eng.* **2015**, *41*, 52–63. [CrossRef]
22. Lei, B.Y.; Tan, E.L.; Chen, S.P.; Ni, D.; Wang, T.F.; Lei, H.J. Reversible watermarking scheme for medical image based on differential evolution. *Expert Syst. Appl.* **2014**, *41*, 3178–3188. [CrossRef]
23. Jindal, S.; Goel, S.; Puri, T.; Bhardwaj, A.; Mahant, I.; Singh, S.; Sood, D. Performance analysis of LSB based watermarking for optimization of PSNR and MSE. *Int. J. Secur. Its Appl.* **2016**, *10*, 345–350. [CrossRef]
24. Cox, I.J.; Kilian, J.; Leighton, F.T.; Shamoon, T. Secure spread spectrum watermarking for multimedia. *IEEE Trans. Image Process.* **1997**, *6*, 1673–1687. [CrossRef] [PubMed]
25. Kaur, H.; Kaur, E.V. Invisible video multiple watermarking using optimized techniques. In Proceedings of the Online International Conference on Green Engineering and Technologies, Coimbatore, India, 19 November 2016.
26. Bayoudh, I.; Jabra, S.B.; Zagrouba, E. Online multi-sprites based video watermarking robust to collusion and transcoding attacks for emerging applications. *Multimedia Tools Appl.* **2017**, *77*, 14361–14379. [CrossRef]
27. Masoumi, M.; Rezaei, M.; Hamza, A.B. A blind spatio-temporal data hiding for video ownership verification in frequency domain. *AEU-Int. J. Electron. Commun.* **2015**, *69*, 1868–1879. [CrossRef]
28. Tokar, T.; Kanocz, T.; Levicky, D. Digital watermarking of uncompressed video in spatial domain. In Proceedings of the 19th International Conference Radioelektronika, Bratislava, Slovakia, 22–23 April 2009.
29. Preda, R.O.; Vizireanu, N. New robust watermarking scheme for video copyright protection in the spatial domain. *UPB Sci. Bull.* **2011**, *73*, 93–104.
30. Venugopala, P.S.; Sarojadevi, H.; Chiplunkar, N.N.; Bhat, V. Video watermarking by adjusting the pixel values and using scene change detection. In Proceedings of the 5th International Conference on Signal and Image Processing, Bangalore, India, 8–10 January 2014.
31. Bahrami, Z.; Tab, F.A. A new robust video watermarking algorithm based on SURF features and block classification. *Multimedia Tools Appl.* **2018**, *77*, 327–345. [CrossRef]

32. Li, X.; Wang, X.J.; Yang, W.M.; Wang, X. A robust video watermarking scheme to scalable recompression and transcoding. In Proceedings of the International Conference on Electronics Information and Emergency Communication, Beijing, China, 17–19 June 2016.
33. Li, J.F.; Sui, A.N. A digital video watermarking algorithm based on DCT domain. In Proceedings of the 5th International Joint Conference on Computational Sciences and Optimization, Harbin, China, 23–26 June 2012.
34. Liu, G.Q.; Zheng, X.S.; Zhao, Y.L.; Li, N. A robust digital video watermark algorithm based on DCT domain. In Proceedings of the International Conference on Computer Application and System Modeling, Taiyuan, China, 22–24 October 2010.
35. Cheng, M.Z.; Xi, M.C.; Yuan, K.G.; Wu, C.H.; Lei, M. Recoverable video watermark in DCT domain. *J. Comput.* **2013**, *8*, 533–538. [CrossRef]
36. Nguyen, T.T.; Duan, D.N. A robust blind video watermarking in DCT domain using even-odd quantization technique. In Proceedings of the International Conference on Advanced Technologies for Communications, Ho Chi Minh City, Vietnam, 14–16 October 2015.
37. Bayoudh, I.; Jabra, S.B.; Zagrouba, E. A robust video watermarking for real-time application. In Proceedings of the 18th International Conference on Advanced Concepts for Intelligent Vision Systems, Antwerp, Belgium, 18–21 September 2017.
38. Thanh, T.M.; Hiep, P.T.; Tam, T.M.; Tanaka, K. Robust semi-blind video watermarking based on frame-patch matching. *AEU-Int. J. Electron. Commun.* **2014**, *68*, 1007–1015. [CrossRef]
39. Chen, B.; Wornell, G.W. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. *IEEE Trans. Inf. Theory* **2001**, *47*, 1423–1443. [CrossRef]
40. Yang, C.H.; Huang, H.Y.; Hsu, W.H. An adaptive video watermarking technique based on DCT domain. In Proceedings of the 8th International Conference on Computer and Information Technology, Sydney, Australia, 8–11 July 2008.
41. Huang, H.Y.; Yang, C.H.; Hsu, W.H. A video watermarking technique based on pseudo-3D DCT and quantization index modulation. *IEEE Trans. Inf. Forensics Secur.* **2010**, *5*, 625–637. [CrossRef]
42. Campisi, P.; Neri, A. 3D-DCT video watermarking using quantization-based methods. In Proceedings of the 15th European Signal Processing Conference, Poznan, Poland, 3–7 September 2007.
43. Cedillo-Hernandez, A.; Cedillo-Hernandez, M.; Miyatake, M.N.; Meana, H.P. A spatiotemporal saliency-modulated JND profile applied to video watermarking. *J. Vis. Commun. Image Represent.* **2018**, *52*, 106–117. [CrossRef]
44. Abdulfetah, A.A.; Sun, X.; Yang, H. Robust adaptive video watermarking scheme using visual models in DWT domain. *Inf. Technol. J.* **2010**, *9*, 1409–1414. [CrossRef]
45. El'Arbi, M.; Koubaa, M.; Charfeddine, M.; Amar, C.B. A dynamic video watermarking algorithm in fast motion areas in the wavelet domain. *Multimedia Tools Appl.* **2011**, *55*, 579–600. [CrossRef]
46. Singh, K.M. A robust rotation resilient video watermarking scheme based on the SIFT. *Multimedia Tools Appl.* **2018**, *77*, 16419–16444. [CrossRef]
47. Gao, Q.; Li, Z.; Chen, S.Q. A video dual watermarking algorithm against geometric attack based on integer wavelet and SIFT. In Proceedings of the International Conference on Cryptography, Security and Privacy, Wuhan, China, 17–19 March 2017.
48. Preda, R.O.; Vizireanu, D.N. A robust digital watermarking scheme for video copyright protection in the wavelet domain. *Measurement* **2010**, *43*, 1720–1726. [CrossRef]
49. Preda, R.O.; Vizireanu, D.N. Robust wavelet-based video watermarking scheme for copyright protection using the human visual system. *J. Electron. Imaging* **2011**, *20*, 146–152. [CrossRef]
50. Gupta, G.; Gupta, V.K.; Chandra, M. An efficient video watermarking based security model. *Microsyst. Technol.* **2018**, *24*, 2539–2548. [CrossRef]
51. Masoumi, M.; Amiri, S. A blind scene-based watermarking for video copyright protection. *AEU-Int. J. Electron. Commun.* **2013**, *67*, 528–535. [CrossRef]
52. Bhardwaj, A.; Verma, V.S.; Jha, R.K. Robust video watermarking using significant frame selection based on coefficient difference of lifting wavelet transform. *Multimedia Tools Appl.* **2018**, *77*, 19659–19678. [CrossRef]
53. Kerbiche, A.; Jabra, S.B.; Zagrouba, E.; Charvillat, V. Robust video watermarking approach based on crowdsourcing and hybrid insertion. In Proceedings of the International Conference on Digital Image Computing: Techniques and Applications, Sydney, Australia, 29 November–1 December 2017.

54. Himeur, Y.; Boukabou, A. A robust and secure key-frames based video watermarking system using chaotic encryption. *Multimedia Tools Appl.* **2018**, *77*, 8603–8627. [CrossRef]
55. Adul, V.; Mwangi, E. A robust video watermarking approach based on a hybrid SVD/DWT technique. In Proceedings of the IEEE AFRICON: Science, Technology and Innovation for Africa, Cape Town, South Africa, 18–20 September 2017.
56. Panda, J.; Garg, P. An efficient video watermarking approach using scene change detection. In Proceedings of the India International Conference on Information Processing, Delhi, India, 12–14 August 2016.
57. Sathya, S.P.A.; Ramakrishnan, S. Fibonacci based key frame selection and scrambling for video watermarking in DWT-SVD domain. *Wirel. Pers. Commun.* **2018**, *102*, 2011–2031. [CrossRef]
58. Agilandeeswari, L.; Ganesan, K. A robust color video watermarking scheme based on hybrid embedding techniques. *Multimedia Tools Appl.* **2016**, *75*, 8745–8780. [CrossRef]
59. Ponnisathya, S.; Ramakrishnan, S.; Dhinakaran, S.; Sabari, A.P.; Dhamodharan, P. Chaotic map based video watermarking using DWT and SVD. In Proceedings of the International Conference on Inventive Communication and Computational Technologies, Coimbatore, India, 10–11 March 2017.
60. Shanmugam, M.; Chokkalingam, A. Performance analysis of 2 level DWT-SVD based non blind and blind video watermarking using range conversion method. *Microsyst. Technol.* **2018**, 1–9. [CrossRef]
61. Zhang, X.P.; Li, K. Comments on "An SVD-based watermarking scheme for protecting rightful Ownership". *IEEE Trans. Multimedia* **2005**, *9*, 421–423.
62. Kerbiche, A.; Jabra, S.B.; Zagrouba, E.; Charvillat, V. A robust video watermarking based on feature regions and crowdsourcing. *Multimedia Tools Appl.* **2018**, *77*, 26769–26791. [CrossRef]
63. Gaj, S.; Rathore, A.K.; Sur, A.; Bora, P.K. A robust watermarking scheme against frame blending and projection attacks. *Multimedia Tools Appl.* **2017**, *76*, 20755–20779. [CrossRef]
64. Joshi, A.M.; Gupta, S.; Girdhar, M.; Agarwal, P.; Sarker, R. Combined DWT-DCT-based video watermarking algorithm using Arnold transform technique. In Proceedings of the International Conference on Data Engineering and Communication Technology, Lavasa City, India, 10–11 March 2016.
65. Kunhu, A.; Nisi, K.; Sabnam, S.; Majida, A.; Al-Mansoori, S. Index mapping based hybrid DWT-DCT watermarking technique for copyright protection of videos files. In Proceedings of the Online International Conference on Green Engineering and Technologies, Coimbatore, India, 19 November 2016.
66. Jiang, D.Y.; Li, D.; Kim, J.W. A spread spectrum zero video watermarking scheme based on dual transform domains and log-polar transformation. *Int. J. Multimedia Ubiquitous Eng.* **2015**, *10*, 367–378. [CrossRef]
67. Gall, D.L. MPEG: A video compression standard for multimedia applications. *Commun. ACM* **1991**, *34*, 46–58. [CrossRef]
68. Luthra, A.; Sullivan, G.J.; Wiegand, T. Introduction to the special issue on the H.264/AVC video coding standard. *IEEE Trans. Circuits Syst. Video Technol.* **2003**, *13*, 557–559. [CrossRef]
69. Pan, Z.Q.; Lei, J.J.; Zhang, Y.; Sun, X.M.; Kwong, S. Fast motion estimation based on content property for low-complexity H.265/HEVC encoder. *IEEE Trans. Broadcast.* **2016**, *62*, 675–684. [CrossRef]
70. Frossard, P.; Verscheure, O. AMISP: A complete content-based MPEG-2 error-resilient scheme. *IEEE Trans. Circuits Syst. Video Technol.* **2001**, *11*, 989–998. [CrossRef]
71. Wang, Y.; Pearmain, A. Blind MPEG-2 video watermarking in DCT domain robust against scaling. *IEE Proc. Vis. Image Signal Process.* **2006**, *153*, 581–588. [CrossRef]
72. Li, J.F.; Wang, Y.B.; Dong, S.S. Video watermarking algorithm based DC coefficient. In Proceedings of the 2nd International Conference on Image, Vision and Computing, Chengdu, China, 2–4 June 2017.
73. Biswas, S.; Das, S.R.; Petriu, E.M. An adaptive compressed MPEG-2 video watermarking scheme. *IEEE Trans. Instrum. Meas.* **2005**, *54*, 1853–1861. [CrossRef]
74. Tsai, T.H.; Wu, C.Y.; Fang, C.L. Design and implementation of a joint data compression and digital watermarking system in an MPEG-2 video encoder. *J. Signal Process. Syst.* **2014**, *74*, 203–220. [CrossRef]
75. Khalilian, H.; Bajic, I.V. Video watermarking with empirical PCA-based decoding. *IEEE Trans. Image Process.* **2013**, *22*, 4825–4840. [CrossRef] [PubMed]
76. Barni, M.; Bartolini, F.; Checcacci, N. Watermarking of MPEG-4 video objects. *IEEE Trans. Multimedia* **2005**, *7*, 23–32. [CrossRef]
77. Bian, X.B.; Zhu, Q.X. Video protection for MPEG-4 FGS with watermarking. *Multimedia Tools Appl.* **2008**, *40*, 61–87. [CrossRef]

78. Alattar, A.M.; Lin, E.T.; Celik, M.U. Digital watermarking of low bit-rate advanced simple profile MPEG-4 compressed video. *IEEE Trans. Circuits Syst. Video Technol.* **2003**, *13*, 787–800. [CrossRef]
79. Su, P.C.; Kuo, T.Y.; Li, M.H. A practical design of digital watermarking for video streaming services. *J. Vis. Commun. Image Represent.* **2017**, *42*, 161–172. [CrossRef]
80. Gujjunoori, S.; Amberker, B.B. DCT based reversible data embedding for MPEG-4 video using HVS characteristics. *J. Inf. Secur. Appl.* **2013**, *18*, 157–166. [CrossRef]
81. Joshi, A.M.; Mishra, V.; Patrikar, R.M. Design of real-time video watermarking based on Integer DCT for H.264 encoder. *Int. J. Electron.* **2015**, *102*, 141–155. [CrossRef]
82. He, Y.L.; Yang, G.B.; Zhu, N.B. A real-time dual watermarking algorithm of H.264/AVC video stream for video-on-demand service. *AEU-Int. J. Electron. Commun.* **2012**, *66*, 305–312. [CrossRef]
83. Zhang, W.W.; Li, X.; Zhang, Y.Z.; Zhang, R.; Zheng, L.X. Robust video watermarking algorithm for H.264/AVC based on JND model. *KSII Trans. Internet Inf. Syst.* **2017**, *11*, 2741–2761.
84. Buhari, A.M.; Ling, H.C.; Baskaran, V.M.; Wong, K. Fast watermarking scheme for real-time spatial scalable video coding. *Signal Process. Image Commun.* **2016**, *47*, 86–95. [CrossRef]
85. Gaj, S.; Patel, A.S.; Sur, A. Object based watermarking for H.264/AVC video resistant to RST attacks. *Multimedia Tools Appl.* **2016**, *75*, 3053–3080. [CrossRef]
86. Fallahpour, M.; Shirmohammadi, S.; Ghanbari, M. A high capacity data hiding algorithm for H.264/AVC video. *Secur. Commun. Netw.* **2015**, *8*, 2947–2955. [CrossRef]
87. Nair, R.; Varadharajan, V.; Joglekar, S.; Nallusamy, R.; Paul, S. Robust transcoding resistant watermarking for H.264 standard. *Multimedia Tools Appl.* **2014**, *73*, 763–778. [CrossRef]
88. Li, J.; Liu, H.M.; Huang, J.W.; Shi, Y.Q. Reference index-based H.264 video watermarking scheme. *ACM Trans. Multimedia Comput. Commun. Appl.* **2012**, *8*, 33. [CrossRef]
89. Mohammed, A.A.; Ali, N.A. Robust video watermarking scheme using high efficiency video coding attack. *Multimedia Tools Appl.* **2018**, *77*, 2791–2806. [CrossRef]
90. Gaj, S.; Sur, A.; Bora, P.K. A robust watermarking scheme against re-compression attack for H.265/HEVC. In Proceedings of the 5th National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics, Patna, India, 16–19 December 2015.
91. Gaj, S.; Kanetkar, A.; Sur, A.; Bora, P.K. Drift-compensated robust watermarking algorithm for H.265/HEVC video stream. *ACM Trans. Multimedia Comput. Commun. Appl.* **2017**, *13*, 11. [CrossRef]
92. Liu, Y.X.; Liu, S.Y.; Zhao, H.G.; Liu, S.; Feng, C. A data hiding method for H. In 265 without intra-frame distortion drift. In Proceedings of the 13th International Conference on Intelligent Computing, Liverpool, UK, 7–10 August 2017.
93. Liu, Y.X.; Liu, S.Y.; Zhao, H.G.; Liu, S. A new data hiding method for H.265/HEVC video streams without intra-frame distortion drift. *Multimedia Tools Appl.* **2018**. [CrossRef]
94. Cai, C.T.; Feng, G.; Wang, C.; Han, X. A reversible watermarking algorithm for high efficiency video coding. In Proceedings of the 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics, Shanghai, China, 14–16 October 2017.
95. Chang, P.C.; Chung, K.L.; Chen, J.J.; Lin, C.H.; Lin, T.J. A DCT/DST-based error propagation-free data hiding algorithm for HEVC intra-coded frames. *J. Vis. Commun. Image Represent.* **2014**, *25*, 239–253. [CrossRef]
96. Elrowayati, A.A.; Abdullah, M.F.L.; Manaf, A.A.; Alfagi, A.S. Robust HEVC video watermarking scheme based on repetition-BCH syndrome code. *Int. J. Softw. Eng. Its Appl.* **2016**, *10*, 263–270. [CrossRef]
97. Dutta, T.; Gupta, H.P. A robust watermarking framework for high efficiency video coding (HEVC)—Encoded video with blind extraction process. *J. Vis. Commun. Image Represent.* **2016**, *38*, 29–44. [CrossRef]
98. Dutta, T.; Gupta, H.P. An efficient framework for compressed domain watermarking in P frames of high-efficiency video coding (HEVC)—Encoded video. *ACM Trans. Multimedia Comput. Commun. Appl.* **2017**, *13*, 12. [CrossRef]
99. Long, M.; Peng, F.; Li, H.Y. Separable reversible data hiding and encryption for HEVC video. *J. Real-Time Image Process.* **2018**, *14*, 171–182. [CrossRef]
100. Swati, S.; Hayat, K.; Shahid, Z. A watermarking scheme for high efficiency video coding (HEVC). *PLoS ONE* **2014**, *9*, e105613. [CrossRef] [PubMed]
101. Wang, C.Y.; Shan, R.Y.; Zhou, X. Anti-HEVC recompression video watermarking algorithm based on the all phase biorthogonal transform and SVD. *IETE Tech. Rev.* **2018**, *35*, 1–17. [CrossRef]

102. Yang, J.; Li, S.B. An efficient information hiding method based on motion vector space encoding for HEVC. *Multimedia Tools Appl.* **2018**, *77*, 11979–12001. [CrossRef]
103. Shanableh, T. Altering split decisions of coding units for message embedding in HEVC. *Multimedia Tools Appl.* **2018**, *77*, 8939–8953. [CrossRef]
104. Sujatha, P.; Devi, R. A glance of digital watermarking techniques with an evaluation of Haar and Daubechies wavelet. *Int. J. Appl. Eng. Res.* **2017**, *9*, 9652–9657.
105. Tew, Y.; Wong, K. An overview of information hiding in H.264/AVC compressed video. *IEEE Trans. Circuits Syst. Video Technol.* **2014**, *24*, 305–319. [CrossRef]
106. Asikuzzaman, M.; Pickering, M.R. An overview of digital video watermarking. *IEEE Trans. Circuits Syst. Video Technol.* **2018**, *28*, 2131–2153. [CrossRef]