IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 14, 2020, accepted June 16, 2020, date of publication June 22, 2020, date of current version July 1, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3004049

HEVC Watermarking Techniques for Authentication and Copyright Applications: Challenges and Opportunities

ALI A. ELROWAYATI[1], (Member, IEEE), MOHAMED A. ALRSHAH[2], (Senior Member, IEEE), MOHAMMAD FAIZ LIEW ABDULLAH[3], (Senior Member, IEEE), AND ROHAYA LATIP[2], (Member, IEEE)

[1]Department of Electronic Engineering, College of Industrial Technology, Misurata, Libya
[2]Department of Communication Technology and Network, Faculty of Computer Science and IT, Universiti Putra Malaysia, Serdang 43400, Malaysia
[3]Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia, Parit Raja 86400, Malaysia

Corresponding authors: Ali A. Elrowayati (elrowayati@yahoo.com), Mohamed A. Alrshah (mohamed.asnd@gmail.com), and Mohammad Faiz Liew Abdullah (faiz@uthm.edu.my)

This work was supported by the Universiti Putra Malaysia (UPM).

ABSTRACT Recently, High-Efficiency Video Coding (HEVC/H.265) has been chosen to replace previous video coding standards, such as H.263 and H.264. Despite the efficiency of HEVC, it still lacks reliable and practical functionalities to support authentication and copyright applications. In order to provide this support, several watermarking techniques have been proposed by many researchers during the last few years. However, those techniques are still suffering from many issues that need to be considered for future designs. In this paper, a Systematic Literature Review (SLR) is introduced to identify HEVC challenges and potential research directions for interested researchers and developers. The time scope of this SLR covers all research articles published during the last six years starting from January 2014 up to the end of April 2020. Forty-two articles have met the criteria of selection out of 343 articles published in this area during the mentioned time scope. A new classification has been drawn followed by an identification of the challenges of implementing HEVC watermarking techniques based on the analysis and discussion of those chosen articles. Eventually, recommendations for HEVC watermarking techniques have been listed to help researchers to improve the existing techniques or to design new efficient ones.

INDEX TERMS Authentication, copyright, HEVC, H.265, SLR, systematic review, video, watermarking.

I. INTRODUCTION

In the last decade, video coding standards have been advancing to provide better data compression while maintaining high-quality visual resolution. Further, authentication and copyright protection have become a key interest to protect video content. However, accessing and tampering video contents became an easy task that disturbs the process of authentication and copyright protection due to the availability of video content and advanced video editing tools on the Internet. This increases the necessity of finding solutions that can protect copyrights, detect, and localize video tampering [1]. Thus, integrated solutions in video compression standards to provide copyright protection, and authentication are significantly needed, in which these solutions must have the ability to validate authentication, copyright information, and content integrity.

The previous video codecs, such as H.263 and H.264, have been successfully protected by many watermarking techniques [2]–[5]. However, the High-Efficiency Video Coding (HEVC) standard is poising to replace those watermarking techniques, despite their success, in order to maintain the flexibility, reliability, and robustness of the HEVC [6]. Furthermore, applying watermarking techniques for HEVC video protection is relatively a new research trend that is full of legal challenges such as copyright protection, ownership proofing, tampering detection, and authentication [1], [7], [8].

Although HEVC watermarking techniques have been existing for a few years, this field suffers from the absence

The associate editor coordinating the review of this manuscript and approving it for publication was Zhaoqing Pan.

of Systematic Literature Review (SLR). As well-known, SLR papers are very necessary to ease obtaining the latest updates, such as the open issues and research gaps, in a specific topic to save the time and effort of the researchers who are willing to contribute to the field. Indeed, the main contributions of this paper are:

- Highlighting the necessity of using watermarking with the HEVC.
- Presenting a new classification of the existing and/or possible watermarking techniques.
- Disclosing common challenges and issues of integrating watermarking techniques into the HEVC codec.
- Summarizing the potential applications of authentication and copyrighting that need to be considered in future HEVC watermarking techniques.
- Answering several common critical questions related to HEVC watermarking in order to open the door for new trends and domains in this area.

The remainder of this paper has been structured as follows: Section II presents the method and procedure of this SLR; including the study questions, searching strategy and selection criteria. Section III shows statistics, classifications, analysis, and discussion with highlighting the challenges and open issues in this area. Finally, Section IV concludes the work, and Section V presents the future directions, respectively.

II. SLR METHOD AND PROCEDURE

This section describes the followed procedure in this paper to present an unbiased coverage of studied literature. The process includes: defining the directive study questions, determining the search strategy, and assessing articles based on the selection criteria.

A. DEFINING THE DIRECTIVE STUDY QUESTIONS

Based on gaps found in the recent articles related to the scope of this research, the following eight important questions (Qs) are going to be answered in this paper:

Q1. What are the main differences among data hiding, steganography, cryptography, and watermarking terms?

Q2. Is there still a need for HEVC watermarking techniques to support copyright and authentication applications?

Q3. What are the current watermarking techniques that are used or can be applied for the HEVC codec to provide authentication and copyright functionalities?

Q4. What are the possible options to implement watermarking techniques into the HEVC codec for authentication and copyright applications?

Q5. What are the main watermark zone selection criteria that can be applied to design efficient HEVC watermarking techniques for authentication and copyright applications?

Q6. What are the common metrics used to evaluate the performance of video watermarking techniques?

Q7. What are the main challenges in HEVC video watermarking?

Q8. Are there any real-time HEVC video watermarking techniques implemented on hardware platform?

Q1 aims to illustrate the main difference among data hiding, steganography, cryptography, and watermarking terms. **Q2** aims at highlighting the necessity of watermarking techniques for authenticating and copyright-protecting HEVC videos. **Q3** investigates the existing watermarking techniques and their applicability to the HEVC standard. **Q4** discusses the possible options of the HEVC video watermarking techniques for authentication and copyright applications. **Q5** discusses the main watermark zone selection criteria that can be applied for designing HEVC video watermarking techniques for authentication and copyright applications. In **Q6**, the common metrics used to evaluate the performance of general video watermarking are discussed. **Q7** presents the most critical challenges of the existing HEVC watermarking techniques, including common and security challenges for both authentication and copyright applications. Finally, **Q8** finds whether real-time HEVC video watermarking techniques are implemented on hardware platforms.

B. SEARCHING STRATEGY AND SELECTION CRITERIA

In this research, three criteria have been used for paper selection:

- The scope of this review is limited to published research on HEVC video watermarking techniques for authentication and copyright applications.
- The time scope of this SLR covers all research papers published in period from January 2014 up to the end of April 2020.
- General keywords and their alternative spellings and synonyms have been used to search in the digital libraries. These keywords have been used with the Boolean (AND) and (OR) which are used to connect among the keywords and their alternative spellings and synonyms as shown in Table 1.

The searching process targets the well-known *ScienceDirect, Scopus, IEEExplore, Web of Science* and the other academic digital libraries that contain peer-reviewed journal articles, conference proceedings, and book chapters. Multiple academic tools, such as Google Scholar engine and EndNote X7.5, have been used for gathering and obtaining a comprehensive list of relevant articles. These tools have been used to perform an automatic search in the identified resources using the most appropriate search strings, keywords, and synonyms, as in Table 1. Initially, this search strategy produces lists of related and interesting articles including many duplicated and redundant items. For this reason, avoiding duplication and redundancy during the articles selection process was a significant step to consolidate similar articles to obtain a list of the most relevant and unique articles.

Specifically, all obtained articles are filtered using standard search procedures and guidelines as in [9]. More specifically,

TABLE 1. Searching keywords, synonyms, and boolean operators.

High Efficiency Video Coding	OR	HEVC	OR	H.265

AND

Watermarking	OR	Robust Watermarking	OR
Fragile Watermarking	OR	Readable Watermarking	OR
Detectable Watermarking	OR	Zero-Watermarking	OR
Information Hiding	OR	Data Embedding	OR
Security	OR	Authentication	OR
Copyright	OR	Video Forensics	OR
Double Compression Detection	OR	Re-compression Detection	OR
Tampering Detection	OR	Semi-fragile	

TABLE 2. Inclusion and exclusion criteria.

Inclusion criteria	Exclusion criteria
Directly related to the main topic	Irrelevant to the main topic
Presents HEVC watermarking technique, method and results	Published in a preliminary conference
Presents experimental dataset, evaluation metrics and discussion	Review papers or unpublished papers
Answers the presented research questions	Incomplete or includes hidden parts
Written in English	Not written in English

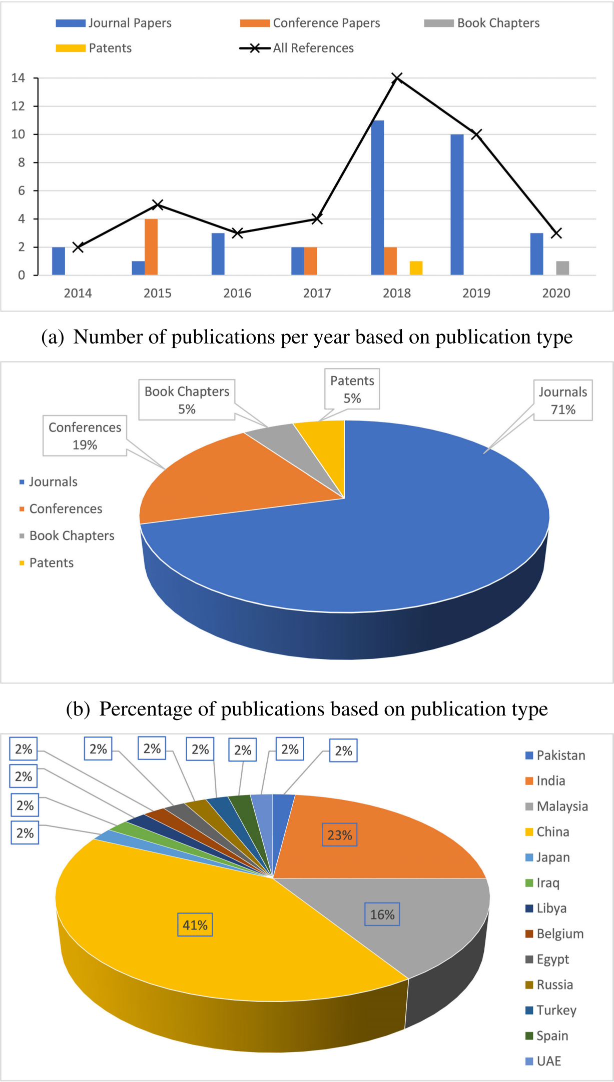
the inclusion and exclusion criteria, shown in Table 2, are applied for each article to choose the most relevant ones.

After filtering the articles using the inclusion and exclusion criteria, the obtained list of articles is considered the final comprehensive Primary Study List (PSL), which includes the most relevant and related articles without overlapping, redundancy and/or duplication.

III. ANALYSIS AND DISCUSSION

As a result of the aforementioned searching strategy and selection criteria, the obtained PSL has only included 42 articles selected based on the inclusion and exclusion criteria from a total of 343 articles, as shown in Table 3. Specifically, there were 298 articles excluded from the list since they were not satisfying the inclusion criteria. In this section, the metadata of the obtained PSL articles has been analyzed to present some useful statistics. Then, the questions of the study have been answered based on the analysis and criticism of the PSL articles.

Fig. 1(a), shows the distribution of the PSL articles over the last five years based on the article's type. In general, it is clear that the number of publications in this field is very limited. However, it is also clear that the number of publications has been dramatically increased in the last two years. The first data embedding technique, which inserts and hides data into HEVC video content to protect copyright information, has been published in 2014 as a journal paper (reference [10]). As for the first fragile HEVC watermarking technique to support authentication features, it has been published also in 2014 as a journal paper (reference [11]). As for the first robust HEVC watermarking technique against the re-compression attack, it has been published under a conference proceeding in 2015 (reference [12]). To conclude, it is clearly noticed that HEVC watermarking received increasing attention in the year 2017 onwards.



(a) Number of publications per year based on publication type

(b) Percentage of publications based on publication type

(c) Percentage of publications based on country

FIGURE 1. PSL statistics based on type, year, and country.

As for Fig. 1(b), it shows the percentage of all article types in the PSL; 71% journal papers, 19% conference papers, 5% chapter of books, and 5% patents. Therefore, the researchers in this field need to focus more on publishing conference papers to enrich the discussion and ideas about the HEVC. As well as, they need to publish their full research papers in high-impact journals.

Regarding Fig. 1(c), it shows the distribution of the PSL articles based on the author's country. It is very clear that China, India, and Malaysia have been the most contributing countries in terms of published research articles in this area with 41%, 23%, and 16%, respectively. As for the remaining 20%, it has been equally distributed among the other countries; Belgium, Libya, Iraq, Pakistan, Japan, Egypt, Spain, Russia, Turkey, and UAE; with 2% for each country.

TABLE 3. The obtained PSL articles selected based on the inclusion and exclusion criteria.

No.	Author(s), Year, Ref#	Title	Reference Type	Country
1	Chang et al., 2014 [10]	A DCT/DST-based error propagation-free data hiding algorithm for HEVC intra-coded frames.	Journal Article	China
2	Swati et al., 2014 [11]	Watermarking scheme for high efficiency video coding (HEVC).	Journal Article	Pakistan
3	Gaj et al., 2015 [12]	A robust watermarking scheme against re-compression attack for H.265/HEVC.	Conference Proceedings	India
4	Abdullah et al., 2015 [13]	Recent methods and techniques in video watermarking and their applicability to the next generation video codec.	Journal Article	Libya
5	Huang et al., 2015 [14]	Detection of double compression for HEVC videos based on the co-occurrence matrix of DCT coefficients.	Conference Proceedings	China
6	Ogawa, & Ohtake, 2015 [15]	Watermarking for HEVC/H.265 stream.	Conference Proceedings	Japan
7	Tew et al., 2015 [16]	HEVC video authentication using data embedding technique.	Conference Proceedings	Malaysia
8	Dutta & Gupta, 2016 [17]	A robust watermarking framework for high efficiency video coding (HEVC) – Encoded video with blind extraction process.	Journal Article	India
9	Elrowayati et al., 2016 [18]	Robust HEVC video watermarking scheme based on repetition-BCH syndrome code.	Journal Article	Malaysia
10	Tew et al., 2016 [19]	Multi-layer authentication scheme for HEVC video based on embedded statistics.	Journal Article	Malaysia
11	Dutta & Gupta, 2017 [8]	An efficient framework for compressed domain watermarking in P frames of high-efficiency video coding (HEVC)–Encoded video.	Journal Article	India
12	Elrowayati et al., 2017 [7]	Tampering detection of double-compression with the same quantization parameter in HEVC video streams.	Conference Proceedings	Malaysia
13	Gaj et al., 2017 [20]	Drift-compensated robust watermarking algorithm for H. 265/HEVC video stream.	Journal Article	India
14	Xu et al., 2017 [21]	Zero-watermarking registration and detection method for HEVC video streaming against requantization transcoding.	Google Patents	China
15	Jiang et al., 2018 [22]	HEVC Double Compression Detection Based on SN-PUPM Feature.	Conference Proceedings	China
16	Jo et al., 2018 [23]	A Reversible Watermarking Algorithm in the Lossless Mode of HEVC.	Journal Article	China
17	Joa et al., 2018 [24]	A watermarking method by modifying QTCs for HEVC.	Journal Article	China
18	Kaur et al., 2018 [25]	An efficient watermarking scheme for enhanced high efficiency video coding/H.265.	Journal Article	India
19	Liu et al., 2018 [26]	A robust and improved visual quality data hiding method for HEVC.	Journal Article	China
20	Mohammed & Ali, 2018 [27]	Robust video watermarking scheme using high efficiency video coding attack.	Journal Article	Iraq
21	Tew et al., 2018 [1]	Separable authentication in encrypted HEVC video.	Journal Article	Malaysia
22	Mareen et al., 2018 [28]	A Novel Video Watermarking Approach Based on Implicit Distortions	Journal Article	Belgium
23	Liu et al., 2018 [29]	Hiding Bitcoin Transaction Information Based on HEVC	Conference Proceedings	China
24	Joshi et al., 2018a [30]	Real-Time Implementation of Blind and Robust Watermarking for HEVC Video Coding.	Conference Proceedings	India
25	Joshi, 2018b [31]	VLSI Implementation of Video Watermarking for Secure HEVC Coding Standard.	Journal Article	India
26	Li, Wang & Xu, 2018 [32]	Detection of double compression in HEVC videos based on TU size and quantized DCT coefficients.	Journal Article	China
27	Liang et al., 2018 [33]	Detection of double compression for HEVC videos with a fake bitrate.	Journal Article	China
28	Wang et al., 2018 [34]	Anti-HEVC Recompression Video Watermarking Algorithm Based on the All Phase Biorthogonal Transform and SVD.	Journal Article	China
29	El-Shafai et al., 2019 [35]	Security of 3D-HEVC transmission based on fusion and watermarking techniques.	Journal Article	Egypt
30	X.Yu, et al., 2019 [36]	A Hybrid Transforms-Based Robust Video Zero-Watermarking Algorithm for Resisting High Efficiency Video Coding Compression.	Journal Article	China
31	L.Yu, et al., 2019 [37]	HEVC double compression detection under different bitrates based on TU partition type.	Journal Article	China
32	Shanableh, 2019 [38]	Data Embedding in HEVC Video by Modifying the Partitioning of Coding Units.	Journal Article	UAE
33	Kaur et al., 2019a [39]	An efficient watermarking scheme for enhanced high efficiency video coding/H.265.	Journal Article	India
34	Jiang, et al., 2019a [40]	Detection of Double Compressed HEVC Videos Using GOP-Based PU Type Statistics.	Journal Article	China
35	Kaur et al., 2019b [41]	An efficient authentication scheme for high efficiency video coding/H.265.	Journal Article	India
36	Fang et al., 2019 [42]	Detection of HEVC Double Compression with Different Quantization Parameters Based on Property of DCT Coefficients and TUs.	Journal Article	China
37	Jang et al., 2019 [43]	Biological Viral Infection Watermarking Architecture of MPEG/H. 264/AVC/HEVC	Journal Article	China
38	Jiang, et al., 2019 b [44]	Detection of HEVC Double Compression with the Same Coding Parameters Based on Analysis of Intra-Coding Quality Degradation Process	Journal Article	China
39	Galiano et al., 2020 [45]	Efficient embedding and retrieval of information for high-resolution videos coded with HEVC	Journal Article	Spain
40	Favorskaya, et al., 2019 [46]	Authentication and Copyright Protection of Videos Under Transmitting Specifications	Chapter of Book	Russia
41	Konyar et al., 2020 [47]	Matrix encoding-based high-capacity and high-fidelity reversible data hiding in HEVC	Journal Article	Turkey
42	Gaj et al., 2020 [48]	Prediction mode based H. 265/HEVC video watermarking resisting re-compression attack	Journal Article	India

A. Q1: WHAT ARE THE MAIN DIFFERENCES AMONG DATA HIDING, STEGANOGRAPHY, CRYPTOGRAPHY, AND WATERMARKING TERMS?

Data hiding is a general term comprising a wide range of content problems beyond embedding messages, such as steganography, cryptography, and watermarking. The differences among these terms are fundamental and based on different requirements, designs, and technical solutions. The steganography is a word derived from the Greek word (Steganographia), where *steganos* means "*covered*" and *graphia* means "*writing*". Steganography is an age-old technique of hiding plain data within another hosting file as a concealed communication, which allows exchanging information without arousing any suspicion. As for cryptography, it is used to protect the hidden message by encrypting its content. More specifically, the third parties in the steganography should not know about the existence of the plain text in the hosting media, while in the encryption, the existence of the protected data is known for the public. As for the digital watermarking, it is the process of embedding information into digital media, no matter it is perceptible or imperceptible to the third parties. For instance, most broadcasting providers use perceptible watermarks that are visible for the public to protect the copyright of the broadcasted content.

Furthermore, the watermarks can be also hidden or encrypted into the hosting video for authentication purposes such as preventing unauthorized use for the broadcasted content [49]–[52]

There are four fundamental differences between steganography and watermarking:

1) Watermarks have to be resistant against possible attacks unlike messages in steganography.
2) Watermarks could be visible or invisible, while messages in steganography must be hidden.
3) In steganography, there is no relationship between the host file and the message, while the watermark uses a relevant message to protect or maintain the ownership and/or the authentication of the host file [53].
4) Based on the number of senders and receivers, steganography is usually a one-to-one application, while watermarking is usually a one-to-many application [54].

B. Q2: IS THERE STILL A NEED FOR HEVC WATERMARKING TECHNIQUES TO SUPPORT COPYRIGHT AND AUTHENTICATION APPLICATIONS?

Fig. 1(a) shows that HEVC watermarking is an open area for research due to the clear increase in the number of publications in the last few years. In addition, the HEVC video standard and its watermarking for authentication and copyright purposes become very widely used by video streaming industries, such as Netflix, HBO Go, and others.

The only way to do video watermarking is by embedding/extracting the watermark into/from video content during the encoding and decoding processes, respectively, as the video streaming companies exactly do. Moreover, many encoding tools, video editing software, and some video capturing cards now provide functionalities of embedding/extracting watermarks into/from HEVC encoded video streams. Therefore, the integrity check, tampering detection, high visual quality assurance, bitrate control, and readability of watermarks on the receiver side, are significantly required to fulfill the market and industry needs. Consequently, the use of both robust and fragile watermarking techniques for HEVC video standard is very helpful, which requires a huge concern of researchers. Hence, watermarking techniques can be mainly used for:

Authentication: The wide range of video applications, the high accessibility to video, and the availability of video editing software allow unauthorized personnel to easily tamper any video, which highly concerns many video production companies [1]. Therefore, this concern has motivated the need for authentication functionalities to detect and localize any unauthorized tampering in HEVC videos, where fragile or semi-fragile watermarks could be used in order to do so. These types of watermarks are aimed to be destroyed in case of any unauthorized alteration of watermarked videos.

Copyright Protection: It concerns the identification of content owners to protect their ownership. Thus, robust watermarks have to be used for copyright protection to ensure that watermarks are persistently associated with the video contents. Robust techniques rely on watermarking stable zones in the video to ensure that the copyright information is all the time existing in the video to identify its owner.

C. Q3: WHAT ARE THE CURRENT WATERMARKING TECHNIQUES THAT ARE USED OR CAN BE APPLIED FOR THE HEVC CODEC TO PROVIDE AUTHENTICATION AND COPYRIGHT FUNCTIONALITIES?

Video watermarking has different techniques depending on the targeted application; fragile/semi-fragile techniques are commonly used for authentication purpose and robust techniques are used for copyright applications. In general, the watermarking methods designed for the previous standards; such as MJPEG, H.263, and H.264; can be applied to the HEVC. However, these watermarking techniques cannot be straightforwardly applied to the HEVC standard due to its new features and tools, which have not been considered in the previous codecs. Thus, the existing watermarking techniques have to be improved or modified to fit the environment of the HEVC standard and its requirements. These watermarking techniques can be categorized as in Fig. 2, which is a combination of new information with some common classifications presented in previous literature [49], [55]–[57].

1) BASED ON THE DOMAIN

The domain is a place or a stage in which the watermark is embedded, which can be categorized into two main categories:

1.1 ***Spatial domain:*** in this domain, the watermarking can be performed in a bitstream-wise or in a pixel-wise manner, as explained below:

- ***Bitstream-wise:*** the watermarking is done at the entropy part of the codec, where the watermarking can be done using either the Least Significant Bit (LSB) or the Most Significant Bit (MSB). More specifically, the watermark is directly embedded into or extracted from a compressed bitstream, which can be embedded as a string of bits in the Context Adaptive Binary Arithmetic Coding (CABAC) of the HEVC entropy part or it can be extracted as a feature from the bitstream itself, similarly as proposed in [58], in which a string of bits was embedded into the H.264 CABAC. Moreover, watermarks can be embedded into the motion vector data, which is a particular case of bitstream domain technique, where watermarks can be inserted into the MSB in the motion vector data [3], [59].

  Indeed, this approach presents high fragility, which is significantly proper for authentication and inappropriate for copyright applications. The watermarking in this domain is proportionally simple and proper for real-time video streaming since

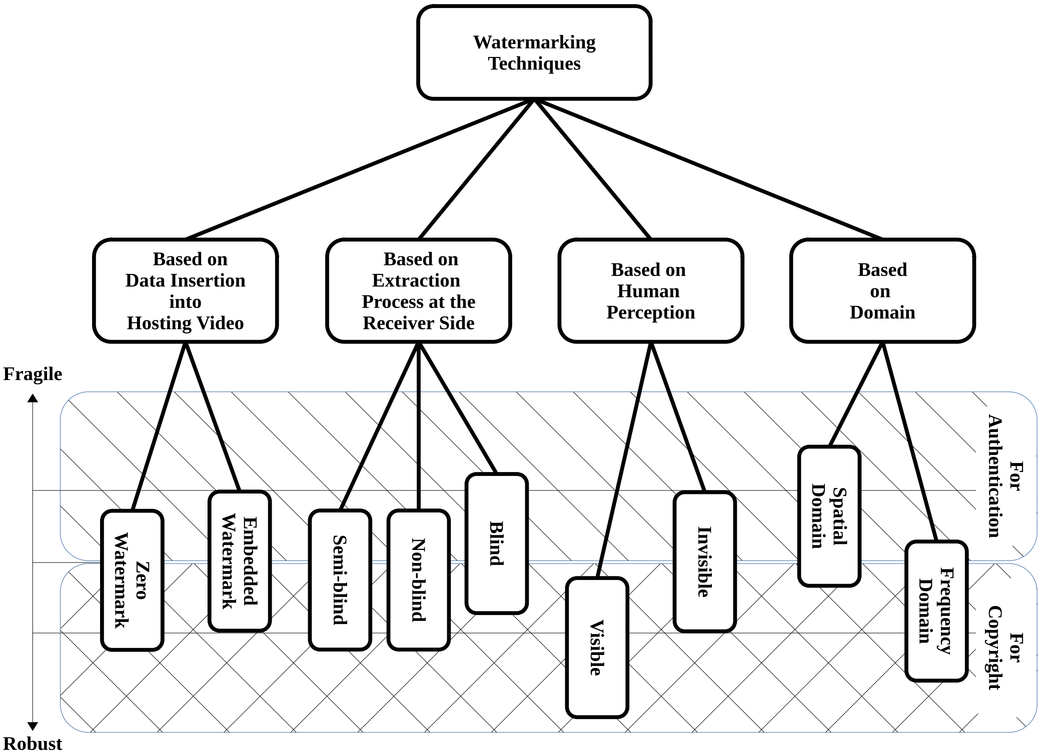


FIGURE 2. Classification of the commonly used watermarking techniques.

it works directly on the bitstream. However, this approach results in some critical issues including visual distortion and fragility against common image processing operations; such as rotation, resizing and video re-compression, etc.

- ***Pixel-wise:*** in this domain, the watermarking is done based on the hosting frame statistical features such as histograms [60], [61] and moments [62] that can be used as an extracting-based or embedding-based watermarking technique. More specifically, these features can be used in a non-blind manner, in which the decoder needs information about the hosting frame to validate the watermark. Otherwise, these features can be used in a blind manner, in which the information of the hosting frame is not required at the decoder side. Similar to the bit-wise domain, the pixel-wise domain suffers from high complexity, visual distortion, and high fragility against video re-compression, etc. That is why it can be much more suitable for authentication applications.

1.2 ***Frequency domain:*** in this domain, there are many common approaches, such as Discrete Sine Transform (DST) and Discrete Cosine Transform (DCT). Despite that the watermarking techniques in this domain are highly robust, they still suffer from high complexity issues [1], [12], [18], [41], [42]. They are commonly used for both copyright and authentication applications due to their high robustness against unintentional attacks. However, they are not proper for real-time video streaming due to their complexity unless parallel processing is considered.

2) BASED ON HUMAN PERCEPTION

In this category, the watermarks can be either visible or invisible:

2.1 ***Visible watermarking:*** is mostly used for copyright protection. However, this technique can be highly fragile if the watermark is placed in a non-significant part of the video, where it can be covered, cropped, or removed. In fact, the robustness of this technique could be significantly improved if the visible watermark changes its location randomly over the video time, which makes the watermark removal an uneasy task. Therefore, visible watermarking requires to be perceptible and non-removable. However, it is still not easy for video owners to detect illegal video distribution when visible watermarks are used. For this reason, video owners need to rely on invisible watermarks for better tracking of illegal videos [63].

2.2 ***Invisible watermarking:*** it can be fragile or robust depending on how and where the watermark is embedded in the video. Therefore, the invisible watermarking techniques are very commonly used for both copyright and authentication applications. According to the resistance level against intentional or unintentional

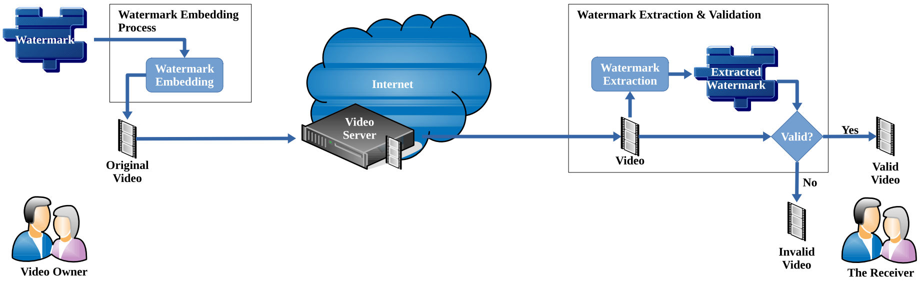


FIGURE 3. Blind watermarking architecture.

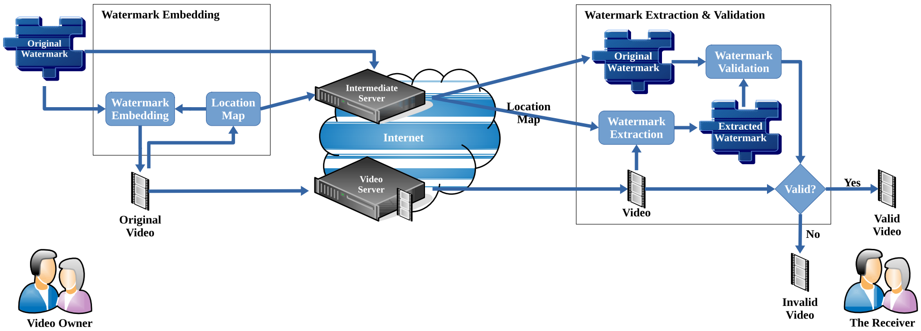


FIGURE 4. Non-blind watermarking architecture.

attacks, invisible watermarking techniques can be further classified as robust or fragile [49], [64]. Specifically, the watermarking technique is considered robust against attacks if the watermark can survive after the watermarked video is altered or attacked. These robust watermarking techniques are primarily suitable for copyright protection applications. In contrast, fragile watermarking is a technique in which the watermark will be destroyed if the watermarked video is altered or attacked. These fragile watermarking techniques are generally suitable for authentication applications as well as for tampering detection.

3) BASED ON THE EXTRACTION PROCESS AT THE RECEIVER SIDE

In this category, there are three main classes:

3.1 ***Blind watermarking:*** is a way of extracting watermarks without using their original information at the receiver side to detect and validate them, as shown in Fig. 3. This category can be visible or invisible and it can be used for copyright protection and authentication. The main problem with this category, when it is being used for copyright, is that the watermark could be non-detectable if the watermarked video encountered some attacks, such as frame dropping and/or filtering. To overcome this problem, the Forward Error Correction FEC) approach can be used to detect and correct errors in the recovered watermark, as proposed in [18]. Moreover, statistical approaches; such as moments, histograms, and hybrid transforms; can be also used to overcome this issue, as proposed in [54], [60]–[62].

3.2 ***Non-blind watermarking:*** is an approach used for extracting watermarks at the receiver side using the original watermark information to detect and validate them, as shown in Fig. 4. This type can be visible or invisible and it is appropriate for both authentication and copyright protection. The most common approach of this category is the zero-watermarking, which relies on the features of the video itself that need to be known at the receiver side in order to be able detectable and validatable [21], [36], [65]–[67]. The main issue with this type is that an intermediate authentication server is required for the transmitter to share the original watermark information with the receiver to use it for watermark extraction and validation, which increases complexity and cost of the implementation of this approach.

3.3 ***Semi-blind watermarking:*** is an approach used for extracting watermarks at the receiver side using the location map that points to the used positions to embed the watermark into the hosting video, in order to make the watermark detectable and validatable, as shown in Fig. 5. This type can be visible or invisible and it is appropriate for both authentication and copyright protection. Even though this approach helps to reduce the sensitivity to synchronization errors, it is still suffering from some critical issues such as the extra transmission overhead due to attaching the location map with the watermarked video [17]. In order for researchers to

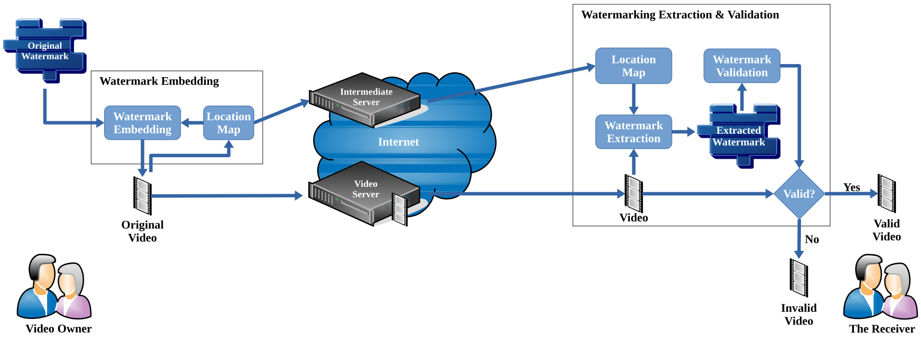


FIGURE 5. Semi-blind watermarking architecture.

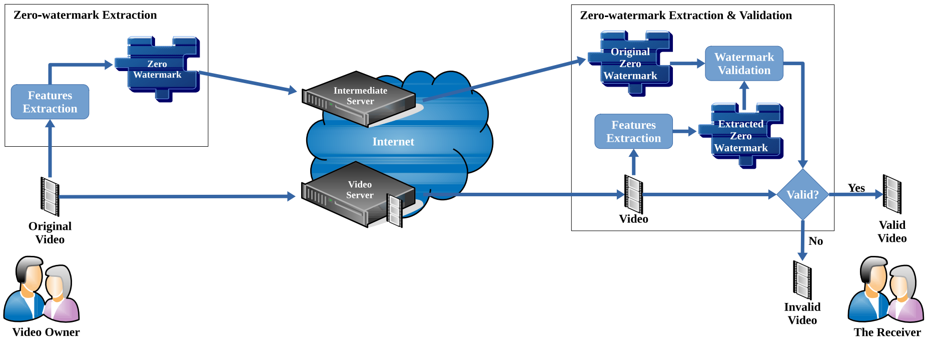


FIGURE 6. Zero-watermarking architecture.

avoid this issue, a secure channel through an intermediate authorization server is used to send the location map to the receiver, which inherits the same issue introduced by the non-blind method [8], [68]–[71].

4) BASED ON THE DATA INSERTION INTO HOSTING VIDEO

In this category, there are two main classes:

4.1 ***Zero-watermarking:*** can be used for authentication and copyright protection applications. It works based on extracting some features of the video itself to be used as a watermark, thus no information will be embedded into the original video, as shown in Fig. 6. These features have to be known at the receiver side in order to make the watermark detectable and validatable, which makes this category falls under the non-blind approach [21], [36], [65]–[67].

Indeed, the zero-watermarking is an excellent solution to avoid the visual quality degradation encountered by the conventional watermarking techniques, where the later can be highly robust on the expense of the video visual quality and bitrate [72]. However, the zero-watermarking approach mainly relies on an intermediate server to share the original watermark information with the receiver to use it for watermark extraction and validation. Specifically, the sender will share the original zero-watermark with the receiver trough out the intermediate server if the used approach is non-blind, while the location map of the extracted features only will be shared with the receiver if the used approach is semi-blind. In general, the intermediate server used in this approach is considered the main weakness that increases its complexity and cost of implementation.

4.2 ***Embedded-watermarking:*** is a method to inject some external data into a video, where this method can rely on blind approach (as in Fig. 3), non-blind approach (as in Fig. 4) or semi-blind approach (as in Fig. 5). Embedded-watermarking is suitable for both authentication and copyright protection with less complexity compared to the zero-watermarking techniques. However, this approach is still suffering from some critical problems caused by injecting data into the video, such as (1) video bitrate increase (2) visual quality degradation (3) survivability against the common attacks [1], [8], [16], [17], [68]–[71].

D. Q4: WHAT ARE THE POSSIBLE OPTIONS TO IMPLEMENT WATERMARKING TECHNIQUES INTO THE HEVC CODEC FOR AUTHENTICATION AND COPYRIGHT APPLICATIONS?

In general, HEVC watermarks could be embedded into videos (embedding-based watermarking technique) or extracted from videos (zero-watermarking technique). Regardless of the used approach, there are four possible options that can be used to perform video watermarking at the codec level.

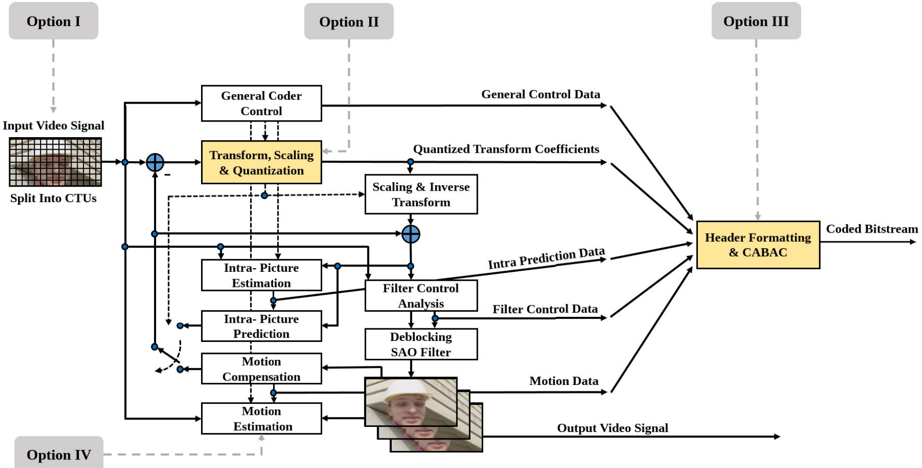


FIGURE 7. Possible watermarking options for HEVC video standard.

In Fig. 7, we have highlighted the possible watermarking options for the HEVC video standard:

Option I: Although the option of using watermarking methods based on the spatial domain in a pixel-wise manner is not new, however, they have only been used in the image watermarking area for many years [60]–[62]. This option is also suitable for video watermarking since videos are chains of sequential images. This option is highly fragile against the common attacks, that is why it can be much more suitable for authentication applications. In this option, the watermarking can be performed based on the hosting frame statistical features, such as histograms and moments that can be used as extracting-based or embedding-based watermarking techniques. However, using histograms and moments could significantly increase the codec complexity and may lead to visual distortion. In general, this option can not be directly applied to the HEVC standard due to some differences between the HEVC and image codecs, such as the variability of the HEVC transform block size that varies from 4×4 to 32×32, and the high embedding capacity of the videos compared to images due to the presence of the time domain in the video. Thus, these differences have to be considered in order to design a successful watermarking technique for the HEVC standard based on the spatial domain in a pixel-wise manner. To the best of our knowledge, there is no HEVC watermarking technique performed based on this option yet.

Option II: Watermarking can be performed based on the frequency domain techniques as proposed in [4], [73], [74] that was designed for H.264. However, these techniques cannot be directly applied to the HEVC standard due to the variability of the transform block size, which varies from 4×4 to 32×32 and also due to the increase of the intra-modes up to 35 in HEVC rather than 9 intra-modes as in H.264 standard. Additionally, the HEVC uses the DST transform for blocks of 4×4 size and the DCT transform for blocks of 8×8 to 32×32 size, while only DCT transform is used in the H.264 standard. Moreover, both H.264 and H.265 rely only on the Y channel for watermarking while the chromatic channel is never used in the literature, especially in the embedding-based watermarking techniques [68], [75]. Thus, these differences have to be considered to design a new watermarking technique fitting the HEVC standard.

Recently, [8], [17], [18], [20], [23], [26], [39] developed new robust HEVC watermarking techniques based on the transform domain that are slightly robust compared to the spatial domain watermarking techniques as in Option I. In [11], the watermark is embedded into the quantized transform coefficients during the encoding process. However, the authors did not report the robustness level against the common types of attacks. In [10], a new hiding data method for HEVC based on the intra-frame error propagation effect technique was proposed, in which the blocks are classified based on the intra-prediction modes. However, this method is fragile and very sensitive to common attacks such as image re-compression and image processing attacks [17].

Option III: The watermark can be directly embedded into the compressed encoded bitstream at the bit-wise spatial domain. However, the H.264 methods used previously in this domain cannot be directly applied to the current HEVC standard, due to differences between the HEVC CABAC and the H.264 CABAC.

Recently, [30], [31] proposed two hardware-based HEVC watermarking techniques for ownership verification. Both techniques use AC-NZ coefficients into the arithmetic algorithms at the CABAC for embedding and extracting watermarks, where they also control the bitrate increase and minimize the complexity. However, both techniques suffer from slightly high drift and synchronization errors due to the CABAC open loop that lacks feedback to minimize errors. Moreover, using this option is fragile to some extent and sensitive to common attacks such as re-compression and image processing attacks. For more details, refer to Q3-1.1.

Option IV: Watermarking can be also performed on motion vector data, which can be defined as a particular case of bitstream domain technique [3], [59]. The watermark can be inserted into the MSBs of motion vectors. However, to apply the watermarking on motion vector data in HEVC should consider the differences between the motion-compensated prediction algorithm applied in the HEVC codec and the motion-compensated prediction algorithm applied in the H.264. To the best of our knowledge, there is no HEVC watermarking technique performed using this option yet.

E. Q5: WHAT ARE THE MAIN WATERMARK ZONE SELECTION CRITERIA THAT CAN BE APPLIED TO DESIGN EFFICIENT HEVC WATERMARKING TECHNIQUES FOR AUTHENTICATION AND COPYRIGHT APPLICATIONS?

The watermark zone selection is very crucial for the embedding process, the extraction process, and the targeted application. For instance, the main goal of watermarking techniques, targeting copyright applications, is to survive against attacks in order to protect intellectual property rights. Therefore, the watermarking techniques, in this case, would select the invariant or stable regions of the video content to embed or extract the copyright information, which in turn would increase the robustness of the technique. On the other hand, the watermarking techniques, targeting authentication applications, would select the variant or unstable regions of the video content in order to increase the sensitivity to any attack, which is used to detect and localize any tampering on the video content. In general, the watermark zone selection can be done based on four main criteria, as described below:

1) COLOR CHANNEL SELECTION

The watermarking techniques use Luminance channel (Y) for embedding watermark information because the modification in the Y channel would not affect the Human Visual System (HVS) compared to embedding watermark information in chromatic channels. Moreover, the Y channel cannot be removed without causing a significant impact or total damage of the watermarked video, while the chromatic channels can be removed without affecting the visual quality. More specifically, removing the chromatic channels of the video will not cause a visual distortion but will remove colors from the video and will convert it to the grayscale mode [68], [75].

2) FRAME SELECTION

Generally, video codecs divide the video stream into Group of Pictures (GOP), which includes three types of frames; I, P, and B. The I-frame is an intra-coded frame, which is coded independently of all other frame types. As regarding the P-frame, it is a predictive coded frame that contains the motion-compensated difference information relative to the previously decoded frame, while the B-frame is a bi-predictive coded frame that contains the motion-compensated difference information relative to the previously decoded frames. In fact, the P and B frames are considered as unstable and sensitive areas due to containing a small Number of Non-Zero (NNZ) coefficients. For this reason, both could be used to embed/extract watermarks designed for highly fragile authentication applications. However, using them for watermarking will lead to visual quality distortion, bitrate increase, and increase of vulnerability to the common attacks. As for the I-frames, they are classified as stable areas due to containing large NNZ coefficients that can be used for embedding and/or extracting watermarks if a robust watermarking technique is needed. Additionally, I-frames can be used for watermarking techniques designed for authentication purposes as well [1], [76].

3) BLOCK SELECTION

The blocks in each frame are classified into stable blocks and unstable blocks based on the following parameters: the size of the block, NNZ coefficients, and motion information.

3.1 ***Block size:*** The intra-prediction modes of HEVC have block sizes of 32 × 32 down to 4 × 4. In each frame, a block is considered stable if its size is equal to 4 × 4, otherwise, it would be considered as an unstable block, where the unstable blocks have limited details compared to stable blocks that are very rich of details. For this reason, the unstable blocks are prone to be changed into other block sizes if they were exposed to any attack process [17], [25]. To summarize, 4 × 4 blocks could be used for watermark embedding or feature extraction regardless the type of the frame (I, P or B), however, 4 × 4 blocks in the I-frame are preferable for robust watermarking techniques while 4 × 4 blocks in P-/B-frames are much suitable for fragile techniques that could be used for authentication applications [1], [8], [17].

3.2 ***The NNZ quantized coefficients:*** It plays a significant role during the block selection process, where it can be used to differentiate between stable blocks and the extremely stable ones. Specifically, 4 × 4 blocks with high NNZ coefficients contain a lot of picture details compared to other blocks with the same size with less NNZ. Thus, blocks with high NNZ coefficients have a high level of stability that could be utilized for watermark embedding or feature extraction. Moreover, the use of blocks with high NNZ coefficients for watermarking will lead to trivial bitrate increase and less sensitivity to synchronization errors [17], [25], [68].

3.3 ***Motion information:*** It plays another critical role in choosing stable blocks for watermarks embedding or feature extraction that can reduce the impact of synchronization error. As well-known, the frames could contain static, low-motion, or high-motion picture components, where frames with low-motion components are considered highly stable with low sensitivity to synchronization errors [17].

4) COEFFICIENT SELECTION

It is an essential part to minimize the propagation drift and the bitrate increase, and also to minimize the impact of the synchronization errors. For instance, the blocks can be classified into groups based on the intra-prediction modes, to determine the protected pixel sets regardless of their block sizes to be used for embedding without causing the propagation drift error [10]. Similarly, [20] applied the same approach proposed in [10] but only uses blocks of 4 × 4 size to produce a robust watermarking technique with minimal propagation drift errors.

Since using the zero-frequency DC coefficients for watermark embedding will increase the bitrate and the visual distortion, AC coefficients are considered more suitable to reduce the aforementioned problems. Moreover, using the high-frequency AC coefficients will increase the fragility of the watermarking technique because it could be removed intentionally or unintentionally using image processing operations. As for the middle-frequency AC coefficients, they could be the key point to reduce the visual distortion errors due to the difficulty of recognition by the human eyes compared to the DC coefficients. Furthermore, using the middle-frequency AC coefficients for watermark embedding could highly increase robustness and resistance of the technique against the synchronization errors and the image processing operations [68].

F. Q6: WHAT ARE THE COMMON METRICS USED TO EVALUATE THE PERFORMANCE OF VIDEO WATERMARKING TECHNIQUES?

In order to evaluate a watermarking technique, there are several evaluation metrics that could be used depending on the target of the technique.

1) PEAK SIGNAL TO NOISE RATIO (PSNR)

PSNR is commonly used to examine the quality of the image or frame, which is calculated as the ratio between the maximum possible power of the original image and the power of the watermarked image. According to [77], the PSNR for YUV video sequence is calculated using Equation (1) as follows:

$$PSNR = \frac{(6 \times PSNR_Y) + PSNR_U + PSNR_V}{8}, \qquad (1)$$

where $PSNR_Y$ is the PSNR of the Luma component, and $PSNR_U$ and $PSNR_V$ denote the color components.

2) BIT ERROR RATE (BER) AND WATERMARKING ROBUSTNESS RATE (WRR)

BER and WRR are used to measure the robustness of watermarking techniques. According to [17], [78], the BER and WRR are defined as in the equations (2) and (3), respectively:

$$BER = \frac{E_b}{T_b}, \qquad (2)$$

where E_b is the number of error bits and T_b is the total bits sent, while WRR is the complement of the BER calculated as below:

$$WRR = 1 - BER \qquad (3)$$

3) NORMALIZED CROSS-CORRELATION (NCC)

NCC is also used to measure the robustness of watermarking techniques, by determining the similarity between the original watermark W and the recovered watermark W', as computed in Equation (4) [79] below:

$$NCC = \frac{\sum_{m=1}^{M}\sum_{n=1}^{N} W(m,n)W'(m,n)}{\sqrt{\sum_{m=1}^{M}\sum_{n=1}^{N} W(m,n)^2 \sum_{m=1}^{M}\sum_{n=1}^{N} W'(m,n)^2}}, \qquad (4)$$

where m and n are the dimensions of the watermark.

4) BIT INCREASE RATE (BIR)

BIR is another important metric used to measure the efficiency of a video watermarking technique by computing the bitrate increase after embedding a watermark in a hosting video. The bitrate can be calculated as $Bitrate(bits/sec) = \frac{V}{T}$, where V is the video file size in bits and T is the playback time in secs. As for the percentage of increase, it can be calculated as in Equation (5) [69], [80] below:

$$BIR = \frac{WV_{br} - O_{br}}{O_{br}} \times 100, \qquad (5)$$

where WV_{br} represents the watermarked video bitrate and O_{br} denotes the original video bitrate.

5) EMBEDDING CAPACITY RATIO PER FRAME (ECRF)

ECRF is used to measure the embedding capacity of the watermarking technique, which can be calculated by dividing the amount of embedded watermark data on the total amount of cover frame, as in Equation (6) [68]:

$$ECRF = \frac{D_{embedded}}{F_{size}} \times 100, \qquad (6)$$

where $D_{embedded}$ is the size of embedded data and F_{size} is the size of the hosting frame before embedding the watermark data, where the higher the ECRF is the better.

G. Q7: WHAT ARE THE MAIN CHALLENGES IN HEVC VIDEO WATERMARKING?

Indeed, most HEVC watermarking techniques are suffering from many challenges; where some of these challenges are common and especially affecting watermarking techniques designed for both authentication and copyright applications. Moreover, some of these challenges could affect the watermarking techniques depends on the application, where some could affect the techniques designed for authentication while some could affect techniques designed for copyright.

1) COMMON CHALLENGES

The common challenges discussed in this subsection could affect the HEVC video itself and/or the HEVC bitstream. Specifically, under this category of challenges, we have two main issues as follows:

a: VISUAL DISTORTION ISSUE

In fact, visual distortion could happen only when embedding-based watermarking techniques are used, while it could never happen when using zero-watermarking techniques. Generally, there are two main causes of visual distortion when embedding-based watermarking techniques are used with HEVC:

- The use of AC-Zero or DC coefficients has a severe negative impact on the visual quality of the HEVC video, due to the increase of errors during the reversing procedure of the video at the decoder side. Moreover, the change of the aforementioned coefficients will also lead to a bitrate increase of the HEVC video, which is not a preferable scenario. For this reason, the watermark information has to be embedded into the AC Non-Zero (NZ) coefficients to reduce potential errors during the HEVC video retrieval process at the decoder side.

  However, using the AC-NZ coefficients alone still cannot guarantee the avoidance of video visual distortion. For example, [1], [8], [14], [16], [19], [26], [81] proposed embedding-based watermarking techniques based on using AC-NZ coefficients to avoid the visual distortion but all of these proposed techniques suffered from the error drift issues that are still affecting the visual quality of watermarked videos while the bitrate is maintained at the minimum level.
- The error drift is defined as an error caused by modifying some pixels of a block that affect or change the pixels of other blocks. Specifically, this error propagates to several blocks in the same frame or other frames predicted from the modified block, which yields degrading in the visual quality of the watermarked video. Therefore, to avoid this problem, the selection of coefficients is significantly important to protect the adjacent blocks from being affected by the propagated error(s) caused by modifying a certain block.

  The first research to prevent the error drift issue on HEVC videos was proposed by Chang et al (2014) [10]. It classified pixels in two (protected and unprotected) pixels groups out of all block sizes, where the coefficients generated from the protected pixels group is used for embedding information to avoid intra-coded frame errors. However, this technique suffers from minor visual distortion due to the non-precise selection of the protected pixels group.

  Reference [20] finds the residual blocks by applying the inverse discrete sine transform on the 4 × 4 blocks only to determine the protected set of pixels to find a 3 × 3 residual protected subblock out of the selected residual 4 × 4 block. This approach showed an acceptable level of robustness but it could not completely prevent the distortion drift due to quantization errors that propagate to the neighboring blocks [82].

  Reference [82] embeds the watermark into the intra-prediction residual 4 × 4 blocks at the spatial domain. This approach showed an acceptable level of robustness while the distortion drift errors were significantly avoided. However, this technique is not robust enough against the frame dropping/exchange attack, for this reason, it is highly recommended to use the error correction codes to strengthen it against such attack.

  In [41], 4 × 4 intra-luma transform blocks of I-frames are divided into two sets: (1) Robust set is used for embedding the generated code in order to make this code survival against unintentional attacks; such as re-compression attacks, noise attacks, and frame dropping attacks; while (2) Fragile set is used to generate authentication code in order to check the video integrity. Despite that it works fine for both copyright and authentication applications, however, it showed a slight visual distortion due to the un-consideration of drift errors. Recently, [47] proposed a new technique based on a matrix encoding approach that maintains free error drift with high embedding capacity, high fidelity, and minimum visual distortion.

b: BITRATE INCREASE ISSUE

As mentioned early, watermarking techniques should straightforwardly use the AC-NZ coefficients to minimize the bitrate increase, especially when constrained channel capacity is used [83] as proposed in [1], [10], [11], [15], [17], [18], [45]. As well-known, the NNZ coefficients are directly proportional to the nature of the video itself in terms of richness of details and motion. Therefore, videos with low details and motion could have low NNZ coefficients that could be insufficient to carry the watermark information. Consequently, this may lead to the use of zero or DC coefficients which will severely affect the visual distortion and the bitrate increase.

c: SYNCHRONIZATION ERROR ISSUE

This issue is very important since it negatively affects any watermarking techniques regardless of what approach is used. As aforementioned in Q5, embedding a watermark into an HEVC video using inaccurate selection criteria could cause drifting errors that could lead to synchronization issues. However, synchronization errors also happen due to the size change of blocks located in smooth regions of any HEVC video frames if the video is exposed to any attack, which leads to extraction failure of the watermark at the decoder side [17], [18].

In fact, using accurate selection criteria to find the appropriate blocks for watermarking is a crucial task to reduce the probability of synchronization error, however, it can not be completely avoided. For this reason, implementing an error detection and correction code is highly recommended for watermarking techniques to minimize the synchronization errors [18].

2) AUTHENTICATION CHALLENGES

Video watermarking is considered efficient for authentication if it could detect and localize any tampering on video

TABLE 4. Comparison of the latest HEVC video watermarking techniques based on their authentication capabilities.

Year	Ref#	Watermarking Technique	Capabilities		
			Tampering Detection	Localization Ability	Double Compression Detection
2015	[16]	Embedding-based	Yes	Yes	No
2015	[14]	Zero-watermark	No	No	Yes*
2016	[19]	Embedding-based	Yes	Yes	No
2017	[7]	Zero-watermark	Yes	No	Yes
2018	[1]	Embedding-based	Yes	Yes	No
2018	[21]	Zero-watermark	Yes	NM	NM
2018	[33]	Zero-watermark	Yes	No	Yes
2018	[32]	Embedding-based	No	No	Yes*
2018	[22]	Zero-watermark	No	No	Yes
2019	[37]	Zero-watermark	No	No	Yes*
2019	[40]	Zero-watermark	No	No	Yes
2019	[41]	Embedding-based	Yes	Yes	No
2019	[42]	Zero-watermark	No	No	Yes*
2019	[44]	Zero-watermark	No	No	Yes
2020	[46]	Embedding-based	Yes	Yes	No
2020	[84]	Zero-watermark	No	No	Yes

(*) = Works well only with different bitrates
(NM) = Not Mentioned, (NA) = Not Applicable

content. Usually, fragile watermarking techniques are used for authentication purposes, in which they could employ either embedding-based watermarking or zero-watermarking techniques.

However, HEVC video watermarking for authentication purposes still faces many challenges. Therefore, it is essential to highlight the arisen issues in the study of applying fragile watermarking techniques on HEVC standard to make it easier for researchers in this field to have a comprehensive overview of the most common issues and challenges. For better understanding, we listed these issues and challenges in this subsection with a brief description, discussion, and analyses. Additionally, Table 4 shows a brief comparison of the latest HEVC watermarking techniques based on their authentication capabilities.

Tew *et al.* (in [1], [16], [19]) proposed three authentication watermarking techniques that embed some extracted features from the video and its encoding parameters. These embedded features are used at the decoder side to verify the integrity and to localize the tampering in the video. In 2015 [16], they proposed the first authentication technique for the HEVC standard with two layers, detection layer, and localization layer. It works based on generating the authentication code as a sequence of pairs, where each pair is a combination of the position and size of each used block in order. In 2018 [1], [19], they improved their previous work by involving an encryption technique as a new layer, namely the verification layer. However, the proposed techniques in [1], [16], [19] introduced major visual distortion and bitrate increase caused by error drift propagation issues due to their dependency on fragile embedding-based watermarking techniques. Moreover, these techniques were not able to distinguish between the re-compression attack and other types of attacks.

In 2018, Jiang *et al.* [21] registered the first patent of using a zero-watermarking technique for HEVC video streaming against the re-compression attack. It directly generates a zero-watermark based on processing depth features of the video stream without any modification on the original video. Thereafter, the watermark is encrypted and registered in the third-party institutions. Despite the disclosure of the way of detecting the re-compression attack with different quantization parameters, the re-compression attack with the same quantization parameters was not mentioned in this patent.

In 2019 [41], the authors divided all 4 × 4 intra-luma transform blocks of I-frames into two sets: (1) Fragile set is used to generate authentication code in order to check the video integrity; while (2) Robust set is used for embedding the generated code in order to make this code survival against unintentional attacks; such as re-compression attacks, noise attacks, and frame dropping attacks. Even though it works fine for both copyright and authentication applications, however, it showed a slight visual distortion due to neglecting the issue of drift errors.

Indeed, the detection of double compression in HEVC is a significant feature in the authentication domain since most of the common video tampering attacks are usually applied to the spatial domain. Thus, the attacker decompresses the sequential video stream into frames to get ready for video tampering or modification, then, the tampered video has to be re-compressed and injected again as a video stream in the channel. Hence, double compression is still an essential issue in the video authentication process [85].

In 2015, Huang *et al.* [14], Li *et al.* [32], and Fang *et al.* [42] presented a technique for distinguishing double compression attacks by analyzing the distribution of NNZ coefficients for the smooth regions of video frames. Specifically, it calculates the difference between the frequency of residual coefficients of the first and second compressions. Unfortunately, this technique failed to detect the second compression due to negligible frequency when the same quantization parameters were used in both compressions.

In 2017 [7], a new detection technique for double HEVC compression with the same quantization parameters was proposed based on some features extracted from the 4 × 4 transform blocks of the I-frames. The technique was able to detect double compression attacks even if the same quantization parameters are used. However, Jiang *et al.* [44] proposed a similar technique that relies on features extracted from different block sizes instead of 4×4 only, which could achieve better results compared to [7].

Moreover, Yu *et al.* [84] proposed a technique for distinguishing double HEVC compression by mixing the two approaches proposed in [7], [44]. However, this work detects only whether the HEVC videos were double-compressed by a third party or not, even if it is re-compressed by the same bitrate. Unfortunately, this work has not mentioned the tampering localization issue and the detection of other intentional and unintentional attacks was neglected as well.

References [22], [33], [40] proposed three algorithms based on Prediction Unit (PU) features that are used to distinguish between the first and second compressions. The main shortage of these three algorithms was neglecting all other

TABLE 5. Comparison of the latest HEVC video watermarking techniques based on their resistance against attacks.

Attack	Reference and Year							
	[12] 2015	[18] 2016	[17] 2016	[8] 2017	[25] 2018	[82] 2019	[36] 2019	[46] 2020
Re-compression	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cropping	NM	NM	NM	NM	NM	NM	Yes	NM
Rotation	NM	NM	NM	NM	NM	NM	Yes	NM
Scaling	NM	NM	NM	NM	NM	NM	NM	Yes
Gaussian Noise	NM	NM	Yes	Yes	Yes	Yes	NM	Yes
Gaussian Filtering	NM	NM	Yes	NM	Yes	Yes	NM	NM
Salt and Pepper	NM	NM	Yes	Yes	NM	Yes	NM	Yes
Frame Delete/Replace	NM	Yes	NM	NM	Yes	NM	NM	NM
AWGN Noise	NM	Yes	NM	NM	NM	NM	NM	NM
Rayleigh Fading Noise	NM	Yes	NM	NM	NM	NM	NM	NM

NM = Not Mentioned, AWGN = Additive White Gaussian Noise

features such as transform blocks properties and coefficients distributions, which led to lower accuracy compared to [7], [37], [44].

Recently in 2020, [46] studied the selection of relevant regions in I-frames under predefined restrictions and conditions based on transmission specifications. It uses the stable regions to embed the invariant features and the unstable zones of the I-frames to embed a fragile watermark. Simulation results showed high resistance to some common attacks, however, the embedding capacity of the proposed algorithm was very limited, which significantly affects the recovery quality of the watermark and the PSNR value if the size of the embedded watermark increases.

3) COPYRIGHT CHALLENGES

Video watermarking techniques for copyright applications are required to be as robust as possible, where the robustness term implies the capability of a watermark to resist the common attacks in order to reach safely to the decoder side. Usually, robust watermarking techniques are used for copyright purposes, in which they could employ either embedding-based watermarking or zero-watermarking techniques [24]–[26], [28], [29], [81], [86], [87].

In the meantime, the state-of-the-art literature on HEVC watermarking for copyright is still in its initial stage. In this SLR, we found a limited number of researches on HEVC watermarking techniques for copyright applications. Therefore, it is very important to highlight the arisen issues in the area of applying robust watermark techniques to the HEVC standard for this category of applications. In the upcoming paragraphs, we present a brief description, discussion, and analysis for the most common issues hindering the robustness measure. Moreover, Table 5 shows a comparative summary of the current robust HEVC video watermarking techniques based on their resistance against the common attacks.

In 2015, [12] proposed a blind embedding-based watermarking technique, which alters the NNZ coefficients of 4 × 4 transform blocks of the HEVC video sequence. Simulation results showed the robustness of this technique against re-compression attacks. However, it suffered from bitrate increase issue due to altering zero coefficients to NZ, which negatively affected the BIR and the visual quality of the HEVC video.

In 2016, [18] applied the repetition and the Bose-Chaudhuri-Hocquenghem (BCH) codes to detect and correct errors in order to improve the robustness of the proposed watermarking technique against the common attacks. However, this approach introduced high complexity that negatively affects the total performance of the watermarking process.

Later, Dutta *et al.* proposed two embedding-based approaches [8], [17] that embed the watermark in stable zones of the I-frames and P-frames, respectively. The main shortage of these two techniques was their sensitivity to synchronization and drift errors. For this reason, the authors decided to send the location map (*palette*) to the decoder side which increased the robustness of these techniques at the expense of transmission overhead.

In 2018, [25] proposed an efficient drift-free embedding-based watermarking technique using the stable zones of the HEVC I-frames. Experimental results reveal the robustness against re-compression, noise, and temporal attacks while maintaining the visual quality and the bitrate increase. However, its robustness is still low under the frame dropping, and Gaussian filter and noise attacks compared to the recent references which were not taken into this work account, where it was only compared to [12], [17] published in 2015 and 2016, respectively. Moreover, it also neglected the motion characteristics during the selection of embedding zones, which adds the possibility of being affected by synchronization errors.

In 2019, [82] proposed a new technique that embeds the watermark into the intra-prediction residual 4 × 4 blocks at the spatial domain. This approach showed an acceptable level of robustness due to the avoidance of distortion drift errors. However, this technique is not robust enough against the frame dropping/exchange attack, for this reason, it is highly recommended to use the Error detection and correction codes to strengthen it against such attacks.

In the same year, [36] proposed a robust video zero-watermarking technique based on the discrete wavelet transform and singular value decomposition to solve the problems associated with [34] such as false detection bits and visual distortion. This technique showed high robustness against re-compression, common image processing attacks, and geometric attacks. However, this technique is highly complex due to employing hybrid transforms based on the discrete wavelet and bi-orthogonal transform, and singular value decomposition. Moreover, it needs to improve its resistance against high-intensity rotation attacks, and also it has to eliminate the false-alarm problem. Additionally, this technique is not done during the encoding/decoding of the HEVC video, which requires extra processing before and after the encoding and decoding, respectively.

Recently in 2020, [46] uses the stable regions to embed the invariant features, where simulation results showed high resistance to some attacks; such as noise, color, and brightness correction of frames, and scaling. However, the embedding capacity of the proposed algorithm was very limited, which significantly affects the recovery quality of the watermark and the PSNR value if the size of the embedded watermark increases. Moreover, it could be fragile against the frame dropping/exchange attack, for this reason, it is highly recommended to apply the error detection and correction codes to increase its robustness.

4) SECURITY CHALLENGES

Most existing watermarking techniques rely on some operations and rules that could make the extraction process an easy task if these operations and rules become known to the public. In order to solve this issue, some researchers went to use randomization functions in their embedding/extraction operations and rules while some used encryption algorithms to secure the watermark information.

References [8], [17] propose techniques for security based on random functions of embedding blocks selection without encrypting the embedded watermarks. Consequently, if those random functions became known to the public, the watermarks could be easily retrieved by attackers.

Since extracting watermarks is not needed for authentication applications, irreversible cryptography techniques, such as MD5, SHA-1, and SHA-256, are highly recommended to detect unauthorized tampering of HEVC videos. Accordingly, [1], [19] have applied SHA256 hash functions on the extracted features from HEVC videos to prevent code imitation for authenticated video. Contrarily, [46] has applied the Arnold scrambling transform for authentication purposes which is a reversible technique not strong enough to be used for such application.

For copyright applications, the receiver side has to retrieve the embedded watermark from HEVC video, that is why reversible cryptography techniques are highly recommended for such application [88]. Reference [18] implemented an extended Arnold scrambling transform, for copyright application, to encrypt the watermark before embedding it into HEVC video, then, to decrypt it after the extraction process at the receiver side.

Indeed, using cryptography techniques for HEVC codec may receive high interest from researchers in this area to improve the capability of current watermarking techniques at preventing attackers from accessing watermarks information. However, HEVC designers have to balance between security and complexity to increase the practicality of implementing video codecs, especially if real-time video streaming is targeted.

H. Q8: ARE THERE ANY REAL-TIME HEVC VIDEO WATERMARKING TECHNIQUES IMPLEMENTED ON HARDWARE PLATFORM?

Even though most of the existing software-based watermarking solutions are able to perform the embedding and extraction processes on HEVC videos, they are still considered time-consuming solutions due to complexity that affect their applicability for real-time applications.

In fact, these time-consuming solutions could give enough chance to the attackers to attack the HEVC video and to manipulate its content. Thus, it is crucial to develop hardware-based solutions for real-time HEVC watermarking, where watermarks data can be embedded and extracted in a timely manner.

Recently, [30], [31] proposed two real-time HEVC watermarking techniques for ownership verification based on Very-Large-Scale Integration (VLSI) architecture and it was applied on a Field Programmable Gate Array (FPGA) platform. Both techniques use AC-NZ coefficients at the HEVC entropy part for embedding and extracting watermarks, while they control the bitrate increase and minimize the complexity. However, these two techniques suffer from slightly high drift and synchronization errors due to the CABAC open loop that lacks feedback to minimize errors. Moreover, using this option is fragile to some extent and sensitive to the common attacks such as re-compression and image processing attacks, which made it more applicable for authentication applications. For more details, refer to Q3-1.1 and Q4-Option III.

Finally, designing and implementing HEVC hardware-based watermarking techniques that are able to perform properly for real-time applications is still an open challenge. Moreover, hardware-based error detection and correction codes, such as BCH code, could be used with such systems to improve efficiency and robustness to give further support to copyright applications.

IV. CONCLUSION

This SLR has been conducted to explore the current status of the research about HEVC watermarking techniques for authentication and copyright purposes. The main aim of this paper is to collect the related resources and references according to a clear process and specific rules in order to identify the challenges and open issues on the HEVC video watermarking. Additionally, It identifies out the potential research directions for interested researchers and developers.

The time scope of this SLR covers all research articles published in the period of time from January 2014 up to the end of April 2020, where 343 articles published in this area have been found and only 42 articles have met the selection criteria. Then, the selected 42 articles have been analyzed and discussed to identify the challenges of adopting HEVC watermarking techniques to support authentication and copyright purposes. Moreover, a new classification for the existing up-to-date techniques has been drawn based on many factors, such as the domain, extraction and embedding process, human perceptibility, and fragility and robustness factors. Thereafter, this classification has been discussed to give a clear view to researchers who are interested in this area.

Eventually, we dedicate this important reference for researchers who are interested in this area, which will save their time and effort by facilitating the process of finding related works and references. Additionally, this paper summarizes the existing literature and highlights the main challenges and open issues.

V. FUTURE DIRECTIONS

In the future, interested researchers on the HEVC watermarking techniques for authentication and copyright application should consider the followings:

- The watermark zone selection criteria should be carefully set to fit the needs of authentication and copyright applications, which by its role could minimize the bitrate increase and minimize the drift and synchronization errors.
- The error detection and correction codes, such as BCH, could be considered to reduce most types of errors when high-robustness watermarking is required.
- All potential attacks that could affect the watermark readability have to be taken into account to allow the watermarks to stand strongly against them when high-robustness watermarking is required.
- There should be a great balance between complexity and security.
- Hardware-based solutions to support real-time applications should be considered.
- It might be a great idea if we take the Versatile Video Coding (VVC) features and HEVC features into account when developing watermarking techniques to make it ready for the VVC standard.

ACKNOWLEDGMENT

The technical and logistic parts of this work have been achieved by a research team formed of members from the College of Industrial Technology - Libya, Universiti Putra Malaysia, and Universiti Tun Hussein Onn Malaysia.

REFERENCES

[1] Y. Tew, K. Wong, R. C.-W. Phan, and K. N. Ngan, "Separable authentication in encrypted HEVC video," *Multimedia Tools Appl.*, vol. 77, pp. 24165–24184, Feb. 2018.

[2] S.-W. Park and S.-U. Shin, "Authentication and copyright protection scheme for H.264/AVC and SVC," *J. Inf. Sci. Eng.*, vol. 27, no. 1, pp. 129–142, 2011.

[3] D. Bhowmik, "Robust watermarking techniques for scalable coded image and video," Ph.D. dissertation, Dept. Electron. Elect. Eng., Univ. Sheffield, Sheffield, U.K., 2011.

[4] T. Dutta, A. Sur, and S. Nandi, "MCRD: Motion coherent region detection in H.264 compressed video," in *Proc. IEEE Int. Conf. Multimedia Expo (ICME)*, Jul. 2013, pp. 1–6.

[5] S.-W. Lo, Z. Wei, X. Ding, and R. H. Deng, "Generic attacks on content-based video stream authentication," in *Proc. IEEE Int. Conf. Multimedia Expo Workshops (ICMEW)*, Jul. 2014, pp. 1–6.

[6] ITU Press Release. (2013). *New Video Codec to Ease Pressure on Global Networks*. [Online]. Available: https://www.itu.int/net/pressoffice/press_releases/2013/01.aspx

[7] A. A. Elrowayati, M. F. L. Abdullah, A. A. Manaf, and A. S. Alfagi, "Tampering detection of double-compression with the same quantization parameter in HEVC video streams," in *Proc. 7th IEEE Int. Conf. Control Syst., Comput. Eng. (ICCSCE)*, Nov. 2017, pp. 174–179.

[8] T. Dutta and H. P. Gupta, "An efficient framework for compressed domain watermarking in P frames of high-efficiency video coding (HEVC)—Encoded video," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 13, no. 1, p. 12, 2017.

[9] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *J. Syst. Softw.*, vol. 80, no. 4, pp. 571–583, Apr. 2007.

[10] P.-C. Chang, K.-L. Chung, J.-J. Chen, C.-H. Lin, and T.-J. Lin, "A DCT/DST-based error propagation-free data hiding algorithm for HEVC intra-coded frames," *J. Vis. Commun. Image Represent.*, vol. 25, no. 2, pp. 239–253, Feb. 2014.

[11] S. Swati, K. Hayat, and Z. Shahid, "A watermarking scheme for high efficiency video coding (HEVC)," *PLoS ONE*, vol. 9, no. 8, pp. 1–8, 2014.

[12] S. Gaj, A. Sur, and P. K. Bora, "A robust watermarking scheme against re-compression attack for H.265/HEVC," in *Proc. 5th Nat. Conf. Comput. Vis., Pattern Recognit., Image Process. Graph. (NCVPRIPG)*, Dec. 2015, pp. 1–4.

[13] M. F. L. Abdullah, A. A. Elrowayati, A. A. Manaf, and Z. S. Zubi, "Recent methods and techniques in video watermarking and their applicability to the next generation video codec," *J. Theor. Appl. Inf. Technol.*, vol. 74, no. 1, pp. 1–11, 2015.

[14] M. Huang, R. Wang, J. Xu, D. Xu, and Q. Li, "Detection of double compression for HEVC videos based on the co-occurrence matrix of DCT coefficients," in *Proc. Int. Workshop Digit. Watermarking*. Cham, Switzerland: Springer, 2015, pp. 61–71.

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

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

[17] 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.

[18] A. A. Elrowayati, M. F. L. Abdullah, A. A. Manaf, and A. S. Alfagi, "Robust HEVC video watermarking scheme based on repetition-BCH syndrome code," *Int. J. Softw. Eng. Appl.*, vol. 10, no. 1, pp. 263–270, Jan. 2016.

[19] Y. Tew, K. Wong, R. C.-W. Phan, and K. N. Ngan, "Multi-layer authentication scheme for HEVC video based on embedded statistics," *J. Vis. Commun. Image Represent.*, vol. 40, pp. 502–515, Oct. 2016.

[20] S. Gaj, A. Kanetkar, A. Sur, and P. K. Bora, "Drift-compensated robust watermarking algorithm for H.265/HEVC video stream," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 13, no. 1, pp. 1–24, Jan. 2017.

[21] G. Jiang, J. Wang, M. Yu, and F. Chen, "Zero-watermarking registration and detection method for HEVC video streaming against requantization transcoding," U.S. Patent 9 947 065, Apr. 17, 2018.

[22] Q. Xu, T. Sun, X. Jiang, and Y. Dong, "HEVC double compression detection based on SN-PUPM feature," in *Proc. Int. Workshop Digit. Watermarking*. Cham, Switzerland: Springer, 2017, pp. 3–17.

[23] K. Jo, W. Lei, Z. Li, and X. Song, "A reversible watermarking algorithm in the lossless mode of HEVC," *IJ Netw. Secur.*, vol. 20, no. 5, pp. 844–852, 2018.

[24] K. Joa, W. Lei, and Z. Li, "A watermarking method by modifying QTCs for HEVC," *Comput., Perform. Commun. Syst.*, vol. 1, no. 1, pp. 8–16, 2018.

[25] G. Kaur, S. S. Kasana, and M. Sharma, "An efficient watermarking scheme for enhanced high efficiency video coding/H.265," *Multimedia Tools Appl.*, vol. 78, pp. 12537–12559, Oct. 2018.

[26] Y. Liu, H. Zhao, S. Liu, C. Feng, and S. Liu, "A robust and improved visual quality data hiding method for HEVC," *IEEE Access*, vol. 6, pp. 53984–53997, 2018.

[27] A. A. Mohammed and N. A. Ali, "Robust video watermarking scheme using high efficiency video coding attack," *Multimedia Tools Appl.*, vol. 77, no. 2, pp. 2791–2806, Jan. 2018.

[28] H. Mareen, J. De Praeter, G. Van Wallendael, and P. Lambert, "A novel video watermarking approach based on implicit distortions," *IEEE Trans. Consum. Electron.*, vol. 64, no. 3, pp. 250–258, Aug. 2018.

[29] S. Liu, Y. Liu, G. Lv, C. Feng, and H. Zhao, "Hiding bitcoin transaction information based on HEVC," in *Proc. Int. Conf. Smart Blockchain*. Cham, Switzerland: Springer, 2018, pp. 1–11.

[30] A. Joshi, V. Jain, S. Ladda, and R. Kumar, "Real-time implementation of blind and robust watermarking for HEVC video coding," in *Proc. IEEE Int. Symp. Smart Electron. Syst. (iSES) (Formerly iNiS)*, Dec. 2018, pp. 58–63.

[31] A. M. Joshi, *VLSI Implementation of Video Watermarking for Secure HEVC Coding Standard*. Boca Raton, FL, USA: CRC Press, 2018.

[32] Q. Li, R. Wang, and D. Xu, "Detection of double compression in HEVC videos based on TU size and quantised DCT coefficients," *IET Inf. Secur.*, vol. 13, no. 1, pp. 1–6, Jan. 2019.

[33] X. Liang, Z. Li, Y. Yang, Z. Zhang, and Y. Zhang, "Detection of double compression for HEVC videos with fake bitrate," *IEEE Access*, vol. 6, pp. 53243–53253, 2018.

[34] C. Wang, R. Shan, and X. Zhou, "Anti-HEVC recompression video watermarking algorithm based on the all phase biorthogonal transform and SVD," *IETE Tech. Rev.*, vol. 35, no. 1, pp. 42–58, Dec. 2018.

[35] W. El-Shafai, S. El-Rabaie, M. M. El-Halawany, and F. E. A. El-Samie, "Security of 3D-HEVC transmission based on fusion and watermarking techniques," *Multimedia Tools Appl.*, vol. 78, no. 19, pp. 27211–27244, Oct. 2019.

[36] X. Yu, C. Wang, and X. Zhou, "A hybrid transforms-based robust video zero-watermarking algorithm for resisting high efficiency video coding compression," *IEEE Access*, vol. 7, pp. 115708–115724, 2019.

[37] L. Yu, Y. Yang, Z. Li, Z. Zhang, and G. Cao, "HEVC double compression detection under different bitrates based on TU partition type," *EURASIP J. Image Video Process.*, vol. 2019, no. 1, p. 67, Dec. 2019.

[38] T. Shanableh, "Data embedding in HEVC video by modifying the partitioning of coding units," *IET Image Process.*, vol. 13, no. 11, pp. 1909–1913, 2019.

[39] G. Kaur, S. S. Kasana, and M. K. Sharma, "An efficient watermarking scheme for enhanced high efficiency video coding/h.265," *Multimedia Tools Appl.*, vol. 78, no. 9, pp. 12537–12559, May 2019.

[40] X. Jiang, P. He, T. Sun, and R. Wang, "Detection of double compressed HEVC videos using GOP-based PU type statistics," *IEEE Access*, vol. 7, pp. 95352–95363, 2019.

[41] G. Kaur, S. S. Kasana, and M. K. Sharma, "An efficient authentication scheme for high efficiency video coding/H.265," *Multimedia Tools Appl.*, vol. 78, no. 15, pp. 21245–21271, Aug. 2019.

[42] Q. Fang, X. Jiang, T. Sun, Q. Xu, and K. Xu, "Detection of HEVC double compression with different quantization parameters based on property of DCT coefficients and TUs," in *Proc. 12th Int. Congr. Image Signal Process., Biomed. Eng. Informat. (CISP-BMEI)*, Oct. 2019, pp. 1–6.

[43] B.-J. Jang, S.-H. Lee, Y.-S. Lee, and K.-R. Kwon, "Biological viral infection watermarking architecture of MPEG/H.264/AVC/HEVC," *Electronics*, vol. 8, no. 8, p. 889, Aug. 2019.

[44] X. Jiang, Q. Xu, T. Sun, B. Li, and P. He, "Detection of HEVC double compression with the same coding parameters based on analysis of intra coding quality degradation process," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 250–263, 2020.

[45] D. R. Galiano, A. A. Del Barrio, G. Botella, and D. Cuesta, "Efficient embedding and retrieval of information for high-resolution videos coded with HEVC," *Comput. Electr. Eng.*, vol. 81, Jan. 2020, Art. no. 106541.

[46] M. N. Favorskaya and V. V. Buryachenko, "Authentication and copyright protection of videos under transmitting specifications," in *Computer Vision in Advanced Control Systems*. Cham, Switzerland: Springer, 2020, pp. 119–160.

[47] M. Z. Konyar, O. Akbulut, and S. Öztürk, "Matrix encoding-based high-capacity and high-fidelity reversible data hiding in HEVC," *Signal, Image Video Process.*, vol. 14, pp. 897–905, Jan. 2020.

[48] S. Gaj, A. Sur, and P. K. Bora, "Prediction mode based H.265/HEVC video watermarking resisting re-compression attack," *Multimedia Tools Appl.*, pp. 1–31, Feb. 2020, doi: 10.1007s11042-019-08301-w.

[49] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*. San Mateo, CA, USA: Morgan Kaufmann, 2007.

[50] M. Shahidan, "Multilayer reversible watermarking using non-underflow difference expansion," M.S. thesis, UTM, Johor Bahru, Malaysia, 2012.

[51] D. Kesdogan, J. Egner, and R. Büschkes, "Stop-and-go-mixes providing probabilistic anonymity in an open system," in *Proc. Int. Workshop Inf. Hiding*. Berlin, Germany: Springer, 1998, pp. 83–98.

[52] I. S. Moskowitz and L. Chang, "An entropy-based framework for database inference," in *Proc. Int. Workshop Inf. Hiding*. Berlin, Germany: Springer, 1999, pp. 405–418.

[53] D. Chen, X. Luo, and Y.-M. Wang, "Steganography preserving the property of the histogram for JPEG images," *J. Electron. Inf. Technol.*, vol. 28, no. 2, pp. 252–256, 2006.

[54] P. K. Gupta and S. K. Shrivastava, "Improved RST-attacks resilient image watermarking based on joint SVD-DCT," in *Proc. Int. Conf. Comput. Commun. Technol. (ICCCT)*, Sep. 2010, pp. 46–51.

[55] F.-H. Wang, J.-S. Pan, and L. C. Jain, *Innovations in Digital Watermarking Techniques*, vol. 232. Berlin, Germany: Springer-Verlag, 2009.

[56] M. Boreiry and M.-R. Keyvanpour, "Classification of watermarking methods based on watermarking approaches," in *Proc. Artif. Intell. Robot. (IRANOPEN)*, Apr. 2017, pp. 73–76.

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

[58] D. Zou and J. A. Bloom, "H.264 stream replacement watermarking with CABAC encoding," in *Proc. IEEE Int. Conf. Multimedia Expo*, Jul. 2010, pp. 117–121.

[59] J. Zhang, J. Li, and L. Zhang, "Video watermark technique in motion vector," in *Proc. 14th Brazilian Symp. Comput. Graph. Image Process.*, 2001, pp. 179–182.

[60] 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.

[61] R. Rajkumar and A. Vasuki, "Reversible and robust image watermarking based on histogram shifting," *Cluster Comput.*, vol. 22, no. S5, pp. 12313–12323, Sep. 2019.

[62] G. Duan, X. Zhao, A. Chen, and Y. Liu, "An improved Hu moment invariants based classification method for watermarking algorithm," in *Proc. Int. Conf. Inf. Netw. Secur. (ICINS)*, 2014, pp. 1–5.

[63] T. M. Thanh and P. T. Hiep, "Frame background influence based invisible watermarking to visible video watermarking," in *Proc. Int. Conf. Adv. Technol. Commun. (ATC)*, Oct. 2013, pp. 563–568.

[64] P. Singh and R. S. Chadha, "A survey of digital watermarking techniques, applications and attacks," *Int. J. Eng. Innov. Technol.*, vol. 2, no. 9, pp. 165–175, 2013.

[65] Q. Xu, J. Lu, X. Peng, S. Yuan, and L. Li, "A video zero-watermarking algorithm based on text detection," in *Proc. IEEE 16th Int. Conf. Commun. Technol. (ICCT)*, Oct. 2015, pp. 328–333.

[66] G.-J. Xu and R.-D. Wang, "A video zero-watermark algorithm against RST attacks," in *Proc. Asia–Pacific Conf. Inf. Process.*, vol. 2, Jul. 2009, pp. 15–18.

[67] Z. Shen and U. Kintak, "A novel image zero-watermarking scheme based on non-uniform rectangular," in *Proc. Int. Conf. Wavelet Anal. Pattern Recognit. (ICWAPR)*, Jul. 2017, pp. 78–82.

[68] A. Mansouri, A. M. Aznaveh, F. Torkamani-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.

[69] M. Noorkami and R. M. Mersereau, "Digital video watermarking in P-frames with controlled video bit-rate increase," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 441–455, Sep. 2008.

[70] J. Li, H. Liu, J. Huang, and Y. Q. Shi, "Reference index-based H.264 video watermarking scheme," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 8, no. 2S, pp. 1–22, Sep. 2012.

[71] T. Dutta, A. Sur, and S. Nandi, "A robust compressed domain video watermarking in P-frames with controlled bit rate increase," in *Proc. Nat. Conf. Commun. (NCC)*, Feb. 2013, pp. 1–5.

[72] G. Feng and K. Huang, "H.264 video standard based zero watermarking technology," in *Proc. Int. Conf. Anti-Counterfeiting, Secur. Identificat. (ASID)*, Oct. 2013, pp. 1–4.

[73] M.-G. Ko, J.-W. Suh, and J.-E. Hong, "Error detection scheme based on fragile watermarking for H.264/AVC," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2011, pp. 1061–1064.

[74] E. Elbasi and A. M. Eskicioglu, "Robust video watermarking scheme in transform domains," in *Proc. Bildiriler Kitabi ISC Turkey*, 2007, vol. 68, no. 9.

[75] A. Piper, R. Safavi-Naini, and A. Mertins, "Coefficient selection methods for scalable spread spectrum watermarking," in *Proc. Int. Workshop Digital Watermarking*. Berlin, Germany: Springer, 2003, pp. 235–246.

[76] M. Noorkami and R. M. Mersereau, "Compressed-domain video watermarking for H.264," in *Proc. IEEE Int. Conf. Image Process.*, vol. 2, 2005, p. II-890.

[77] V. Sze, M. Budagavi, and G. J. Sullivan, *High Efficiency Video Coding (HEVC): Algorithms and Architectures* (Integrated Circuit and Systems), vol. 39. Cham, Switzerland: Springer, 2014, pp. 49–90.

[78] H. Nyeem, W. Boles, and C. Boyd, "Digital image watermarking: Its formal model, fundamental properties and possible attacks," *EURASIP J. Adv. Signal Process.*, vol. 2014, no. 1, p. 135, Dec. 2014.

[79] A. I. Hammouri, B. Alrifai, and H. Al-Hiary, "An intelligent watermarking approach based particle swarm optimization in discrete wavelet domain," *Int. J. Comput. Sci. Issues*, vol. 10, no. 2, p. 330, 2013.

[80] Y. Liu, M. Hu, X. Ma, and H. Zhao, "A new robust data hiding method for H.264/AVC without intra-frame distortion drift," *Neurocomputing*, vol. 151, pp. 1076–1085, Mar. 2015.

[81] 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.

[82] Y. Zhou, C. Wang, and X. Zhou, "An intra-drift-free robust watermarking algorithm in high efficiency video coding compressed domain," *IEEE Access*, vol. 7, pp. 132991–133007, 2019.

[83] K.-S. Kim, H.-Y. Lee, D.-H. Im, and H.-K. Lee, "Practical, real-time, and robust watermarking on the spatial domain for high-definition video contents," *IEICE Trans. Inf. Syst.*, vol. E91-D, no. 5, pp. 1359–1368, May 2008.

[84] Y. Yu, H. Yao, R. Ni, and Y. Zhao, "Detection of fake high definition for HEVC videos based on prediction mode feature," *Signal Process.*, vol. 166, Jan. 2020, Art. no. 107269.

[85] Z. Huang, F. Huang, and J. Huang, "Detection of double compression with the same bit rate in MPEG-2 videos," in *Proc. IEEE China Summit Int. Conf. Signal Inf. Process. (ChinaSIP)*, Jul. 2014, pp. 306–309.

[86] A. A. Elrowayati, Z. S. Zubi, and M. A. Abdulali, "Copyright protecting using secure watermarking images in DWT domain," in *Proc. Recent Adv. Telecommun., Signals Syst.* Boston, MA, USA: WSEAS, 2012, pp. 89–94.

[87] M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for images based on additive homomorphic property," *IEEE Trans. Image Process.*, vol. 14, no. 12, pp. 2129–2139, Dec. 2005.

[88] T. R. Singh, K. M. Singh, and S. Roy, "Video watermarking scheme based on visual cryptography and scene change detection," *AEU-Int. J. Electron. Commun.*, vol. 67, no. 8, pp. 645–651, Aug. 2013.

ALI A. ELROWAYATI (Member, IEEE) received the bachelor's degree in electronic engineering from the College of Industrial Technology, Misurata, Libya, in 2001, the master's in electrical engineering from the Faculty of Engineering, Misurata University, Libya, in 2011, and the Ph.D. degree from the Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia, in 2020. He is currently a Lecturer with the Electronic Engineering Department, College of Industrial Technology, Misurata. He is working on a High-Efficiency Video Watermarking project for Copyright Protection and Authentication support. His research interests are image processing, video coding, watermarking, and neural networks.

MOHAMED A. ALRSHAH (Senior Member, IEEE) received the B.Sc. degree in computer science from Naser University, Libya, in 2000, and the M.Sc. and Ph.D. degrees in communication technology and networks from Universiti Putra Malaysia, in May 2009 and February 2017, respectively. He is currently a Senior Lecturer with the Department of Communication Technology and Networks, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM). He has published a number of articles in high-impact factor scientific journals. His research interests include high-speed TCP protocols, high-speed wired and wireless networks, parallel and distributed algorithms, WSN, the IoT, and cloud computing.

MOHAMMAD FAIZ LIEW ABDULLAH (Senior Member, IEEE) received the B.Sc. degree (Hons.) in electrical engineering (communication), the Diploma Education degree, and the Master of Engineering degree in optical fiber communication from the University of Technology Malaysia (UTM), in 1997, 1999, and 2000, respectively, and the Ph.D. degree in wireless optical communication engineering from The University of Warwick, U.K., in August 2007. He started his career as a Lecturer at Polytechnic Seberang Prai (PSP), in 1999, and he has been transferred to University Tun Hussein Onn Malaysia (UTHM), in 2000. He is currently a Professor with the Department of Communication Engineering, Faculty of Electrical and Electronic Engineering, UTHM. He had 18 years' experience of teaching in higher education, which involved the subject optical fiber communication, advanced optical communication, and advanced digital signal processing. His research interests include wireless and optical communication, solar cell fabrication, image watermarking, and robotics in communication.

ROHAYA LATIP (Member, IEEE) received the Bachelor of Computer Science degree from University Technology Malaysia, Malaysia, in 1999, and the M.Sc. degree in distributed system and the Ph.D. degree in distributed database from University Putra Malaysia. She was the Head of the HPC Section, University Putra Malaysia, from 2011 to 2012, and consulted the campus grid project and also the wireless project for the hostel of the UPM campus. She is currently an Associate Professor with the Faculty of Computer Science and Information Technology, University Putra Malaysia. She is also the Head of the Department of Communication Technology and Network. She is also a Co-Researcher with the Institute for Mathematics Research (INSPEM). Her research interests include big data, cloud and grid computing, network management, and distributed database.

• • •