An Overview of Digital Video Watermarking

Md. Asikuzzaman, *Member, IEEE*, and Mark R. Pickering, *Member, IEEE*

***Abstract*— The illegal distribution of a digital movie is a common and significant threat to the film industry. With the advent of high-speed broadband Internet access, a pirated copy of a digital video can now be easily distributed to a global audience. A possible means of limiting this type of digital theft is digital video watermarking whereby additional information, called a watermark, is embedded in the host video. This watermark can be extracted at the decoder and used to determine whether the video content is watermarked. This paper presents a review of the digital video watermarking techniques in which their applications, challenges, and important properties are discussed, and categorizes them based on the domain in which they embed the watermark. It then provides an overview of a few emerging innovative solutions using watermarks. Protecting a 3D video by watermarking is an emerging area of research. The relevant 3D video watermarking techniques in the literature are classified based on the image-based representations of a 3D video in stereoscopic, depth-image-based rendering, and multi-view video watermarking. We discuss each technique, and then present a survey of the literature. Finally, we provide a summary of this paper and propose some future research directions.**

***Index Terms*— Watermarking, robustness, geometric attack, depth-image-based rendering (DIBR), multi-view video.**

I. Introduction

VIDEO piracy is the act of acquiring, copying and then selling or distributing a copyrighted video without the consent of the copyright owner. Over the last decade, online video piracy has become a significant concern for studios and movie producers. With the availability of high-speed broadband access and a multitude of Internet streaming sites, a pirated copy is readily accessible to a global audience for viewing online and downloading within just days of its release to theaters. A block diagram illustrating the unauthorized distribution of a copyrighted video is shown in Fig. 1. Usually, a movie is first released to theaters and then to digital versatile disk (DVD) after approximately sixteen weeks [1]. Currently, camcorder theft is one of the most significant problems facing the film industry and is the single largest source of video piracy [2].

When this type of theft occurs, a copy of a digital movie is captured from a large-screen movie theater using a camcorder and then distributed worldwide via the Internet without any copyright protection. Approximately 90 percent of the first available versions of illegally distributed new release films are pirated in this way [2]. Although there are strict laws in many countries against camcording, they have proven to be ineffective and it has not been possible to prevent this practice. An example of the severity of this criminal activity is that more than seven million illegal copies of the Batman movie "The Dark Knight" were downloaded in the first six months following its release despite a thoroughly planned anti-piracy campaign run by the Warner Brothers studio [3].

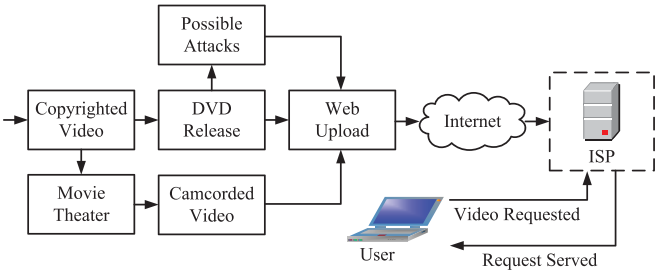


Fig. 1. Illegal distribution of a copyrighted video.

An unauthorized user may also create an illegal copy of a movie from a DVD and distribute it through a web server while a pirate may perform different types of intentional and unintentional attacks before uploading a movie to the Internet. Video piracy not only harms the film industry by causing losses of revenue for production houses but its effect reverberates throughout the global economy and results in losses of jobs and businesses. One study indicated that, in the twelve months to July 2010, the Australian economy lost more than $1.37 billion in revenue as a result of movie theft [4]. Therefore, concern over protecting the copyright of digital video content is increasing [5]–[7].

Several techniques designed to protect video content from unauthorized access include cryptography, steganography and watermarking. Cryptography, which means "secret writing", comes from the Greek words *kryptós* for "hidden or secret" and *graphein* for "writing". It involves processes of communication where a message, called *plaintext*, is scrambled into *ciphertext* using a specific key which is then required to retrieve the message. The processes of scrambling and unscrambling the message using this key are called encryption and decryption respectively. The purpose of encryption is to make data unintelligible to unauthorized persons during its transmission from a sender to receiver. However, once the data is decrypted at the receiver's end, it is no longer protected from unauthorized distribution.

Steganography is derived from the Greek words *steganos* and *graphein* meaning "covered, concealed or protected" and

Manuscript received November 30, 2016; revised March 2, 2017 and May 9, 2017; accepted May 28, 2017. Date of publication June 5, 2017; date of current version September 13, 2018. This paper was recommended by Associate Editor P. Comesana-Alfaro. *(Corresponding author: Md. Asikuzzaman.)*

The authors are with the School of Engineering and Information Technology, The University of New South Wales, Canberra, ACT 2600, Australia (e-mail: m.asikuzzaman@adfa.edu.au; m.pickering@adfa.edu.au).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCSVT.2017.2712162

(a) (b)

Fig. 2. Illustration of steganography: (a) image of a tree with a steganographically hidden image and (b) image of a cat extracted from (a).

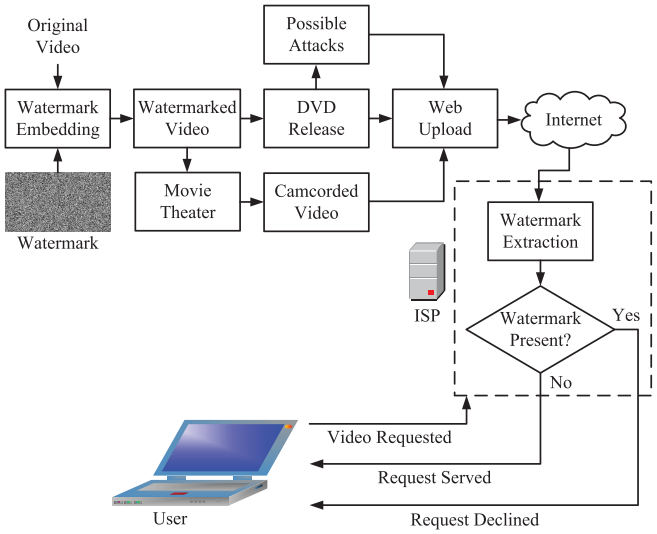


Fig. 3. Diagram of a generic digital video watermarking system for protecting illegal distribution of a video content.

"writing" respectively, and is the art of concealing a message in other data to prevent its detection. A visual example of steganography is provided in Fig. 2 [8] which shows an image of a tree with a steganographically hidden image of a cat (Fig. 2(a)) that is extracted by removing all but the two least significant bits (LSBs) of each color component and subsequently applying normalization (Fig. 2(b)).

Watermarking, which also contains a secret message within the host data, is a particular form of data hiding with a different purpose than steganography. It is the process of marking different types of digital data, such as text, audio, images, video or 3D models, to claim ownership of their copyright. It embeds information, which can be a company logo, image or any particular kind of content, in the host data. The embedded information can be either visible or invisible depending on the type of application while it must be perceptually invisible in steganography. In the case of watermarking, it must be statistically detectable when the secret key used for embedding is known, but it can be statistically detectable or undetectable when such a key is unknown. On the other hand, it must be statistically undetectable in steganography, although it is not the requirement in watermarking when the key is not known. Therefore, steganography is a particular case of watermarking, where the statistically undetectability constraint is considered. Of particular note is the fact that a watermarking system must be robust to intentional attacks aimed at removing the hidden message whereas robustness is typically not required for a steganographic system [9]. A watermarking system consisting of an encoder and decoder is shown in Fig. 3. Before the release of a movie, a watermark is embedded in the video content, with illegal contents able to be protected by a watermark-decoding filter being provided to an Internet Service Provider (ISP). Then, when a user requests that a video be downloaded from the server, the ISP can filter it to check for the presence of a watermark. The presence of a watermark indicates that the request to download the movie should be cancelled.

As the popularity of 3D videos is increasing daily due to the availability of low-cost 3DTVs, not only 2D but also 3D video content can be distributed illegally without any copyright protection. 3D data are usually distributed in image-based representations, not only as a 3D video but also individually as 2D content. Therefore, protecting these views from unauthorized distribution is becoming very important.

In the literature, many different watermarking techniques have been proposed and overviews of these techniques are provided in many papers, each focusing on a specific component. For example, Podilchuk and Delp [10] reviewed the algorithms described in the literature based on the applications, technology and system requirements of different media types, such as digital images, video, audio and text. Langelaar *et al.* [11] provided a state-of-the-art overview for digital image and video data while video watermarking as an extension of the watermarking of still images is discussed in [12]. Langelaar *et al.* [11] and Doërr and Dugelay [12] both [11] and [12] considered some new video watermarking applications and described specific challenges. Lin *et al.* [13] described advances in digital rights management (DRM) systems, including encryption and watermarking for protecting video content, and identified the challenges and directions for further investigation of video DRM. Stutz and Uhl [14] surveyed encryption techniques for H.264 AVC/SVC (advanced video coding/scalable video coding) compressed video. Recently, Tew and Wong [15] published a survey focusing on information-hiding techniques designed especially for H.264/AVC compressed video. Smolic *et al.* [16] published a critical overview of coding algorithms for 3DTV (3D television) and discussed the watermarking of 3D data, including 3D geometric structures and 2D representations of 3D videos (e.g., multi-view videos).

In the literature, many watermarking techniques [17]–[27] have also been introduced for protecting digital audio signals from illegal distribution. Recently, a comprehensive overview of twenty years' research and development work on digital audio watermarking was presented by Hia *et al.* in [28]. Other survey papers [29]–[31] also summarized different aspects of audio watermarking from the literature. However, as the focus of our overview paper is on digital video watermarking,

we do not consider digital audio watermarking. In this paper, we focus on aspects of both 2D and 3D video watermarking and consider the application of recent technologies to these data formats. We first introduce watermarking applications and then discuss their critical challenges in detail. The watermarking techniques are categorized based on the domain in which the watermark is embedded. We then describe each embedding domain and review related state-of-the-art techniques. As robustness to a geometric attack is still an unsolved problem in the field of digital image and video watermarking, we discuss geometric-invariant watermarking techniques and outline a possible solution. In the last part of this work, we focus on an image-based representation of 3D video watermarking.

The remainder of this paper is organized as follows. Section II describes applications of video watermarking and Section III presents the possible challenges that need to be considered during the design of a video watermarking algorithm. A brief overview of the RGB (red, green and blue) and YUV color spaces commonly used for watermark embedding is provided in Section IV, with the watermarking techniques classified based on the domain in which the watermark is embedded. Complete pictures of these techniques, including an overview of their backgrounds, and pros and cons as well as relevant literature, are also provided. In Section V, geometric-invariant watermarking techniques are discussed. Image-based representations of a 3D video are classified in Section VI and some existing works related to these techniques are discussed. An overall discussion of this paper and suggested future research directions are presented in Section VII, with Section VIII summarizing and concluding the paper.

II. Applications of Video Watermarking

In the early 1990s, researchers proposed some possible applications of digital watermarking which included image tagging, copyright enforcement, counterfeit protection and controlled access to image data [32]. A wider range of applications of video watermarking [11], [12], including copyright protection, broadcast monitoring, copy control, video authentication and fingerprinting were introduced in the early 2000s. The most widely adopted of these applications are discussed in the following subsections.

- *Copyright Protection:* a copyright owner can embed a watermark containing the copyright information in a host video which, when decoded, can be used as proof of ownership. However, as the intention of pirates is to infringe the copyright of video content by removing the watermark, it should be robust to various attacks in practical applications.
- *Broadcast Monitoring:* video content, e.g., commercial advertisements, is distributed over television networks and whether the content has been broadcast as contracted can be verified using a passive or active monitoring system. As the former compares the received and original videos, a large amount of storage is required whereas digital video watermarking can provide active monitoring in an invisible and robust way.
- *Copy or Playback Control:* watermarking can also be used to control digital playback and recording devices, e.g., a DVD player, for the purpose of preventing unauthorized copying or playing. If a device detects the presence of a watermark during playback or copying of a video content, it prevents from being copied or played for other than its stipulated use. However as video streaming has become widespread, it can also be exploited to control online streaming or downloading by placing a watermark-decoding filter at the ISP network node.
- *Video Authentication:* a watermark embedded in a host video can be used to check the authenticity of its content. There are some critical applications, such as video surveillance and medical imaging, in which protecting the content from alteration is very important. A fragile watermark (i.e., one that cannot survive any alteration applied to the watermarked data) helps to detect tampering and provides information as to which parts of the data have been altered.
- *Fingerprinting:* as we discussed in the previous section, the illegal distribution of video content after copying a movie using a camcorder from the theater is a major problem. A video content owner can use this technique to trace the source of illegal copies. In this method, a unique watermark is embedded in each copy issued to each customer or movie theater in which the movie is to be released. It may contain a customer's identification or information relating to the movie theater so that, in the case of copyright violation, the content owner can easily blame the customer or cinema which allowed the illegal copy through camcording.
- *Online Location:* with the availability of high-speed broadband access and a multitude of Internet streaming sites, the pirated content is uploaded to the web and readily accessible to the global audience for viewing online and downloading. The content owner can embed the watermark before its release. Internet search services continuously look at the web for the watermarked video content and notify the owner of where their content was found.
- *Content Filtering:* watermarking can be used for triggering and blocking of content. The watermark is embedded in the host video content before its transmission with each instance of the content carrying specific information. When the watermark is detected by the watermark decoder, a specific action, e.g. an advertisement, could be triggered at specific times within the content. It might also trigger a specific call to action to a guardian if a specific piece of content is restricted for children.

III. Challenges for Video Watermarking

After a watermark is embedded in a host video, it may be subjected to different types of attacks and the watermark is extracted at the decoder from the attacked version of the watermarked video. Therefore, there are some issues, such as the imperceptibility of the watermark, capacity, its blind detection, the robustness to attacks and security of the

(a) (b) (c)

Fig. 4. (a) original image, (b) image with visible watermark and (c) image with imperceptible watermark.

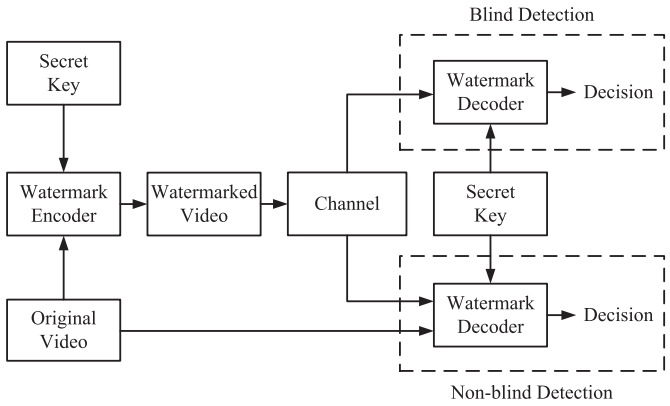


Fig. 5. Block diagram showing blind and non-blind watermark extraction methods.

watermark, that must be considered during the design of a watermarking algorithm [11], [12], [33]–[35].

A. Imperceptibility

A watermark is embedded as additional information to that in an original video and can be visible or invisible. In the former, owners (e.g., television stations) superimpose their logos over a transmitted video to plainly indicate their ownership, as shown in Fig. 4(b). However, the focus of this paper is invisible watermarking which is more difficult because the watermark must be imperceptible to the human visual system (HVS) so as not to degrade the video's visual quality. Imperceptibility refers to the invisibility of the watermark in a video displayed in a movie theater. A watermarking algorithm is imperceptible if the human eye cannot distinguish between an original and watermarked video [36], as shown in Fig. 4(c). As the user of a watermarked video does not have access to the original video for comparison, it is impossible for him/her to notice small modifications in the watermarked video [37]. Therefore, a watermarking algorithm must ensure that the watermark embedded in a host video does not significantly affect the visual quality of this video.

B. Payload

Data payload refers to the number of watermarking bits embedded in an image or video. The payload of the watermark affects the imperceptibility of the watermark. Increasing the payload causes greater visibility of the watermark and vice versa. Therefore, it is important to consider the trade-off between payload and imperceptibility during the design of an algorithm. The payload requirement is different for different watermarking applications [38]. A watermarking system that embeds multiple bits is referred to as multi-bit watermarking. In this approach, the embedded watermark contains a message which must be decoded. On the other hand, a zero-bit watermarking system provides access control by checking for the presence of the watermark at the decoder, i.e., the output of the decoder will be either "watermark present" or "watermark absent".

C. Blind Detection

A watermark extraction system can be either non-blind or blind, as illustrated in Fig. 5. In the non-blind system, to extract the watermark at the decoder, the original un-watermarked and watermarked videos are compared which requires a large amount of database storage that may often not be available. A solution to this is to use a blind detection system in which the watermark is extracted from a watermarked video without using the original content, that is, the original video is not available at the decoder end during extraction. Watermark extraction is easier and more robust using the non-blind system. However, in the case of most practical applications, the original host video is not available for watermark extraction at the decoder. Therefore, the watermark should be detectable without reference to the original video content, i.e., the extraction should be blind.

D. Robustness to Attacks

In recent years, attacks against watermarking systems have become complicated [39], with some robustness-related and others security-related. Robustness means the resistance of a watermark to blind non-targeted modifications or the common media operations of regular users. These modifications may be performed to either fulfil the needs of the user or intentionally remove the watermark. These operations are likely to degrade the quality of the video and result in the watermark decoder either no longer being able to extract the watermark or extract it with more errors. The robustness of a watermarking scheme refers to its ability to maintain functionality after the watermarked video has been distorted [32], [40]. The typical types of distortions include signal processing and geometric attacks, and temporal de-synchronization.

1) Signal Processing Attacks: Signal processing attacks are very common types of distortions which reduce a watermark's energy by changing the pixel values of the watermarked video frames [41]. They include additional noise caused by transmission of the video signal over the channel and filtering or de-noising to remove the watermark signal. To reduce storage needs or increase transmission efficiency, a lossy compression, such as MPEG-1, MPEG-2, MPEG-4, H.264/AVC and H.265/HEVC, is typically performed on the video data. This compression may degrade the perceptual quality of the video and, as a result, remove the watermark even if this is not the primary goal. The main purpose of video compression is removal of the spatial redundancy of a video by eliminating

its high-frequency information which is visually less sensitive. The amount of compression applied is a trade-off among the quality of the video, disk space and hardware cost [42]. In addition, users may transcode the video into a different compression format which may also remove the watermark.

2) Geometric Attacks: While signal processing attacks alter the pixel values of the video frames but maintain their positions, geometric attacks change the geometric positions of a frame's elements, i.e., break the frames spatial synchronization. The most common geometric attacks used in digital video watermarking include upscaling, rotation, cropping and downscaling to an arbitrary resolution. In a poorly supervized movie theater, as a high-quality camcorder can record a high-definition (HD) copy of a movie from the large screen, it is able to maintain the movie's original resolution and quality. However, if the camcorder is improperly placed (intentionally or unintentionally), geometric attacks, such as upscaling (zooming), rotation and cropping, usually occur during camcording. Also, illegal content, pirated from sources other than camcording, may be subjected to geometric attacks intentionally designed to remove the watermark. The resolution of the pirated HD content is usually not compatible with portable devices, such as smart phones, portable multimedia players (PMPs), personal digital assistants (PDAs) and tablets. Therefore, a pirate may downscale a HD video to a resolution compatible with portable devices and distribute the movie worldwide via the Internet. It should be noted that as different systems support different display formats, the aspect ratios of an original watermarked video and its downscaled version might be different. The most popular aspect ratios used in HD television (HDTV) and standard-definition television (SDTV) are 16:9 and 4:3 respectively, with the former wider than the latter [43]. As downscaling in resolution and geometric attacks are reasons for the loss of both video and watermark information, the robustness of a watermark following these operations is also an important consideration when designing a watermarking approach.

3) Temporal Synchronization: A digital video watermarking system faces both spatial (geometric) and temporal synchronization attacks. Temporal synchronization is the process of maintaining synchronization among the frames in a video sequence. This is one of the challenges inherent in blind watermark extraction. Such attacks include frame dropping, frame insertion, frame swapping and frame rate conversion, as shown in Fig. 6. Frame insertion and dropping involve simply inserting and dropping a small number of frames from a watermarked video sequence respectively. On the other hand, frame swapping modifies the order of the same frames in a watermarked video and may not be perceptible to the human eye. If a video watermarking system uses a key to embed a watermark at the encoder and, at the same time, depends on the same key to extract it at the decoder, synchronization between frames at both the encoder and decoder is required for accurate extraction. As frame rate conversion is a common process responsible for frame dropping or insertion and causes this type of extraction to fail, a watermark extraction algorithm must consider such types of video attacks.

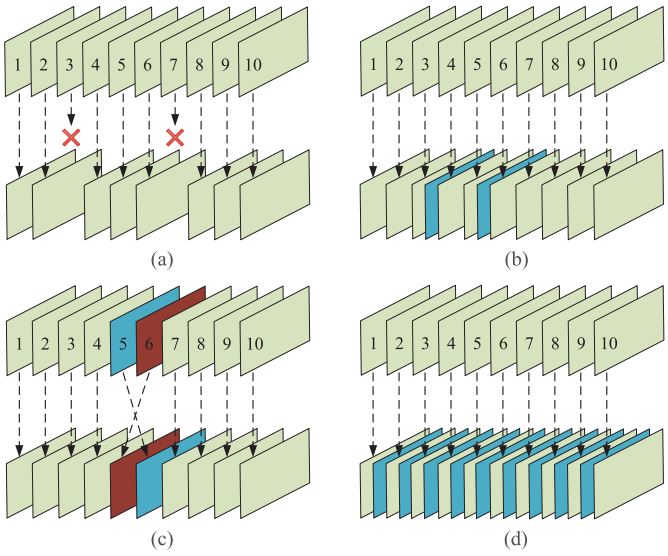


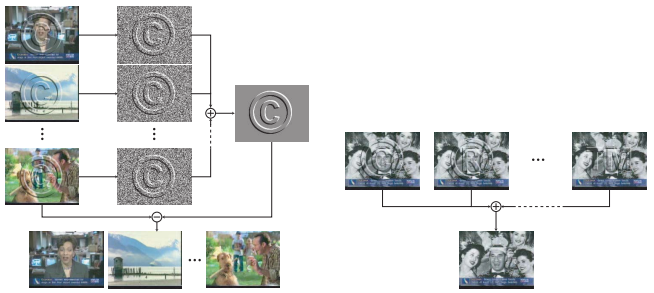
Fig. 6. Temporal synchronization attacks: (a) frame dropping - two frames are dropped; (b) frame insertion - two frames are inserted; (c) frame swapping - order of the two frames are changed; and (d) frame rate conversion - frame rate is doubled.

E. Security of the Watermark

Robustness-related attacks are common media operations that affect both video and watermark signals and affecting the watermark might not be the main goal. On the other hand, security-related attacks are intended to gain knowledge about an embedding and/or extraction system in order to remove a watermark [44], [45]. Some possible attacks that can be used to create an un-watermarked video by removing the watermark from a watermarked one are collusion attacks [46], watermarked-only attack (WOA) [47]–[49] and multiple watermark embedding [32], [50]. Although multiple watermark embedding can also be used to illegally claim ownership of the video content.

1) Collusion Attacks: Collusion attacks can take the form of watermark estimation re-modulation (WER), temporal frame averaging (TFA) and averaging multiple copies of the same video content. In the case of a WER attack, an estimate of the watermark is obtained by averaging initial estimations of the watermark extracted from a large number of watermarked frames [51] in a video sequence. Finally, the estimated watermark is subtracted from the watermarked frame to remove the watermark. Hence if the same watermark is repeated in a large number of different video frames, it is quite easy to estimate and then remove. Therefore, a potential attacker can remove the watermark while maintaining its visual quality. The example in Fig. 7(a) shows the same watermark embedded repetitively in a large number of frames of different scenes which enables un-watermarked frames to be recovered by a WER attack. However, such an attack fails if uncorrelated watermarks are embedded in uncorrelated frames.

In a TFA attack, a temporal low-pass filter is applied to a number of consecutive frames [46]. When a different watermark is embedded in a small number of similar frames, this type of attack can remove the watermark without introducing



(a) (b)

Fig. 7. Illustration of the collusion attacks [52]: (a) watermark estimation re-modulation (WER); and (b) temporal frame averaging (TFA).

any significant visual distortion. The illustration in Fig. 7(b) shows uncorrelated watermarks in different frames of the same scene removed by a TFA attack. It should be noted that the TFA attack is not very useful if neighbouring frames in a video sequence are not similar because applying a temporal low-pass filter to more than two or three frames when the content is changing rapidly results in very poor quality. When correlated frames are watermarked by a single watermark, a TFA attack strengthens rather than destroys the watermark.

Combining multiple copies of the same video, that has been watermarked with different keys, is another way to create a new un-watermarked copy. The attackers can collect several versions of the same video contents carrying uncorrelated watermarks from multiple users. Averaging these copies eliminates the effect of the watermark and generates an un-watermarked copy of that content.

2) Watermarked Only Attack: An adversary may observe several videos watermarked with the same key (WOA [47]–[49]) to estimate the watermark. If several watermarked versions of the same video sequence are obtained, estimations of the watermark will be similar to when it is repeatedly estimated from the same frame. However, an attacker might be able to estimate a watermark if the watermarked contents are different because he/she now has a large number of different frames watermarked with the same key.

3) Multiple Watermark Embedding: Another possible attack that can be used to generate an un-watermarked sequence or illegally claim the ownership of the original content is embedding an unauthorized watermark into the host sequence that is already watermarked. If a second watermark is embedded for illegally claiming the ownership of the original content, very likely the effect of the first watermark is not erased, as both watermarks will be independent. In order to generate an un-watermarked sequence, i.e., erasing the effect of the first watermark, a more sophisticated attack should be considered. As the main limitation of this attack is degradation in the resultant video caused by multiple watermarks, unauthorized embedding is not useful if perceptual quality is important. Although, it might be the case that the doubly watermarked sequence is still perceptually equivalent to the host sequence depending on the distortions caused by the first watermark and subsequently the second watermark.

IV. Watermark Embedding Techniques

In recent years, applications using grayscale images or videos have been extended to color ones. Each color frame in a video sequence has three components, red (R), green (G) and blue (B), in an RGB color space. Alternatively, luminance (Y) and chrominance (U and V) components in the YUV domain can be generated from the RGB source. The Y channel represents the overall intensity and most of the information about a frame and the U and V channels represent the color information.

In the RGB color space, watermark embedding is accomplished by marking either each color channel separately [53]–[60] or only a specific channel, e.g., blue [61]. However, except for the blue channel to which the HVS is less sensitive, this space is highly correlated and not suitable for watermarking applications [62]. On the other hand, most techniques [63]–[70] consider the Y in the YUV color space as the watermark embedding channel. Although a watermark is embedded in the Y channel to survive color to grayscale conversion [71], recent applications have been extended to color from grayscale images or videos. As the Y channel typically contains more bits than the U channel, it may be able to accommodate a larger watermark. However, as a distortion in the Y channel is more noticeable to the HVS than distortion in the U and V channels [72], [73], watermarking using this channel does not support a high-strength watermark. This results in poor defense against attacks as robustness is directly proportional to the strength of the watermark. Therefore, other methods [74]–[81] embed the watermark in the chrominance channel to provide enhanced robustness. Then, once the watermark is embedded using the YUV domain, an inverse operation is performed to return it to the RGB color space.

After selecting a watermark embedding channel, the watermark can be embedded directly in a frame or transformed to the other domain before being embedded. Based on the domain in which the watermark is embedded, watermarking techniques can be classified as compressed, spatial and transform domain watermarking. The watermark can also be embedded into the encrypted domain [82]–[84].

A. Compressed Domain Watermarking

In compressed domain watermarking techniques, the watermark is embedded in an encoded bit stream generated using encoders conforming to MPEG-2 [85], MPEG-4 [86], H.264/AVC [87], H.265/HEVC [88], etc. standards. It should be noted that most of these techniques are employed in the discrete cosine transform (DCT) domain [89] using specific components of the compression technique (e.g., variable-length coding) to embed the watermark. In this section, we discuss MPEG-2, MPEG-4, H.264/AVC and H.265/HEVC video watermarking techniques.

1) MPEG-2 Video Watermarking: MPEG-2 [85] is a widely used compression standard as the format for digital TV signals broadcast by terrestrial, cable and direct-broadcast satellite TV systems. It is also used to store movies and other programs on DVD discs with data rates up to about 10 Mbps. In this

compression standard, the frames of a video sequence are compressed into three kinds, intra-coded (I-frames), predictively coded (P-frames) and bi-directionally predictively coded (B-frames). Many existing compressed domain watermarking techniques [64], [79], [89]–[94] in the literature focus on embedding a watermark in the MPEG-2 bit stream.

Hartung and Girod [90] proposed a watermarking algorithm based on the spread spectrum watermarking in the uncompressed domain and a compatible extension of this method in the compressed domain, i.e., in a MPEG-2 video bit stream. This scheme transforms an encrypted, pseudo-random signal using the DCT and then embeds it in the MPEG-2 bit stream. The watermark of this method is extracted from the decoded video in a blind fashion. Chung *et al.* in [91] also developed a watermarking technique for MPEG-2 video by exploiting the direct-sequence spread spectrum technique. This technique focuses on the watermark embedding strength and area of embedding to retain the quality of the watermarked video. It extracts the watermark from the watermarked MPEG-2 bit stream without depending on the original video sequence. Biswas *et al.* [92], the authors also perform partial decoding of the compressed bit stream as in the method by Hartung and Girod [90]. However, their technique uses scene-based multiple gray-level watermarks that provide more perceptual information and improve the visual quality of the watermarked video. The spread spectrum watermark is then embedded by modifying the DCT coefficients. Their experimental results demonstrate that this scheme is robust to several types of attacks. In [89], a video watermarking algorithm that can be performed in the VLC domain of the MPEG-2 video bit stream is designed. However, although it exploits a frame-dependent watermark to deal with a watermark estimation attack (WEA), it does not consider geometric attacks.

Lee *et al.* [64], Choi *et al.* [79], and Wang and Pearmain [93] proposed video watermarking algorithms which embed the watermark in the MPEG-2 video stream. These techniques partly decode the compressed video, then embed the watermark in the low-frequency DCT coefficients and, finally, re-encode the watermarked video to the MPEG-2 video stream. As the scheme in [93] focuses on only cropping and downscaling in resolution attacks, it is vulnerable to a temporal synchronization attack caused by a frame rate change and/or camcording. Although this problem is overcome in [64] and [79], the first method performs poorly against geometric attacks and the second one is unable to retain the visual quality of the watermarked video. Celik *et al.* [94] developed a digital video watermarking technique for a MPEG-2 video that can survive cropping, de-interlacing, re-sizing, DivX compression and camcording. It embeds the watermark by modulating a subset of quantization matrices used for video encoding but, although it is robust to different attacks, it is still weak against rotation.

2) MPEG-4 Video Watermarking: MPEG-4 [86] is one of the latest compression standards designed specifically for low-bandwidth (less than 1 Mbps bit rate) audio-video encoding purposes. It is based on the MPEG-1 and MPEG-2 standards and adds some more features. The main functionality of this standard is object-based coding whereby audio-video objects can be individually defined and then rendered together to form scenes.

Alattar *et al.* in [95] proposed a video watermarking scheme for a low bit-rate MPEG-4 compressed video. This technique embeds a synchronization template for protection against geometric attacks. A gain control feature is included to improve the visual quality of the watermarked video by adjusting the watermark's embedding strength based on local image characteristics. This technique also introduces a method for controlling the data rate of the watermarked video that is suitable for a low bit-rate video. In [96], an adaptive watermarking algorithm based on a MPEG-4 video stream, in which the watermark is embedded in the low-frequency DCT coefficients of the I frame, is discussed. An adaptive strength factor is designed based on the direct current (DC) and low-frequency coefficients. This factor is different for each image block. Hence this scheme adapts to the HVS and is robust to commonly used attacks.

As one of the key points of the MPEG-4 standard is the possibility of accessing and manipulating objects in a video sequence [97], object-watermarking techniques should consider that the watermark must still be detectable even if the object is manipulated. In the literature, some watermarking techniques [97]–[99] are designed based on MPEG-4 video objects. Barni *et al.* [97] embed the watermark in each object of a MPEG-4 video stream by imposing specific relationships between some predefined pairs of quantized DCT coefficients in the Y channel blocks of pseudo-randomly selected intra- and inter-macro blocks. In this blind watermarking system, frequency masking is used to improve both the visual quality and robustness to attacks but its robustness is verified only against bit-rate decreasing and frame dropping. Boulgouris *et al.* [98] proposed a watermarking scheme for MPEG-4 natural video objects in which both synchronization and watermark signals are embedded to enable fast synchronization recovery in the case of object manipulation. Lu and Liao in [99] designed a watermarking algorithm based on the concept of communications with side information for a MPEG-4 video object. In this scheme, the eigenvectors of a video object are calculated to determine its major and minor orientation tendencies and used to deal with geometric transformations. Although it is claimed to be robust to several types of attack, it can deal with only histogram equalization, flipping and blurring.

3) H.264/AVC Video Watermarking: H.264/AVC [87], also known as part 10 of MPEG-4, is a state-of-the-art compression technique. It is currently the most commonly used video compression standard with better video quality and lower bit rates than previous standards. It incorporates various new features that improve the compression efficiency and has become popular for various video technologies, including HDTV broadcasting, camcorder (e.g., Sony, Panasonic), video surveillance, video storage (e.g., Blu-ray disc, HD DVD disc), video streaming, etc.

An overview of digital video watermarking in a H.264/AVC compressed video presented by Tew and Wong in [15] identifies the stages, including the prediction process, transformation, quantization and entropy coding, in which the

watermark embedding takes place and then reviews relevant watermarking techniques for each of them. Stutz and Uhl [14] provided a critical overview of the encryption technique in the H.264 AVC/SVC (scalable video coding) compressed domain.

Several watermarking algorithms [100]–[111] have recently been proposed for H.264 compressed video. In [100], the watermark is embedded in the quantized DCT coefficients of the Y residuals to avoid decompressing the video while a human visual model based on a 4×4 DCT block is used to increase the payload and robustness while limiting visual distortion. The watermark at the decoder is extracted from the decoded video sequence in order to make the algorithm robust to intra-prediction mode changes. The experimental results show that the proposed scheme is robust to several attacks. The watermark embedding performed by Mansouri *et al.* in [102] uses the syntactic elements of the H.264 compressed bit stream. It avoids full decoding and re-encoding both in the embedding and extracting processes. This technique exploits appropriate sub-macro blocks for embedding through a spatiotemporal analysis to enhance the quality of the watermarked video and robustness to attacks. In [104], a grayscale image watermark is pre-processed and then embedded in the compressed domain for copyright protection. This pre-processing increases the robustness and capacity of the video watermarking algorithm. The experimental results validate the robustness of this scheme to several attacks.

Watermark embedding in the H.264/AVC domain can also be achieved by exploiting the motion vectors as proposed in [105]–[109] where the techniques [107]–[109] utilize the motion vector difference (MVD) to embed the watermark. Guo and Pan [107] proposed a H.264 watermarking scheme for a video stream switching application. This method embeds the watermark by modifying the MVD's horizontal and vertical offsets. Experimental results show that this technique achieves the requirement of the watermarking for stream switching application. Jiang *et al.* [108] proposed a motion vector based copyright protection technique for a H.264 video stream with drift compensation. This scheme embeds the watermark in the motion vector residuals of macroblocks with the smallest partition size to hold visual impact and distortion drift to a minimum. In the watermark embedding process, the energy compaction property of the DCT is applied to the motion vector residual group to achieve robustness against an intentional attack. Xu *et al.* [109] proposed an algorithm for embedding additional data in the encrypted version of a H.264/AVC bit stream. This technique consists of video encryption, data embedding and data extraction phases. By analyzing the properties of the H.264/AVC codec, the codewords of the intra-prediction modes, motion vector differences and residual coefficients are encrypted with stream ciphers. Finally, the watermark is embedded in the encrypted domain using a codeword substitution technique. At the decoder, watermark extraction can be performed in either the encrypted or decrypted domain.

Ma *et al.* in [110] analyzed the problem of intra-frame distortion drift induced by data hiding in the H.264/AVC video streams. Their scheme embeds the watermark in the quantized 4×4 DCT block of the I frame. They define the paired coefficients and exploit the intra-frame prediction modes of their adjacent blocks to ensure that any distortion does not propagate to neighboring blocks. The experimental results show that this scheme can effectively eliminate intra-frame distortion drift and achieve a higher-quality watermarked video than other existing schemes. Pröfrock *et al.* proposed a fragile, blind and erasable H.264/AVC video authentication technique that avoids the continuous motion prediction error in [111]. This algorithm utilizes some of the skipped macroblocks to embed the erasable watermark. The watermark consists of an encrypted hash value and a certificate containing a public key. The advantage of this scheme is the possibility to erase the watermark and to reconstruct the original H.264 video. The algorithm achieves low video quality degradations.

4) H.265/HEVC Video Watermarking: High-efficiency video coding (HEVC), also known as H.265, is a new video compression standard developed by the JCT-VC group, a collaboration between the ISO/IEC MPEG and ITU-T VCEG [88] groups. It is a next-generation video coding standard and has recently been used in many applications. In contrast to the previous state-of-the-art H.264/AVC standard, it is able to compress a video twice as efficiently and produce a video of similar perceptual quality [112]. In addition, it is a hybrid video compression standard based on intra-/inter-predictions and a transformation process.

As HEVC is the latest compression standard, very few watermarking techniques for a H.265/HEVC compressed video [113]–[117] have been published in the literature. In [113], the watermark is embedded in the LSBs of the non-zero quantized transform coefficients selected during the encoding phase. The experimental results show that this scheme achieves watermark imperceptibility and robustness to bit-rate conversion. Tew and Wong [114] proposed a watermarking technique in the HEVC domain using the coding block size decision on every coding tree unit to embed a watermark in the non-zero DCT coefficients based on predefined mapping rules. Their simulation results show that this scheme achieves a higher-quality watermarked video for a high bit rate with an insignificant degradation in perceptual video quality for a low bit rate. Another watermarking method developed by Ogawa and Ohtake [115] for H.265/HEVC video streams embeds the watermark during a video's encoding process using the HEVC compression technique but the quality of the watermarked video and robustness of the scheme are not discussed. Tew *et al.* proposed another video watermarking technique for HEVC video authentication in [116] which includes weight generation, video feature extraction and two layers of authentication. The experimental results show that the quality of the watermarked video is maintained. Dutta and Gupta [117] designed a blind video watermarking technique in which a readable watermark is embedded in the I frames of a HEVC-encoded video. To improve the watermarking security, this scheme exploits a random key to select the blocks in which to embed the watermark. The authors claim that their framework limits increase in the video bit rate and degradation of visual quality. In addition, this technique is robust to image processing and re-encoding attacks.

While, in compressed domain watermarking, the watermark is embedded in the compressed bit stream, in uncompressed domain watermarking systems, it is embedded in either the spatial or transform domain, as described below.

B. Spatial Domain Watermarking

Watermark embedding in the spatial domain is achieved by directly modifying the pixel values of the embedding channel of a video frame. More details of such techniques can be found in [32]. Generally, this type of watermarking system can be classified as one of the following methods.

- *LSB-based:* in these methods [118]–[120], the LSB of each pixel in the host image is modified to embed the watermark. This is the simplest technique in a spatial domain watermarking system [10]. As the LSBs carry less relevant information, modifying them does not affect perceptual quality. However, the watermark can be easily removed as the LSB of a pixel is vulnerable to compression and other attacks.
- *Block-based:* in these approaches [121]–[123], the host image is divided into different blocks before the watermark is embedded in them. The intensity of each pixel in the blocks is then adjusted according to the watermark. These methods are simple and computationally efficient.
- *Statistical:* these methods are based on a pseudo-random, statistical model referred to as a Patchwork model [124], [125]. It embeds the watermark in a host image using a Gaussian distribution. Here two sets of pixels called patches (e.g., A and B) are chosen pseudo-randomly with the image data in patch A lightened and that in patch B darkened. Then, the presence of the watermark is detected by comparing the sum of the differences between A and B. However, this method is sensitive to geometric attacks as the watermark is highly related to the positions of the marked patches.
- *Feature point-based:* in these approaches [126]–[131], the invariant features of an image are modified at the encoder to embed the watermark. The presence of the embedded watermark is then checked at the decoder.

As the watermark is embedded directly in the frame without any transformation, these types of approaches are very simple and computationally efficient. However, they have a relatively low information-hiding capacity and limited robustness to normal media operations, such as filtering or lossy compression [132]. Spatial domain watermarking approaches also have limited defense against cropping during which some watermark information is lost.

C. Transform Domain Watermarking

In a transform domain watermarking system, before embedding the watermark, the host frame in a video sequence is converted to a new domain. This conversion is achieved by utilizing the most commonly used transforms, such as singular value decomposition (SVD), the discrete Fourier transform (DFT), DCT and wavelet-based transforms (e.g., discrete wavelet transform (DWT) and dual-tree complex wavelet transform (DT CWT)). Each of these transforms has its own characteristics for representing a video frame in different ways [133]. During the watermark embedding process, the transform domain coefficients are modified by the watermark and then an inverse transform applied on these modified coefficients to generate a watermarked frame. These types of techniques are robust, stable and provide more imperceptibility than spatial domain-based approaches [134]–[137].

1) Singular Value Decomposition: SVD is a technique that can be used to mathematically extract the singular values from a 2D image that represent the image's intrinsic algebraic image properties [138]. Considering that a frame (f) of a video sequence is a square matrix of size $M \times M$, its SVD is defined as:

$$f = USV^T \tag{1}$$

where U and V are orthogonal (or unitary) matrices and S is a diagonal matrix, with the diagonal elements in the descending order of S are called the singular values of f.

SVD-based watermarking approaches [66], [138]–[144] embed the watermark by modifying either U and V or S. SVD techniques are typically used in video watermarking due to the good stability of the singular values, that is, when a small perturbation is added to a frame, these values do not change significantly [68], [139]. Although this characteristic of the SVD provides robustness to attacks, a limitation is that performing it on an image is computationally expensive [139].

A SVD-based non-blind watermarking scheme in which the SVD is applied on the host image using (1) to find the singular values was proposed by Liu and Tan [138]. In this approach, the singular values are modified by adding the watermark and then the SVD performed again on the resultant matrix to calculate the modified singular values. Finally, the original singular values are replaced by the modified values to obtain the watermarked image. An inverse operation is performed at the decoder to extract the watermark from the distorted watermarked image by applying the SVD on that image. In order to do this, the watermark is estimated from the corrupted frame using both the original and distorted singular values. The experimental results show that this approach is robust to common image-processing operations, such as filtering, JPEG compression, scaling, rotation and cropping. Dogan *et al.* [141] proposed another non-blind scheme based on the SVD in which the watermark is directly added to the singular values. Then the watermarked frame is obtained by replacing the original singular values by the modified values. The original values are subtracted from the modified ones at the decoder to extract the watermark. However, as the original singular values are required at the decoder to extract the watermark, the above schemes are impractical because the availability of the singular values depends on the availability of the original image at the decoder which is not present in most practical applications.

2) Discrete Fourier Transform: For a 2D DFT, that is, the DFT of a frame ($f(x, y)$) of size $M \times N$, its forward and inverse transforms are defined as [145]:

$$F(u, v) = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) e^{-j2\pi \left(\frac{ux}{M} + \frac{vy}{N}\right)} \tag{2}$$

for $u = 0, 1, 2, \ldots, M-1$ and $v = 0, 1, 2, \ldots, N-1$.

$$f(x, y) = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u, v) e^{j2\pi \left(\frac{ux}{M} + \frac{vy}{N}\right)} \tag{3}$$

for $x = 0, 1, 2, \ldots, M-1$ and $y = 0, 1, 2, \ldots, N-1$.

The DFT function ($F(u, v)$) produces a set of complex coefficients consisting of the real and imaginary parts at each frequency (u, v). An important property of the DFT is the translational invariance of its magnitude component [146].

Several watermarking approaches which operate in the DFT domain, e.g., [131], [147]–[153], have been introduced. One proposed in [147] embeds the watermark in a 1D signal, with the embedding performed by taking the DFT of the image, re-sampling the Fourier magnitudes into log-polar coordinates and then integrating them along the log-radial dimension. This scheme is robust to scaling, rotation and translation but has limited robustness to cropping. Lu *et al.* [152] combined the advantages of feature detection and image normalization to provide robustness to signal processing and geometric attacks. In their scheme, some feature points are extracted from the input image using a multi-resolution feature-point detection filter. Image disks centered at the extracted feature points are selected and image normalization applied on them. Then, the watermark is embedded in the DFT sub-band coefficients of each disk separately, and the inverse DFT followed by inverse image normalization applied on each watermarked disk. Finally, each disk is covered by the watermarked disk to obtain the watermarked image. At the decoder, the watermark extraction is achieved by performing a correlation between the watermark embedding coefficients and original watermark. As the radii of the disks cannot reflect the original size, when the watermarked image is re-sized, there is a false negative detection.

3) Discrete Cosine Transform: Like the DFT, the DCT converts a signal into elementary frequency components [154] and is used in the most popular compression formats, such as JPEG, MPEG and H.26x [155], due to its good energy compaction properties. However, its coefficients are real rather than complex like those of the DFT. DCT-based watermarking can be classified into two categories, global and block-based. In the former, a full DCT is performed on the whole frame while, in the latter, a frame is divided into non-overlapping blocks and the DCT performed on each block. The coefficient at $(0, 0)$ is known as the DC component and the others as the AC components. These coefficients are divided into three different frequency bands, low, middle and high, with the mid-frequency one usually exploited for watermark embedding. Because the low-frequency band and DC component carry the most signal energy of the frame, they are the most important parts of a video signal and any modification of this band greatly affects the perceived distortion by the human eye. On the other hand, although the high-frequency band supports more distortion, this can be removed through compression and noise attacks [139].

As DCT-based watermarking schemes are usually robust to low-pass filtering, noise addition, sharpening, brightness and contrast adjustments, blurring, compression, etc., they are comparatively better than spatial domain watermarking approaches. However, they are computationally more expensive and provide limited protection against geometric attacks such as scaling, rotation and cropping.

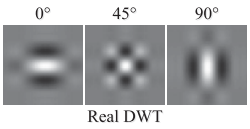
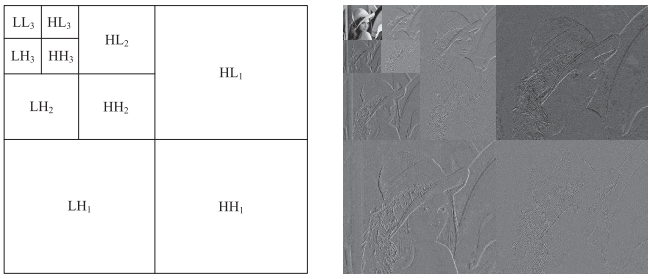


Fig. 8. 2D impulse responses of reconstruction filters in the 2D DWT oriented at angles of 0°, 45° and 90°.

In the literature, several DCT-based approaches [64], [67], [79], [93], [156]–[163] for fulfilling different requirements of digital video watermarking have been proposed. Some [64], [93] are robust to downscaling in resolution and embed the watermark in the low-frequency DCT coefficients. These methods take advantage of the fact that downscaling in the spatial domain of a frame is approximately similar to eliminating the high-frequency band in the DCT domain. However, as changes in the low-frequency DCT coefficients severely degrade the visual quality of a watermarked video, these techniques cannot retain the original quality of the video. Another scheme proposed in [79] uses the low-frequency DCT coefficients of the U channel to embed the watermark, where the DC component is not considered in the watermark-embedding region because any change in it is easily visible as flickering to human eyes. However, as the coefficients around this component usually have large values and any modification of them can also be seen as slight flickering, this algorithm fails to produce a watermarked video that is imperceptible to the HVS. In [159], the watermark is embedded in the watermark minimal sequences (WMSs) of the Y channel by modulating the low-frequency DCT coefficients to provide robustness to geometric attacks. However, frame rate change, which is responsible for frame dropping/insertion from/in an entire video sequence, distorts the WMS. As at least one WMS is required to extract the watermark using this algorithm, this approach has limited defense against frame rate change. Thanh *et al.* [162] proposed a frame-patch matching-based video watermarking algorithm using KAZE features.[1] In this approach, the feature points of the frame patch are matched to those of all frames in the video to synchronize the embedding and extraction regions. The watermark is embedded in the DCT domain of randomly generated blocks in the matched region and, to extract it, the embedded region from the distorted video is synchronized at the decoder using KAZE feature matching. Although this scheme is robust to geometric, video processing and temporal attacks, as the cost of the matching process is high, it is not applicable for real-time video watermarking.

4) Discrete Wavelet Transform: The DWT is a mathematical tool that decomposes an image or video frame into a lower-resolution approximation image (LL) and three detail components, vertical (LH), diagonal (HH) and horizontal (HL).

[1]A KAZE feature is a multi-scale feature detection and description algorithm using nonlinear scale spaces [164].



(a) (b)

Fig. 9. Configuration of the DWT coefficients at each level for a 3-level decomposition: (a) three directional sub-bands (LH, HH and HL) oriented at angles of 0°, 45° and 90°; and (b) magnitudes of sub-band images of the *Lena* test input image.

The approximation image (LL) is the low-frequency part and detail components LH, HH and HL are the high-frequency part with decompositions able to be conducted at different DWT levels. A 2D DWT produces three sub-bands at each level oriented at angles of 0°, 45° and 90°, with the 2D impulse responses of the reconstruction filters shown in Fig. 8. Three directional sub-bands oriented at angles of 0°, 45° and 90° at each level for a 3-level DWT are shown in Fig. 9(a) and the corresponding sub-band images of the *Lena* test image after applying a 3-level DWT are shown in Fig. 9(b).

In the literature, several DWT-based watermarking approaches, e.g., [65], [89], [139], [149], [150], [165]–[174], have been introduced. A chaos-based wavelet domain method for still images, in which the watermark is embedded in the DWT coefficients of a sub-image, is implemented in [65]. After extracting the watermarked sub-image from the whole image, a watermark extraction technique is applied. Although this method is robust to cropping, it provides limited defense against rotation. Another approach based on the DWT proposed in [165] has poor robustness to geometric attacks compared with that of the DT CWT-based approach described in [175]. In a hybrid watermarking scheme based on the DWT and SVD introduced by Lai and Tsai [139], as the SVD transform of an image is computationally inefficient, the host image is decomposed into four sub-bands (LL, LH, HL and HH). Then, the SVD is applied to only the LH and HL sub-bands of a 1-level Haar DWT rather than to the entire image. The watermark is divided into two parts which are then embedded in the singular values of LH and HL. Finally, the watermark is extracted from these two sub-bands using the original singular values. Another hybrid watermarking technique, in which a redundant DWT (RDWT) is used with the SVD to embed a watermark in an image, was proposed by Makbol and Khoo [166]. In the embedding process, a 1-level RDWT decomposition is applied on the image to generate four sub-bands, LL, LH, HL and HH. The watermark is embedded in each sub-band and then an inverse RDWT is applied on these sub-bands to provide the watermarked image. Finally, the watermark is extracted from each sub-band.

5) Dual-Tree Complex Wavelet Transform: Two major problems of the DWT in its critically decimated form (Mallat's dyadic filter tree [176]) are its lack of shift invariance, i.e., a small shift in the input signal can cause large variations in energy across the sub-bands at different scales, and poor directional selectivity. The complex wavelet transform (CWT) overcomes these two limitations by including limited redundancy in the transform but is unable to obtain perfect reconstruction further than level 1. To solve this problem, the dual-tree CWT (DT CWT) was developed by Nick Kingsbury [177]–[180]. It employs two filter bank trees, one for each of the real and imaginary parts of the wavelet coefficients, rather than one as do the DWT and CWT. Also, while a 2D DWT produces three sub-bands at each level oriented at angles of 0°, 45° and 90°, the 2D DT CWT produces six sub-bands of complex coefficients at each level at angles of ± 15°, ± 45° and ± 75°. The 2D impulse responses of the reconstruction filters are shown in Fig. 10.

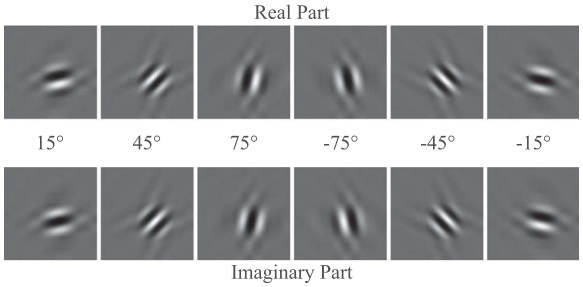
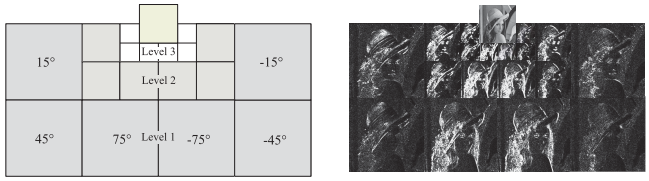


Fig. 10. 2D impulse responses oriented at angles of ± 15°, ± 45° and ± 75° of the reconstruction filters in the DT CWT.



(a) (b)

Fig. 11. Configuration of the DT CWT coefficients at each level for a 3-level decomposition: (a) six directional sub-bands oriented at angles of ± 15°, ± 45° and ± 75°; and (b) magnitudes of sub-band images of the *Lena* test input image.

(f) of dimension $M \times N$, the complex wavelet coefficients at level l can be defined as:

$$F_{l,d}(u_l, v_l) = R_{l,d}(u_l, v_l) + j\, I_{l,d}(u_l, v_l) \tag{4}$$

or in polar form as:

$$F_{l,d}(u_l, v_l) = |F_{l,d}(u_l, v_l)| e^{j\theta_{l,d}(u_l, v_l)} \tag{5}$$

where $d = 1, 2, \ldots, 6$ are the six directional sub-bands, $R_{l,d}(u_l, v_l)$ and $I_{l,d}(u_l, v_l)$ are the real and imaginary components of $F_{l,d}(u_l, v_l)$ respectively, and

$$|F_{l,d}(u_l, v_l)| = \sqrt{R^2_{l,d}(u_l, v_l) + I^2_{l,d}(u_l, v_l)} \tag{6}$$

and

$$\theta_{l,d}(u_l, v_l) = \tan^{-1}\left[\frac{I_{l,d}(u_l, v_l)}{R_{l,d}(u_l, v_l)}\right] \tag{7}$$

are the magnitude and phase components of $F_{l,d}(u_l, v_l)$ respectively.

A visual illustration of six directional sub-bands at each level for a 3-level DT CWT and the magnitudes of the corresponding sub-band coefficients of the *Lena* test image

TABLE I

QUANTITATIVE COMPARISON OF COMPRESSED, SPATIAL AND TRANSFORM DOMAIN WATERMARKING SCHEMES (BER: BIT ERROR RATE, NC: NORMALIZED CORRELATION, WDR: WATERMARK DETECTION RATIO, FPS: FRAME PER SECOND, PSNR: PEAK SIGNAL TO NOISE RATIO, "–": ATTACK NOT CONSIDERED, NUMERICAL VALUE "*,*" STANDS FOR "AMOUNT OF ATTACK,ROBUSTNESS")

Algorithms		[79]	[181]	[101]	[117]	[121]	[126]	[140]	[148]	[159]	[166]
Type of Domain		MPEG-2	MPEG-4	H.264/AVC	H.265/HEVC	Spatial	Spatial	SVD	DFT	DCT	DWT-SVD
PSNR (dB)		51.20	>38.00	>32.50	32.14	30.69	41.78	43.68	44.21	>38.00	54.73
Robustness Evaluated by		BER	NC	BER	BER	NC	WDR	NC	NC	BER	NC
Attacks	Upscaling	1.5,0.00	1.5,0.91	–	–	–	0.87	2,0.92	1.3,0.85	2,0.85	2,0.95
	Downscaling	0.5,0.00	0.5,0.98	–	–	0.25,0.95	–	0.5,0.92	0.6,0.78	0.5,0.00	0.5,0.95
	Rotation (degree)	4,0.56	20,0.75	–	–	12,0.85	0.95	50,0.95	20,0.84	20,26.93	2,0.98
	Cropping (%)	20,1.10	40,0.85	–	–	–	–	–	–	25,27.8	–
	Frame Rate Change (FPS)	20,0.00	24,0.95	–	–	–	–	–	–	0.00	–
	Gaussian Noise	–	0.72	9.72	0.17	–	–	0.87	0.68	–	0.89
	Filtering	0.56	0.95	–	0.16	0.96	–	0.98	0.95	–	0.98
	Compression	–	–	12.39	–	0.95	0.90	0.96	0.32	0.00	0.95
	Salt and Pepper	–	–	–	0.15	–	–	0.96	0.80	–	0.89
	Camcording	2.95	–	–	–	–	–	–	–	9.88	–

after applying a 3-level DT CWT are shown in Fig. 11(a) and Fig. 11(b) respectively. Compared with the DWT, the DT CWT possesses more desirable properties of perfect reconstruction, good directional selectivity, approximate shift invariance and efficient order-N computation. Its approximate shift invariance can be obtained by doubling the sampling rates in both trees through eliminating the down-sampling by 2 after the level 1 filters. If a frame is re-sampled after scaling or rotation, the magnitudes of the low-frequency DT CWT coefficients are approximately the same, a characteristic that produces a watermarking algorithm robust to geometric attacks. Therefore, in terms of providing robustness to geometric distortions, the DT CWT is superior to the DFT, DCT and DWT transforms as a watermark embedding domain. As it has efficient order-N computation, it requires a computational time of less than 2^m times that of the fully decimated DWT for mD signals [178], [179]. It also introduces limited redundancy of 4:1 for 2D signals which plays an important role in creating watermarks. Over the last decade, a few research studies [74]–[78], [175], [182]–[191] of watermarking schemes using the DT CWT as an embedding domain have been conducted, as discussed in Section V-C.

In this part of the paper, we discussed the domain in which the watermark is embedded. The experimental quantitative results of some compressed, spatial and transform domain watermarking methods are summarized in Table I.

V. GEOMETRIC INVARIANT WATERMARKING

Many digital video watermarking techniques for protecting digital image and video contents by overcoming the challenges of video watermarking have been proposed in the literature. However, although significant progress has been made in this field, geometric attacks, such as scaling, rotation, cropping, downscaling in resolution and aspect ratio change, are still open issues. These types of attacks are very easy to implement and introduce de-synchronization between a watermark encoder and decoder, causing the decoder to either no longer be able to extract the watermark or extract it with a larger error. Image and video watermarking schemes which deal with geometric attacks can be roughly divided into feature-, synchronization- and invariant transform domain-based algorithms which are discussed in the remainder of this section.

A. Feature-Based Watermarking

In feature-based approaches [126]–[131], [192]–[194], the geometrically invariant features of an image are exploited for embedding and extracting the watermark. However, feature-point detection has some limitations [195] as a geometric transform may vary its results, thereby creating false feature points and causing the failure of watermark extraction. In particular, scaling and local distortions significantly affect local operators. Also, as it is difficult to retain the same salient feature points in a group of pictures, these algorithms have, to date, been used mainly for image watermarking.

B. Synchronization-Based Watermarking

Synchronization-based algorithms rectify geometric distortions before watermark extraction. They compute the geometric parameters using an exhaustive search, image registration or template insertion. Then, compensate the original format using these parameters and, finally, extract the watermark from the rectified version. Watermark synchronization using an exhaustive search randomly searches the space of coordinate transformations to locate the watermark at the watermark decoder. It should be noted that this is computationally costly in a large search space and increases the probability of false detection during the search process [196], [197]. Image registration overcomes this problem by aligning the watermark with a reference one using a registration algorithm prior to the watermark extraction and is used to recover the transformation parameters occurring in the watermarked image or video due to geometric attacks. Although registration algorithms [198]–[200] are effective for non-blind watermarking techniques, extraction in a blind watermarking system is difficult [201]. A template insertion approach is another way of protecting against geometric attacks [149], [202] whereby a template that does not carry any information is embedded during the watermark embedding process and then used to detect the transformation parameters before extracting the watermark. However, in these types of techniques, an attacker

can easily access and then delete the template by eliminating the peak in the DFT domain [192].

C. Invariant Transform Domain-Based Watermarking

The final category, invariant transform domain-based watermarking, embeds the watermark in domains invariant to geometric attacks. In the literature, most of these techniques [126], [147], [148], [202]–[204] exploit the Fourier-Mellin transform (FMT) domain which has scaling- and rotation-invariant properties, for dealing with attacks including rotation, scaling and translation (RST). Although FMT-based approaches are effective in theory, unfortunately, they are not suitable for real-time applications as they are computationally expensive and vulnerable to cropping [193], [201].

Loo and Kingsbury [182] first developed an alternative approach using the DT CWT. They considered the DT CWT to be a potentially suitable domain for watermarking as it has approximate shift invariance and good directional selectivity properties [177]–[180]. These characteristics provide inherent robustness to geometric attacks, including scaling, rotation and cropping. As a result, it is becoming a popular choice as a watermark embedding domain [74]–[78], [175], [183]–[191]. In [183], the watermark is embedded in the top two levels of a 4-level DT CWT using a spread spectrum technique. However, as its extraction technique is not blind, this method cannot be applied if the original video content is not present at the decoder. Abdallah *et al.* [188] proposed a SVD-based video watermarking algorithm in the DT CWT domain in an attempt to achieve robustness by combining the benefits of these two transforms. In this approach, the watermark is embedded in the singular values of the level 2 sub-bands of a 2-level DT CWT of a frame rather than directly on the DT CWT coefficients. The watermark at the decoder is extracted without using the original video although the singular values of the original video are required. The experimental results demonstrate that the performance of this hybrid (DT CWT-SVD) scheme for signal processing attacks is better than that of the DWT-SVD based approach. However, it should be noted that the robustness of the watermark to geometric distortions is not discussed. The blind watermarking approach proposed in [175] adds the watermark into the magnitudes of the level 3 and level 4 high-pass complex coefficients of a 4-level DT CWT of the Y channel. This method is robust to upscaling, rotation, cropping and lossy compression. As, to human eyes, distortion in luminance is more noticeable than distortion in chrominance [72], [73], applying this method does not support a high-strength watermark. Therefore, if an imperceptible watermark is required, its robustness is less than that of one obtained from a chrominance channel embedding method [74]–[81].

In [76], three versions of a digital video watermarking algorithm using the U channel based on the DT CWT are proposed. The first and second versions use an identical key for watermark embedding and detection while the third version does not require a key to extract the watermark. In the first version, watermark embedding and extraction are performed on the level 3 DT CWT coefficients. This approach is robust to H.264/AVC compression as well as other geometric attacks, such as rotation, upscaling and cropping, but cannot survive frame rate conversion and downscaling attacks. To achieve robustness to downscaling in arbitrary resolution, in the second version, rather than extracting the watermark from one fixed level of the DT CWT decomposition (level 3), it is extracted from any level(s) depending on the downscaling resolution. However, it is still susceptible to frame rate conversion attacks if the same random watermark generation key is required at the decoder to extract the watermark. The third version is a keyless detection approach in which the watermark is extracted from a frame using only information from within that frame without the watermark generation key used for embedding. As, in this approach, the watermark extraction is not affected by temporal de-synchronization, such as frame dropping/insertion or frame rate conversion, it is robust to camcording. Asikuzzaman *et al.* in [78] proposed a DT CWT and SVD based hybrid watermarking scheme using the U channel of a video frame in which the watermark is embedded in the singular values of the level 3 coefficients of a 3-level DT CWT. This scheme achieves imperceptibility and robustness to geometric attacks, noise addition and H.264/AVC compression. However, as the original embedded bit pattern is exploited at the decoder, it fails to extract the watermark when a temporal synchronization attack, including frame dropping or insertion, is applied. Therefore, it cannot tackle frame rate conversion and camcording.

Geometric invariant watermarking, which is discussed in this section, is an important part of the design of a watermarking algorithm. A quantitative comparison of some noteworthy geometric invariant watermarking schemes is presented in Table II.

VI. 3D Video Watermarking

According to the dimensions of the components of scene representations in which the watermark is embedded and extracted, 3D watermarking methods can be classified into three categories: 3D/3D, 3D/2D and 2D/2D [16]. 3D/3D systems [205]–[211] are used to protect a 3D geometrical structure with both the embedding and extraction of the watermark performed in a 3D space. 3D/2D schemes [212], [213] embed the watermark according to the geometry or texture of a 3D object but extract it from the 2D data (image or video) obtained after projecting the object onto 2D image planes. 2D/2D methods [214]–[243] protect the image-based representation of a 3D scene and the embedding and extraction of the watermark are performed directly on the 2D image or video. In this paper, we focus on only 2D/2D watermarking in which image-based representations of 3D contents are protected from unauthorized distribution by protecting the 2D data.

In the literature, an image-based 3D video can be represented by exploiting stereo imaging, depth image-based rendering (DIBR) [244]–[250] and multi-view imaging systems, as discussed in the remainder of this section.

A. Stereoscopic Video Watermarking

In stereo imaging, the left and right views are captured using two cameras placed in the approximate positions of two

TABLE II

QUANTITATIVE COMPARISON OF GEOMETRIC INVARIANT WATERMARKING SCHEMES (BER: BIT ERROR RATE, NC: NORMALIZED CORRELATION, WDR: WATERMARK DETECTION RATIO, FNR: FALSE NEGATIVE RATE, FPS: FRAME PER SECOND, PSNR: PEAK SIGNAL TO NOISE RATIO, "–": ATTACK NOT CONSIDERED, NUMERICAL VALUE "*,*" STANDS FOR "AMOUNT OF ATTACK,ROBUSTNESS")

Algorithms		[194]	[202]	[204]	[175]	[187]	[188]	[74]	[76]	[78]
Type of Domain		Spatial	DFT	DCT	DT CWT	DT CWT	SVD-DT CWT	DT CWT	DT CWT	SVD-DT CWT
PSNR (dB)		51.83	38.00	38.40	41.00	–	–	41.00	38.64	48.23
Robustness Evaluated by		BER	WDR	BER	NC	NC	NC	FNR	FNR	FNR
Attacks	Upscaling	1.2,0.03	2,0.78	2,8.00	1.15,0.74	1.15,0.74	–	1.20,0.52	1.07,0.00	1.16,0.00
	Downscaling	0.8,0.03	0.75,0.78	0.5,0.00	–	–	–	–	0.25,0.00	0.25,0.00
	Rotation (degree)	25,0.03	1.00	80,0.00	9,0.50	9,0.68	–	10,0.90	7,0.00	16,0.00
	Cropping (%)	30,0.02	50,0.89	–	10,0.98	–	–	20,0.52	7,0.00	16,0.00
	Frame Rate Change (FPS)	–	–	–	–	–	–	–	25,0.00	–
	Gaussian Noise	0.03	–	–	–	0.59	0.99	–	–	0.00
	Filtering	0.06	1.00	0.23	–	0.75	–	–	–	–
	Compression	0.01	0.74	0.00	1.00	0.85	0.99	0.00	0.00	0.00
	Salt and Pepper	0.01	–	–	–	–	0.99	–	–	–
	Camcording	–	–	–	–	–	–	–	0.88	–

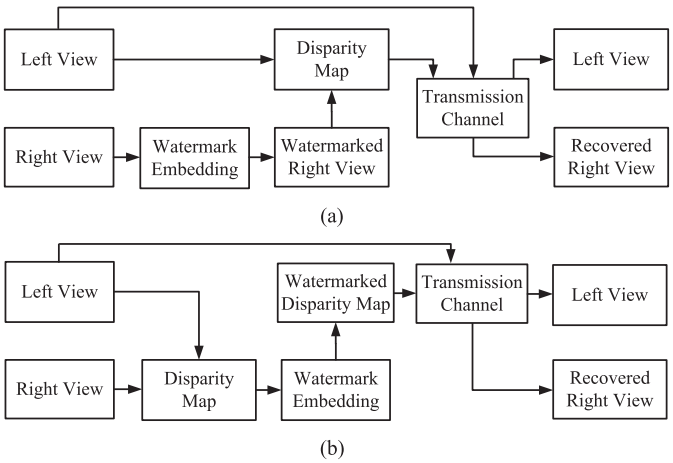


Fig. 12. Stereoscopic (a) view-based and (b) disparity-based watermarking.

eyes. According to the principles of the HVS, two eyes have specific disparities and the brain generates a 3D effect from both their views. This stereo pair can be represented using a disparity map generated from the left and right views and then with the left rather than both the color left and right views transmitted via the communication channel to reduce the transmission bandwidth. The right image is reconstructed at the receiver from the left view and disparity map. Protection schemes for stereoscopic images can be categorized as view-based [214]–[219] and disparity-based [220], [221], as shown in Fig. 12. In the former, stereoscopic images are protected by protecting both or either view whereas, in the latter, the watermark is added into the disparity map.

1) View-Based Watermarking: In the view-based watermarking scheme proposed in [214], a DCT is applied on the right view of a stereo image pair and the watermark is embedded in the DCT coefficients using the characteristics of the HVS. Then, the disparity map is estimated using the left and watermarked right images with, finally, the disparity map and left image transmitted through the transmission channel. At the receiver, the watermarked right image is reconstructed from the received left view and disparity map using an adaptive disparity-matching algorithm and then the watermark is extracted from the reconstructed right image using a decoding algorithm. The method proposed in [215] follows the same procedure as that in [214] for embedding and extracting the watermark but uses the DWT rather than the DCT. Although these methods perform better than pixel- and block-matching algorithms, their systems are not blind. Also, as they protect only the right view by embedding the watermark in it, the left view can be misused as 2D content. Ou *et al.* demonstrated another view-based scheme in [219]. In this method, a watermark is first created based on a feature map extracted from the watermarked stereo image pair, during the verification process that records the positions of unmatched blocks between the stereo images, and is then embedded in the left image. Subsequently, the embedded watermark is extracted from the watermarked left image and converted into an estimated feature map. Ownership is proved when the feature map and the estimated feature map are similar. As this scheme requires both views to extract the watermark, any view can be distributed individually.

2) Disparity-Based Watermarking: Disparity-based stereoscopic watermarking methods can be represented by the works in [220] and [221]. In [220], both the view- and disparity-based methods are introduced and the practical trade-off between transparency and robustness is demonstrated. In the view-based approach, the watermark is embedded in the right view which is generated from the left view and disparity map at the receiver. On the other hand, in a disparity-based method, the disparity map is computed from the left and right views and the watermark embedded in it. Then, the watermarked disparity map and left view are transmitted through the communication channel with the right view reconstructed at the receiver. An adaptive watermarking model based on disparity vectors after analyzing the characteristics of a stereo image is proposed in [221]. An insertion technique which combines spread spectrum principles and low-density parity check error-correcting codes is robust to recording but does not provide any subjective evaluation of imperceptibility. Both these methods face the same problem as view-based techniques of being capable of protecting the stereo pairs but not the individual view.

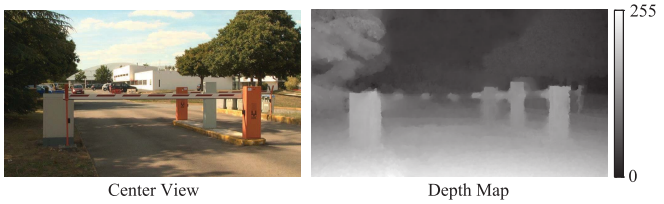


Fig. 13. Center view plus depth map.

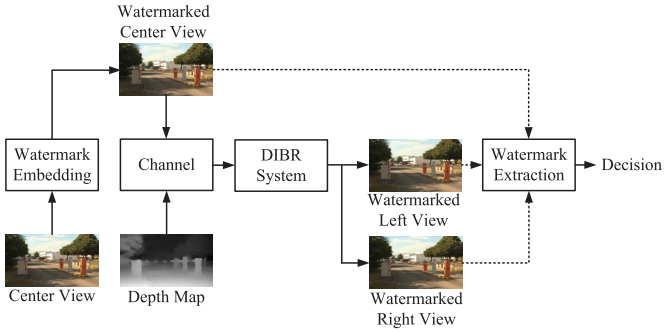


Fig. 14. Diagram of a DIBR video watermarking system.

B. DIBR Video Watermarking

A DIBR system, which is considered to be a convenient and practical 3D representation technology [231], consists of the center view and depth map (see Fig. 13). The center view and depth map are transmitted over the channel rather than the left and right color views. At the receiver, the virtual left and right views are synthesized from them. This approach has the advantage that a depth map can be compressed more efficiently than color views [245], [251]. It should be noted that not only can the left and right views generated using a DIBR technique be distributed as 3D content but the center, left and right views can also be distributed individually as 2D content. Therefore, protecting them from unauthorized distribution is becoming very important. A diagram of the overall system for protecting DIBR contents is depicted in Fig. 14.

In the literature, there are several watermarking techniques for protecting DIBR 3D images and videos [222]–[237]. A digital watermarking approach for protecting a DIBR 3D video's center, left and right views, in which the watermark is embedded in the DT CWT coefficients of the center view, was proposed by Asikuzzaman *et al.* in [222]. At the receiver, the left and right views are generated from the watermarked center view and depth map using the DIBR technique. Then, the watermark is extracted from the center, left and right views in a blind fashion. This scheme is robust to the most common video distortions, including geometric attacks such as scaling, rotation and cropping, as well as lossy JPEG compression and additive noise. Recently, they proposed another work in [225] for the purpose of protecting DIBR 3D video. In this method, the watermark is embedded in both of the chrominance channels of the center view using the DT CWT. The watermark is extracted from the center, left, and right views in a blind fashion. This watermark is robust to geometric distortions, downscaling to an arbitrary resolution, and the most common video distortions, including H.264/AVC and 3D-H.265/HEVC compressions and additive noise. This method can also survive baseline distance adjustment and both 2D and 3D camcording. Pei and Wang [228] proposed a 3D watermarking scheme in based on a depth no-synthesis-error (D-NOSE) model which can detect the regions of depth images suitable for watermark embedding. The watermark is embedded by modifying the depth map with optimal variations in pixel values. As synthesis of the view is very sensitive to variations in depth values, this scheme focuses mainly on the synthesis error and the D-NOSE model is used to create a high-quality 3D video with no synthesis error under a normal rendering condition. However, this method has limited defense against commonly used attacks. A DCT-based method for the center and virtual left and right views aimed at protecting all three views was proposed in [230]. Although it is robust to JPEG compression and additive noise, its performance against geometric attacks was not tested. Wang *et al.* [231] exploited scale-invariant feature transform (SIFT)-based feature points to synchronize a watermark but focused on only signal processing and omitted geometric attacks. Another blind method in the DT CWT domain for the same purposes was introduced by Kim *et al.* in [232]. In this method, the watermark is embedded in the level 2 and level 3 coefficients of a 3-level DT CWT decomposition of the Y channel of the center view using a quantization process and then extracted from the center, left and right views in a blind fashion to protect all views. This approach is robust to scaling and baseline distance adjustment but demonstrates poor performances after rotation and a combination of these attacks. Although this algorithm can survive JPEG image compression, it fails for the H.264/AVC compression of a video sequence because its GOP (group of pictures) structure with I, P and B coded frames compression adds an extra challenge.

C. Multi-View Video Watermarking

In a multi-view imaging system, a number of views of a scene are captured simultaneously from multiple camera angles with advances in image-based rendering (IBR) technology then generating a realistic arbitrary view of the scene from them. As IBR is a much easier and faster technique than others for generating a virtual view, it has recently received a great deal of interest. One of its major applications is free-view television (FTV) whereby a TV viewer can freely choose the viewing position and angle of a transmitted multi-view video using an IBR technique and generate the arbitrary view and then the video sequence. As well as generating stereo views using the center view and depth map, as previously discussed, the DIBR system can also be used to generate virtual views in the multi-view imaging system of a FTV application. But, as there is a possibility of unauthorized distribution of this content, a protection system for FTV is also required.

In the two aforementioned categories, the watermarking techniques try to protect stereo pairs. However, for this scenario, those in the literature [238]–[243] focus on protecting both the original and virtual views by embedding the watermark in the original views. Halici and Alatan [238]

TABLE III

QUANTITATIVE COMPARISON OF 3D VIDEO WATERMARKING SCHEMES (BER: BIT ERROR RATE, NC: NORMALIZED CORRELATION, FNR: FALSE NEGATIVE RATE, FPS: FRAME PER SECOND, PSNR: PEAK SIGNAL TO NOISE RATIO, "–": ATTACK NOT CONSIDERED, NUMERICAL VALUE "*,*" STANDS FOR "AMOUNT OF ATTACK,ROBUSTNESS")

Algorithms		[219]	[220]	[222]	[225]	[226]	[230]	[232]	[236]	[241]	[243]
Type of View		Stereo	Stereo	DIBR	DIBR	DIBR	DIBR	DIBR	DIBR	Multi-view	Multi-view
Type of Domain		DCT	DWT	DT CWT	DT CWT	Spatial	DCT	DT CWT	DWT	Spatial	DCT
PSNR (dB)		>42.00	31.91	41.23	43.00	44.5	42.43	42.15	45.70	–	33.40
Robustness Evaluated by		BER	BER	FNR	FNR	BER	BER	BER	BER	NC	BER
Attacks	Upscaling	2,0.01	–	1.10,0.17	1.15,0.00	–	1.5,0.5	1.5,0.04	1.5,0.05	–	–
	Downscaling	0.9,0.01	–	–	0.25,0.00	–	0.5,0.46	0.5,0.19	0.5,0.05	–	–
	Rotation (degree)	45,0.01	–	5,0.48	15,0.00	–	10,0.55	10,0.36	10,0.09	–	–
	Cropping (%)	–	–	10,0.17	15,0.00	–	10,0.51	10,0.40	10,0.16	80,0.02	30,0.08
	Frame Rate Change (FPS)	–	–	–	50,0.00	–	–	–	–	–	–
	Gaussian Noise	–	0.00	0.00	0.00	0.30	0.15	0.36	0.22	0.04	0.23
	Filtering	0.01	0.00	–	–	–	0.43	0.31	0.22	–	0.03
	Compression	0.01	0.00	0.00	0.29	0.24	0.32	0.18	0.10	0.04	0.09
	Salt and Pepper	–	–	–	–	–	–	–	–	–	0.20
	Camcording	–	–	–	0.16	–	–	–	–	–	–

proposed a correlation-based watermarking method using the DIBR technique in FTV systems. In this scheme, a watermark pattern is warped for each view and then embedded in the texture maps of those views in the spatial domain. The watermark is extracted from an arbitrarily rendered view using the correlation between the rendered image and rendered watermark. In [240], the same watermark is embedded in each view and then extracted from the virtual views generated by exploiting the well-known and useful IBR technique, a process called light field rendering [252]. This method successfully extracts the watermark for a case in which the imaginary camera is arbitrarily located on the camera plane. However, in order to estimate the position and rotation for the imaginary view, it considers that the original views are available at the decoder during the extraction of the watermark. An extension of this work was proposed in [241] in which watermark extraction from the virtual views is achieved for both known and unknown camera positions and rotations. For an unknown position, variations in the watermark pattern due to IBR operations are analyzed and estimated. However, this scheme considers a static scene consisting of only one object, and only attacks in the transmission channel of the multi-view video of the virtual views. Another scheme which also uses a static scene for the purpose of embedding and extraction embeds the watermark in each view of the light field images by exploiting the spatial sensitivity of the HVS in [242]. The watermark's imperceptibility accomplished by modulating its strength according to its presence. A spread spectrum-based multi-bit watermarking scheme for a free-view video was proposed in [243]. The watermark is embedded in each frame of multiple views using the direct-sequence code division multiple access (DS-CDMA) method while the watermark extraction is performed by applying the DCT of the virtual views generated for an arbitrary view. The experimental results demonstrate that this method is not only robust to view synthesis but also common signal processing attacks. A quantitative comparison of some stereoscopic, DIBR and multi-view watermarking techniques is given in Table III.

VII. DISCUSSION AND FUTURE RESEARCH DIRECTIONS

Watermarking in 2D and 3D videos has become more demanding. It is currently a fundamental part of research into the applications of copyright protection, broadcast monitoring, copy control and video authentication. Although, DVD copy control is one of the ways to prevent unauthorized distribution, it is not the only required means of protection as a viewer may have access to an illegal copy of a movie before the release of its DVD version. These illegal copies are obtained from poorly supervized movie theaters and distribute illegally days after the movies release. The illegal copies are then mass-produced for global online distribution. Therefore, the most urgent research requirement is the need for theatrical content protection and online copy control. Watermarking can also be used in the applications of content filtering as well as online location of the illegal content.

There are some important requirements that must be considered during the design of a digital image and video watermarking algorithm. This paper presents a survey of both 2D and 3D video watermarking techniques with the aim of addressing these requirements. It is clear that there has been a significant volume of research on 2D image and video watermarking reported in the literature over the past two decades. Although these efforts undoubtedly form a strong foundation for various watermarking techniques, imperceptible and robust watermarking still remains a challenging issue.

As the HVS has less sensitivity to chrominance distortion than luminance distortion, watermark embedding in the chrominance channel achieves a watermark more robust to geometric distortion and compression while still maintaining visual imperceptibility. However, it is evident from the literature that most watermarking techniques consider the luminance channel for embedding the watermark. The visual qualities of most watermarking techniques are evaluated using an objective test, such as the peak signal to noise ratio (PSNR). It often does not reflect the true perceptual quality of a video's content due to the non-linear behavior of the HVS although it is claimed that high-quality watermarked videos are obtained in terms of the PSNR. However, depending on the watermark embedding channel or region of a frame, the effect of the watermark might be visible to the HVS. Therefore, the standard committees of the MPEG and JPEG rely solely on subjective tests when evaluating candidate compression algorithms. Although a few researchers evaluated the quality of their techniques in terms of subjective testing,

i.e., the mean opinion score (MOS), future techniques should consider using only this quality assessment metric. The recommendations of the International Telecommunication Union-Radiocommunication (ITU-R) to use the subjective methods to assess 2D and 3D videos can be found in [253] and [254] respectively. While techniques which quantify a watermark's imperceptibility based on subjective testing use a display monitor or projector screen, further research could use a wide-screen theater-grade laboratory setup. Such an extensive field trial is critical for the target market as any hint of a watermark appearing during the showing of a watermarked movie in a theater would mean poor customer satisfaction.

In the literature, the different types of domains, such as spatial, transform and compressed, used to embed a watermark have different pros and cons. Spatial domain-based watermarking techniques are simpler and more computationally efficient than the others although their performances are poor in terms of robustness to attacks. In most practical applications, video contents are stored in a compressed form due to storage limitations. Therefore, transform domain-based watermarking techniques partially decode a compressed video stream, embed the watermark in it and then re-compress it to create a watermarked video. However, as calculating raw video frames from a compressed video and compressing them again are required, these techniques are more complex and time consuming than compressed domain-based techniques. However, time complexity is not a major issue because the computing power could be significantly increased using a modern high-speed super-computer. Also, transform domain-based techniques provide more imperceptibility and robustness to attacks than both compressed and spatial domain-based techniques.

Over the past two decades, a great deal of research using the compressed domain has been conducted, with most studies focusing on existing compression standards, including MPEG-2, MPEG-4 and H.264/AVC. The latest compression standard, H.265/HEVC, is now replacing the others as it contains many advanced features. Although some researchers have embedded the watermark in the H.265/HEVC domain, as very few papers have been published, this field is relatively young. Therefore, it seems that there is a great deal of scope to explore this area for developing a watermarking technique. As the robustness of existing techniques to image or video compression are assessed using any of the existing compression methods, there is potential for further research into watermarking techniques that can deal with H.265/HEVC compression which is the next-generation compression standard.

From the beginning of the invention of image and video watermarking, research has been aimed at dealing with different challenges. However, to the best of our knowledge, there is no proposal in the literature that can fulfil all its requirements, in particular, imperceptibility, security and robustness to compression, geometric attacks, downscaling to an arbitrary resolution and camcording. The DT CWT possesses approximate shift invariance and good directional selectivity properties which are not found in other transforms, such as the DFT, DCT and DWT. These properties of the DT CWT help to achieve robustness to geometric attacks. Although the work proposed in [76] and [225] and some other proposals in the literature have been conducted using the DT CWT to address these issues, there is scope for further improving its performance in relation to this attack. Some researchers consider that machine-learning techniques can also be used to improve the watermark detection rate. This technique allows prediction from past behaviour or desired observations. As most of the machine learning based approaches [255]–[257] in the literature embed the watermark into images only, there is also scope to adapt this approach for improved video watermarking algorithms.

While, in the literature, digital video watermarking research considers only the laboratory environment. For example, a watermarked video is captured from a small monitor or TV screen to assess the performance of techniques in terms of camcording, a real-world setup adds some extra challenges and difficulties. However, evaluations could be conducted in a large-screen movie theater to investigate the feasibility of these methods. The performance of the watermark decoder can also be evaluated at an ISP while the watermarked contents are monitored. This should be a tailored experiment with a known server, clients and contents to ensure that it is as transparent as possible to existing customers of the particular ISP.

Most techniques in the literature belong to 2D image and video watermarking while 3D versions receive less attention. With the increasing popularity of 3DTVs, protecting 3D videos from illegal distribution is also becoming important. In existing stereoscopic watermarking techniques, researchers have tried to protect either the left or right view while avoiding the other one although copyright protection for an individual view is required. Therefore, there is room in this field to further improve the performances of these techniques. With the advent of DIBR and IBR, a viewer can easily select the viewing angle and position of a multi-view video in FTV. Although generating a multi-view video using DIBR and IBR systems is still under investigation, designing watermarking techniques for it could be a future research topic.

Video signals are usually always tied to their corresponding audio signals. In the case of a music video, the audio track might be extracted from the video signal to use for the other purposes. Therefore it is important to preserve the copyright ownership of both the audio and video components. A few proposals in the literature [165], [258], [259] jointly process these components, but there is scope for future work on these multimodal watermarking techniques.

VIII. Summary and Conclusion

In this paper, we surveyed digital watermarking techniques for both 2D and 3D video contents. Firstly, an overview of digital video watermarking applications and their challenges, such as the imperceptibility and security of a watermark, blind detection and robustness to attacks was provided. In the literature, a great deal of work has been undertaken by researchers to develop a digital image or video watermarking algorithm that deals with these issues. The watermark embedding techniques were classified based on the domain in which they embedded the watermark, including compressed, spatial and

transform. Each technique was discussed in detail and some existing works related to them were then reviewed. Transform domain watermarking techniques were considered to be robust, stable and provide more imperceptibility than spatial and compressed domain-based approaches. We also discussed geometric-invariant watermarking techniques and surveyed relevant studies. An overview of image-based representations of 3D videos, including stereoscopic, DIBR and multi-view, was provided and some related works were reviewed. In the final part of this paper, an overall discussion of this study and recommendations for future research were presented.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions, which helped a lot in improving the quality of the paper.

REFERENCES

[1] E. Smith and L. A. E. Schuker, "Studios unlock DVD release dates," *Wall Street J.*, Feb. 2010.
[2] J. D. Koch, M. D. Smith, and R. Telang, "Camcording and film piracy in Asia–Pacific economic cooperation economies," Int. Intell. Property Inst., Washington, DC, USA, Tech. Rep., Aug. 2011.
[3] B. Stelter and B. Stone, "Digital pirates winning battle with studios," *New York Times*, Feb. 2009.
[4] *Economic Consequences of Movie Piracy—Australia*, The Media, Content Technol. Res. Specialists, Ipsos MediaCT, Australia, Jan. 2011.
[5] A. Piva, F. Bartolini, and M. Barni, "Managing copyright in open networks," *IEEE Internet Comput.*, vol. 6, no. 3, pp. 18–26, May 2002.
[6] C.-S. Lu and H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Trans. Image Process.*, vol. 10, no. 10, pp. 1579–1592, Oct. 2001.
[7] C.-S. Lu, S.-K. Huang, C.-J. Sze, and H.-Y. M. Liao, "Cocktail watermarking for digital image protection," *IEEE Trans. Multimedia*, vol. 2, no. 4, pp. 209–224, Dec. 2000.
[8] (Dec. 23, 2003). *Steganography*. [Online]. Available: http://en.wikipedia.org/wiki/Steganography
[9] N. Terzija, "Robust digital image watermarking algorithms for copyright protection," Ph.D. dissertation, Faculty Eng., Univ. Duisburg-Essen, Duisburg, Germany, Oct. 2006.
[10] C. I. Podilchuk and E. J. Delp, "Digital watermarking: Algorithms and applications," *IEEE Signal Process. Mag.*, vol. 18, no. 4, pp. 33–46, Jul. 2001.
[11] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data. A state-of-the-art overview," *IEEE Signal Process. Mag.*, vol. 17, no. 5, pp. 20–46, Sep. 2000.
[12] G. Doërr and J. L. Dugelay, "A guide tour of video watermarking," *Signal Process., Image Commun.*, vol. 18, no. 4, pp. 263–282, Apr. 2003.
[13] E. I. Lin, A. M. Eskicioglu, R. L. Lagendijk, and E. J. Delp, "Advances in digital video content protection," *Proc. IEEE*, vol. 93, no. 1, pp. 171–183, Jan. 2005.
[14] T. Stutz and A. Uhl, "A survey of H.264 AVC/SVC encryption," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 22, no. 3, pp. 325–339, Mar. 2012.
[15] Y. Tew and K. Wong, "An overview of information hiding in H.264/AVC compressed video," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 24, no. 2, pp. 305–319, Feb. 2014.
[16] A. Smolic *et al.*, "Coding algorithms for 3DTV—A survey," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 11, pp. 1606–1621, Nov. 2007.
[17] P. Bassia, I. Pitas, and N. Nikolaidis, "Robust audio watermarking in the time domain," *IEEE Trans. Multimedia*, vol. 3, no. 2, pp. 232–241, Jun. 2001.
[18] M. D. Swanson, B. Zhu, A. H. Tewfik, and L. Boney, "Robust audio watermarking using perceptual masking," *Signal Process.*, vol. 66, no. 3, pp. 337–355, 1998.
[19] B. Lei, I. Y. Soon, and E.-L. Tan, "Robust SVD-based audio watermarking scheme with differential evolution optimization," *IEEE Trans. Audio, Speech, Language Process.*, vol. 21, no. 11, pp. 2368–2378, Nov. 2013.
[20] Y. Erfani, R. Pichevar, and J. Rouat, "Audio watermarking using spikegram and a two-dictionary approach," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 4, pp. 840–852, Apr. 2017.
[21] X. Tang, Z. Ma, X. Niu, and Y. Yang, "Robust audio watermarking algorithm based on empirical mode decomposition," *Chin. J. Electron.*, vol. 25, no. 6, pp. 1005–1010, 2016.
[22] R. Li, S. Xu, and H. Yang, "Spread spectrum audio watermarking based on perceptual characteristic aware extraction," *IET Signal Process.*, vol. 10, no. 3, pp. 266–273, 2016.
[23] Y. Xiang, I. Natgunanathan, Y. Rong, and S. Guo, "Spread spectrum-based high embedding capacity watermarking method for audio signals," *IEEE/ACM Trans. Audio, Speech, Language Process.*, vol. 23, no. 12, pp. 2228–2237, Dec. 2015.
[24] M. Fallahpour and D. Megías, "Audio watermarking based on Fibonacci numbers," *IEEE/ACM Trans. Audio, Speech, Language Process.*, vol. 23, no. 8, pp. 1273–1282, Aug. 2015.
[25] G. Hua, J. Goh, and V. L. L. Thing, "Time-spread echo-based audio watermarking with optimized imperceptibility and robustness," *IEEE/ACM Trans. Audio, Speech, Language Process.*, vol. 23, no. 2, pp. 227–239, Feb. 2015.
[26] H. J. Kim and Y. H. Choi, "A novel echo-hiding scheme with backward and forward kernels," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 885–889, Aug. 2003.
[27] Z. Liu and A. Inoue, "Audio watermarking techniques using sinusoidal patterns based on pseudorandom sequences," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 801–812, Aug. 2003.
[28] G. Hua, J. Huang, Y. Q. Shi, J. Goh, and V. L. L. Thing, "Twenty years of digital audio watermarking—A comprehensive review," *Signal Process.*, vol. 128, pp. 222–242, Nov. 2016.
[29] M. Zakariah, M. K. Khan, and H. Malik, "Digital multimedia audio forensics: Past, present and future," *Multimedia Tools Appl.*, pp. 1–32, Jan. 2017.
[30] S. P. S. Chauhan and S. A. M. Rizvi, "A survey: Digital audio watermarking techniques and applications," in *Proc. Int. Conf. Comput. Commun. Technol.*, Sep. 2013, pp. 185–192.
[31] J. Bajpai and A. Kaur, "A literature survey—Various audio watermarking techniques and their challenges," in *Proc. Int. Conf.-Cloud Syst. Big Data Eng. (Confluence)*, Jan. 2016, pp. 451–457.
[32] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proc. IEEE*, vol. 87, no. 7, pp. 1079–1107, Jul. 1999.
[33] I. J. Cox and M. L. Miller, "Review of watermarking and the importance of perceptual modeling," *Proc. SPIE*, vol. 3016, pp. 92–99, Jun. 1997.
[34] I. J. Cox, M. L. Miller, and J. A. Bloom, "Watermarking applications and their properties," in *Proc. Int. Conf. Inf. Technol., Coding Comput.*, 2000, pp. 6–10.
[35] C. D. Vleeschouwer, J. F. Delaigle, and B. Macq, "Invisibility and application functionalities in perceptual watermarking an overview," *Proc. IEEE*, vol. 90, no. 1, pp. 64–77, Jan. 2002.
[36] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies," *Proc. IEEE*, vol. 86, no. 6, pp. 1064–1087, Jun. 1998.
[37] G. Voyatzis, N. Nikolaidis, and I. Pitas, "Digital watermarking: An overview," in *Proc. Eur. Signal Process. Conf.*, Sep. 1998, pp. 13–16.
[38] I. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. San Francisco, CA, USA: Morgan Kaufmann, 2002.
[39] M. Barni, I. J. Cox, T. Kalker, and H. J. Kim, "Digital watermarking," in *Proc. Int. Workshop Digit. Watermarking*, Sep. 2005, pp. 1–483.
[40] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—A survey," *Proc. IEEE*, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.
[41] I. A. Nasir and A. B. Abdurrman, "A robust color image watermarking scheme based on image normalization," in *Proc. World Congr. Eng.*, vol. 3. Jul. 2013, pp. 1–6.
[42] Y. Wang, J. Ostermann, and Y.-Q. Zhang, "Video compression standards," in *Video Processing and Communications*. Englewood Cliffs, NJ, USA: Prentice-Hall, Sep. 2011.
[43] Y. Wang, J. Ostermann, and Y.-Q. Zhang, "Video formation, perception, and representation," in *Video Processing and Communications*. Englewood Cliffs, NJ, USA: Prentice-Hall, Sep. 2011.
[44] P. Comesaña, L. Pérez-Freire, and F. Pérez-González, "Fundamentals of data hiding security and their application to spread-spectrum analysis," in *Information Hiding* (Lecture Notes in Computer Science), vol. 3727. Berlin, Germany: Springer, 2005, pp. 146–160.
[45] P. Bas and F. Cayre, "Achieving subspace or key security for WOA using natural or circular watermarking," in *Proc. Workshop Multimedia Security*, 2006, pp. 80–88.

[46] G. Doërr and J.-L. Dugelay, "Security pitfalls of frame-by-frame approaches to video watermarking," *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 2955–2964, Oct. 2004.

[47] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security part one: Theory," *Proc. SPIE*, vol. 5681, pp. 746–757, Mar. 2005.

[48] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: Theory and practice," *IEEE Trans. Signal Process.*, vol. 53, no. 10, pp. 3976–3987, Oct. 2005.

[49] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security part two: Practice," *Proc. SPIE*, vol. 5681, pp. 758–767, Mar. 2005.

[50] F. Hartung, J. K. Su, and B. Girod, "Spread spectrum watermarking: Malicious attacks and counterattacks," *Proc. SPIE*, vol. 3657, pp. 147–158, Apr. 1999.

[51] M. J. Holliman, W. W. Macy, and M. M. Yeung, "Robust frame-dependent video watermarking," *Proc. SPIE*, vol. 3971, pp. 186–197, May 2000.

[52] G. Doërr, "Security issue and collusion attacks in video watermarking," Ph.D. dissertation, School Inf. Commun. Sci. Technol., Univ. Nice Sophia Antipolis, Nice, France, Jun. 2005.

[53] H. Mirza, H. Thai, and Z. Nakao, "Digital video watermarking based on RGB color channels and principal component analysis," in *Int. Conf. Knowledge-Based Intelligent Inform. Eng. Syst.*, Berlin, Germany: Springer, 2008, pp. 125–132.

[54] K. Miyara, T. D. Hien, H. Harrak, Y. Nagata, and Z. Nakao, "Multichannel color image watermarking using PCA eigenimages," in *Intelligent Information Processing and Web Mining* (Advances in Soft Computing), vol. 35. Berlin, Germany: Springer, 2006, pp. 287–296.

[55] M. Barni, F. Bartolini, and A. Piva, "Multichannel watermarking of color images," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 12, no. 3, pp. 142–156, Mar. 2002.

[56] P. Tsai, Y.-C. Hu, and C.-C. Chang, "A color image watermarking scheme based on color quantization," *Signal Process.*, vol. 84, no. 1, pp. 95–106, Jan. 2004.

[57] N. V. Dharwadkar and B. B. Amberker, "Secure watermarking scheme for color image using intensity of pixel and LSB substitution," *J. Comput.*, vol. 1, no. 1, pp. 1–6, Dec. 2009.

[58] V. Saxena, P. Khemka, A. Harsulkar, and J. Gupta, "Performance analysis of color channel for DCT based image watermarking scheme," *Int. J. Secur. Appl.*, vol. 1, no. 2, pp. 41–47, Oct. 2007.

[59] C.-H. Chou and K.-C. Liu, "A perceptually tuned watermarking scheme for color images," *IEEE Trans. Image Process.*, vol. 19, no. 11, pp. 2966–2982, Nov. 2010.

[60] Y. He, W. Liang, J. Liang, and M. Pei, "Tensor decomposition-based color image watermarking," *Proc. SPIE*, vol. 9069, pp. 90690U-1–90690U-6, Jan. 2014.

[61] M. R. A. Lari, S. Ghofrani, and D. McLernon, "Using curvelet transform for watermarking based on amplitude modulation," *Signal, Image Video Process.*, vol. 8, no. 4, pp. 687–697, May 2014.

[62] S. A. M. Gilani, I. Kostopoulos, and A. N. Skodras, "Color image-adaptive watermarking," in *Proc. Int. Conf. Digit. Signal Process.*, vol. 2. 2002, pp. 721–724.

[63] A. Karmakar, A. Phadikar, and A. Mukherjee, "Video watermarking scheme resistant to rotation and collusion attacks," in *Emerging Trends in Computing and Communication* (Lecture Notes in Electrical Engineering), vol. 298. Berlin, Germany: Springer, Feb. 2014, pp. 95–101.

[64] M.-J. Lee, D.-H. Im, H.-Y. Lee, K.-S. Kim, and H.-K. Lee, "Real-time video watermarking system on the compressed domain for high-definition video contents: Practical issues," *Digit. Signal Process.*, vol. 22, no. 1, pp. 190–198, Jan. 2012.

[65] Z. Dawei, C. Guanrong, and L. Wenbo, "A chaos-based robust wavelet-domain watermarking algorithm," *Chaos Solitons Fractals*, vol. 22, no. 1, pp. 47–54, Oct. 2004.

[66] W. Kong, B. Yang, D. Wu, and X. Niu, "SVD based blind video watermarking algorithm," in *Proc. Int. Conf. Innov. Comput., Inf. Control*, vol. 1. Aug./Sep. 2006, pp. 265–268.

[67] H.-Y. Huang, C.-H. Yang, and W.-H. Hsu, "A video watermarking technique based on pseudo-3-D DCT and quantization index modulation," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 4, pp. 625–637, Dec. 2010.

[68] P. Bao and X. Ma, "Image adaptive watermarking using wavelet domain singular value decomposition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 15, no. 1, pp. 96–102, Jan. 2005.

[69] M. Kutter and S. Winkler, "A vision-based masking model for spread-spectrum image watermarking," *IEEE Trans. Image Process.*, vol. 11, no. 1, pp. 16–25, Jan. 2002.

[70] A. Koz and A. A. Alatan, "Oblivious spatio-temporal watermarking of digital video by exploiting the human visual system," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 3, pp. 326–337, Mar. 2008.

[71] A. M. Reed and B. T. Hannigan, "Adaptive color watermarking," *Proc. SPIE*, vol. 4675, pp. 222–229, Apr. 2002.

[72] N. Kingsbury. (Jun. 8, 2005). Human vision. Connexions. [Online]. Available: http://cnx.org/content/m11084/latest/

[73] C. A. Párraga, G. Brelstaff, T. Troscianko, and I. R. Moorhead, "Color and luminance information in natural scenes," *J. Opt. Soc. Amer. A, Opt. Image Sci.*, vol. 15, no. 3, pp. 563–569, Mar. 1998.

[74] M. Asikuzzaman, M. J. Alam, A. J. Lambert, and M. R. Pickering, "A blind digital video watermarking scheme with enhanced robustness to geometric distortion," in *Proc. Int. Conf. Digit. Image Comput. Techn. Appl.*, Dec. 2012, pp. 1–8.

[75] M. Asikuzzaman, M. J. Alam, A. J. Lambert, and M. R. Pickering, "A blind high definition videowatermarking scheme robust to geometric and temporal synchronization attacks," in *Proc. IEEE Vis. Commun. Image Process.*, Nov. 2013, pp. 1–6.

[76] M. Asikuzzaman, M. J. Alam, A. J. Lambert, and M. R. Pickering, "Imperceptible and robust blind video watermarking using chrominance embedding: A set of approaches in the DT CWT domain," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 9, pp. 1502–1517, Sep. 2014.

[77] M. Asikuzzaman, M. J. Alam, A. J. Lambert, and M. R. Pickering, "A blind and robust video watermarking scheme using chrominance embedding," in *Proc. Int. Conf. Digit. Image Comput., Techn. Appl.*, Nov. 2014, pp. 1–6.

[78] M. Asikuzzaman, M. J. Alam, and M. R. Pickering, "A blind and robust video watermarking scheme in the DT CWT and SVD domain," in *Proc. Picture Coding Symp.*, May 2015, pp. 277–281.

[79] D. Choi, H. Do, H. Choi, and T. Kim, "A blind MPEG-2 video watermarking robust to camcorder recording," *Signal Process.*, vol. 90, no. 4, pp. 1327–1332, Apr. 2010.

[80] K. Surachat and T. Amornraksa, "Pixel-wise based digital watermarking using Weiner filter in chrominance channel," in *Proc. Int. Symp. Commun. Inf. Technol.*, Sep. 2009, pp. 887–892.

[81] K. Surachat and T. Amornraksa, "Pixel-wise based digital watermarking using mean filter in chrominance channel," in *Proc. Int. Symp. Intell. Signal Process. Commun. Syst.*, Jan. 2009, pp. 525–528.

[82] J. Zhou, W. Sun, L. Dong, X. Liu, O. C. Au, and Y. Y. Tang, "Secure reversible image data hiding over encrypted domain via key modulation," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 26, no. 3, pp. 441–452, Mar. 2016.

[83] H.-Z. Wu, Y.-Q. Shi, H.-X. Wang, and L.-N. Zhou, "Separable reversible data hiding for encrypted palette images with color partitioning and flipping verification," *IEEE Trans. Circuits Syst. Video Technol.*, doi: 10.1109/TCSVT.2016.2556585.

[84] W. Zhang, H. Wang, D. Hou, and N. Yu, "Reversible data hiding in encrypted images by reversible image transformation," *IEEE Trans. Multimedia*, vol. 18, no. 8, pp. 1469–1479, Aug. 2016.

[85] *Information Technology—Generic Coding of Moving Pictures and Associated Audio Information: Video*, document ISO/IEC 13818-2, International Organization for Standardization, 2000.

[86] *Information Technology—Coding of Audio-Visual Objects: Video*, document ISO/IEC 14496-2, International Organization for Standardization, 1998.

[87] T. Wiegand, G. J. Sullivan, G. Bjøntegaard, and A. Luthra, "Overview of the H.264/AVC video coding standard," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 7, pp. 560–576, Jul. 2003.

[88] G. J. Sullivan, J.-R. Ohm, W.-J. Han, and T. Wiegand, "Overview of the High Efficiency Video Coding (HEVC) standard," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 22, no. 12, pp. 1649–1668, Dec. 2012.

[89] C. S. Lu, J.-R. Chen, and K.-C. Fan, "Real-time frame-dependent video watermarking in VLC domain," *Signal Process., Image Commun.*, vol. 20, no. 7, pp. 624–642, Aug. 2005.

[90] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," *Signal Process.*, vol. 66, no. 3, pp. 283–301, May 1998.

[91] T.-Y. Chung, M.-S. Hong, Y.-N. Oh, D.-H. Shin, and S.-H. Park, "Digital watermarking for copyright protection of MPEG2 compressed video," *IEEE Trans. Consum. Electron.*, vol. 44, no. 3, pp. 895–901, Aug. 1998.

[92] S. Biswas, S. R. Das, and E. M. Petriu, "An adaptive compressed MPEG-2 video watermarking scheme," *IEEE Trans. Instrum. Meas.*, vol. 54, no. 5, pp. 1853–1861, Oct. 2005.

[93] Y. Wang and A. Pearmain, "Blind MPEG-2 video watermarking robust against geometric attacks: A set of approaches in DCT domain," *IEEE Trans. Image Process.*, vol. 15, no. 6, pp. 1536–1543, Jun. 2006.

[94] M. Celik, J. Talstra, A. Lemma, and S. Katzenbeisser, "Camcorder capture robust low-complexity watermarking of MPEG-2 bitstreams," in *Proc. IEEE Int. Conf. Image Process.*, vol. 5. Sep. 2007, pp. 489–492.

[95] A. M. Alattar, E. T. Lin, and M. U. Celik, "Digital watermarking of low bit-rate advanced simple profile MPEG-4 compressed video," *IEEE Trans. Circuits Syst. for Video Technol.*, vol. 13, no. 8, pp. 787–800, Aug. 2003.

[96] M. Yong, T. Yu-Min, and Q. Yun-Hui, "Adaptive video watermarking algorithm based on MPEG-4 streams," in *Proc. Int. Conf. Control, Autom., Robot. Vis.*, Dec. 2008, pp. 1084–1088.

[97] M. Barni, F. Bartolini, and N. Checcacci, "Watermarking of MPEG-4 video objects," *IEEE Trans. Multimedia*, vol. 7, no. 1, pp. 23–32, Feb. 2005.

[98] N. V. Boulgouris, F. D. Koravos, and M. G. Strintzis, "Self-synchronizing watermark detection for MPEG-4 objects," in *Proc. 8th IEEE Int. Conf. Electron., Circuits Syst. (ICECS)*, vol. 3. Sep. 2001, pp. 1371–1374.

[99] C.-S. Lu and H.-Y. M. Liao, "Video object-based watermarking: A rotation and flipping resilient scheme," in *Proc. Int. Conf. Image Process.*, vol. 2. Oct. 2001, pp. 483–486.

[100] M. Noorkami and R. M. Mersereau, "A framework for robust watermarking of h.264-encoded video with controllable detection performance," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 1, pp. 14–23, Mar. 2007.

[101] D. Xu, R. Wang, and J. Wang, "A novel watermarking scheme for H.264/AVC video authentication," *Signal Process., Image Commun.*, vol. 26, no. 6, pp. 267–279, Jul. 2011.

[102] A. Mansouri, A. M. Aznaveh, F. T. Azar, and F. Kurugollu, "A low complexity video watermarking in H.264 compressed domain," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 4, pp. 649–657, Dec. 2010.

[103] P.-C. Su, C.-S. Wu, I.-F. Chen, C.-Y. Wu, and Y.-C. Wu, "A practical design of digital video watermarking in H.264/AVC for content authentication," *Signal Process., Image Commun.*, vol. 26, nos. 8–9, pp. 413–426, Oct. 2011.

[104] J. Zhang, A. T. S. Ho, G. Qiu, and P. Marziliano, "Robust video watermarking of H.264/AVC," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 54, no. 2, pp. 205–209, Feb. 2007.

[105] Y. Cao, X. Zhao, and D. Feng, "Video steganalysis exploiting motion vector reversion-based features," *IEEE Signal Process. Lett.*, vol. 19, no. 1, pp. 35–38, Jan. 2012.

[106] H. A. Aly, "Data hiding in motion vectors of compressed video based on their associated prediction error," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 14–18, Mar. 2011.

[107] Y. Guo and F. Pan, "Information hiding for H.264 in video stream switching application," in *Proc. IEEE Int. Conf. Inf. Theory Inf. Secur.*, Dec. 2010, pp. 419–421.

[108] X. Jiang, T. Sun, Y. Zhou, W. Wang, and Y.-Q. Shi, "A robust H.264/AVC video watermarking scheme with drift compensation," *Sci. World J.*, vol. 2014, Feb. 2014, Art. no. 802347.

[109] D. Xu, R. Wang, and Y. Q. Shi, "Data hiding in encrypted H.264/AVC video streams by codeword substitution," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 596–606, Apr. 2014.

[110] X. Ma, Z. Li, H. Tu, and B. Zhang, "A data hiding algorithm for H.264/AVC video streams without intra-frame distortion drift," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 20, no. 10, pp. 1320–1330, Oct. 2010.

[111] D. Pröfrock, H. Richter, M. Schlauweg, and E. Müller, "H.264/AVC video authentication using skipped macroblocks for an erasable watermark," *Proc. SPIE*, vol. 5960, pp. 1480–1489, Jun. 2005.

[112] J. R. Ohm, G. J. Sullivan, H. Schwarz, T. K. Tan, and T. Wiegand, "Comparison of the coding efficiency of video coding standards—Including High Efficiency Video Coding (HEVC)," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 22, no. 12, pp. 1669–1684, Dec. 2012.

[113] S. Swati, K. Hayat, and Z. Shahid, "A watermarking scheme for High Efficiency Video Coding (HEVC)," *PLoS ONE*, vol. 9, no. 8, p. e105613, 2014.

[114] Y. Tew and K. Wong, "Information hiding in HEVC standard using adaptive coding block size decision," in *Proc. IEEE Int. Conf. Image Process.*, Oct. 2014, pp. 5502–5506.

[115] K. Ogawa and G. Ohtake, "Watermarking for HEVC/H.265 stream," in *Proc. IEEE Int. Conf. Consum. Electron.*, Jan. 2015, pp. 102–103.

[116] Y. Tew, K. Wong, and R. C.-W. Phan, "HEVC video authentication using data embedding technique," in *Proc. IEEE Int. Conf. Image Process.*, Sep. 2015, pp. 1265–1269.

[117] T. Dutta and H. P. Gupta, "A robust watermarking framework for High Efficiency Video Coding (HEVC)—Encoded video with blind extraction process," *J. Vis. Commun. Image Represent.*, vol. 38, pp. 29–44, Jul. 2016.

[118] Y. K. Lee and L. H. Chen, "High capacity image steganographic model," *IEE Proc.-Vis., Image Signal Process.*, vol. 147, no. 3, pp. 288–294, Jun. 2000.

[119] E. T. Lin and E. J. Delp, "A review of data hiding in digital images," in *Proc. Image Process., Image Quality, Image Capture Syst. Conf.*, 1999, pp. 274–278.

[120] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," *IEEE Trans. Image Process.*, vol. 14, no. 2, pp. 253–266, Feb. 2005.

[121] S. Kimpan, A. Lasakul, and S. Chitwong, "Variable block size based adaptive watermarking in spatial domain," in *Proc. IEEE Int. Symp. Commun. Inf. Technol.*, vol. 1. Oct. 2004, pp. 374–377.

[122] V. Darmstaedter, J.-F. Delaigle, J. J. Quisquater, and B. Macq, "Low cost spatial watermarking," *Comput. Graph.*, vol. 22, no. 4, pp. 417–424, Aug. 1998.

[123] P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," *IEEE Trans. Image Process.*, vol. 10, no. 10, pp. 1593–1601, Oct. 2001.

[124] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Syst. J.*, vol. 35, nos. 3–4, pp. 313–336, 1996.

[125] I.-K. Yeo and H. J. Kim, "Generalized patchwork algorithm for image watermarking," *Multimedia Syst.*, vol. 9, no. 3, pp. 261–265, Sep. 2003.

[126] H. S. Kim and H.-K. Lee, "Invariant image watermark using Zernike moments," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 766–775, Aug. 2003.

[127] J. S. Seo and C. D. Yoo, "Image watermarking based on invariant regions of scale-space representation," *IEEE Trans. Signal Process.*, vol. 54, no. 4, pp. 1537–1549, Apr. 2006.

[128] J.-S. Tsai, W.-B. Huang, and Y.-H. Kuo, "On the selection of optimal feature region set for robust digital image watermarking," *IEEE Trans. Image Process.*, vol. 20, no. 3, pp. 735–743, Mar. 2011.

[129] A. Nikolaidis and I. Pitas, "Robust watermarking of facial images based on salient geometric pattern matching," *IEEE Trans. Multimedia*, vol. 2, no. 3, pp. 172–184, Sep. 2000.

[130] P. Bas, J. M. Chassery, and B. Macq, "Geometrically invariant watermarking using feature points," *IEEE Trans. Image Process.*, vol. 11, no. 9, pp. 1014–1028, Sep. 2002.

[131] C.-W. Tang and H.-M. Hang, "A feature-based robust digital image watermarking scheme," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 950–959, Apr. 2003.

[132] R. Thanki and K. Borisagar, "A technical review of digital image watermarking techniques," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 3, no. 5, pp. 1290–1299, May 2013.

[133] K. S. Dhaliwal and R. Kaur, "Comparative study of single watermarking to multiple watermarking over a color image new," *Int. J. Latest Trends Eng. Technol.*, vol. 2, no. 2, pp. 43–48, Mar. 2013.

[134] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[135] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT-domain system for robust image watermarking," *Signal Process.*, vol. 66, no. 3, pp. 357–372, May 1998.

[136] Z.-M. Lu, H.-Y. Zheng, and J.-W. Huang, "A digital watermarking scheme based on DCT and SVD," in *Proc. Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, vol. 1. Nov. 2007, pp. 241–244.

[137] S. P. Mohanty, N. Ranganathan, and R. K. Namballa, "VLSI implementation of invisible digital watermarking algorithms towards the development of a secure jpeg encoder," in *Proc. IEEE Workshop Signal Process. Syst.*, Aug. 2003, pp. 183–188.

[138] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Trans. Multimedia*, vol. 4, no. 1, pp. 121–128, Mar. 2002.

[139] C.-C. Lai and C.-C. Tsai, "Digital image watermarking using discrete wavelet transform and singular value decomposition," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 11, pp. 3060–3063, Nov. 2010.

[140] N. M. Makbol and B. E. Khoo, "A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition," *Digital Signal Process.*, vol. 33, no. 10, pp. 134–147, Oct. 2014.

[141] S. Dogan, T. Tuncer, E. Avci, and A. Gulten, "A robust color image watermarking with singular value decomposition method," *Adv. Eng. Softw.*, vol. 42, no. 6, pp. 336–346, Jun. 2011.

[142] J. M. Guo and H. Prasetyo, "Security analyses of the watermarking scheme based on redundant discrete wavelet transform and singular value decomposition," *AEU-Int. J. Electron. Commun.*, vol. 68, no. 9, pp. 816–834, Sep. 2014.
[143] Y. Wu, "On the security of an SVD-based ownership watermarking," *IEEE Trans. Multimedia*, vol. 7, no. 4, pp. 624–627, Aug. 2005.
[144] X.-P. Zhang and K. Li, "Comments on 'an SVD-based watermarking scheme for protecting rightful ownership,"' *IEEE Trans. Multimedia*, vol. 7, no. 3, pp. 593–594, Jun. 2005.
[145] R. Gonzalez and R. Woods, *Digital Image Processing*. Englewood Cliffs, NJ, USA: Prentice-Hall, 2002.
[146] R. Bracewell, *The Fourier Transform and Its Applications*. New York, NY, USA: McGraw-Hill, 2000.
[147] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, and Y. M. Lui, "Rotation, scale, and translation resilient watermarking for images," *IEEE Trans. Image Process.*, vol. 10, no. 5, pp. 767–782, May 2001.
[148] D. Zheng, J. Zhao, and A. E. Saddik, "RST-invariant digital image watermarking based on log-polar mapping and phase correlation," *IEEE Trans. Circuits Syst. for Video Technol.*, vol. 13, no. 8, pp. 753–765, Aug. 2003.
[149] X. Kang, J. Huang, Y. Q. Shi, and Y. Lin, "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 776–786, Aug. 2003.
[150] Q. Cheng and T. S. Huang, "Robust optimum detection of transform domain multiplicative watermarks," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 906–924, Apr. 2003.
[151] M. Ramkumar and A. N. Akansu, "On the design of data hiding methods robust to lossy compression," *IEEE Trans. Multimedia*, vol. 6, no. 6, pp. 947–951, Dec. 2004.
[152] W. Lu, H. Lu, and F.-L. Chung, "Feature based robust watermarking using image normalization," *Comput. Elect. Eng.*, vol. 36, no. 1, pp. 2–18, Jan. 2010.
[153] V. Solachidis and L. Pitas, "Circularly symmetric watermark embedding in 2-D DFT domain," *IEEE Trans. Image Process.*, vol. 10, no. 11, pp. 1741–1753, Nov. 2001.
[154] C.-F. Wu and W.-S. Hsieh, "Digital watermarking using zerotree of DCT," *IEEE Trans. Consum. Electron.*, vol. 46, no. 1, pp. 87–94, Feb. 2000.
[155] S. D. Roy, X. Li, Y. Shoshan, A. Fish, and O. Yadid-Pecht, "Hardware implementation of a digital watermarking system for video authentication," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 23, no. 2, pp. 289–301, Feb. 2013.
[156] J. R. Hernandez, M. Amado, and F. Perez-Gonzalez, "DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure," *IEEE Trans. Image Process.*, vol. 9, no. 1, pp. 55–68, Jan. 2000.
[157] C.-T. Hsu and J.-L. Wu, "Hidden digital watermarks in images," *IEEE Trans. Image Process.*, vol. 8, no. 1, pp. 58–68, Jan. 1999.
[158] W. C. Chu, "DCT-based image watermarking using subsampling," *IEEE Trans. Multimedia*, vol. 5, no. 1, pp. 34–38, Mar. 2003.
[159] H. Ling, L. Wang, and F. Zou, "Real-time video watermarking scheme resistant to geometric distortions," *J. Electron. Imaging*, vol. 20, no. 1, pp. 013025-1–013025-14, Jan. 2011.
[160] A. Cedillo-Hernandez, M. Cedillo-Hernandez, M. Garcia-Vazquez, M. Nakano-Miyatake, H. Perez-Meana, and A. Ramirez-Acosta, "Transcoding resilient video watermarking scheme based on spatio-temporal HVS and DCT," *Signal Process.*, vol. 97, pp. 40–54, Apr. 2014.
[161] C.-T. Hsu and J.-L. Wu, "DCT-based watermarking for video," *IEEE Trans. Consum. Electron.*, vol. 44, no. 1, pp. 206–216, Feb. 1998.
[162] T. M. Thanh, P. T. Hiep, T. M. Tam, and K. Tanaka, "Robust semi-blind video watermarking based on frame-patch matching," *AEU-Int. J. Electron. Commun.*, vol. 68, no. 10, pp. 1007–1015, Oct. 2014.
[163] S. D. Lin and C.-F. Chen, "A robust DCT-based watermarking for copyright protection," *IEEE Trans. Consum. Electron.*, vol. 46, no. 3, pp. 415–421, Aug. 2000.
[164] P. F. Alcantarilla, A. Bartoli, and A. J. Davison, "KAZE features," in *Proc. Eur. Conf. Computer Vision*, vol. 7577. Berlin, Germany: Springer, 2012, pp. 214–227.
[165] P. W. Chan, M. R. Lyu, and R. T. Chin, "A novel scheme for hybrid digital video watermarking: Approach, evaluation and experimentation," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 15, no. 12, pp. 1638–1649, Dec. 2005.
[166] N. M. Makbol and B. E. Khoo, "Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition," *AEU-Int. J. Electron. Commun.*, vol. 67, no. 2, pp. 102–112, Feb. 2013.
[167] M. Amini, M. Ahmad, and M. Swamy, "A robust multibit multiplicative watermark decoder using vector-based hidden Markov model in wavelet domain," *IEEE Trans. Circuits Syst. Video Technol.*, doi: 10.1109/TCSVT.2016.2607299.
[168] G. Bhatnagar and B. Raman, "A new robust reference watermarking scheme based on DWT-SVD," *Comput. Standards Inter.*, vol. 31, no. 5, pp. 1002–1013, Sep. 2009.
[169] O. S. Faragallah, "Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain," *AEU-Int. J. Electron. Commun.*, vol. 67, no. 3, pp. 189–196, Mar. 2013.
[170] L. Wang, H. Ling, F. Zou, and Z. Lu, "Real-time compressed-domain video watermarking resistance to geometric distortions," *IEEE Multimedia Mag.*, vol. 19, no. 1, pp. 70–79, Jan. 2012.
[171] A. A. Reddy and B. N. Chatterji, "A new wavelet based logo-watermarking scheme," *Pattern Recognit. Lett.*, vol. 26, no. 7, pp. 1019–1027, May 2005.
[172] Y. Wang, J. F. Doherty, and R. E. V. Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images," *IEEE Trans. Image Process.*, vol. 11, no. 2, pp. 77–88, Feb. 2002.
[173] S.-H. Wang and Y.-P. Lin, "Wavelet tree quantization for copyright protection watermarking," *IEEE Trans. Image Process.*, vol. 13, no. 2, pp. 154–165, Feb. 2004.
[174] M. Barni, F. Bartolini, and A. Piva, "Improved wavelet-based watermarking through pixel-wise masking," *IEEE Trans. Image Process.*, vol. 10, no. 5, pp. 783–791, May 2001.
[175] L. E. Coria, M. R. Pickering, P. Nasiopoulos, and R. K. Ward, "A video watermarking scheme based on the dual-tree complex wavelet transform," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 466–474, Sep. 2008.
[176] S. G. Mallat, "A theory for multiresolution signal decomposition: The wavelet representation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 11, no. 7, pp. 674–693, Jul. 1989.
[177] N. Kingsbury, "Image processing with complex wavelets," *Philos. Trans. Roy. Soc. London A, Math., Phys. Eng. Sci.*, vol. 357, pp. 2543–2560, Sep. 1999.
[178] N. Kingsbury, "Shift invariant properties of the dual-tree complex wavelet transform," in *Proc. Int. Conf. Acoust., Speech, Signal Process.*, vol. 3. Mar. 1999, pp. 1221–1224.
[179] N. Kingsbury, "The dual-tree complex wavelet transform: A new technique for shift invariance and directional filters," in *Proc. IEEE Digit. Signal Process. Workshop*, Aug. 1998, p. 86.
[180] N. Kingsbury, "A dual-tree complex wavelet transform with improved orthogonality and symmetry properties," in *Proc. Int. Conf. Image Process.*, vol. 2. Sep. 2000, pp. 375–378.
[181] H. Ling, L. Wang, F. Zou, Z. Lu, and P. Li, "Robust video watermarking based on affine invariant regions in the compressed domain," *Signal Process.*, vol. 91, no. 8, pp. 1863–1875, Aug. 2011.
[182] P. Loo and N. Kingsbury, "Digital watermarking using complex wavelets," in *Proc. IEEE Int. Conf. Image Process.*, vol. 3. Sep. 2000, pp. 29–32.
[183] N. Terzija and W. Geisselhardt, "Digital image watermarking using complex wavelet transform," in *Proc. Workshop Multimedia Secur.*, Sep. 2004, pp. 193–198.
[184] M. Pickering, L. E. Coria, and P. Nasiopoulos, "A novel blind video watermarking scheme for access control using complex wavelets," in *Proc. Int. Conf. Consum. Electron.*, Jan. 2007, pp. 1–2.
[185] R. Kwitt, P. Meerwald, and A. Uhl, "Blind DT-CWT domain additive spread-spectrum watermark detection," in *Proc. Int. Conf. Digit. Signal Process.*, Jul. 2009, pp. 1–8.
[186] S. Mabtoul, E. Hassan, I. Elhaj, and D. Aboutajdine, "Robust color image watermarking based on singular value decomposition and dual tree complex wavelet transform," in *Proc. Int. Conf. Electron., Circuits Syst.*, Dec. 2007, pp. 534–537.
[187] J. Liu and K. She, "Robust image watermarking using dual tree complex wavelet transform based on human visual system," in *Proc. Int. Conf. Image Anal. Signal Process.*, Apr. 2010, pp. 675–679.
[188] H. A. Abdallah, M. M. Hadhoud, and A. A. Shaalan, "SVD-based watermarking scheme in complex wavelet domain for color video," in *Proc. Int. Conf. Comput. Eng. Syst.*, Dec. 2009, pp. 455–460.
[189] L. Coria, P. Nasiopoulos, R. Ward, and M. Pickering, "An access control video watermarking method that is robust to geometric distortions," in *Proc. Int. Conf. Digit. Inf. Manage.*, vol. 1. Oct. 2007, pp. 460–465.

[190] X. Tang and L. Chen, "A color video watermarking algorithm based on DTCWT and motion estimation," in *Proc. WRI Int. Conf. Commun. Mobile Comput.*, vol. 3. Jan. 2009, pp. 413–417.

[191] A. I. Thompson, A. Bouridane, and F. Kurugollu, "Spread transform watermarking for digital multimedia using the complex wavelet domain," in *Proc. ECSIS Symp. Bio-Inspired, Learn., Intell. Syst. Secur.*, Aug. 2007, pp. 123–132.

[192] S. Xiang, H. J. Kim, and J. Huang, "Invariant image watermarking based on statistical features in the low-frequency domain," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 6, pp. 777–790, Jun. 2008.

[193] X. Wang, J. Wu, and P. Niu, "A new digital image watermarking algorithm resilient to desynchronization attacks," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 4, pp. 655–663, Dec. 2007.

[194] T. Zong, Y. Xiang, I. Natgunanathan, S. Guo, W. Zhou, and G. Beliakov, "Robust histogram shape-based method for image watermarking," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 25, no. 5, pp. 717–729, May 2015.

[195] Y. Liu, "Digital video watermarking robust to geometric attacks and compressions," Ph.D. dissertation, Ottawa-Carleton Inst. Elect. Comput. Eng., School Elect. Eng. Comput. Sci., Univ. Ottawa, Ottawa, ON, Canada, Oct. 2011.

[196] M. Barni, "Effectiveness of exhaustive search and template matching against watermark desynchronization," *IEEE Signal Process. Lett.*, vol. 12, no. 2, pp. 158–161, Feb. 2005.

[197] J. F. Lichtenauer, I. Setyawan, T. Kalker, and R. L. Lagendijk, "Exhaustive geometrical search and the false positive watermark detection probability," *Proc. SPIE*, vol. 5020, pp. 203–214, Jun. 2003.

[198] P. Nguyen, R. Balter, N. Montfort, and S. Baudry, "Registration methods for nonblind watermark detection in digital cinema applications," *Proc. SPIE*, vol. 5020, pp. 553–562, Jun. 2003.

[199] H. Cheng and M. A. Isnardi, "Spatial temporal and histogram video registration for digital watermark detection," in *Proc. IEEE Int. Conf. Image Process.*, vol. 2. Sep. 2003, pp. II-735–II-738.

[200] D. Delannay, C. de Roover, and B. M. M. Macq, "Temporal alignment of video sequences for watermarking systems," *Proc. SPIE*, vol. 5020, pp. 481–492, Jun. 2003.

[201] Y. T. Lin, C. Y. Huang, and G. C. Lee, "Rotation, scaling, and translation resilient watermarking for images," *IET Image Process.*, vol. 5, no. 4, pp. 328–340, Jun. 2011.

[202] S. Pereira and T. Pun, "Robust template matching for affine resistant image watermarks," *IEEE Trans. Image Process.*, vol. 9, no. 6, pp. 1123–1129, Jun. 2000.

[203] J. J. K. O'Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Signal Process.*, vol. 66, no. 3, pp. 303–317, May 1998.

[204] P. Dong, J. G. Brankov, N. P. Galatsanos, Y. Yang, and F. Davoine, "Digital watermarking robust to geometric distortions," *IEEE Trans. Image Process.*, vol. 14, no. 12, pp. 2140–2150, Dec. 2005.

[205] Y. Liu, B. Prabhakaran, and X. Guo, "Spectral watermarking for parameterized surfaces," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1459–1471, Oct. 2012.

[206] R. Ohbuchi, H. Masuda, and M. Aono, "Watermarking three-dimensional polygonal models through geometric and topological modifications," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 551–560, May 1998.

[207] N. Sakr, N. D. Georganas, J. Zhao, and E. M. Petriu, "Multimodal vision—haptic perception of digital watermarks embedded in 3-D meshes," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 5, pp. 1047–1055, May 2010.

[208] Z. Yu, H. H. S. Ip, and L. F. Kwok, "A robust watermarking scheme for 3D triangular mesh models," *Pattern Recognit.*, vol. 36, no. 11, pp. 2603–2614, Nov. 2003.

[209] S. Zafeiriou, A. Tefas, and I. Pitas, "Blind robust watermarking schemes for copyright protection of 3D mesh objects," *IEEE Trans. Vis. Comput. Graphics*, vol. 11, no. 5, pp. 596–607, Sep. 2005.

[210] J. M. Konstantinides, A. Mademlis, P. Daras, P. A. Mitkas, and M. G. Strintzis, "Blind robust 3-D mesh watermarking based on oblate spheroidal harmonics," *IEEE Trans. Multimedia*, vol. 11, no. 1, pp. 23–38, Jan. 2009.

[211] A. G. Bors, "Watermarking mesh-based representations of 3-D objects using local moments," *IEEE Trans. Image Process.*, vol. 15, no. 3, pp. 687–701, Mar. 2006.

[212] J. Bennour and J. Dugelay, "Protection of 3D object through silhouette watermarking," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, vol. 2. May 2006, pp. 221–224.

[213] E. Garcia and J. L. Dugelay, "Texture-based watermarking of 3D video objects," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 853–866, Aug. 2003.

[214] D. C. Hwang, K. H. Bae, M. H. Lee, and E. S. Kim, "Real-time stereo image watermarking using discrete cosine transform and adaptive disparity maps," *Proc. SPIE*, vol. 5241, pp. 233–242, Nov. 2003.

[215] D. C. Hwang, K. H. Bae, and E. S. Kim, "Stereo image watermarking scheme based on discrete wavelet transform and adaptive disparity estimation," *Proc. SPIE*, vol. 5208, pp. 196–205, Jan. 2004.

[216] J. N. Ellinas, "Reversible watermarking on stereo image sequences," *Int. J. Signal Process.*, vol. 5, no. 3, pp. 210–215, 2009.

[217] D. C. Hwang, K. H. Bae, J. H. Ko, and E. S. Kim, "3D watermarking scheme in stereo vision system," *Proc. SPIE*, vol. 5909, pp. 590928-1–590928–10, Aug. 2005.

[218] C. Burini, S. Baudry, and G. Doërr, "Blind detection for disparity-coherent stereo video watermarking," *Proc. SPIE*, vol. 9028, pp. 90280B-1–90280B-11, Feb. 2014.

[219] Z. H. Ou and L. H. Chen, "A robust watermarking method for stereo-pair images based on unmatched block bitmap," *Multimedia Tools Appl.*, vol. 75, no. 6, pp. 3259–3280, 2016.

[220] A. Chammem, M. Mitrea, and F. Prêteux, "DWT-based stereoscopic image watermarking," *Proc. SPIE*, vol. 7863, pp. 786326-1–786326-10, Feb. 2011.

[221] Z. Zhang, Z. Zhu, and L. Xi, "Novel scheme for watermarking stereo video," *Int. J. Nonlinear Sci.*, vol. 3, no. 1, pp. 74–80, 2007.

[222] M. Asikuzzaman, M. J. Alam, A. J. Lambert, and M. R. Pickering, "A blind watermarking scheme for depth-image-based rendered 3D video using the dual-tree complex wavelet transform," in *Proc. IEEE Int. Conf. Image Process.*, Oct. 2014, pp. 5497–5501.

[223] H. D. Kim, J. W. Lee, S. J. Ryu, H. Y. Choi, and H. K. Lee, "DIBR 3D video watermarking with faster DT-CWT quantization," in *Proc. IASTED Int. Conf. Signal Process., Pattern Recognit. Appl.*, Feb. 2013, pp. 222–226.

[224] N. Zhu, G. Ding, and J. Wang, "A novel digital watermarking method for new viewpoint video based on depth map," in *Proc. 8th Int. Conf. Intell. Syst. Design Appl.*, vol. 2, Nov. 2008, pp. 3–7.

[225] M. Asikuzzaman, M. J. Alam, A. J. Lambert, and M. R. Pickering, "Robust DT CWT-based DIBR 3D video watermarking using chrominance embedding," *IEEE Trans. Multimedia*, vol. 18, no. 9, pp. 1733–1748, Sep. 2016.

[226] M. J. Lee, J. W. Lee, and H. K. Lee, "Perceptual watermarking for 3D stereoscopic video using depth information," in *Proc. Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Oct. 2011, pp. 81–84.

[227] Y. H. Lin and J. L. Wu, "A novel blind watermarking scheme for depth-image-based rendering 3D images," in *Proc. Int. Workshop 3D Video Process.*, Oct. 2010, pp. 39–44.

[228] S. C. Pei and Y. Y. Wang, "Auxiliary metadata delivery in view synthesis using depth no synthesis error model," *IEEE Trans. Multimedia*, vol. 17, no. 1, pp. 128–133, Jan. 2015.

[229] M. Hefeeda, T. ElGamal, K. Calagari, and A. Abdelsadek, "Cloud-based multimedia content protection system," *IEEE Trans. Multimedia*, vol. 17, no. 3, pp. 420–433, Mar. 2015.

[230] Y. H. Lin and J. L. Wu, "A digital blind watermarking for depth-image-based rendering 3D images," *IEEE Trans. Broadcast.*, vol. 57, no. 2, pp. 602–611, Jun. 2011.

[231] S. Wang, C. Cui, and X. Niu, "Watermarking for DIBR 3D images based on SIFT feature points," *Measurement*, vol. 48, pp. 54–62, Feb. 2014.

[232] H.-D. Kim, J.-W. Lee, T.-W. Oh, and H.-K. Lee, "Robust DT-CWT watermarking for DIBR 3D images," *IEEE Trans. Broadcast.*, vol. 58, no. 4, pp. 533–543, Dec. 2012.

[233] K. A. Arun and P. J. Poul, "Protection of depth-image-based rendering 3D images using blind watermarking," in *Proc. Int. Conf. Comput., Commun. Netw. Technol.*, Jul. 2013, pp. 1–6.

[234] S. R. Zadokar, V. B. Raskar, and S. V. Shinde, "A digital watermarking for anaglyph 3D images," in *Proc. Int. Conf. Adv. Comput., Commun. Inf.*, Aug. 2013, pp. 483–488.

[235] Y. Yang, J. Sun, W. Wan, and H. Yuan, "Contourlet transform based digital watermarking resisting 2D-3D conversion," in *Proc. 3DTV-Conf., True Vis.-Capture, Transmiss. Dispaly 3D Video*, Oct. 2013, pp. 1–4.

[236] C. Cui, S. Wang, and X. Niu, "A novel watermarking for DIBR 3D images with geometric rectification based on feature points," *Multimedia Tools Appl.*, vol. 76, no. 1, pp. 649–677, 2017.

[237] T. Bashir, I. Usman, and J. Rehman, "Secure digital watermarking using optimized improved spread spectrum and BCH coding for DIBR 3D-TV system," *Multimedia Tools Appl.*, vol. 75, no. 13, pp. 7697–7713, 2015.
[238] E. Halici and A. A. Alatan, "Watermarking for depth-image-based rendering," in *Proc. IEEE Int. Conf. Image Process.*, Nov. 2009, pp. 4217–4220.
[239] J. Franco-Contreras, S. Baudry, and G. Doërr, "Virtual view invariant domain for 3D video blind watermarking," in *Proc. Int. Conf. Image Process.*, Sep. 2011, pp. 2761–2764.
[240] A. Koz, C. Cigla, and A. A. Alatan, "Free-view watermarking for free-view television," in *Proc. IEEE Int. Conf. Image Process.*, Oct. 2006, pp. 1405–1408.
[241] A. Koz, C. Cigla, and A. A. Alatan, "Watermarking of free-view video," *IEEE Trans. Image Process.*, vol. 19, no. 7, pp. 1785–1797, Jul. 2010.
[242] E. E. Apostolidis and G. A. Triantafyllidis, "Watermark selection for light field rendering in FTV," in *Proc. 3DTV Conf., True Vis.-Capture, Transmiss. Display of 3D Video*, May 2008, pp. 385–388.
[243] H. Tian, Z. Wang, Y. Zhao, R. Ni, and L. Qin, "Spread spectrum-based multi-bit watermarking for free-view video," in *Proc. Int. Workshop Digit. Forensics Watermarking*, 2012, pp. 156–166.
[244] C. Fehn *et al.*, "An evolutionary and optimised approach on 3D-TV," in *Proc. Int. Broadcast Conf.*, 2002, pp. 357–365.
[245] C. Fehn, "Depth-image-based rendering (DIBR), compression, and transmission for a new approach on 3D-TV," *Proc. SPIE*, vol. 5291, pp. 93–104, Jan. 2004.
[246] A. Redert *et al.*, "ATTEST: Advanced three-dimensional television system technologies," in *Proc. Int. Symp. 3D Data Process. Vis. Transmiss.*, 2002, pp. 313–319.
[247] J. Flack, P. V. Harman, and S. Fox, "Low-bandwidth stereoscopic image encoding and transmission," *Proc. SPIE*, vol. 5006, pp. 206–214, May 2003.
[248] L. Zhang and W. J. Tam, "Stereoscopic image generation based on depth images for 3D TV," *IEEE Trans. Broadcast.*, vol. 51, no. 2, pp. 191–199, Jun. 2005.
[249] P. Ndjiki-Nya *et al.*, "Depth image-based rendering with advanced texture synthesis for 3-D video," *IEEE Trans. Multimedia*, vol. 13, no. 3, pp. 453–465, Jun. 2011.
[250] J. Lei, C. Zhang, Y. Fang, Z. Gu, N. Ling, and C. Hou, "Depth sensation enhancement for multiple virtual view rendering," *IEEE Trans. Multimedia*, vol. 17, no. 4, pp. 457–469, 2015.
[251] Y. C. Fan and T. C. Chi, "The novel non-hole-filling approach of depth image based rendering," in *Proc. 3DTV Conf., True Vis.-Capture, Transmiss. Display 3D Video*, 2008, pp. 325–328.
[252] M. Levoy and P. Hanrahan, "Light field rendering," in *Proc. Comput. Graph. Interaction Techn.*, 1996, pp. 31–42.
[253] *Methodology for the Subjective Assessment of the Quality of Television Pictures*, document Rec. ITU-R BT.500-11, Radiocommunication Sector International Telecommunication Union, 2002.
[254] *Subjective Methods for the Assessment of Stereoscopic 3DTV Systems*, document Rec. ITU-R BT.2021, Radiocommunication Sector of International Telecommunication Union, Aug. 2012.
[255] H. Peng, J. Wang, and W. Wang, "Image watermarking method in multiwavelet domain based on support vector machines," *J. Syst. Softw.*, vol. 83, no. 8, pp. 1470–1477, 2010.
[256] J. H. Hsiao, C. S. Chen, L. F. Chien, and M. S. Chen, "A new approach to image copy detection based on extended feature sets," *IEEE Trans. Image Process.*, vol. 16, no. 8, pp. 2069–2079, Aug. 2007.
[257] A. Khan, S. F. Tahir, A. Majid, and T. S. Choi, "Machine learning based adaptive watermark decoding in view of anticipated attack," *Pattern Recognit.*, vol. 41, no. 8, pp. 2594–2610, 2008.
[258] J. Dittmann, M. Steinebach, I. Rimac, S. Fischer, and R. Steinmetz, "Combined video and audio watermarking: Embedding content information in multimedia data," *Proc. SPIE*, vol. 3971, pp. 455–464, 2000.
[259] J. Dittmann and M. Steinebach, "Joint watermarking of audio-visual data," in *Proc. IEEE 4th Workshop Multimedia Signal Process.*, 2001, pp. 601–606.

Md. Asikuzzaman (S'12–M'15) received the B.Sc. degree in electronics and telecommunication engineering from the Rajshahi University of Engineering & Technology, Rajshahi, Bangladesh, in 2010, and the Ph.D. degree in electrical engineering from the University of New South Wales, Canberra, Australia, in 2015, under a very competitive University International Postgraduate Award Scholarship. He is currently a Research Associate with the School of Engineering and Information Technology, The University of New South Wales. His current research interests include 2D and 3D video watermarking, 3D modeling, medical imaging, and video coding.

Mark R. Pickering (S'92–M'95) was born in Biloela, Australia, in 1966. He received the B.Eng. degree in electrical engineering from the Capricornia Institute of Advanced Education, Rockhampton, Australia, in 1988, and the M.Eng. and Ph.D. degrees in electrical engineering from the University of New South Wales, Canberra, Australia, in 1991 and 1995, respectively. He was a Lecturer from 1996 to 1999 and a Senior Lecturer from 2000 to 2009 with the School of Electrical Engineering and Information Technology, The University of New South Wales. He is currently an Associate Professor with the University of New South Wales. His research interests include video and audio coding, medical imaging, data compression, information security, data networks, and error-resilient data transmission.