Multimed Tools Appl (2018) 77:30911–30937
https://doi.org/10.1007/s11042-018-6036-z

Efficient multi-level security for robust 3D color-plus-depth HEVC

Walid El-Shafai[1] · **El-Sayed M. El-Rabaie**[1] · **M. El-Halawany**[1] · **Fathi E. Abd El-Samie**[1]

Received: 14 August 2017 / Revised: 26 February 2018 / Accepted: 20 April 2018 /
Published online: 2 June 2018
© Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract This paper presents two robust hybrid watermarking techniques for securing the Three-Dimensional High Efficiency Video Coding (3D-HEVC). The first watermarking technique is the homomorphic-transform-based Singular Value Decomposition (SVD) in Discrete Wavelet Transform (DWT) domain. The second watermarking technique is the three-level Discrete Stationary Wavelet Transform (DSWT) in Discrete Cosine Transform (DCT) domain. The objective of the two proposed hybrid watermarking techniques is to increase the immunity of the watermarked 3D-HEVC streams to attacks. Also, we propose a wavelet-based fusion technique to combine two depth watermark frames into one fused depth watermark frame. Then, the resultant fused depth watermark is encrypted using chaotic Baker map to increase the level of security. After that, the resultant chaotic encrypted fused depth watermark is embedded in the 3D-HEVC color frames using the proposed hybrid watermarking techniques to produce the watermarked 3D-HEVC streams. In addition to achieving multi-level security in the transmitted 3D-HEVC streams, the proposed hybrid techniques reduce the required bit rate for transmitting the color-plus-depth 3D-HEVC data over limited-bandwidth networks. The performance of the proposed hybrid techniques is compared with those of the state-of-the-art techniques. Extensive simulation results on standard 3D video sequences have been conducted in the presence of attacks. The obtained results confirm that the proposed hybrid fusion-encryption-watermarking techniques achieve not only

✉ Walid El-Shafai
eng.waled.elshafai@gmail.com

El-Sayed M. El-Rabaie
elsayedelrabaie@gmail.com

M. El-Halawany
mmohamedelhalawany@gmail.com

Fathi E. Abd El-Samie
fathi_sayed@yahoo.com

[1] Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

a good perceptual quality with high Peak Signal-to-Noise Ratio (PSNR) values and less bit rate, but also high correlation coefficient values between the original and extracted watermarks in the presence of attacks. Furthermore, the proposed hybrid techniques improve the capacity of information embedding and the robustness without affecting the perceptual quality of the original 3D-HEVC frames. Indeed, the extraction of the encrypted, fused, primary, and secondary depth watermark frames is possible in the presence of attacks.

Keywords 3D-HEVC watermarking · Wavelet fusion · Homomorphic transform · SVD · DSWT · DCT · Chaotic encryption

1 Introduction

The Three-Dimensional Video-plus-Depth (3DV + D) comprises diverse video streams captured by different cameras around an object. Therefore, it is an imperative assignment to perform efficient compression to transmit and store the 3DV + D content to meet the future requirements, whilst preserving a decisive reception quality. Also, the security of the transmitted 3DV + D is a critical issue for protecting its copyright content. Due to the fast progress in multimedia data communication network developments and applications [5, 6, 12, 42–45], users can easily and arbitrarily distribute or access digital multimedia data from networks. The ownership security has become an important issue for individuals, and it requires more interest. Thus, there is a significant threat to copyright owners and digital multimedia producers to conserve their multimedia from intruder prospection to avert loss in transmitted data [2, 15, 37]. Steganography can be employed to secure the multimedia data. It is a methodology of hiding information by embedding data into given media (called cover media) without making any visible changes in these media [1, 3, 4, 13, 14, 20, 30]. Also, watermarking is one of the most preferred methods to secure digital multimedia files in the domains of copyright protection and data authentication, where a watermark secret code is inserted into the transmitted digital multimedia, and it contains information about the creator of the media, the copyright owner, or the authorized user.

The utilization of digital watermarks for efficient video transmission can be beneficial to ensure copyright protection. A digital watermark can be embedded either in a compressed video or an uncompressed video [16]. Video information are always transported and stored in the form of compressed data. The uncompressed video watermarking techniques can also be utilized for the compressed video bit streams, however, they require complete video re-encoding and decoding for the watermark insertion or extraction. In different cases, the complete video stream decoding process is not recommended. So, the compressed video watermarking has recently acquired more attentiveness. Furthermore, the watermark insertion and extraction in compressed data has less computations, because the complete re-encoding and decoding of the transmitted stream is not required for embedding and extracting the watermark bits.

Recently, several video encoding standards have emerged. The objective of thes encoding standards is to achieve high data compression, while maintaining an acceptable quality. The 3D-HEVC is the most recently used encoding standard in different applications [8, 40, 41]. It has received a broad attentiveness, and it is expected to rapidly take the place of the traditional 2D video coding in numerous applications. The predictive 3D H.265/HEVC framework is used to compress the transmitted 3DV sequences. In the 3D-HEVC system, the original 3D Video (3DV) consisting of multiple video streams is captured for the same

object by various cameras. Thus, to transport the 3DV over limited-resources networks, a highly efficient compression standard is needed, whilst preserving a high reception quality. The 3D-HEVC exploits the advantage of the time and space matching between frames in the same stream in addition to the inter-view matching within the different 3DV streams to enhance the encoding process.

The 3DV + D is a common format of 3D video representation that has recently been discussed intensively [31]. In this format, data about scene-per-pixel geometry is available. Depth data is very essential in 3D applications. It is beneficial for adaptable depth conception to harmonize various 3D displays. Moreover, it optimizes the 3DV stored bits compared to the traditional 2D videos. Because all object pixels have identical depth values, the depth information can be utilized to recognize the object boundaries. Due to the importance of the depth data corresponding to the texture color data of the transmitted 3DV, it must be utilized to represent the transmission of 3DV + D content over wireless networks. Unfortunately, the utilization of depth data increases the transmission bit rate due to the need of an additional transmission bandwidth to transmit the color data of the 3DV + D content.

Therefore, one of the main contributions of this paper is to present robust and reliable hybrid compressed video watermarking techniques for efficient transmission of 3D-HEVC compressed bit streams. These techniques have the following characteristics:

1. **Quality**. The quality of the watermarked 3D-HEVC frames resulting from the embedding process is maintained as high as possible by efficiently choosing the most suitable domain for watermark embedding.
2. **Robustness and Security**. The proposed watermark embedding and extraction procedures are robust. The embedded watermarks can survive different types of attacks.
3. **Transmission Bit Rate**. The proposed watermarking techniques reduce the transmission bit rate through hiding and embedding multiple depth frames into the corresponding color frames of the transmitted 3D-HEVC data.
4. **Complexity**. The computational cost due to watermark embedding is kept minimum.

The rest of this paper is organized as follows. Section 2 introduces the existing hybrid watermarking related works. Section 3 gives an explanation of the proposed hybrid fusion-encryption-watermarking techniques. Simulation results and the comparative study are presented in Section 4. The conclusions are presented in Section 5.

2 Related works

With the emerging evolution of 3D-HEVC applications, the security and copyright protection have become important aspects for the 3DV content storage and transmission. Multimedia watermarking techniques are employed for protecting the 3DV + D data copyright. These techniques are classified into two main categories; spatial- and transform-domain techniques. The spatial-domain techniques hide the watermark in the given video frames by directly adjusting their pixel values. They are simple to carry out and need less computations. Unfortunately, they are not robust enough to attacks. The transform-domain watermarking techniques adjust the video frames coefficients in a certain transform domain based on the adopted watermark embedding method. Thus, the transform-domain watermarking techniques achieve more robustness than those of the spatial-domain watermarking techniques.

There are few research works on 3DV data watermarking, and most of them deal with Depth-Based Image Rendering (DBIR) [8]. Thus, 3DV watermarking is still in its rudimentary phase. A watermarking method in the wavelet domain for stereo images was introduced in [7]. It depends on extracting the depth map from the stereo-pairs for watermark embedding. In [25], a visual model for watermarking of High Definition (HD) stereo images in DCT domain was presented. It is based on the visual sensitivity of the human eye to identify the perceptual modifications in the watermark embedding process. A blind diverse watermarking method was suggested in [23] based on DBIR method performed on the center image and the depth image generated by the content provider. Kim et al. [21] introduced a watermarking method for 3D images through the quantization of the Dual-Tree Complex Wavelet Transform (DT-CWT) coefficients. To improve the watermark robustness. Two features of the DT-CWT have been utilized; the approximate shift invariance and the directional selectivity. In [19], some efficient and robust hybrid watermarking schemes for different color image systems have been presented.

An efficient watermarking method for 3D images based on DBIR scheme was presented in [38] by utilizing the Scale-Invariant Feature Transform (SIFT) to choose some suitable regions for watermarking and the spread spectrum technique to insert the watermark data in the DCT coefficients of the selected regions. A 3DV blind watermarking technique based on a virtual view invariant domain was introduced in [11]. The average luminance values of the 3DV frames are chosen for watermark embedding. Swati et al. [36] suggested a fragile watermarking method, in which the watermark is inserted in the Least Significant Bit (LSB) of the non-zero quantized coefficients in the HEVC compressed video. Ogawa et al. [29] proposed an efficient watermarking scheme for HEVC bit streams that inserts the watermark information in the video compression phase. Also, there are several traditional works for watermarking of the 2D H.264/AVC compressed bit streams. Zhang et al. [46] suggested a video watermarking technique, where the security information is represented in a pre-processed binary data sequence and embedded into the middle frequency coefficients in the I frame. To enhance the watermark verification, the signs of the coefficients are altered depending on the watermark. The work introduced in [46] has been enhanced in [47] by concentrating on gray-scale characteristics and patterns. Qiu et al. [32] suggested a robust intra-frame watermark embedding scheme in quantized DCT coefficients and a fragile inter-frame watermark embedding method in motion vectors.

Kuo and Lo [22] enhanced the video watermark embedding scheme that was suggested in [32] by selecting more appropriate regions for both robust and fragile watermark embedding within the H.264 compressed video through the video encoding process. In [26], the process of watermark embedding is executed through the direct change of some data bits within the bit stream, however the pre-embedding process has complex computations. In [27], the same authors of [26] suggested a non-blind and robust watermarking method by utilizing the Watson Visual Model for watermark embedding in the I frame. Their proposed non-blind method [27] was extended for the P frame in [28], where the watermark bits are embedded in all non-zero coefficients of the P frame. An information hiding model was implemented in [10] to choose the watermark embedding area based on the forbidden-zone-data-hiding concepts. The sign parity of the coefficients and the values of the middle-frequency coefficients are altered for watermark embedding in the I frame [39]. In [9], the watermark is embedded in the non-zero coefficients of the P frame in the compressed domain to achieve better perceptual quality of the watermarked video frames and a minimal increase in video bit rate. In [34], a structure preserving non-blind H.264 watermarking technique was suggested to insert the watermark

through substituting secret bits in the motion vector differences of the non-reference images. Su et al. [35] suggested another non-blind watermark embedding algorithm for the I frames and P frames. The watermark embedding is implemented based on the spread spectrum technique and the Watson Visual Model [27].

It is noticed that several authors introduced a lot of work on 3D image watermarking in the spatial domain. Most recent 3D image and video watermarking techniques have been implemented in transform domains. Generally, there are few contributions in the literature on 3D compressed video watermarking techniques. Some of these introduced techniques have critical problems with watermark verification and extraction. The traditional video watermarking techniques have not achieved adequate watermarked and extracted watermark subjective and objective qualities in the presence of multimedia attacks. Thus, they have low robustness and imperceptibility. Moreover, most of the traditional video watermarking techniques work on uncompressed images. So, they require more computations in the watermark insertion and extraction processes, where a complete encoding and decoding of the transmitted stream are needed for embedding and extracting the watermark data. Thus, they increase the computational overhead. Furthermore, the traditional video watermarking techniques failed in selecting the most suitable regions inside the host frames for watermark embedding. Thus, they have an effect on the imperceptibility and quality of the watermarked frames, and they also increase the computations.

Taking into account the limitations of the state-of-the-art video watermarking techniques, the main contribution of this paper is to present an efficient hybrid framework for secure 3DV communication. This framework consists of transform-domain watermarking, wavelet-based fusion, and chaotic encryption techniques to efficiently protect the copyright of the 3DV + D HEVC streams to preserve both robustness and imperceptibility. Moreover, the proposed hybrid framework saves the 3D-HEVC transmission bit rates. Therefore, they have good imperceptibility, high quality, high robustness, acceptable bit rate, low computational complexity, and adequate immunity to different types of multimedia attacks compared to the traditional watermarking techniques.

3 The proposed hybrid fusion-encryption-watermarking techniques

In this section, the proposed hybrid fusion-encryption-watermarking techniques are introduced. We present the homomorphic transform based SVD watermarking in the DWT domain and the three-level DSWT watermarking in the DCT domain. They are suggested for 3DV data hiding taking into account increasing the embedding capacity without affecting the quality of the watermarked 3DV streams. In the proposed hybrid techniques, two depth watermark frames are firstly fused using the proposed wavelet based fusion technique. Then, the resultant fused depth watermark is encrypted utilizing the chaotic Baker map encryption technique. After that, the resultant encrypted fused depth watermark is embedded into the original 3DV color frames using the proposed hybrid watermarking techniques to produce the watermarked 3D-HEVC streams. So, the proposed hybrid fusion-encryption-watermarking framework consists of three different phases as shown in Fig. 1. In the first phase, the primary depth watermark frame is fused with the secondary depth watermark frame using the proposed wavelet-based fusion technique to produce the fused depth watermark frame. In the second phase, the fused depth watermark frame is encrypted using the chaotic Baker map encryption technique. In the third phase, the encrypted fused depth watermark frame is embedded into the original 3D-HEVC color frames using the proposed hybrid watermarking techniques. The

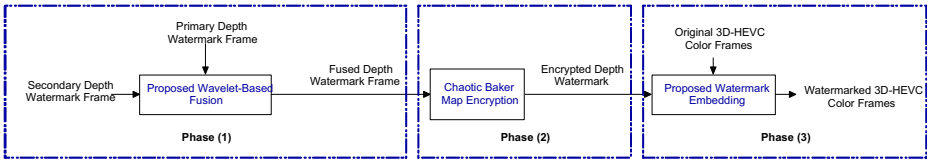


Fig. 1 The proposed hybrid fusion-encryption-watermarking framework

watermark extraction process is performed in three reverse steps; the extraction of the fused depth watermark frame, the decryption process, and the anti-fusion process to extract the primary and secondary depth watermark frames.

In the first phase, we exploit the proposed wavelet-based fusion technique, which is effective for combining perceptually important image features. It is used for many applications such as medical applications and remote sensing applications. The basic idea of the proposed wavelet-based fusion technique is that the two depth watermark frames are firstly transformed using the DWT transform. Then, the fusion process is executed and after that the Inverse DWT (IDWT) is employed to construct the fused depth watermark frame. The proposed wavelet-based fusion process is shown in Fig. 2.

In the second phase, the resultant fused depth watermark frame is encrypted with the proposed 2D chaotic Baker map encryption technique to increase the level of security of the transmitted 3D-HEVC data. Then, the encrypted fused depth watermark frame is embedded to the 3D-HEVC color frames as will be discussed in more details in Sections 3.1 and 3.2. The discretized chaotic Baker map randomizes a square matrix by assigning each pixel to another location in a bijective manner. The discretized chaotic Baker map will be denoted by $B_{(n_1,\ldots,n_l)}$, where the sequence of l integers, $n_1, n_2, \ldots, n_l$, is selected such that each integer n_i divides N, and $N_i = n_1 + \ldots + n_i$. The pixel at (r, s) with $N_i \le r < N_i + n_i$ and $0 \le s < N$ is mapped to:

$$B_{(n_1,\ldots n_k)}(r,s) = \left[\frac{N}{n_i}(r - N_i) + s \bmod \left(\frac{N}{n_i}\right), \frac{n_i}{N}\left(s - s \bmod \left(\frac{N}{n_i}\right)\right) + N_i\right] \quad (1)$$

The steps of chaotic Baker map randomization can be summarized as follows:

1. An $N \times N$ square matrix is divided into l vertical rectangles of height N and width n_i with $n_1 + n_2 + \ldots + n_l = \mathrm{N}$.
2. Each vertical rectangle is divided into n_i blocks, and each block contains N points.
3. Each of these blocks is mapped to a row of pixels.

An example of the chaotic Baker map randomization of an 8×8 matrix is shown in Fig. 3. The secret key is (2, 4, 2). Hence, $N = 8$, $n_1 = 2$, $n_2 = 4$, and $n_3 = 2$. The N is defined as the total

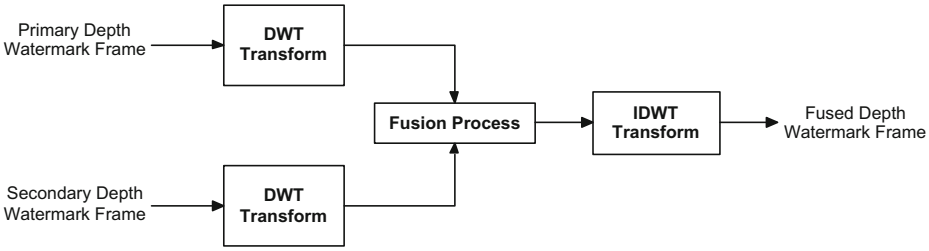


Fig. 2 The proposed wavelet-based fusion process of the two primary and secondary depth watermark frames

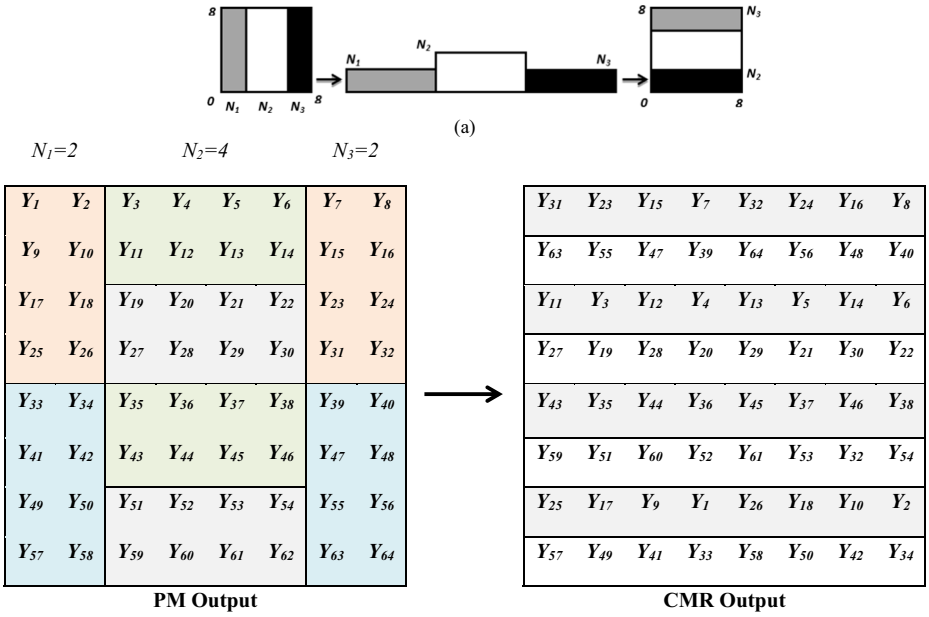


Fig. 3 Chaotic Baker map randomization example using a secret key of (2, 4, 2): (**a**) Discretized Baker map, (**b**) The 8 × 8 randomized output

number of rows of the square matrix, while N_i is the total number of columns in each vertical division. In the introduced example of chaotic Baker map randomization presented in Fig. 3, we assumed that $N = 8$, and $N_i = (2,4,2)$.

3.1 Homomorphic-transform-based SVD watermarking in the DWT domain

In this section, the proposed homomorphic-transform-based SVD watermarking in the DWT domain is introduced. The proposed framework for encrypted fused depth watermark embedding is shown in Fig. 4, and that for encrypted fused depth watermark extraction is shown in Fig. 5. In this technique, the encrypted fused depth watermark frames are inserted in the chosen wavelet transform coefficients of the 3DV luminance (Y) components of the color frames. The first step of this technique is the transformation of the RGB color space to the YUV color space. The 2D DWT is used to split each Y frame into four sub-bands, which are the approximation sub-band (low frequency LL), the horizontal detail sub-band (high frequency LH), the vertical detail sub-band (high frequency HL), and the diagonal detail sub-band (high frequency HH). So, the wavelet transform is performed on the luminance (Y) component of every color frame within the 3DV stream. The reflectance components of the LL sub-bands are extracted through the homomorphic transform. The encrypted fused depth watermark frame is embedded by employing the SVD algorithm on the extracted reflectance components of the LL sub-bands.

The main contribution of the proposed homomorphic-transform-based SVD watermarking in the DWT domain is the utilization of the homomorphic transform jointly with the DWT and SVD transforms. So, the homomorphic transform improves the performance of the

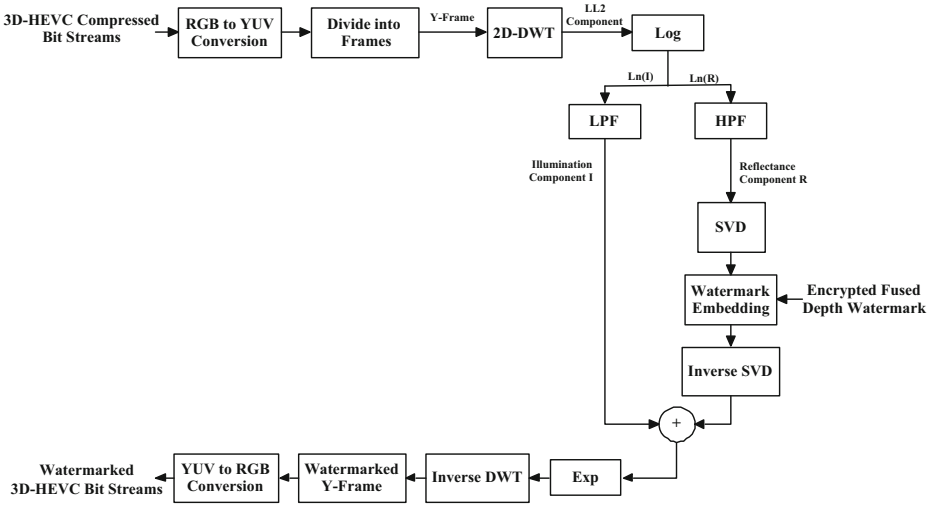


Fig. 4 Watermark embedding in the proposed technique of homomorphic-transform-based SVD watermarking in the DWT domain

watermarking process through choosing the most suitable regions inside the host color frames for watermark embedding to maintain the imperceptibility and robustness of the watermarked frames. The homomorphic transform is performed based on the fact that the frame intensity is represented by the multiplication of light illumination and reflectance of objects inside images. Because the illumination is approximately constant and the reflectance is variable from an image to another, the image reflectance represents the most important component of the transmitted images. Thus, the image reflectance can be extracted through the homomorphic transform, and then it is used for watermark embedding. Therefore, the homomorphic transform is utilized to efficiently choose the most suitable frequency regions inside the host color

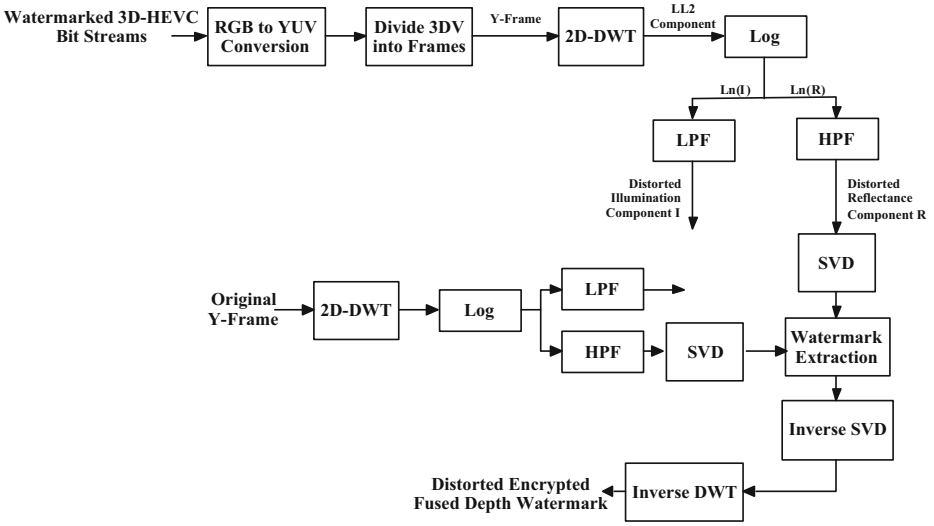


Fig. 5 Watermark extraction in the proposed technique of homomorphic transform based SVD watermarking in the DWT domain

frames for watermark embedding.

$$F_{LL}(n_1, n_2) = I(n_1, n_2) \times R(n_1, n_2) \tag{2}$$

$$\ln[F_{LL}(n_1, n_2)] = \ln[I(n_1, n_2)] + \ln[R(n_1, n_2)] \tag{3}$$

$$\mathbf{R} = \mathbf{U}\mathbf{S}\mathbf{V}^{\mathrm{T}} \tag{4}$$

$$\mathbf{D} = \mathbf{S} + k\mathbf{W} \tag{5}$$

$$\mathbf{D} = \mathbf{U}_{\mathbf{w}}\mathbf{S}_{\mathbf{w}}\mathbf{V}_{\mathbf{w}}^{\mathrm{T}} \tag{6}$$

$$\mathbf{R}_{\mathbf{w}} = \mathbf{U}\mathbf{S}_{\mathbf{w}}\mathbf{V}^{\mathrm{T}} \tag{7}$$

$$\mathbf{X}_{\mathbf{w}} = \mathbf{R}_{\mathbf{w}} + \mathbf{I} \tag{8}$$

$$\mathbf{F}_{\mathbf{LL}_{\mathbf{w}}} = \exp\left(\mathbf{X}_{\mathbf{w}}\right) \tag{9}$$

The low-frequency LL sub-band intensity can be formulated by (2), where $I(n_1, n_2)$ is the illumination and $R(n_1, n_2)$ is the reflectance of the selected color frame, whose values at the spatial coordinates (n_1, n_2) are positive scalar quantities. The homomorphic transform is executed as given in (3). A High Pass Filter (HPF) and a Low Pass Filter (LPF) are applied to the ln $[F_{LL}(n_1, n_2)]$ to separate the illumination from the reflectance. We can represent ln $[R(n_1, n_2)]$ and ln $[I(n_1, n_2)]$ in matrix form as **R** and **I** matrices. After that, the SVD is applied on the reflectance **R** matrix as in (4), where **U** and **V** are orthogonal matrices and **S** is a diagonal matrix. The Singular Values (SVs) of the matrix **R** are the entries of the **S** matrix. Then, the encrypted fused depth watermark (**W** matrix) is combined with the SVs of the reflectance **R** matrix as in (5). After that, the SVD is employed on the modified matrix (**D** matrix) as given by (6), and then the frame ($\mathbf{R}_{\mathbf{w}}$ matrix) is obtained by utilizing the modified matrix ($\mathbf{S}_{\mathbf{w}}$ matrix) as in (7). The inverse homomorphic transform is applied on the **I** and $\mathbf{R}_{\mathbf{w}}$ to get a matrix $\mathbf{X}_{\mathbf{w}}$ as in (8), and then the low-frequency sub-band of the watermarked frame ($\mathbf{F}_{\mathbf{LL_w}}$) can be obtained by (9). The inverse DWT is implemented to get the 3DV watermarked frame $\mathbf{F}_{\mathbf{w}}$.

For the extraction of the possibly distorted encrypted fused depth watermark from the possibly corrupted watermarked 3D-HEVC frames, given the $\mathbf{U}_{\mathbf{w}}$, $\mathbf{S}_{\mathbf{w}}$, $\mathbf{V}_{\mathbf{w}}$ matrices and the possibly distorted frame $\mathbf{F}_{\mathbf{w}}$, the above-mentioned steps are reversely executed. The homomorphic transform is applied on the LL sub-band of the watermarked frame $\mathbf{F}_{\mathbf{LLw}}$. A HPF is utilized to obtain the possibly distorted reflectance component $\mathbf{R}^{*}_{\mathbf{w}}$, and then the SVD is employed on the $\mathbf{R}^{*}_{\mathbf{w}}$ matrix as given by (10). The matrix that includes the watermark is computed by (11), and so the possibly corrupted encrypted

fused depth watermark is obtained by (12).

$$\mathbf{R}_{\mathbf{w}}^{*} = \mathbf{U}^{*}\mathbf{S}_{\mathbf{w}}^{*}\mathbf{V}^{*^{\mathrm{T}}} \tag{10}$$

$$\mathbf{D}^{*} = \mathbf{U}_{\mathbf{w}}\mathbf{S}_{\mathbf{w}}^{*}\mathbf{V}_{\mathbf{w}}^{\mathrm{T}} \tag{11}$$

$$\mathbf{W}^{*} = \left(\mathbf{D}^{*} - \mathbf{S}\right)/k \tag{12}$$

3.2 Three-level DSWT watermarking in the DCT domain

In this technique, the transformation from the RGB color space to the YUV color space is the first step, and then the DCT is applied on each Y-frame. The three-level DSWT is utilized to divide the DCT domain into four sub-bands, which are the approximation sub-band (A), the horizontal sub-band (H), the vertical sub-band (V), and the diagonal sub-band (D). These A, H, V, and D sub-band matrices have identical sizes. The encrypted fused depth watermark frame is embedded on the matrix A.

The encrypted fused depth watermark frame embedding steps are shown in Fig. 6 and summarized below:

Step 1: The original compressed 3DV stream is transformed from the RGB to the YUV color space, and then the luminance Y values of the 3DV frames are further utilized.
Step 2: The converted 3DV stream is partitioned into groups of k frames.
Step 3: The DCT components of each Y-frame are obtained using the 2D-DCT transform.
Step 4: The determined DCT components of each Y-frame are decomposed into four sub-ands (A, H, V, and D) using the 3-level DSWT.
Step 5: The encrypted fused depth watermark frame is embedded into the matrix A of each Y-frame by multiplying the watermark by a key K and adding it to the matrix A, where $0 < K < 1$.
Step 6: The inverse DSWT is implemented, and then the inverse DCT to obtain the watermarked Y-frame, and thus the watermarked 3DV stream.

The encrypted fused depth watermark frame extraction steps are shown in Fig. 7, and summarized below:

Step 1: The watermarked 3DV is transformed from the RGB to the YUV color space, and just the luminance Y values of the frames are further processed.

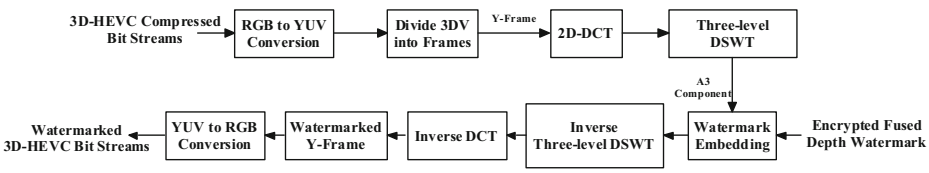


Fig. 6 Watermark embedding in the proposed technique of three-level DSWT watermarking in the DCT domain

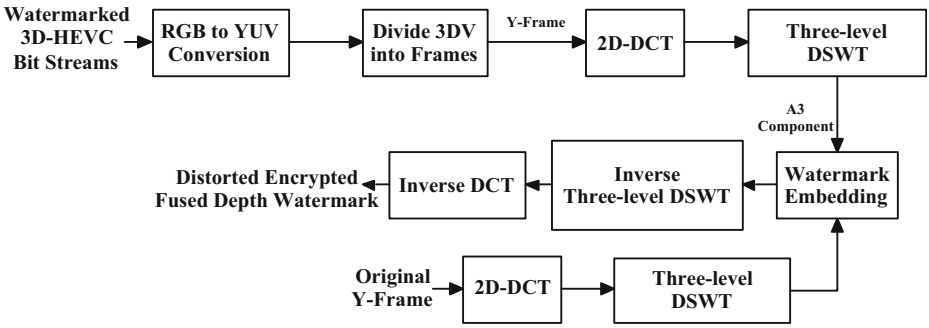


Fig. 7 Watermark extraction in the proposed technique of three-level DSWT watermarking in the DCT domain

Step 2: The converted watermarked 3DV stream is partitioned into groups of k frames.
Step 3: The DCT components are extracted from each watermarked Y-frame using the 2D-DCT transform.
Step 4: The determined DCT components of each Y-frame are decomposed into four frequency sub-bands (A_w, H, V, D) utilizing the 3-level DSWT.
Step 5: The possibly-distorted encrypted fused depth watermark frame is extracted from the matrix A_w of each watermarked Y-frame by subtracting the matrix A of the original frame from the matrix A_w of the watermarked frame and dividing the result by K.

4 Simulation results and discussions

To assess the performance of the proposed hybrid fusion-encryption-watermarking techniques, several simulation tests on the standard well-known 3DV + D (Shark and PoznanStreet) 1920 × 1088 sequences [24] have been carried out. For each sequence, the coded 3D H.265/HEVC bit streams are produced by employing the reference HM codec [17]. All simulation tests have been performed using an Intel® Core™i7-4500 U CPU @1.80GHz and 2.40GHz with 8GB RAM, working with Windows 10 64-bit operating system, and using MATLAB 2017a. The visual results ensure watermark invisibility and no degradation in the watermarked frames quality compared to the original frames. The PSNRs of the watermarked frames and the Normalized Correlation (NC) values of the extracted possibly-corrupted encrypted fused, decrypted fused, primary, and secondary depth watermarks are estimated. The PSNR is calculated by (13) and (14) [8], where MSE is the Mean Square Error between the original host and watermarked color frames, A is the original color frame, A_w is the watermarked color frame, and $M \times N$ is the size of the host and the watermarked color frames. The NC is estimated by (15), where **W** is the original depth watermark and **W*** is the extracted corrupted depth watermark. In our simulations, we apply different types of attacks on the watermarked frames, and then we extract the encrypted fused, decrypted fused, primary, and secondary depth watermarks to test the robustness of the proposed techniques. We have run two experiments for each proposed watermarking technique. The first one uses the 3DV + D Shark sequence by selecting color frame 50 as a test host Y-frame, depth frame 50 as a primary depth watermark frame, and depth frame 100 as a secondary depth watermark frame. The other experiment uses the 3DV + D PoznanStreet sequence by selecting color frame 100 as a test host Y-frame, depth frame 100 as a primary

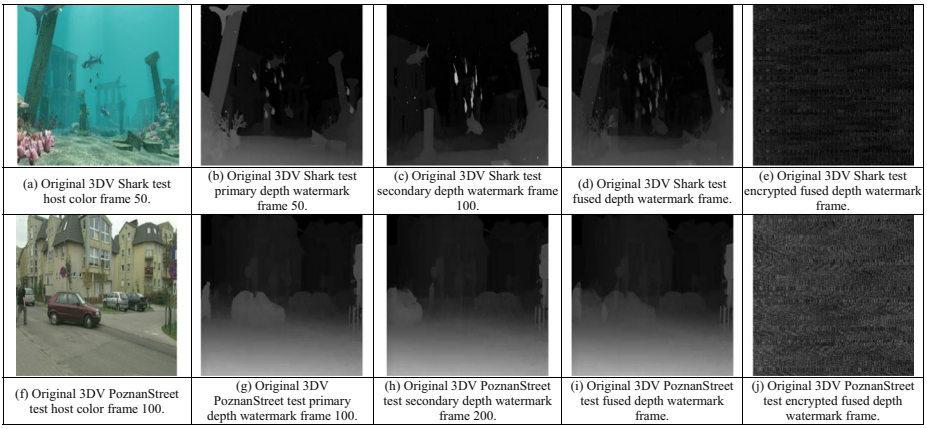


Fig. 8 The 3D-HEVC Shark and PoznanStreet host color frame and primary, secondary, fused, and encrypted fused depth watermark frames

depth watermark frame, and depth frame 200 as a secondary depth watermark frame as shown in Fig. 8, which also shows their fused and encrypted fused depth watermark frames.

$$PSNR(dB) = 10\log_{10}\left(255^2/MSE\right) \tag{13}$$

$$MSE = \frac{1}{M \times N}\sum_{x=0,y=0}^{M-1,N-1}\left(A_w(x,y) - A(x,y)\right)^2 \tag{14}$$

$$NC = \frac{\mathbf{W}^*.\mathbf{W}}{\|\mathbf{W}^*\|.\|\mathbf{W}\|} \tag{15}$$

To clarify the efficiency of the proposed hybrid fusion-encryption-watermarking techniques in protecting and securing the transmitted 3DV + D HEVC bit streams in the presence of attacks, we have compared their performance with those of the state-of-the-art hybrid watermarking techniques such as the DCT + DWT, DWT + SVD, and DCT + SVD [18, 19, 33]. The comparisons depend on both subjective visual results and objective results; the PSNRs of the watermarked frames and the NC of the extracted watermark frames. In the introduced simulation results, the DWT + Homomorphic + SVD refers to the first proposal of the homomorphic transform based SVD watermarking in the DWT domain, and the DCT + DSWT refers to the second proposal of the three-level DSWT watermarking in the DCT domain. Figures 9 and 10 show the visual results with the PSNR and NC values of the color watermarked and extracted encrypted fused, decrypted fused, primary, and secondary depth watermark frames for the Shark and PoznanStreet 3DV streams without attacks compared to those of the state-of-the-art techniques. It is clear from Figs. 9 and 10 that there is a high similarity between the original and watermarked frames in the proposed techniques compared to the state-of-the-art techniques. Moreover, the proposed DWT + Homomorphic + SVD technique introduces better watermarked and extracted

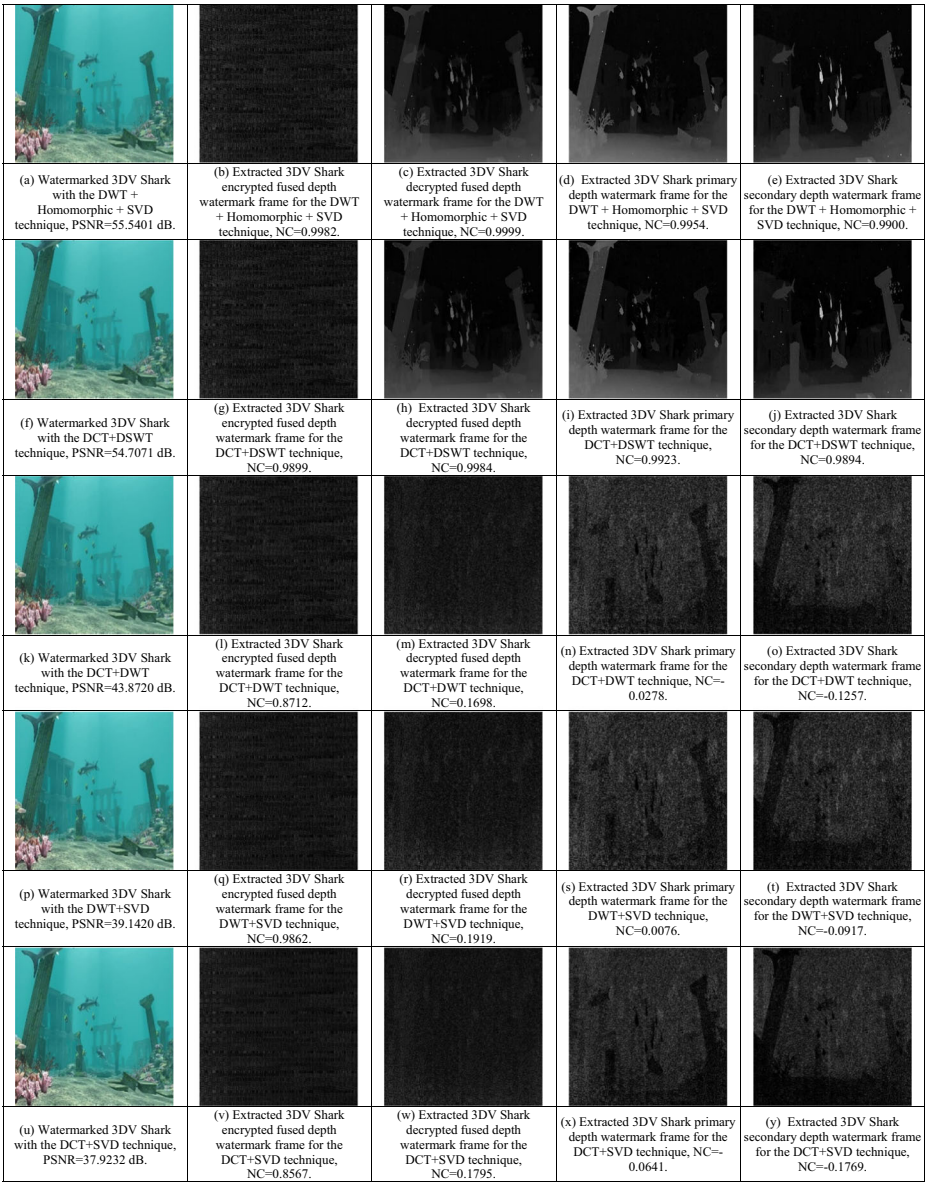


Fig. 9 3DV watermarked and extracted encrypted fused, decrypted fused, primary, and secondary depth watermark Shark frames without attacks

watermark frames than those of the proposed DCT + DSWT technique. The proposed techniques achieve high PSNR and NC values for all tested 3DV frames compared to those of the related works.

In Tables 1, 2, 3, 4, and 5, we compare the objective PSNR values of the watermarked color frames and the NC values of the extracted encrypted fused, decrypted fused, primary, and secondary depth watermark frames of the Shark and

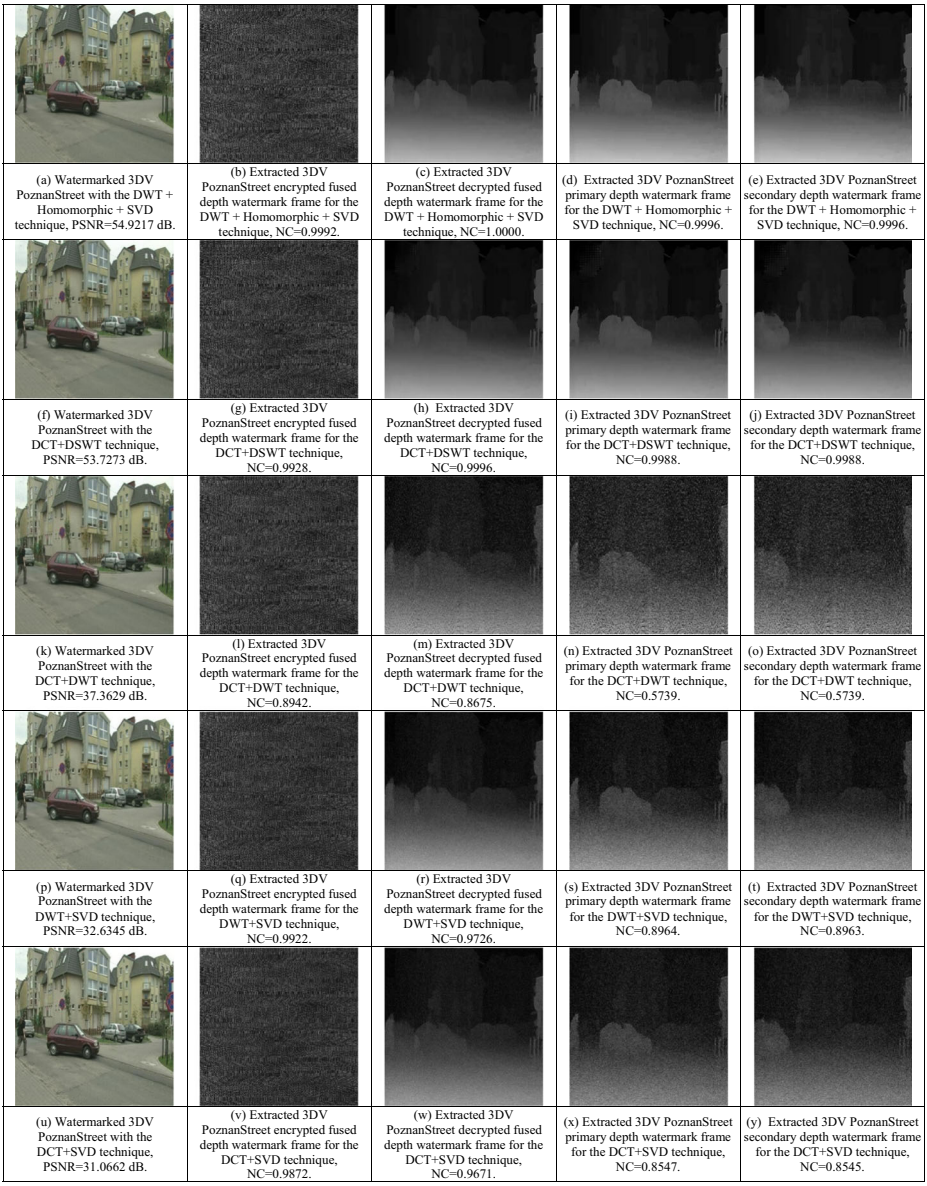


Fig. 10 3DV watermarked and extracted encrypted fused, decrypted fused, primary, and secondary depth watermark PoznanStreet frames without attacks

PoznanStreet 3D-HEVC sequences for the proposed watermarking techniques and the state-of-the-art watermarking techniques at different types of attacks. From all presented simulation results, we deduce that the suggested techniques always achieve superior PSNR and NC values. It can be realized that the proposed techniques have a meaningful average gain in objective PSNR and NC for all tested 3D-HEVC sequences for different types of attacks.

Table 1 Objective average PSNR values of the watermarked color frames and average NC, NC1, NC2, and NC3 values of the extracted encrypted fused, decrypted fused, primary, and secondary depth watermark frames for the Shark and PoznanStreet 3DV streams with different rotation attacks

Watermarking technique	PSNR (dB) / NC / NC1 / NC2 / NC3					
	Shark			PoznanStreet		
	Rotation 30°	Rotation 45°	Rotation 60°	Rotation 30°	Rotation 45°	Rotation 60°
DWT + Homomorphic + SVD	13.8681/0.9915/0.9796/ 0.9604/0.9059	13.2712/0.9847/0.9688/ 0.9425/0.8686	13.0665/0.9914/0.9794/ 0.9601/0.9052	10.8066/0.9900/0.9953/ 0.9859/0.9857	10.4848/0.9597/0.9850/ 0.9599/0.9598	10.5233/0.9894/0.9950/ 0.9851/0.9849
DCT + DSWT	13.8646/0.4763/0.4471/ 0.3593/0.2288	13.2667/0.4638/ 0.4313/ 0.3510/0.2247	13.0609/0.4721/ 0.4439/ 0.3622/0.2340	10.7999/0.6882/0.6846/ 0.4855/0.4798	10.4776/0.6807/0.6733/ 0.4782/0.4734	10.5150/0.6872/0.6825/ 0.4838/0.4786
DCT + DWT [18]	13.8566/0.1181/0.0283/ −0.0096/−0.0257	13.2657/0.1099/0.0266/ −0.0089/−0.0226	13.0730/0.1154/0.0293/ −0.0072/−0.0221	10.7760/0.2055/0.2017/ 0.1037/0.1029	10.4535/0.2076/0.2038/ 0.1060/0.1048	10.4936/0.2180/0.2141/ 0.1085/0.1071
DWT + SVD [33]	13.7909/0.2953/0.0747/ 0.0406/−0.0029	13.1897/0.2663/0.0669/ 0.0332/−0.0056	12.9737/0.3079/0.0759/ 0.0412/0.0008	10.7110/0.2005/0.2159/ 0.1323/0.1335	10.3879/0.2056/0.2192/ 0.1362/0.1373	10.4160/0.3416/0.3539/ 0.2373/0.2396
DCT + SVD [19]	13.7564/0.3950/0.0802/ 0.0420/0.0055	13.1588/0.3527/0.0713/ 0.0336/0.0023	12.9428/0.4097/0.0846/ 0.0474/0.0085	10.6384/0.3268/0.3361/ 0.2206/0.2226	10.3243/0.3289/0.3368/ 0.2327/0.2347	10.3497/0.4660/0.4736/ 0.3440/0.3466

Table 2 Objective average PSNR values of the watermarked color frames and average NC, NC1, NC2, and NC3 values of the extracted encrypted fused, decrypted fused, primary, and secondary depth watermark frames for the Shark and PoznanStreet 3DV streams with different Gaussian noise attacks

Watermarking technique	PSNR (dB) / NC / NC1 / NC2 / NC3					
	Shark			PoznanStreet		
	Gaussian noise 0.01	Gaussian noise 0.05	Gaussian noise 0.1	Gaussian noise 0.01	Gaussian noise 0.05	Gaussian noise 0.1
DWT + Homomorphic + SVD	22.7362/0.9984/0.9994/0.9947/0.9879	16.6569/0.9982/0.9974/0.9913/0.9792	14.4421/0.9971/0.9951/0.9875/0.9699	22.7608/0.9995/0.9997/0.9986/0.9986	16.2193/0.9980/0.9982/0.9937/0.9937	14.0804/0.9954/0.9975/0.9910/0.9910
DCT + DSWT	22.7204/0.9057/0.9043/0.8729/0.7797	16.6624/0.8172/0.8044/0.7948/0.6547	14.4407/0.7823/0.7667/0.7624/0.6079	22.7726/0.9734/0.9825/0.9484/0.9483	16.2111/0.9420/0.9503/0.8904/0.8902	14.1054/0.9246/0.9304/0.8593/0.8590
DCT + DWT [18]	22.6913/0.2538/0.0579/−0.0104/−0.0461	16.6209/0.1562/0.0333/−0.0114/−0.0369	14.4085/0.1367/0.0291/−0.0131/−0.0309	22.6262/0.4666/0.4565/0.2526/0.2519	16.1727/0.2973/0.2922/0.1640/0.1637	14.0673/0.2567/0.2521/0.1418/0.1415
DWT + SVD [33]	22.6207/0.7469/0.1460/0.0367/−0.0268	16.5731/0.4986/0.0999/0.0459/0.0139	14.3610/0.4351/0.0865/0.0392/0.0167	22.4011/0.9045/0.8828/0.7122/0.7134	16.1346/0.6314/0.6233/0.4459/0.4452	14.0454/0.5313/0.5252/0.3809/0.3799
DCT + SVD [19]	22.6116/0.7996/0.1470/0.0904/0.0493	16.5773/0.7925/0.1509/0.1122/0.0776	14.3547/0.7756/0.1487/0.1136/0.0810	22.2604/0.8720/0.8458/0.7369/0.7371	16.1488/0.8090/0.7838/0.7062/0.7041	14.0641/0.7798/0.7546/0.6890/0.6863

Table 3 Objective average PSNR values of the watermarked color frames and average NC, NC1, NC2, and NC3 values of the extracted encrypted fused, decrypted fused, primary, and secondary depth watermark frames for the Shark and PoznanStreet 3DV streams with different types of blurring attacks

Watermarking technique	PSNR (dB) / NC / NC1 / NC2 / NC3					
	Shark			PoznanStreet		
	Motion blur	Disk blur	Average blur	Motion blur	Disk blur	Average blur
DWT + Homomorphic + SVD	25.9881/0.9976/0.9996/0.9946/0.9892	24.5801/0.9975/0.9996/0.9945/0.9890	27.6878/0.9977/0.9996/0.9947/0.9893	24.7233/0.9985/0.9999/0.9994/0.9994	22.9862/0.9983/0.9999/0.9993/0.9992	27.0875/0.9987/0.9999/0.9995/0.9995
DCT + DSWT	25.9962/0.9600/0.9694/0.9455/0.9142	24.5871/0.9392/0.9505/0.9269/0.8689	27.6935/0.9722/0.9827/0.9658/0.9423	24.7438/0.9730/0.9835/0.9587/0.9586	22.9336/0.9660/0.9785/0.9464/0.9464	27.1064/0.9817/0.9913/0.9758/0.9757
DCT + DWT [18]	25.9455/0.4671/0.0996/−0.0143/−0.0750	24.5559/0.4396/0.0929/−0.0161/−0.0747	27.5317/0.5707/0.1162/−0.0200/−0.0915	24.5653/0.5132/0.5003/0.2684/0.2686	22.9060/0.4709/0.4590/0.2433/0.2435	26.8000/0.5952/0.5789/0.3084/0.3085
DWT + SVD [33]	25.8544/−0.0262/−0.0087/−0.1185/−0.1510	24.5463/−0.1696/−0.0383/−0.1166/−0.1326	27.4885/0.3488/0.0654/−0.1027/−0.1648	24.2762/0.2807/0.2562/−0.1346/−0.1340	22.7759/−0.0053/−0.0211/−0.2547/−0.2541	26.3348/0.6645/0.6280/0.1334/0.1341
DCT + SVD [19]	25.8548/−0.6595/−0.1187/−0.1913/−0.1910	24.5647/−0.6885/−0.1307/−0.1907/−0.1796	27.5511/−0.5724/−0.0938/−0.1851/−0.1971	24.2636/−0.7980/−0.7598/−0.7703/−0.7629	22.7957/−0.8084/−0.7797/−0.7978/−0.7891	26.3650/−0.6539/−0.6020/−0.7052/−0.6998

Table 4 Objective average PSNR values of the watermarked color frames and average NC, NC1, NC2, and NC3 values of the extracted encrypted fused, decrypted fused, primary, and secondary depth watermark frames for the Shark and PoznanStreet 3DV streams with different types of JPEG compression attacks

Watermarking technique	PSNR (dB) / NC / NC1 / NC2 / NC3					
	Shark			PoznanStreet		
	JPEG 20%	JPEG 40%	JPEG 60%	JPEG 20%	JPEG 40%	JPEG 60%
DWT + Homomorphic + SVD	29.1280/0.9981/0.9999/0.9953/0.9901	31.1161/0.9979/0.9998/0.9951/0.9898	35.3064/0.9983/0.9998/0.9953/0.9897	29.5490/0.9992/1.0000/0.9996/0.9996	31.9972/0.9991/1.0000/0.9996/0.9996	36.2439/0.9994/1.0000/0.9996/0.9996
DCT + DSWT	29.1315/0.9747/0.9803/0.9604/0.9333	31.1122/0.9791/0.9898/0.9762/0.9618	35.2997/0.9858/0.9948/0.98470.9790	29.5608/0.9873/0.9949/0.9826/0.9826	31.9945/0.9893/0.9974/0.9912/0.9912	36.2174/0.9907/0.9989/0.9962/0.9962
DCT + DWT [18]	29.0208/0.4976/0.1054/−0.0156/−0.0781	30.9073/0.5888/0.1175/−0.0214/−0.0933	34.7455/0.7201/0.1428/−0.0210/−0.1022	28.9264/0.6172/0.5996/0.3220/0.3221	30.9752/0.7010/0.6798/0.3726/0.3732	33.6697/0.8016/0.7772/0.4681/0.4680
DWT + SVD [33]	28.7789/0.9433/0.1902/0.0136/−0.0957	30.4643/0.9592/0.1871/.0002/−0.1024	33.8612/0.9927/0.1930/0.0171/−0.0782	27.9570/0.9853/0.9636/0.8664/0.8663	29.2554/0.9836/0.9621/0.8572/0.8573	31.0738/0.9941/0.9757/0.9121/0.9120
DCT + SVD [19]	28.6857/0.0963/0.0526/−0.1045/−0.1884	30.2434/0.1690/0.0633/−0.1456/−0.2268	33.4270/0.9566/0.1859/0.0404/−0.0404	27.2895/0.8986/0.8782/0.5635/0.5638	28.4862/0.9698/0.9493/0.7271/0.7267	30.1330/0.9938/0.9759/0.9173/0.9173

Table 5 Objective average PSNR values of the watermarked color frames and average NC, NC1, NC2, and NC3 values of the extracted encrypted fused, decrypted fused, primary, and secondary depth watermark frames for the Shark and PoznanStreet 3DV streams with resizing and crop attacks

Watermarking technique	PSNR (dB) / NC / NC1 / NC2 / NC3			
	Shark		PoznanStreet	
	Resize attack	Crop attack	Resize attack	Crop attack
DWT + Homomorphic + SVD	28.5293/0.9977/0.9997/0.9947/0.9894	15.0973/0.9975/0.9997/0.9946/0.9864	28.2876/0.9987/0.9999/0.9995/0.9995	16.2212/0.9986/0.9999/0.9995/0.9995
DCT + DSWT	28.5315/0.9798/0.9887/0.9764/0.9621	15.0974/0.9680/0.9825/0.9592/0.9506	28.2902/0.9865/0.9949/0.9855/0.9855	16.2210/0.9849/0.9964/0.9881/0.9881
DCT + DWT [18]	28.4216/0.5854/0.1190/−0.0190/−0.0927	15.0921/0.4319/0.0964/−0.0047/−0.0593	27.8613/0.6098/0.5927/0.3165/0.3166	16.1884/0.7092/0.6892/0.4061/0.4057
DWT + SVD [33]	28.2532/0.5641/0.1089/−0.0762/−0.1577	15.0840/−0.0487/−0.0641/−0.0493/−0.0179	27.1393/0.8143/0.7765/0.3513/0.3521	16.1309/0.8070/0.8034/0.2577/0.2613
DCT + SVD [19]	28.2800/−0.5171/−0.0811/−0.1752/−0.1934	15.0804/−0.0114/−0.0107/−0.0090/−0.0052	27.1192/−0.4956/−0.4472/−0.6511/−0.6468	16.0909/0.7524/0.7663/−0.2290/−0.2268

From Table 1 presenting the simulation results in the case of different rotation attacks, it is noticed that both the DWT + Homomorphic + SVD and the DCT + DSWT watermarking techniques give the highest PSNR values between the original and watermarked frames. Also, it is clear that the DWT + Homomorphic + SVD technique achieves the best results in the case of the rotation attack. From Table 2 presenting the simulation results in the case of different Gaussian noise attacks, it is noticed that the proposed hybrid watermarking techniques give not only the highest PSNR values between the original and watermarked frames, but also the best correlation values between the original and the primary, and secondary depth watermark frames. In addition, it is clear that the DWT + Homomorphic + SVD technique achieves the best results in the case of the Gaussian noise attack. From Table 3 including the simulation results in the case of different (Motion, Disk, and Average) blurring attacks, it is noticed that both the DWT + Homomorphic + SVD and the DCT + DSWT watermarking techniques give not only the highest PSNR values between the original and watermarked frames, but also the best correlation values between the original and the extracted primary, and secondary depth watermark frames. Moreover, it is clear that the DWT + Homomorphic + SVD technique achieves the best results with different types of blurring attacks.

From Table 4 including the simulation results with different JPEG compression attacks, it is noticed that the proposed hybrid watermarking techniques give not only the highest PSNR values between the original and watermarked frames, but also the best correlation values between the original and extracted watermarks. In addition, it is clear that the DWT + Homomorphic + SVD technique achieves the best results with the JPEG compression attack. From Table 5 including the simulation results with resizing and crop attacks, it is noticed that all the presented watermarking techniques in this paper present good results of high PSNR values between the original and watermarked frames, and also high correlation values between the original and extracted primary, and secondary depth watermark frames. It is also clear that the proposed hybrid watermarking techniques still achieve the best results. It is clear that the DWT + Homomorphic + SVD technique achieves the best results in the case of resizing and crop attacks. From all presented simulation results, we deduce that the suggested hybrid techniques always achieve superior PSNR and NC values. It can be realized that the proposed techniques have a meaningful average gain in objective PSNR and NC for all tested 3DV + D HEVC frames with different types of attacks.

Table 6 presents the average CPU time results of the proposed embedding techniques compared to the state-of-the-art embedding techniques for the Shark and PoznanStreet 3DV + D HEVC streams without attacks. It is noticed that the proposed hybrid techniques introduce acceptable embedding CPU processing times, and hence they can be recommended for online and real-time video transmission applications. The DCT + DWT technique has the shortest CPU processing time, and the DCT + SVD technique has the longest CPU processing times in the watermark embedding process.

It is known that the color and depth frames of the transmitted 3DV + D HEVC sequences need two separate channels for their transmission over networks. In order to further confirm the performance efficiency of the proposed hybrid fusion-watermarking techniques in minimizing the required bandwidth for transmitting the 3DV + D data over limited-resources wireless networks, we run more simulation tests.

Table 6 Average CPU embedding times of all techniques for the Shark and PoznanStreet 3D-HEVC streams

Watermarking technique	CPU time of embedding technique (Seconds)	
	Shark	PoznanStreet
DWT + Homomorphic + SVD	1.8659	1.9582
DCT + DSWT	1.5489	1.5697
DCT + DWT [18]	0.9625	0.9882
DWT + SVD [33]	1.4827	1.5639
DCT + SVD [19]	2.3294	2.3517

The results prove that the proposed hybrid fusion-watermarking techniques can jointly transmit the color and depth frames on the same channel through embedding multiple fused depth frames within the color frames of the 3DV + D. Table 7 shows the size in bytes of the original host color frame, original primary, secondary, and fused watermark depth frames, and watermarked color frames for the Shark and PoznanStreet 3DV streams. From this table, it is noticed that the size of the fused watermark depth frame is smaller than the summation of the sizes of the primary and secondary watermark depth frames. Also, it is noticed that the size of the watermarked color frame is smaller than the summation of the sizes of the host color frame and the fused watermark depth frame. Therefore, it is clear that the proposed techniques and all presented techniques give good results in minimizing the required channel bandwidth for transmitting the color and depth frames of the transmitted 3DV + D data. Thus, instead of the transmission of the color and depth frames separately needing more transmission bandwidth, we transmit both the color and depth frames on the same channel that has a bandwidth less than that required for transmitting color and depth frames, separately. This is achieved through hiding multiple fused depth frames inside the color frames of the transmitted 3DV + D data. So, the proposed fusion and watermarking techniques improve the capacity of the embedded information, save the transmission bit rate, and subsequently enhance the channel bandwidth-efficiency.

Therefore, it is noticed from all presented objective and subjective results that the proposed hybrid fusion-encryption-watermarking techniques are good candidates for securing the transmission of 3DV + D HEVC data and they can survive different types of multimedia attacks. Moreover, the proposed hybrid techniques save the transmission bit rate by using multiple depth frames within the color frames. So, they minimize the required transmission bandwidth for streaming the 3DV + D HEVC data over the limited-resources networks, and thus they enhance bandwidth-efficiency of the communication channel. The subjective and objective results also prove that there is no remarkable difference between the original and the watermarked frames, which reveals the fidelity of the proposed hybrid fusion-encryption-watermarking techniques.

5 Conclusions

This paper introduced efficient and robust hybrid fusion-encryption-watermarking techniques for 3D-HEVC streams. It also presented a comparative study between these proposed hybrid techniques and the existing state-of-the-art techniques. The

Table 7 Size of the transmitted host, primary, secondary, fused watermark, and watermarked frames for the Shark and PoznanStreet 3DV streams

Watermarking technique	Size of the transmitted frame (Bytes)									
	Shark					PoznanStreet				
	Host color frame	Watermark primary depth frame	Watermark secondary depth frame	Watermark fused depth frame	Watermarked color frame	Host color frame	Watermark primary depth frame	Watermark secondary depth frame	Watermark fused depth frame	Watermarked color frame
DWT + Homomorphic + SVD	38.718	16.384	16.384	16.492	40.960	47.293	12.288	12.288	12.395	49.152
DCT + DSWT	38.718	16.384	16.384	16.492	40.963	47.293	12.288	12.288	12.395	49.158
DCT + DWT [18]	38.718	16.384	16.384	16.492	40.981	47.293	12.288	12.288	12.395	49.319
DWT + SVD [33]	38.718	16.384	16.384	16.492	41.015	47.293	12.288	12.288	12.395	49.865
DCT + SVD [21]	38.718	16.384	16.384	16.492	41.007	47.293	12.288	12.288	12.395	49.748

evaluation metrics for the comparisons on standard 3D-HEVC streams include the stability, reliability, and robustness. Experimental results revealed the superiority of the proposed techniques in maintaining high robustness and fidelity in the presence of different types of attacks compared to the existing hybrid techniques. Also, the proposed techniques achieve high degree of capacity, security, and robustness without affecting on the 3DV perceptual quality in the presence of attacks. They can extract the encrypted, fused, primary, and secondary depth watermark frames with high probability of detection and good quality. Furthermore, the proposed techniques show that the proposed wavelet-based fusion technique can be used as a new way to embed more watermark frames into the watermarking system. Thence, the proposed techniques can be utilized for minimizing the transmission bit rate of the streamed color-plus-depth 3D-HEVC data.

References

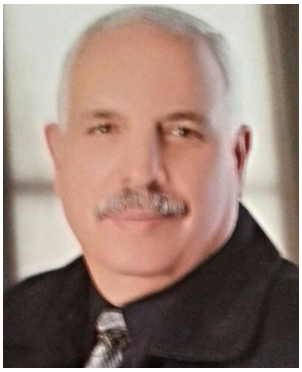
1. Abu-Marie W, Gutub A, Abu-Mansour H (2010) Image based steganography using truth table based and determinate array on rgb indicator. Int J Signal Image Process 1(3):196–204
2. Al-Otaibi A, Gutub A (2014) 2-leyer security system for hiding sensitive text data on personal computers. Lect Notes Inform Theory 2:151–157
3. Al-Otaibi A, Gutub A (2014) Flexible stego-system for hiding text in images of personal computers based on user security priority. In: International Conference on Advanced Engineering Technologies (AET) pp 250–256
4. Alotaibi N, Gutub A, Khan E (2015) Stego-system for hiding text in images of personal computers. In: The 12th learning and technology conference: wearable tech/wearable learning
5. Bhimani J, Mi N, Leeser M, Yang Z (2017) FiM: performance prediction for parallel computation in iterative data processing applications. In: IEEE 10th International Conference on Cloud Computing (CLOUD) pp 359–366
6. Bhimani J, Yang Z, Leeser M, Mi N (2017) Accelerating big data applications using lightweight virtualization framework on enterprise cloud. In: IEEE High Performance Extreme Computing Conference (HPEC) pp 1–7
7. Campisi P (2008) Object-oriented stereo-image digital watermarking. J Electron Imaging 17(4):043024
8. Dutta T, Gupta P (2016) A robust watermarking framework for high efficiency video coding (HEVC)–encoded video with blind extraction process. J Vis Commun Image Represent 38:29–44
9. Dutta T, Sur A, Nandi S (2013) A robust compressed domain video watermarking in P-frames with controlled bit rate increase. In: National Conference on Communications (NCC) pp 1–5
10. Esen E, Alatan A (2011) Robust video data hiding using forbidden zone data hiding and selective embedding. IEEE Trans Circuits Syst Video Technol 21(8):1130–1138
11. Franco-Contreras J, Baudry S, Doërr G (2011) Virtual view invariant domain for 3D video blind watermarking. In: IEEE 18th International Conference on Image Processing (ICIP) pp 2761–2764
12. Gao H, Yang Z, Bhimani J, Wang T, Wang J, Sheng B, Mi N (2017) AutoPath: harnessing parallel execution paths for efficient resource allocation in multi-stage big data frameworks. In: IEEE 26th International Conference on Computer Communication and Networks (ICCCN) pp 1–9
13. Gutub A (2010) Pixel indicator technique for RGB image steganography. J Emerg Technol Web Intell 2(1):56–64
14. Gutub A, Ankeer M, Abu-Ghalioun M, Shaheen A, Alvi A (2008) Pixel indicator high capacity technique for RGB image based Steganography. In: IEEE 5th International Workshop on Signal Processing and its Applications (WoSPA)
15. Gutub A, Al-Juaid N, Khan E (2017) Counting-based secret sharing technique for multimedia applications. Multimed Tools Appl 1–29. https://doi.org/10.1007/s11042-017-5293-6
16. Hartung F, Girod B (1998) Watermarking of uncompressed and compressed video. Signal Process 66(3):283–301
17. HEVC Reference Software (2014) http://hevc.kw.bbc.co.uk/trac/browser/jctvc-hm/tags

18. Joshi M, Gupta S, Girdhar M, Agarwal P, Sarker R (2017) Combined DWT–DCT-based video watermarking algorithm using Arnold transform technique. In: International conference on data engineering and communication technology. Singapore: Springer pp 455–463
19. Khalid A (2017) Utilization of watermarking schemes for securing digital images. Master Thesis, Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University
20. Khan F, Gutub A (2007) Message concealment techniques using image based steganography. In: IEEEGCC
21. Kim D, Lee W, Oh W, Lee K (2012) Robust DT-CWT watermarking for DIBR 3D images. IEEE Trans Broadcast 58(4):533–543
22. Kuo Y, Lo C (2010) A hybrid scheme of robust and fragile watermarking for H.264/AVC video. In: IEEE international symposium on Broadband Multimedia Systems and Broadcasting (BMSB) pp 1–6
23. Lin H, Wu L (2011) A digital blind watermarking for depth-image-based rendering 3D images. IEEE Trans Broadcast 57(2):602–611
24. Mueller K, Vetro A (2014) Common test conditions of 3D-MVV core experiments. Joint Collaborative Team on 3D Video Coding Extensions JCT3V-G1100, 7th Meeting: San Jose, USA
25. Niu Y, Souidene W, Beghdadi A (2011) A visual sensitivity model based stereo image watermarking scheme. In: IEEE 3rd European Workshop on Visual Information Processing (EUVIP) pp 211–215
26. Noorkami M, Mersereau M (2005) Compressed-domain video watermarking for H.264. In: IEEE International Conference on Image Processing (ICIP) pp II–890
27. Noorkami M, Mersereau M (2007) A framework for robust watermarking of H.264-encoded video with controllable detection performance. IEEE Trans Inf Forensics Secur 2(1):14–23
28. Noorkami M, Mersereau M (2008) Digital video watermarking in P-frames with controlled video bit-rate increase. IEEE Trans Inf Forensics Secur 3(3):441–455
29. Ogawa K, Ohtake G (2015) Watermarking for HEVC/H.265 stream. In: IEEE International Conference on Consumer Electronics (ICCE) pp 102–103
30. Parvez T, Gutub A (2011) Vibrant color image steganography using channel differences and secret data distribution. Kuwait J Science Eng 38(1):127–142
31. Purica I, Mora G, Pesquet-Popescu B, Cagnazzo M, Ionescu B (2016) Multiview plus depth video coding with temporal prediction view synthesis. IEEE Trans Circuits Syst Video Technol 26(2):360–374
32. Qiu G, Marziliano P, Ho T, He D, Sun Q (2004) A hybrid watermarking scheme for H. 264/AVC video. In: 17th International Conference on Pattern Recognition (ICPR) pp 865–868
33. Singh D, Singh K (2017) DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. Multimed Tools Appl 76(11):13001–13024
34. Stütz T, Autrusseau F, Uhl A (2014) Non-blind structure-preserving substitution watermarking of H.264/CAVLC inter-frames. IEEE Trans Multimed 16(5):1337–1349
35. Su C, Wu S, Chen F, Wu Y, Wu C (2011) A practical design of digital video watermarking in H.264/AVC for content authentication. Signal Process Image Commun 26(8):413–426
36. Swati S, Hayat K, Shahid Z (2014) A watermarking scheme for high efficiency video coding (HEVC). PLoS One 9(8):e105613
37. Tew Y, Wong K (2014) An overview of information hiding in H.264/AVC compressed video. IEEE Trans Circuits Syst Video Technol 24(2):305–319
38. Wang S, Cui C, Niu X (2014) Watermarking for DIBR 3D images based on SIFT feature points. Measurement 48:54–62
39. Xu D, Wang R, Wang J (2011) A novel watermarking scheme for H.264/AVC video authentication. Signal Process Image Commun 26(6):267–279
40. Yan C, Zhang Y, Xu J, Dai F, Li L, Dai Q, Wu F (2014) A highly parallel framework for HEVC coding unit partitioning tree decision on many-core processors. IEEE Signal Process Lett 21(5):573–576
41. Yan C, Zhang Y, Xu J, Dai F, Zhang J, Dai Q, Wu F (2014) Efficient parallel framework for HEVC motion estimation on many-core processors. IEEE Trans Circuits Syst Video Technol 24(12):2077–2089
42. Yan C, Xie H, Liu S, Yin J, Zhang Y, Dai Q (2018) Effective Uyghur language text detection in complex background images for traffic prompt identification. IEEE Trans Intell Transp Syst 19(1):220–229

43. Yan C, Xie H, Yang D, Yin J, Zhang Y, Dai Q (2018) Supervised hash coding with deep neural network for environment perception of intelligent vehicles. IEEE Trans Intell Transp Syst 19(1):284–295
44. Yang Z, Wang J, Evans D, Mi N (2016) AutoReplica: automatic data replica manager in distributed caching and data processing systems. In: IEEE 35th International Performance Computing and Communications Conference (IPCCC) pp 1-6
45. Yang Z, Hoseinzadeh M, Andrews A, Mayers C, Evans T, Bolt T, Swanson S (2017) AutoTiering: automatic data placement manager in multi-tier all-flash datacenter. In: IEEE 36th International Performance Computing and Communications Conference (IPCCC)
46. Zhang J, Ho T (2006) Efficient video authentication for H.264/AVC. In: first International Conference on Innovative Computing, Information and Control (ICICIC) pp 46–49
47. Zhang J, Ho T, Qiu G, Marziliano P (2007) Robust video watermarking of H.264/AVC. IEEE Trans Circuits Syst II: Express Briefs 54(2):205–209

Walid El-Shafai was born in Alexandria, Egypt, on April 19, 1986. He received the B.Sc degree in Electronics and Electrical Communication Engineering from Faculty of Electronic Engineering (FEE), Menoufia University, Menouf, Egypt in 2008 and M.Sc degree from Egypt-Japan University of Science and Technology (E-JUST) in 2012. He is currently working as a Teaching Assistant and Ph.D. Researcher in ECE Dept. FEE, Menoufia University. His research interests are in the areas of 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, 3D Video Watermarking and Encryption, Error Resilience and Concealment Algorithms for H.264/AVC, H.264/MVC and H.265/HEVC Video Codecs Standards.

El-Sayed M. El-Rabaie Prof. S. El-Rabaie (SM'92) was born in Sires Elian, Egypt, in 1953. He received the B.Sc. degree (with honors) in radio communications from Tanta University, Tanta, Egypt, in 1976, the M.Sc. degree in communication systems from Menoufia University, Menouf, Egypt, in 1981, and the Ph.D. degree in microwave device engineering from Queen's University of Belfast, Belfast, U.K., in 1986. In his doctoral research, he constructed a Computer-Aided Design (CAD) package used in nonlinear circuit simulations based on the harmonic balance techniques. Up to February 1989, he was a Postdoctoral Fellow with the Department of Electronic Engineering, Queen's University of Belfast. He was invited as a Research Fellow in the College of Engineering and Technology, Northern Arizona University, Flagstaff, in 1992 and as a Visiting Professor at Ecole Polytechnique de Montreal, Montreal, QC, Canada, in 1994. He has authored and co-authored more than 300 papers and nineteen textbooks. He was given several awards (Salah Amer Award of Electronics in 1993, The Best Researcher on (CAD) from Menoufia University in 1995). He acts as a reviewer and member of the editorial board for several scientific journals. He has participated in translating the first part of the Arabic Encyclopedia. Professor El-Rabaie was the Head of the Electronics and Communication Engineering Department, Faculty of Electronic Engineering, Menoufia University, and after that the Vice Dean of Postgraduate Studies and Research at the same Faculty. Prof. El-Rabaie is involved now in different research areas including CAD of nonlinear microwave circuits, nanotechnology, digital communication systems, biomedical signal processing, acoustics, antennas, and digital image processing. Now he is reviewer for the Quality Assurance and Accreditation of Egyptian for Higher Education. E-mail: srabie1@yahoo.com, Mobile: 0020128498170.



M. El-Halawany received the M.Sc. degree in electrical engineering from Menoufia University in Egypt in 1982. He received the Ph.D. degree from Wroclaw University in 1989. He is a Professor Emeritus in the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University. His areas of interest are signal processing, image processing, and digital communications.

Fathi E. Abd El-Samie received the B.Sc. (Honors), M.Sc., and Ph.D. degrees from Menoufia University, Menouf, Egypt, in 1998, 2001, and 2005, respectively. He is a Professor at the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Egypt. He is a co-author of several papers and textbooks. 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. Dr. Abd El-Samie was a recipient of the Most Cited Paper Award from the Digital Signal Processing journal in 2008.