

Received August 9, 2020, accepted August 18, 2020, date of publication August 27, 2020, date of current version September 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3019840

Efficient HEVC Integrity Verification Scheme for Multimedia Cybersecurity Applications

OSAMA S. FARAGALLAH^{1,2}, ASHRAF AFIFI^{1,3}, HALA S. EL-SAYED⁴,
MOHAMMED A. ALZAIN¹, JEHAD F. AL-AMRI¹, FATHI E. ABD EL-SAMIE⁵, (Member, IEEE),
AND WALID EL-SHAFI⁵

¹Department of Information Technology, College of Computers and Information Technology, Taif University, Al-Hawiya 21974, Saudi Arabia

²Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

³Department of Electrical Engineering and Computers, Higher Technological Institute, 10th of Ramadan 228, Egypt

⁴Department of Electrical Engineering, Faculty of Engineering, Menoufia University, Shebin El-kom 32511, Egypt

⁵Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

Corresponding author: Osama S. Faragallah (osam_sal@yahoo.com)

This work was supported by the Deanship of Scientific Research, Taif University, Saudi Arabia, under Project 1-439-6083.

ABSTRACT Multimedia cybersecurity is a prevalent research topic in the digital world due to the rapid progress of digital multimedia and Internet applications. Watermarking, encryption, and steganography schemes are employed to attain multimedia data confidentiality and robustness. However, these schemes are externally applied on trusted computers, and there has been a lack of similar schemes that can be effectively and efficiently enabled through an untrusted transmission medium. In this work, a self-embedding-based High-Efficiency Video Coding (HEVC) transmission and integrity verification framework is presented. This framework is robust and reliable for verifying the integrity of HEVC frames transmitted through insecure communication channels. Firstly, the transmitted HEVC frames are divided into a number of blocks with a certain block size. After that, a discrete transform is used for self-embedding of watermarks from each block into another one depending on a predefined mechanism. The Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Discrete Fourier Transform (DFT) are tested for this task. The watermarked HEVC frames are transmitted through a wireless communication channel, and hence they become subject to different attacks and corruptions. At the receiver side, the secret watermarks in each block are sensed with a correlation-based method to discover dubious counterfeit operations. To verify the reliability of the suggested transmission framework and its ability to achieve high protection and robust content verification of the transmitted HEVC frames over insecure communication channels, different HEVC analyses and comparisons are performed. Simulation results demonstrate the suitability of the suggested transmission framework for different multimedia cybersecurity applications. Furthermore, the comparative analysis shows that the DFT is an efficient discrete transform that can be employed with the proposed transmission framework to guarantee a higher HEVC frame integrity. It allows higher sensitivity to simple modifications in the transmitted watermarked HEVC frames. This makes the suggested cybersecurity framework applicable, secure, and appropriate for multimedia integrity verification purposes.

INDEX TERMS HEVC cybersecurity, watermarking, DCT, DWT, DFT, integrity verification.

I. INTRODUCTION

With the fast progress in multimedia cybersecurity schemes, unlawful disclosing and alteration of distributed confidential secret data have become common issues. The data related to some applications such as cybersecurity and Internet applications can be categorized as highly-sensitive data. If illegal disclosing or modification is performed on this data without

The associate editor coordinating the review of this manuscript and approving it for publication was Zahid Akhtar¹.

authorization, this will result in severe adverse effects [1]. So, there is a high necessity to enhance the security of data during the transmission by guaranteeing availability, confidentiality and data integrity [2]. Confidentiality is the guarantee of data secrecy to allow authorized and intended receivers only to understand the sensitive data. Data integrity guarantees that the information has not been modified by an unlicensed party or any other transmission effect. Availability means that information resources are available in an efficient manner, when required for authorized users. The security violations

of highly-sensitive data transmission precautions affect the availability, confidentiality, and integrity. When the availability is violated, a serious process failure may occur [3]. Confidentiality violation (disclosure of restricted data) can assist a person or a group planning theft, sabotage, and other malevolent or illegal acts. Integrity violation (modification of highly-sensitive data) may disrupt the normal processing of data, and it tends to have a severe impact on this transmitted data. So, there is a large motivation to enhance the security of the transmitted multimedia data through an untrusted communication medium.

With the vast utilization of multimedia content, there is a need for non-degradable information transmission media. Unfortunately, the ease with which digital videos can be modified makes the verification of video integrity important. Consequently, the threat of copyright violations of multimedia information has grown because of the immense evolution of the Internet and communication networks. These networks offer rapid and error-free communication of unapproved duplicates and conceivably-manipulated versions of multimedia content.

Recently, data-hiding techniques have had a great importance in different security application areas [4]. Steganography and watermarking are the main trends of the fast-developing data hiding techniques. Encryption techniques are considered as other tools of data protection. They depend on changing the confidential source data such that it becomes impossible to be correctly interpreted, outside the closed loop of intended senders and recipients. Video steganography is the art of hiding secret video frames in other innocent video frames. Video encryption means the manipulation of multimedia data with an encryption technique to make the data unreadable by anyone, except the legitimate users. Video watermarking means the embedding of digital watermarks into video frames to achieve integrity and guarantee the ownership of the digital video content. Video steganography, watermarking, and encryption may be implemented in different domains [5]. In the simple steganography, a straightforward falsification may be employed on the video frame pixels without any transformations. In high-level steganography, certain transforms can be performed before the steganography process. The DCT, DFT, and DWT are considered as the most popular candidates for data hiding applications [6].

As a consequence of the widespread copyright violation of multimedia, watermarking of video frames has become of interest in data hiding, video authentication, identification, verification, and copyright control [7], [8]. There are various criteria according to which digital watermarking techniques are mainly classified like robustness, perceptibility degree, and methodology of data hiding and recovery. The robustness criterion illustrates the capability of the secret watermark to withstand the data alteration attacks. Watermarking techniques can be categorized as robust, fragile, or semi-fragile techniques [9]–[11]. A reliable and robust watermark is utilized for preserving security and copyright due to its capa-

bility to resist different types of processing. On the contrary, fragile watermarking is adopted for integrity verification. The embedded watermark sensitivity to any intentional or unintentional modifications may be used as a measure of content modification.

Digital video watermarking can be utilized to verify video content and integrity through embedding either an invisible or a visible watermark. In conventional watermarking techniques [9], [10], the decoder knows the watermarks utilized for comparison with the extracted watermarks. Therefore, these techniques require additional processing in watermark embedding, verification, and extraction. Moreover, most of the state-of-the-art watermarking techniques assume no channel noise and attack-free environments [9]–[14]. In practical scenarios, there are severe third parties and channel noise.

To prevent forgery and verify the image and video content integrity, some traditional methods have been introduced [12]–[17]. These methods must have high sensitivity to catch any little alterations, attacks, and tampering performed on the transmitted streams. In [1], the authors suggested a cost-effective commutative HEVC data hiding and encryption algorithm for video streaming applications. This algorithm allows encrypting a steganographic stream without obstructing with the concealed signal. It allows also executing the steganography process on a ciphered stream, whilst still permitting ideal deciphering. Moreover, it produces an HEVC bit stream with a format-compliance property. Numerous experimental evaluations on standard video streams of different contents and resolutions have been presented.

An informed detector model for HEVC frame transmission was suggested in [3]. For better perceptual quality, this model inserts the watermark into the P frames. Moreover, for better robustness and high security, the model selects the most proper HEVC blocks for watermark embedding purposes based on an arbitrary secret key and the spatio-temporal traits of the encoded HEVC stream. Massive security analyses have been performed to test the model efficiency. The outcomes proved that the model successfully regulates the bit rate increase and the perceptual video quality degradation. In addition, it is secure and robust in the presence of different image processing and re-encoding attacks.

In [4], a reversible separable HEVC encryption/hiding framework was introduced. In this framework, the RC4 algorithm is employed to encrypt the signs of the residual coefficients, and the motion vector differences in amplitudes and signs of the encoded HEVC frames. In addition, the hidden data are embedded into the residual non-zero AC coefficients of the compressed video frames. The simulation results proved that this framework introduces high security and robustness, while keeping the HEVC format compliance property. In [6], the authors suggested an efficient motion vector (MV) space-based HEVC encoding/hiding scheme. This scheme defines the mapping between the points in the MV space and the MV set. Simulation outcomes on various HEVC streams verified that this scheme introduces a better

performance than those of the existing MV-based data hiding schemes.

The authors of [7] presented an HEVC watermarking scheme in the compressed domain for improving the video content security. The watermark information is compressed using the biorthogonal phase transform, and then it is embedded in the HEVC quantized coefficients based on singular value decomposition. The test outcomes revealed that the secret watermark information is efficiently extracted by increasing the value of the quantization parameter. Moreover, this watermarking scheme achieves a better performance in the presence of noise attacks. In [8], two different multi-stage HEVC security frameworks were introduced depending on watermarking, encryption, and fusion techniques. The first HEVC security framework is based on a hybrid structure of singular value decomposition and homomorphic transform in the DWT domain. The second framework is based on the utilization of the discrete stationary wavelet transform in the DCT domain. Both introduced HEVC security frameworks adopt DWT fusion of multiple watermarks before embedding in the compressed HEVC frames. In addition, the presented security frameworks employ chaotic encryption for ciphering of the fused watermarks before the embedding process. The experimental findings proved the superior performance of both introduced multi-level HEVC security frameworks in the presence of various channel attacks.

In [11], the authors suggested a robust HEVC intra-drift-free embedding/extraction algorithm that is based on a multi-coefficient modification scheme. The embedding algorithm inserts the watermark data into the HEVC intra-frames in the compressed domain. The simulation tests on different standard streams validated the efficiency of this HEVC watermarking algorithm with superior robustness and imperceptibility compared to the existing HEVC watermarking algorithms. The authors of [13] introduced a blind HEVC watermarking scheme in the compressed and phase domains. This scheme is based on the utilization of complex Hadamard transform and a conjugate symmetric transform in the DFT domain. Simulation results demonstrated that the introduced watermarking scheme offers acceptable subjective and objective outcomes with good imperceptibility and robustness in the presence of multimedia attacks.

A video-watermarking-based tampering detection algorithm in the compressed domain was introduced for real-time multimedia authentication applications [16]. It adopts a DCT embedding strategy. The experimental outcomes reveal that this algorithm can detect the occurrence of spatio-temporal, temporal, and spatial tempering. Moreover, it introduces higher robustness, minimal increase in the video bit rate, less video distortion, and an acceptable embedding capacity in contrast to the existing related algorithms. In [17], the authors suggested a copyright protection algorithm for HEVC watermarking based on the discrete sine transform (DST) using scrambled watermarks that are inserted into the intermediate frequency-domain coefficients of the compressed HEVC luminance component. The experimental findings demon-

strated that this algorithm has a terrific embedding/extraction performance in the presence of video attacks.

In [18], an H.265/HEVC video watermarking algorithm was presented for embedding secret watermarks in the I and P compressed frames to improve the copyright protection of video streaming services. This algorithm minimizes the overall video degradation with the possibility of embedding multiple watermarks. In [19], the authors introduced an HEVC hiding scheme for intra-compressed frames in the DCT and DST domains. The secret watermark is inserted into the DST or DCT coefficients. The test outcomes confirm that this video hiding scheme has the advantage of no errors, low bit rate coding, and higher embedding capacity compared to the previous related algorithms.

In [20], an enhanced video integrity verification system based on a watermarking algorithm was presented. This algorithm differentiates attacks against video data from ordinary changes by isolating header hash and time code values inserted in the video data itself. The evaluation findings indicate that this integrity verification algorithm is better than the existing algorithms that employ the digital signature concept. In [21], an HEVC high-payload watermarking algorithm was introduced. This algorithm is applicable in different multimedia applications including metadata hiding and broadcasting. The secret watermark is inserted into the quantized coefficients throughout the video compression procedure. Then, through the decoding procedure, the embedded watermark is completely extracted and detected. The simulation outcomes demonstrate that this watermarking algorithm presents higher video quality levels and minimal bit rates.

The authors of [22] presented a data-embedding-based HEVC authentication algorithm. The main advantage of this algorithm is that it contains two layers of authentication: video feature extraction, and weight generation. The experimental outcomes on different classes of video streams confirm that the whole perceptual HEVC quality is preserved after the authentication code insertion, while introducing a higher capability of tampering detection. In [23], the authors introduced an efficient video integrity verification algorithm for digital forensic services. This algorithm verifies the video content integrity and achieves protection in legacy surveillance applications. It works on the MP4 or AVI video frames remaining in the slack space as an alternative for the timestamp data that is susceptible to tampering and manipulations.

A multi-stage HEVC authentication framework in compressed domain was introduced in [24]. This framework is based on securing the most sensitive HEVC coded units. It embeds an authentication tag in the temporal HEVC slices (QP parameter values, non-zero DCT coefficients, and prediction modes). This framework offers three authentication levels for detecting and localizing the tampered regions in the compressed HEVC stream. A comprehensive evaluation study has been performed on different classes of HEVC streams to validate the multi-layer authentication framework. The outcomes reveal that this framework presents higher

perceptual video quality in severe attack conditions. In [25], a video verification scheme was introduced for encrypted video content integrity using a homomorphic encryption algorithm for cloud computing applications. In this scheme, a dynamic strategy is employed to verify the video data integrity.

In [26], the authors introduced a hybrid approach for HEVC frame authentication and encryption in the compressed sensing domain. It ensures video format compliance that allows the authentication mechanism to be performed regardless of the HEVC stream nature, whether it is a plain-text or an encrypted stream. In this approach, a two-layer authentication process is adopted in the verification procedure. Moreover, the syntax elements of the Suffix Bins, Sign Bins, and Transform Skip Bins of the compressed HEVC frames are encrypted to completely hide the video content. The simulation outcomes prove that this approach could efficiently localize and detect the tampered regions compared to the conventional related authentication algorithms. In [27], an HEVC frame authentication algorithm based on a transform unit was introduced to identify the video data double compression process. This algorithm also protects the syntax elements of the prediction units and coding tree units in addition to its capability of HEVC double encoding detection. A support vector machine is employed to classify double and single encoded streams. The simulation outcomes prove the high performance level of the algorithm by offering higher-accuracy results.

In [28], an HEVC hiding/encryption system for cloud computing applications was proposed. The HEVC-CABAC strings are partially ciphered before the hiding process to preserve the format compliance feature. After performing the HEVC encryption, secret data is inserted into the ciphered frames with a specialized coefficient modification scheme. The main advantage of this system is that the deciphered video quality is satisfactory, because the HEVC frame coefficients are vaguely modified. In addition, the ciphered and marked HEVC bit streams meet the format compatibility requirements, while saving an identical bit rate. Furthermore, the merit of this system is that at the receiving side, the extraction of the secret data could be performed in the ciphered or deciphered domain. This video authentication system could be applicable and compatible with various application scenarios. More evaluations on standard HEVC streams for testing the security performance of this hiding/encryption system were performed revealing the superiority of the introduced system compared to the related authentication systems.

Although some works were introduced for video authentication and integrity verification in the presence of attacks and noise, they do not achieve reliable authentication against most types of attacks. They are also not robust to channel noise attacks. Therefore, this work introduces a reliable and secure HEVC integrity verification cybersecurity transmission framework. It is characterized by video self-embedding-based watermarking. This framework aims to verify the HEVC integrity and enhance the confidentiality of distributed

highly-sensitive data. It provides higher protection of digital transmitted HEVC frames and avoids severe impacts of security violations. The data integrity is verified through the proposed transmission framework, while imperceptibility is maintained. Thus, it is fundamentally aimed to verify and enforce the two basic security objectives of confidentiality and integrity for transmitted digital HEVC data whether for cybersecurity applications or for transmission over an untrusted communication medium.

Therefore, the main key contributions of this paper can be summarized as follows:

- Proposal of self-embedding-based video integrity verification and transmission framework that is robust and reliable for verifying the integrity of HEVC frames transmitted through insecure communication channels.
- Investigation of the integrity verification performance with different discrete transforms for determining the best one that efficiently allows authentication of HEVC streams transmitted through insecure communication channels.
- Determination of the optimum block size of the HEVC frames that achieves the best integrity verification performance with a high ability of tampering detection.
- Extensive statistical analysis of attack and noise effects on the tampering detection task of the suggested integrity verification framework.
- The proposed self-embedding-based HEVC integrity verification framework has the capability of embedding different watermarks in different HEVC blocks, where each block can have a different watermark from another neighbouring block within the same HEVC frame. This introduces a great advantage of increasing HEVC frame security.
- The proposed integrity verification framework achieves both high imperceptibility and high tampering detection sensitivity even in the case of simple and tiny manipulations and modifications in the transmitted watermarked HEVC frames.

The rest of this work is coordinated as follows. Section 2 demonstrates the basics of different transforms that can be used for data embedding. The suggested HEVC integrity verification and transmission framework is explained in detail in section 3. The extensive simulation and comparison outcomes are analyzed in section 4. Finally, section 5 gives the conclusions and the future work.

II. DISCRETE TRANSFORMS FOR DATA EMBEDDING

Transform-domain data embedding techniques have proved better embedding performance than that of spatial-domain data embedding. The most popular transform-domain techniques utilized for data embedding are the DCT, DWT, and DFT. Most transform-domain watermarking techniques hide the watermarks inside the transform coefficients of the host video frames. After coefficient conversion, the data is transformed again into the spatial domain [18]–[20].

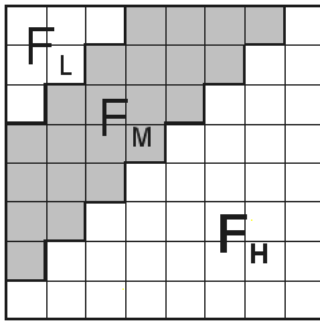


FIGURE 1. DCT regions.

A. DISCRETE COSINE TRANSFORM (DCT)

The DCT represents a dedicated data series as a summation of cosine functions oscillating at various frequencies. The 2D-DCT is often used in image and video processing [19]. When it is used on a video frame, it separates it into high-, medium-, and low-frequency elements (FH, FM, and FL) as indicated in Fig. 1. The low-frequency range comprises most energy of the input frame. On contrary, the high-frequency components may be affected by noise or compression. So, for the watermark embedding process, the middle-frequency coefficients are utilized. This has a little effect on video frame visibility and impracticability [29]–[31].

Generally, the DCT of an $M \times N$ video frame $f(x, y)$ can be defined by Eq. (1) as:

$$F_{DCT}(u, v) = a(v)a(u) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \cos\left(\frac{\pi u(2x+1)}{2M}\right) \times \cos\left(\frac{\pi v(2y+1)}{2N}\right) \quad (1)$$

where the u has values of $0, 1, 2, \dots, M-1$ and v has values of $0, 1, 2, \dots, N-1$.

B. DISCRETE WAVELET TRANSFORM (DWT)

The DWT separates a video frame into four different sub-bands. The low-resolution approximation sub-band (LL) contains low-frequency wavelet coefficients constituting the significant power of the video frame. The diagonal (HH), vertical (LH), and horizontal (HL) detail components are high-frequency sub-bands of the video frame in which the edges and texture details exist. This procedure can be repeated to compute multi-scale wavelet decomposition. Figure 2 shows an illustration of the two-level DWT [32].

C. DISCRETE FOURIER TRANSFORM (DFT)

The DFT is considered as one of the main signal processing tools. For a two-dimensional video frame $f(x, y)$ with a size of $M \times N$, the definitions of the DFT and the inverse DFT are given as in Eqs. (2) and (3), respectively [33]:

$$F_{DFT}(u, v) = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) e^{-j2\pi(ux/M+vy/N)} \quad (2)$$

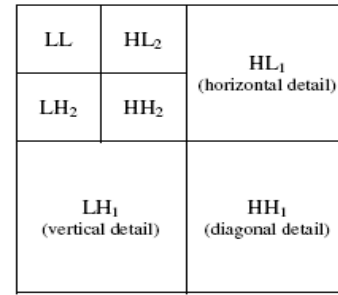


FIGURE 2. 2D DWT regions.

$$f(x, y) = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F_{DFT}(u, v) e^{j2\pi(ux/M+vy/N)} \quad (3)$$

The DFT of a video frame is complex with certain phase and magnitude components of the video frame. The secret watermark may be inserted into the phase or the magnitude. Some watermarking schemes depend on the amplitude of the DFT due to the shift-invariance property. The phase of the DFT may also be exploited for its sensitivity to changes.

III. THE PROPOSED HEVC SELF-EMBEDDING SECURITY FRAMEWORK

In this section, the proposed framework is explained in detail. It is utilized for achieving confidence, integrity verification, and tampering detection. The proposed framework consists of two modules. The first module is exploited for watermarking and the second module is employed for verification. The two modules are discussed and explained below. Since the main objective of this work is the tampering detection, a fragile self-embedding process is employed. It is simple, efficient, and robust as it is based on block-based self-watermarking in the embedding process instead of utilizing external watermarks. Therefore, the proposed self-embedding-based HEVC integrity verification framework has the capability of embedding different and multiple watermarks in different HEVC blocks. Each block has a different watermark from another neighboring block within the same HEVC frame. This introduces a great advantage of detecting simple and tiny manipulations in the transmitted watermarked HEVC frames. Moreover, it keeps the perceptual HEVC frame quality.

A. THE PROPOSED PROTECTION MODULE

The protection module is described in a stepwise manner with a Transform Domain (TD) technique, which is the DCT, DFT, or DWT. The steps of the proposed protection module are summarized as follows:

1. Dividing the input HEVC frame (f) into two similar parts f_1 and f_2 . After that, the f_1 and f_2 parts are divided into different non-overlapping 4×4 , 8×8 , 16×16 , 32×32 , 64×64 , or 128×128 blocks.
2. Implementation of the discrete transform on each block of f_1 and f_2 .

3. Insertion of certain rows and columns from each block of f_1 into a corresponding block of f_2 and vice versa. For example, the first row and column of the DCT of a block are weighted and inserted in the last row and column of the DCT of the corresponding block. The first row and column are selected as they have most of the block energy. They are weighted with a small weight and inserted in the last row and column of another block to avoid deterioration of the overall frame quality.
4. Implementation of the inverse discrete transform on each block.
5. Rearrangement of the HEVC frame.

B. THE PROPOSED VERIFICATION MODULE

The following steps describe the flow of the watermark extraction and verification module:

- 1) Receiving the watermarked HEVC frame.
- 2) The watermarked HEVC frame (z) is divided into two similar parts z_1 and z_2 . After that, the z_1 and z_2 parts are divided into different non-overlapping 4×4 , 8×8 , 16×16 , 32×32 , 64×64 , or 128×128 blocks.
- 3) The discrete transform is applied on each block.
- 4) Inserted rows and columns in f_2 are extracted and correlated with the corresponding ones in f_1 and vice versa. The correlation coefficient values are used as indicators for HEVC frame manipulation. Low correlation values ensure frame manipulation, while high values ensure frame integrity.

IV. SIMULATION RESULTS AND COMPARATIVE ANALYSIS

Several experiments on standard (Ballroom, Dancer, Exit, and Kendo) HEVC sequences have been carried out. Sample frames are shown in Fig. 3. The proposed framework has been evaluated with DCT, DWT, and DFT embedding techniques and different non-overlapping blocks of size 4×4 , 8×8 , 16×16 , 32×32 , 64×64 , and 128×128 .

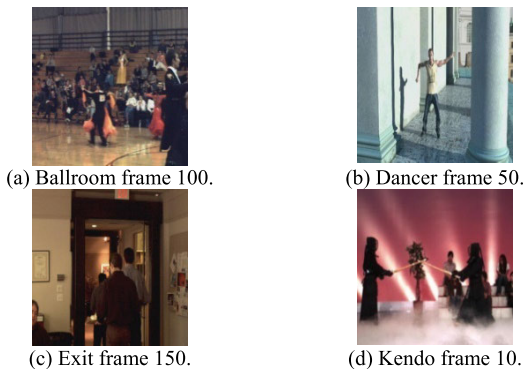


FIGURE 3. Different samples of input original HEVC frames.

We use statistical analysis to evaluate the detection sensitivity of the proposed framework. Statistical analysis is necessary to demonstrate the high level of sensitivity of the proposed framework to any small manipulation attacks.

The evaluation metrics utilized for evaluating the proposed framework are the correlation coefficient (C_r) between the original watermarks and the extracted watermarks, the Peak Signal-to-Noise Ratio ($PSNR$), the Mean Square Error (MSE) of the HEVC frames after watermark embedding, and the degree of similarity between the HEVC frame histograms before and after watermark embedding. The correlation is measured for all blocks of HEVC frames and plotted as shown in Tables 4, 6, 8, and 10.

The correlation coefficient is estimated with Eq. 4 as follows.

$$C_r = \frac{N^2 \cdot cov(X, Y)}{\sum_{i=1}^N (X_i - E_X)^2 \cdot \sum_{i=1}^N (Y_i - E_Y)^2} \tag{4}$$

where $cov(X, Y) = E((X - E_X)(Y - E_Y))$. X and Y are the vectors of the embedded and extracted watermarks, respectively. Both E_X and E_Y are the means of X and Y , respectively.

The MSE is estimated between original and watermarked HEVC frames as follows:

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (f(i, j) - f'(i, j))^2 \tag{5}$$

where $f(i, j)$ is the intensity of the original HEVC frame and $f'(i, j)$ is the intensity of the watermarked HEVC frame. The $PSNR$ is a metric that is used for ranking of the quality of the watermarked HEVC frame taking the original one as a reference. It can be formulated mathematically as in equation (6). A higher $PSNR$ value is an indication of high watermarked HEVC frame quality.

$$PSNR = 10 \log \left(\frac{255^2}{MSE} \right) \tag{6}$$

In the following sections, we present the statistical performance analysis of the proposed verification module with and without attacks. In addition, the effect of Additive White Gaussian Noise (AWGN) is also considered.

A. EVALUATION OF THE PROTECTION MODULE

The performance evaluation of the suggested protection module is investigated in this section through estimation of the MSE , $PSNR$, and C_r metrics. Firstly, they are estimated for every used transform to determine which transform is more suitable and efficient for the proposed framework. The correlation coefficient, the MSE , and the $PSNR$ values are estimated for each watermarked HEVC frame with different block sizes of 128×128 , 64×64 , 32×32 , 16×16 , 8×8 , and 4×4 , and are listed in Tables 1, 2, and 3. Higher correlation coefficient, higher $PSNR$, and lower MSE values are recommended for a better protection process.

From the preliminary outcomes in Tables 1, 2, and 3, it is remarked that the performance of the proposed framework using DCT or DWT embedding deteriorates as the block size is decreased, while the performance of the proposed framework using DFT is enhanced as the block size is decreased.

TABLE 1. Quality metrics for the watermarked HEVC frames with DCT embedding and different block sizes.

| Block Size | Video Quality Metrics | | | | | | | | | | | |
|------------|-----------------------|--------|--------|--------|----------|---------|---------|---------|----------|--------|--------|--------|
| | MSE | | | | PSNR | | | | C_r | | | |
| | Ballroom | Dancer | Exit | Kendo | Ballroom | Dancer | Exit | Kendo | Ballroom | Dancer | Exit | Kendo |
| 128×128 | 0.0043 | 0.0076 | 0.0032 | 0.0079 | 77.887 | 75.3662 | 79.2438 | 75.3077 | 1 | 1 | 1 | 1 |
| 64×64 | 0.0082 | 0.0158 | 0.0079 | 0.0148 | 75.0844 | 72.1942 | 76.2691 | 72.5618 | 1 | 1 | 1 | 1 |
| 32×32 | 0.0161 | 0.0329 | 0.0292 | 0.0272 | 72.1824 | 69.0200 | 73.323 | 69.9221 | 1 | 1 | 1 | 1 |
| 16×16 | 0.0380 | 0.0732 | 0.0274 | 0.0552 | 68.4134 | 65.5486 | 69.9095 | 66.8545 | 1 | 1 | 1 | 1 |
| 8×8 | 0.1800 | 0.2924 | 0.0973 | 0.1554 | 66.4139 | 59.5255 | 64.3615 | 62.3526 | 1 | 0.9999 | 1 | 1 |
| 4×4 | 1.2827 | 3.1866 | 0.6069 | 0.8038 | 53.11 | 49.165 | 56.5185 | 55.1862 | 0.9996 | 0.9995 | 0.9999 | 0.9999 |

TABLE 2. Quality metrics for the watermarked HEVC frames with DWT embedding and different block sizes.

| Block Size | Video Quality Metrics | | | | | | | | | | | |
|------------|-----------------------|--------|--------|--------|----------|---------|---------|---------|----------|--------|--------|--------|
| | MSE | | | | PSNR | | | | C_r | | | |
| | Ballroom | Dancer | Exit | Kendo | Ballroom | Dancer | Exit | Kendo | Ballroom | Dancer | Exit | Kendo |
| 128×128 | 174.930 | 297.09 | 85.746 | 369.92 | 32.0227 | 29.4616 | 35.3778 | 28.800 | 0.9488 | 0.9556 | 0.9800 | 0.9592 |
| 64×64 | 313.049 | 540.21 | 183.29 | 610.5 | 32.0227 | 26.8627 | 32.0937 | 26.4300 | 0.9088 | 0.9216 | 0.8584 | 0.9307 |
| 32×32 | 560.179 | 1269.1 | 375.01 | 1129.9 | 26.9124 | 23.154 | 28.9258 | 23.7298 | 0.8475 | 0.8312 | 0.9141 | 0.8736 |
| 16×16 | 5947.86 | 2197.4 | 645.09 | 2056.7 | 24.336 | 20.7692 | 26.5607 | 21.1097 | 0.7348 | 0.7378 | 0.8510 | 0.7768 |
| 8×8 | 1832.53 | 3862.9 | 1227.5 | 3816.5 | 21.814 | 18.319 | 23.782 | 18.4251 | 0.5633 | 0.6034 | 0.7387 | 0.6038 |
| 4×4 | 3133.5 | 39381. | 2115.9 | 6512.3 | 19.482 | 15.965 | 21.4225 | 16.105 | 0.3333 | 0.4302 | 0.5693 | 0.3319 |

TABLE 3. Quality metrics for the watermarked HEVC frames with DFT embedding and different block sizes.

| Block Size | Video Quality Metrics | | | | | | | | | | | |
|------------|-----------------------|--------|--------|--------|----------|---------|---------|---------|----------|--------|--------|--------|
| | MSE | | | | PSNR | | | | C_r | | | |
| | Ballroom | Dancer | Exit | Kendo | Ballroom | Dancer | Exit | Kendo | Ballroom | Dancer | Exit | Kendo |
| 128×128 | 53.2823 | 13.214 | 31.699 | 224.01 | 37.2640 | 42.983 | 39.7700 | 30.7030 | 0.9453 | 0.9581 | 0.9593 | 0.9296 |
| 64×64 | 44.8649 | 22.916 | 21.447 | 80.594 | 38.0499 | 40.6017 | 41.4187 | 35.198 | 0.9543 | 0.9611 | 0.9771 | 0.9548 |
| 32×32 | 53.2589 | 15.354 | 17.218 | 40.893 | 37.1327 | 42.324 | 42.1061 | 38.0942 | 0.9522 | 0.9686 | 0.9815 | 0.9743 |
| 16×16 | 31.8377 | 13.587 | 6.2873 | 18.155 | 36.2336 | 42.8588 | 46.3090 | 41.6723 | 0.9641 | 0.9769 | 0.9894 | 0.9879 |
| 8×8 | 15.2166 | 8.9524 | 2.8778 | 7.4154 | 42.3733 | 44.666 | 49.6053 | 45.5564 | 0.9779 | 0.9856 | 0.9926 | 0.9944 |
| 4×4 | 2.8804 | 3.2692 | 16.750 | 1.3181 | 49.5935 | 49.0381 | 57.0239 | 53.0301 | 0.9911 | 0.9941 | 0.9971 | 0.9980 |

More specifically, with DFT embedding, the best results in terms of lower *MSE*, higher *PSNR*, and higher C_r values are obtained with a block size of 4×4 . On the other hand, with DCT and DWT embedding, the best results are observed with a large block size of 128×128 .

For building a robust and effective data integrity verification and protection framework, it is necessary to embed the watermarks in as many blocks as possible without affecting the HEVC frame visibility. Therefore, it is recommended to use the proposed protection and verification framework with smaller HEVC block sizes. Thence, the proposed framework employing DFT embedding is the best compared to those that depend on the DCT and DWT embedding techniques. This is attributed to the fact that the DFT embedding technique achieves the lowest *MSE*, the highest *PSNR*, and the highest C_r values at the optimum block size of 4×4 .

Therefore, from Tables 1, 2, and 3, it is noticed that the results of the proposed framework using the DFT embedding technique are better than those obtained by employing the DWT and the DCT embedding techniques, especially with a

block size of 4×4 . Henceforth, the proposed framework with DFT embedding is the best recommended choice for HEVC cybersecurity applications with small block sizes.

Table 4 shows the visual results obtained with the four tested original HEVC frames and their histograms, the watermarked HEVC frames and their histograms, and the block-based correlation coefficients with the DFT embedding technique and a block size of 4×4 . From the results presented in Table 4, it is indicated that the proposed framework with the DFT embedding technique achieves appreciated outcomes of imperceptibility and unchanged HEVC frame histograms.

It is clear from Table 4 that there is a coincidence between the watermarked and the original HEVC frames for all tested streams. Moreover, the resulting histograms are identical. In addition, the proposed framework with DFT embedding achieves high correlation values for all tested HEVC frames. All these results demonstrate that the proposed framework with DFT embedding is a recommended choice for achieving robust protection and data integrity verification.

TABLE 4. Simulation results of the protection module, the original HEVC frames and their histograms, the watermarked frames and their histograms, and the correlation using DFT embedding with a 4×4 block size.

| HEVC stream | Obtained results | | |
|-------------|--------------------------------|--------------------------------|--|
| Ballroom | a. Original Image | b. Watermarked Image | |
| | c. Histogram of original Image | d. Histogram of forensic Image | |
| | | | |
| | | | |
| Dancer | a. Original Image | b. Watermarked Image | |
| | c. Histogram of original Image | d. Histogram of forensic Image | |
| | | | |
| | | | |
| Exit | a. Original Image | b. Watermarked Image | |
| | c. Histogram of original Image | d. Histogram of forensic Image | |
| | | | |
| | | | |
| Kendo | a. Original Image | b. Watermarked Image | |
| | c. Histogram of original Image | d. Histogram of forensic Image | |
| | | | |
| | | | |

B. EVALUATION OF THE VERIFICATION MODULE WITHOUT ATTACKS

In addition to testing the performance efficiency of the protection module in the previous section, the verification module of the proposed self-embedding cybersecurity framework is evaluated in three scenarios. Firstly, the verification model is tested with the assumption that the transmission medium is free from errors, and there are no attacks on the watermarked HEVC frames. Secondly, the verification model is tested with attacks. Finally, the verification model is tested in the presence of the AWGN through the transmission process. In this section, we discuss the first scenario of no attacks, and the results are given in Table 5.

As usual, lower *MSE*, higher *PSNR*, and higher correlation values indicate a better verification process. From the results presented in Table 5, it is observed that the best results are obtained with a block size of 4×4 . In general, the proposed framework using the DFT embedding is the best recommended choice for achieving a robust verification process with small block sizes.

To examine the reliability of the proposed HEVC integrity verification framework, we investigated the results of the four tested HEVC streams that have different visual properties. Table 6 shows the visual results of the four tested HEVC frames and their histograms, HEVC frames after watermark extraction and their histograms, and the correlation

TABLE 5. Quality metrics for watermarked HEVC frames of the verification process using the DFT embedding without attacks.

| Block Size | Video Quality Metrics | | | | | | | | | | | |
|------------|-----------------------|---------|---------|---------|----------|---------|---------|---------|----------------|--------|--------|--------|
| | MSE | | | | PSNR | | | | C _v | | | |
| | Ballroom | Dancer | Exit | Kendo | Ballroom | Dancer | Exit | Kendo | Ballroom | Dancer | Exit | Kendo |
| 128×128 | 53.9021 | 16.5463 | 32.7901 | 224.067 | 37.223 | 42.0158 | 39.6230 | 30.7018 | 0.94606 | 0.9391 | 0.9597 | 0.9227 |
| 64×64 | 44.3837 | 24.0133 | 22.2613 | 83.2940 | 38.0862 | 40.4005 | 41.2030 | 35.0368 | 0.9557 | 0.9623 | 0.9722 | 0.9558 |
| 32×32 | 54.2513 | 18.8000 | 18.2513 | 44.7823 | 37.0628 | 41.4458 | 41.8716 | 37.6967 | 0.9547 | 0.9701 | 0.9884 | 0.9755 |
| 16×16 | 32.6467 | 16.1904 | 6.9128 | 21.9716 | 39.1522 | 42.1077 | 45.9559 | 40.8501 | 0.9677 | 0.9793 | 0.9905 | 0.9890 |
| 8×8 | 18.1724 | 16.6238 | 5.1518 | 11.2307 | 41.6788 | 42.0535 | 47.2279 | 43.8171 | 0.9823 | 0.9883 | 0.9941 | 0.9955 |
| 4×4 | 9.5266 | 12.6309 | 3.5544 | 5.9354 | 44.8533 | 43.6154 | 49.2175 | 46.9356 | 0.9950 | 0.9967 | 0.9984 | 0.9989 |

TABLE 6. Simulation results of the verification module without attacks, original HEVC frames and their histograms, frames after watermark extraction and their histograms, and correlation values with DFT embedding using a 4 × 4 block size.

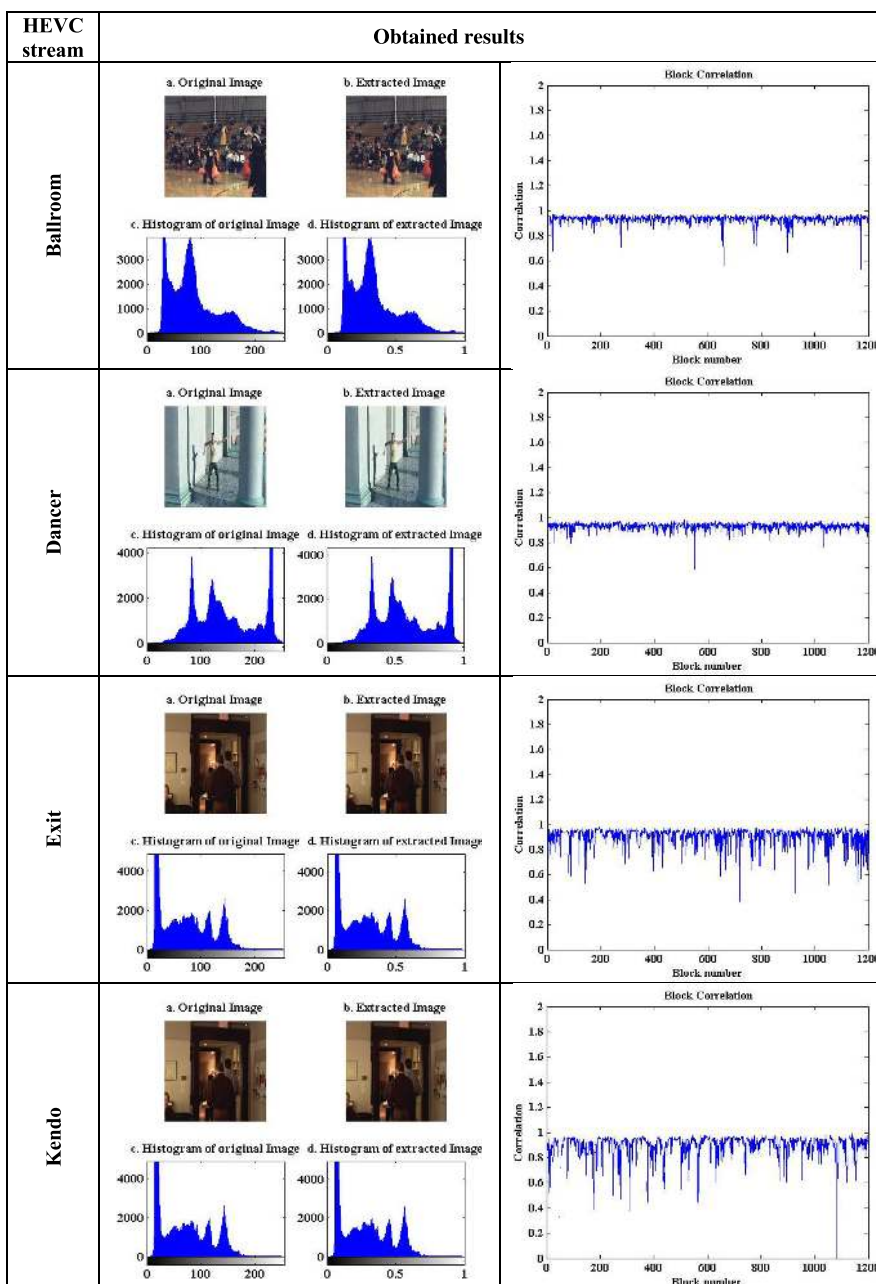


TABLE 7. Quality metrics for the verification process with DFT embedding using a 4×4 block size in the presence of different types of attacks.

| Attack Type | Video Quality Metrics | | | | | | | | | | | |
|------------------------|-----------------------|--------------------|--------------------|--------------------|----------|--------|--------|--------|----------|--------|---------|--------|
| | MSE | | | | PSNR | | | | C_r | | | |
| | Ballroom | Dancer | Exit | Kendo | Ballroom | Dancer | Exit | Kendo | Ballroom | Dancer | Exit | Kendo |
| Median filtering | 8.80×10^3 | 3.0×10^3 | 65×10^3 | 1.84×10^3 | 14.8113 | 9.9366 | 16.539 | 11.804 | 0.0233 | 0.0244 | -0.0045 | 0.023 |
| Blurring | 2.02×10^3 | 2.9×10^3 | 66×10^3 | 1.82×10^3 | 14.8145 | 9.9342 | 16.540 | 11.802 | 0.0202 | 0.0205 | -0.0050 | 0.019 |
| Cropping | 8.84×10^3 | 2.66×10^3 | 62.3×10^3 | 1.83×10^3 | 14.8282 | 9.9454 | 16.551 | 11.815 | 0.0251 | 0.2240 | 0.0013 | 0.029 |
| Intensity change | 8.90×10^3 | 2.67×10^3 | 65.3×10^3 | 1.85×10^3 | 14.7948 | 9.9134 | 16.518 | 11.787 | -0.0010 | 0.0017 | 0.0013 | -0.001 |
| Contrast change | 8.92×10^3 | 2.69×10^3 | 65.5×10^3 | 1.84×10^3 | 14.7998 | 9.9134 | 16.517 | 11.789 | -0.0010 | 0.0017 | 0.0013 | -0.001 |
| Block intensity change | 8.87×10^3 | 2.68×10^3 | 65.2×10^3 | 1.85×10^3 | 14.8128 | 9.9282 | 16.538 | 11.801 | -0.0275 | 0.530 | 0.0609 | -0.009 |
| Block sharpening | 8.84×10^3 | 2.67×10^3 | 64.8×10^3 | 1.83×10^3 | 14.8282 | 9.9454 | 16.551 | 11.815 | 0.0252 | 0.0225 | 0.0002 | 0.029 |

coefficients in the absence of attacks for DFT embedding with a 4×4 block size. It is clear from Table 6 that in the case of no modifications or attacks, there is a high visual similarity between the original HEVC frame and the HEVC frames after watermark extraction. It is noteworthy that the majority of block-by-block correlation coefficient values are close to unity, which confirms the efficiency and robustness of the proposed integrity verification module.

C. EVALUATION OF THE VERIFICATION MODULE WITH ATTACKS

The watermark detection sensitivity is considered as a major aspect related to the integrity verification module evaluation. It describes the ability of the proposed framework to detect any small video manipulation even it is visibly undetectable. To introduce a comprehensive assessment of the proposed framework performance, the detection sensitivity analysis is built upon two aspects. The first aspect is the statistical analysis. The second aspect is the visual detection, which depends on the visual properties of the output of the verification module. Most video manipulations with a forensic nature are intended to be visually undetectable, and the video receiver cannot visually detect the forensic act that usually has a severe impact on the video content.

Different statistical analyses are used to study the behavior of the verification module in the presence of different manipulation attacks. Small-scale video manipulation attacks are those manipulations that affect a small relative area of an intended video frame. In most cases, these attacks are mainly intended to be tampering acts, and usually the tampering cannot be visually detected. In this section, we will focus on studying the ability of the proposed framework to detect large-scale video manipulation attacks that affect a large relative area of an intended video frame. These modifications may be mainly performed with forgery intent such as video frame cropping, and other devious geometrical video processing actions. On the other hand, there may be an unintentional video modifications such as the existence of noise

that affects the transmitted video frames. However, in this section, we focus on different types of intentional large-scale attacks such as median filtering, video frame cropping, video frame intensity change, video frame contrast change, video frame block intensity change, and block sharpening.

Table 7 presents the results in terms of the *MSE*, *PSNR*, and C_r values for the four tested HEVC streams. Table 8 introduces the visual outcomes of the four tested original HEVC frames and their histograms, HEVC frames after watermark extraction and their histograms, and their block-based correlation coefficient values in the presence of different types of attacks using a 4×4 block size.

To have a highly sensitive and robust verification module against the introduced tampering and forgery attacks, we need to obtain the results at the receiver side with high *MSE*, low *PSNR*, and low C_r values. Therefore, from all presented results in Tables 7 and 8, it is observed that the proposed framework with DFT embedding demonstrates a high sensitivity to video manipulation attacks. In other words, these results prove the tampering detection capability and high robustness of the proposed framework based on DFT embedding in the presence of different modifications and attacks.

D. EVALUATION OF THE VERIFICATION MODULE WITH AWGN

The integrity verification module is implemented with an error-prone AWGN channel as a wireless medium. Here, the proposed module is examined at different Signal-to-Noise Ratio (*SNR*) values to validate its change detection sensitivity. The received HEVC frames and the HEVC frames after watermark extraction in the presence of AWGN with $SNR = 0, 10, 20, 30,$ and 40 dB are investigated. Table 9 presents the results in terms of the *MSE*, *PSNR*, and C_r values in the presence of AWGN with different channel *SNRs*. Table 10 introduces the visual results of the four tested HEVC frames and their histograms, HEVC frames after watermark extraction and their histograms, and the correlation coefficients in the

TABLE 8. Simulation results of the verification module with DFT embedding using a 4×4 block size in the presence of different types of attacks.



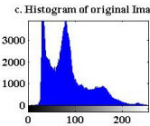
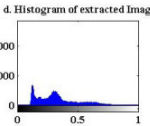
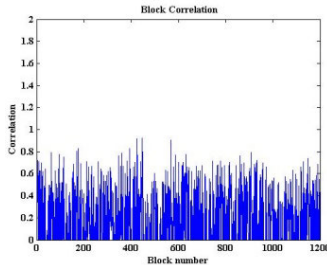


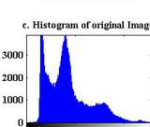
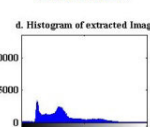
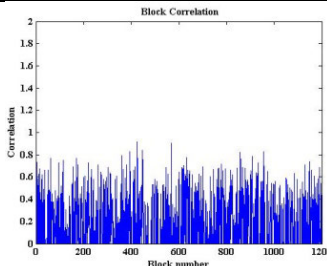


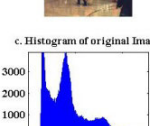
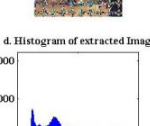
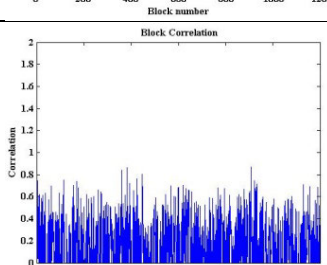


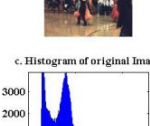
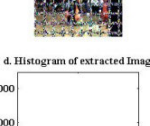
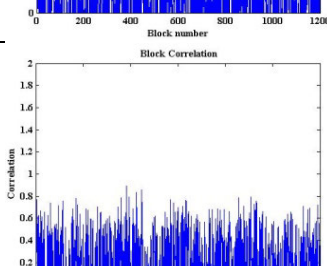


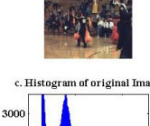
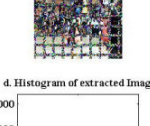
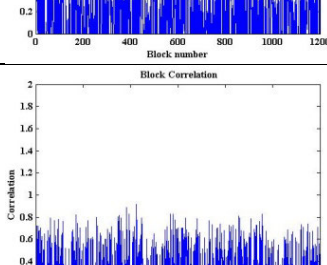


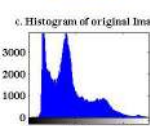
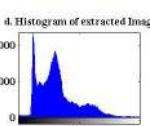
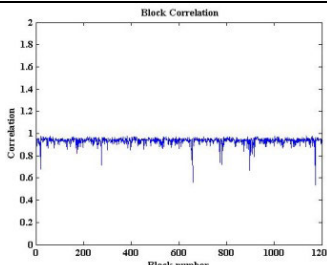
| HEVC stream | Type of Attack | Obtained results | | |
|-------------|------------------------------|--|--|--|
| Ballroom | Median filtering |     |  | |
| | Video frame blurring |     |  | |
| | Video frame cropping |     |  | |
| | Video frame intensity change |     |  | |
| | Video frame contrast change |     |  | |
| | Block intensity change |     |  | |

TABLE 8. (Continued.) Simulation results of the verification module with DFT embedding using a 4×4 block size in the presence of different types of attacks.



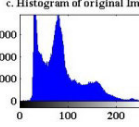
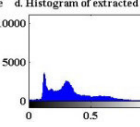
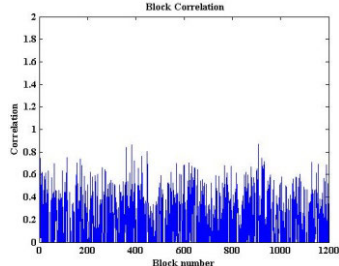


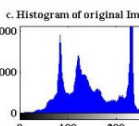
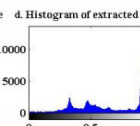
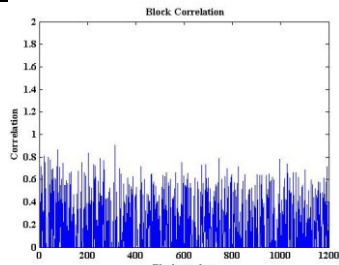


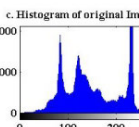
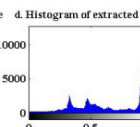
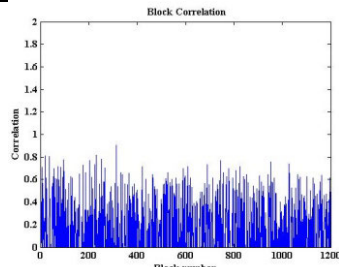


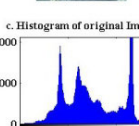
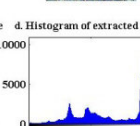
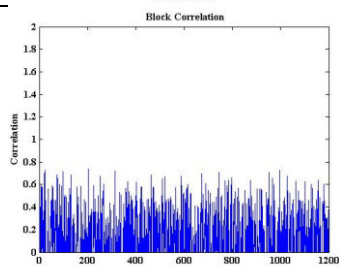


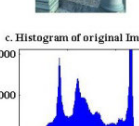
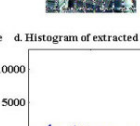
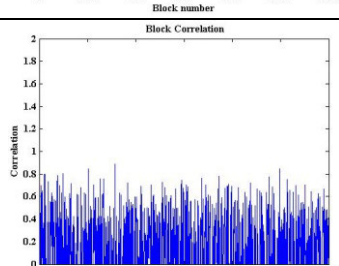


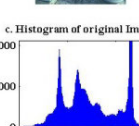
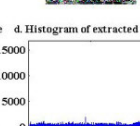
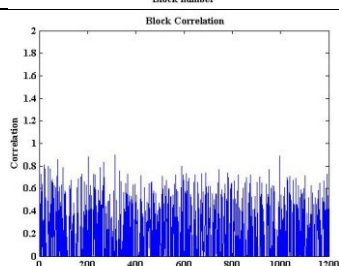
| | | | |
|---------------|-------------------------------------|--|--|
| | Block sharpening |     |  |
| Dancer | Median filtering |     |  |
| | Video frame blurring |     |  |
| | Video frame cropping |     |  |
| | Video frame intensity change |     |  |
| | Video frame contrast change |     |  |

TABLE 8. (Continued.) Simulation results of the verification module with DFT embedding using a 4×4 block size in the presence of different types of attacks.

| | | | |
|-------------|-------------------------------------|--|--|
| | Block intensity change | | |
| | Block sharpening | | |
| Exit | Median filtering | | |
| | Video frame blurring | | |
| | Video frame cropping | | |
| | Video frame intensity change | | |

TABLE 8. (Continued.) Simulation results of the verification module with DFT embedding using a 4×4 block size in the presence of different types of attacks.


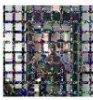
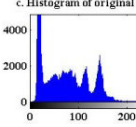
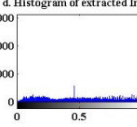
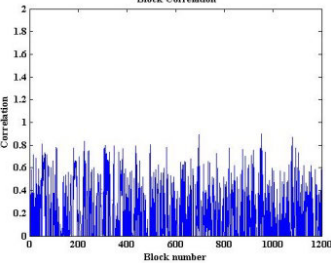


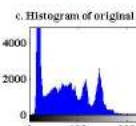
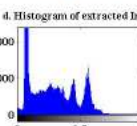
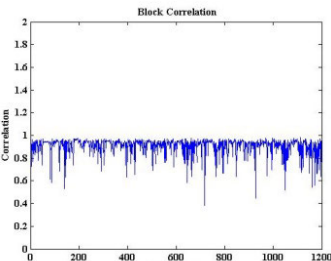


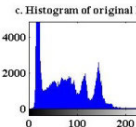
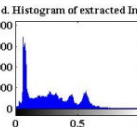
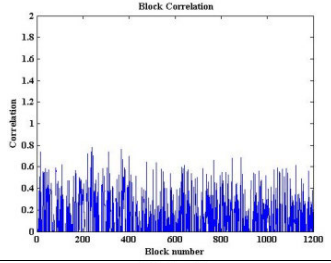


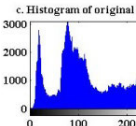
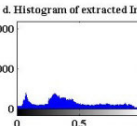
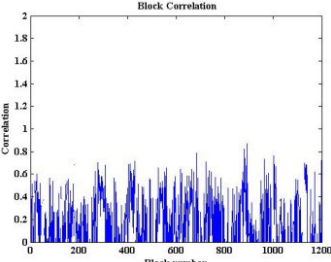

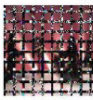
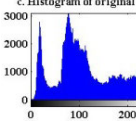
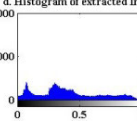
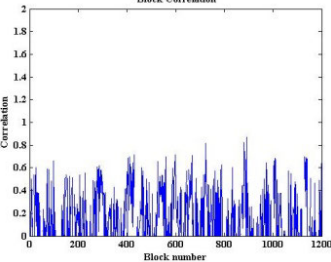


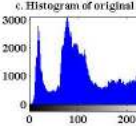
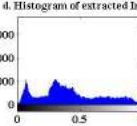
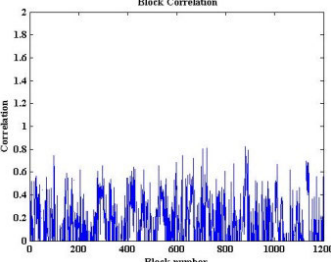
| | | | |
|-------|-----------------------------|--|--|
| Kendo | Video frame contrast change |     |  |
| | Block intensity change |     |  |
| | Block sharpening |     |  |
| | Median filtering |     |  |
| | Video frame blurring |     |  |
| | Video frame cropping |     |  |

TABLE 8. (Continued.) Simulation results of the verification module with DFT embedding using a 4×4 block size in the presence of different types of attacks.

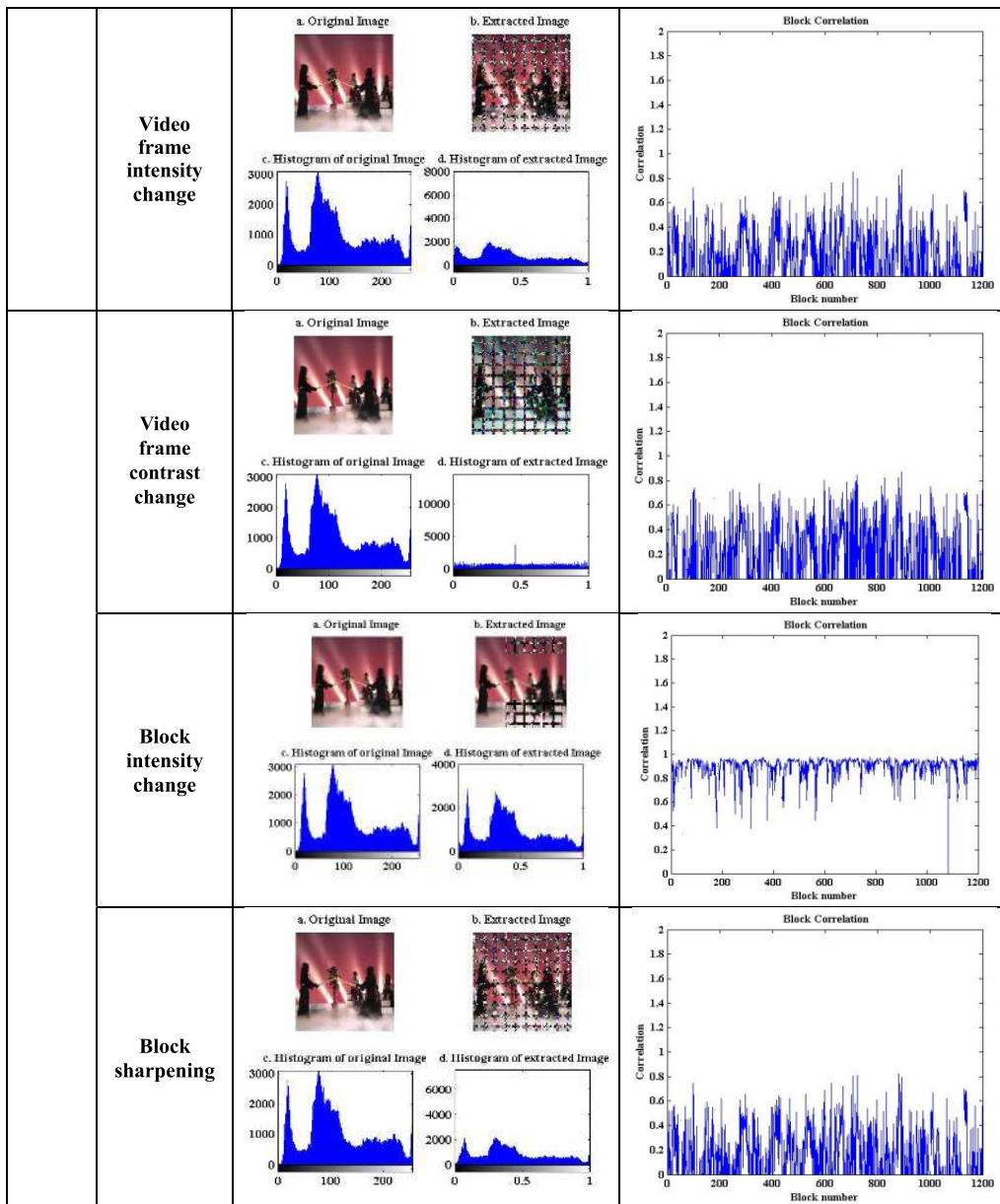


TABLE 9. Quality metrics for the verification module with DFT embedding using a 4×4 block size in the presence of AWGN.

| SNR | Video Quality Metrics | | | | | | | | | | | |
|-------|-----------------------|--------------------|--------------------|--------------------|----------|--------|---------|---------|----------|---------|---------|--------|
| | MSE | | | | PSNR | | | | C_r | | | |
| | Ballroom | Dancer | Exit | Kendo | Ballroom | Dancer | Exit | Kendo | Ballroom | Dancer | Exit | Kendo |
| 0 dB | 8.969×10^3 | 2.63×10^3 | 64.8×10^3 | 1.71×10^3 | 14.7724 | 9.9982 | 16.5750 | 11.8554 | 0.0047 | -0.0015 | 0.00087 | 0.0014 |
| 10 dB | 8.820×10^3 | 2.67×10^3 | 64.9×10^3 | 1.81×10^3 | 14.8413 | 9.9343 | 16.5498 | 11.8098 | 0.0018 | -0.0068 | -0.0035 | 0.0063 |
| 20 dB | 8.831×10^3 | 2.66×10^3 | 64.8×10^3 | 1.79×10^3 | 14.8340 | 9.9470 | 16.5533 | 11.8450 | 0.0047 | 0.0023 | 0.034 | 0.0053 |
| 30 dB | 8.829×10^3 | 2.65×10^3 | 64.8×10^3 | 1.78×10^3 | 14.8341 | 9.9476 | 16.5516 | 11.8228 | 0.0153 | 0.0010 | 0.0186 | 0.0180 |
| 40 dB | 8.831×10^3 | 2.65×10^3 | 64.8×10^3 | 1.76×10^3 | 14.8336 | 9.9473 | 16.5515 | 11.8226 | 0.0501 | 0.0392 | 0.0641 | 0.0577 |

presence of AWGN at different channel SNRs using a 4×4 block size.

Tables 9 and 10 show that the manipulated noisy HEVC frames appear to be visually unchanged, which means that

there is a difficulty in visual extraction of the changed information hidden in watermarked noisy frames. The tables also show that the proposed module has a high sensitivity to the AWGN channel. Therefore, the suggested verification

TABLE 10. Simulation results of the verification module with DFT embedding using a 4×4 block size in the presence of AWGN.



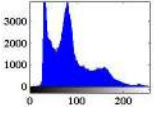
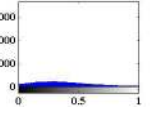
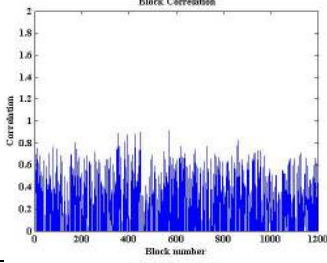


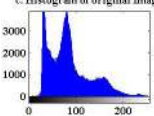
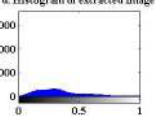
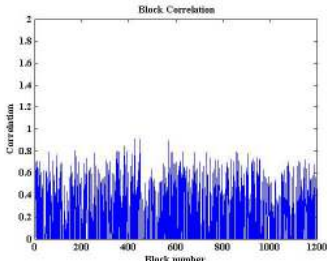


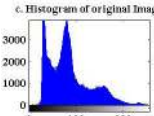
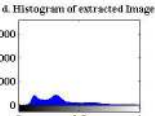
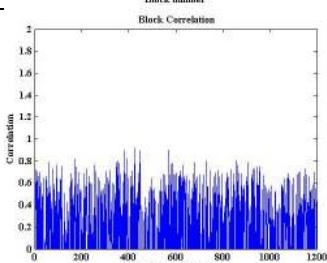


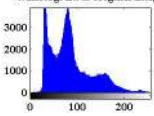
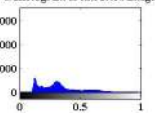
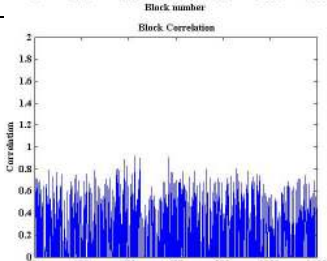


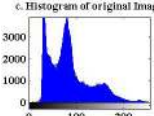
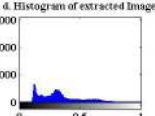
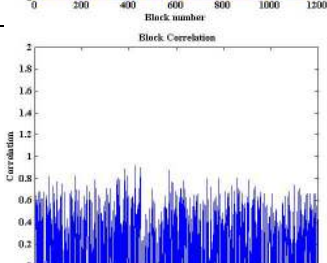


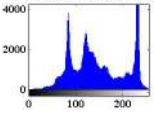
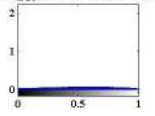
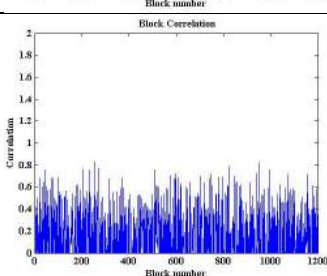
| HEVC stream | SNR | Obtained results | | |
|-------------|-------|--|--|--|
| Ballroom | 0 dB |     |  | |
| | 10 dB |     |  | |
| | 20 dB |     |  | |
| | 30 dB |     |  | |
| | 40 dB |     |  | |
| | 0 dB |     |  | |

TABLE 10. (Continued.) Simulation results of the verification module with DFT embedding using a 4 × 4 block size in the presence of AWGN.



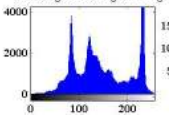
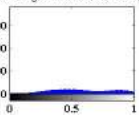
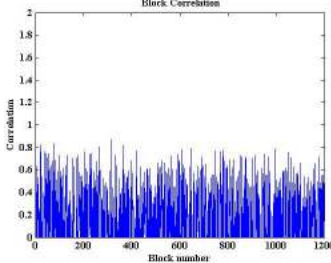


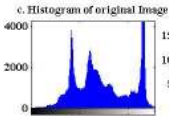
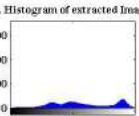
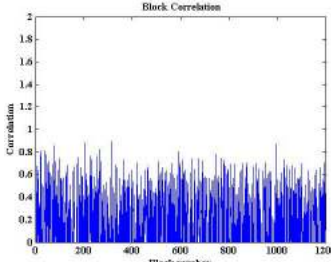


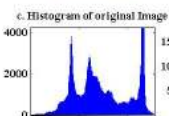
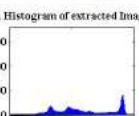
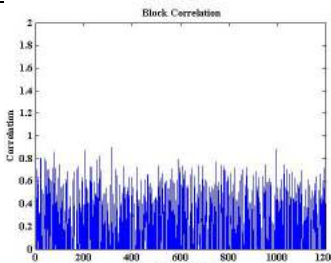


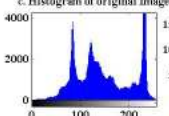
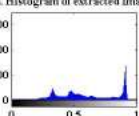
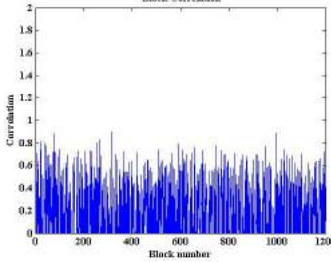


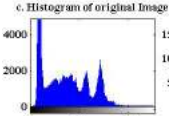
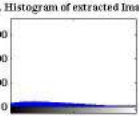
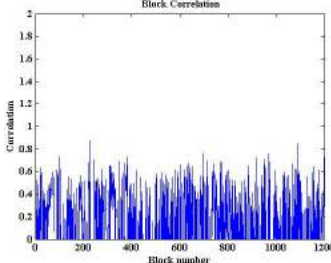

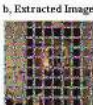
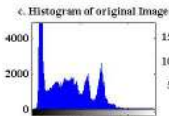
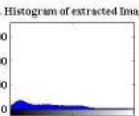
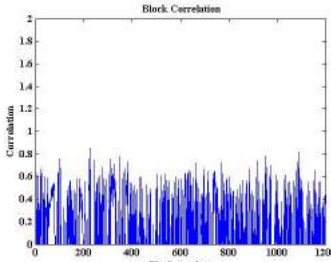
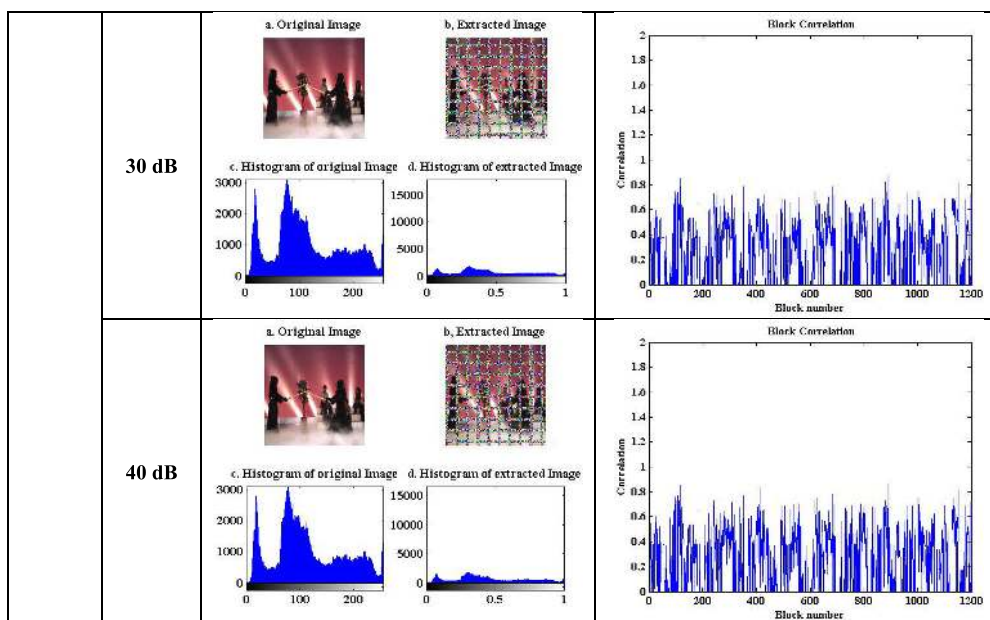
| | | | |
|--------|-------|--|--|
| Dancer | 10 dB |     |  |
| | 20 dB |     |  |
| | 30 dB |     |  |
| | 40 dB |     |  |
| | 0 dB |     |  |
| | 10 dB |     |  |

TABLE 10. (Continued.) Simulation results of the verification module with DFT embedding using a 4 × 4 block size in the presence of AWGN.

| | | | |
|-------|-------|--|--|
| Exit | 20 dB | | |
| | 30 dB | | |
| | 40 dB | | |
| Kendo | 0 dB | | |
| | 10 dB | | |
| | 20 dB | | |

TABLE 10. (Continued.) Simulation results of the verification module with DFT embedding using a 4 × 4 block size in the presence of AWGN.



framework is able to authenticate the HEVC frames. The correlation values and histogram results ensure the ability to detect the AWGN effect.

V. CONCLUSION AND FUTURE WORK

This paper introduced a high-fidelity HEVC protection and verification framework. This framework employs a certain transform technique for inserting internal block-based watermarks into other blocks of the transmitted HEVC frames. The DCT, DWT, and DFT embedding techniques have been examined in the proposed framework. The DFT embedding technique proves its efficiency to be more applicable according to the imperceptibility concept, high protection, secure verification, and high performance level. Simulation results proved the possibility of watermark protection and integrity verification, in addition to achieving high robustness against multimedia attacks and channel noise. The simulation results also revealed the high sensitivity of the proposed framework to different types of video tampering and channel noise, although the received tampered HEVC frames appear to be visually unchanged. It has been proved that the proposed HEVC integrity verification framework may be utilized for achieving confidential multimedia communication through unreliable wireless channels and detecting any forensic operations. In conclusion, the proposed framework applicability can be extended to guarantee HEVC frame confidence. For robust communication of HEVC frames, we target incorporating steganography and encryption approaches in the suggested cybersecurity framework to accomplish a better degree of protection for attaining an acceptable HEVC frame broadcasting with better integrity verification. Additionally,

we plan to develop and execute HEVC integrity verification procedures that encompass deep-learning-based protection tools.

REFERENCES

- [1] D. Xu, "Commutative encryption and data hiding in HEVC video compression," *IEEE Access*, vol. 7, pp. 66028–66041, 2019.
- [2] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-Sayed, E. A. Naeem, M. A. Alzain, J. F. Al-Amri, B. Soh, and F. E. A. El-Samie, "Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications," *IEEE Access*, vol. 8, pp. 42491–42503, 2020.
- [3] 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, pp. 1–24, Jan. 2017.
- [4] M. Long, F. Peng, and H.-Y. Li, "Separable reversible data hiding and encryption for HEVC video," *J. Real-Time Image Process.*, vol. 14, no. 1, pp. 171–182, Jan. 2018.
- [5] F. Y. Shih, *Digital Watermarking and Steganography: Fundamentals and Techniques*. Boca Raton, FL, USA: CRC Press, 2017.
- [6] J. Yang and S. Li, "An efficient information hiding method based on motion vector space encoding for HEVC," *Multimedia Tools Appl.*, vol. 77, no. 10, pp. 11979–12001, May 2018.
- [7] 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.
- [8] W. El-Shafai, E.-S.-M. El-Rabaie, M. El-Halawany, and F. E. A. El-Samie, "Efficient multi-level security for robust 3D color-plus-depth HEVC," *Multimedia Tools Appl.*, vol. 77, no. 23, pp. 30911–30937, Dec. 2018.
- [9] 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.
- [10] M. Asikuzzaman and M. R. Pickering, "An overview of digital video watermarking," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 9, pp. 2131–2153, Sep. 2018.
- [11] 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.

- [12] K. Meenakshi, K. Swaraja, and P. Kora, "A robust DCT-SVD based video watermarking using zigzag scanning," in *Soft Computing and Signal Processing*. Singapore: Springer, 2019, pp. 477–485.
- [13] K. Meenakshi, K. S. Prasad, and C. S. Rao, "Development of low-complexity video watermarking with conjugate symmetric sequency-complex Hadamard transform," *IEEE Commun. Lett.*, vol. 21, no. 8, pp. 1779–1782, Aug. 2017.
- [14] M. Botta, D. Cavagnino, and V. Pomponiu, "Protecting the content integrity of digital imagery with fidelity preservation: An improved version," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 10, no. 3, pp. 1–5, Apr. 2014.
- [15] X. Yu, C. Wang, and X. Zhou, "A survey on robust video watermarking algorithms for copyright protection," *Appl. Sci.*, vol. 8, no. 10, p. 1891, Oct. 2018.
- [16] M. Fallahpour, S. Shirmohammadi, M. Semsarzadeh, and J. Zhao, "Tampering detection in compressed digital video using watermarking," *IEEE Trans. Instrum. Meas.*, vol. 63, no. 5, pp. 1057–1072, May 2014.
- [17] G. Linjie and Z. Ming, "A HEVC video watermarking algorithm based on copyright protection," *Microcomput. Appl.*, vol. 11, p. 15, 2014.
- [18] Y. H. Seo, Y. S. Lee, and D. W. Kim, "H. 265/HEVC Video Watermarking Method with High Image Quality," *J. Broadcast Eng.*, vol. 24, no. 1, pp. 97–104, 2019.
- [19] 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.
- [20] I. Echizen, S. Singh, T. Yamada, K. Tanimoto, S. Tezuka, and B. Huet, "Integrity verification system for video content by using digital watermarking," in *Proc. Int. Conf. Service Syst. Service Manage.*, vol. 2, Oct. 2006, pp. 1619–1624.
- [21] S. Swati, K. Hayat, and Z. Shahid, "A watermarking scheme for high efficiency video coding (HEVC)," *PLoS ONE*, vol. 9, no. 8, Aug. 2014, Art. no. e105613.
- [22] 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.
- [23] S. Lee, J. E. Song, W. Y. Lee, Y. W. Ko, and H. Lee, "Integrity verification scheme of video contents in surveillance cameras for digital forensic investigations," *IEICE Trans. Inf. Syst.*, vol. 98, no. 1, pp. 95–97, 2015.
- [24] 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.
- [25] R. Liu, J. Liu, J. Zhang, and M. Zhang, "Video data integrity verification method based on full homomorphic encryption in cloud system," *Int. J. Digit. Multimedia Broadcast.*, vol. 2018, pp. 1–9, Oct. 2018.
- [26] Y. Tew, K. Wong, R. C.-W. Phan, and K. N. Ngan, "Separable authentication in encrypted HEVC video," *Multimedia Tools Appl.*, vol. 77, no. 18, pp. 24165–24184, Sep. 2018.
- [27] 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.
- [28] D. Xu, "Data hiding in partially encrypted HEVC video," *ETRI J.*, vol. 42, no. 3, pp. 446–458, Jun. 2020.
- [29] S. A. Parah, J. A. Sheikh, F. Ahad, N. A. Loan, and G. M. Bhat, "Information hiding in medical images: A robust medical image watermarking system for E-healthcare," *Multimedia Tools Appl.*, vol. 76, no. 8, pp. 10599–10633, Apr. 2017.
- [30] K. A. Al-Afandy, W. El-Shafai, E. S. M. El-Rabaie, F. E. A. El-Samie, O. S. Faragallah, A. El-Mhalaway, A. M. Shehata, G. M. El-Banby, and M. M. El-Halawany, "Robust hybrid watermarking techniques for different color imaging systems," *Multimedia Tools Appl.*, vol. 77, pp. 25709–25759, 2019.
- [31] L. Laouamer and O. Tayan, "A semi-blind robust DCT watermarking approach for sensitive text images," *Arabian J. Sci. Eng.*, vol. 40, no. 4, pp. 1097–1109, Apr. 2015.
- [32] O. Benrhouma, H. Hermassi, and S. Belghith, "Tamper detection and self-recovery scheme by DWT watermarking," *Nonlinear Dyn.*, vol. 79, no. 3, pp. 1817–1833, Feb. 2015.
- [33] M. Urvoy, D. Goudia, and F. Atrousseau, "Perceptual DFT watermarking with improved detection and robustness to geometrical distortions," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 7, pp. 1108–1119, Jul. 2014.



OSAMA S. FARAGALLAH received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees in computer science and engineering from Menoufia University, Menouf, Egypt, in 1997, 2002, and 2007, respectively. From 1997 to 2002, he was a Demonstrator with the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, where he was an Assistant Lecturer, from 2002 to 2007. Since 2007, he has been a Teaching Staff Member with the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, where he is currently a Professor. His current research interests include network security, cryptography, the Internet security, multimedia security, image encryption, watermarking, steganography, data hiding, medical image processing, and chaos theory.

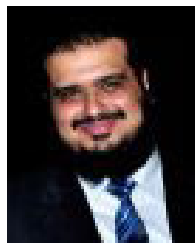


ASHRAF AFIFI received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees in electronic and communication engineering from Zagazig University, Egypt, in 1987, 1995, and 2002, respectively. He is currently a Professor with the Department of Computer Engineering, Faculty of Computers and Information Technology, Taif University, Saudi Arabia. His research interests include communication security, image processing, and image encryption.



HALA S. EL-SAYED received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees in electrical engineering from Menoufia University, Shebin El-Kom, Egypt, in 2000, 2004, and 2010, respectively. From 2002 to 2004, she was a Demonstrator with the Department of Electrical Engineering, Faculty of Engineering, Menoufia University, where she was an Assistant Lecturer, from 2004 to 2010. Since 2010, she has been a Teaching Staff Member with the Department of Electrical Engineering, Faculty

of Engineering, Menoufia University, where she is currently an Assistant Professor. Her research interests include database security, cybersecurity, network security, data hiding, image encryption, wireless sensor networks, secure building automation systems, medical image processing, and biometrics.



MOHAMMED A. ALZAIN received the bachelor's degree in computer science from King Abdulaziz University, Saudi Arabia, in 2004, the master's degree in information technology from La Trobe University, Melbourne, VIC, Australia, in 2010, and the Ph.D. degree from the Department of Computer Science and Computer Engineering, La Trobe University, in September 2014. He is currently an Associate Professor with the College of Computers and Information Technology, Taif

University, Saudi Arabia. His research interests include cloud computing security, multimedia security, image encryption, steganography, and medical image processing.



JEHAD F. AL-AMRI graduated from the Centre for Computing and Social Responsibility, De Montfort University. He is currently an Associate Professor with the Department of Information Technology, Faculty of Computers and Information Technology, Taif University, Saudi Arabia. His research interests include cloud computing security, multimedia security, image encryption, steganography, and medical image processing.



FATHI E. ABD EL-SAMIE (Member, IEEE) received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees from Menoufia University, Menouf, Egypt, in 1998, 2001, and 2005, respectively. Since 2005, he has been a Teaching Staff Member with the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University. His current research interests include image enhancement, image restoration, image interpolation, super-resolution reconstruction of images, data hiding, multimedia communications, medical image processing, optical signal processing, and digital communications. He was a recipient of the Most Cited Paper Award from the Digital Signal Processing Journal, in 2008.



WALID EL-SHAFI was born in Alexandria, Egypt. He received the B.Sc. degree in electronics and electrical communication engineering from the Faculty of Electronic Engineering (FEE), Menoufia University, Menouf, Egypt, in 2008, the M.Sc. degree from the Egypt-Japan University of Science and Technology (E-JUST), in 2012, and the Ph.D. degree from the Faculty of Electronic Engineering, Menoufia University, in 2019. He is currently working as a Lecturer and an Assistant Professor with the ECE Department FEE, Menoufia University. His research interests include wireless mobile and multimedia communications systems, image and video signal processing, efficient 2D video/3D multi-view video coding, multi-view video plus depth coding, 3D multi-view video coding and transmission, quality of service and experience, digital communication techniques, cognitive radio networks, adaptive filters design, 3D video watermarking, steganography, and encryption, error resilience and concealment algorithms for H.264/AVC, H.264/MVC and H.265/HEVC video codecs standards, cognitive cryptography, medical image processing, speech processing, security algorithms, software defined networks, Internet of Things, medical diagnoses applications, FPGA implementations for signal processing algorithms and communication systems, cancellable biometrics and pattern recognition, image and video magnification, artificial intelligence for signal processing algorithms and communication systems, modulation identification and classification, image and video super-resolution and denoising, deep learning in signal processing, and communication systems applications.

• • •